Overview

Citrix SecurSpaces™ es un entorno de desarrollo seguro basado en la nube (CDE) diseñado para mejorar la productividad de los desarrolladores mientras mantiene una seguridad de nivel empresarial. Su propósito es optimizar el aprovisionamiento y la gestión de entornos de codificación, para que las organizaciones puedan aumentar la eficiencia y la colaboración entre equipos internos y externos. equipos.

Ofrece una incorporación rápida a través de espacios de trabajo preconfigurados basados en contenedores que son accesibles desde cualquier lugar, lo que lo hace ideal para equipos híbridos y remotos. La plataforma se puede implementar en nubes públicas o privadas y en servidores autohospedados, y admite un funcionamiento totalmente aislado para entornos de alta seguridad.

Al centralizar los recursos de desarrollo y eliminar las dependencias locales, SecurSpaces ayuda a proteger el código fuente, las credenciales y la propiedad intelectual. Aplica controles de acceso y se integra con modelos de seguridad como Zero Trust, lo que reduce el riesgo de fugas de datos y respalda las prácticas de DevSecOps. prácticas.

La plataforma también ayuda a reducir los costes de portátiles de alta especificación, mantenimiento y software de seguridad, al tiempo que proporciona visibilidad y gobernanza en tiempo real sobre el ciclo de vida del desarrollo. Sus entornos se integran con herramientas DevOps comunes y flujos de trabajo CI/CD.

Otros nombres que verá

Otros dos nombres aparecen en el producto y en su entorno. Ambos se refieren a SecurSpaces.

NOMBRE	DÓNDE LO ENCONTRARÁ
Espacios de desarrollador seguros	La extensión SSH para IDE basados en VS Code se publica como **Citrix Secure Developer Spaces - Remote SSH**, y la barra lateral que añade lleva el mismo nombre. Los dominios de implementación utilizan la forma abreviada, como en `assets.sds.citrix.com`.

NOMBRE	DÓNDE LO ENCONTRARÁ
Strong Network™	El nombre de la plataforma antes de que Citrix la adquiriera. Sobrevive en identificadores que no se pueden renombrar sin romper las implementaciones existentes: el directorio `strong_network_startup` que debe proporcionar una imagen, las rutas `/strong/` dentro de un espacio de trabajo y las imágenes `strongnetwork` en Docker Hub.

Dónde ir a continuación

SI DESEA	EMPIECE AQUÍ
Consulte las especificaciones, los límites y con qué se integra	SecurSpaces de un vistazo
Comprenda lo que la plataforma hace por los desarrolladores	SecurSpaces para desarrolladores
Vea cómo encajan las piezas	Arquitectura
Cree su primer espacio de trabajo	Cree su primer espacio de trabajo
Implemente la plataforma	Requisitos del sistema
Comprenda cómo está estructurada la plataforma	Conceptos
Conceda acceso a esta documentación a un asistente de IA	Conceda acceso a su asistente de IA

Para asistentes y agentes de IA

Esta documentación se publica en el formato llms.txt:

- Índice: https://assets.sds.citrix.com/llms.txt
- Corpus completo: https://assets.sds.citrix.com/llms-full.txt

Si ejecuta SecurSpaces, su propia instancia sirve los mismos archivos en `/docs/llms.txt` y `/docs/llms-full.txt`, coincidiendo con su versión implementada. Consulte Dé acceso a su asistente de IA.

About SecurSpaces

Esta sección explica qué es Citrix SecurSpaces™, para quién es y cómo funciona.

PÁGINA	QUÉ CUBRE
SecurSpaces para desarrolladores	Qué es un espacio de trabajo, qué cambia en su día a día y qué permanece igual.
SecurSpaces para ingenieros de IA y ML	Espacios de trabajo con soporte de GPU, grandes asignaciones de recursos, datos de entrenamiento compartidos y acceso gobernado a proveedores de IA.
SecurSpaces de un vistazo	Plataformas compatibles, límites, integraciones y modelos de implementación en una sola página.
Cómo funciona	El plano de control, los espacios de trabajo y el servicio de proxy que componen la plataforma, y cómo se inicia un espacio de trabajo.
Conceptos	Cómo encajan la plataforma, las organizaciones, los proyectos y los espacios de trabajo.
SecurSpaces Flex	Un servicio administrado por Citrix en Azure que ofrece espacios de trabajo Linux seguros a través de Citrix Platform Flex.
Vídeos	Testimonios, demostraciones de productos y seminarios web grabados para SecurSpaces.

SecurSpaces for developers

`Developer`

Citrix SecurSpaces™ le proporciona un entorno de desarrollo potente y preconfigurado que puede abrir en segundos, desde cualquier dispositivo, cualquier navegador o su IDE favorito. Piense en ello como su propia máquina de desarrollo Linux dedicada, siempre lista, siempre consistente y accesible desde cualquier lugar.

Esta guía explica qué es SecurSpaces, cómo se compara con lo que está acostumbrado y presenta los conceptos clave que encontrará.

Cómo funciona

Su espacio de trabajo es un entorno de desarrollo Linux completo que se ejecuta en la nube. Tiene todo lo que su proyecto necesita — IDE, terminal, código fuente, herramientas de compilación y dependencias — configurado y listo para usar. Se conecta a él desde su navegador o un IDE instalado localmente.

Cuando inicie sesión en SecurSpaces, verá su proyecto y las plantillas de espacio de trabajo disponibles. Elige una plantilla, selecciona iniciar y, en cuestión de segundos, tendrá un entorno en ejecución con sus repositorios clonados, sus herramientas instaladas y su IDE conectado. Eso es todo, ya está programando.

Qué le ofrece

Empiece a programar en minutos, no en días

Se acabó el "instala esto, configura aquello, pide acceso a Dave". Su espacio de trabajo viene precargado con todo lo que su proyecto necesita: los tiempos de ejecución de lenguaje correctos, las herramientas de compilación, las dependencias y el acceso al repositorio ya están configurados.

Sus herramientas, a su manera

Utilice sus archivos de configuración (dot files), extensiones, atajos de teclado y configuración de shell. SecurSpaces es compatible con VS Code (navegador y escritorio), IDE de JetBrains, Cursor, Windsurf, Kiro y cualquier otro editor que se conecte a través de SSH. Usted elige cómo trabajar.

Cualquier dispositivo se convierte en una máquina de desarrollo

Trabaje desde su portátil, un cliente ligero, una tableta o incluso una máquina prestada. Su espacio de trabajo es el mismo en todas partes porque se ejecuta en la nube, no en su hardware local.

Potencia cuando la necesite

¿Necesita más CPU para una compilación pesada? ¿GPU para el entrenamiento de ML? Escale los recursos bajo demanda, sin necesidad de solicitar hardware. Su espacio de trabajo puede ser más potente que cualquier portátil.

Experimenta libremente

Crea un nuevo espacio de trabajo en segundos. Prueba algo arriesgado, rómpelo, deséchalo, empieza de nuevo. El coste de experimentar es casi nulo.

Entornos consistentes en todo el equipo

Todos en tu proyecto usan las mismas herramientas base, las mismas versiones, la misma configuración. Si funciona en tu espacio de trabajo, funciona en el de todos. El «funciona en mi máquina» deja de ser un problema.

Lo que permanece igual

Si vienes de un flujo de trabajo basado en un portátil, VDI o WSL, la mayor parte de lo que sabes sigue siendo aplicable:

- **Flujo de trabajo de Git** — Clonar, ramificar, confirmar, enviar. Lo mismo de siempre.
- **Terminal** — Shell completo de Linux con tus herramientas, alias y scripts.
- **IDE** — Conecta tu IDE de escritorio o usa la versión basada en navegador. Tú eliges.
- **Tus archivos** — Todo lo que guardes en tu directorio de inicio persiste entre sesiones.
- **Acceso root** — Tienes control total dentro de tu espacio de trabajo.

Qué es diferente

SecurSpaces cambia *dónde* ocurre tu desarrollo, no *cómo* desarrollas. Esto es lo que realmente es diferente:

CONFIGURACIÓN TRADICIONAL	CON SECURSPACES
El código reside en tu portátil	El código reside en tu espacio de trabajo en la nube (no lo puedes perder si tu portátil falla)
Instalas y mantienes tus propias herramientas	El propietario de tu proyecto configura el entorno base en una plantilla

CONFIGURACIÓN TRADICIONAL	CON SECURSPACES
El hardware limita lo que puedes construir	Los recursos del espacio de trabajo escalan independientemente de tu dispositivo
La configuración del entorno lleva horas o días	Inicia un espacio de trabajo preconfigurado en segundos
Depuración de "Funciona en mi máquina"	Todos comparten el mismo entorno base
Incorporación a un nuevo proyecto = configuración manual	Elige una plantilla y empieza a programar

El cambio de mentalidad clave: Tu portátil (o navegador) es una *ventana* a tu espacio de trabajo, no el espacio de trabajo en sí. Todo se ejecuta en la nube; tu dispositivo es solo la pantalla.

Terminología clave

Estos son los términos que verás al usar SecurSpaces:

TÉRMINO	SIGNIFICADO
Espacio de trabajo	Su entorno personal de desarrollo en la nube. Contiene su IDE, código, herramientas y terminal. Puede tener varios espacios de trabajo para diferentes proyectos o ramas.
Plantilla	Un esquema de espacio de trabajo preconfigurado creado por el propietario de su proyecto. Define la imagen del contenedor, las herramientas, los repositorios y la asignación de recursos para que pueda empezar inmediatamente sin configuración manual.
Proyecto	Una unidad organizativa que agrupa espacios de trabajo, usuarios y recursos relacionados. El propietario de su proyecto le asigna a uno o más proyectos.
Propietario del proyecto	La persona que gestiona la configuración de su proyecto: plantillas, recursos, controles de acceso y miembros del equipo. Es su primer

TÉRMINO	SIGNIFICADO
	punto de contacto para preguntas específicas del proyecto.
Perfil	Su configuración personal: horario de trabajo, credenciales de Git, configuración de shell, secretos y preferencias del IDE. Se aplican a todos sus espacios de trabajo.
Integraciones	Conexiones a servicios externos (GitHub, GitLab, Bitbucket, Azure DevOps) que permiten a sus espacios de trabajo acceder a los repositorios de código sin problemas.
Aplicaciones del espacio de trabajo	Aplicaciones que se ejecutan dentro de su espacio de trabajo (como un servidor de desarrollo) a las que puede acceder desde su navegador o compartir con sus compañeros de equipo.
IDE en la nube	El editor VS Code basado en navegador integrado en SecurSpaces. No requiere instalación, solo selecciónelo para abrirlo.

Cómo SecurSpaces encaja en su día a día

Un día típico con SecurSpaces es así:

1. **Empiece su día.** Abra su navegador o IDE. Su espacio de trabajo puede que ya esté en ejecución (según su horario de trabajo) o se iniciará en segundos cuando se conecte.
2. **Escriba código.** Obtenga los últimos cambios, trabaje en su característica, ejecute pruebas, tal como lo haría en una máquina local.
3. **Previsualice y comparta.** Ejecute su aplicación y acceda a ella a través de las aplicaciones del espacio de trabajo. Comparta una vista previa en vivo con sus compañeros de equipo sin necesidad de desplegarla en ningún sitio.
4. **Termine su día.** Cierre su navegador o IDE. Su espacio de trabajo se pausa automáticamente según su horario, ahorrando recursos. Todo estará ahí cuando regrese.

Preguntas frecuentes

¿Es esto solo VDI para desarrolladores? No. VDI transmite una imagen de escritorio a su dispositivo. SecurSpaces le proporciona un entorno de desarrollo Linux real: acceso completo a la terminal, permisos de root, conectividad IDE nativa y la capacidad de ejecutar contenedores y servicios dentro de su espacio de trabajo. Está diseñado para flujos de trabajo de desarrollo, no para virtualización de escritorio.

¿Pierdo mi trabajo cuando cierro el navegador? No. Su directorio de inicio (`/home/developer`) es persistente. Los archivos, el código y las configuraciones se guardan entre sesiones. Sin embargo, los cambios a nivel de sistema fuera de `/home/developer` se restablecen cuando se reinicia un espacio de trabajo; use scripts de inicio o pida al propietario de su proyecto que actualice la plantilla para esos casos.

¿Puedo usar mis propios archivos de configuración y ajustes de IDE? Sí. SecurSpaces admite configuraciones de shell personales (`.bashrc`, `.zshrc`), ajustes de IDE, extensiones de VS Code y scripts de inicio. Configure esto una vez en su perfil y se aplicará a cada espacio de trabajo.

¿Puedo trabajar sin conexión? No, los espacios de trabajo de SecurSpaces requieren una conexión de red ya que se ejecutan en la nube. Si pierde la conectividad, su trabajo se guarda hasta el último cambio, y puede volver a conectarse y reanudar donde lo dejó.

¿Qué pasa con las restricciones de seguridad? Su organización puede aplicar políticas de seguridad específicas (como controles de portapapeles o restricciones de red). Estas son configuradas por su administrador de plataforma para proteger código y datos sensibles. Si encuentra una restricción que no comprende, pregunte al propietario de su proyecto o al administrador de la plataforma.

Próximos pasos

¿Listo para empezar?

1. Inicio rápido: Configure su cuenta — Configure su perfil, acceso a Git y credenciales.
2. Inicio rápido: Cree y conéctese a su espacio de trabajo — Inicie su primer espacio de trabajo y conecte su IDE.

SecurSpaces for AI and ML engineers

`AI/ML Engineer`

Citrix SecurSpaces™ le proporciona un entorno Linux con tanta capacidad de cómputo como su clúster pueda ofrecer, GPUs conectadas cuando las necesite, y acceso compartido a los datos de entrenamiento que no tienen que copiarse en su portátil.

Las partes importantes para el trabajo con modelos son las mismas que importan para cualquier trabajo de desarrollo: el entorno es desechable, los datos no lo son, y ninguno de los dos sale de la plataforma.

Si es nuevo en SecurSpaces, SecurSpaces para desarrolladores cubre los conceptos básicos de los espacios de trabajo, las plantillas y la conexión de un IDE. Esta página cubre lo que es diferente sobre el entrenamiento y la experimentación.

Cómo funciona

Un espacio de trabajo es un entorno Linux dimensionado a partir de una especificación que define el administrador de su plataforma, por lo que la CPU, la memoria, el disco y las GPUs que obtiene se solicitan en lugar de poseerse. Un espacio de trabajo con GPU se programa en un nodo del clúster compatible con GPU cuando lo inicia, y se libera cuando lo detiene.

Los datos de entrenamiento se acceden donde ya residen. En lugar de copiar un conjunto de datos en el espacio de trabajo, adjunta un punto de montaje para leerlo in situ, o un cubo de datos si necesita una instantánea fijada en una versión conocida. Un servidor de notebooks o un punto final de inferencia que ejecute dentro del espacio de trabajo se publica a través de una aplicación de espacio de trabajo, lo que lo sitúa detrás de una URL autenticada en lugar de un puerto abierto. Las solicitudes salientes a los servicios de IA salen a través de la plataforma, de modo que pueden atribuirse y gobernarse.

Las secciones siguientes cubren cada uno de estos puntos a su vez.

Qué te ofrece

Los datos no tienen que moverse

Los datos de entrenamiento permanecen en su almacenamiento y en su clúster. Nada se clona en un portátil, lo que a menudo es la razón principal por la que un equipo adopta la plataforma en primer lugar.

Otra persona puede reproducir tu ejecución

Una plantilla fija la imagen, la cadena de herramientas y los recursos, de modo que un experimento que un colega repita comienza desde el mismo punto que el suyo.

Las GPUs no están en la máquina de una sola persona

Un nodo GPU sirve a quien lo necesite. Solicitas el hardware para la ejecución en lugar de poseerlo.

El acceso se rige sin que usted lo gestione

El acceso al repositorio, los secretos, el tráfico del proveedor de IA y la red saliente se controlan y auditan de forma centralizada, para que no sea usted quien tenga las credenciales.

Computación

Un espacio de trabajo se dimensiona a partir de una especificación que define su administrador de plataforma. Los límites del producto son:

RECURSO	MÁXIMO
CPU	1000 núcleos
Memoria	10.000 GiB
Disco	10.000 GiB
GPU	1000

Estos son los límites que impone la plataforma. Lo que realmente puede solicitar es lo que su administrador haya puesto a disposición en una especificación de espacio de trabajo, limitado por el hardware del clúster. Si el tamaño que necesita no se ofrece, es una conversación con su administrador de plataforma en lugar de un límite del producto.

Las GPU se solicitan como un recuento en la especificación y se programan en nodos con capacidad de GPU. Para saber cómo un administrador de plataforma las proporciona, consulte Espacios de trabajo habilitados para GPU en AKS.

Datos de entrenamiento

Copiar un conjunto de datos en cada espacio de trabajo es lento y duplica datos que quizás no tenga permitido duplicar. SecurSpaces ofrece dos formas de evitarlo, y se comportan de manera diferente.

	PUNTOS DE MONTAJE	CUBOS DE DATOS
Cómo llegan los datos	Una conexión en vivo al almacenamiento externo	Una instantánea copiada en el clúster
Ediciones compartidas	Inmediatamente visible para cada espacio de trabajo que lo utiliza	Requiere un ciclo de publicación
Duplicación	Ninguna — los datos permanecen en el almacenamiento externo	Cada instantánea se replica
Control de versiones	Utilice lo propio del proveedor de almacenamiento	Integrado

Para un conjunto de datos que varios equipos leen, un **punto de montaje** suele ser la elección correcta: es almacenamiento de archivos POSIX montado en el espacio de trabajo, no hay cuota de tamaño por montaje y no se copia nada. Para un conjunto de datos que desea fijar en una versión conocida, un **cubo de datos** le ofrece eso.

Consulte Elija entre cubos de datos y puntos de montaje.

Un punto de montaje es infraestructura compartida: cada espacio de trabajo que lo monta trabaja con los mismos archivos en vivo. Planifique las copias de seguridad y la retención en el proveedor de almacenamiento, junto con el resto de su plataforma de datos. Consulte Límites y comportamiento de los puntos de montaje.

Cuadernos y trabajos de larga duración

Se puede acceder a un servidor de cuadernos, un panel de control o un punto final de inferencia que se ejecute en su espacio de trabajo a través de una aplicación de espacio de trabajo, que publica un puerto a través de una URL autenticada. Consulte Compartir una aplicación en ejecución.

Los espacios de trabajo se pausan cuando están inactivos, lo que evita que el tiempo de GPU se gaste en entornos que nadie está utilizando. Para un trabajo que se ejecuta sin supervisión —una ejecución de entrenamiento nocturna, una evaluación de lotes larga—, pida a un administrador de plataforma o a un oficial de seguridad que active **Omitir programación** para ese espacio de trabajo. El espacio de trabajo seguirá ejecutándose hasta que lo detenga. Consulte Detección de inactividad del espacio de trabajo.

Acceso a proveedores de IA

El tráfico de los espacios de trabajo a los servicios de IA puede enrutarse a través de una Pasarela de IA interna. Cuando está configurada, las solicitudes llevan encabezados que identifican al usuario, el proyecto y el espacio de trabajo, de modo que el uso es atribuible y se puede informar sobre él.

Esta es una integración a nivel de plataforma, no algo que usted configure. Consulte Pasarela de IA.

El acceso saliente también se rige por la política de red, por lo que los dominios a los que puede acceder un espacio de trabajo —incluidos los registros de modelos y paquetes— pueden estar restringidos. Si una descarga está bloqueada, esa es la razón. Consulte Políticas de red.

Próximos pasos

- Configurar su cuenta
- Su primer espacio de trabajo
- Qué persiste en un espacio de trabajo
- Gestionar cadenas de herramientas del espacio de trabajo

SecurSpaces at a glance

Un resumen de en qué se ejecuta Citrix SecurSpaces™, con qué se integra y dónde están sus límites, para cualquiera que decida si se adapta a su entorno.

Cada cifra aquí es propiedad de otra página, que está vinculada desde su fila. Siga el enlace cuando necesite los detalles o las advertencias.

Dónde se ejecuta

Modelo de implementación	Autohospedado en su propio clúster de Kubernetes, en su nube, en las instalaciones o completamente aislado (air-gapped)
Alternativa gestionada	SecurSpaces Flex, un servicio operado por Citrix facturado a través de créditos de Platform Flex

Kubernetes	1.34 o posterior, en un clúster dedicado a SecurSpaces
Arquitectura de nodo	`amd64` solamente. `arm64`, incluido AWS Graviton, no es compatible
Plataformas certificadas	Amazon EKS, Azure AKS, Google GKE, Red Hat OpenShift, VMware Tanzu Kubernetes Grid, Nutanix Kubernetes Platform

Consulte Requisitos del sistema.

Qué necesita de su infraestructura

Ingress	NetScaler CPX recomendado y desplegable mediante el gráfico; NGINX, HAProxy y la API de puerta de enlace de Kubernetes también son compatibles
Base de datos	MongoDB, ya sea gestionado como Atlas, o desplegado en el clúster
Registro	Cualquier registro compatible con OCI, por ejemplo, Amazon ECR, Azure Container Registry, Google Artifact Registry o JFrog Artifactory
DNS y TLS	Dos dominios con certificados válidos, uno de ellos un comodín para el proxying del espacio de trabajo

Consulte Ingress y Requisitos del sistema.

Con qué se integra

Proveedores de identidad	SAML 2.0, OpenID Connect, Google OAuth, Microsoft Entra ID
Aprovisionamiento de usuarios	SCIM

Repositorios de código	GitHub, GitLab, Bitbucket, Azure DevOps, cada uno autoalojado o gestionado
Secretos	Almacenamiento de secretos integrado, o HashiCorp Vault
Artefactos	JFrog Artifactory
Portal para desarrolladores	Plugin de Backstage
Aplicaciones y escritorios virtuales	Citrix DaaS
Tráfico de IA	Enrutado a través de una puerta de enlace de IA con atribución por usuario

Consulte Identidad y acceso y Integraciones.

Cómo los desarrolladores acceden a un espacio de trabajo

En el navegador	IDE en la nube basado en VS Code
Desde un IDE local	A través de SSH, desde VS Code Desktop, JetBrains Gateway, Cursor, Windsurf o Kiro
Escritorio gráfico	Disponible a través de una imagen de espacio de trabajo habilitada para GUI
Aplicación publicada	A través de Citrix DaaS

Consulte Desarrollar en un espacio de trabajo.

Automatización

La plataforma se puede operar como código, así como a través de la consola, lo cual es importante si gestiona entornos con un equipo de plataforma en lugar de hacerlo manualmente.

API REST	Cubre lo que cubre la consola: espacios de trabajo, proyectos, organizaciones, recursos, usuarios e informes. Autenticado con una

	clave de API. Habilitado por un indicador de función de plataforma
Proveedor de Terraform	Gestiona usuarios, organizaciones, proyectos, grupos y plantillas de espacios de trabajo. Distribuido a través de su implementación en lugar del registro público
Implementación	Valores de Helm y la CLI de Strong Installer, para que la configuración del clúster resida en el control de versiones

Consulte API, proveedor de Terraform y Instalar con la CLI de Strong Installer.

Límites

CPU por espacio de trabajo	1000 núcleos
Memoria por espacio de trabajo	10 000 GiB
Disco por espacio de trabajo	10 000 GiB
GPU por espacio de trabajo	1000
Usuarios y espacios de trabajo	Sin límite de usuarios. SecurSpaces se incluye en la Citrix Platform License, sin nueva SKU

Estos son los límites máximos del producto, no recomendaciones. Lo que puede solicitar está limitado por el hardware de su clúster. Consulte Dimensionamiento.

> **Nota:**
>
> Los espacios de trabajo son contenedores Linux, por lo que las cadenas de herramientas que requieren macOS o hardware de Apple — iOS, iPadOS, macOS, desarrollo de watchOS y tvOS — no pueden ejecutarse en SecurSpaces. Esta es una propiedad de la plataforma, no una deficiencia de la misma.

Escala indicativa

IMPLEMENTACIÓN	NODOS DE SERVICIO	NODOS DE ESPACIO DE TRABAJO	BASE DE DATOS
50 desarrolladores, prueba de concepto	Uno de 8 vCPU / 32 GiB	8 vCPU / 32 GiB, autoescalado	20 GiB
500 desarrolladores	Dos de 8 vCPU / 32 GiB	16 vCPU / 64 GiB, autoescalado	100 GiB

Los nodos de espacio de trabajo escalan según cuántos espacios de trabajo se ejecuten *simultáneamente*, no cuántos existan, por lo que la detección de inactividad es la mayor palanca individual para el coste. Consulte Dimensionamiento.

Seguridad y gobernanza

Código fuente	Permanece en el espacio de trabajo; nunca llega al punto final
Herramientas	Los desarrolladores no ensamblan sus propios entornos. Un espacio de trabajo se crea a partir de una plantilla propiedad de la plataforma y con control de versiones que fija la imagen, las cadenas de herramientas, las fuentes de paquetes y las extensiones, de modo que cada espacio de trabajo creado a partir de ella es idéntico
Control de red	Políticas de egreso por espacio de trabajo, aplicadas en el proxy
Protección de datos	Controles de portapapeles, descarga y carga
Auditoría	Cada acción registrada, exportable a un SIEM, conservada en la plataforma durante 360 días
Controles	31 controles identificados en 8 dominios, en el catálogo de controles

Con la plataforma Citrix más amplia	DaaS, Secure Private Access y Chrome Enterprise Premium añaden controles en la ruta de acceso delante de un espacio de trabajo. Consulte Controles por capas

Consulte Seguridad y cumplimiento.

Pruébalo

Evaluación más rápida	La VM de 1 clic ejecuta toda la plataforma en una única máquina virtual, sin necesidad de clúster
Prueba de producción	Implementar en un clúster y seguir la instalación estándar

Consulta Implementar un entorno de evaluación y Plataformas de Kubernetes.

Información relacionada

- Cómo funciona
- Requisitos del sistema
- Dimensionamiento
- Seguridad y cumplimiento

How it works

Citrix SecurSpaces™ es una plataforma nativa de la nube para alojar entornos de desarrollo en la nube (CDE). Se ejecuta completamente en Kubernetes, ya sea en su propia cuenta en la nube o en su propio hardware, y puede funcionar de forma totalmente aislada (air-gapped). Los entornos de desarrollo están en contenedores y se basan en Linux, y no se instala nada en el dispositivo del desarrollador.

La plataforma consta de tres partes:

- **El plano de control.** Un conjunto de microservicios y una base de datos de configuración. El plano de control contiene organizaciones, proyectos, políticas, recursos y el estado del espacio de trabajo. No contiene el código del desarrollador.
- **Espacios de trabajo.** Cada espacio de trabajo es un pod de Kubernetes que ejecuta una imagen de contenedor, con su propia CPU, memoria y asignación de disco. Los espacios de trabajo se crean a partir de plantillas, se pausan cuando están inactivos y se eliminan según su configuración de retención.
- **El servicio de proxy de SecurSpaces.** Todo el tráfico que sale de un espacio de trabajo pasa a través de él — HTTP y HTTPS, TCP y UDP, DNS y SSH. Aquí es donde se inyectan las credenciales, se aplica la política de red y se registra el tráfico.

Dado que cada ruta de entrada y salida de un espacio de trabajo termina en el servicio de proxy de SecurSpaces, la plataforma puede dar a los desarrolladores acceso a repositorios, registros y servicios internos sin necesidad de colocar credenciales de larga duración en el dispositivo del desarrollador.

Cómo se conectan los desarrolladores

Los desarrolladores acceden a un espacio de trabajo de dos maneras:

- **En el navegador.** VS Code para la Web se sirve desde el espacio de trabajo a través de HTTPS. No se instala localmente, por lo que se puede utilizar cualquier dispositivo administrado o no administrado.
- **Desde un IDE o terminal local.** VS Code Desktop, JetBrains Gateway, Cursor, Kiro y Windsurf se conectan a través de SSH, al igual que un terminal simple.

La ruta del navegador es la que admite el conjunto completo de controles de prevención de pérdida de datos, porque la plataforma renderiza la sesión. Consulte Conectarse a través de SSH, y IDE compatibles para ver las versiones y limitaciones.

Descripción general de los componentes

La siguiente tabla describe los componentes arquitectónicos clave y las tecnologías que cada uno admite.

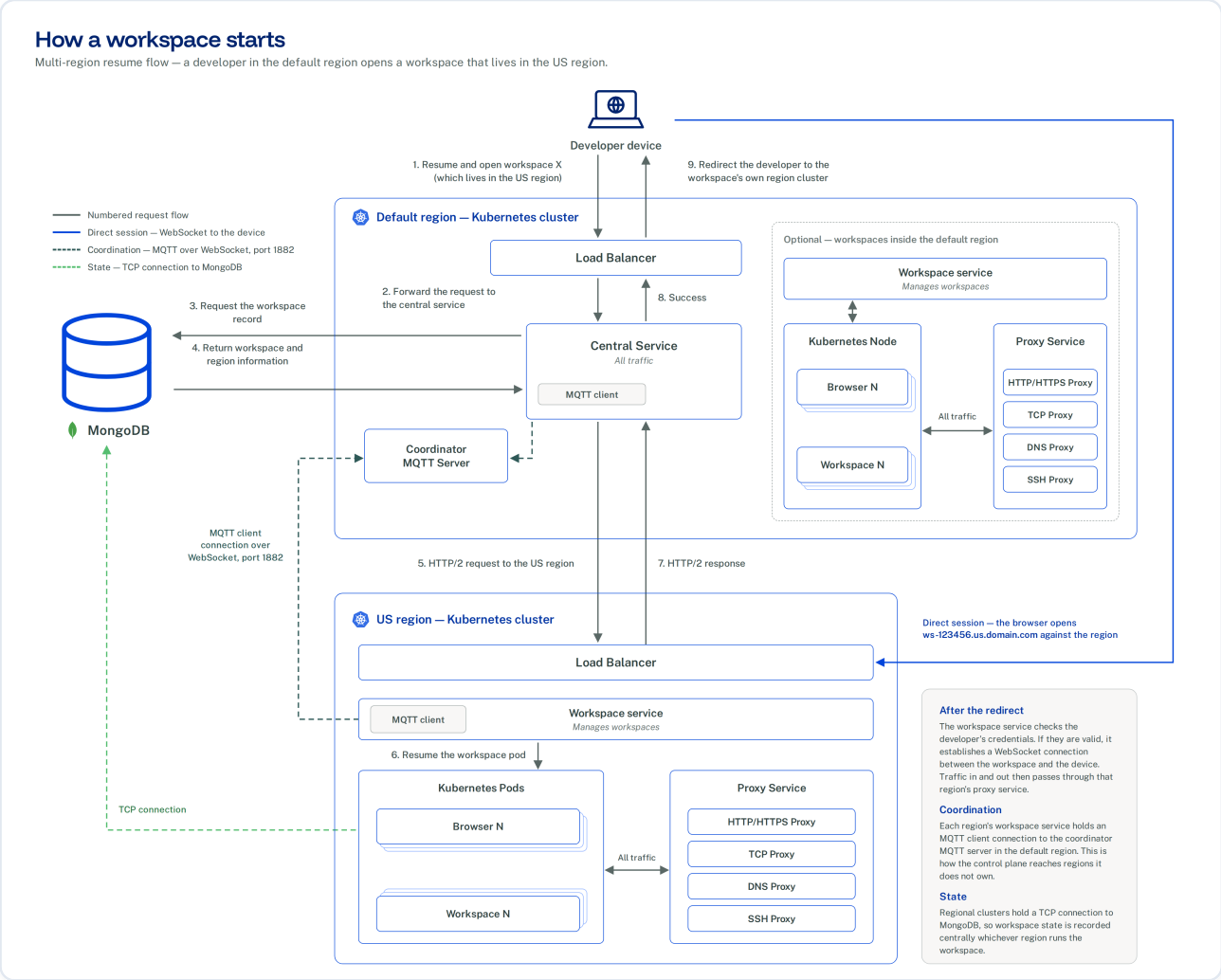
COMPONENTE	DESCRIPCIÓN	TECNOLOGÍAS COMPATIBLES
Plataforma	Entorno nativo de la nube, basado en contenedores (CDE)	Kubernetes o Red Hat OpenShift. Consulte las Guías de implementación.
Balanceo de carga	Gestión del tráfico y control de entrada	NetScaler CPX (recomendado y desplegado por el gráfico de SecurSpaces), NGINX, HAProxy o la API de Kubernetes Gateway.
Base de datos	Almacenamiento de metadatos y estado del espacio de trabajo	MongoDB
Autenticación	Integración de proveedor de identidad y multifactor	Google OAuth, Microsoft OAuth, SAML, SCIM y OpenID Connect (OIDC).
Código fuente	Integraciones con sistemas de control de versiones	GitHub, GitLab y Bitbucket (autohospedado y gestionado); Azure DevOps (gestionado).
Artefactos	Gestión de imágenes de contenedor y almacenamiento de credenciales	Cualquier registro de contenedores compatible con OCI (por ejemplo, JFrog Artifactory, Amazon ECR o Google Artifact Registry); HashiCorp Vault para secretos y credenciales.
Registros	Telemetría del sistema y del espacio de trabajo	Análisis del sistema y el Catálogo de registros de eventos para pistas de auditoría. Admite la integración SIEM utilizando el formato de evento común (CEF).

Para el dimensionamiento de la infraestructura y los requisitos de red, consulte Requisitos del sistema.

Cómo se inicia un espacio de trabajo

Una implementación de una sola región resuelve un espacio de trabajo dentro de un clúster. Una implementación multirregión puede colocar un espacio de trabajo en una región cercana al desarrollador, o en una región requerida por las reglas de residencia de datos, manteniendo un único plano de control y un único punto de entrada.

El siguiente diagrama muestra a un desarrollador en la región predeterminada abriendo un espacio de trabajo que reside en la región de EE. UU. región.



El diagrama numera esta secuencia del 1 al 4 y del 6 al 10.

1. El desarrollador reanuda y abre un espacio de trabajo. La solicitud llega al balanceador de carga en la región predeterminada.
2. El balanceador de carga reenvía la solicitud al servicio central.
3. El servicio central solicita el registro del espacio de trabajo a MongoDB.

4. MongoDB devuelve la información del espacio de trabajo, incluida la región a la que pertenece el espacio de trabajo.
5. El servicio central envía una solicitud HTTP/2 al clúster en la región de EE. UU.
6. El servicio de espacio de trabajo en esa región reanuda el pod del espacio de trabajo.
7. La región devuelve una respuesta HTTP/2.
8. La región predeterminada informa del éxito.
9. El desarrollador es redirigido al clúster en la propia región del espacio de trabajo.

El navegador del desarrollador abre entonces la URL del espacio de trabajo directamente contra esa región, por ejemplo `ws-123456.us.domain.com`. El servicio del espacio de trabajo comprueba las credenciales del desarrollador y, si son válidas, establece una conexión WebSocket entre el espacio de trabajo y el dispositivo. A partir de ese momento, la sesión se ejecuta contra el clúster regional, y el tráfico de entrada y salida del espacio de trabajo pasa a través del servicio de proxy de SecurSpaces en esa región.

Dos canales de soporte se ejecutan continuamente y no forman parte de la secuencia numerada:

- **Coordinación.** El servicio de espacio de trabajo en cada región mantiene una conexión de cliente MQTT con el servidor MQTT coordinador en la región predeterminada, a través de WebSocket en el puerto 1882. Aparece en el diagrama como el enlace WebSocket sin numerar. Así es como el plano de control llega a las regiones que no posee.
- **Estado.** Los clústeres regionales mantienen una conexión TCP con MongoDB, por lo que el estado del espacio de trabajo se registra de forma centralizada, independientemente de la región que ejecute el espacio de trabajo.

Los espacios de trabajo también pueden ejecutarse en la región predeterminada. Esto es opcional, y una implementación puede mantener la región predeterminada solo para el plano de control.

Guías de implementación

SecurSpaces se puede implementar en cualquier infraestructura compatible con Kubernetes, incluyendo la nube pública, hardware local y entornos híbridos. Las siguientes guías cubren objetivos de implementación comunes:

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Red Hat OpenShift

Para evaluar SecurSpaces en una única VM, consulte Implementar un entorno de evaluación.

La VM de 1 clic

Una instalación de producción de SecurSpaces se ejecuta en un clúster de Kubernetes que usted construye, con un registro y una base de datos que usted proporciona. Esa es la forma adecuada para usuarios reales, y demasiado trabajo para una evaluación. La VM de 1 clic elimina ese trabajo al ejecutar toda la plataforma en una única máquina virtual: un clúster K3s de un solo nodo con los servicios de la plataforma, la base de datos y el ingreso de NetScaler.

El mismo instalador lo construye de dos maneras. En la nube, el instalador crea la propia VM con Terraform y configura DNS y TLS. Para una VM local, el instalador no puede acceder a su hipervisor, por lo que genera un script de implementación en su lugar. Usted ejecuta el script en la VM, y el instalador asigna un nombre de host `try.sds.citrix.com` a la dirección IP de la VM. El nombre de host es lo que hace que el certificado TLS sea válido, por lo que lo usa en lugar de la dirección IP.

Debido a esta división, una implementación local implica dos máquinas. El host del instalador prepara la implementación, y el host de destino la ejecuta. Se mantienen separadas porque el host de destino debe comenzar limpio: el script instala su propio K3s y tiempo de ejecución de contenedores, y entra en conflicto con cualquier otro que ya esté allí.

La desventaja es una plataforma sin redundancia y sin ruta de actualización. La VM de 1 clic está diseñada para ser creada, evaluada y desechada. Un piloto con usuarios reales debe estar en un clúster. Consulte Implementar en un clúster.

Información relacionada

- Cómo funciona el servicio de proxy de SecurSpaces
- Límites de confianza y flujos de datos
- Conceptos clave
- Requisitos del sistema

Concepts

Citrix SecurSpaces™ se organiza en cuatro niveles anidados. Casi todo en esta documentación —permisos, recursos, configuraciones de seguridad— se define en uno de ellos y se aplica a todo lo que está por debajo.

```
Platform
└── Organization
    └── Project
        └── Workspace
```

Los cuatro niveles

NIVEL	QUÉ ES	QUIÉN TRABAJA EN ESTE NIVEL
Plataforma	La implementación en su conjunto y la base para todo lo que contiene	Administradores de plataforma, oficiales de seguridad
Organización	Un grupo de proyectos, normalmente una unidad de negocio o un cliente	Propietarios de la organización
Proyecto	Un equipo, con sus miembros, recursos y reglas de seguridad	Propietarios del proyecto
Espacio de trabajo	Un único entorno de desarrollo en contenedores	Desarrolladores

¿Por qué importa el anidamiento?

De la jerarquía se derivan dos cosas, y estas explican la mayor parte de lo que verá en la interfaz.

La configuración se hereda. Una configuración realizada en un nivel más amplio se aplica a todo lo que está debajo. Un nivel más específico normalmente puede anularla, a menos que el nivel más amplio imponga el valor. Algunas configuraciones funcionan al revés: el desarrollo remoto a través de SSH debe permitirse en *todos* los niveles superiores, por lo que el propietario de un proyecto no puede habilitarlo si la plataforma lo tiene desactivado. Consulte Política del espacio de trabajo.

Los roles están vinculados al proyecto. La misma persona puede tener un rol diferente en cada proyecto al que pertenezca. Lo que puede ver y cambiar depende del rol que tenga allí, no de una única configuración a nivel de cuenta. Consulte Roles y permisos.

Si una página, botón o configuración descrita en esta documentación no es visible para usted, la razón habitual es una de estas dos: su rol no tiene el permiso, o un nivel más amplio ha fijado la configuración.

Información relacionada

- Cómo funciona — la arquitectura y los componentes
- Roles y permisos
- Configuración de proyectos y organizaciones

Platform

La plataforma está organizada en organizaciones y proyectos. Una serie de operaciones están disponibles a nivel de plataforma. Por ejemplo, los espacios de trabajo, los recursos y los usuarios pueden gestionarse a nivel de plataforma por usuarios con un rol de plataforma, como el administrador o el oficial de seguridad. Las métricas de gobernanza, como la información y los registros de auditoría, también se agregan a nivel de plataforma.

El administrador de la plataforma tiene una vista de todos los espacios de trabajo que se ejecutan en la plataforma, es decir, en todas las organizaciones y proyectos, para que puedan actualizarse rápidamente, por ejemplo, la configuración de contenedores. El administrador también puede tener una vista general de los usuarios incorporados.

Los recursos se pueden gestionar a nivel de plataforma para que estén disponibles en todas las organizaciones y proyectos. Esto se aplica a todos los tipos de recursos compatibles con la plataforma.

Los paneles de información y auditorías están disponibles a nivel de plataforma, lo que permite seleccionar y agregar métricas en todas las organizaciones y proyectos.

Finalmente, una variedad de configuraciones y operaciones son relevantes a nivel de plataforma. Por ejemplo, estas incluyen configuraciones globales del espacio de trabajo relacionadas con el rendimiento y la seguridad, configuraciones globales de autenticación y funciones de cumplimiento, por nombrar algunas.

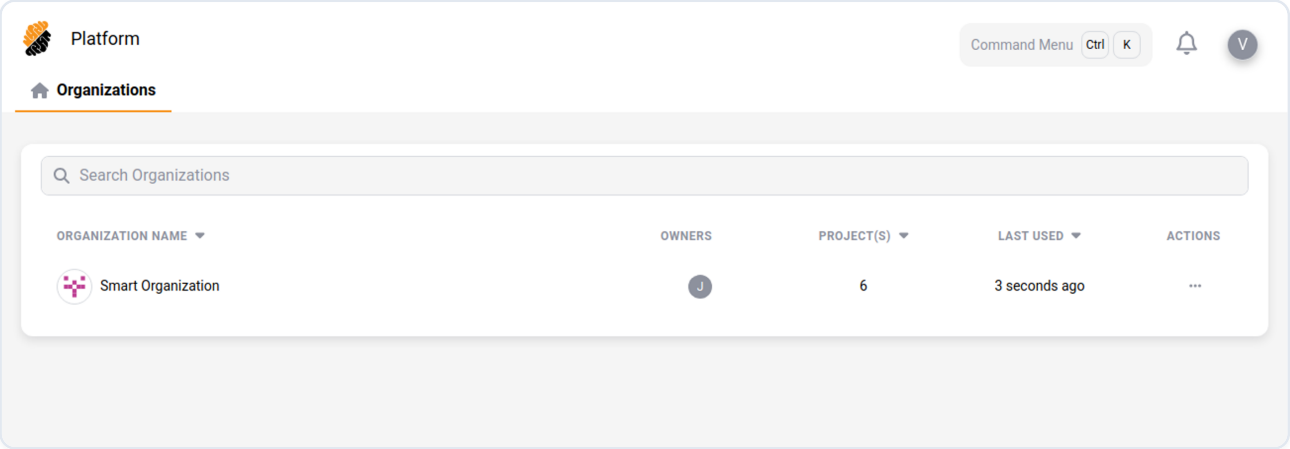
- Ver organizaciones
- Configuración de la plataforma

Ver organizaciones

Las organizaciones se pueden ver a nivel de plataforma y se listan en una tabla.

Un administrador puede crear una organización.

Haga clic en el logotipo de Citrix SecurSpaces™ para **ver sus organizaciones** a las que pertenece.



Lista de organizaciones

Configuración de la plataforma `Admin`

Para un control exhaustivo sobre las configuraciones de su plataforma, visite la página dedicada de Configuración de la plataforma.

Información relacionada

- Organizaciones
- Proyectos
- Espacios de trabajo
- Conceptos

Organizations

La plataforma permite a los administradores y propietarios de la plataforma organizar proyectos en organizaciones. Una **Organización** es la entidad principal que agrupa proyectos, desarrolladores, recursos y reglas de seguridad para un proyecto de desarrollo.

- Características de la organización
- Ver los proyectos de la organización
- Crear una organización

- Configuración de la organización

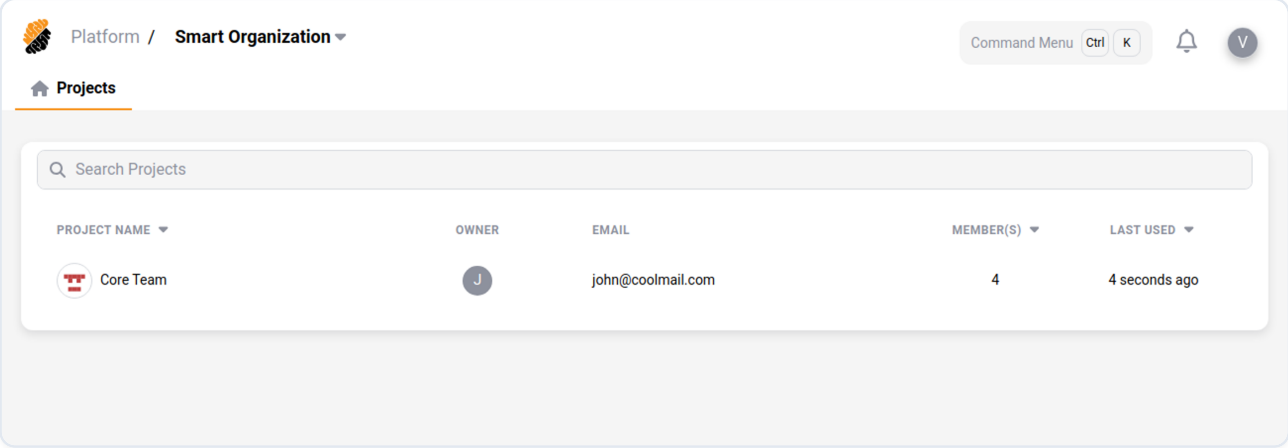
Características de la organización

Una organización se define por las siguientes características:

- **Nombre de la organización**,
- **Propietario de la organización**,
- **Correo electrónico del propietario de la organización**,
- **Proyecto(s)** que contiene,
- **Recursos, como contenedores base, políticas, etc.**

Ver los proyectos de la organización

En un proyecto, al hacer clic en el nombre de su **organización** en la esquina superior izquierda de la pantalla, puede mostrar todos los **proyectos** que contiene.



Crear una organización `Admin`

Puede crear una organización pulsando el botón "**Add New Organization**".

Deberá seleccionar la siguiente información:

- **Nombre de la organización**,
- **Propietario**. Es decir, cualquier usuario con los permisos adecuados para poseer una organización.

> **Información**

> Para crear una organización, debe ser un ***Admin***.

> Un **Admin** puede crear una organización en nombre de un propietario con los permisos para ser el **organization owner**.

Configuración de la organización `Admin`

Para un control exhaustivo sobre las configuraciones de su organización, visite la página dedicada de Organization Settings.

Información relacionada

- Plataforma
- Proyectos
- Espacios de trabajo
- Conceptos

Projects

Un **Proyecto** dentro de una Organización agrupa desarrolladores, recursos y reglas de seguridad. El objetivo de un proyecto es proporcionar al equipo de desarrollo todos los recursos necesarios para el desarrollo, así como mecanismos de control de acceso y gobernanza al propietario del proyecto.

- Características del proyecto
- Crear un proyecto
- Configuración del proyecto

Características del proyecto

Un proyecto se define por las siguientes características:

- **Nombre**,
- **Propietario del proyecto**, es decir, cualquier usuario con los permisos adecuados para poseer un proyecto,
- **Correo electrónico del propietario del proyecto**,
- **Miembro(s)**, es decir, el usuario que pertenece al proyecto,
- **Recursos, incluyendo espacios de trabajo, contenedores base, repositorios, etc.**

Crear un proyecto `Admin`

Puede crear un proyecto pulsando el botón "**Añadir nuevo proyecto**".

Deberá seleccionar la siguiente información:

- **Nombre del proyecto**,
- **Propietario**, es decir, cualquier usuario existente en la plataforma o un nuevo usuario (para incorporar).

> **Información**

> Para crear un proyecto, debes ser un **propietario de la organización**.

> Un **administrador** puede crear un proyecto y asignarlo a un usuario.

Configuración del proyecto `Project Owner`

Para un control exhaustivo sobre las configuraciones de tu proyecto, visita la página dedicada de Configuración del proyecto.

Información relacionada

- Organizaciones
- Plataforma
- Espacios de trabajo
- Conceptos

Workspaces

Un espacio de trabajo es un entorno de desarrollo en la nube (CDE) disponible para codificación y ciencia de datos. Se puede acceder a los espacios de trabajo (/es-es/securspaces/develop/develop-in-a-workspace.html#choose-how-you-connect) o a través de una (/es-es/securspaces/develop/workspaces/connect-over-ssh.html) desde un IDE instalado localmente.

Los espacios de trabajo se ejecutan en línea sobre una máquina virtual y se gestionan mediante un orquestador de contenedores para mayor resiliencia. El rendimiento de un espacio de trabajo, es decir, las capacidades de cómputo y almacenamiento, se establece según las especificaciones de la máquina virtual subyacente.

Los espacios de trabajo son, técnicamente hablando, procesos virtuales, con el objetivo de reemplazar el uso de una máquina virtual para el desarrollo de código y la ciencia de datos. Son

ligeros, por lo que pueden iniciarse y pausarse mucho más rápido que una máquina virtual equivalente.

> **Importante:**

> Los espacios de trabajo de Citrix SecurSpaces™ están contenerizados y son **efímeros**. El contenedor se recrea a partir de su imagen base cada vez que se inicia el espacio de trabajo, por lo que cualquier cosa instalada o modificada fuera del directorio persistente `/home/developer/` —por ejemplo, paquetes del sistema instalados con `apt` — no sobrevive a un reinicio. Antes de instalar herramientas o depender de cambios a nivel de sistema, lea (/es-es/securspaces/develop/what-persists.html) para elegir un enfoque que persista.

> Un espacio de trabajo se define por las siguientes características:

- **Información básica**: como nombre, propietario, opciones para compartir,
- **CPU/RAM/Almacenamiento**: rendimiento asignado al espacio de trabajo.
- **Puertos**: puertos para ejecutar aplicaciones,
- **Estado**: es decir, en ejecución, implementando o en pausa

Dónde ir a continuación

- Conozca la página de Espacios de trabajo
- Crear un Espacio de trabajo
- Administrar Espacios de trabajo
- Aplicaciones de Espacio de trabajo
- Usar plantillas
- Desarrollar en un espacio de trabajo
- Conectarse por SSH a su espacio de trabajo

Información relacionada

- Organizaciones
- Plataforma
- Proyectos

- Conceptos

SecurSpaces Flex overview

Citrix SecurSpaces™ Flex es un servicio gestionado por Citrix dentro de Citrix Platform Flex que ofrece espacios de trabajo Linux seguros para equipos de desarrollo. Este servicio, ofrecido a través de Citrix Cloud, proporciona entornos de desarrollador alojados en Azure sin necesidad de que el cliente configure o mantenga ninguna infraestructura. Citrix gestiona la plataforma y la infraestructura subyacente de Azure; los clientes conservan el control de la identidad, las imágenes de los espacios de trabajo, las políticas y los datos.

Citrix SecurSpaces Flex incluye:

- Alojamiento de espacios de trabajo de desarrollador gestionado por Citrix en Azure, con un plano de control basado en Azure Kubernetes Service (AKS) y Azure Cosmos DB.
- Espacios de trabajo Linux aislados y en entorno de pruebas accesibles a través del navegador (IDE o terminal basado en PWA), SSH desde IDE locales como VS Code, JetBrains Gateway, Cursor o Windsurf, o una experiencia de aplicación creada por el cliente.
- Dimensionamiento del espacio de trabajo por perfil: Ligero, Medio y Pesado, cada uno asignado a una tarifa de crédito de Platform Flex publicada.
- Niveles de tamaño de espacio de trabajo gestionados por Citrix, para que los perfiles de computación se mantengan alineados con el catálogo de servicios Flex.
- Tamaño del espacio de trabajo y plantilla del espacio de trabajo desacoplados, de modo que una única plantilla se puede emparejar con cualquier perfil de computación bajo demanda.
- Prevención nativa de pérdida de datos (DLP), entrada y salida controladas, control de acceso basado en roles (RBAC) y registro de auditoría completo.
- Entornos de ejecución en entorno de pruebas para agentes de codificación de IA bajo el mismo plano de control que las sesiones de desarrolladores humanos.
- Compatibilidad con Citrix DaaS Flex, con ambos servicios utilizando un grupo de créditos de Platform Flex compartido.

Las implementaciones de Citrix SecurSpaces Flex son planificadas y aprovisionadas por Citrix. Para empezar, póngase en contacto con su equipo de ventas de Citrix o con su especialista en soluciones de Citrix SecurSpaces.

Conceptos y terminología

Esta sección define los términos que los administradores utilizan con frecuencia en Citrix SecurSpaces Flex.

Implementación

Una implementación es la instancia aprovisionada de Citrix SecurSpaces Flex para su organización. Consiste en una región principal de Azure, una URL de acceso personalizada y una cuenta de administrador local inicial. Citrix aprovisiona y gestiona su implementación por usted. Cada organización tiene una implementación; se pueden añadir regiones adicionales de Azure como regiones secundarias después de la implementación.

Región principal

La región principal es la región de Azure donde se alojan el plano de control y la capacidad de ejecución principal de Citrix SecurSpaces Flex. Usted acuerda la región principal con su equipo de Citrix durante la planificación de la implementación. La región principal no se puede cambiar una vez completado el aprovisionamiento.

Regiones secundarias

Las regiones secundarias son regiones adicionales de Azure que se añaden a una implementación existente para ampliar la capacidad del espacio de trabajo, acercando la capacidad a los equipos de desarrollo distribuidos. Para añadir o eliminar una región secundaria, póngase en contacto con su equipo de Citrix.

URL de acceso

La URL de acceso es el subdominio personalizado asignado al entorno Citrix SecurSpaces Flex de su organización, con el formato `https://<yourcompany>.flex.sds.citrix.com`. Usted elige el subdominio con su equipo de Citrix durante la planificación de la implementación. Los desarrolladores y administradores utilizan esta URL para acceder al entorno de Citrix SecurSpaces.

Espacio de trabajo

Un espacio de trabajo es un contenedor Linux aislado y en un entorno limitado (sandbox) que proporciona un entorno de desarrollo seguro para un desarrollador o un agente de IA. Cada espacio de trabajo se ejecuta en el plano de ejecución de Citrix SecurSpaces Flex con vCPU, RAM y almacenamiento persistente definidos. El estado persistente está respaldado por Kubernetes Persistent Volume Claims (PVCs), por lo que el trabajo de múltiples proyectos y

múltiples repositorios sobrevive entre sesiones. Se puede acceder a los espacios de trabajo a través de un navegador, SSH o un IDE local compatible.

Plantilla de espacio de trabajo

Una plantilla de espacio de trabajo es una definición preconfigurada y con control de versiones que incluye la imagen del contenedor, las herramientas preinstaladas, los límites de recursos, los controles de acceso y los scripts de inicio. Las plantillas son la unidad principal de implementación en Citrix SecurSpaces Flex. El cliente posee y aloja las imágenes de contenedor; Citrix aloja y ejecuta la plataforma que las ejecuta. Dado que el tamaño del espacio de trabajo y la plantilla del espacio de trabajo están desacoplados, una única plantilla se puede emparejar con cualquier tamaño de espacio de trabajo bajo demanda. Consulte Plantillas de espacio de trabajo para obtener más información.

Tamaño del espacio de trabajo

El tamaño del espacio de trabajo es el perfil de computación asignado a un espacio de trabajo. Cada tamaño se asigna a una configuración definida de vCPU y RAM con una tarifa de crédito de Platform Flex publicada. Los tamaños de espacio de trabajo disponibles en el lanzamiento son:

TAMAÑO	VCPU	RAM	ALMACENAMIENTO	CARGA DE TRABAJO PREVISTA
Desarrollador (ligero)	2 vCPU	8 GB	32 GB	Codificación general y trabajo de desarrollo rutinario
Desarrollador (medio)	4 vCPU	16 GB	64 GB	Cargas de trabajo mixtas
Desarrollador (pesado)	8 vCPU	32 GB	128 GB	Grandes compilaciones, compilaciones y cargas de trabajo de datos exigentes

El tamaño del espacio de trabajo y la plantilla del espacio de trabajo se configuran de forma independiente. Al estar desacoplados, las organizaciones pueden reutilizar una única plantilla en

espacios de trabajo de diferentes tamaños, y los desarrolladores pueden cambiar los perfiles de computación a medida que cambian las demandas de la carga de trabajo.

Citrix gestiona las definiciones de tamaño del espacio de trabajo en Flex. Cada tamaño pertenece a un nivel gestionado y puede tener versiones más recientes con el tiempo. Los administradores controlan dónde está disponible un nivel, pero no editan los valores de CPU, RAM, almacenamiento o clase de almacenamiento que definen el nivel. Cuando Citrix publica una versión más reciente de un nivel, los espacios de trabajo afectados se pueden actualizar a la versión actual del mismo nivel.

Créditos de Platform Flex

Los créditos de Platform Flex son la unidad de consumo de los servicios de Citrix Platform Flex. Los espacios de trabajo de Citrix SecurSpaces Flex consumen créditos en función del tamaño del espacio de trabajo y del uso diario. El mismo grupo de créditos cubre otros servicios de Platform Flex, incluido Citrix DaaS Flex, por lo que los desarrolladores pueden usar un escritorio virtual de DaaS Flex para tareas generales y un espacio de trabajo de Citrix SecurSpaces Flex para el desarrollo, ambos rastreados a través de un único modelo de crédito unificado sin un ciclo de adquisición separado. Consulte Licencias para Citrix Platform Flex y Consumo e informes de créditos de Platform Flex para obtener más información.

La disponibilidad de los servicios de Citrix Platform Flex y la compensación de créditos de servicio si Citrix incumple un compromiso están cubiertas por el SLA de Platform Flex.

Conectividad de red

Los espacios de trabajo de Citrix SecurSpaces Flex se conectan a los sistemas propiedad del cliente a través de un emparejamiento de red virtual (vNET) de Azure compartido o una puerta de enlace VPN entre el inquilino de Azure gestionado por Citrix y la red del cliente. Esta capa de integración permite el acceso del espacio de trabajo a proveedores de identidad gestionados por el cliente, repositorios de Git, repositorios de artefactos, canalizaciones de CI/CD, orígenes de datos y administradores de secretos. Consulte Conexiones de red para obtener más información.

Toda la documentación de SecurSpaces Flex

Los artículos de Flex se encuentran en la sección que coincide con su propósito, por lo que no están adyacentes en el panel de contenido. Este es el conjunto completo, junto con el acuerdo de nivel de servicio de Platform Flex, que se publica con la documentación de Citrix Platform Flex.

ARTÍCULO	QUÉ CUBRE
Descripción general de seguridad técnica	La arquitectura de seguridad del servicio gestionado por Citrix: tenencia, residencia de datos, cifrado y la división de responsabilidades compartidas
Conexiones de red	Cómo los espacios de trabajo de Flex acceden a su proveedor de identidades, repositorios y otros sistemas propiedad del cliente
Plantillas de espacio de trabajo	Las plantillas disponibles en Flex y lo que ofrece cada una
¿Qué hay de nuevo en SecurSpaces Flex?	Notas de la versión del servicio Flex
SLA de Platform Flex	El compromiso de disponibilidad para los servicios de Platform Flex y la compensación de crédito de servicio

Todo lo demás en esta documentación también se aplica a Flex, excepto donde una página indique lo contrario. Flex es un modelo de implementación para Citrix SecurSpaces™ en lugar de un producto separado, por lo que los artículos de desarrollador, proyecto y plataforma describen el mismo entorno.

Más información

- Licencias para Citrix Platform Flex
- Consumo y generación de informes de créditos de Platform Flex
- SLA de Platform Flex
- Anunciando Citrix SecurSpaces™ Flex: un modelo operativo diferente para las necesidades de desarrollo modernas — Blog ejecutivo
- Dentro de Citrix SecurSpaces™ Flex: una plataforma de espacio de trabajo seguro alojada por Citrix para equipos de desarrollo — Blog de tecnología

SecurSpaces videos

Esta lista de reproducción de vídeos incluye tutoriales y mejores prácticas para Citrix SecurSpaces™, demostrando cómo acelera la innovación con entornos de desarrollador Linux de autoservicio, seguros, escalables y listos para codificar. Descubra cómo estos entornos impulsan

la velocidad de los desarrolladores al tiempo que reducen los costes de infraestructura y los riesgos de seguridad.

Testimonios

Escuche a desarrolladores y líderes de TI sobre cómo SecurSpaces está transformando su flujo de trabajo, impulsando la productividad y reduciendo el riesgo.

TÍTULO	DESCRIPCIÓN	ENLACE
Por qué Citrix utiliza SecurSpaces	SecurSpaces ha revolucionado la experiencia del desarrollador en Citrix. En este testimonio real, nuestros equipos comparten cómo SecurSpaces nos ayudó a pasar de una incorporación lenta y configuraciones complejas a entornos de desarrollo rápidos, seguros y nativos de la nube. Con acceso instantáneo desde cualquier dispositivo, seguridad integrada y una reducción de más del 60 % en el coste total de propiedad, SecurSpaces permite a los equipos distribuidos trabajar más rápido y de forma más segura, sin necesidad de portátiles de altas especificaciones o VDI persistente. Vea cómo simplificamos el desarrollo seguro y aceleramos la innovación.	

Demostraciones

Vea estas demostraciones para ver cómo SecurSpaces ofrece entornos Linux seguros y listos para codificar que aceleran el desarrollo y simplifican el flujo de trabajo.

CITRIX SECURSPACES™

TÍTULO	DESCRIPCIÓN	ENLACE
Integración de SecurSpaces con Backstage	Descubra cómo SecurSpaces se integra con Backstage para impulsar un portal de desarrolladores unificado y de autoservicio. En este vídeo, mostramos cómo los desarrolladores pueden cambiar de contexto con un solo clic utilizando los paneles de Backstage, aprovisionar espacios de trabajo seguros al instante para nuevos proyectos y acelerar la incorporación con entornos y pilas de herramientas preconfigurados. Esta integración ayuda a los equipos a optimizar los flujos de trabajo, mantener el cumplimiento y aumentar la productividad, todo desde su centro Backstage.	
SecurSpaces: Acceso a la red de confianza cero, protección de datos avanzada, prevención de pérdidas	Descubra cómo SecurSpaces proporciona un entorno seguro para que los desarrolladores construyan e innoven sin compromisos. Con el Acceso a la Red de Confianza Cero (ZTNA), la protección de datos avanzada y la prevención de pérdida de datos (DLP), sus equipos pueden colaborar con confianza desde cualquier lugar. Combine la innovación con la seguridad y mantenga su empresa protegida.	

TÍTULO	DESCRIPCIÓN	ENLACE
SecurSpaces: Protección de datos avanzada con Chrome Enterprise Premium	Descubra cómo Chrome Enterprise Premium y SecurSpaces mejoran la protección y seguridad de los datos para las empresas modernas. En este vídeo, exploramos las funciones de seguridad avanzadas que ayudan a los administradores de TI a salvaguardar la información confidencial, garantizar el cumplimiento y proteger los puntos finales en toda su organización. Manténgase a la vanguardia con SecurSpaces y Chrome Enterprise Premium para una empresa más segura e inteligente.	☐
SecurSpaces: Incorporación de desarrolladores con un solo clic	SecurSpaces permite a los equipos de desarrollo autoaprovisionar entornos seguros y estandarizados bajo demanda, acelerando la incorporación de entornos de desarrollo para contratistas y nuevas contrataciones en menos de un minuto.	☐

Seminarios web

Vea nuestros seminarios web grabados para descubrir cómo SecurSpaces empodera a los desarrolladores con entornos Linux seguros, escalables y listos para codificar.

TÍTULO	DESCRIPCIÓN	ENLACE
Automatización y gobernanza de DevSecOps	Aprenda cómo los Entornos de Desarrollo en la Nube (CDE) y los contenedores	☐

TÍTULO	DESCRIPCIÓN	ENLACE
	aceleran DevOps en este seminario web, incluyendo cómo impulsar la productividad del desarrollador, mejorar DevSecOps, reducir costes y mejorar la eficiencia de la infraestructura.	
Lograr el cumplimiento normativo y de seguridad en todo un proceso de desarrollo	Mejore la seguridad de DevOps y logre el cumplimiento de la ISO 27001 con contenedores en línea. En este seminario web, aprenderá a implementar controles de riesgo, automatizar el acceso y gestionar recursos.	
Ampliando el alcance de la ingeniería de plataformas con Entornos de Desarrollo en la Nube	La ingeniería de plataformas impulsa la productividad del desarrollador con DevOps basado en plantillas, mejorando la automatización, la seguridad y el cumplimiento a través de Entornos de Desarrollo en la Nube (CDE).	

Get started

Empiece aquí si es nuevo en Citrix SecurSpaces™. Cada página de esta sección es un tutorial: una única ruta a través de una tarea, con un resultado predecible.

Si se le ha concedido acceso

Su organización ya utiliza SecurSpaces y alguien le ha añadido a un proyecto.

HAGA ESTO	PÁGINA
Configure su perfil, acceso a Git y credenciales	Configure su cuenta
Cree un espacio de trabajo y conéctese a él	Su primer espacio de trabajo
Ejecute algo de principio a fin en unos minutos	Espacio de trabajo Hello World
Trabaje en un proyecto realista	Desarrolle, depure y comparta una aplicación Node.js

Una vez que esté configurado, Desarrollar cubre el trabajo diario.

Si está configurando un proyecto para su equipo

Usted dirige un proyecto y sus desarrolladores están esperando para usarlo.

HAGA ESTO	PÁGINA
Prepare imágenes, repositorios, secretos y una plantilla, luego añada personas	Configure un proyecto para su equipo

Administrar cubre la ejecución del proyecto después de eso.

Si está evaluando la plataforma

Necesita un entorno propio antes de que cualquiera pueda usarlo.

HAGA ESTO	PÁGINA
Configure un entorno de evaluación en una única VM	Implemente un entorno de evaluación

Para una implementación de producción, consulte Implementar.

Información relacionada

- Qué es SecurSpaces
- Conceptos

Set up your account

`Developer`

Esta guía le explica cómo configurar su perfil, conectar sus repositorios de código y preparar sus credenciales en Citrix SecurSpaces™. Complete estos pasos una sola vez: se aplican a todos sus espacios de trabajo y proyectos.

Estos pasos coinciden con la lista de verificación de incorporación que verá la primera vez que inicie sesión. Si ya ha completado un paso en el producto, no dude en saltárselo.

Antes de empezar

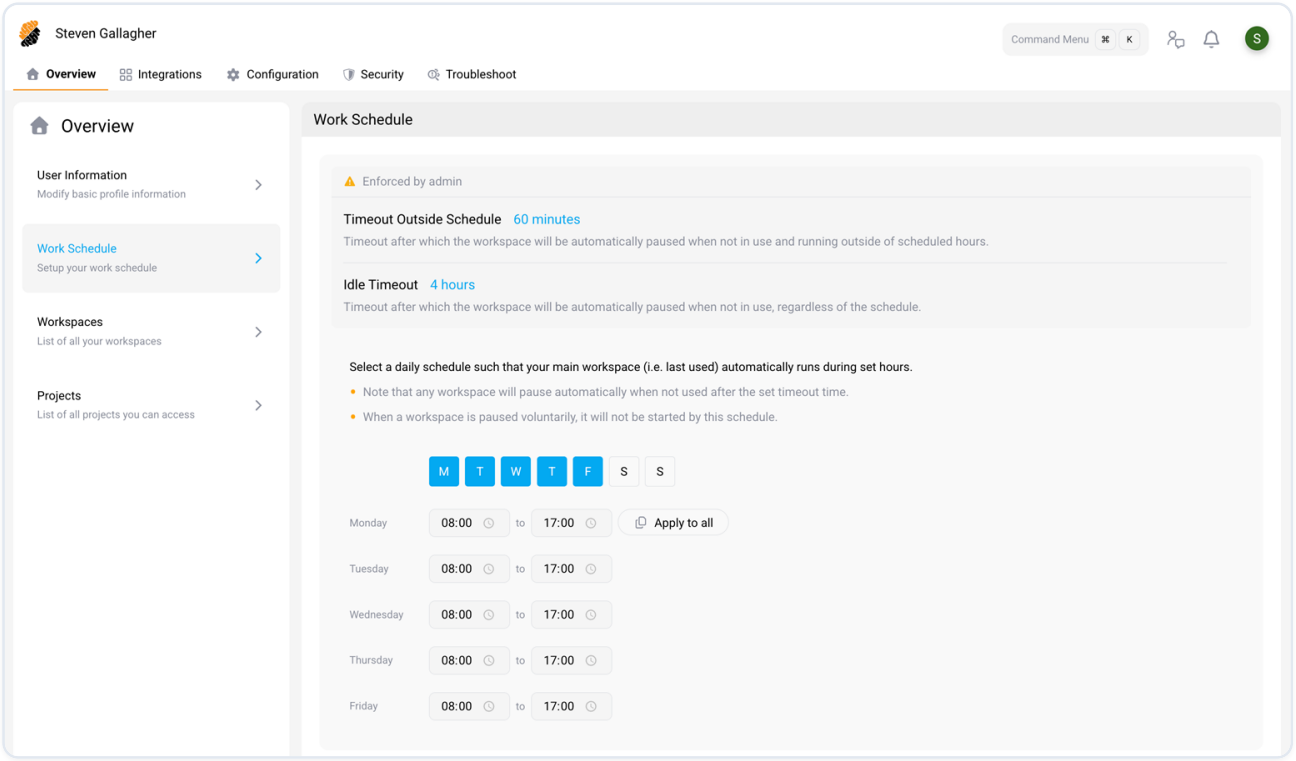
Asegúrese de tener lo siguiente:

- **Una cuenta de SecurSpaces.** El propietario de su proyecto o el administrador de la plataforma le ha añadido a un proyecto. Debería haber recibido un correo electrónico de bienvenida con su URL de inicio de sesión.
- **Credenciales del proveedor de Git.** Su nombre de usuario y contraseña (o un token de acceso personal) para GitHub, GitLab, Bitbucket o Azure DevOps, el que utilice su equipo.

> **¿Vuelve a un nuevo proyecto?** Si ya ha completado la incorporación en otro proyecto de SecurSpaces, su perfil y credenciales se transfieren. Solo necesita verificar que sus integraciones funcionan con los repositorios del nuevo proyecto y, a continuación, pasar a Inicio rápido: Crear y conectarse a su espacio de trabajo.

Paso 1: Revise su perfil

Su perfil contiene su información personal y su horario de trabajo. La mayoría de los campos se importan del proveedor de identidades de su organización y ya deberían ser correctos. Su zona horaria determina cuándo se ejecutan las acciones programadas (como el inicio automático del espacio de trabajo); si trabaja en varias zonas horarias, establezca aquella en la que pase la mayor parte de sus horas de trabajo.



Cómo completar este paso

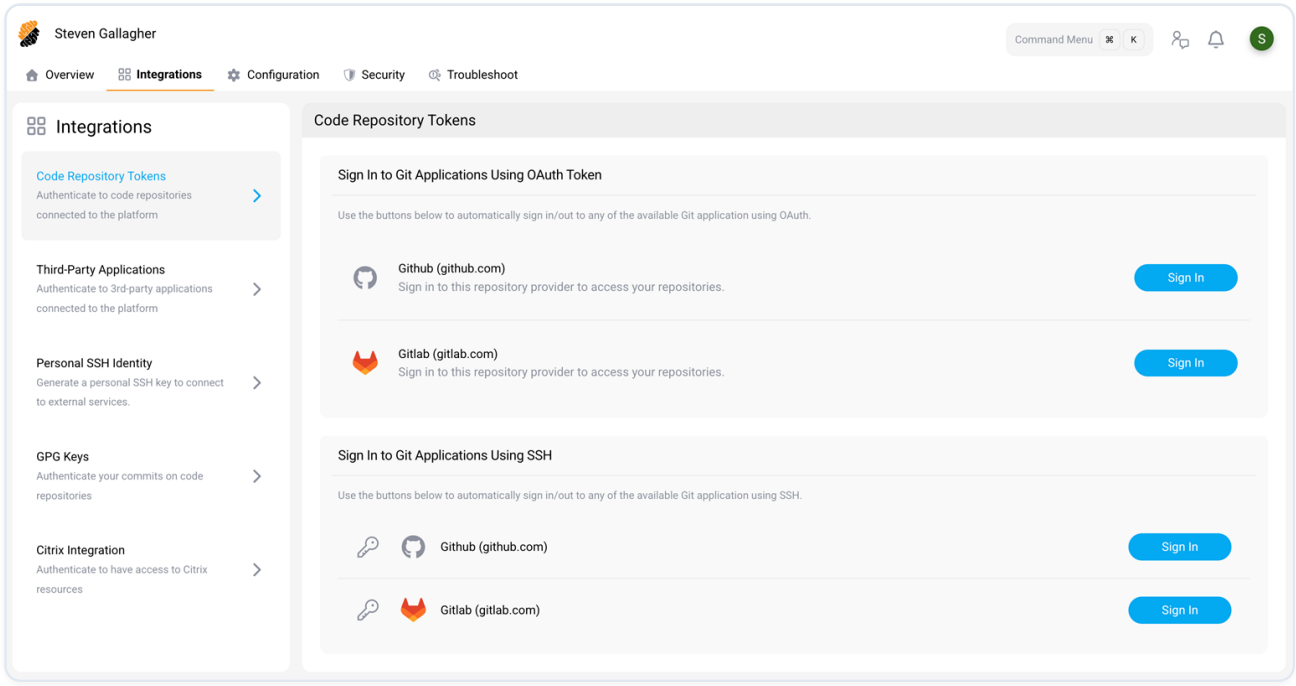
1. Inicie sesión en SecurSpaces y seleccione su **avatar** en la esquina superior derecha, luego seleccione **Perfil**.
2. En **Información de usuario**, revise su nombre y zona horaria. Actualícelos si es necesario.
3. En **Horario de trabajo**, ajuste los días y las horas para que coincidan con su patrón de trabajo habitual.
4. Si todo parece correcto, no se necesitan cambios.

Más información sobre tu perfil

Paso 2: Configurar integraciones

Las integraciones conectan tus espacios de trabajo con repositorios de código y servicios externos. Necesitas al menos un token de repositorio de código configurado para enviar y extraer código desde un espacio de trabajo. Una vez configuradas, tus integraciones se aplican a **todos**

tus espacios de trabajo, incluidos los existentes; no necesitas reconfigurar las credenciales por cada espacio de trabajo.



Cómo completar este paso

1. En tu perfil, ve a la sección de **Integraciones**.
2. En **Tokens de repositorio de código**, autentícate con tu proveedor de repositorio:
    - **OAuth (recomendado):** Selecciona tu proveedor (GitHub, GitLab, Bitbucket o Azure DevOps) y completa el flujo de OAuth. Esto proporciona a todos tus espacios de trabajo acceso sin interrupciones a tus repositorios sin necesidad de iniciar sesión repetidamente: te autenticas una vez aquí y cada espacio de trabajo que crees se conectará automáticamente.
    - **Clave SSH personal:** Si tu organización requiere autenticación basada en SSH, sube tu clave pública SSH o genera un nuevo par de claves.
3. En **Identidad SSH personal** (opcional), genera un par de claves SSH si necesitas conectarte a servicios externos a través de SSH, por ejemplo, una caché de Bazel o un repositorio de artefactos. Añade la clave pública al servicio externo. SecurSpaces aplica automáticamente la clave privada a tus sesiones de espacio de trabajo sin exponerla al código del espacio de trabajo.
4. En **Claves GPG** (opcional), genera o importa una clave GPG para firmar tus confirmaciones de Git.

Más información sobre las integraciones

Paso 3: Personaliza la configuración de tu espacio de trabajo (opcional)

Tus espacios de trabajo funcionan de forma predeterminada, pero puedes personalizarlos con configuraciones de shell personales, ajustes de IDE y scripts de inicio. Estos ajustes se aplican automáticamente a cada nuevo espacio de trabajo que crees. Los archivos de configuración se inyectan en `/home/developer` al inicio del espacio de trabajo, y tu configuración de shell se ejecuta en cada nueva sesión de terminal.

Puede omitir este paso y volver más tarde. Los cambios de configuración se pueden aplicar a los espacios de trabajo existentes utilizando la acción **Personalizar entorno**.

Página de configuración que muestra la selección de shell y el editor de scripts(/en-us/securspaces/media/quick-start/quick-start-set-up-your-account-configuration-1.png)

Cómo completar este paso

1. En su perfil, navegue a la sección **Configuración**.
2. En **Archivos de configuración:**
    - Establezca su **shell predeterminado** (bash o zsh).
    - Cree scripts de shell personalizados (por ejemplo, `.bashrc` o `.zshrc`) con sus alias preferidos, variables de entorno y configuraciones de herramientas.
3. En **Configuración del IDE:**
    - Si ya tiene un espacio de trabajo en ejecución con sus configuraciones preferidas de VS Code o JetBrains, puede **importar** esas configuraciones para usarlas como predeterminadas en todos los espacios de trabajo.
4. En **Script de inicio:**
    - Defina un script personal que se ejecute cada vez que se inicie uno de sus espacios de trabajo. Úselo para instalar herramientas CLI personales, configurar estructuras de directorios o ejecutar comandos de inicialización. Un script configurado en un espacio de trabajo individual anula este. Consulte Scripts de inicio.

Consejos

- **Empiece de forma sencilla.** Siempre puede añadir más personalización más tarde. Un `.bashrc` básico con sus alias favoritos es un buen punto de partida.

- **No instale dependencias de proyecto aquí.** Utilice plantillas de espacio de trabajo o scripts de inicio para herramientas específicas del proyecto. La configuración personal es para sus preferencias (prompt de shell, alias, configuraciones del editor).
- **Pruebe los cambios primero en un espacio de trabajo.** Utilice la acción **Personalizar entorno** en un espacio de trabajo existente antes de aplicarla globalmente.

Más información sobre la configuración del espacio de trabajo(/es-es/securspaces/develop/profile/configuration.html)

Paso 4: Configurar credenciales de seguridad

Los secretos personales, las claves API y las claves SSH permiten que tus espacios de trabajo se autentiquen con servicios y API durante el desarrollo. Los secretos se inyectan en tus espacios de trabajo como variables de entorno o archivos, por lo que no necesitas gestionar las credenciales manualmente dentro de cada espacio de trabajo. El propietario de tu proyecto o el administrador de la plataforma también pueden haber configurado **secretos a nivel de proyecto o de plataforma** que están disponibles automáticamente; consulta con tu equipo si no estás seguro de qué credenciales necesitas añadir personalmente.

Página de seguridad que muestra la sección de secretos personales(/en-us/securspaces/media/quick-start/quick-start-set-up-your-account-security-1.png)

Cómo completar este paso

1. En tu perfil, ve a la sección de **Seguridad**.
2. En **Secretos personales**, añade cualquier credencial que tus espacios de trabajo necesiten — por ejemplo, tokens de acceso para API internas o registros de paquetes. Para cada secreto, elige si inyectarlo como un **archivo** o una **variable de entorno**.
3. En **Acceso remoto a través de SSH**, configura las claves SSH si planeas conectarte a tu espacio de trabajo desde un IDE instalado localmente usando SSH (por ejemplo, VS Code Desktop, JetBrains, Cursor, Windsurf o Kiro).
4. En **Claves API**, añade cualquier clave API que tu flujo de trabajo de desarrollo requiera (por ejemplo, claves para servicios en la nube o API de terceros).

Notas de seguridad importantes

- Los secretos se almacenan cifrados y se inyectan al inicio del espacio de trabajo. **No** son visibles en el código o los registros del espacio de trabajo.

- Si rotas una credencial (por ejemplo, regeneras un token API), actualízala aquí — el nuevo valor se aplica a todos los espacios de trabajo en el siguiente inicio.
- Nunca codifiques secretos directamente en tu repositorio. Utiliza el mecanismo de secretos en su lugar.

Más información sobre las credenciales de seguridad(/es-es/securspaces/develop/profile/security.html)

Pasos siguientes

Su cuenta está completamente configurada. Está listo para crear su primer espacio de trabajo y empezar a programar.

Inicio rápido: Crear y conectarse a su espacio de trabajo

Your first workspace

`Developer`

Este tutorial le lleva desde una consola vacía de SecurSpaces hasta un espacio de trabajo de Citrix SecurSpaces™ en ejecución con el código de su proyecto, listo para trabajar.

Al finalizar, habrá:

- Creado un espacio de trabajo a partir de una plantilla preparada por el propietario de su proyecto
- Lo ha abierto en el IDE en la nube y ha ejecutado un comando en él
- Confirmado que su repositorio de proyecto se ha clonado
- Aprendido cuáles de sus cambios sobreviven a un reinicio

Tarda unos 10 minutos. Siga los pasos en orden.

Antes de empezar

Necesita:

- **Una configuración de cuenta completada** — perfil, integraciones y credenciales. Si no lo ha hecho, empiece con Configurar su cuenta.
- **Una plantilla de espacio de trabajo** para su proyecto. El propietario de su proyecto las prepara. Si no sabe qué plantilla usar, pregúnteles antes de empezar.

Cómo se conectará

Este tutorial utiliza el **IDE en la nube** (VS Code para la web) porque se abre en una pestaña del navegador y no necesita nada instalado.

El IDE en la nube no es su única opción, y para el trabajo diario puede que no sea su preferida. SecurSpaces también admite la conexión desde un IDE instalado localmente a través de SSH, de modo que su editor se ejecuta en su máquina mientras el código, las herramientas y la computación permanecen en el espacio de trabajo. Muchos desarrolladores prefieren esto. Lo configurará después de terminar aquí — consulte Otras formas de conectarse al final.

Paso 1: Crear un espacio de trabajo a partir de una plantilla

Un espacio de trabajo es su entorno personal de desarrollo en la nube: su código, herramientas y dependencias, ya configurados. Las plantillas contienen esa configuración, por lo que no tiene que montarla usted mismo.

1. Desde la página de inicio de SecurSpaces, seleccione **Crear espacio de trabajo**, luego **Crear desde plantilla**.
2. Seleccione la plantilla que su propietario de proyecto le indicó que usara.
3. Revise el resumen de configuración.
4. Seleccione **Iniciar**.

Pantalla de selección de plantilla que muestra las plantillas de espacio de trabajo disponibles(/en-us/securspaces/media/quick-start/quick-start-create-and-connect-template-selection-1.png)

La implementación tarda entre 30 y 90 segundos, y se muestra un indicador de progreso mientras se inicializa. Espere hasta que el estado muestre **En ejecución**.

Paso 2: Abrir el IDE en la nube

1. En la tarjeta del espacio de trabajo, seleccione **Abrir**.
2. VS Code para Web se abre en una nueva pestaña del navegador, ya conectado a su espacio de trabajo.

VS Code para Web ejecutándose dentro de un espacio de trabajo(/en-us/securspaces/media/quick-start/quick-start-create-and-connect-vscode-for-web-1.png)

Abra un terminal en el IDE en la nube y ejecute:

```
whoami
```

Imprime `developer`. Está ejecutando comandos dentro del espacio de trabajo, no en su propia máquina — la pestaña del navegador es solo la ventana hacia él.

Paso 3: Comprobar el código de su proyecto

Si su plantilla incluye repositorios, estos se clonaron mientras se iniciaba el espacio de trabajo. Confirme que:

```
ls /home/developer
```

Su carpeta de proyecto aparece en la lista. Ábrala y compruebe que el repositorio está intacto:

```
cd /home/developer/my-project

git status
```

Git informa de la rama actual y de un árbol de trabajo limpio. Sus credenciales provienen de las integraciones de su perfil, por lo que no tuvo que iniciar sesión en nada.

Si su carpeta de proyecto no está ahí, es posible que su plantilla no incluya un repositorio, o que sus credenciales de Git necesiten atención. Pregunte al propietario de su proyecto qué esperar, y consulte Si falta un repositorio.

Paso 4: Aprenda qué persiste

Los espacios de trabajo no son persistentes por defecto, y esto es lo que más probablemente le sorprenderá más adelante. Cree un archivo en su directorio personal:

```
echo "notes" > /home/developer/scratch.txt
```

Todo lo que esté bajo `/home/developer` —su código, este archivo, su `node_modules`— sobrevive a una pausa o reinicio. Todo lo que esté fuera de él no. Un paquete que instale a nivel de sistema con `apt` desaparecerá la próxima vez que el espacio de trabajo se inicie.

Esa es la regla: **mantenga su trabajo bajo `/home/developer`**. Cuando necesite una herramienta a nivel de sistema de forma permanente, use un script de inicio o pida al propietario de su proyecto que la añada a la imagen de la plantilla. Para más información, consulte Qué persiste en un espacio de trabajo de SecurSpaces.

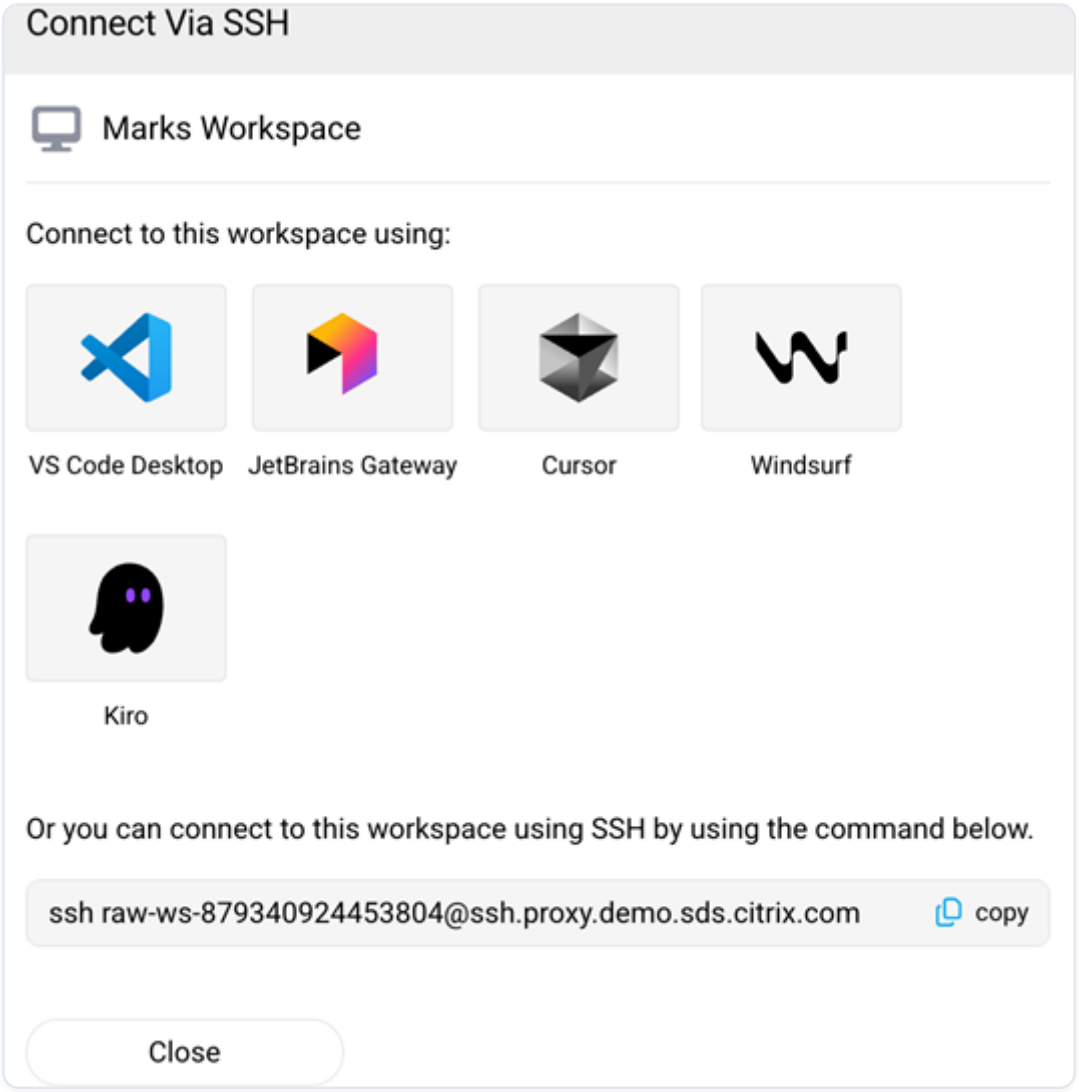
Lo que ha aprendido

Tiene un espacio de trabajo en ejecución con el código de su proyecto, y ha ejecutado comandos dentro de él desde un navegador. En el camino, vio que la plantilla proporcionaba el entorno, su perfil proporcionaba las credenciales, y `/home/developer` es el límite entre lo que persiste y lo que no.

Otras formas de conectar

El IDE en la nube le permitió empezar sin instalar nada. Para sesiones más largas, la mayoría de los desarrolladores cambian a su propio IDE, conectado al mismo espacio de trabajo a través de SSH.

IDE	MÉTODO DE CONEXIÓN
VS Code Desktop, **Cursor**, **Windsurf**, **Kiro**	Un clic, usando la extensión Citrix Secure Developer Spaces - Remote SSH
JetBrains Gateway	Configuración de SSH a través de la interfaz de Gateway
Otros editores compatibles con SSH	Par de claves SSH manual



SSH debe estar habilitado para su proyecto y en el propio espacio de trabajo, y necesita un par de claves SSH en su perfil. Para conocer los requisitos previos y los pasos para cada IDE, consulte Conectarse a un espacio de trabajo a través de SSH.

Qué hacer a continuación

OBJETIVO	GUÍA
Conectarse desde su propio IDE a través de SSH	Conectarse a un espacio de trabajo a través de SSH
Practicar el ciclo de desarrollo en una aplicación autónoma	Espacio de trabajo Hello World
Crear un espacio de trabajo sin plantilla y configurarlo usted mismo	Crear un espacio de trabajo

OBJETIVO	GUÍA
Compartir una aplicación en ejecución con tu equipo	Aplicaciones del espacio de trabajo
Comprender la pausa, la reanudación y el inicio automático	Administrar espacios de trabajo

Obtener ayuda

- **Pregunta a tu propietario de proyecto** sobre plantillas, repositorios y recursos del proyecto.
- **Contacta con tu administrador de plataforma** para problemas de acceso a la cuenta, red o a nivel de plataforma.
- **Consulta la documentación de SecurSpaces** para obtener guías detalladas.

Hello World workspace

`Developer`

El espacio de trabajo Hello World es un entorno de formación autónomo que le permite explorar Citrix SecurSpaces™ de forma práctica. Incluye una aplicación de demostración fullstack; no se requieren credenciales de Git ni acceso a internet.

Utilice este espacio de trabajo para seguir las guías de inicio rápido, ejecutar su primera sesión de incorporación o validar que SecurSpaces funciona correctamente en su entorno.

Antes de empezar

La imagen de contenedor Hello World **no** se incluye con SecurSpaces, por lo que debe añadirse a un proyecto antes de que nadie pueda crear un espacio de trabajo a partir de ella. Un desarrollador no puede hacer esto por sí mismo.

> **Para los propietarios de proyectos:** configure un proyecto de pruebas Hello World dedicado al que cada nuevo desarrollador pueda unirse. Añada la imagen a los recursos de contenedor de ese proyecto una vez —ya sea directamente desde Docker Hub (`strongnetwork/workspace-demo-multi-project`) o desde un registro aprobado por la empresa— y configure los cinco secretos de la base de datos del Paso 1 como secretos del proyecto. Los nuevos desarrolladores pueden entonces iniciar esta guía sin tener que pedir nada. Si su organización examina las imágenes de contenedor antes de usarlas, involucre a

> su administrador de plataforma con antelación: esta imagen se revisa como cualquier otra, así que tómese su tiempo para ello.

> Si es desarrollador y la imagen Hello World no está disponible cuando crea un espacio de trabajo, pida a su propietario de proyecto o administrador de plataforma que lo configure.

Contenido

COMPONENTE	DETALLES
Aplicación	"Proyecto ACME" — una aplicación de gestión de usuarios (buscar, añadir, ver, eliminar usuarios)
Frontend	Next.js + React + TypeScript + Bootstrap
Backend	Rutas de API de Next.js (puntos finales REST)
Base de datos	PostgreSQL 15 (se ejecuta en un contenedor Docker dentro del espacio de trabajo)
Herramientas	Node.js LTS, Yarn, Docker, ESLint, TypeScript
Extensiones de VS Code	GitHub Copilot Chat (preinstalado). Las extensiones de lenguaje y herramientas (ESLint, Prettier, Docker, PostgreSQL Explorer) **no** están preinstaladas; añádelas según sea necesario.

Todo está preconstruido y listo para ejecutarse. El espacio de trabajo funciona sin acceso a internet ni cuentas externas.

Paso 1: Crear un espacio de trabajo

Confirma que la imagen Hello World está disponible en tu proyecto. Si no lo está, consulta Antes de empezar.

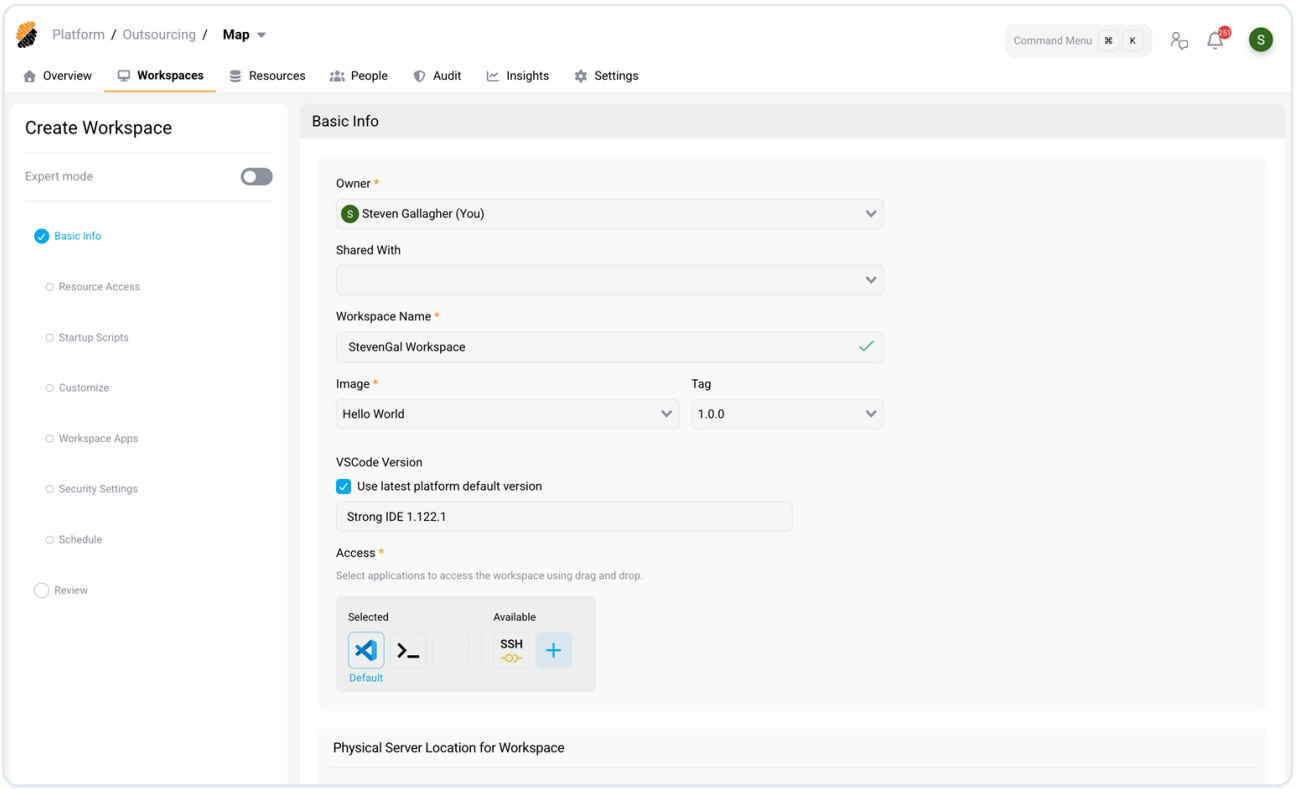
Crea el espacio de trabajo:

1. Desde la página de descripción general de SecurSpaces, selecciona **Crear espacio de trabajo**.

2. En **Información básica**, selecciona la imagen de contenedor y la etiqueta **Hello World** de las imágenes disponibles del proyecto.
3. En **Especificaciones del espacio de trabajo**, selecciona una plantilla con al menos:
    - **CPU:** 2 núcleos
    - **RAM:** 8 GB
4. Navegue al paso de **Control de acceso a recursos** y, en **Secretos**, añada lo siguiente como variables de entorno:

NOMBRE	VALOR
`DB_HOST`	`localhost`
`DB_PORT`	`5432`
`DB_NAME`	`project_acme`
`DB_USER`	`acme_user`
`DB_PASSWORD`	`acme_password`

5. Seleccione **Lanzar**.



Su espacio de trabajo se inicia en menos de 30 segundos. Docker es proporcionado automáticamente por la plataforma (a través de Docker-in-Docker), por lo que no se requiere ninguna configuración adicional.

Paso 2: Comprender cómo se configuran los secretos

La aplicación Hello World se conecta a PostgreSQL utilizando las variables de entorno que añadió en el Paso 1. Estas se inyectan automáticamente en su espacio de trabajo, sin necesidad de un archivo `.env`.

Abra un terminal y verificar:

```
echo $DB_USER    # acme_user

echo $DB_HOST    # localhost
```

La aplicación los lee a través de `process.env` en su código de conexión a la base de datos (`src/lib/db.ts`). `DB_PORT` es opcional; si se omite, el valor predeterminado es `5432`. Como alternativa a las variables individuales `DB_*`, puede proporcionar una única cadena de conexión `DATABASE_URL`; si se establece, esta tendrá prioridad.

Secretos personales vs. secretos del proyecto

TIPO	ESTABLECIDO POR	DÓNDE SE APLICA	CASO DE USO
Secreto personal	Usted, en **Perfil > Seguridad**	Cada espacio de trabajo de su propiedad, por defecto	Sus propias claves API, tokens, credenciales de servicio
Secreto de proyecto	Propietario del proyecto, en los recursos del proyecto	El proyecto, luego adjunto a los espacios de trabajo	Credenciales de base de datos compartidas, claves API de equipo, URL de servicio

Ninguno de los tipos es todo o nada. Tú eliges a qué espacios de trabajo llega un secreto, aunque los dos funcionan de manera diferente:

- **Secretos personales** se inyectan en cada espacio de trabajo que posees por defecto. Para restringir eso, cambia el secreto a **Lista personalizada** y selecciona los espacios de trabajo a

los que se aplica. Un espacio de trabajo que no selecciones no recibe el secreto, lo cual es útil cuando una credencial pertenece a tu propio proyecto pero no a un espacio de trabajo que compartes con otros.

- **Secretos de proyecto** se ponen a disposición del proyecto y luego se adjuntan a espacios de trabajo individuales cuando el espacio de trabajo se crea o a través de la plantilla del espacio de trabajo. Un secreto de proyecto solo llega a los espacios de trabajo a los que está adjunto.

Ambos tipos se pueden inyectar como una **variable de entorno** o como un **archivo**. Los secretos de archivo aparecen en la carpeta `/secrets`; los secretos de entorno aparecen en la salida de `env`.

Tres cosas que vale la pena saber:

- **Los cambios requieren un reinicio.** Añadir, editar o reorientar un secreto surte efecto cuando los espacios de trabajo afectados se reinician, no de inmediato.
- **Los nombres se convierten en nombres de variables de entorno**, por lo que no pueden contener espacios, guiones o caracteres especiales, y los nombres reservados por Linux son rechazados.
- **Los secretos personales prevalecen en caso de conflicto de nombres.** Si un secreto de espacio de trabajo tiene el mismo nombre que uno de tus secretos personales, el valor proviene de tu secreto personal.

En este ejercicio, añadiste los secretos directamente al espacio de trabajo. En un proyecto real, el propietario del proyecto normalmente configuraría los secretos compartidos a nivel de proyecto para que estuvieran disponibles para todos automáticamente. Solo añadirías secretos personales (como tus propias claves API) a través de **Perfil > Seguridad > Secretos personales**.

Paso 3: Iniciar la aplicación

Abre el IDE en la nube (VS Code para la web) y abre una terminal. Inicia la base de datos PostgreSQL y luego el servidor de desarrollo:

```
cd /home/developer/demo-nodejs-postgresql-main

docker-compose up -d    # start PostgreSQL (first run initializes the
database)

yarn dev
```

VS Code detecta el puerto abierto (3000) y muestra una notificación: **"Una aplicación de espacio de trabajo está disponible en el puerto 3000"**. Selecciona **Vista previa** para abrir la aplicación en el navegador integrado de VS Code.

Deberías ver la interfaz del Proyecto ACME. Intenta añadir un usuario y buscar; esto ejercita la pila completa (de React a la API y a PostgreSQL).

Estás listo

Tu espacio de trabajo Hello World está en ejecución y listo para el trabajo de desarrollo. Has experimentado:

- Crear un espacio de trabajo a partir de una imagen de contenedor
- Configurar secretos como variables de entorno
- Ejecutar una aplicación fullstack con una base de datos

Qué hacer a continuación

OBJETIVO	GUÍA
Aprende el ciclo de desarrollo diario de Node.js en SecurSpaces	Tutorial: Desarrollar, depurar y compartir una aplicación Node.js — continúa en este espacio de trabajo
Configura tu entorno de proyecto real	Configura tu cuenta y Crea y conéctate a tu espacio de trabajo
Comprender los conceptos y la terminología de SecurSpaces	¿Qué es SecurSpaces?(/es-es/securspaces/about/securspaces-for-developers.html)

Obtener ayuda

- **Pregunta al propietario de tu proyecto** sobre qué plantilla usar para tu proyecto real.
- **Consulta la documentación de SecurSpaces** para guías detalladas.

Develop, debug, and share a Node.js app

`Developer`

Este tutorial le enseña el ciclo de desarrollo diario en Citrix SecurSpaces™ trabajando con una aplicación real. La ejecuta, la cambia, la depura tanto en el servidor como en el navegador,

detecta errores antes de que lleguen al navegador y comparte el resultado con un compañero de equipo.

Al finalizar, habrá:

- Iniciado una base de datos PostgreSQL y una aplicación Next.js dentro de su espacio de trabajo
- Cambiado la aplicación en ejecución y observado cómo se recargaba
- Inspeccionado los mismos datos a través del navegador, la API y la base de datos
- Pausado el código del lado del servidor y del lado del navegador en un depurador
- Compartido su aplicación en ejecución con su proyecto a través de una única URL

Cada paso se basa en el anterior, así que sígalos en orden. El tutorial completo dura unos 30 minutos.

Antes de empezar

Necesita un espacio de trabajo **Hello World** en ejecución, creado como se describe en Espacio de trabajo Hello World, con los cinco secretos `DB_*` configurados.

La imagen de contenedor de Hello World no está disponible para todos los proyectos de forma predeterminada. Si no la encuentra al crear un espacio de trabajo, pida al propietario de su proyecto que configure un proyecto de prueba de Hello World para su organización. El artículo Espacio de trabajo Hello World les indica qué añadir.

Abra su espacio de trabajo Hello World en el Cloud IDE (VS Code para Web) antes de comenzar el Paso 1.

Paso 1: Compruebe su entorno

Confirme que su espacio de trabajo tiene las herramientas y los secretos de los que depende este tutorial. Abra un terminal en el Cloud IDE y ejecute:

```
node --version

yarn --version
```

Ambos comandos imprimen un número de versión. Las versiones exactas no importan para este tutorial.

Ahora, confirma que las credenciales de la base de datos llegaron a tu espacio de trabajo como variables de entorno:

```
echo $DB_HOST

echo $DB_PORT

echo $DB_NAME

echo $DB_USER

echo $DB_PASSWORD
```

Estos imprimen `localhost`, `5432`, `project_acme`, `acme_user` y `acme_password`.

Si alguno de ellos imprime una línea vacía, los secretos no se añadieron cuando se creó el espacio de trabajo. Vuelve a Espacio de trabajo Hello World, Paso 1, añade los cinco secretos y reinicia el espacio de trabajo antes de continuar.

Observa que no creaste un archivo `.env`. SecurSpaces inyecta los secretos en el espacio de trabajo como variables de entorno, por lo que la aplicación los encuentra sin ninguna configuración local.

Paso 2: Iniciar la base de datos

La aplicación almacena sus usuarios en PostgreSQL, que se ejecuta en un contenedor Docker dentro de tu espacio de trabajo. Inícialo antes que la aplicación, o la primera carga de la página fallará.

```
cd /home/developer/demo-nodejs-postgresql-main

docker-compose up -d
```

La primera ejecución no descarga nada —la imagen ya está en el espacio de trabajo— e inicializa el esquema de la base de datos desde `init.sql`. Tarda unos segundos.

Confirma que el contenedor se está ejecutando:

```
docker ps
```

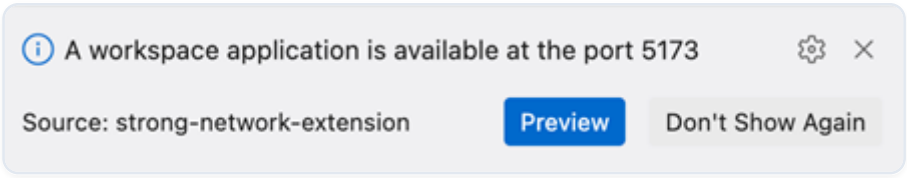
La salida muestra un contenedor llamado `project-acme-db` con un estado que comienza con `Up`. Si la lista está vacía, ejecuta `docker-compose up -d` de nuevo y lee cualquier error que imprima.

Paso 3: Ejecutar la aplicación

Con la base de datos en funcionamiento, inicia el servidor de desarrollo desde el mismo directorio:

```
yarn dev
```

VS Code detecta que la aplicación abrió un puerto y muestra una notificación: **Una aplicación del espacio de trabajo está disponible en el puerto 3000**. Selecciona **Vista previa**.



La aplicación de gestión de usuarios del Proyecto ACME se abre en una pestaña del editor junto a tu código. La dirección de vista previa sigue el patrón `https://<workspace-id>-port-3000.proxy.<domain>`, por lo que la aplicación es accesible a través de la plataforma en lugar de desde tu propia máquina.

Seleccione **Usuarios** en la barra de navegación y, a continuación, añada un usuario. La página lo guarda y lo muestra en la lista.

Acaba de ejercitar toda la pila: la página de React llamó a la API, la API escribió en PostgreSQL y el resultado volvió al navegador. Conserve este usuario; lo volverá a ver en el Paso 5.

Deje `yarn dev` en ejecución.

Paso 4: Realizar un cambio

Cambie la aplicación mientras se ejecuta y observe cómo aparece el resultado sin necesidad de reiniciar.

1. En el IDE en la nube, abra `src/app/page.tsx`.
2. Busque el encabezado de la página y cambie su texto. Por ejemplo, cámbielo a `Welcome to My ACME Project`.
3. Guarde el archivo.

La pestaña de vista previa se actualiza en unos segundos. No reinició el servidor ni reconstruyó nada; el servidor de desarrollo detectó el cambio y recargó la página por usted.

Este es el ciclo en el que pasará la mayor parte del día: editar, guardar, ver. Se comporta exactamente igual que en una máquina local.

Paso 5: Examinar la base de datos

El usuario que añadió en el Paso 3 es una fila real en una base de datos real. Abra una **segunda terminal** para que el servidor de desarrollo siga ejecutándose en la primera y, a continuación, conéctese a PostgreSQL:

```
docker exec -it project-acme-db psql -U acme_user -d project_acme
```

Observe que el indicador cambia: ahora está escribiendo en PostgreSQL, no en el shell. Liste los usuarios:

```
SELECT * FROM users;
```

Su usuario del Paso 3 aparece en los resultados, junto con los usuarios de ejemplo que creó el esquema. La página del navegador, la ruta de la API y esta tabla son tres vistas de los mismos datos.

Salga de PostgreSQL y vuelva al shell:

```
\q
```

Paso 6: Depurar la API

Ahora pausa el código del lado del servidor mientras una solicitud lo atraviesa.

El depurador necesita iniciar la aplicación por sí mismo, así que primero detén el servidor de desarrollo que iniciaste en el Paso 3. Selecciona la terminal que ejecuta `yarn dev` y pulsa **Ctrl+C**.

1. Abre `src/app/api/users/route.ts`.
2. Busca la función `GET` y selecciona el margen a la izquierda de una línea dentro de ella. Un punto rojo marca el punto de interrupción.
3. Abre una nueva terminal y elige **JavaScript Debug Terminal** de la lista de tipos de terminal.

4. En esa terminal, inicia la aplicación de nuevo:

```
cd /home/developer/demo-nodejs-postgresql-main

yarn dev
```

5. Abre la vista previa y selecciona **Users**.

La ejecución se detiene en tu punto de interrupción y el IDE en la nube cambia a la vista de depuración. Expande la variable `result` y abre `result.rows` para ver los registros que PostgreSQL devolvió, incluyendo el usuario que añadiste.

Selecciona **Continuar** para que la solicitud finalice. La página de Usuarios se renderiza entonces como de costumbre.

Ten en cuenta que abriste la página de **Users** en lugar de la página de inicio. La página de inicio es estática y nunca llama a la API, por lo que un punto de interrupción en la ruta de la API nunca se alcanzaría desde ella.

Elimina el punto de interrupción seleccionando de nuevo el punto rojo, y deja la terminal de depuración en ejecución.

Paso 7: Depurar en el navegador

El código del lado del servidor no es el único lugar donde se esconde un problema. Este paso depura el código que se ejecuta en el navegador, lo que requiere una herramienta diferente.

La aplicación tiene un interruptor **Lento** que retrasa cada llamada a la API entre dos y tres segundos en el navegador. Está diseñado para probar los estados de carga.

1. Copia la dirección de vista previa y ábrela en una **pestaña del navegador**. El navegador simple integrado en el Cloud IDE no tiene herramientas de desarrollador, por lo que este paso requiere una pestaña real.
2. Selecciona el interruptor **Slow** en la barra de navegación.
3. Abre las herramientas de desarrollador de tu navegador pulsando **F12**, y selecciona la pestaña **Network**.
4. Vuelve a cargar la página de **Users**. Cada solicitud `/api/users` ahora tarda de dos a tres segundos.
5. Selecciona el interruptor **Fast** y vuelve a cargar. El retraso ha desaparecido.

Para pausar dentro del propio retardo, selecciona la pestaña **Sources**, abre `src/app/utils/delay.ts`, y establece un punto de interrupción dentro de `simulateDelay`. Vuelve a cargar la página de Users. La ejecución se pausa y puedes inspeccionar `isSlowMode` y `slowDelay`.

Ahora has utilizado ambos depuradores: el Terminal de depuración de JavaScript para el código que se ejecuta en el servidor, y tus herramientas de desarrollador del navegador para el código que se ejecuta en la página.

Paso 8: Detecta errores antes de ejecutar el código

Dos comprobaciones encuentran errores sin iniciar la aplicación en absoluto.

Primero, introduce un error de tipo. Abre `src/app/api/users/route.ts`, cambia un parámetro `string` a `number`, y guarda. Luego ejecuta:

```
yarn type-check
```

El comando falla y nombra el archivo, la línea y la discrepancia. Vuelve a cambiar el parámetro y ejecuta `yarn type-check` de nuevo; se ejecuta silenciosamente.

Ahora introduce un error de lint. Añade una variable no utilizada a cualquier archivo `.ts`, como `const unused = 1;`, y guarda. Luego ejecuta:

```
yarn lint
```

Se informa de la variable no utilizada. Elimínala y ejecuta `yarn lint` de nuevo para confirmar que el proyecto está limpio.

Ambas comprobaciones se ejecutan contra tu código, no contra un servidor en ejecución, por lo que detectan errores en segundos.

Paso 9: Comparte la aplicación en ejecución

Finalmente, permite que otra persona abra tu trabajo sin clonar nada ni esperar un despliegue.

Asegúrate de que `yarn dev` siga en ejecución y luego:

1. En la consola de SecurSpaces, abre la página **Project Overview**.
2. En el menú **Workspace Apps**, selecciona **Create Workspace App**.
3. Introduce estos valores:

- **Puerto:** `3000`
- **Nombre:** `ACME Project`
- **Compartir: Project Sharing**

4. Selecciona **Guardar**.

La consola muestra una URL para la aplicación. Cópiala y envíasela a un miembro del proyecto. La abrirán en un explorador y usarán la aplicación que estás ejecutando, sin necesidad de un espacio de trabajo propio.

Cuando termines, elimina la aplicación de espacio de trabajo para dejar de compartir.

Lo que has aprendido

Ejecutaste una aplicación full-stack dentro de un espacio de trabajo, y todo se comportó como lo hace en una máquina local: los mismos comandos, el mismo depurador, las mismas herramientas del navegador. Lo que cambió es dónde se ejecuta el código y dónde residen los datos.

A lo largo del proceso, tú:

- Confirmaste que los secretos llegan como variables de entorno, sin ningún archivo `.env` que gestionar
- Inició una base de datos con Docker dentro de su espacio de trabajo
- Utilizó recarga en caliente, un depurador del lado del servidor y herramientas de desarrollo del navegador
- Ejecutó la verificación de tipos y el linting
- Compartió una aplicación en ejecución a través de una URL en lugar de una implementación

Qué hacer a continuación

OBJETIVO	GUÍA
Aplique estos flujos de trabajo a su propio proyecto	Desarrollar en un espacio de trabajo
Comprender qué sobrevive a un reinicio del espacio de trabajo	Qué persiste en un espacio de trabajo de SecurSpaces
Configure su entorno de proyecto real	Configurar su cuenta

OBJETIVO	GUÍA
Más información sobre cómo compartir una aplicación en ejecución	Aplicaciones del espacio de trabajo

Obtener ayuda

- **Pregunte a su propietario de proyecto** sobre el contenido de la plantilla, las herramientas que faltan o el acceso a la base de datos.
- **Consulte la documentación de SecurSpaces** para obtener guías detalladas.

Set up a project for your team

`Project Owner`

Tienes un proyecto y un equipo esperando usarlo. Esta página te guía a través de la preparación de ese proyecto para que un desarrollador pueda crear un espacio de trabajo y empezar a contribuir, sin configurar nada por sí mismo.

Sigue los pasos en orden. Cada uno se basa en el anterior: los recursos que registras en los pasos 1 a 3 son los que empaquetas en una plantilla en el paso 4, y las personas que añades en el paso 5 son las que la usan.

Antes de empezar

Necesitas un proyecto y un rol que tenga los siguientes permisos. El rol predeterminado de **Propietario del proyecto** los tiene todos. Un **Administrador** tiene todos excepto Seguridad, que solo es necesario para las credenciales de registro privado.

PASO	PERMISO
Revisar imágenes de contenedor	Recursos establecido en **Importar**
Añadir credenciales de registro para un registro privado	**Seguridad** establecido en **Administrar**
Importar un repositorio de código	**Recursos** establecido en **Importar**
Añadir un secreto	**Recursos** establecido en **Administrar**

PASO	PERMISO
Crear una plantilla de espacio de trabajo	**Espacios de trabajo** configurados en **Administrar proyecto**
Añadir usuarios	**Miembros** configurados en **Administrar**

Parte de esto puede que ya esté hecho. Las imágenes, los repositorios y los secretos se pueden registrar a nivel de plataforma o de organización, y su proyecto los hereda. Compruebe lo que ya tiene antes de añadir nada.

Paso 1: Revisar las imágenes de contenedor

Una imagen de contenedor define el entorno base en el que se ejecuta un espacio de trabajo: el sistema operativo, los tiempos de ejecución del lenguaje, y las herramientas que sus desarrolladores esperan encontrar. Su proyecto hereda las imágenes registradas a nivel de plataforma y de organización, así que empiece por comprobar si alguna de ellas ya se adapta a su equipo.

1. Abra **Recursos** y revise las imágenes de contenedor disponibles para el proyecto.
2. Si una imagen heredada funciona para su equipo, pase al paso 2.
3. Para añadir la suya propia, seleccione **Añadir imagen** y proporcione la **URL**, el **Nombre de la imagen** y la **Etiqueta de la imagen**.

Si la imagen se encuentra en un registro privado, añada primero la credencial del registro; de lo contrario, la importación no podrá autenticarse. Los registros públicos no necesitan credenciales.

Consulte Imágenes de contenedor y Imágenes de espacio de trabajo para saber cómo se superponen las cadenas de herramientas sobre una imagen.

Paso 2: Añadir un repositorio de código

Registrar un repositorio con el proyecto es lo que permite a la plataforma inyectar credenciales para él en tiempo de ejecución. Los desarrolladores pueden clonar y enviar sin tener ninguna credencial, que es la razón principal por la que su dispositivo nunca necesita acceso Git a su código fuente.

Los repositorios se importan de un proveedor que su administrador de plataforma ya ha conectado: GitHub, GitLab, Bitbucket o Azure DevOps.

1. Abrir **Recursos** y seleccionar **Importar repositorio**.

2. Seleccionar el proveedor.
3. Seleccionar los repositorios que se pondrán a disposición en este proyecto.

Si el proveedor que necesita no se ofrece, es que aún no se ha conectado a nivel de plataforma. Pida a su administrador de plataforma que lo añada. Consulte Repositorios de código para lo que implica.

Consulte Repositorios de código para la tarea a nivel de proyecto.

Paso 3: Configurar secretos

Un secreto contiene una contraseña, un token o una clave que el código necesita en tiempo de ejecución. Registrarlo en el proyecto significa que se entrega al espacio de trabajo en lugar de guardarse en el repositorio o pegarse en la consola de un desarrollador.

Su proyecto hereda secretos de los niveles de plataforma y organización, así que revíselos primero.

1. Abrir **Recursos > Secretos** y revisar lo que ya tiene el proyecto.
2. Para añadir uno, seleccione **Añadir un nuevo secreto** y proporcione un nombre y un valor.
3. Añada una descripción para que la siguiente persona sepa para qué sirve.

Los secretos se adjuntan a un espacio de trabajo cuando este se crea, o a través de la plantilla que cree en el siguiente paso.

Consulte Secretos.

Paso 4: Crear una plantilla de espacio de trabajo

Este es el paso que convierte los tres anteriores en algo que un desarrollador puede usar. Una plantilla combina una imagen, repositorios, secretos y configuraciones de seguridad en una sola definición, de modo que la creación de un espacio de trabajo se convierte en una única acción con un resultado predecible.

Sin una plantilla, cada desarrollador configura un espacio de trabajo manualmente, y no hay dos exactamente iguales.

1. Abre **Plantillas** y selecciona **Crear nueva plantilla**.
2. Elige una imagen de contenedor, luego añade los repositorios, secretos y configuraciones de seguridad que el equipo necesite.
3. Guárdalo como borrador.

4. Prueba el borrador y luego publícalo como una versión de plantilla.

Un borrador se puede probar antes de que alguien dependa de él, y una versión publicada no se puede editar después, así que prueba antes de publicar.

Dos cosas que vale la pena hacer aquí:

- **Crea más de una plantilla si tu equipo tiene más de un trabajo.** Los desarrolladores front-end y back-end raramente necesitan las mismas herramientas, y una imagen más pequeña se inicia más rápido.
- **Genera un enlace de inicio rápido.** Crea un espacio de trabajo a partir de la plantilla con un solo clic, lo cual es útil desde un README o un portal de ingeniería.

Consulta Plantillas.

Paso 5: Añadir usuarios

Con el entorno listo, incorpora a las personas que lo usarán.

1. Abre **Personas** y selecciona **Añadir nuevo usuario**.
2. Introduce la dirección de correo electrónico del usuario. La plataforma la compara con el proveedor de identidad configurado.
3. Asigna un rol: **Invitado**, **Desarrollador**, **Gerente** o **Propietario del proyecto**.
4. Para contratistas o cualquier persona temporal, selecciona **Establecer fecha de caducidad** y elige cuándo finaliza su acceso.

La mayoría de los desarrolladores deberían tener el rol de **Desarrollador**, lo que les permite crear sus propios espacios de trabajo a partir de tu plantilla. Asigna **Invitado** a alguien que solo necesite consultar, y crea el espacio de trabajo para ellos tú mismo.

Si ninguno de los cuatro roles predeterminados encaja, puedes definir el tuyo propio. Consulta Roles y permisos.

Consulta Añadir y eliminar usuarios.

Qué hacen tus desarrolladores a continuación

Una vez que se ha añadido un desarrollador y existe una plantilla, pueden crear un espacio de trabajo y conectarse a él. Dirígelos a Tu primer espacio de trabajo.

Si prefieres enviarles algo escrito para la incorporación, consulta Incorporar desarrolladores, que incluye una plantilla reutilizable que puedes adaptar.

Información relacionada

- Incorporar desarrolladores
- Administrar
- Roles y permisos
- Recursos del proyecto

Develop

Esta sección es para **desarrolladores** que trabajan dentro de un espacio de trabajo de Citrix SecurSpaces™. Cubre la conexión a un espacio de trabajo, la ejecución de su código, el uso compartido de lo que cree y la configuración que usted puede controlar.

Si no ha utilizado la plataforma antes, empiece con Tutorial: Su primer espacio de trabajo.

Trabajo diario

TAREA	PÁGINA
Conectar, instalar herramientas, ejecutar una aplicación y usar secretos	Desarrollar en un espacio de trabajo
Orientarse en la consola	Descripción general de la consola
Crear, iniciar, detener y compartir espacios de trabajo	Espacios de trabajo
Conectarse desde su propio IDE o terminal	Conectarse a través de SSH

Saber antes de perder el trabajo

TAREA	PÁGINA
Comprender qué archivos sobreviven a un reinicio	Qué persiste en un espacio de trabajo

Acceder a otros sistemas

TAREA	PÁGINA
Acceder a un servidor o servicio fuera de la plataforma	Conectarse a servicios externos a través de SSH

TAREA	PÁGINA
Permitir que un compañero abra algo que estás ejecutando	Compartir una aplicación en ejecución

Tu configuración

TAREA	PÁGINA
Gestionar tus claves SSH, tokens e integraciones	Tu perfil

Configuraciones menos comunes

TAREA	PÁGINA
Mantener los contenedores Docker entre reinicios	Docker persistente
Ejecutar un entorno de escritorio en un espacio de trabajo	Ejecutar un escritorio gráfico
Abrir la consola en su propia ventana	Instalar SecurSpaces como aplicación de escritorio
Trabajar desde un escritorio virtual existente en lugar de un espacio de trabajo	Trabajar desde un escritorio virtual
Dirigir un asistente de IA a esta documentación	Dar acceso a la documentación a su asistente de IA

Cuando algo va mal

TAREA	PÁGINA
Resolver problemas comunes	Solución de problemas

Develop in a workspace

`Developer`

Este artículo cubre el trabajo diario de desarrollo dentro de un espacio de trabajo de Citrix SecurSpaces™: conectarse, instalar herramientas, ejecutar y previsualizar una aplicación, usar secretos y compartir lo que construyas.

Si eres nuevo en SecurSpaces, sigue Tutorial: Tu primer espacio de trabajo primero.

> **Acerca de los ejemplos:** los ejemplos aquí utilizan Node.js, porque se lee claramente sea cual sea el lenguaje en el que trabajes. Nada en esta página es específico de Node. La plataforma trata cada cadena de herramientas de la misma manera, así que sustituye tus propios comandos — `pip install` por `npm install`, `go run` por `yarn dev`, y así sucesivamente.

Elige cómo conectarte

Puedes trabajar en un espacio de trabajo de dos maneras.

MÉTODO	QUÉ ES	IDEAL PARA
IDE en la nube	VS Code para Web, ejecutándose en una pestaña del navegador	Empezar, cualquier dispositivo, sesiones cortas
IDE local a través de SSH	Tu propio IDE instalado, conectado al espacio de trabajo	Trabajo diario, configuración familiar y atajos

El IDE en la nube no necesita instalación: seleccione **Abrir** en la tarjeta del espacio de trabajo y se abrirá en una nueva pestaña.

Una tarjeta de espacio de trabajo que muestra el nombre del espacio de trabajo, el propietario, el estado de ejecución y los botones de acceso al IDE en la nube, al terminal y a SSH(/en-us/securspaces/media/workspace-light-cropped.png)

Los botones de la tarjeta del espacio de trabajo son sus puntos de entrada: el icono de VS Code abre el IDE en la nube, el icono del terminal abre un shell, y el icono de SSH abre el cuadro de diálogo **Conectar vía SSH**.

VS Code para Web es el único IDE en la nube que ofrece la plataforma. Si su equipo necesita un IDE diferente basado en navegador, se puede integrar en una imagen de espacio de trabajo personalizada; hable con el administrador de su plataforma. Para IDE locales, SecurSpaces es

compatible con VS Code Desktop, Cursor, Windsurf, Kiro y JetBrains Gateway, además de cualquier editor compatible con SSH. Consulte Conectarse a un espacio de trabajo vía SSH.

Mover archivos dentro y fuera de un espacio de trabajo

La forma más sencilla de introducir un archivo local es arrastrarlo desde el gestor de archivos a la ventana del IDE en la nube. Para extraer un archivo, utilice la acción **Descargar** del IDE en la nube en el menú contextual del explorador de archivos.

La transferencia de archivos puede estar restringida en su plataforma, ya que es un control de prevención de pérdida de datos. Si arrastrar un archivo no tiene ningún efecto, pregunte al administrador de su plataforma si las transferencias están permitidas para su proyecto.

Instalar herramientas y dependencias

Un espacio de trabajo está en contenedores y es **efímero**: se recrea a partir de su imagen base en cada inicio. Las herramientas que instale en tiempo de ejecución solo persisten si residen en el volumen persistente `/home/developer/`. Las instalaciones a nivel de sistema (por ejemplo, `sudo apt-get install`) se descartan cuando el espacio de trabajo se reinicia.

Antes de instalar nada, elija un enfoque que se ajuste a lo que necesita conservar:

- Las **herramientas con ámbito de usuario** (`nvm`, `pyenv`, `pipx`, `cargo install` y similares) se instalan en `/home/developer/` y persisten automáticamente.
- La **configuración por lanzamiento o los paquetes únicos** pertenecen a un script de inicio.
- Los **paquetes de sistema y tiempos de ejecución compartidos entre un equipo** pertenecen a una imagen de contenedor personalizada.

Las dependencias del proyecto instaladas en su directorio de proyecto persisten, siempre que el proyecto se encuentre en `/home/developer`. Los gestores de paquetes que se instalan globalmente por defecto deben redirigirse a su directorio de inicio. Por ejemplo, con npm:

```
npm config set prefix ~/.npm-global

export PATH=~/.npm-global/bin:$PATH
```

Añada la línea `PATH` a su archivo `.bashrc` o `.zshrc` a través de la configuración de su perfil para que sea permanente.

Para obtener la guía completa y las compensaciones, consulte Lo que persiste en un espacio de trabajo de SecurSpaces.

Ejecutar y previsualizar una aplicación

Inicie su aplicación de la forma habitual:

```
cd /home/developer/my-project

yarn dev
```

Su servidor debe escuchar en `0.0.0.0`, no en `localhost`. Un servidor enlazado a `localhost` solo es accesible desde dentro del contenedor, por lo que la plataforma no puede detectarlo y usted no puede previsualizarlo. La mayoría de los frameworks se enlazan correctamente en modo de desarrollo, pero algunos necesitan que se les indique:

```
npx vite --host 0.0.0.0

npx next dev -H 0.0.0.0
```

Lo mismo se aplica en cualquier lenguaje; por ejemplo, Flask necesita `--host=0.0.0.0`, y un servidor Go debería escuchar en `:8080` en lugar de `127.0.0.1:8080`.

Cuando el servidor se inicia, VS Code detecta el puerto abierto y muestra una notificación: **Una aplicación del espacio de trabajo está disponible en el puerto** . Seleccione **Previsualizar** para abrir la aplicación en una pestaña del editor.

La dirección de previsualización sigue el patrón `https://<workspace-id>-port-<number>.proxy.<domain>`, por lo que el tráfico llega a su aplicación a través de la plataforma. Puede pegar esa dirección en cualquier pestaña del navegador. El panel **Aplicaciones del espacio de trabajo** en la consola de SecurSpaces enumera cada puerto expuesto.

Ejecutar varios servicios a la vez funciona como se espera: un frontend en el puerto 3000 y una API en el puerto 4000 son ambos detectados y ambos accesibles.

Ejecutar servicios de los que depende su proyecto

Los espacios de trabajo admiten Docker-in-Docker, por lo que las bases de datos, cachés y colas de mensajes se ejecutan dentro del espacio de trabajo tal como lo harían en su propia máquina. Defínalos con Docker Compose:

```
# docker-compose.yml

version: '3.8'

services:

  postgres:

    image: postgres:15

    environment:

      POSTGRES_DB: myapp

      POSTGRES_USER: dev

      POSTGRES_PASSWORD: devpass

    ports:

      - "5432:5432"
```

Inícielos, compruébelos y deténgalos:

```
docker-compose up -d

docker ps

docker-compose down
```

Su aplicación accede a estos servicios a través de `localhost`, igual que en el desarrollo local.

Algunas imágenes proporcionan el complemento Docker Compose en lugar del comando independiente. En ese caso, use `docker compose` con un espacio; los subcomandos son idénticos.

Usar secretos y variables de entorno

Las credenciales, tokens y direcciones de servicio llegan a su espacio de trabajo como secretos, inyectados al inicio. No mantiene un archivo `.env` para ellos, y nunca entran en su código o en su historial de Git.

TIPO	ESTABLECIDO POR	DÓNDE SE APLICA
Secreto personal	Usted, en **Perfil > Seguridad**	Cada espacio de trabajo de su propiedad, por defecto
Secreto de proyecto	Propietario del proyecto, en los recursos del proyecto	El proyecto, luego adjunto a los espacios de trabajo

Ninguno de los dos tipos es todo o nada:

- **Los secretos personales** se inyectan en cada espacio de trabajo de su propiedad por defecto. Para restringir eso, cambie el secreto a **Lista personalizada** y seleccione los espacios de trabajo a los que se aplica.
- **Los secretos de proyecto** se adjuntan a espacios de trabajo individuales cuando se crea el espacio de trabajo, o a través de la plantilla de espacio de trabajo.

Ambos tipos se inyectan como una **variable de entorno** o como un **archivo**. Los secretos de archivo aparecen en la `/secrets` carpeta; los secretos de entorno aparecen en la salida `env` y en la API de entorno de su lenguaje:

```
const apiKey = process.env.MY_API_KEY;
```

Tres cosas que vale la pena saber:

- **Los cambios requieren un reinicio.** Añadir, editar o reorientar un secreto surte efecto cuando los espacios de trabajo afectados se reinician.
- **Los nombres se convierten en nombres de variables de entorno**, por lo que no pueden contener espacios, guiones o caracteres especiales, y los nombres reservados por Linux son rechazados.
- **Los secretos personales prevalecen en caso de conflicto de nombres.** Si un secreto del espacio de trabajo tiene el mismo nombre que uno de tus secretos personales, el valor proviene de tu secreto personal.

Para obtener más información, consulta Secretos.

Compartir una aplicación en ejecución

Las aplicaciones del espacio de trabajo exponen una aplicación en ejecución a otros miembros del proyecto, de modo que un revisor, diseñador o probador puede abrir tu trabajo sin una implementación o un espacio de trabajo propio.

1. En la consola de SecurSpaces, abre la página **Project Overview** (Resumen del proyecto).
2. En el menú **Workspace Apps** (Aplicaciones del espacio de trabajo), selecciona **Create Workspace App** (Crear aplicación del espacio de trabajo).
3. Establece el **Puerto** en el que se ejecuta tu aplicación, un **Nombre** y con quién se comparte: **Público**, **Compartir proyecto** o miembros específicos.
4. Selecciona **Save** (Guardar).

También puedes seleccionar el icono **...** en tu espacio de trabajo y seleccionar **Edit Ports** (Editar puertos).

Para obtener más información, consulta Workspace Apps.

Trabajar con un espacio de trabajo compartido

Después de compartir un espacio de trabajo, tú y otro usuario podéis trabajar en él al mismo tiempo. Los cambios aparecen en tiempo real, por lo que podéis coeditar un archivo juntos — útil para trabajar en un problema o para guiar a alguien a través de un código desconocido.

Ambos estáis trabajando en el mismo contenedor, por lo que un comando que uno de vosotros ejecute afectará también a la sesión del otro.

Conservar tu trabajo

Mantén todo lo que te importa bajo `/home/developer`. Eso incluye tu código, tus dependencias y tu configuración de shell. Cualquier cosa fuera de él se descarta cuando el espacio de trabajo se reinicia.

Para las herramientas a nivel de sistema que necesitas siempre, usa un script de inicio o pide a tu propietario de proyecto que las añada a la imagen de plantilla del espacio de trabajo. Consulta Qué persiste en un espacio de trabajo de SecurSpaces.

Solución de problemas

PROBLEMA	SOLUCIÓN
Falta una herramienta en el espacio de trabajo	La plantilla podría ser incorrecta. Pregunta a tu propietario de proyecto cuál usar.
Los paquetes desaparecen después de un reinicio	Mueve tu proyecto y su directorio de dependencias bajo `/home/developer`.

PROBLEMA	SOLUCIÓN
La aplicación no es accesible	Vincula el servidor a `0.0.0.0`, luego verifica el puerto expuesto en **Aplicaciones del espacio de trabajo**.
Las llamadas a una base de datos o servicio fallan	Confirma que el contenedor se ejecuta con `docker ps`, luego inícialo con `docker-compose up -d`.
Los contenedores Docker no se inician	Ejecuta `docker info`. Si Docker no está disponible, pregunta a tu propietario de proyecto sobre el modo privilegiado.
Los cambios en los archivos no activan una recarga	Aumente el límite del observador de archivos con `sudo sysctl -w fs.inotify.max_user_watches=524288`.
`No space left on device`	Elimine los directorios de dependencias no utilizados o aumente el tamaño del disco del espacio de trabajo en **Editar espacio de trabajo > Recursos > Tamaño del disco**.
Arrastrar un archivo al IDE no hace nada	La transferencia de archivos puede estar restringida. Consulte a su administrador de plataforma.

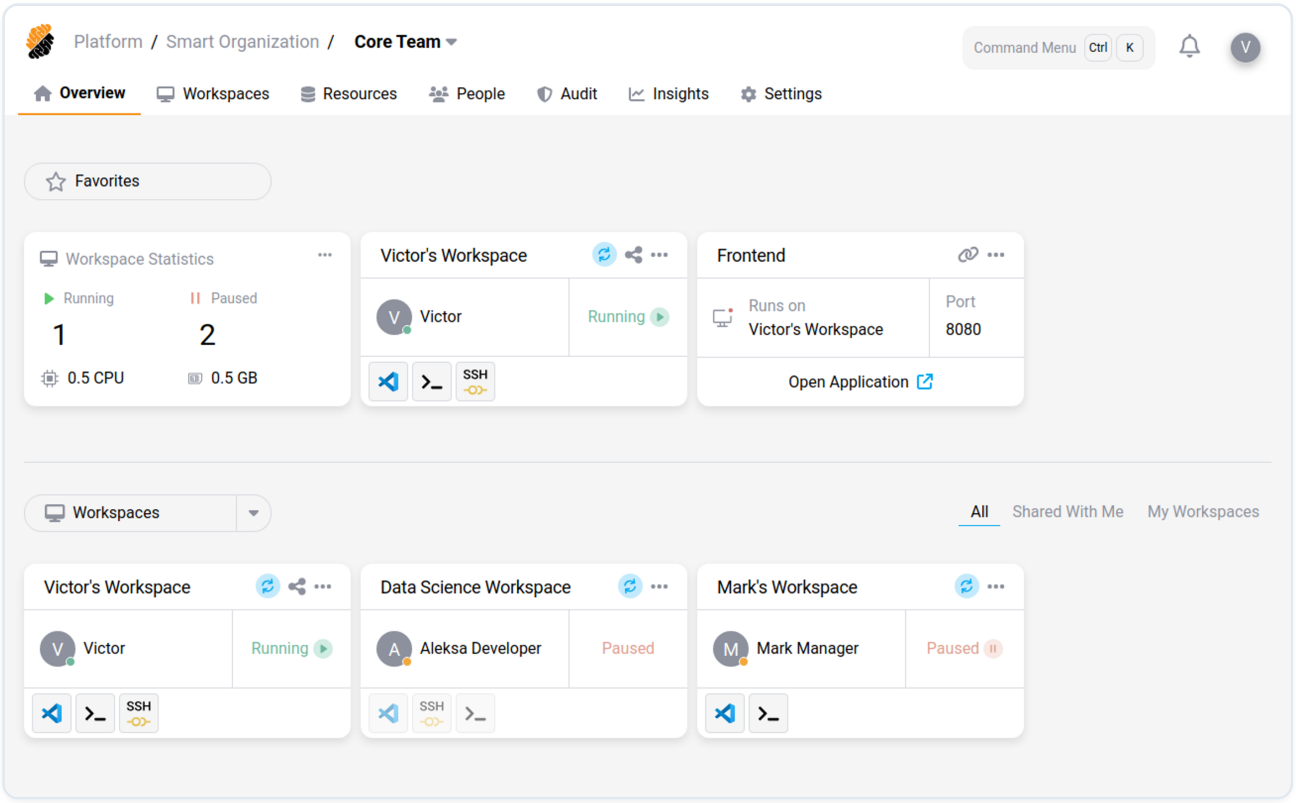
Información relacionada

- Tutorial: Su primer espacio de trabajo
- Conectarse a un espacio de trabajo mediante SSH
- Qué persiste en un espacio de trabajo de SecurSpaces
- Administrar espacios de trabajo
- Aplicaciones del espacio de trabajo

Console overview

La página de Resumen es la primera página que se muestra al acceder a la interfaz de usuario de la plataforma. Contiene los componentes esenciales para permitir un acceso rápido a recursos como espacios de trabajo, aplicaciones, aplicaciones web seguras y métricas.

La **Página de Resumen** es personalizable. Todos los componentes se pueden reordenar según sus preferencias.



- Secciones de visualización
  - Favoritos
  - Espacios de trabajo
  - Aplicaciones del espacio de trabajo
  - Personas y métricas

Menú de comandos

El **Menú de comandos** es una forma de navegar por la consola mediante el teclado. Se encuentra en el encabezado de cada página y se abre con **Ctrl+K**, o **Cmd+K** en macOS. También puede seleccionarlo.

Escriba en **¿Qué desea hacer?** para filtrar o explore los tres grupos:

GRUPO	QUÉ OFRECE
Navegación	Ir a Organizaciones, Proyectos o Configuración del proyecto

GRUPO	QUÉ OFRECE
Perfil	Ir a tu perfil
Espacios de trabajo	Abrir uno de tus espacios de trabajo por nombre

Abrir un espacio de trabajo por nombre es lo más útil de estas opciones, porque no depende de encontrar primero el espacio de trabajo en una lista.

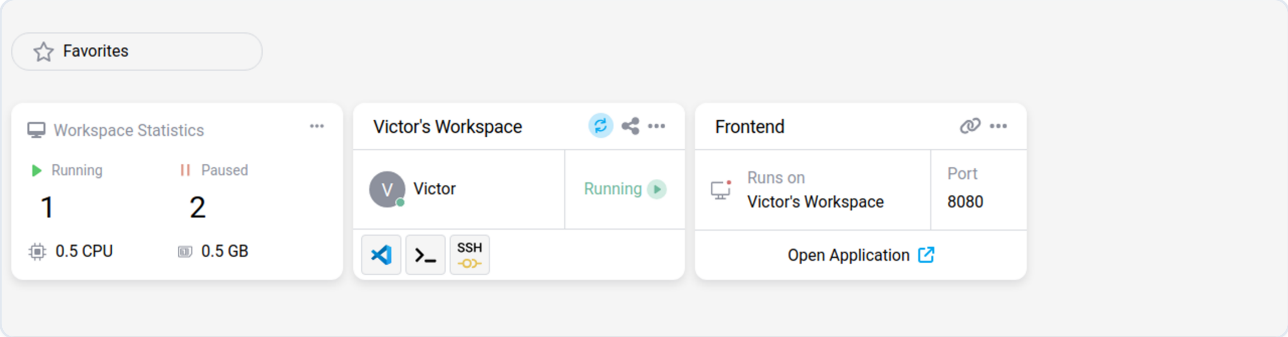
El menú es jerárquico, y las teclas se muestran en la parte inferior: **Intro** selecciona, las **teclas de flecha** mueven, **Retroceso** sube un nivel y **Esc** lo cierra.

> **Nota**
>
> Esto no es lo mismo que la Paleta de comandos dentro de un IDE de espacio de trabajo, que ejecuta comandos contra el propio espacio de trabajo. Consulta Conectarse por SSH.

Secciones de visualización

Favoritos

La sección de **Favoritos** muestra tu lista personal de componentes favoritos, de cualquier sección de la **Página de resumen**.



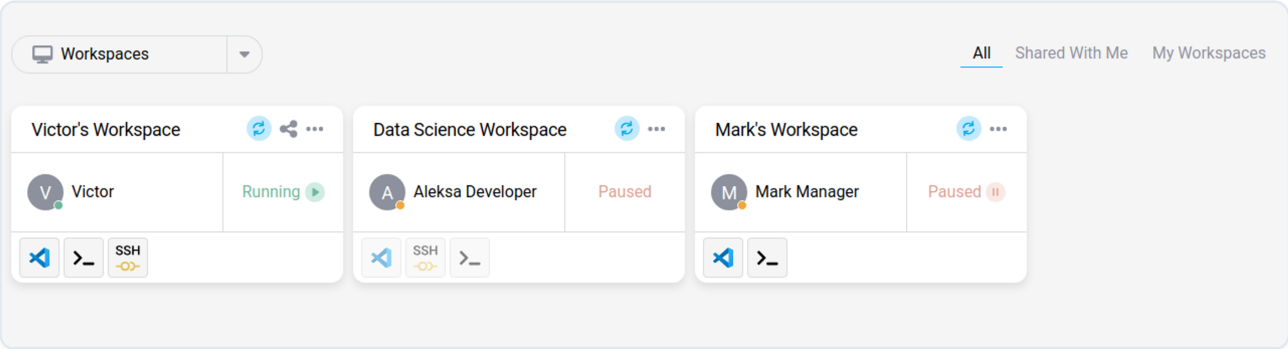
- Para **añadir un elemento** a tu lista, haz clic en su botón "**...**" y en "**Añadir a favoritos**".
- Para **eliminar un elemento** de tu lista, haz clic en su botón "**...**" y en "**Eliminar de favoritos**".

> Consejo:

> Las entradas en la lista de componentes favoritos solo pueden ser componentes de la **Página de resumen**.

Espacios de trabajo

La sección **Espacios de trabajo** muestra todos los Espacios de trabajo del proyecto a los que tienes acceso.

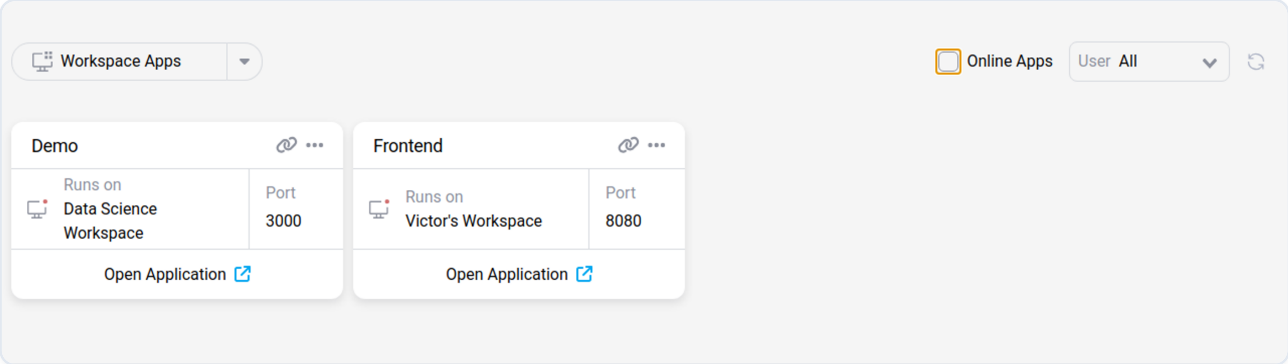


Filtra la lista con **Todos**, **Compartidos conmigo** o **Mis espacios de trabajo**.

- Para crear un nuevo espacio de trabajo, haz clic en el menú desplegable "**Espacios de trabajo**".
- Para gestionar espacios de trabajo, consulta **Gestionar espacios de trabajo**.

Aplicaciones de espacio de trabajo

La sección **Aplicaciones de espacio de trabajo** muestra todas las aplicaciones de espacio de trabajo del proyecto a las que tienes acceso.

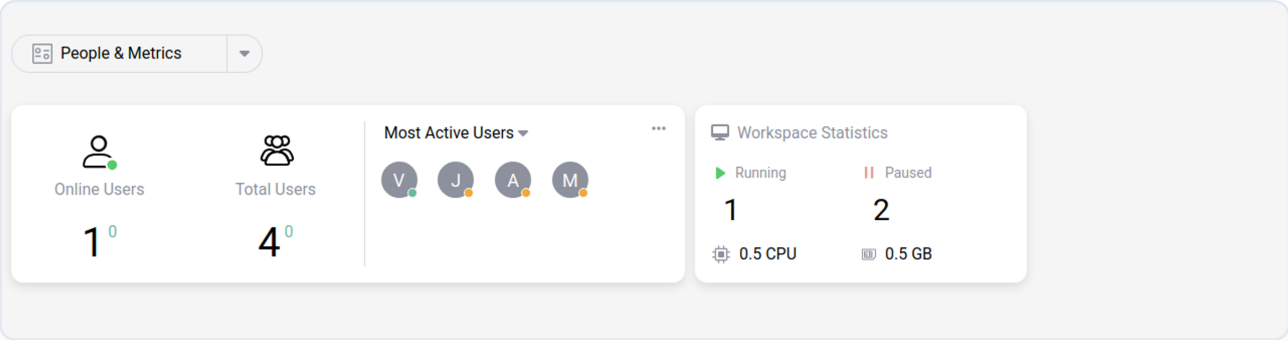


Activa **Aplicaciones en línea** para mostrar solo las aplicaciones que se están ejecutando actualmente, y usa el filtro **Usuario** para mostrar las aplicaciones de un usuario en lugar de **Todos**.

- Para crear una nueva aplicación de espacio de trabajo, haz clic en el menú desplegable "**Aplicaciones de espacio de trabajo**".
- Para gestionar una aplicación de espacio de trabajo, haz clic en su botón "**...**".

Personas y métricas

La sección **Personas y métricas** muestra estadísticas sobre los usuarios del proyecto y métricas sobre la utilización de los recursos.



Las métricas de **Personas** muestran:

- La cantidad de usuarios del proyecto en línea.
- La cantidad total de usuarios del proyecto.
- Estadísticas sobre la cantidad de usuarios en línea durante los últimos siete días.

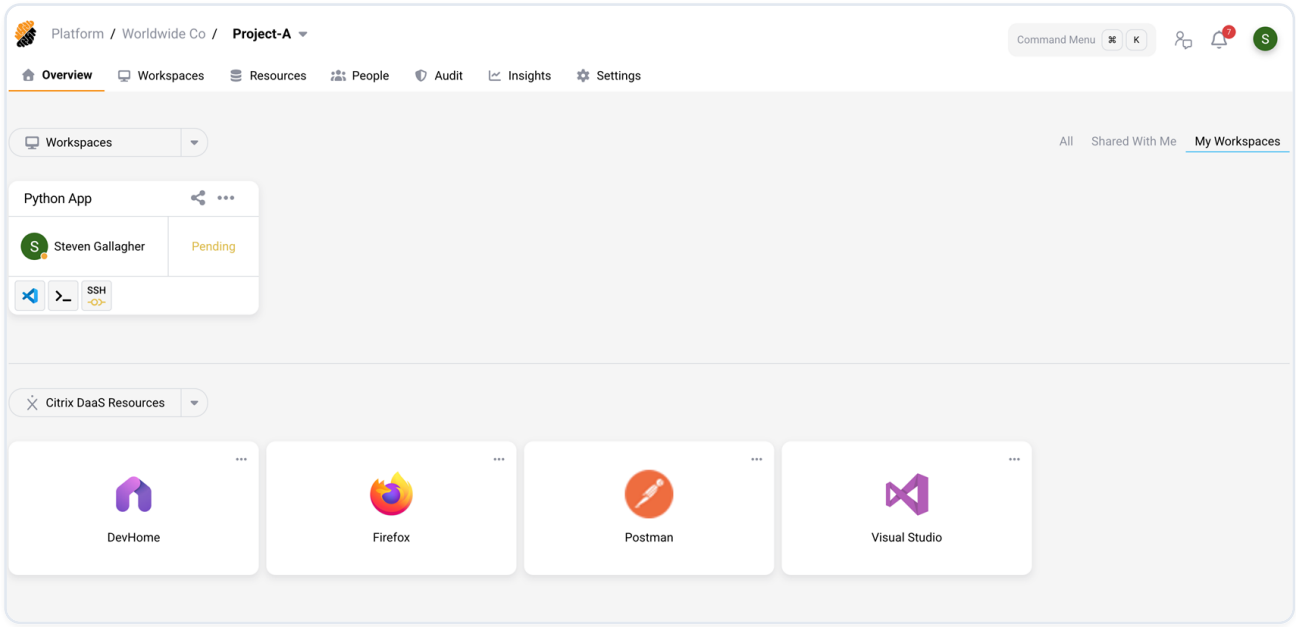
Las métricas de **Espacio de trabajo** muestran:

- Cuántos espacios de trabajo están en ejecución o en pausa.
- El uso total actual de CPU y RAM para su Proyecto.

Consulte la Página de información general para obtener métricas más detalladas.

Recursos de Citrix DaaS

La página de Resumen del proyecto ahora incluye una sección de **Recursos de Citrix DaaS** junto con las secciones existentes de Espacios de trabajo y Aplicaciones de espacio de trabajo. Esta sección muestra las aplicaciones y escritorios virtuales de Citrix que se le han asignado en Citrix DaaS, lo que le proporciona acceso unificado tanto a los espacios de trabajo Citrix SecurSpaces™ basados en Kubernetes como a los recursos basados en Citrix desde una única consola.



Requisitos previos

Antes de que los recursos de Citrix DaaS aparezcan en la página de Resumen:

1. Un administrador de plataforma debe configurar la integración de Citrix DaaS. Consulte Integración de Citrix DaaS.
2. Debe iniciar sesión en su cuenta de Citrix desde **Perfil > Integraciones > Integración de Citrix**. Consulte Integración de Citrix.
3. Debe seleccionar los recursos de Citrix a los que desea acceder. Consulte Seleccionar recursos de DaaS.

Ver y lanzar recursos de Citrix

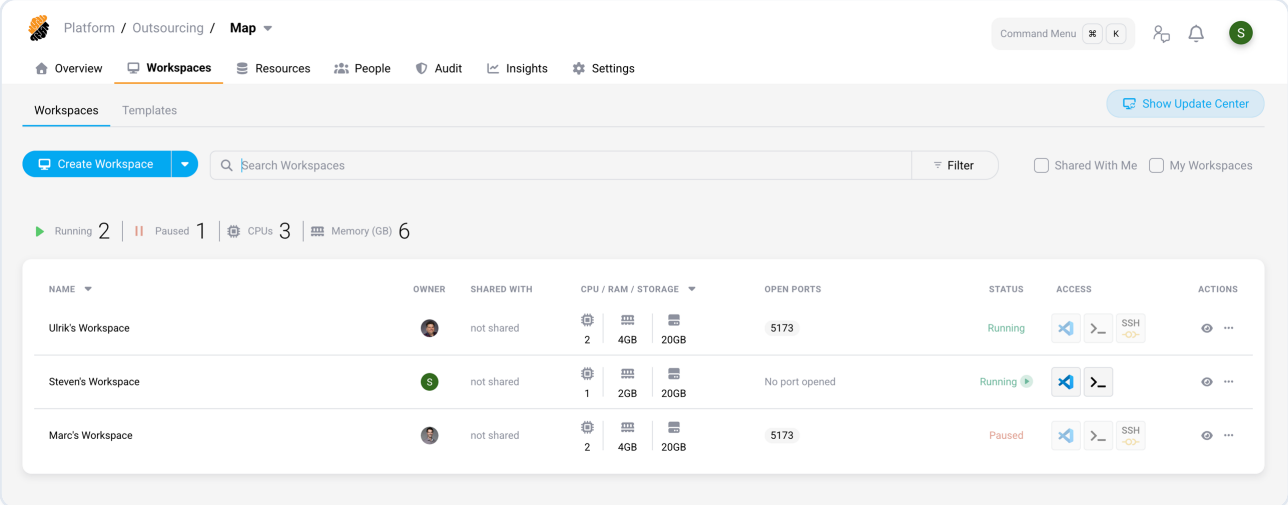
Cuando se cumplen los requisitos previos, la sección **Recursos de Citrix DaaS** de la página de Información general del proyecto muestra las aplicaciones y escritorios virtuales que seleccionó en su perfil. Seleccione un recurso para iniciarlo directamente desde la consola de SecurSpaces.

Si la sección muestra "No Citrix DaaS Resources", verificar que:

- Ha iniciado sesión en su cuenta de Citrix en **Perfil > Integraciones > Integración de Citrix**.
- Ha seleccionado al menos un recurso utilizando el botón **Editar** en la sección **Recursos de DaaS seleccionados** de su perfil.
- Un administrador configura la integración de Citrix DaaS de la plataforma.

Workspaces page

En el ámbito de un proyecto, la **Página de Espacios de Trabajo** muestra todos los espacios de trabajo creados para ese proyecto en particular a los que tiene acceso o puede ver, dependiendo de su nivel de permisos. Esto incluye los espacios de trabajo personales y los espacios de trabajo compartidos con usted. En algunos casos, también incluye las Plantillas de Espacios de Trabajo disponibles en el proyecto.



Búsqueda y filtrado de espacios de trabajo

En proyectos con un gran número de espacios de trabajo, puede ser necesario localizar espacios de trabajo específicos o filtrarlos según ciertas propiedades.

Búsqueda

Utilice la **barra de búsqueda** en la parte superior de la pantalla para encontrar espacios de trabajo por:

- Nombre del espacio de trabajo
- Nombre del propietario
- ID del espacio de trabajo

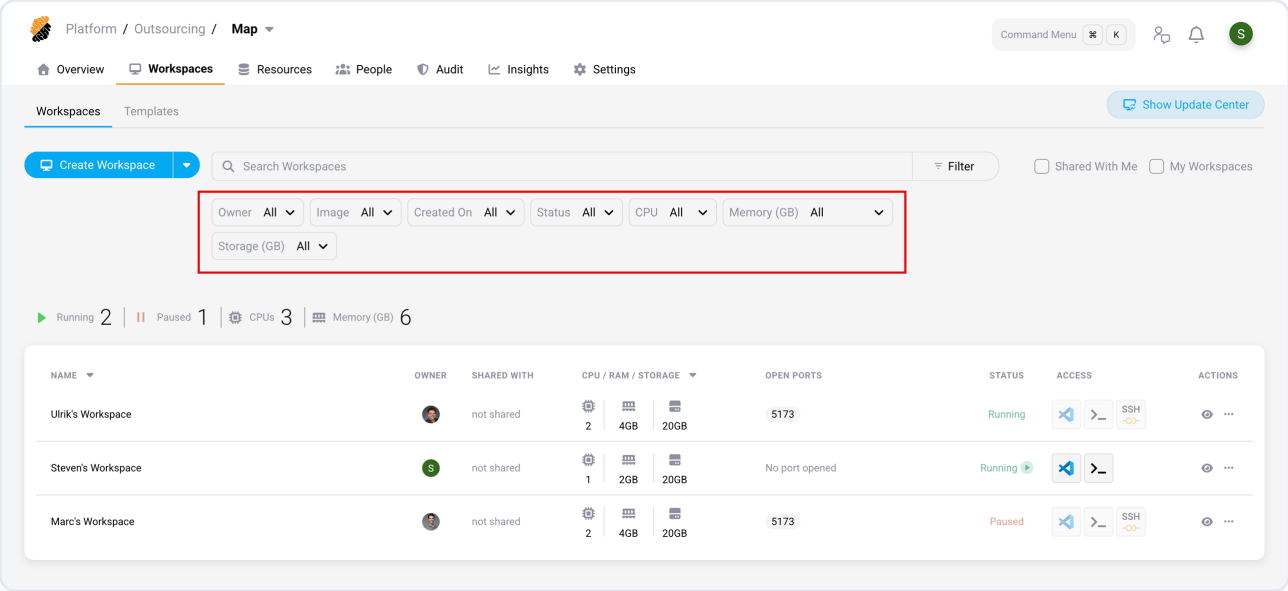
Debajo de la barra de búsqueda, puede ver:

- El número de espacios de trabajo en ejecución y en pausa
- Uso total de CPU
- Uso total de memoria (en GB)

Filtro

Para filtrar espacios de trabajo por propiedades específicas, seleccione el icono de **Filtro** situado a la derecha de la barra de búsqueda. Las opciones de filtro disponibles incluyen:

- Propietario
- Imagen base
- Fecha de creación
- Estado del espacio de trabajo
- Recursos de CPU asignados
- Recursos de memoria asignados
- Espacio en disco asignado



Qué hacer a continuación

- Crear un espacio de trabajo
- Administrar espacios de trabajo
- Crear y administrar aplicaciones de espacio de trabajo
- Crear y administrar plantillas

Create a workspace

Un espacio de trabajo es un entorno de desarrollo en la nube al que se accede a través del IDE del navegador, un terminal o SSH. Citrix SecurSpaces™ crea uno desde la página Espacios de trabajo.

Hay tres rutas. Empezar desde una plantilla es la recomendada, porque la plantilla ya incluye la imagen, los recursos y la política que su proyecto ha acordado.

Configuración básica

Seleccione **Crear espacio de trabajo** en la página Espacios de trabajo o en la página Resumen del proyecto. Se abrirá un cuadro de diálogo **Crear un espacio de trabajo** y le preguntará cómo desea crearlo:

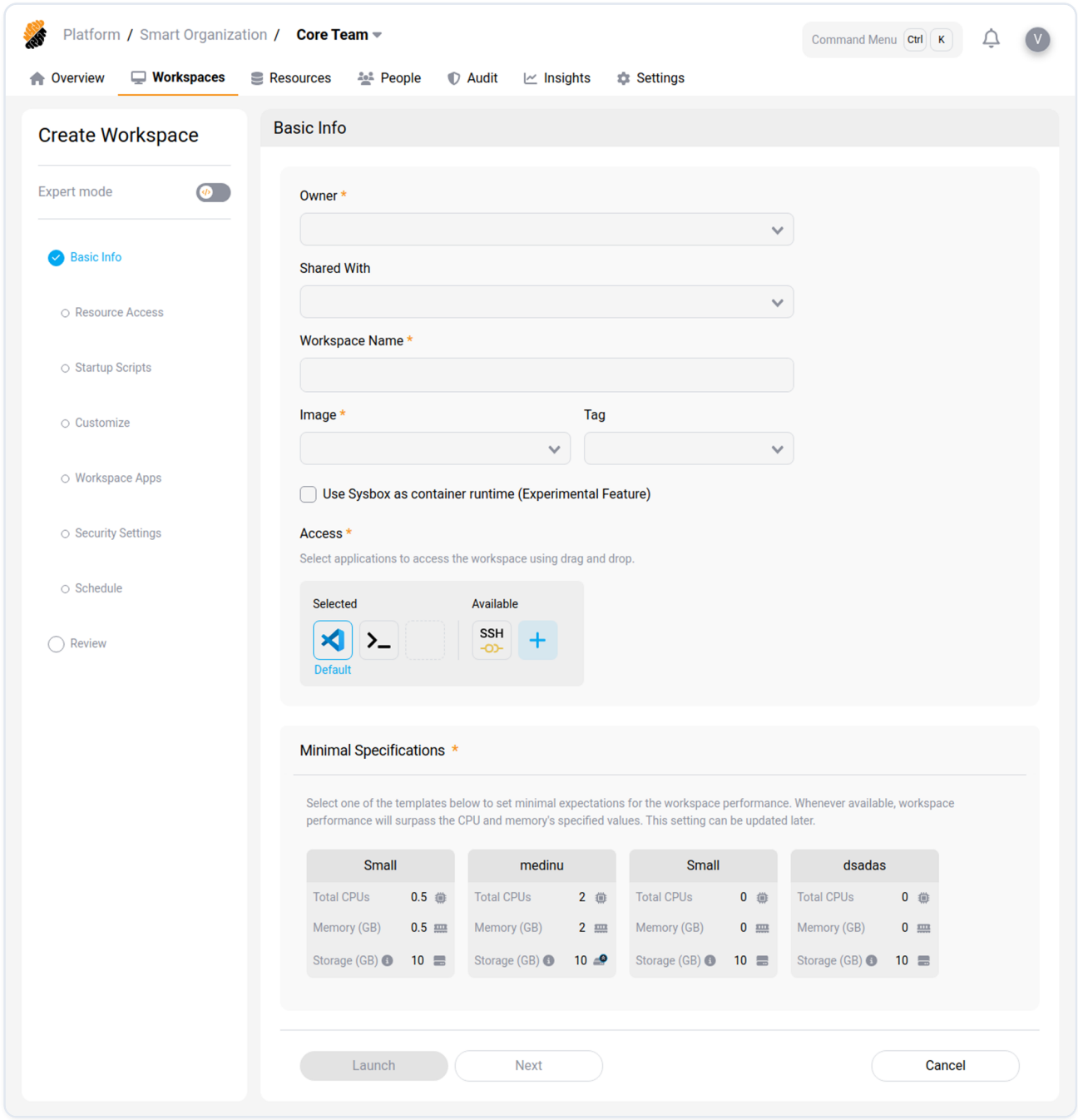
OPCIÓN	QUÉ HACE
Crear desde plantilla (Recomendado)	Comience desde una plantilla predefinida y lista para codificar. Consulte (#from-a-template)
Crear espacio de trabajo personalizado	Configure un nuevo espacio de trabajo desde cero, como se describe a continuación
Copiar espacio de trabajo existente	Duplique la configuración de uno de sus espacios de trabajo. Consulte (#from-an-existing-workspace)

Una opción puede aparecer deshabilitada por dos razones. **Crear desde plantilla** no está disponible cuando el proyecto aún no tiene plantillas. Las otras dos no están disponibles cuando su rol requiere plantillas para la creación de espacios de trabajo; pase el ratón por encima para ver cuál se aplica y póngase en contacto con el propietario de su proyecto si necesita acceso.

Al seleccionar una opción, se abre el asistente correspondiente.

Información básica

El primer paso del asistente contiene la configuración principal: quién es el propietario del espacio de trabajo, qué ejecuta, dónde se ejecuta, y cómo te conectas a él.



Consejo:

Activa el **modo experto** en la parte superior de la barra lateral para editar la configuración del espacio de trabajo directamente como YAML.

CONFIGURACIÓN	QUÉ HACE	MODIFICABLE MÁS TARDE
Propietario	El usuario propietario del espacio de trabajo y con control total sobre su configuración	Sí
Compartido con	Miembros del proyecto que pueden acceder al espacio de trabajo junto con el propietario, para codificación y revisión entre pares. Los usuarios compartidos obtienen el mismo acceso que el propietario	Sí
Nombre del espacio de trabajo	Un nombre único para el espacio de trabajo	No
Imagen de contenedor	Una imagen preconfigurada que contiene las herramientas y dependencias que su proyecto necesita. El propietario o administrador de su proyecto mantiene la lista.	Sí, al reiniciar
Etiqueta	La versión de la imagen a utilizar	Sí, al reiniciar
Versión de VSCode	Qué versión del IDE se ejecuta en el espacio de trabajo. Consulte Versión de VSCode	Sí
Métodos de acceso	Qué métodos de conexión ofrece el espacio de trabajo: **VS Code** para el IDE del navegador,	Sí

CONFIGURACIÓN	QUÉ HACE	MODIFICABLE MÁS TARDE
	Terminal para el terminal del navegador y **SSH**. Cada uno se ejecuta como un servicio en el espacio de trabajo. Seleccione **Añadir** para definir un elemento de acceso personalizado	
Región del espacio de trabajo	Dónde se implementa el espacio de trabajo, lo que afecta a la latencia y la residencia de los datos. Elija una región cercana a sus repositorios y registros de paquetes; si usted y sus recursos difieren, priorice el que esté más cerca de usted.	No
Especificaciones del espacio de trabajo	La plantilla de recursos de cómputo. El rendimiento puede superar estos valores cuando la capacidad está disponible. Seleccione el icono de disco en la tarjeta de especificaciones para aumentar el almacenamiento.	Sí

Nota:

Las plantillas de especificaciones disponibles y sus valores dependen de cómo su administrador de plataforma haya configurado el entorno.

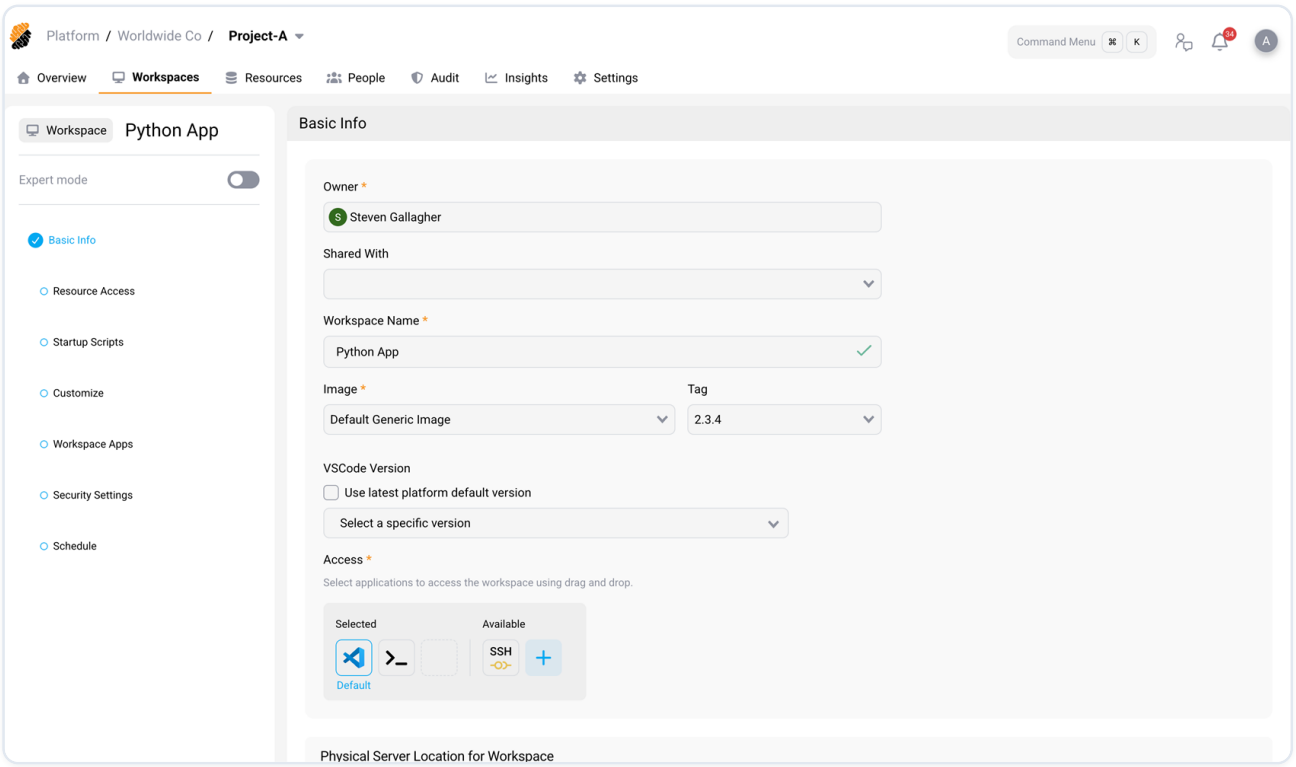
> Cambiar la imagen o la etiqueta en un espacio de trabajo en ejecución solo surte efecto después de que el espacio de trabajo se reinicia, porque el contenedor se recrea a partir de la nueva imagen. La consola le informa de esto y le pide que confirme antes de que reinicie el espacio de trabajo. Los archivos bajo `/home/developer` no se ven afectados. Consulte Qué persiste en un espacio de trabajo.

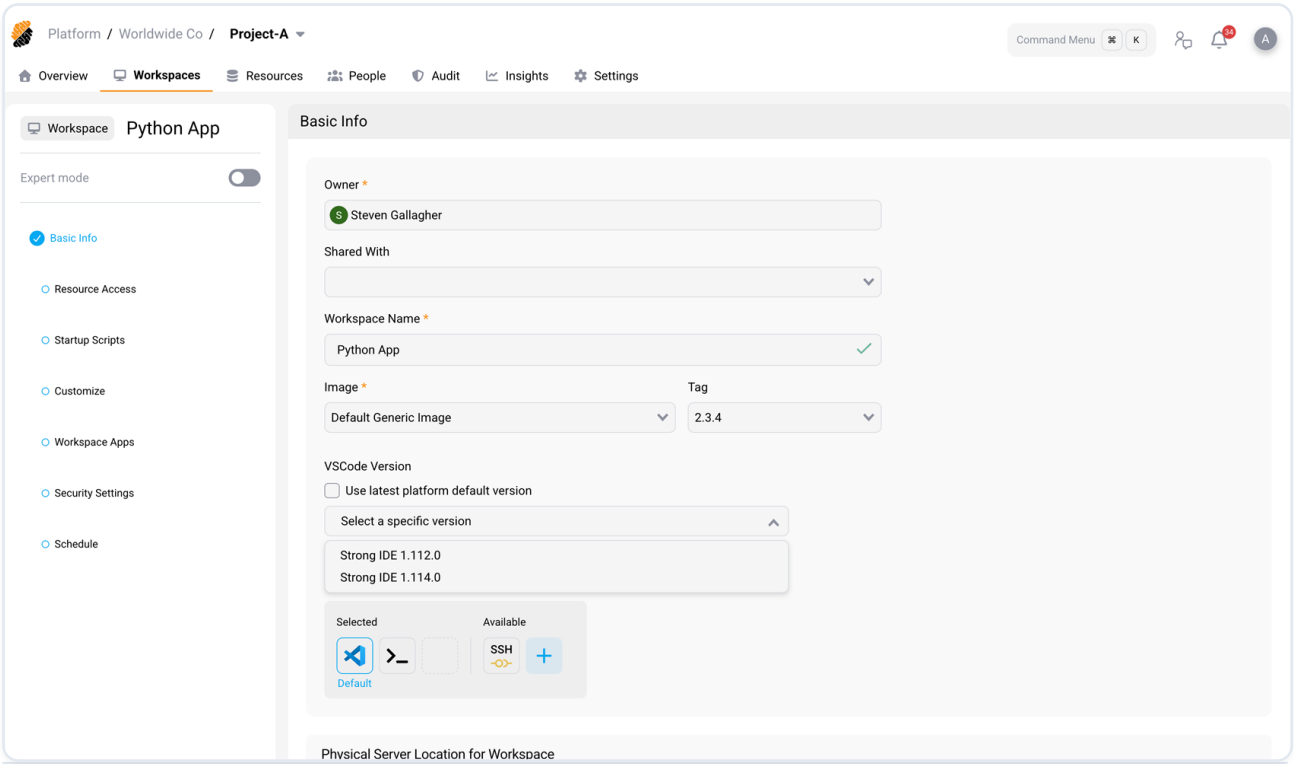
Cuando la configuración básica sea correcta, seleccione **Iniciar** para crear el espacio de trabajo inmediatamente, o **Siguiente** para continuar con los pasos restantes.

Versión de VSCode

Por defecto, seleccione **Usar la última versión predeterminada de la plataforma** y el espacio de trabajo seguirá la versión del IDE designada como predeterminada de la plataforma. Cuando ese valor predeterminado cambie, el espacio de trabajo adoptará el nuevo en su siguiente inicio.

Desactive la casilla para habilitar **Seleccionar una versión específica** y fijar el espacio de trabajo a una versión. La lista muestra las versiones del IDE importadas en su ámbito, las más recientes importadas primero. Un espacio de trabajo fijado no se actualiza cuando cambia el valor predeterminado de la plataforma.





SITUACIÓN	QUÉ SUCEDE
No se han importado versiones	La casilla de verificación y la lista no están disponibles, y el espacio de trabajo informa que no hay versiones de VSCode disponibles
Ninguna versión seleccionada, casilla de verificación desmarcada	El espacio de trabajo utiliza la imagen IDE integrada que se incluye con la versión de la plataforma instalada
Cambia la versión en un espacio de trabajo existente	El cambio surte efecto en el siguiente inicio. El directorio de inicio (`/home/developer`) no se ve afectado

Las versiones disponibles dependen de lo que se haya importado en el registro de la plataforma. Consulte Versiones de VSCode.

> **Nota:**

> Esta configuración también está disponible cuando edita un espacio de trabajo existente y cuando crea o edita una plantilla de espacio de trabajo. Una plantilla almacena la configuración, por lo que los espacios de trabajo creados a partir de ella heredan la versión fijada o el comportamiento de actualización automática.

Elementos de acceso personalizados

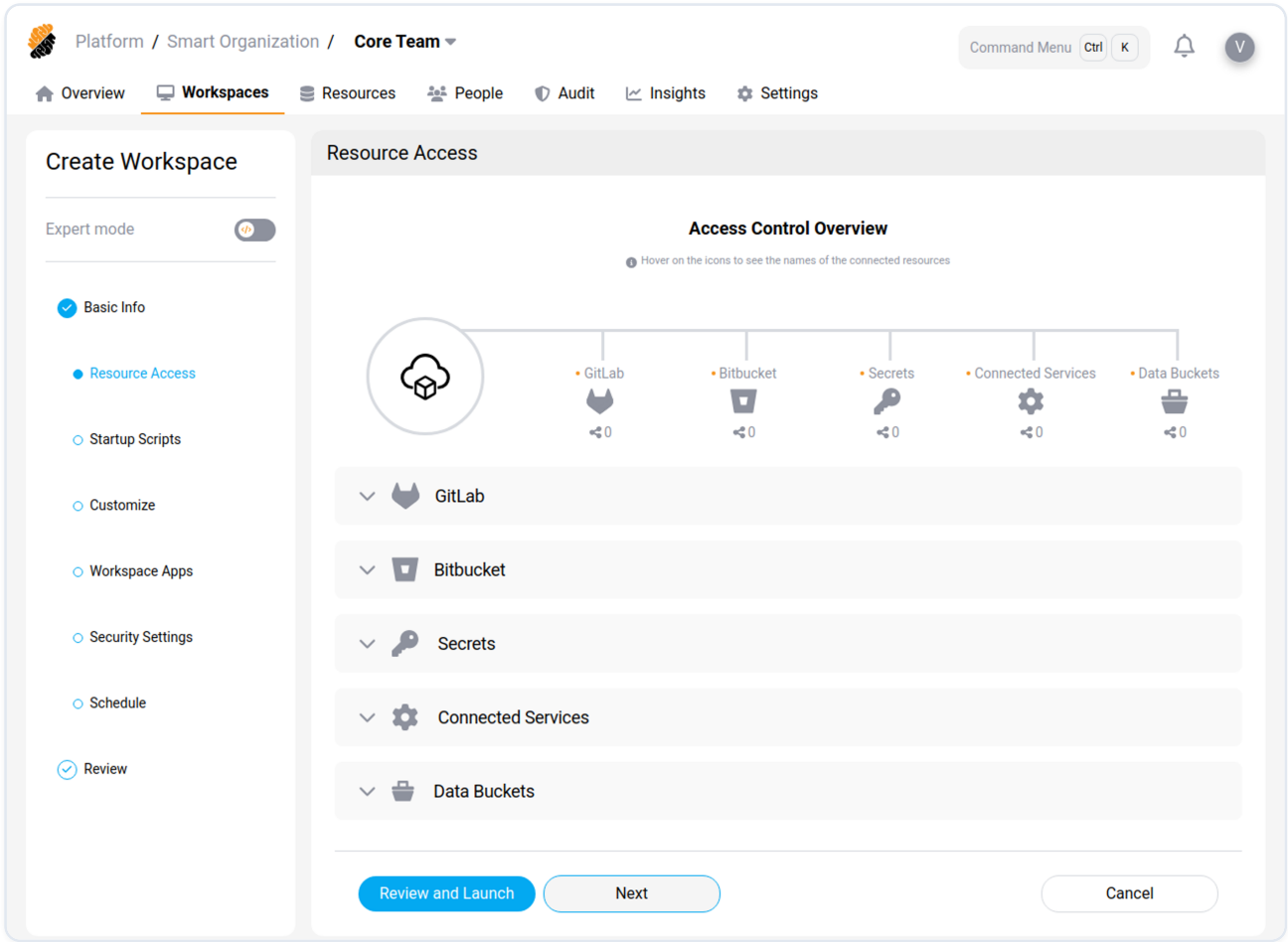
Un elemento de acceso personalizado proporciona acceso con un solo clic a un servicio o herramienta que se ejecuta dentro del espacio de trabajo. Utilícelo cuando los métodos de acceso integrados no cubran una herramienta de desarrollo, un servicio interno o un punto de entrada de aplicación.

CAMPO	QUÉ CONTIENE
Nombre	La etiqueta que se muestra a los usuarios del espacio de trabajo
Puerto	El puerto en el que el servicio escucha dentro del espacio de trabajo
Comando	El comando que inicia o se conecta al servicio
Icono	Una imagen opcional para el elemento de acceso
Sonda de estado	Un comando opcional que comprueba si el elemento está en línea

Los elementos de acceso personalizados también se pueden gestionar a través de la API REST, tanto para espacios de trabajo como para plantillas de espacios de trabajo. Consulte API REST.

Control de acceso a recursos

Adjunte recursos del proyecto al espacio de trabajo. Un recurso debe existir ya en el proyecto o la organización, y es posible que necesite derechos de acceso para usarlo.



RECURSO	QUÉ HACE AL ADJUNTARLO
Aplicaciones Git y repositorios	Conecta una aplicación Git completa o repositorios individuales ya importados en el proyecto u organización. Puede establecer la carpeta en el espacio de trabajo donde se clonarán los archivos.
Secretos	Hace que los secretos estén disponibles como archivos o variables de entorno. Elija un secreto existente o cree uno nuevo.
Servicios HTTP y SSH conectados	Hace que un servicio conectado esté disponible como variables de entorno. Los servicios disponibles dependen del proyecto, la organización y la configuración de la plataforma.

Si falta un repositorio

Los repositorios adjuntos aquí se clonan mientras se inicia el espacio de trabajo. Si falta un repositorio después de que el espacio de trabajo alcance el estado **Running**, realice estas comprobaciones en orden:

1. **Compruebe la configuración del espacio de trabajo.** Seleccione el espacio de trabajo y revise su configuración de Control de acceso a recursos. Confirme que el repositorio que espera aparece en la lista y anote la carpeta en la que se clona.
2. **Compruebe sus credenciales del proveedor de Git.** Confirme que se ha autenticado con el proveedor y la cuenta correctos en las integraciones de su perfil.
3. **Intente clonar manualmente** para averiguar cuál de los dos es el culpable:

   ```
   git clone <your-repository-url>
   ```

   Un error de permiso apunta a sus credenciales. Una clonación exitosa apunta a la configuración del espacio de trabajo — póngase en contacto con el propietario de su proyecto.

Scripts de inicio

La imagen del contenedor proporciona las herramientas fijas — lenguajes, compiladores, paquetes del sistema. Un script de inicio gestiona lo que cambia entre usuarios, ramas o ejecuciones, y no pertenecería a una imagen compartida.

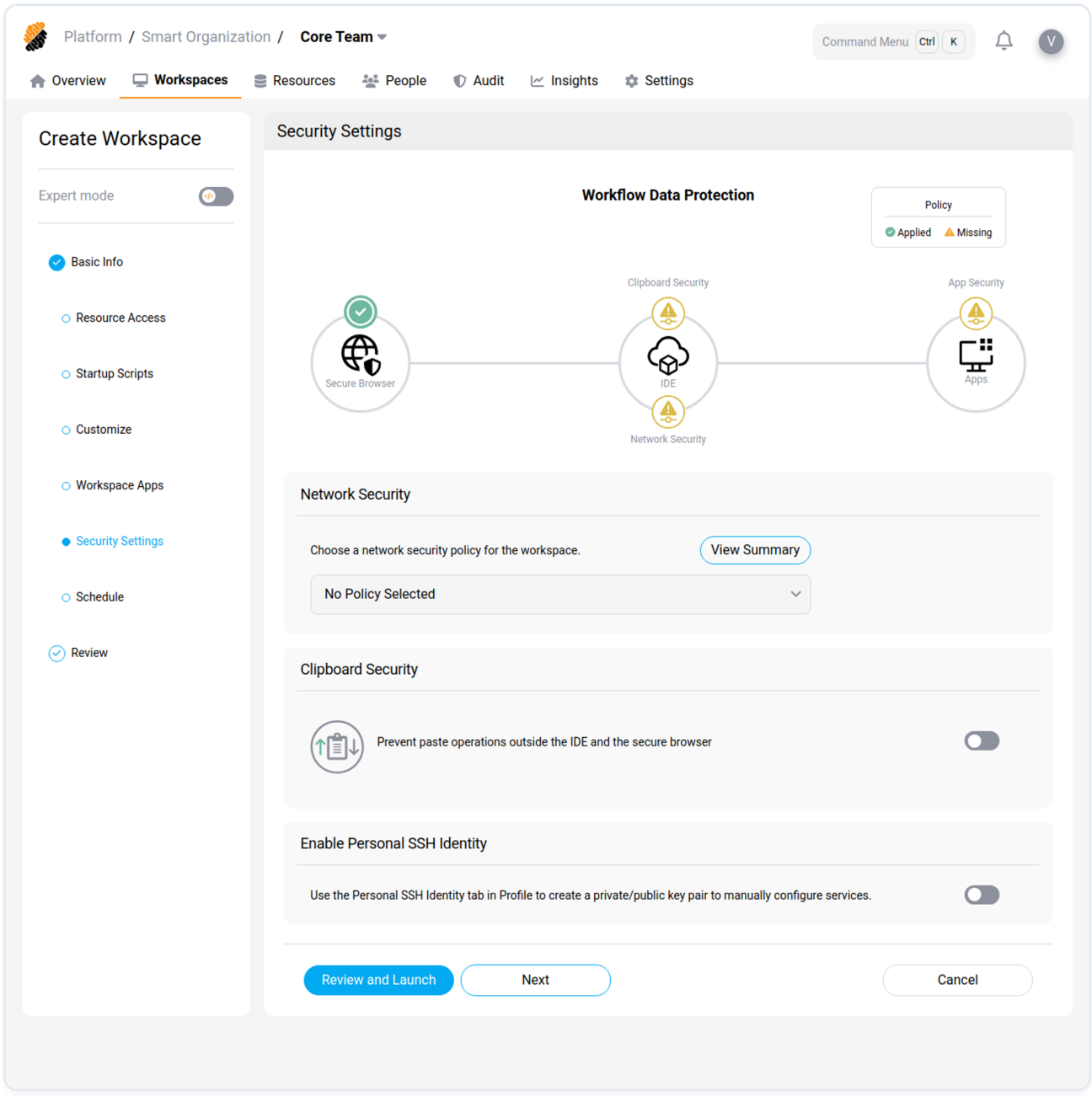
Un script de inicio se ejecuta cada vez que se inicia el espacio de trabajo, ya sea antes o después del inicio. Usos comunes:

USO	EJEMPLOS
Instalar dependencias que cambian a menudo	`npm install`, `apt update`, o compilar binarios para que coincidan con la rama actual
Iniciar servicios que el tiempo de ejecución no gestiona	Instancias locales de PostgreSQL, Redis o MongoDB, y procesos en segundo plano como observadores de archivos o ejecutores de pruebas
Informar de la disponibilidad	Comprobaciones de estado que confirman que los servicios están activos antes de entregar el terminal, o un mensaje que enumera los comandos disponibles

> **Nota:**
>
> Dado que el script se ejecuta en cada inicio, escríbalo de manera que ejecutarlo más de una vez sea seguro.

Prevención de pérdida de datos

Requiere que el permiso Security esté configurado en **Gestionar**.



La **Configuración de seguridad** controla lo que el espacio de trabajo puede alcanzar y lo que puede salir de él:

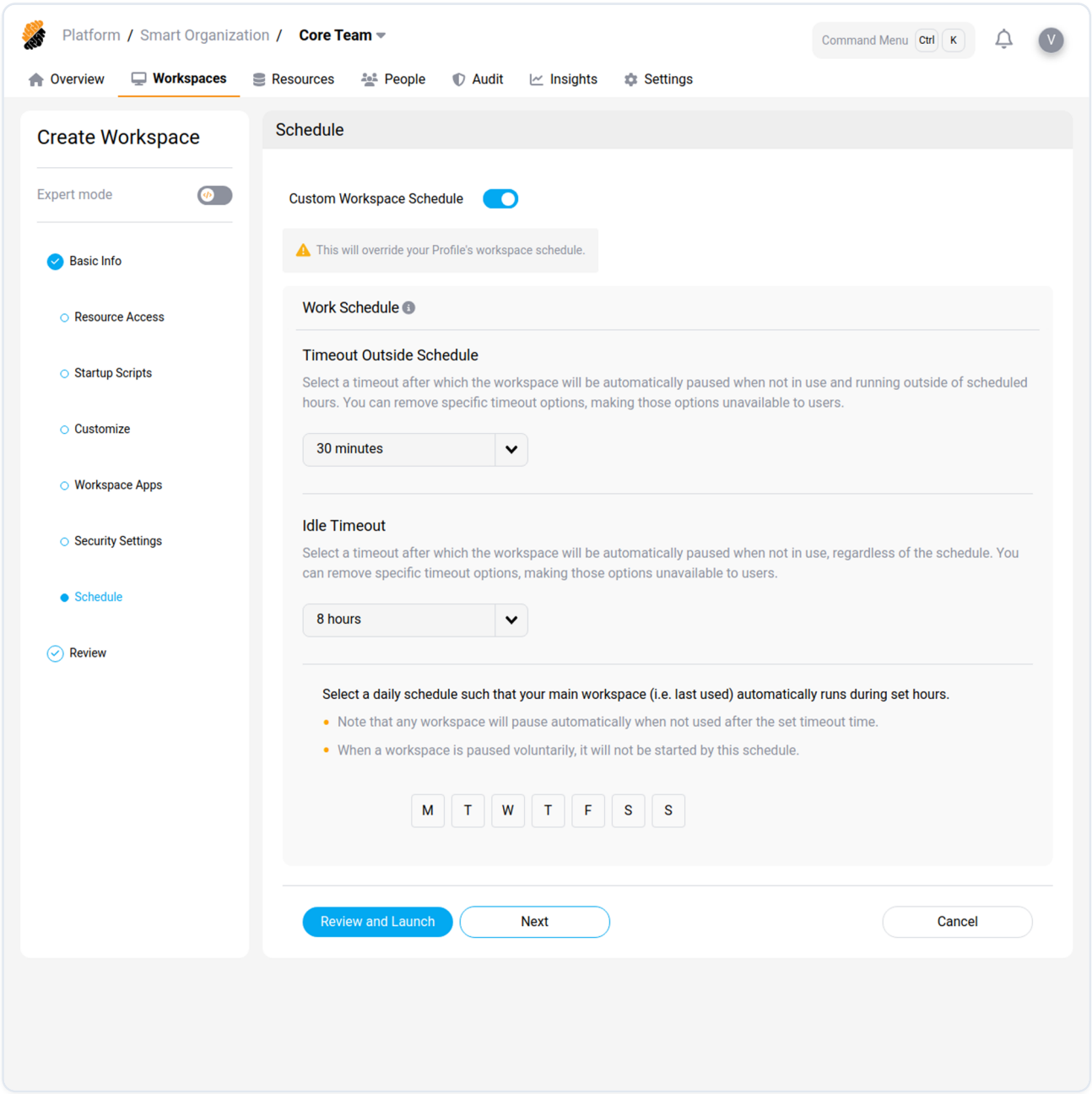
CONFIGURACIÓN	QUÉ HACE
Política de red	Aplica una política de red al espacio de trabajo, controlando el tráfico saliente. Las políticas son recursos de proyecto u organización, definidos por un usuario con **Seguridad** configurada en **Administrar**.
Seguridad del portapapeles	Impide pegar fuera del IDE y del navegador seguro.
Seguridad de las aplicaciones	Restringe las aplicaciones del espacio de trabajo al navegador seguro.

Gestión de acceso seguro controla cómo se conectan los desarrolladores:

CONFIGURACIÓN	QUÉ HACE
Desarrollo remoto a través de SSH	Permite conexiones SSH al espacio de trabajo.
Habilitar identidad SSH personal	Permite a los usuarios usar su identidad SSH personal desde dentro del espacio de trabajo.

Horario de trabajo personalizado

Define un horario de trabajo personalizado para el espacio de trabajo.



Iniciar

Revise la configuración e inicie. El espacio de trabajo se implementa automáticamente. Puede editar su configuración en cualquier momento desde las Visión general o Espacios de trabajo páginas.

Desde un espacio de trabajo existente

Seleccione **Crear espacio de trabajo** y, a continuación, **Copiar espacio de trabajo existente**. Proporcione el espacio de trabajo que desea copiar y el propietario del nuevo espacio de trabajo, y luego seleccione **Iniciar**.

> **Consejo:**

> Seleccione **Personalizar** para editar la copia como si la estuviera creando desde cero.

Desde una plantilla

Seleccione **Crear espacio de trabajo** y, a continuación, **Crear desde plantilla**. Esta es la ruta recomendada: una plantilla contiene la imagen, los recursos, las credenciales y la política acordados por su proyecto, de modo que el espacio de trabajo sea coherente con el de los demás.

Proporcione el nombre de la plantilla y el propietario del espacio de trabajo, y luego seleccione **Iniciar**.

> **Consejo:**
>
> Seleccione **Personalizar** para editar el espacio de trabajo como si lo estuviera creando desde cero.

Información relacionada

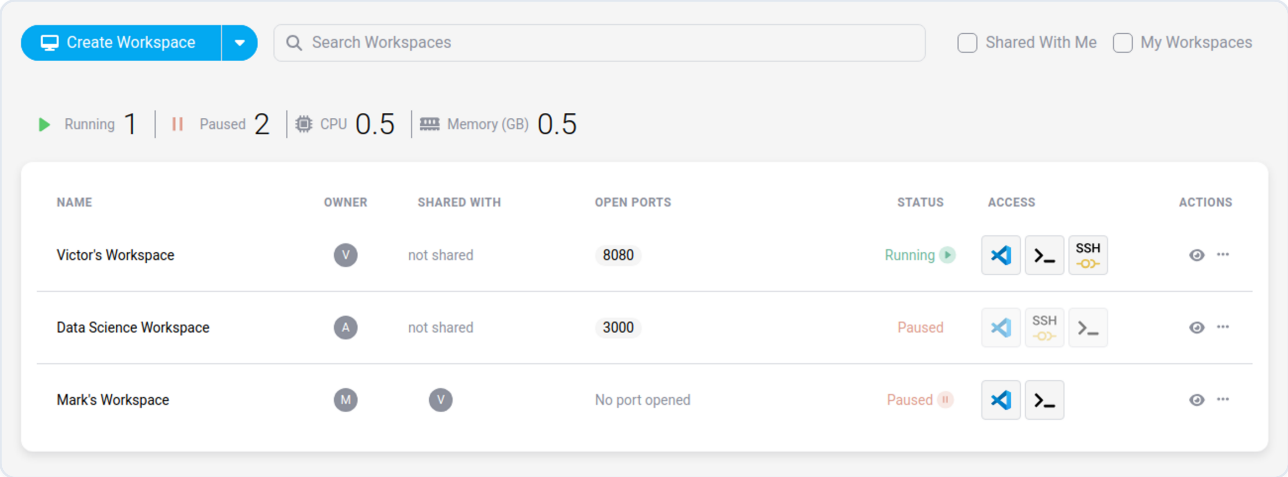
- Conectarse por SSH
- Administrar espacios de trabajo
- Página de Workspaces(/es-es/securspaces/develop/workspaces.html)
- Versiones de VSCode(/es-es/securspaces/administer/platform-resources/ide-versions.html)

Manage workspaces

Los espacios de trabajo se gestionan desde las páginas Visión general y Espacios de trabajo. Una vez que se le hayan asignado uno o más espacios de trabajo, aparecerán en ambas páginas mencionadas. El último espacio de trabajo utilizado se iniciará automáticamente según la programación de su perfil. Además, un espacio de trabajo podría pausarse automáticamente según la configuración de su plataforma después de un período de inactividad.

Ver espacios de trabajo

La lista de sus espacios de trabajo (de su propiedad o compartidos con usted) se muestra en las páginas Visión general y Espacios de trabajo. El estado del espacio de trabajo se muestra junto a su nombre.



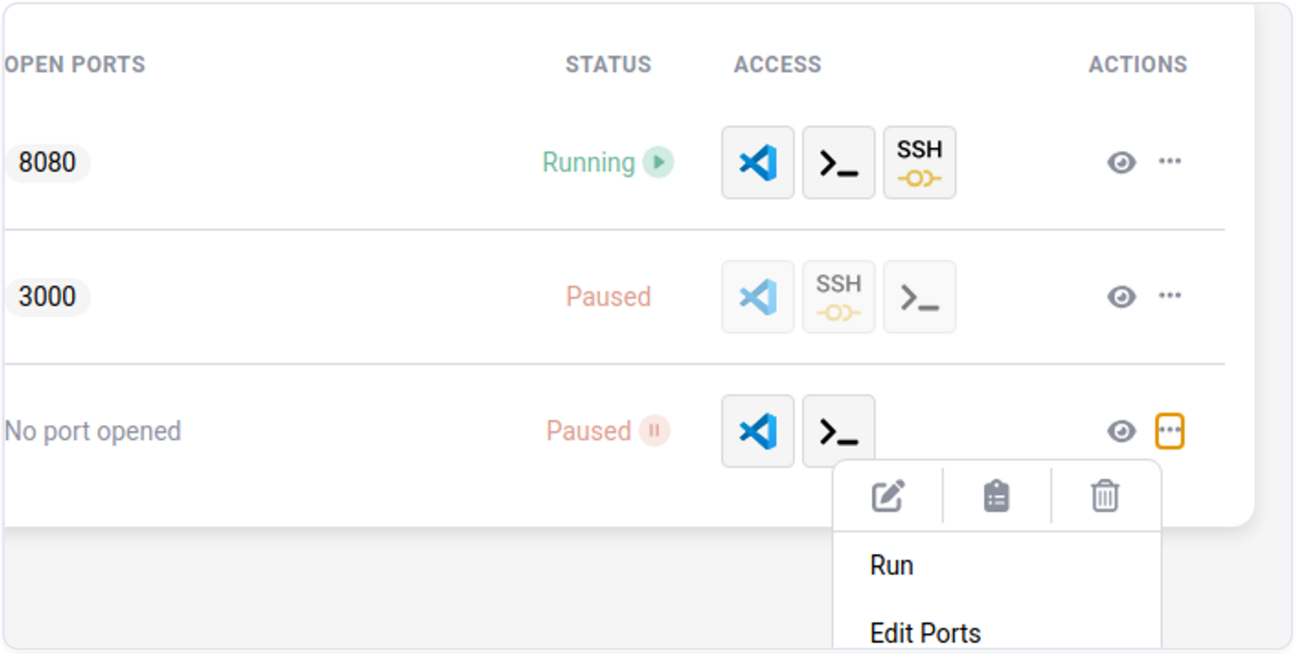
- Para **abrir un espacio de trabajo pausado**, haga clic en el botón "**start**". Esto abrirá el IDE en la nube del espacio de trabajo en su navegador.
- Para **abrir un espacio de trabajo en ejecución**, haga clic en el botón "**running**". Esto abrirá el IDE en la nube del espacio de trabajo en su navegador.
- Para **abrir su espacio de trabajo usando un terminal CLI**, haga clic en el menú desplegable junto a "**running text**" y luego en el botón "**Open Terminal**".

Acciones de los espacios de trabajo

Al hacer clic en el icono "**...**" de un espacio de trabajo, puede seleccionar acciones adicionales como se explica a continuación.

- **Ejecutar** o **Pausar** le permiten iniciar y pausar el espacio de trabajo, respectivamente.
- **Editar** le permite cambiar la configuración del espacio de trabajo tal como se seleccionó al crearlo.
- **Eliminar** borra su configuración y archivos locales. Deberá confirmar la acción insertando el nombre del espacio de trabajo.
- **Editar puertos** le permite gestionar las aplicaciones del espacio de trabajo que se ejecutan en los puertos de su espacio de trabajo.
- **Personalizar entorno** le permite actualizar el según la configuración de su perfil (*Solo si el espacio de trabajo es suyo*).
- **Actualizar** vuelve a desplegar el espacio de trabajo para sincronizarlo con su última configuración.
- **Compartir** le permite compartir el acceso al espacio de trabajo con el usuario de otro proyecto. Aprenda a trabajar con un espacio de trabajo compartido (*Solo si el espacio de trabajo es suyo*).

- **Guardar como plantilla** le permite guardar la configuración del espacio de trabajo como una plantilla para su posterior reutilización (requiere que el permiso Espacios de trabajo esté configurado en **Administrar proyecto**).



Recuperar un espacio de trabajo eliminado

Un espacio de trabajo eliminado se mueve a una papelera de reciclaje y se puede restaurar desde Configuración general del proyecto hasta que caduque. El período de retención es de **7 días por defecto**, pero el administrador de su plataforma puede configurarlo entre 1 y 99 días, así que consúlteles si no está seguro de cuánto tiempo dispone. Consulte Espacios de trabajo pendientes de eliminación.

> **Nota:**
>
> Solo el propietario de un proyecto puede recuperar un espacio de trabajo. Si no tiene los privilegios necesarios, póngase en contacto con el propietario de su proyecto.

Información relacionada

- Conectarse a través de SSH
- Crear un espacio de trabajo
- Página de espacios de trabajo

Connect over SSH

Una conexión basada en SSH le permite trabajar en un espacio de trabajo de Citrix SecurSpaces™ desde un IDE instalado localmente como VS Code, Cursor, Windsurf, Kiro o JetBrains. Su IDE se ejecuta en su máquina mientras el código, las herramientas y la computación permanecen en el espacio de trabajo en la nube.

SecurSpaces proporciona extensiones dedicadas para estos IDE que simplifican la gestión de energía del espacio de trabajo y las conexiones SSH con un solo clic. Para los IDE sin una extensión de SecurSpaces, puede conectarse manualmente utilizando un par de claves SSH estándar.

IDE compatibles

VS Code Desktop, Cursor, Windsurf y Kiro se conectan con un solo clic utilizando la extensión de SecurSpaces. JetBrains Gateway se conecta a través de su propia configuración SSH, y cualquier otro editor compatible con SSH se conecta con un par de claves manual. Para ver la lista completa y el método de conexión para cada uno, consulte IDE compatibles.

Requisitos previos

Antes de poder conectarse a un espacio de trabajo a través de SSH, verificar lo siguiente:

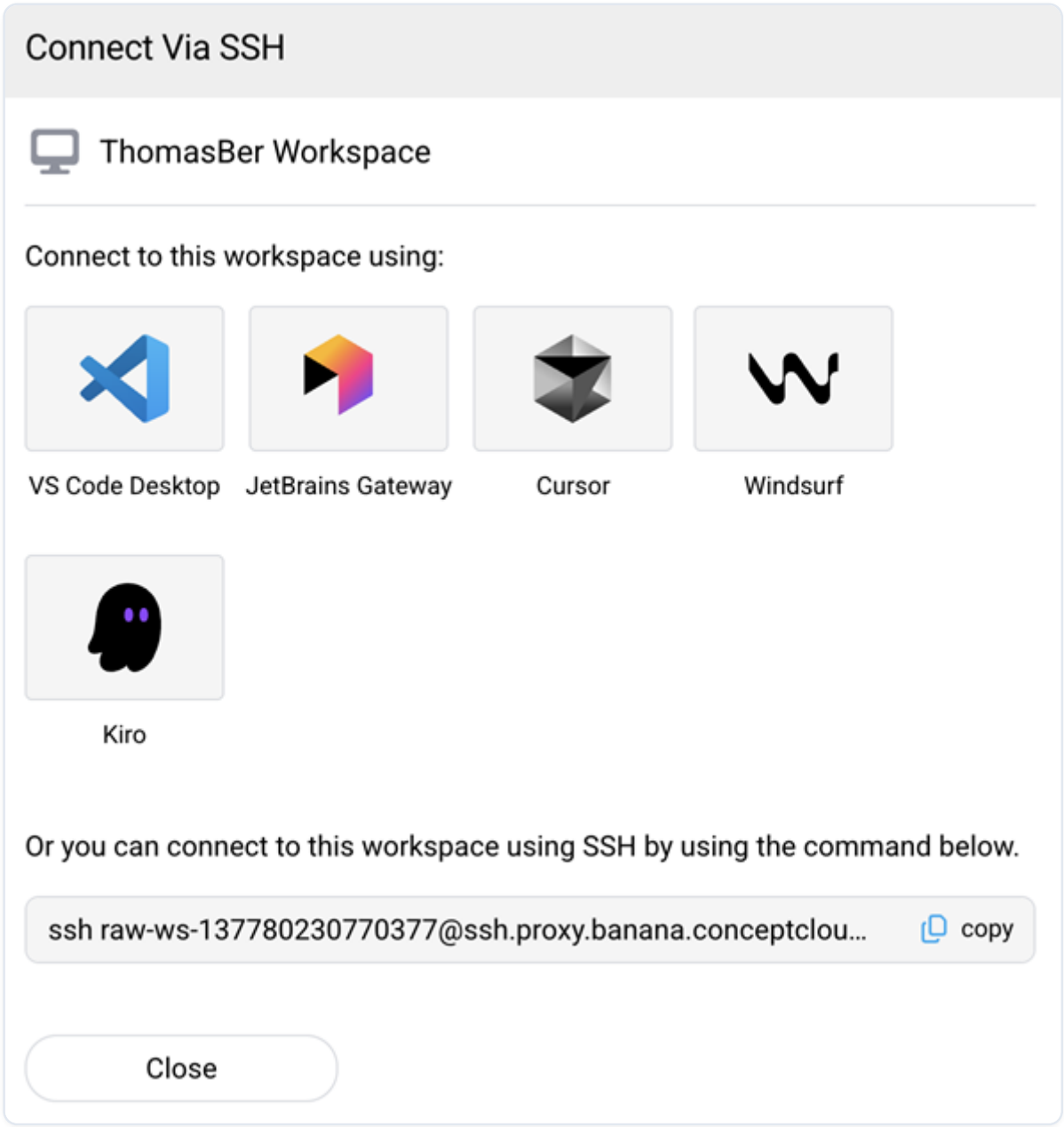
- **El desarrollo remoto a través de SSH está habilitado.** Un administrador de plataforma, propietario de organización o propietario de proyecto debe habilitar esta configuración en **Configuración del espacio de trabajo > Configuración de seguridad > Desarrollo remoto a través de SSH**. Esta configuración está disponible a nivel de plataforma, organización y proyecto.
- **SSH está habilitado en el espacio de trabajo.** Al crear o editar un espacio de trabajo, vaya a **Información básica > Acceso** y arrastre el icono de **SSH** a **Seleccionado**. Los espacios de trabajo sin SSH habilitado muestran una etiqueta de "Sin acceso SSH" y no pueden aceptar conexiones SSH.

Conectarse usando VS Code, Cursor, Windsurf o Kiro

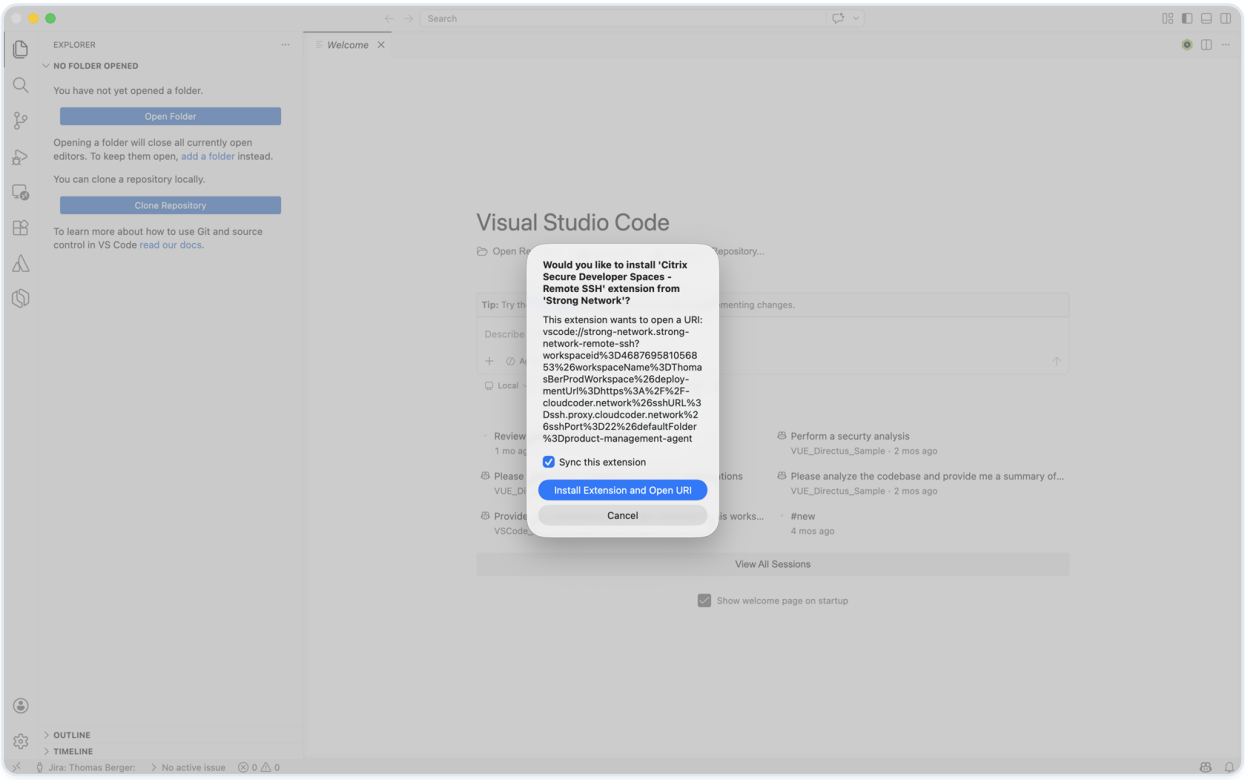
SecurSpaces proporciona la extensión **Citrix Secure Developer Spaces - Remote SSH** para IDE basados en VS Code (VS Code, Cursor, Windsurf y Kiro). Al seleccionar cualquiera de estos IDE en el cuadro de diálogo **Conectar a través de SSH**, se utiliza el esquema URI personalizado del IDE para iniciar la aplicación, instalar la extensión de SecurSpaces si es necesario y establecer automáticamente la conexión SSH.

La forma más rápida de empezar es iniciar la conexión desde la consola de SecurSpaces:

1. En la consola de SecurSpaces, navegue a la página **Espacios de trabajo** o **Resumen** del proyecto.
2. Localice un espacio de trabajo con el icono de **SSH** visible en la columna **Acceso** y selecciónelo.
3. En el cuadro de diálogo **Conectar a través de SSH**, seleccione su IDE (por ejemplo, **VS Code Desktop**).



4. Su IDE local se abre. Si es su primera conexión, se le pedirá que instale la extensión **Citrix Secure Developer Spaces - Remote SSH**. Seleccione **Instalar extensión y abrir URI**.



5. La extensión se conecta al espacio de trabajo automáticamente.

Instalar la extensión manualmente

Si prefiere configurar la extensión antes de iniciar una conexión desde la consola:

1. Instale la extensión Citrix Secure Developer Spaces - Remote SSH desde VS Code Marketplace.
2. Abra la barra lateral de la extensión. Antes de iniciar sesión, muestra un campo de **URL del entorno**.
3. Introduzca la URL de su entorno de SecurSpaces y seleccione **Conectar**. Se le redirigirá a su navegador para iniciar sesión.
4. Después de iniciar sesión, la barra lateral muestra los espacios de trabajo disponibles para usted, agrupados por proyecto.

Qué instala la extensión

Usted instala una extensión, **Citrix Secure Developer Spaces - Remote SSH**. Tiene dos partes:

- La parte que se ejecuta en su máquina local proporciona la barra lateral, el inicio de sesión, la lista de espacios de trabajo, las conexiones SSH y la barra de estado. Su token de acceso permanece en su máquina y nunca se coloca en el espacio de trabajo.
- Un componente complementario empaquetado en su interior se ejecuta en el espacio de trabajo. Informa de la actividad para que un espacio de trabajo que esté utilizando activamente

no se pause por detección de inactividad, y responde a las mediciones de red descritas en Supervisar la calidad de la conexión.

El componente complementario se instala en el espacio de trabajo automáticamente cuando se conecta. No hay nada que configurar. Si utilizó una versión anterior de la extensión SecurSpaces, es posible que se le pida que elimine la extensión remota anterior y reinicie su IDE.

Administrar espacios de trabajo desde la extensión

La barra lateral de la extensión es el punto de entrada de SecurSpaces dentro de su IDE. Seleccione el icono de SecurSpaces en la barra de actividad para abrirla. Los espacios de trabajo se agrupan por proyecto, y el espacio de trabajo al que está conectado se resalta y se ordena en la parte superior.

Each workspace row shows its current state, and workspaces without SSH enabled are labeled. You can act on a workspace from its row controls or by right-clicking the row. Right-clicking a running workspace offers **Connect in current window**, **Connect in new window**, **Edit workspace**, and **Delete workspace**. A paused workspace offers **Edit workspace** and **Delete workspace**.

Para ver la lista completa de estados, controles de fila y acciones del menú contextual, consulte Barra lateral de la extensión.

Iniciar o pausar un espacio de trabajo muestra el progreso hasta que el nuevo estado se estabiliza.

Pausar el espacio de trabajo al que está conectado actualmente cierra la conexión remota y le devuelve a una ventana local.

> **Advertencia**

> Eliminar un espacio de trabajo lo elimina permanentemente junto con todos sus datos, y no se puede deshacer. Pause un espacio de trabajo en ejecución antes de eliminarlo.

Abrir repositorios, puntos de montaje y aplicaciones

Expanda un espacio de trabajo para ver lo que contiene. El espacio de trabajo conectado se expande automáticamente la primera vez que se conecta a él.

- **Repositorios** — los repositorios de código clonados en el espacio de trabajo. Seleccione uno para abrir esa carpeta en su IDE, o haga clic derecho y seleccione **Abrir en terminal** para abrir una terminal en esa ubicación.
- **Puntos de montaje** — el almacenamiento compartido adjunto al espacio de trabajo. Los puntos de montaje de solo lectura están etiquetados. Seleccione uno para abrir la carpeta, o haga clic derecho y seleccione **Abrir en terminal**.
- **Aplicaciones** — las aplicaciones del espacio de trabajo que se están ejecutando, como Jupyter Lab o una aplicación de vista previa. Seleccione una aplicación para abrirla en su navegador predeterminado, o haga clic derecho y seleccione **Copiar URL**.

Las aplicaciones solo se pueden abrir mientras el espacio de trabajo está en ejecución.

Abrir la consola de SecurSpaces desde su IDE

Algunas acciones abren la consola de SecurSpaces en su navegador en lugar de realizarse en el IDE. La consola aplica sus permisos a estas acciones.

- **Abrir consola SDS** — abre su entorno SecurSpaces.
- **Añadir espacio de trabajo** — el botón **+** en el encabezado de un proyecto inicia el flujo de creación de espacio de trabajo.
- **Editar configuración del perfil** — abre su perfil.
- **Solucionar problemas de conexión** — abre la página de perfil utilizada para diagnosticar problemas de conexión.

Estos comandos también están disponibles en la Paleta de comandos en **Citrix SDS**.

Supervisar la calidad de la conexión

Mientras está conectado a un espacio de trabajo, la barra de estado muestra el estado de la conexión, el nombre del espacio de trabajo y el tiempo de ida y vuelta de la conexión. El color cambia a medida que aumenta la latencia, por lo que una conexión lenta es visible sin necesidad de abrir nada.

Pase el ratón por encima de la barra de estado para obtener más detalles, incluido un ancho de banda estimado. Selecciónela para **Volver a medir la red ahora** o para **Desactivar el monitor de red**. Ambas acciones también están disponibles en la Paleta de comandos, junto con **Activar el monitor de red** para volver a activar la supervisión.

Desactivar el monitor detiene las mediciones y oculta la barra de estado. La elección persiste a través de los reinicios.

Cada ventana del IDE ejecuta su propio monitor para el espacio de trabajo al que está conectada esa ventana.

> **Nota**
>
> Estas mediciones describen la capacidad de respuesta de la conexión que utiliza su IDE, lo que incluye SSH y la sobrecarga del protocolo. Son una guía de cómo se siente la conexión, más que una referencia de red pura.

Si faltan algunas acciones

La extensión se actualiza con más frecuencia que la plataforma a la que se conecta. Cuando su plataforma SecurSpaces es más antigua que la extensión, las acciones que dependen de características más nuevas de la plataforma se ocultan en lugar de mostrarse y fallar.

Si la extensión oculta algo, la parte inferior de la barra lateral indica *Aquí aparecerán más acciones después de que su administrador de SDS actualice la plataforma*. Los repositorios, los puntos de montaje y las aplicaciones, junto con las acciones de la consola mencionadas anteriormente, son las características afectadas. Pida a su administrador de plataforma que actualice SecurSpaces.

Conectarse usando JetBrains Gateway

JetBrains Gateway permite conexiones SSH desde los IDE de JetBrains (IntelliJ IDEA, PyCharm, GoLand y otros).

Instalar JetBrains Gateway

Descargue e instale JetBrains Gateway.

Crear una conexión SSH

1. En JetBrains Gateway, seleccione **Nueva conexión** en **Conexión SSH**.

2. Haga clic en el icono de configuración junto a **Conexión**, luego haga clic en **+** para añadir una nueva configuración SSH.
3. En la consola de SecurSpaces, seleccione el icono **SSH** en su espacio de trabajo, luego seleccione **JetBrains Gateway** en el diálogo. El comando SSH se muestra en la parte inferior del diálogo.
4. Introduzca los detalles de conexión del comando SSH:

- **Host** — La parte después de `@` (por ejemplo, `ssh.proxy.cloudcoder.network`).
- **Nombre de usuario** — La parte antes de `@` (por ejemplo, `raw-ws-468769581056853`).
- **Tipo de autenticación** — Seleccione **Par de claves** y proporcione la ruta a su clave privada.

> **Consejo:**
>
> Ignore el prefijo `ssh` y el carácter `@` al dividir el comando en Host y Nombre de usuario.

5. Haga clic en **Probar conexión** para verificar la configuración, luego haga clic en **Aceptar**.

6. Seleccione su nueva configuración como la **Conexión** y haga clic en **Comprobar conexión y continuar**.
7. Elija el IDE de JetBrains que desea usar y la carpeta del proyecto a abrir, luego haga clic en **Descargar IDE y conectar**.

> **Consejo:**
>
> El IDE se descarga en su espacio de trabajo, no en su máquina local.

8. Una vez completada la instalación del IDE, estará conectado a su espacio de trabajo.

Conexión SSH manual

Si su IDE carece de una extensión dedicada de SecurSpaces o de una integración con JetBrains Gateway, puede conectarse utilizando un par de claves SSH estándar. Este enfoque funciona con cualquier terminal o editor compatible con SSH.

Generar un par de claves SSH

En sistemas UNIX y similares a UNIX, ejecute `ssh-keygen` en su terminal:

```
ssh-keygen
```

- Pulse **Intro** para aceptar la ruta y el nombre de archivo predeterminados, o especifique una ubicación personalizada.
- Introduzca una frase de contraseña cuando se le solicite (recomendado para mayor seguridad), o pulse **Intro** para omitir.
- El comando genera un par de claves: una clave privada (por ejemplo, `id_rsa`) y una clave pública (por ejemplo, `id_rsa.pub`).

Subir su clave pública

Sube la clave pública a la sección **Claves SSH** en tu página Perfil > Seguridad.

Tipos de clave compatibles: `ssh-rsa`, `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, `ecdsa-sha2-nistp521`, `ssh-ed25519`, `sk-ecdsa-sha2-nistp256@openssh.com`, `sk-ssh-ed25519@openssh.com`.

Autoriza tu espacio de trabajo

Después de subir tu clave, autoriza el/los espacio(s) de trabajo que deben aceptar conexiones usando esta clave.

Conectar desde un terminal

1. En la consola de SecurSpaces, selecciona el icono **SSH** en tu espacio de trabajo para abrir el diálogo **Conectar vía SSH**.
2. Copia el comando SSH que se muestra en la parte inferior del diálogo.
3. Ejecuta el comando en tu terminal:

```
ssh raw-ws-468769581056853@ssh.proxy.cloudcoder.network
```

Ahora estás conectado a tu espacio de trabajo vía SSH.

Caducidad y renovación de la clave

Una clave pública que registras para el acceso SSH no dura indefinidamente. Es válida por un período fijo — **7 días por defecto** — después del cual la plataforma deja de aceptarla. Un administrador de la plataforma establece el período, por lo que tu implementación podría usar uno diferente.

Lo que tienes que hacer al respecto depende completamente de cómo te conectes:

CÓMO TE CONECTAS	QUÉ SUCEDE CUANDO LA CLAVE CADUCA
La extensión de SecurSpaces para VS Code, Cursor, Windsurf o Kiro	Nada. La extensión renueva la clave por ti.
JetBrains Gateway con el plugin de SecurSpaces	Nada. El plugin renueva la clave por ti.
Cualquier otro cliente SSH — `ssh` simple, un emulador de terminal o el soporte genérico de SSH remoto propio de un IDE	**Lo renuevas tú mismo.** La conexión deja de funcionar hasta que lo hagas.

Por eso, una configuración que funcionó la semana pasada puede empezar a rechazar conexiones sin que nada haya cambiado. La clave caducó y nada la renovó, porque el cliente que utilizas no tiene forma de hacerlo.

Renovar una clave manualmente

1. Ve a **Perfil > Seguridad > Acceso remoto por SSH**.
2. Vuelve a subir tu clave pública y autoriza los espacios de trabajo que deberían aceptarla.

Puedes seguir usando el mismo par de claves; lo que caduca es el registro, no la clave en sí. Consulta Seguridad.

> **Nota:**
>
> Si te conectas desde un script, un trabajo programado o cualquier otra cosa desatendida, planifica esto. No hay renovación automática fuera de las integraciones IDE de SecurSpaces, por lo que una conexión desatendida fallará cada vez que la clave caduque hasta que alguien la vuelva a registrar.

Mantener una sesión activa

Una sesión SSH que se conecta normalmente y luego se interrumpe después de un período de inactividad suele haber sido cerrada por algo entre tú y el espacio de trabajo, no por el propio espacio de trabajo. Las conexiones TCP inactivas suelen ser terminadas por proxies corporativos, VPN, balanceadores de carga y pasarelas NAT.

Enviar tráfico periódicamente evita que la conexión parezca inactiva. En `~/.ssh/config` en tu máquina local:

```
Host *

    ServerAliveInterval 60

    ServerAliveCountMax 3
```

Eso solicita un keepalive cada 60 segundos y se rinde después de tres sin respuesta. VS Code Remote-SSH, JetBrains Gateway y `ssh` leen este archivo, por lo que se aplica a todos los clientes a la vez.

Para el trabajo que debe sobrevivir completamente a la conexión, ejecútelo bajo un multiplexor de terminal como `tmux` o `screen`, o con `nohup`. El proceso sobrevive entonces a la desconexión y usted se vuelve a conectar a él después.

> **Nota:**

> Una sesión que termina mientras usted está ausente también podría ser que el espacio de trabajo se pausó en lugar de que la conexión se cayera. La detección de inactividad detiene los espacios de trabajo según un horario. Consulte Ciclo de vida del espacio de trabajo.

Recuperar un terminal corrupto

Después de una sesión interrumpida, el terminal puede mostrar caracteres extraños, secuencias como `\^[[<35;80;24M`, un prompt faltante o duplicado, o ninguna respuesta al escribir.

Esto ocurre cuando un programa a pantalla completa estaba ejecutándose en el momento en que se perdió la conexión. Programas como `tmux`, `vim`, `less`, `top` y las herramientas CLI interactivas ponen el terminal en un modo especial —a menudo habilitando el informe del ratón— y lo restauran cuando salen limpiamente. Una conexión perdida no les da la oportunidad de hacerlo, por lo que el terminal se queda en ese modo y el movimiento del ratón o el desplazamiento llegan como texto.

Para restaurarlo:

```
reset
```

Si `reset` no está disponible o el terminal no responde, `stty sane` seguido de **Ctrl+L** suele funcionar.

Para reducir la frecuencia con la que esto ocurre:

- Añada el keepalive anterior, para que las sesiones se caigan con menos frecuencia en primer lugar.
- Desactive el informe del ratón en las herramientas que lo habilitan. En `tmux`, elimine o comente `set -g mouse on` en `~/.tmux.conf`.
- Desvincúlese de una sesión de multiplexor con su propia combinación de teclas en lugar de cerrar la ventana del terminal.

Información relacionada

- Solución de problemas
- Crear un espacio de trabajo
- Administrar espacios de trabajo
- Página de espacios de trabajo

What persists in a SecurSpaces workspace

Información general

Los espacios de trabajo de Citrix SecurSpaces™ están en contenedores y son efímeros. Cada vez que se inicia un espacio de trabajo, el contenedor se recrea a partir de su imagen base, por lo que cualquier cosa que instale o cambie fuera del volumen persistente no persiste entre reinicios.

Hay exactamente una ubicación cuyo contenido sobrevive a los reinicios del espacio de trabajo, las actualizaciones de imagen y los cambios de infraestructura:

```
/home/developer/
```

Todo lo demás —paquetes del sistema instalados con `apt`, archivos en `/etc`, `/usr`, `/opt`, `/var` y el resto del sistema de archivos raíz— reside en un sistema de archivos temporal y se descarta cuando se recrea el contenedor del espacio de trabajo.

Esta página describe las tres formas de hacer que los cambios persistan entre reinicios, cuándo usar cada una y las ventajas y desventajas.

1. Guardar archivos en `/home/developer`

El caso más simple y común. Cualquier cosa que escriba en `/home/developer/` está en un volumen persistente y estará allí la próxima vez que abra el espacio de trabajo.

Esto incluye:

- Código fuente, incluidos los repositorios Git clonados
- Configuración del shell: `~/.bashrc`, `~/.profile`, `~/.zshrc`, `~/.inputrc`
- Configuración del editor y del IDE: `~/.config/`, `~/.vscode/`, `~/.config/JetBrains/`
- Datos de usuario específicos de la herramienta: `~/.aws/`, `~/.kube/`, `~/.docker/`, `~/.npm/`, `~/.cargo/`

Las instalaciones de herramientas con ámbito de usuario también funcionan aquí, porque se instalan en su directorio de inicio por defecto: `nvm`, `pyenv`, `rustup`, `uv`, `pipx`, `cargo install`, `npm install -g` (con un prefijo en `~/`), módulos Go en `~/go` y otros.

```
# Example: Install Node.js global tools into ~/.local (persists across
restarts)

mkdir -p ~/.local

npm config set prefix ~/.local

echo 'export PATH="$HOME/.local/bin:$PATH"' >> ~/.bashrc

npm i -g yarn pnpm typescript
```

```
# Example: Install Python CLI tools with pipx (installs into ~/.local by
default)

pipx install ruff

pipx install pre-commit
```

Después de la configuración inicial, estas herramientas permanecen disponibles entre reinicios sin ningún script de inicio.

Si una herramienta solo ofrece un instalador a nivel de sistema (normalmente `apt install` o cualquier cosa que escriba en `/usr/local/`), la instalación se restablece en el siguiente reinicio. Utilice una de las dos opciones siguientes en su lugar.

2. Scripts de inicio

Cada espacio de trabajo puede ejecutar un **Script de preinicio** (antes de que se inicie el IDE) y un **Script de postinicio** (después de que el espacio de trabajo esté listo). Ambos se ejecutan en cada inicio del espacio de trabajo.

Esta es la herramienta adecuada para:

- Instalar paquetes del sistema que deben estar presentes antes de empezar a trabajar — `sudo apt-get update && sudo apt-get install -y <packages>`
- Iniciar servicios en segundo plano que tu proyecto necesita — una base de datos local, un intermediario de mensajes, un demonio de compilación
- Establecer variables de entorno o escribir archivos de configuración en ubicaciones fuera de `/home/developer/` que tus herramientas esperan
- Ejecutar la configuración de inicio de sesión que depende de secretos o valores en tiempo de ejecución

Dónde configurar los scripts de inicio

Los scripts de inicio se pueden definir en tres niveles:

1. **Nivel de espacio de trabajo** — Se establece durante la creación del espacio de trabajo o en la configuración del espacio de trabajo. Se aplica solo a ese espacio de trabajo.
2. **Nivel de plantilla** — Definido en una plantilla de espacio de trabajo. Se aplica a todos los espacios de trabajo creados a partir de la plantilla.
3. **Nivel de perfil** — Se establece en Perfil → Configuración. Se aplica a todos los espacios de trabajo de tu propiedad, a menos que un script a nivel de espacio de trabajo lo anule.

> **Nota:**
>
> Un script de inicio a nivel de espacio de trabajo anula el script a nivel de perfil.

Ejemplo: Instalar paquetes del sistema (preinicio)

```
#!/bin/bash

sudo apt-get update -qq && sudo apt-get install -y -qq gh
```

Ejemplo: Iniciar un servicio en segundo plano (después del inicio)

```
#!/bin/bash

sudo service postgresql start
```

Consideraciones importantes

- Los scripts se ejecutan en **cada** inicio. Manténgalos idempotentes y lo más rápidos posible, ya que añaden tiempo directamente al inicio de su espacio de trabajo.
- Si reinstala los mismos paquetes `apt` en cada lanzamiento, esto añade tiempo de inicio innecesario. Mueva esas instalaciones a una imagen personalizada (siguiente sección) y conserve el script para las tareas que realmente necesiten ejecutarse al inicio.
- Los errores en un script de preinicio pueden impedir que el espacio de trabajo se inicie. Pruebe los cambios con cuidado.
- No almacene secretos en scripts. En su lugar, utilice los secretos gestionados por la plataforma de SecurSpaces.

3. Imágenes de contenedor personalizadas

Para cualquier cosa persistente entre sesiones —paquetes del sistema, tiempos de ejecución de lenguajes, herramientas de línea de comandos, configuración base— el enfoque recomendado es incluirlo en una imagen de contenedor.

Por qué esto es preferible para una configuración compartida y persistente

- **Construir una vez, reutilizar en todas partes.** Cada espacio de trabajo lanzado desde la plantilla se inicia en segundos con todo ya instalado.
- **Reproducible.** La imagen es un artefacto fijado y versionado. Cada desarrollador obtiene el mismo entorno, lo que elimina la desviación de la configuración.
- **Compartible.** Un equipo o toda una organización puede estandarizar una única imagen en lugar de que cada desarrollador mantenga su propio script de inicio.

- **Sin penalización en el tiempo de inicio.** Las capas se extraen y se almacenan en caché en los nodos del clúster, no se reinstalan por cada espacio de trabajo.

El flujo de trabajo

1. Escriba un `Dockerfile` que parta de `FROM` la imagen base de SecurSpaces de su elección.
2. Añada su `RUN apt-get install …`, cadenas de herramientas de lenguaje, herramientas de línea de comandos globales, configuración base de `/etc`, y cualquier configuración que deba ser la misma para todos los que usen esta plantilla.
3. Cree y envíe la imagen a su registro de contenedores (Docker Hub, GHCR, ECR, ACR, GAR, JFrog, Harbor — cualquier cosa accesible desde el clúster de SecurSpaces).
4. Haga referencia a la imagen en su plantilla de espacio de trabajo o en la configuración individual del espacio de trabajo.

Dockerfile de ejemplo

```
FROM your-base-image:latest



# Install system-level dependencies

RUN apt-get update && apt-get install -y --no-install-recommends \

    build-essential \

    cmake \

    libssl-dev \

    && rm -rf /var/lib/apt/lists/*



# Install a specific Go version

RUN wget -q https://go.dev/dl/go1.22.0.linux-amd64.tar.gz \

    && tar -C /usr/local -xzf go1.22.0.linux-amd64.tar.gz \

    && rm go1.22.0.linux-amd64.tar.gz
```

```
ENV PATH="/usr/local/go/bin:${PATH}"
```

Importante:

Las imágenes personalizadas deben cumplir los requisitos de imagen de contenedor de SecurSpaces: un cliente SSH, Git y Git LFS, y un usuario llamado `developer` con UID 1000. Para ver la lista completa, consulte Requisitos de imagen de contenedor.

Cómo importar la imagen

Después de crear y enviar la imagen a su registro, impórtela en SecurSpaces en **Recursos → Imágenes de contenedor**. Si su registro es privado, asegúrese de que SecurSpaces tenga credenciales para él — consulte la configuración de recursos de Imágenes de contenedor en la configuración de su proyecto u organización.

Para ver los pasos detallados, consulte Cómo actualizar una imagen de contenedor existente. Para ver Dockerfiles y scripts de ejemplo, consulte el repositorio de imágenes de ejemplo de Citrix.

Docker dentro de un espacio de trabajo

Los espacios de trabajo pueden crear y ejecutar contenedores. Para saber qué puede hacer el espacio de trabajo y cómo integrar el cliente Docker en su imagen, consulte Usar Docker dentro de un espacio de trabajo.

Lo que persiste es la parte que corresponde aquí:

QUÉ	SOBREVIVE A UN REINICIO
Archivos en `/home/developer`, incluyendo cualquier cosa que monte en un contenedor	Sí
Imágenes que extrae o compila	Solo con Docker persistente
Contenedores, volúmenes y la caché de compilación	No

Docker persistente es una característica con licencia y está desactivado por defecto, por lo que volver a extraer o reconstruir imágenes después de un reinicio es el comportamiento predeterminado en lugar de un fallo.

Los datos escritos dentro de un contenedor en ejecución nunca se conservan cuando se elimina el contenedor, con o sin Docker persistente; almacena en caché imágenes, no el estado del contenedor. Para conservar lo que produce un contenedor, monte un directorio de `/home/developer` en él. Consulte Cómo persistir datos de contenedores.

Elegir entre los tres

QUIERE PERSISTIR	USAR
Código fuente, archivos de configuración (dot files), ajustes del IDE, herramientas instaladas por el usuario	`/home/developer/`
Configuración por lanzamiento que depende del estado de ejecución, o un paquete rápido de un solo uso	Script de inicio
Paquetes del sistema, tiempos de ejecución, herramientas básicas compartidas en un equipo	Imagen personalizada

Un patrón común es combinar los tres: una imagen personalizada proporciona el entorno base, un script corto posterior al inicio gestiona cualquier elemento dinámico, y su configuración personal reside en `/home/developer/`.

Referencias

- Crear un espacio de trabajo — Scripts de inicio
- Plantillas de espacio de trabajo
- Perfil — Configuración — Script de inicio
- Imágenes de contenedor
- Cómo actualizar una imagen de contenedor existente
- Repositorio de imágenes de ejemplo en GitHub
- Imágenes precompiladas en Docker Hub

Connect to external services over SSH

A menudo necesita acceder a sistemas fuera de su espacio de trabajo a través de SSH — para enviar a un repositorio Git alojado en Azure DevOps, implementar en un servidor de ensayo o abrir una sesión en un host de base de datos remoto.

De forma predeterminada, el servicio proxy de SecurSpaces bloquea el SSH saliente de los espacios de trabajo. Una de las dos opciones debe estar habilitada primero, y ambas son habilitadas por un propietario de proyecto o un oficial de seguridad:

OPCIÓN	LO QUE USTED HACE	LO QUE HACE SU ADMINISTRADOR
Identidad SSH personal	Genere su propia clave en su perfil y registre la clave pública en el servicio de destino	Activa **Habilitar identidad SSH personal** para el espacio de trabajo o la plantilla
Servicios SSH conectados	Nada. Ejecute `ssh <service-name>`.	Crea el servicio con sus credenciales y lo adjunta al espacio de trabajo

Si ninguna está habilitada, consulte SSH saliente bloqueado.

Los administradores deben consultar Habilitar SSH saliente.

Opción 1: Identidad SSH personal

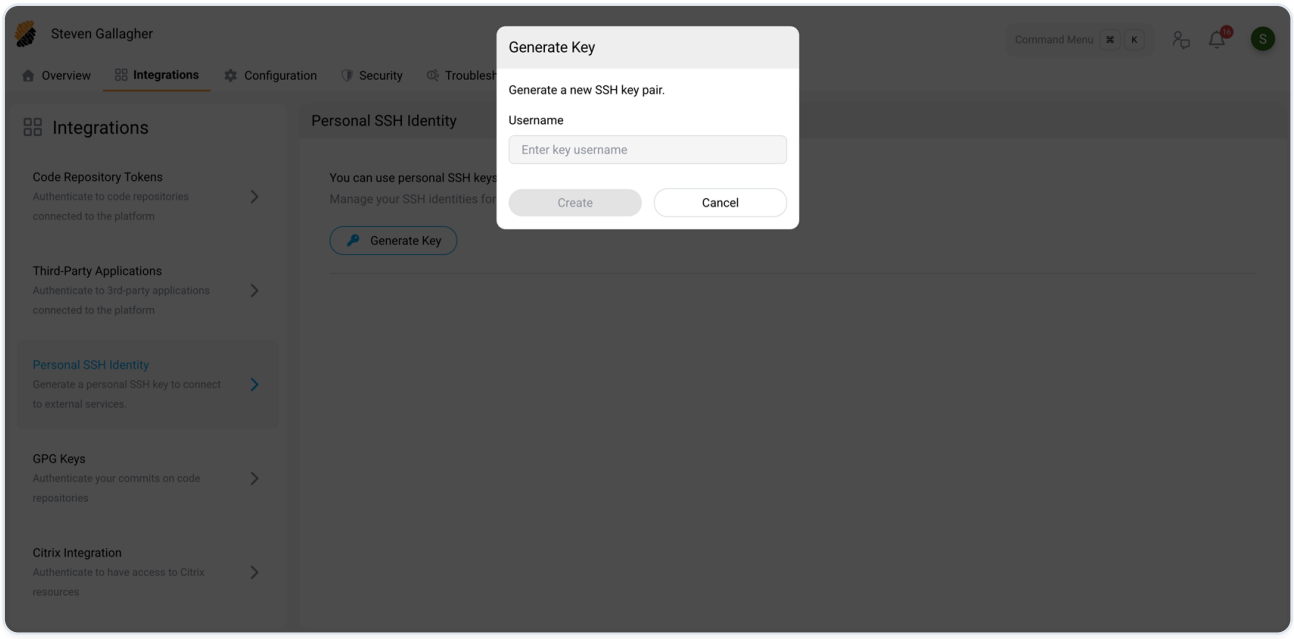
La plataforma genera y guarda un par de claves SSH para usted. La clave privada se aplica automáticamente cuando se conecta y nunca se expone dentro del espacio de trabajo.

Requisito: un propietario de proyecto o un oficial de seguridad ha activado **Habilitar identidad SSH personal** para su espacio de trabajo o su plantilla.

Generar su clave

1. Seleccione su imagen de perfil en la esquina superior derecha para abrir su perfil.
2. Vaya a **Integraciones** > **Identidad SSH personal**.
3. Seleccione **Generar clave**.
4. Introduzca un nombre de usuario predeterminado, por ejemplo `git`. Puede anularlo por servicio al conectarse.

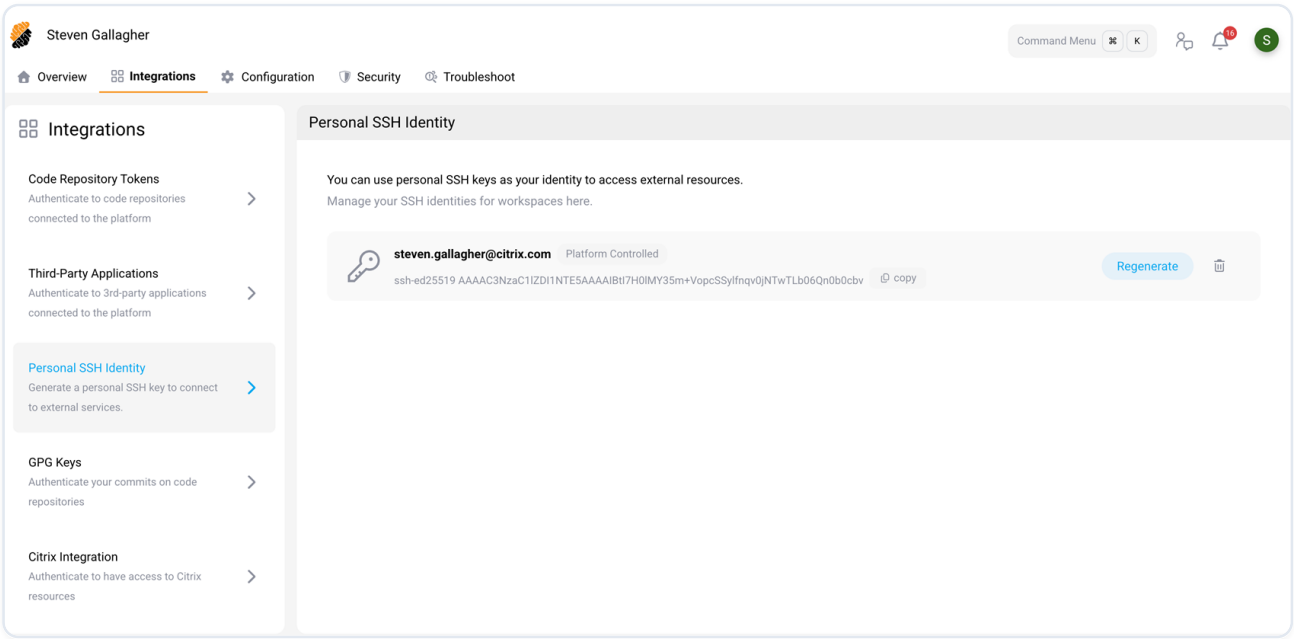
5. Seleccione **Crear**.



La plataforma genera el par y muestra la clave pública. La clave se aplica a los espacios de trabajo nuevos y existentes.

Registrar la clave pública

1. En la página de **Identidad SSH personal**, seleccione **Copiar**.
2. Añada la clave pública al servicio de destino, por ejemplo, añadiéndola a `~/.ssh/authorized_keys` en el host. Los pasos exactos dependen del servicio.



Conectar

Abra un terminal en cualquier espacio de trabajo donde la Identidad SSH personal esté habilitada y conéctese como de costumbre:

```
ssh <username>@<hostname>
```

SecurSpaces aplica su clave privada. No hay ninguna clave que gestionar dentro del espacio de trabajo.

Opción 2: Servicios SSH conectados

Su administrador define el host de destino y sus credenciales una vez, y luego lo adjunta al espacio de trabajo. Usted no maneja una clave ni una contraseña.

Abra un terminal en el espacio de trabajo y use el nombre del servicio como host:

```
ssh gcp-vm
```

SecurSpaces le autentica automáticamente.

SSH saliente está bloqueado

Si no hay ningún método SSH configurado para el host al que intenta acceder, el proxy cierra la sesión y el terminal lo muestra antes de que ocurra. Dependiendo del cliente, también podría ver `no signers found for request` o `ssh: no auth passed yet`, lo que significa lo mismo: el espacio de trabajo no tiene credenciales SSH que presentar.

```
SSH access to external hosts is disabled by default in this workspace.

To connect, an administrator must enable one of:

  - Personal SSH Identity (per-user key) - in the workspace/template
Security Settings

  - a Connected SSH Service - then run: ssh <service-name>

See: https://docs.citrix.com/en-us/securspaces/workspace/ssh-connectivity
```

Pida a un propietario de proyecto o a un oficial de seguridad que habilite una de las dos opciones. La identidad SSH personal es adecuada para acceder a sus propias cuentas; un servicio SSH conectado es adecuado para un host que utiliza todo el equipo.

> **Nota:**
>
> Este mensaje aparece solo cuando la conexión SSH en sí está bloqueada por falta de un método configurado. Una conexión que falla porque el destino no está en una lista de permitidos es un asunto de política de red. Consulte Monitorizar y solucionar problemas.

Información relacionada

- Habilitar SSH saliente
- Servicios SSH conectados
- Integración

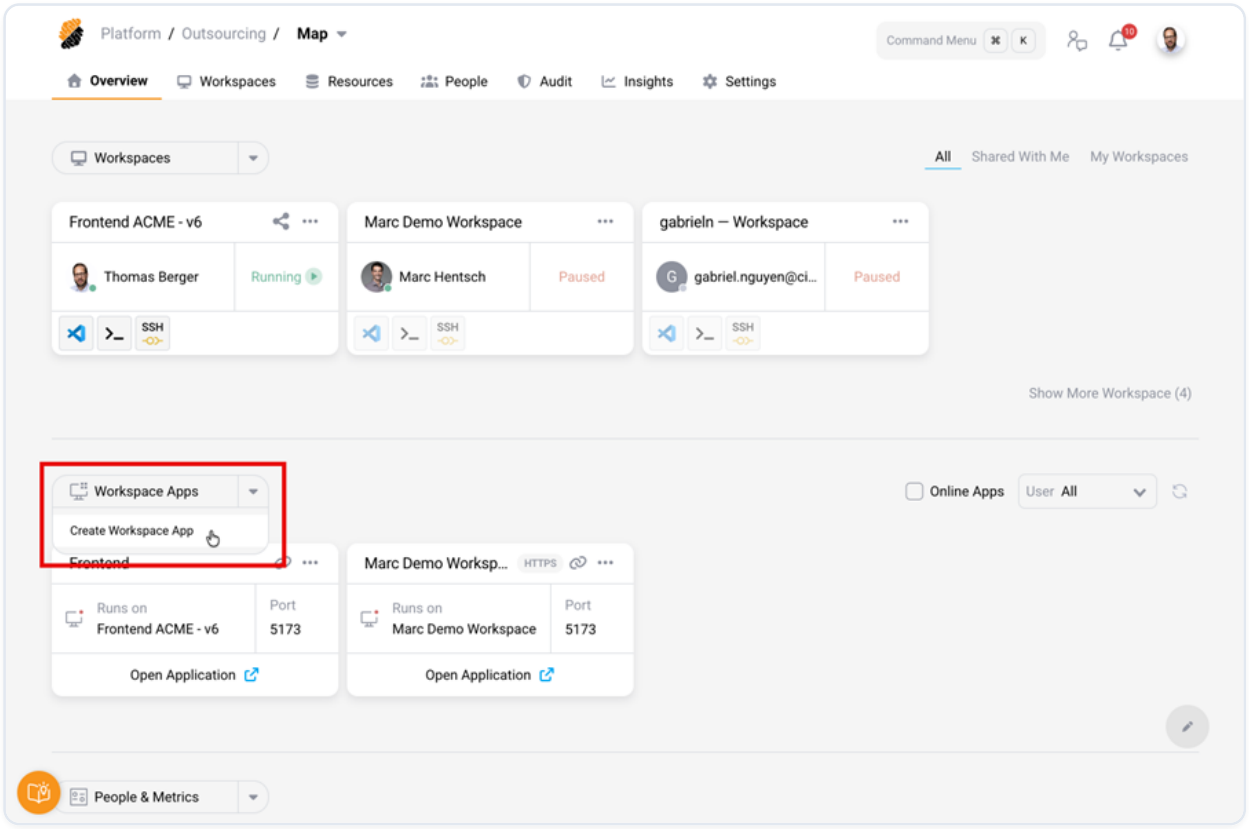
Share a running application

Una **aplicación de espacio de trabajo** le permite acceder a una aplicación o proceso a través de HTTP o HTTPS que se ejecuta en un puerto de su espacio de trabajo. Puede tener varias aplicaciones de espacio de trabajo adjuntas a un único espacio de trabajo, cada una accediendo a una aplicación que se ejecuta en un puerto diferente. Los casos de uso comunes incluyen probar aplicaciones web, webhooks y devoluciones de llamada, y exponer las interfaces web de las herramientas de desarrollo.

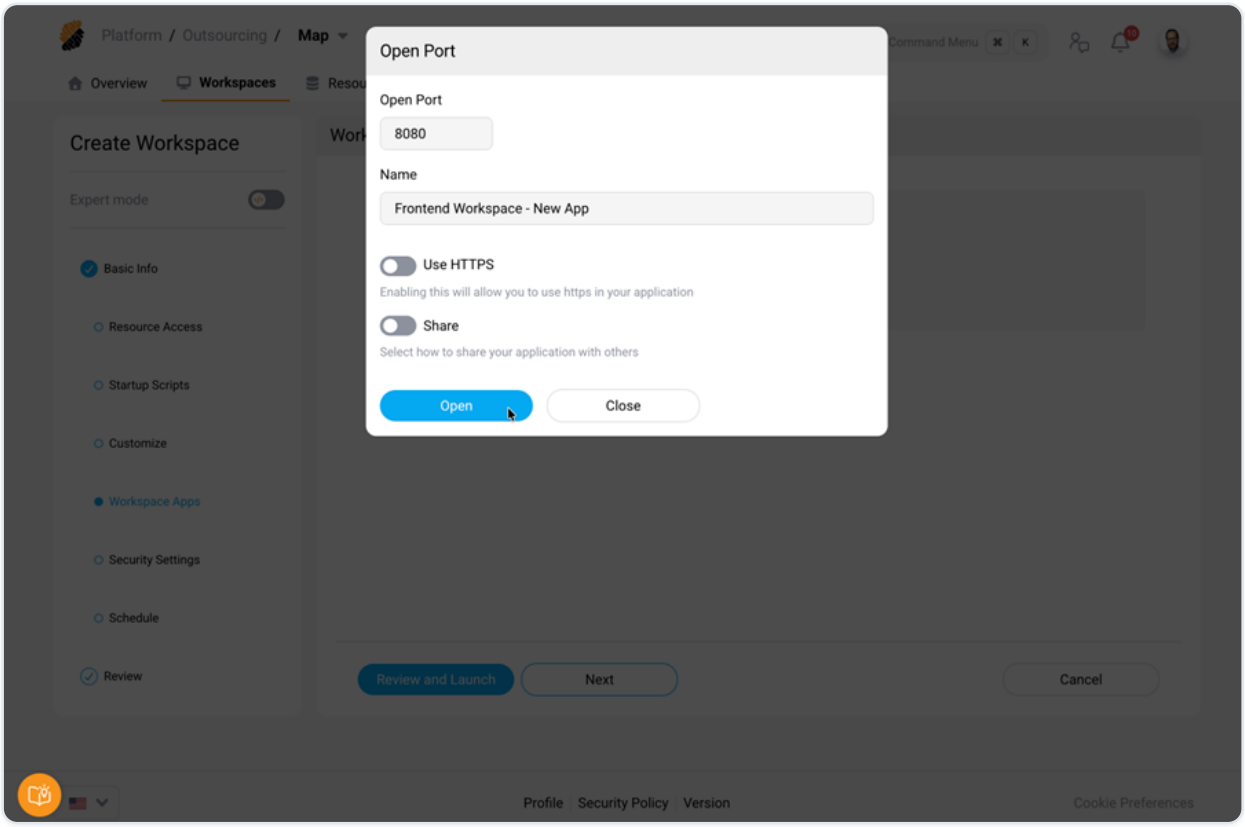
Crear una aplicación de espacio de trabajo

Las aplicaciones de espacio de trabajo se pueden crear de diferentes maneras.

- Desde la página de descripción general del proyecto, seleccione el botón **Crear aplicación de espacio de trabajo** del menú desplegable **Aplicaciones de espacio de trabajo** y siga las instrucciones en pantalla.



- Al crear o editar un espacio de trabajo o una plantilla de espacio de trabajo, seleccione el menú **Aplicaciones de espacio de trabajo** en el asistente y siga las instrucciones en pantalla. Al añadir una aplicación de espacio de trabajo a una plantilla, todos los espacios de trabajo secundarios heredan esta configuración automáticamente.



- Haga clic en el icono **"..."** en un espacio de trabajo y seleccione **Editar puertos**.

En cualquier caso, debe introducir la siguiente información:

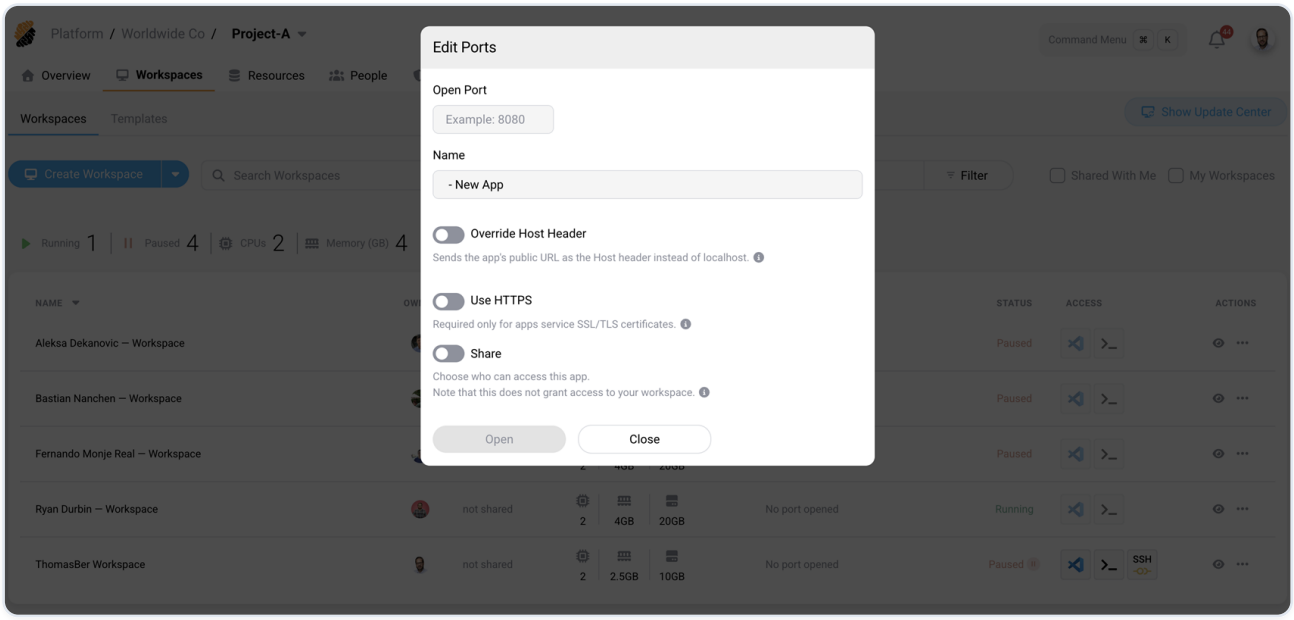
1. **Puerto** — El puerto donde la aplicación o el proceso se está ejecutando en su espacio de trabajo.
2. **Nombre** — Un nombre para mostrar de la aplicación de espacio de trabajo. Citrix SecurSpaces™ utiliza este nombre para hacer referencia a la aplicación.
3. **Anular encabezado de host** — Habilite esta opción cuando su aplicación rechace solicitudes debido a una falta de coincidencia del encabezado de host. Consulte Anular encabezado de host para obtener más detalles.
4. **Usar HTTPS** — Habilite esta opción solo si su aplicación sirve sus propios certificados TLS. Para la mayoría de los escenarios, déjelo desactivado. Independientemente de esta configuración, la plataforma siempre se expone a través de HTTPS, por lo que la conexión del navegador aparece como HTTPS. El interruptor controla únicamente si la plataforma llama a la aplicación dentro del espacio de trabajo utilizando HTTP o HTTPS.
5. **Compartir** — Controle quién puede acceder a la aplicación. Consulte Compartir una aplicación de espacio de trabajo para ver las opciones.

> **Sugerencia**

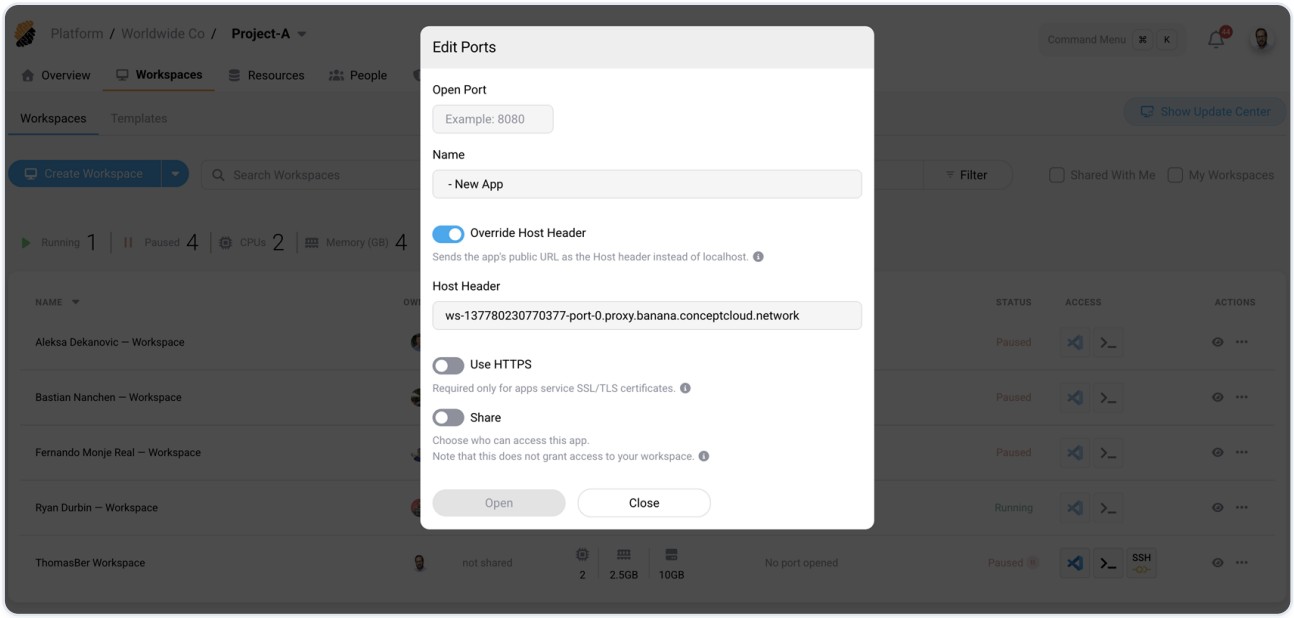
> Cuando cree una aplicación de espacio de trabajo para un proyecto Node.js, asegúrese de que el número de puerto coincida con el que está abierto en el localhost del espacio de trabajo.

Anular encabezado de host

Cuando una aplicación de espacio de trabajo se ejecuta detrás del servicio de proxy de SecurSpaces, algunas aplicaciones (como Jupyter Notebook o pgAdmin) pueden bloquear las solicitudes debido a una falta de coincidencia entre el encabezado Host y el encabezado Origin. Por defecto, el proxy reenvía `localhost` como el encabezado Host, mientras que el encabezado Origin contiene la URL pública de la aplicación del espacio de trabajo. Las aplicaciones que no comprueban `X-Forwarded-Host` interpretan esto como una solicitud de origen cruzado y la rechazan.



Habilite **Anular encabezado de host** para que el proxy envíe la URL pública de la aplicación del espacio de trabajo en el encabezado Host en lugar de `localhost`. Esto alinea los encabezados Host, Origin y X-Forwarded-Host para que la aplicación funcione sin una configuración de proxy por herramienta.



Cuando está habilitado, aparece un campo **Encabezado de host**, rellenado previamente con el nombre de dominio completo (FQDN) de la aplicación del espacio de trabajo. Puede aceptar el valor predeterminado o introducir un valor personalizado.

> **Importante**

> Deje **Anular encabezado de host** deshabilitado para flujos de trabajo de desarrollo local donde el servidor espera `localhost` como encabezado Host. Habilitarlo en esos casos puede romper la aplicación.

Compartir una aplicación de espacio de trabajo

Puede compartir una aplicación de espacio de trabajo al crearla o editando una existente.

Para actualizar las propiedades de una aplicación de espacio de trabajo, puede:

- En la página de Resumen del proyecto, haga clic en el icono **"..."** de la aplicación del espacio de trabajo y seleccione **Editar**.
- Haga clic en el icono **"..."** del espacio de trabajo que aloja la aplicación y seleccione **Editar puertos**.

Hay tres opciones para compartir:

- **Público** — Cualquiera con el enlace que pueda conectarse al entorno de SecurSpaces a través de la red puede acceder a la aplicación del espacio de trabajo.
- **Compartir proyecto** — Solo los miembros del proyecto de SecurSpaces pueden acceder a la aplicación del espacio de trabajo.
- **Compartir con miembros del proyecto** — Solo los miembros seleccionados del proyecto de SecurSpaces pueden acceder a la aplicación del espacio de trabajo.

Conceder acceso a una aplicación de espacio de trabajo no proporciona acceso al espacio de trabajo que ejecuta la aplicación. Para compartir un espacio de trabajo con otro usuario, utilice la funcionalidad **Compartir espacio de trabajo**.

> **Nota**

> La opción de compartir **Público** se rige por una política a nivel de plataforma. Un administrador de plataforma debe habilitar **Permitir la creación de aplicaciones de espacio de trabajo públicas** en Configuración de aplicaciones de espacio de trabajo para que el uso compartido público surta efecto. Los dos nombres se refieren a la misma capacidad: **Público** es el modo de compartir que selecciona en una aplicación individual, mientras que **Permitir la creación de aplicaciones de espacio de trabajo públicas** es la política de plataforma que lo permite. Si la política está deshabilitada, una aplicación de

> espacio de trabajo configurada como **Público** aún requiere que los espectadores se autentiquen en la plataforma.

Acceder a una aplicación de espacio de trabajo mediante una clave API

Puede acceder a una aplicación de espacio de trabajo en ejecución mediante programación con una clave API en lugar de autenticarse interactivamente en un navegador. Esto es útil para scripts, pipelines de CI, webhooks y otras llamadas automatizadas.

Este método solo funciona cuando un administrador de plataforma habilita **Permitir acceso a aplicaciones de espacio de trabajo mediante claves API** en Configuración de aplicaciones de espacio de trabajo. Cuando la política está deshabilitada, la plataforma ignora las claves API y la solicitud recurre a la autenticación estándar.

Para autenticar una solicitud, incluya su clave API en el encabezado `Strong-Network-Authorization`:

```
Strong-Network-Authorization: <API_KEY>
```

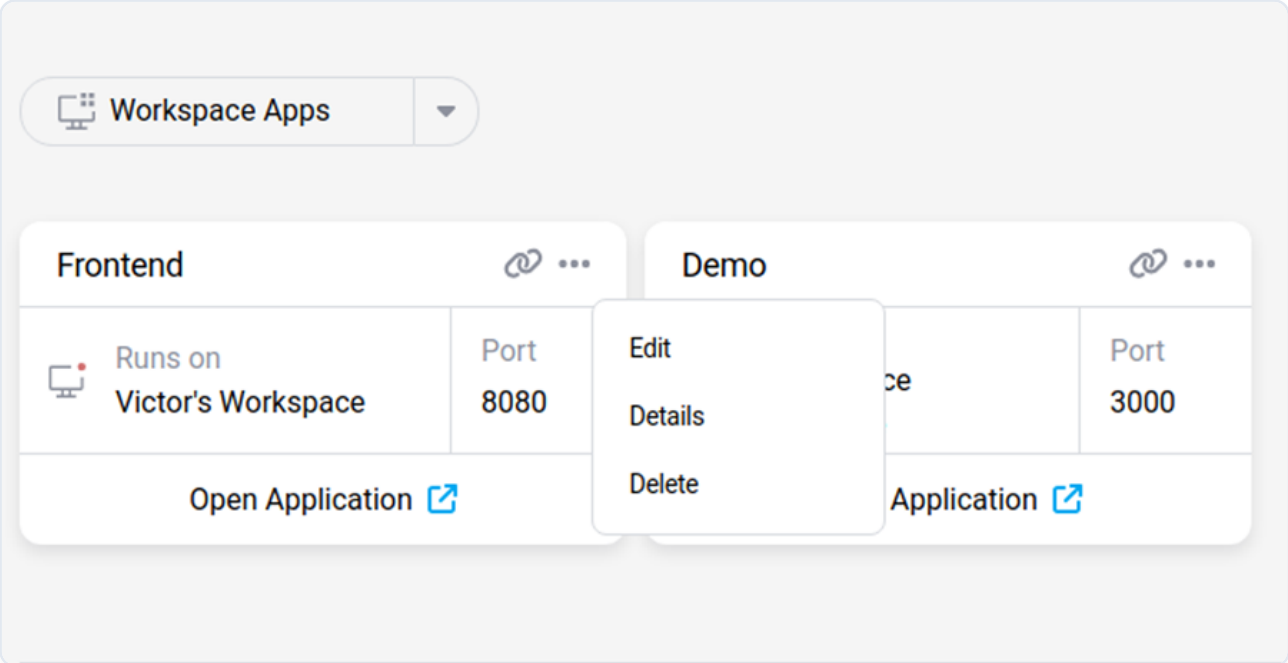
La clave API concede acceso solo cuando su ámbito coincide con la aplicación del espacio de trabajo y el usuario que creó la clave tiene permiso para acceder a la aplicación, es decir, el usuario es propietario del espacio de trabajo, la aplicación se comparte con el proyecto o la aplicación se comparte directamente con ese usuario.

Por ejemplo, para llamar a una aplicación de espacio de trabajo que se ejecuta en el puerto 8010:

```
curl -v \

  -H "Strong-Network-Authorization: <API_KEY>" \

  https://<workspace-app-public-url>/your/app/path
```

Eliminar una aplicación de espacio de trabajo

Puede eliminar una aplicación de espacio de trabajo desde la página de Información general pulsando el icono **"..."** y seleccionando **Eliminar**. También puede eliminar una aplicación de espacio de trabajo haciendo clic en el icono **"..."** en un espacio de trabajo y seleccionando **Editar puertos**.



Your profile

> **¿Configurando por primera vez?**

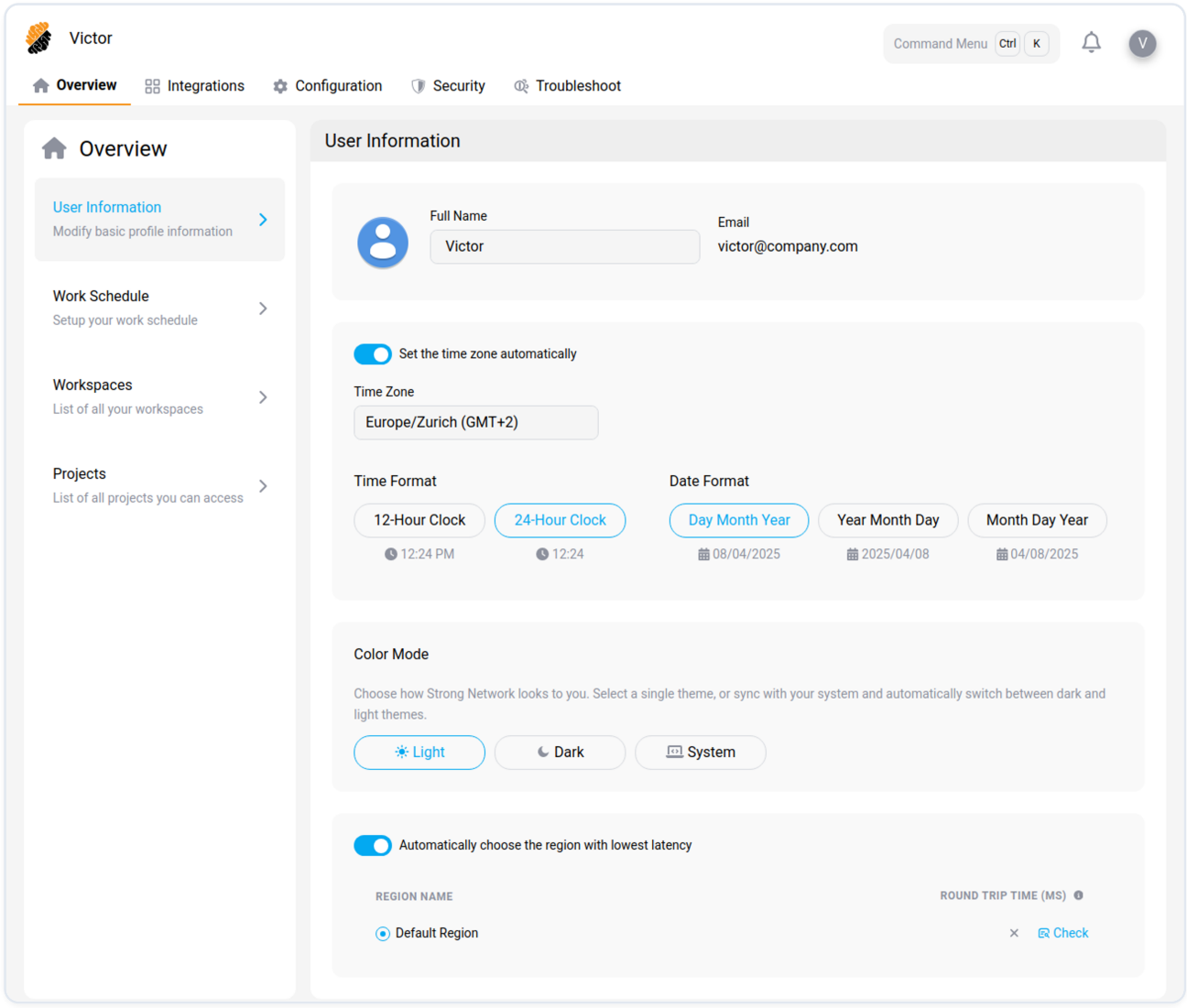
> Configurar su cuenta le guía a través de estas cuatro páginas en orden, como una tarea guiada de primera ejecución. Utilice las páginas siguientes cuando desee obtener los detalles de una configuración específica.

> Las páginas de **Perfil y Configuración de la cuenta** le permiten gestionar datos personales y establecer preferencias sobre sus hábitos de trabajo. Por ejemplo, puede configurar un horario de trabajo para que su espacio de trabajo se implemente automáticamente en horas preestablecidas.

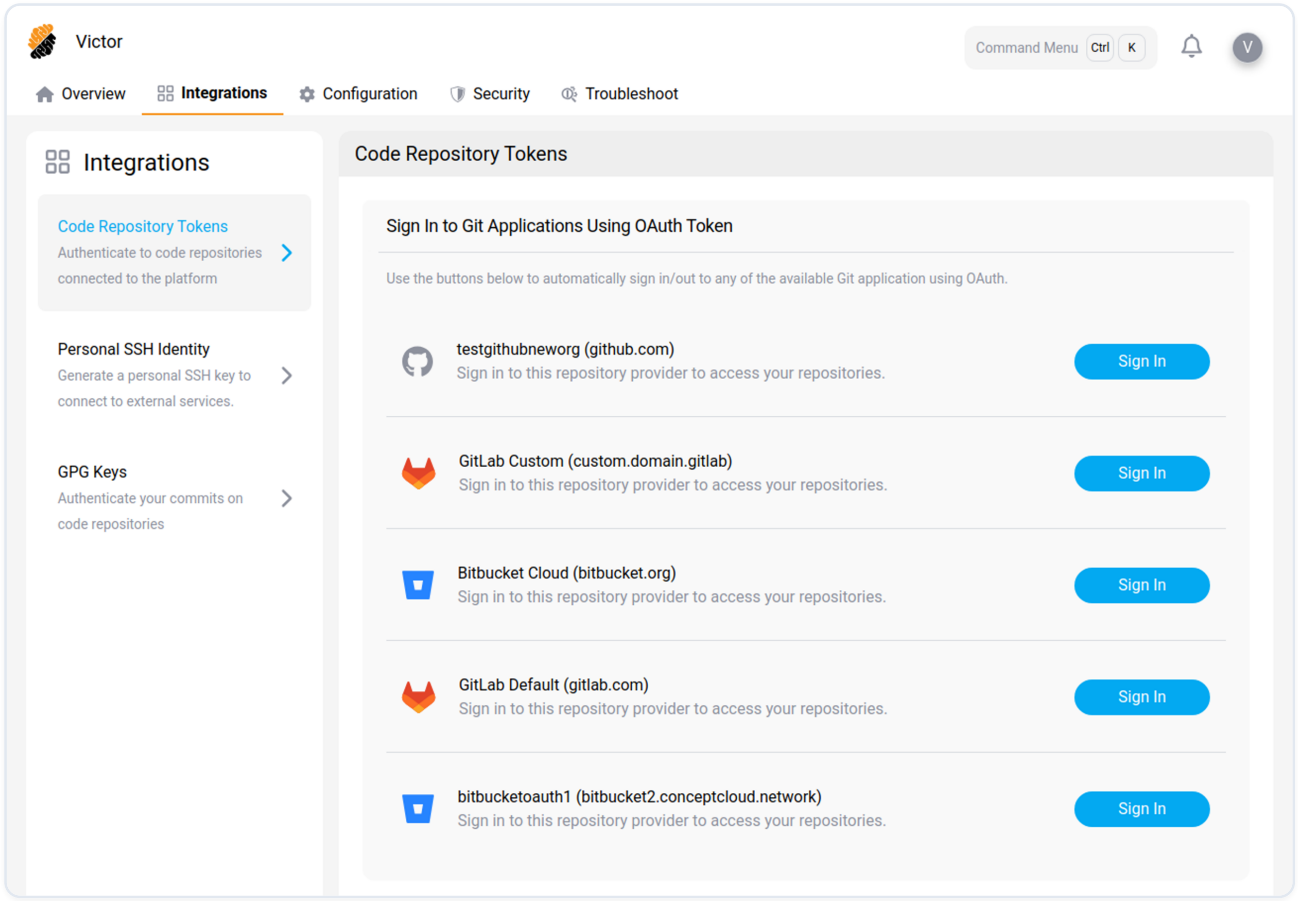
El perfil también se utiliza para almacenar cualquier archivo de configuración personal, como .bashrc, etc., necesario para personalizar sus espacios de trabajo.

Además, puede usar el perfil para registrar configuraciones de IDE, incluidos los complementos instalados, y replicarlas en todos los espacios de trabajo. Finalmente, el perfil es el lugar para gestionar los diferentes tokens de autenticación y claves de acceso para autenticarse en las aplicaciones GIT adjuntas a las plataformas y accesibles desde los espacios de trabajo.

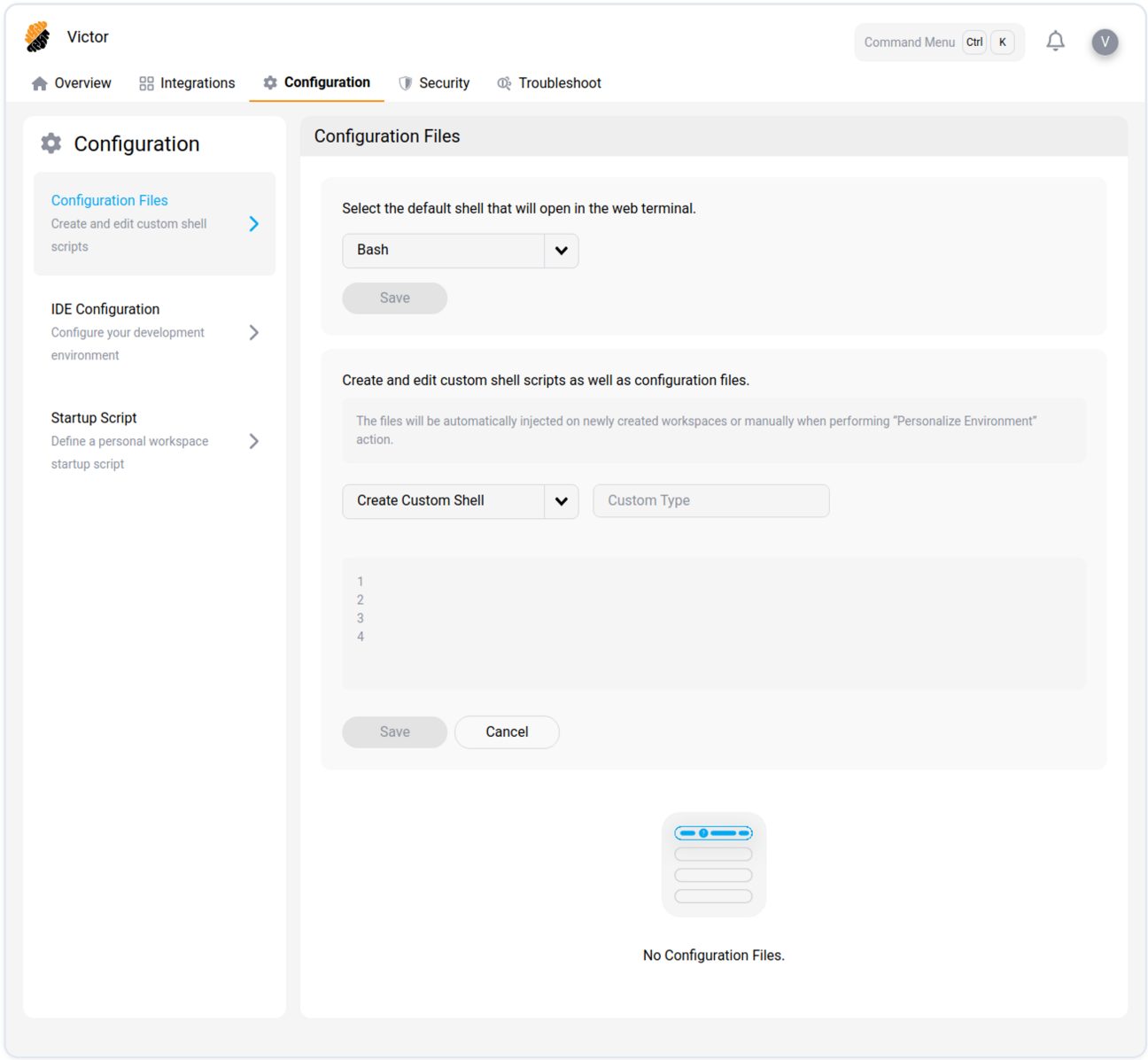
La **Página de Resumen** le permite editar información personal, definir un horario de trabajo, ver los espacios de trabajo propios y la membresía del proyecto.



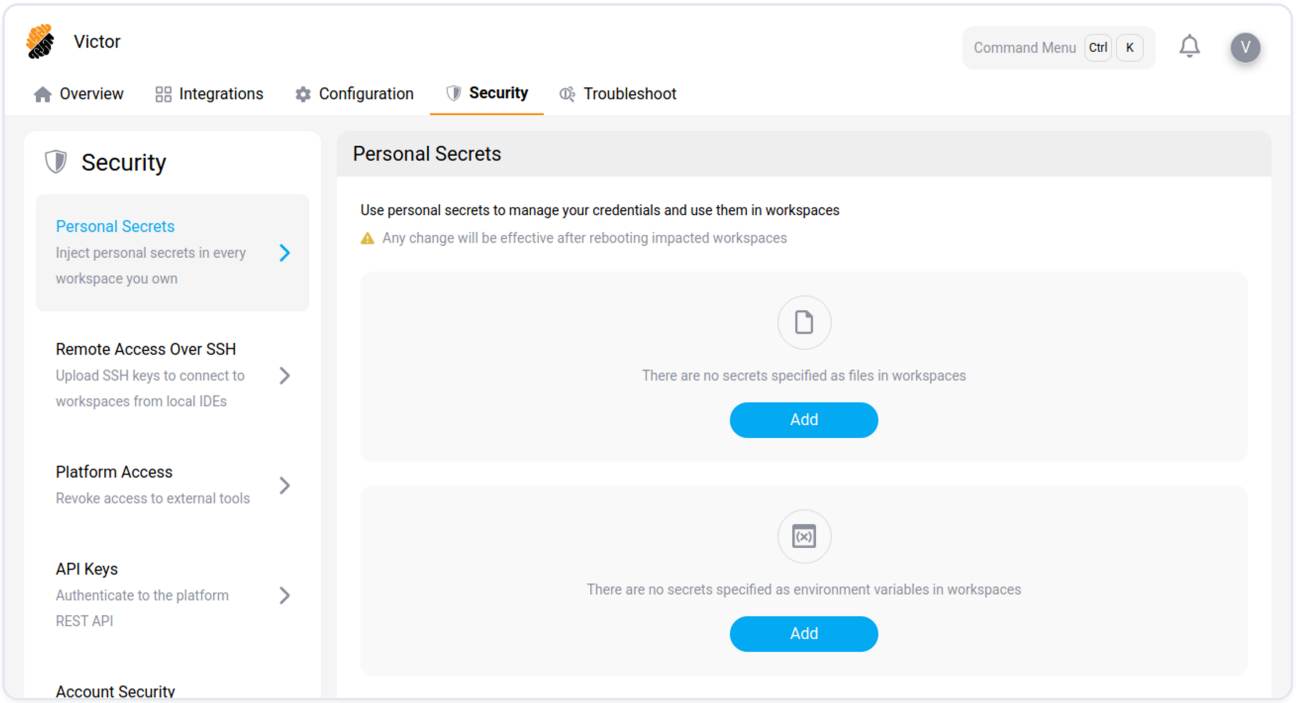
La **Página de Integración** le permite crear y editar diferentes tokens de autenticación, identidad SSH personal y claves GPG.



La **Página de Configuración** le permite crear y editar archivos de configuración personalizados, configuraciones de IDE y scripts de inicio de espacio de trabajo.



La **Página de Seguridad** le permite crear y editar claves API, claves SSH y secretos personales.



Menú de la cuenta

Seleccione su imagen de perfil en la parte superior derecha de la pantalla para abrir el menú de la cuenta. Junto con las páginas de perfil y la configuración del tema, el menú incluye:

- **REST API** — la especificación de la API para su implementación. Consulte REST API.
- **Documentación** — este conjunto de documentación.
- **Novedades** — las notas de la versión de SecurSpaces, en una nueva pestaña del navegador.
- **Sus organizaciones** y **Sus proyectos** — las organizaciones y proyectos a los que pertenece.

Contenido

- **Página de resumen**
- **Página de integración**
- **Página de configuración**
- **Página de seguridad**
- **Solución de problemas** — cuatro herramientas de diagnóstico para la conexión IDE, la latencia de la región, DNS y los protocolos de red

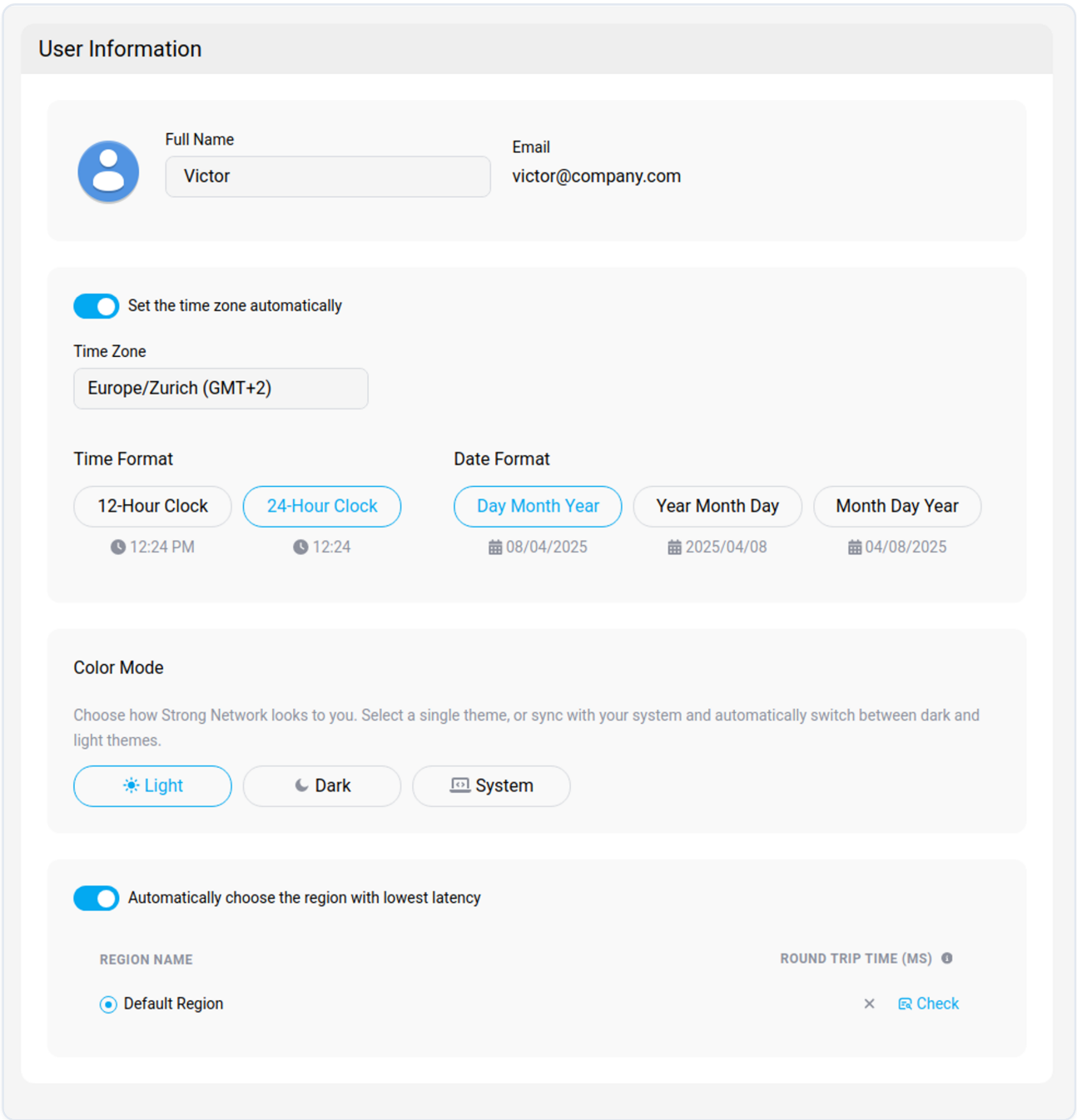
Profile overview

La **página de resumen del perfil** sirve como un resumen completo de la información del usuario, su propiedad de espacios de trabajo y la pertenencia a proyectos.

- Información del usuario
- Horario de trabajo
- Espacios de trabajo
- Proyectos

Información del usuario

En la sección de **Información del usuario** puede modificar el nombre y la zona horaria de su usuario. El correo electrónico vinculado a su perfil no se puede modificar. La imagen de perfil se recupera de su proveedor de identidad cuando está disponible.



Preferencias de visualización

La misma pestaña contiene la configuración que controla cómo se ve la consola para usted. Se aplican solo a su cuenta, le siguen entre dispositivos y no afectan a lo que ven otras personas.

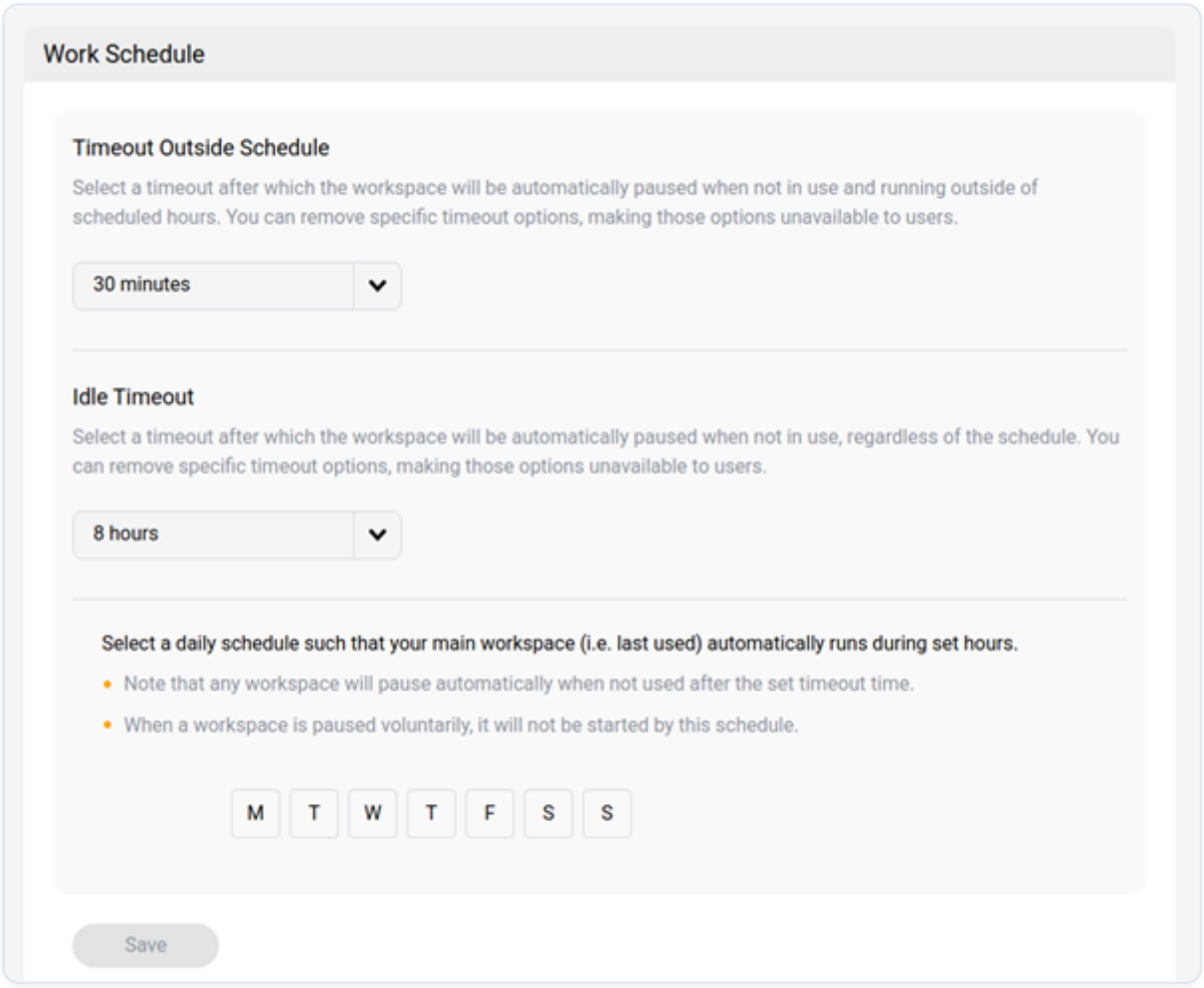
CONFIGURACIÓN	OPCIONES
Zona horaria	Establecer manualmente o activar **Establecer la zona horaria automáticamente**
Formato de hora	12 horas o 24 horas
Formato de fecha	Día/Mes/Año, Año/Mes/Día o Mes/Día/Año
Modo de color	**Claro**, **Oscuro** o **Sistema** para seguir la configuración de su sistema operativo
Idioma de la interfaz	**Inglés (Estados Unidos)** o **Francés (Suiza)**

El **Idioma de la interfaz** cambia los menús, las etiquetas y los mensajes del sistema en la consola. No traduce el contenido que usted o sus administradores hayan creado, como nombres de proyectos, nombres de espacios de trabajo o descripciones de plantillas, y no cambia el idioma dentro de un espacio de trabajo o su IDE.

Debajo de estas configuraciones, **Elegir automáticamente la región con la latencia más baja** permite que la plataforma seleccione una región para usted. La tabla debajo de ella enumera cada región con su tiempo de ida y vuelta, y **Comprobar** lo mide de nuevo.

Horario de trabajo

En la sección **Horario de trabajo**, puede configurar el horario de trabajo de su perfil. Durante las horas establecidas, su espacio de trabajo principal (es decir, el último utilizado) se implementa automáticamente.



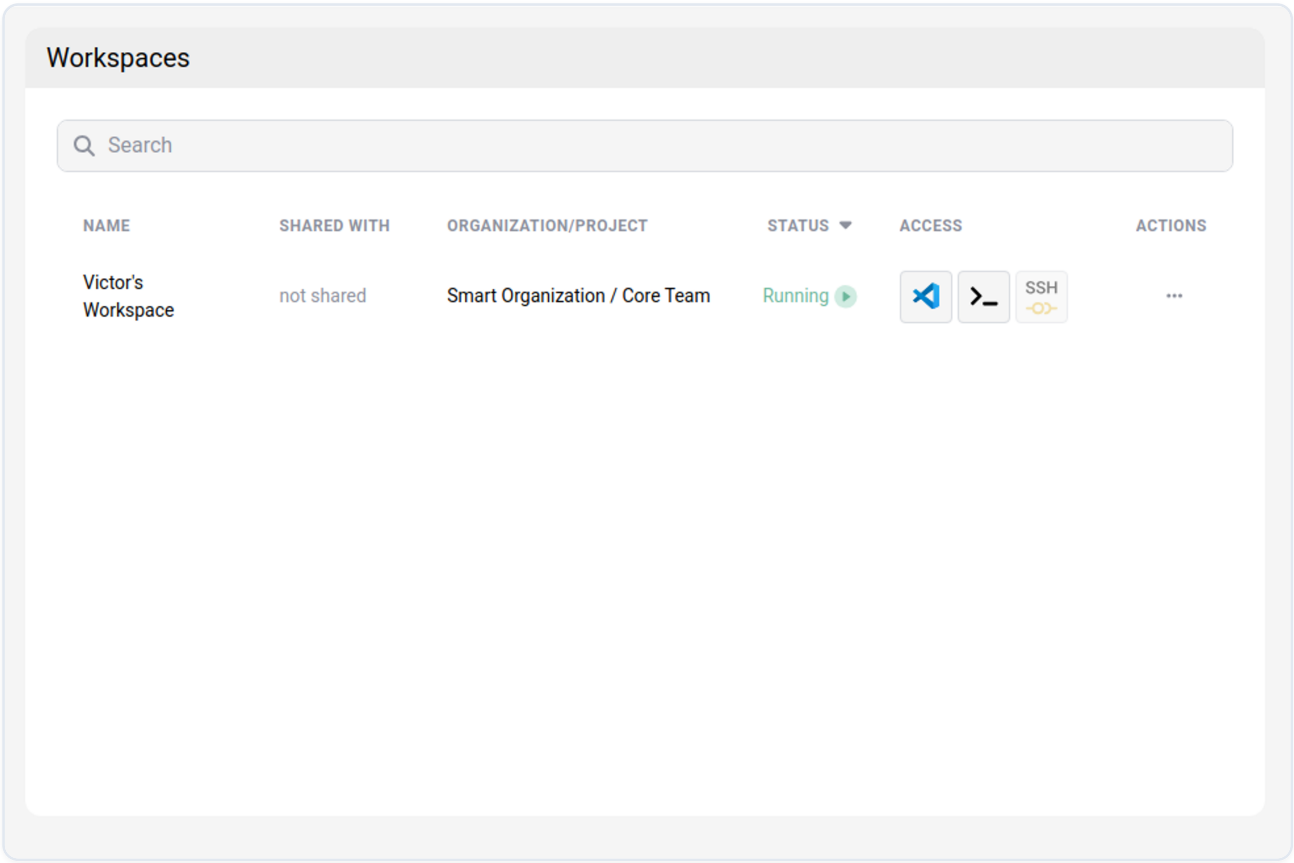
> Consejo:

> Los espacios de trabajo se pausarán automáticamente cuando no se utilicen durante un tiempo preestablecido, normalmente 60 minutos, dependiendo de la configuración de su plataforma.

> Cuando un espacio de trabajo se pausa voluntariamente, no se verá afectado por el horario.

Espacios de trabajo

En la sección **Espacios de trabajo**, puede encontrar detalles sobre sus espacios de trabajo individuales en todos los proyectos de los que forma parte. Al seleccionar la opción "**...**" en un espacio de trabajo específico, puede realizar directamente acciones como ejecutar, pausar, editar, ver detalles o eliminar el espacio de trabajo.



Espacios de trabajo pendientes de eliminación

Sus espacios de trabajo se enumeran en dos secciones. **Espacios de trabajo activos** enumera los espacios de trabajo que puede usar ahora. **Espacios de trabajo pendientes de eliminación** enumera sus propios espacios de trabajo que se han movido a la papelera de reciclaje y aún pueden recuperarse.

Un espacio de trabajo suele llegar a esta sección porque su administrador configuró una acción personalizada que elimina los espacios de trabajo después de un período de inactividad. Eliminar un espacio de trabajo usted mismo también lo coloca aquí.

Cada entrada muestra la fecha y hora en que el espacio de trabajo se elimina permanentemente, en UTC.

> **Nota**

> La fecha mostrada es la fecha límite para la eliminación permanente, no la fecha en que el espacio de trabajo se movió a la papelera de reciclaje. Después de esa fecha, el espacio de trabajo no se puede recuperar.

> Para recuperar un espacio de trabajo, seleccione **Restaurar** y confirme. El espacio de trabajo vuelve a **Espacios de trabajo activos**.

La restauración cuenta para el número máximo de espacios de trabajo que se le permite tener. Si ya ha alcanzado su límite, elimine o libere otro espacio de trabajo primero.

Para eliminar un espacio de trabajo inmediatamente en lugar de esperar la fecha límite, seleccione **Eliminar** y confirme. La eliminación permanente no se puede deshacer.

Notificaciones por correo electrónico sobre eliminación pendiente

Cuando una acción personalizada mueve uno de sus espacios de trabajo a la papelera de reciclaje, SecurSpaces le envía un correo electrónico. Usted recibe:

- Un mensaje cuando el espacio de trabajo se mueve a la papelera de reciclaje.
- Un recordatorio 24 horas antes de que el espacio de trabajo se elimine permanentemente.

Ambos mensajes nombran el espacio de trabajo y su proyecto, indican la hora de eliminación permanente en UTC y enlazan a esta página. Si restaura el espacio de trabajo, el recordatorio se cancela.

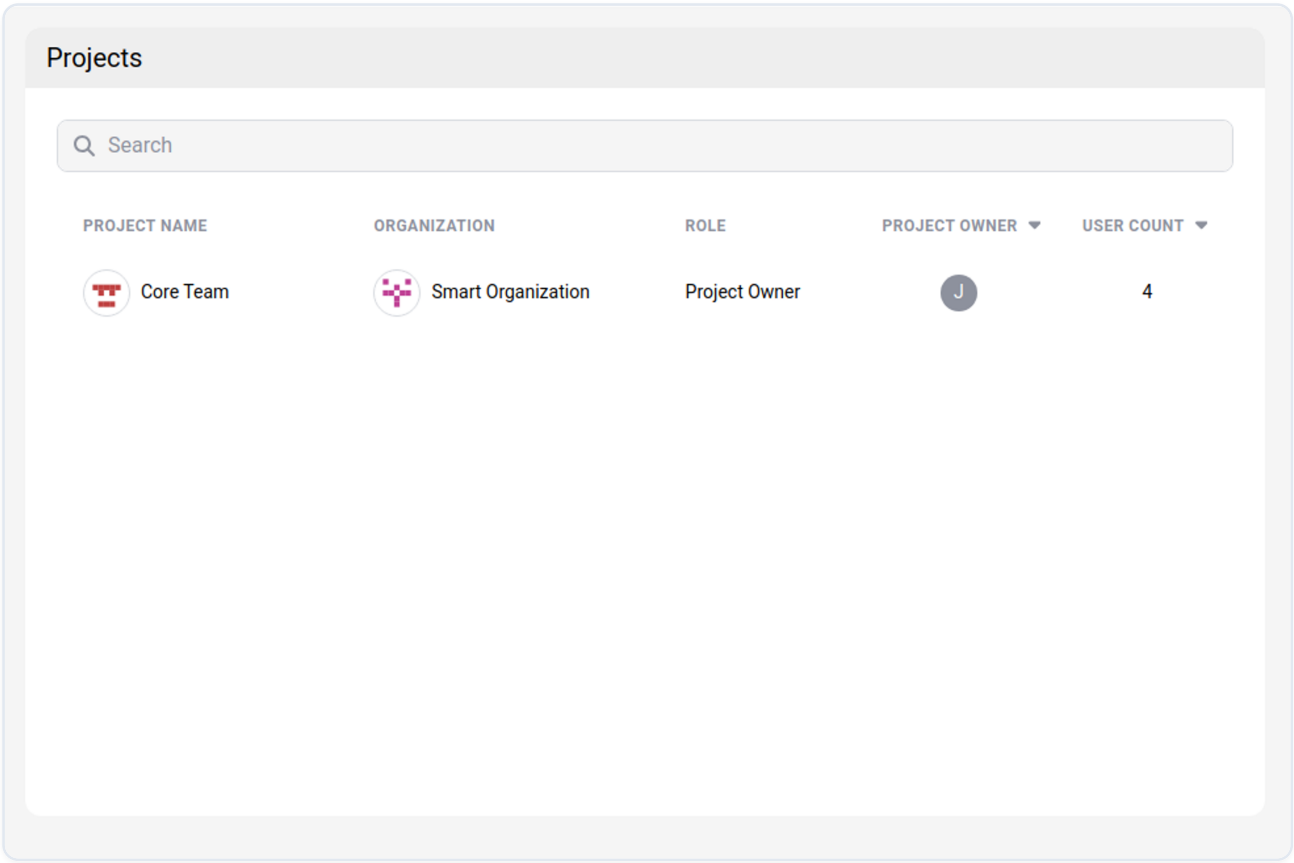
Restaurar un espacio de trabajo como administrador

Los propietarios de proyectos, los administradores de plataforma y los responsables de seguridad pueden restaurar cualquier espacio de trabajo dentro de su ámbito, en lugar de solo los suyos propios. Abra **Espacios de trabajo eliminados** desde la configuración del proyecto o la configuración del espacio de trabajo de la plataforma, busque el espacio de trabajo y seleccione **Restaurar**.

Para el período de retención que controla cuánto tiempo permanece recuperable un espacio de trabajo eliminado, consulte Configuración del espacio de trabajo.

Proyectos

La sección **Proyectos** muestra información sobre cada proyecto del que es miembro, dentro de las organizaciones a las que pertenece. Esto incluye detalles como el nombre del proyecto, la organización que aloja el proyecto, su rol dentro del proyecto, el propietario del proyecto y el número de usuarios involucrados en el proyecto. Al hacer clic en el nombre de un proyecto, puede acceder a su panel de control para obtener más información.



Información relacionada

- Configuración
- Integraciones
- Seguridad
- Su perfil

Integrations

En la **Página de Integración** puede gestionar las diferentes claves de acceso, secretos y tokens vinculados al perfil del usuario. Esto incluye **Tokens de Repositorio de Código**, **Identidad SSH Personal** y **Claves GPG**. Las claves y los tokens se utilizan para autenticar y autorizar el acceso a diferentes servicios, como las aplicaciones de repositorio remoto. Al gestionar sus claves, tokens y secretos en una única ubicación, los usuarios pueden llevar un seguimiento fácilmente de cuáles se están utilizando, con qué propósito, y pueden revocar o añadir nuevos según sea necesario. La página también permite al usuario ver, crear y eliminar estos elementos, gestionar los niveles de acceso y tener una visión general de su fecha de caducidad. Esto ayuda a garantizar que solo los usuarios autorizados tengan acceso a los recursos y servicios necesarios, y que el acceso se revoque cuando sea preciso.

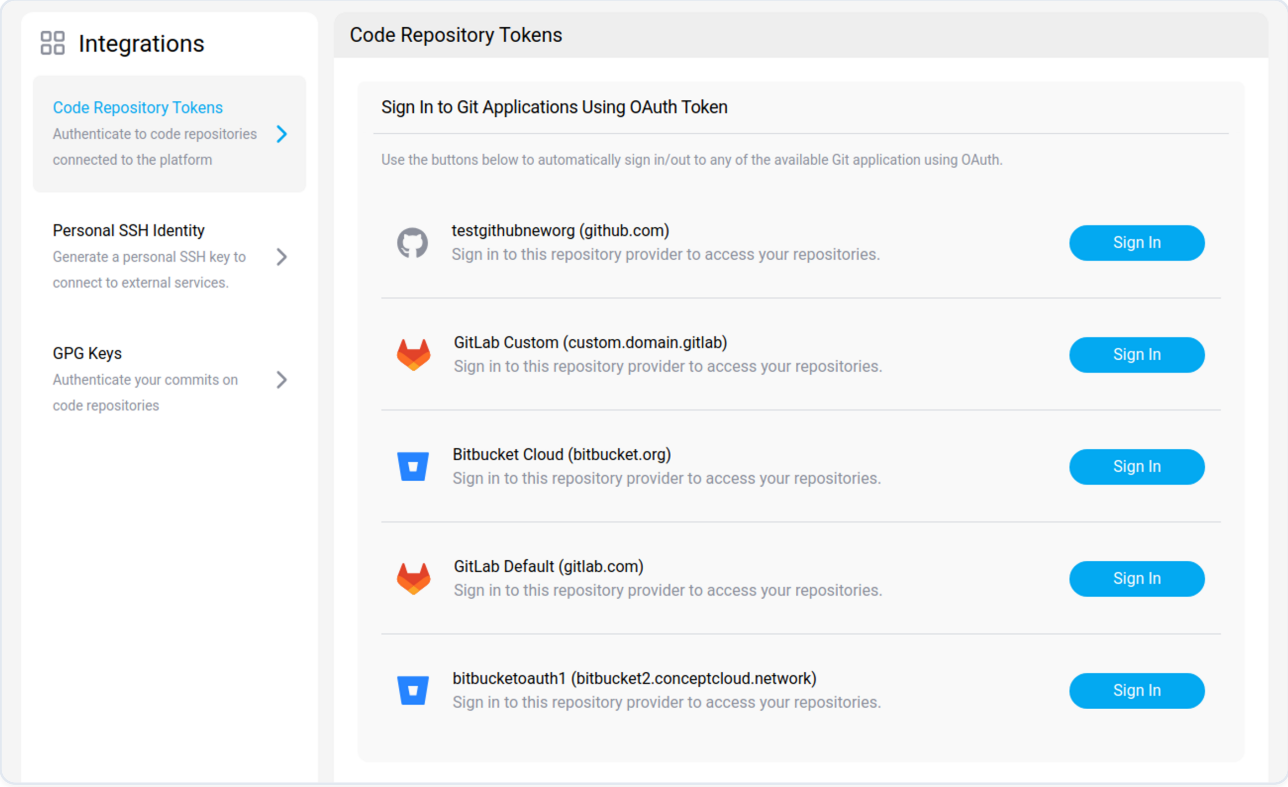
- Tokens de Repositorio de Código

- Identidad SSH Personal
- Claves GPG
- Integración de Citrix

Tokens de Repositorio de Código

En **Tokens de Repositorio de Código**, puede configurar la autenticación, utilizando **Tokens de Autenticación OAuth** o **Claves SSH Personales**, para los siguientes proveedores de Git:

- **GitHub**,
- **GitLab**,
- y **Bitbucket**. Para algunos de estos proveedores de Git, tiene la opción de elegir entre las opciones 'Predeterminado' o 'Interno'. Un 'Servicio Interno' es autoalojado, mientras que un 'Servicio Predeterminado' está alojado en la nube.



Para saber cómo se añaden los repositorios como recursos de proyecto, consulte Repositorios de código.

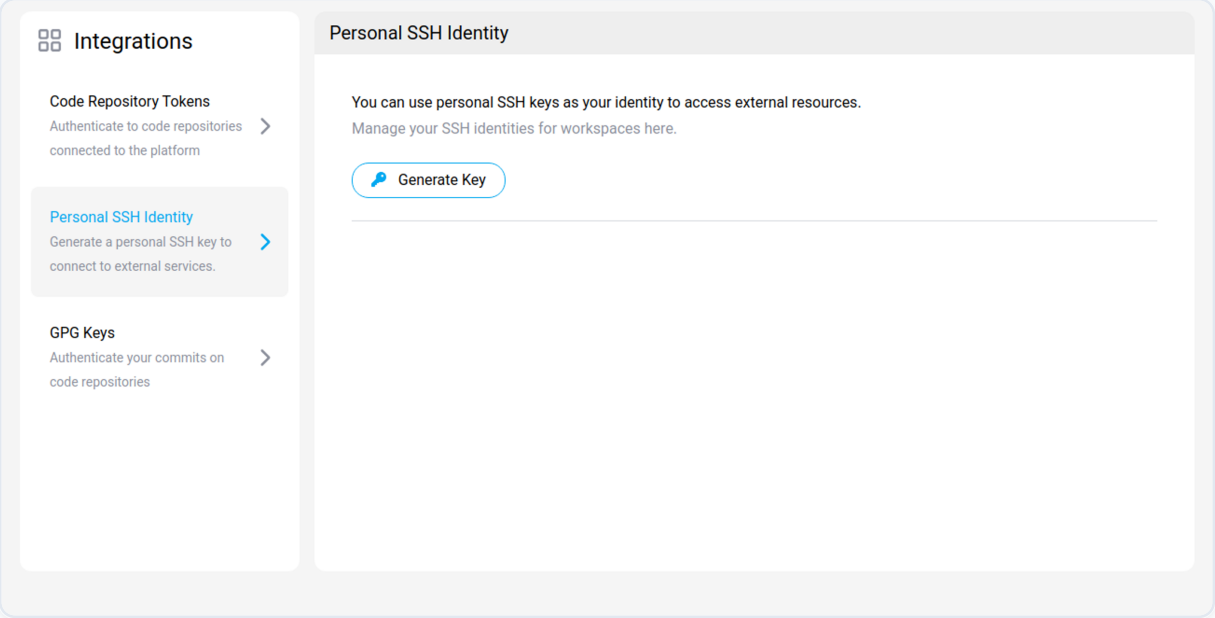
Identidad SSH Personal

Utilice la opción de identidad SSH personal para autenticarse con recursos externos a través de SSH.

Para configurarlo, seleccione Generar clave. El sistema crea un par de claves pública/privada y muestra la clave pública. Añada esta clave pública a su servicio SSH externo como opción de autenticación. Cuando acceda al servicio externo, Citrix SecurSpaces™ aplica automáticamente la clave privada a su sesión. Esto elimina la necesidad de una gestión manual de claves y evita que el código malicioso en el espacio de trabajo extraiga la clave. **Nota:** La clave SSH se aplica tanto a los espacios de trabajo nuevos como a los existentes.

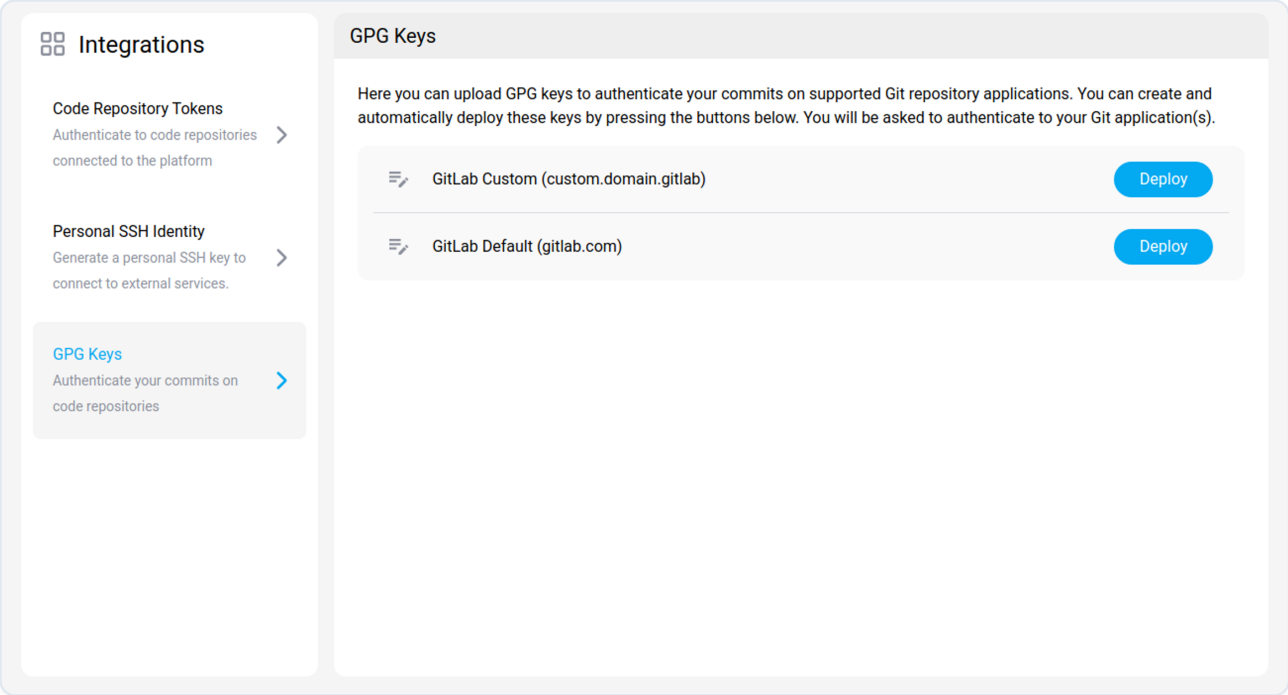
Importante:

Para conectarse a los servicios SSH, debe configurar una identidad SSH personal o configurar el servicio SSH como un recurso del proyecto.



Claves GPG

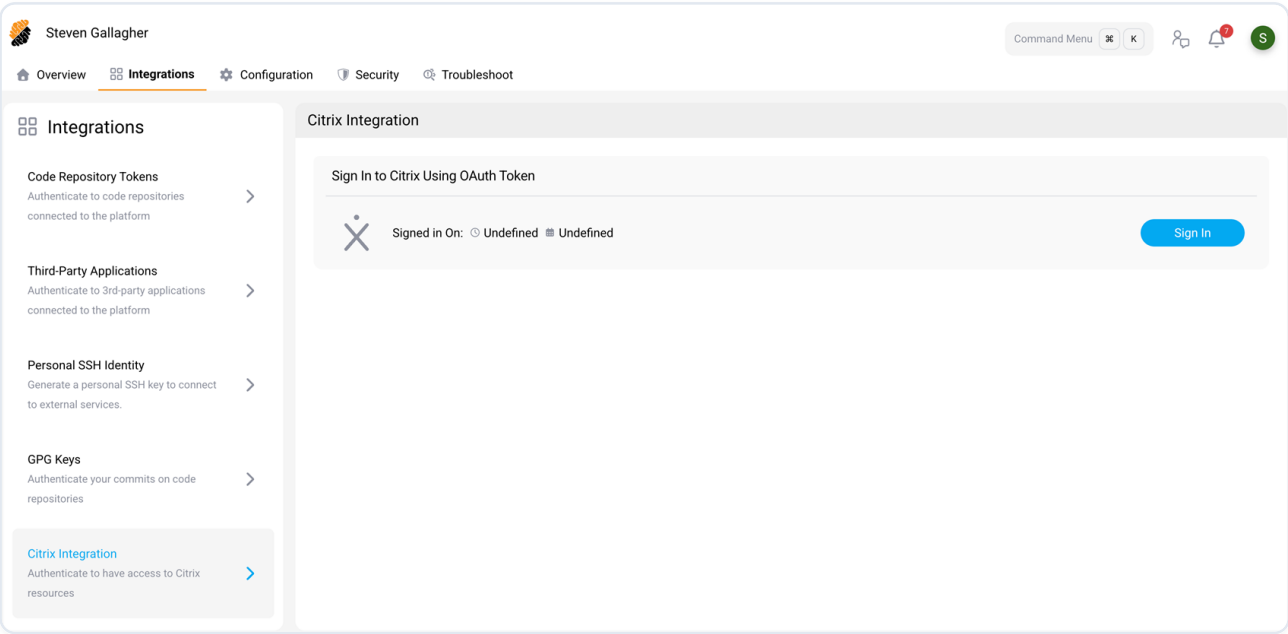
Puede generar e implementar automáticamente claves GPG para autenticar sus confirmaciones en aplicaciones de repositorio Git compatibles (es decir, GitHub).



Integración de Citrix

La sección **Integración de Citrix** de la página Integraciones le permite iniciar sesión en su cuenta de Citrix para acceder a las aplicaciones y escritorios virtuales de Citrix DaaS directamente desde la consola de SecurSpaces. Después de iniciar sesión, sus recursos de Citrix asignados aparecerán en la página de Resumen del proyecto.

Esta sección está disponible en **Perfil > Integraciones > Integración de Citrix**.



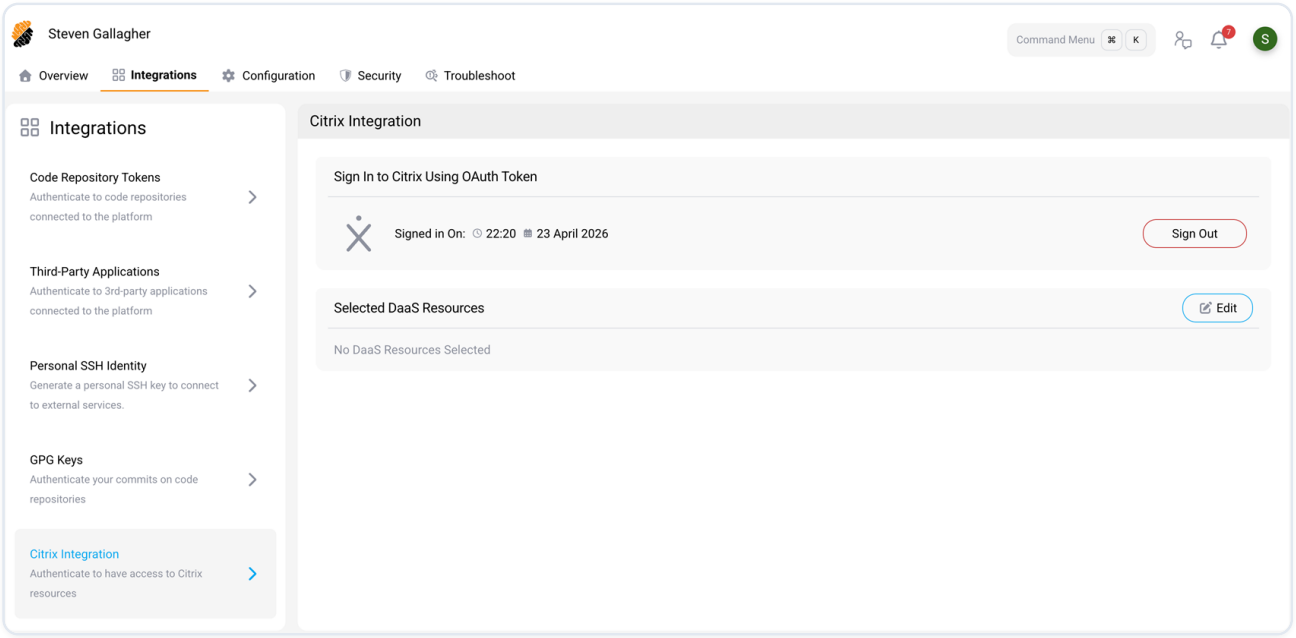
Requisitos previos

- El administrador de su plataforma SecurSpaces debe configurar primero la integración de Citrix DaaS en **Configuración del sistema > Integraciones > Integración de Citrix DaaS**. Consulte Integración de Citrix DaaS.
- Necesita una cuenta de Citrix Workspace con aplicaciones o escritorios virtuales asignados a usted.

Iniciar sesión en Citrix

1. Vaya a **Perfil > Integraciones**.
2. En la barra lateral izquierda, seleccione **Integración de Citrix**.
3. En **Iniciar sesión en Citrix con token OAuth**, seleccione **Iniciar sesión**.
4. Complete la autenticación en el cuadro de diálogo de inicio de sesión de Citrix Workspace que se abre.

Después de iniciar sesión, la página muestra la marca de tiempo de su inicio de sesión y un botón de **Cerrar sesión**.



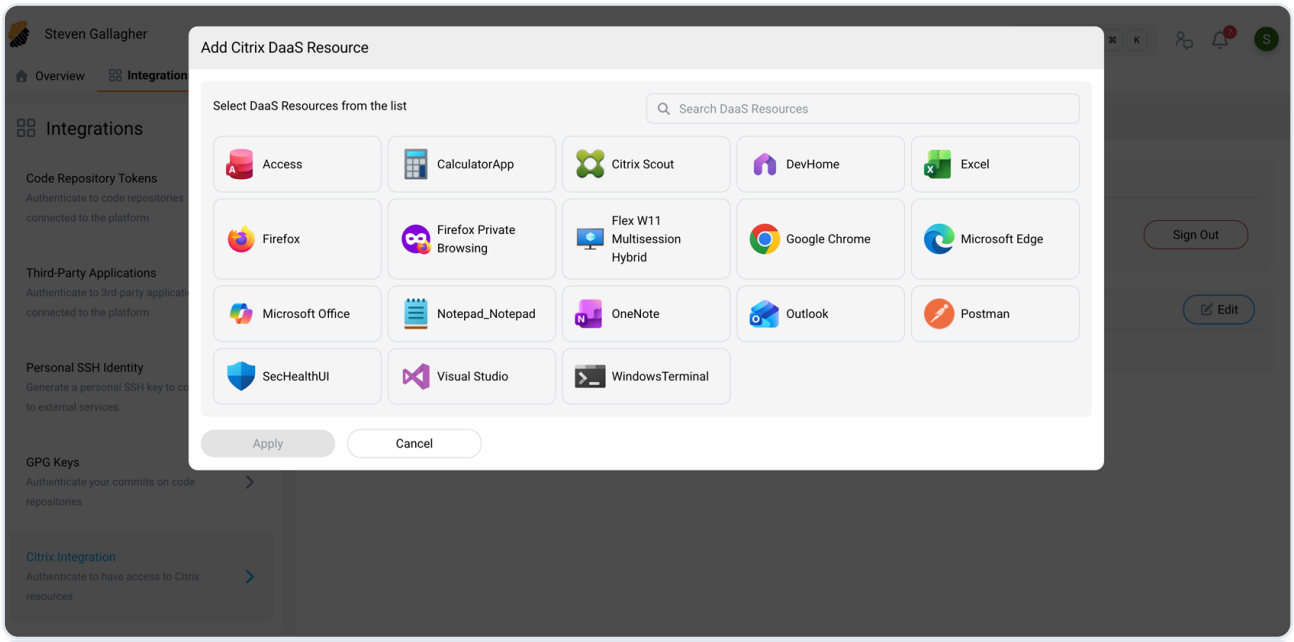
Seleccionar recursos de DaaS

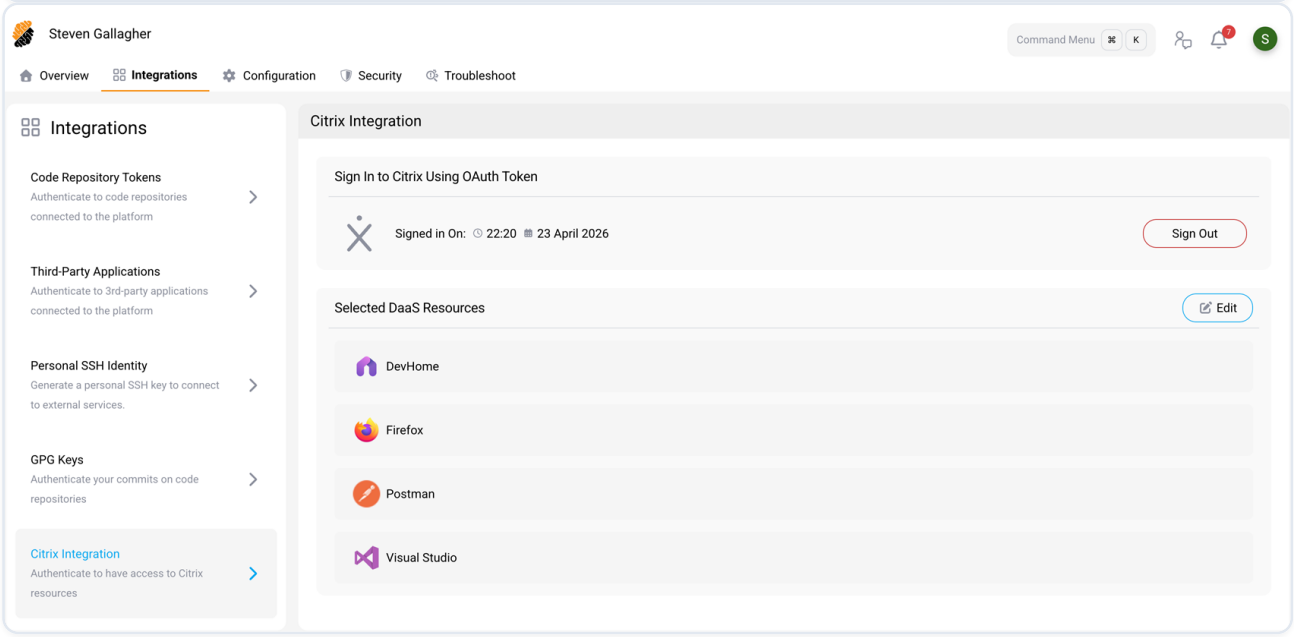
Después de iniciar sesión, aparece una sección de **Recursos de DaaS seleccionados** debajo del área de inicio de sesión. Utilice esta sección para elegir a qué aplicaciones y escritorios virtuales de Citrix desea acceder desde la consola de SecurSpaces.

1. Seleccione **Editar** junto a **Recursos de DaaS seleccionados**.

2. En el cuadro de diálogo **Agregar recurso de Citrix DaaS**, explore o busque los recursos disponibles.
3. Seleccione uno o más recursos de la lista.
4. Seleccione **Aplicar**.

Los recursos seleccionados aparecen ahora en **Recursos de DaaS seleccionados** en esta página y en la sección **Recursos de Citrix DaaS** de la página de Resumen del proyecto.





Iniciar recursos de Citrix

Después de seleccionar los recursos, estos aparecen en la página de Información general del proyecto en **Recursos de Citrix DaaS**. Seleccione un recurso para iniciarlo. Consulte Recursos de Citrix DaaS.

Cerrar sesión

Para desconectar su cuenta de Citrix, vuelva a **Perfil > Integraciones > Integración de Citrix** y seleccione **Cerrar sesión**. Sus recursos de Citrix DaaS seleccionados ya no aparecerán en la página de Información general del proyecto.

Información relacionada

- Configuración
- Información general
- Seguridad
- Su perfil

Configuration

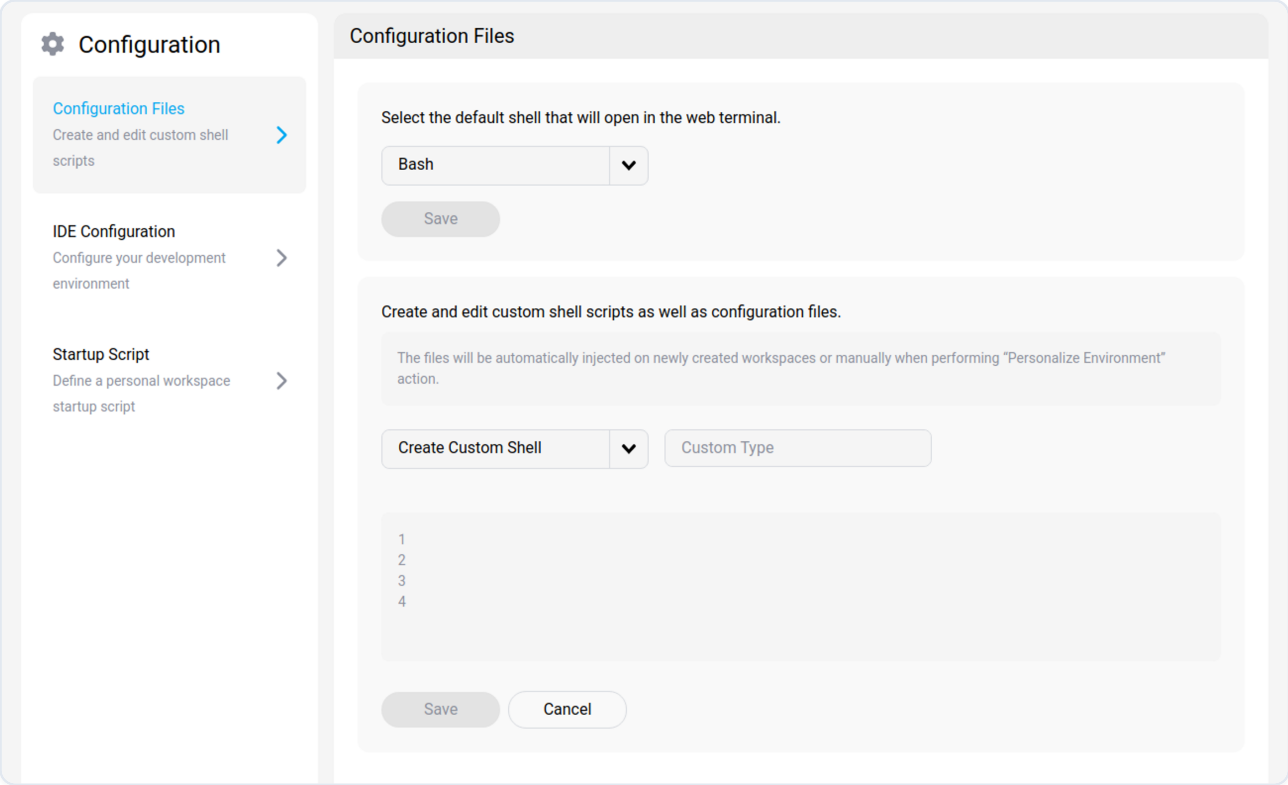
La **página de configuración** se utiliza para crear y editar scripts de shell personalizados y archivos de configuración, configurar su IDE y definir scripts de inicio de espacio de trabajo personales. También puede configurar ajustes adicionales (por ejemplo, tema) haciendo clic en la imagen de perfil en la parte superior derecha de la pantalla.

- Administrar archivos de configuración
- Archivos dot
- Configuración del IDE
- Script de inicio
- Tema
- Idioma

Administrar archivos de configuración

Utilice la sección de **Archivos de configuración** para personalizar su entorno de desarrollo. Puede especificar su shell predeterminado preferido y crear scripts de configuración personalizados (como .bashrc o .zshrc) que se apliquen automáticamente a sus espacios de trabajo.

Esto garantiza que cada nuevo espacio de trabajo que cree incluya sus alias preferidos, variables de entorno y configuraciones de herramientas sin necesidad de una configuración manual cada vez.



Establecer el shell predeterminado

Puede definir qué shell se inicia automáticamente cuando abre un terminal web en su espacio de trabajo.

1. Vaya a **Configuración > Archivos de configuración**.
2. En **Seleccionar el shell predeterminado que se abrirá en el terminal web**, seleccione el menú desplegable.
3. Elija su shell preferido (por ejemplo, **Bash**).
4. Seleccione **Guardar**.

Crear y editar archivos de configuración personalizados

Puede crear scripts de shell y archivos de configuración personalizados para mantener la persistencia de la configuración de su entorno. Estos archivos se inyectan automáticamente en:

- **Espacios de trabajo recién creados**: Los archivos se aplican durante el proceso de creación del espacio de trabajo.
- **Espacios de trabajo existentes**: Puede aplicar actualizaciones manualmente seleccionando la acción **Personalizar entorno** dentro de un espacio de trabajo.

PARA CREAR UN NUEVO ARCHIVO DE CONFIGURACIÓN

1. Vaya a la sección **Archivos de configuración**.

2. En el área **Crear y editar scripts de shell personalizados**, seleccione el menú desplegable **Crear shell personalizado**.
3. Seleccione el tipo de archivo que desea configurar (por ejemplo, **Bash Shell** o **Zsh Shell**).
    - Si selecciona **Tipo personalizado**, introduzca el nombre de archivo específico en el campo adyacente.
4. Introduzca su script o código de configuración en el panel del editor.
5. Seleccione **Guardar**.

Configuraciones de ejemplo

Puede copiar y pegar los siguientes ejemplos en su archivo **.bashrc** para mejorar la productividad y la seguridad.

MEJORAR LA NAVEGACIÓN POR DIRECTORIOS

Utilice estos alias para listar archivos con más detalle (incluidos archivos ocultos y tamaños de archivo) y para navegar por las carpetas rápidamente.

```
# List all files including hidden ones

alias ll='ls -alF'

alias la='ls -A'



# Go back one or two directories

alias ..='cd ..'

alias ...='cd ../..'
```

EVITAR ELIMINACIONES ACCIDENTALES

Añada avisos de seguridad a los comandos críticos para asegurarse de que confirma antes de eliminar o sobrescribir archivos.

```
# Ask for confirmation before executing

alias rm='rm -i'

alias cp='cp -i'
```

```
alias mv='mv -i'
```

CONFIGURAR ACCESOS DIRECTOS DE GIT

Reduzca la escritura repetitiva para operaciones comunes de Git.

```
# Check status

alias gs='git status'



# Add all changes

alias ga='git add .'



# Commit with a message

alias gc='git commit -m'



# Push changes

alias gp='git push'
```

Archivos dot

Utilice los **archivos dot** para aplicar su configuración personal de shell, editor y herramientas a los espacios de trabajo de Citrix SecurSpaces™ espacios de trabajo. Conecte un repositorio de Git una vez, y SecurSpaces lo clona en `~/.dotfiles` en cada espacio de trabajo seleccionado.

Los archivos dot son una configuración por usuario. Utiliza su integración de Git conectada y afecta solo a los espacios de trabajo que usted posee.

Antes de empezar

Antes de configurar los dot files, asegúrese de que:

- Su repositorio de archivos dot está disponible a través de GitHub, GitLab, Bitbucket, Azure DevOps o Azure DevOps con Entra ID.

- Ha conectado el proveedor de Git correspondiente en **Perfil > Integración**.
- Su repositorio incluye uno de los scripts de instalación compatibles.

SecurSpaces busca el primer script de instalación que exista en este orden:

1. `install.sh`
2. `install`
3. `bootstrap.sh`
4. `bootstrap`
5. `setup.sh`
6. `setup`
7. `script/bootstrap`
8. `script/setup`

Si el archivo es ejecutable, SecurSpaces lo ejecuta directamente. De lo contrario, SecurSpaces lo ejecuta con `bash`.

Configurar archivos dot

1. Vaya a **Perfil > Configuración > Archivos dot**.
2. Seleccione la **Integración del repositorio de código** que pueda acceder a su repositorio de archivos dot.
3. Introduzca la **URL del repositorio de archivos dot**, o seleccione **Examinar repositorios** y elija el repositorio.
4. Seleccione el **Tiempo de espera del script de instalación**. El tiempo de espera puede ser de 1 a 10 minutos.
5. En **Aplicar archivos dot a**, seleccione una de las siguientes opciones:
    - **Todos mis espacios de trabajo** — Aplica los archivos dot a cada espacio de trabajo que poseas.
    - **Solo espacios de trabajo seleccionados** — Aplica los archivos dot solo a los espacios de trabajo que selecciones.
6. Selecciona **Guardar cambios**.

Resultado esperado: La próxima vez que un espacio de trabajo incluido se inicie o reanude, SecurSpaces clona el repositorio en `~/.dotfiles` y ejecuta el script de instalación.

Aplicar archivos dot a un espacio de trabajo existente

Para volver a aplicar los archivos dot sin esperar a que se reinicie un espacio de trabajo:

1. Abre el menú de acciones del espacio de trabajo.
2. Selecciona **Personalizar entorno**.

Resultado esperado: SecurSpaces ejecuta el script de instalación de los archivos dot de nuevo. Utiliza esta acción después de cambiar tu repositorio de archivos dot o después de actualizar la configuración de los archivos dot.

Revisar la salida de los archivos dot

La salida de los archivos dot aparece en los registros de inicio del espacio de trabajo bajo **Aplicando archivos dot**. El registro muestra la salida de clonación, la salida del script y el código de salida del script.

Los archivos dot no bloquean el inicio del espacio de trabajo. Si el repositorio no se puede clonar, no se encuentra ningún script de instalación, el script sale con un error o el tiempo de espera expira, SecurSpaces registra el resultado en los registros y continúa iniciando el espacio de trabajo.

Cambiar o eliminar archivos dot

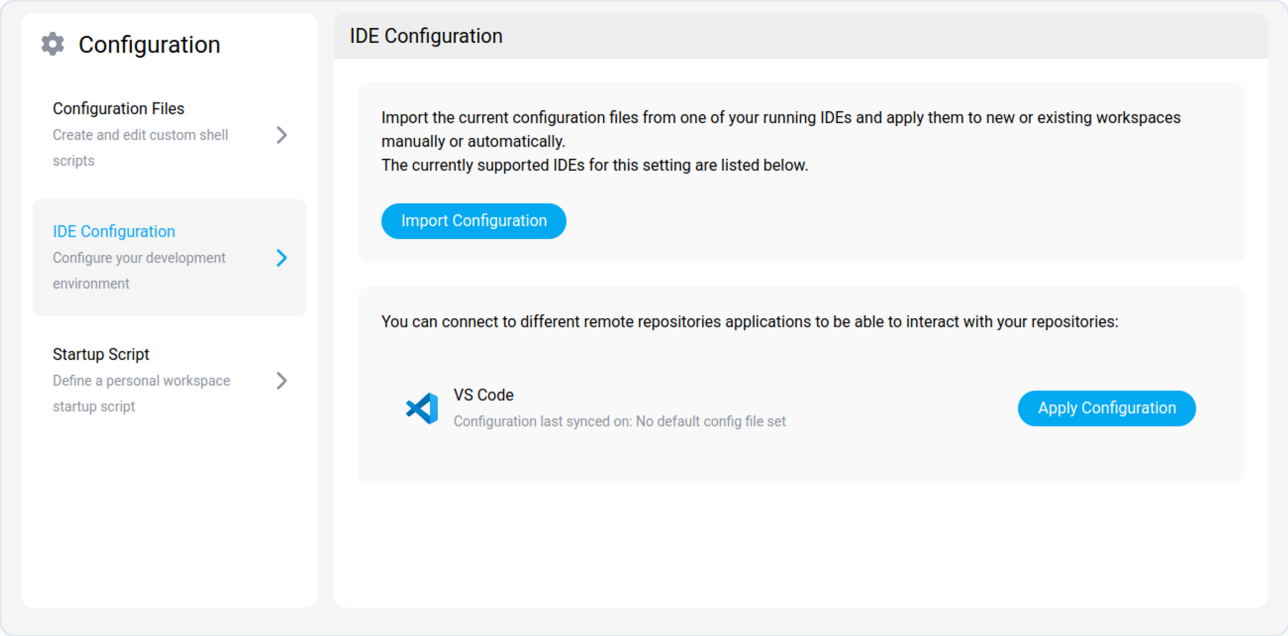
Puedes actualizar o eliminar tu configuración de archivos dot en cualquier momento:

- Para usar un repositorio diferente, actualiza la **URL del repositorio de archivos dot** y selecciona **Guardar cambios**.
- Para dejar de aplicar los archivos dot, seleccione **Eliminar configuración de archivos dot**.
- Para limitar dónde se ejecutan los archivos dot, elija **Solo espacios de trabajo seleccionados** y seleccione los espacios de trabajo a incluir.

La eliminación de la configuración detiene futuras ejecuciones de archivos dot. No elimina un directorio `~/.dotfiles` existente de ningún espacio de trabajo.

Configuración del IDE

Los archivos de configuración del IDE se pueden gestionar desde la **configuración del perfil**. Una configuración debe importarse inicialmente desde un espacio de trabajo **en ejecución**. Luego, se puede aplicar a espacios de trabajo nuevos o existentes de forma manual o automática.



Los IDEs actualmente compatibles son:

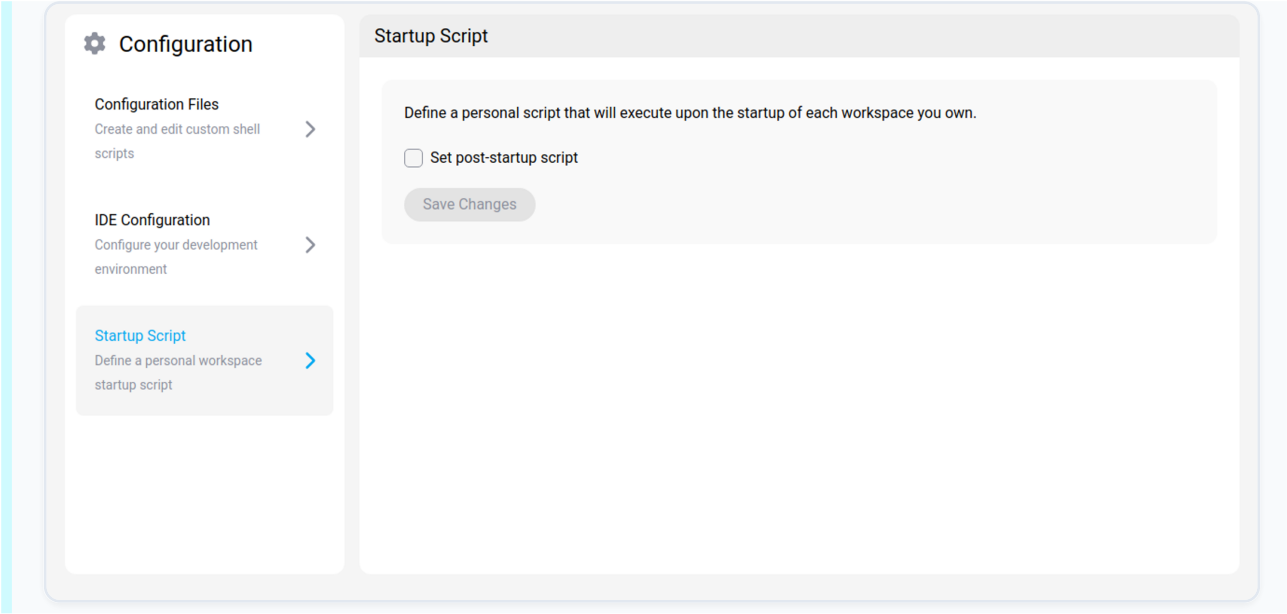
- **VSCode**,
- **cualquier IDE de Jetbrains**.

Script de inicio

Puede definir un script personal que se ejecutará en cada inicio de los espacios de trabajo de su propiedad. Para scripts configurados en un espacio de trabajo individual, consulte Scripts de inicio.

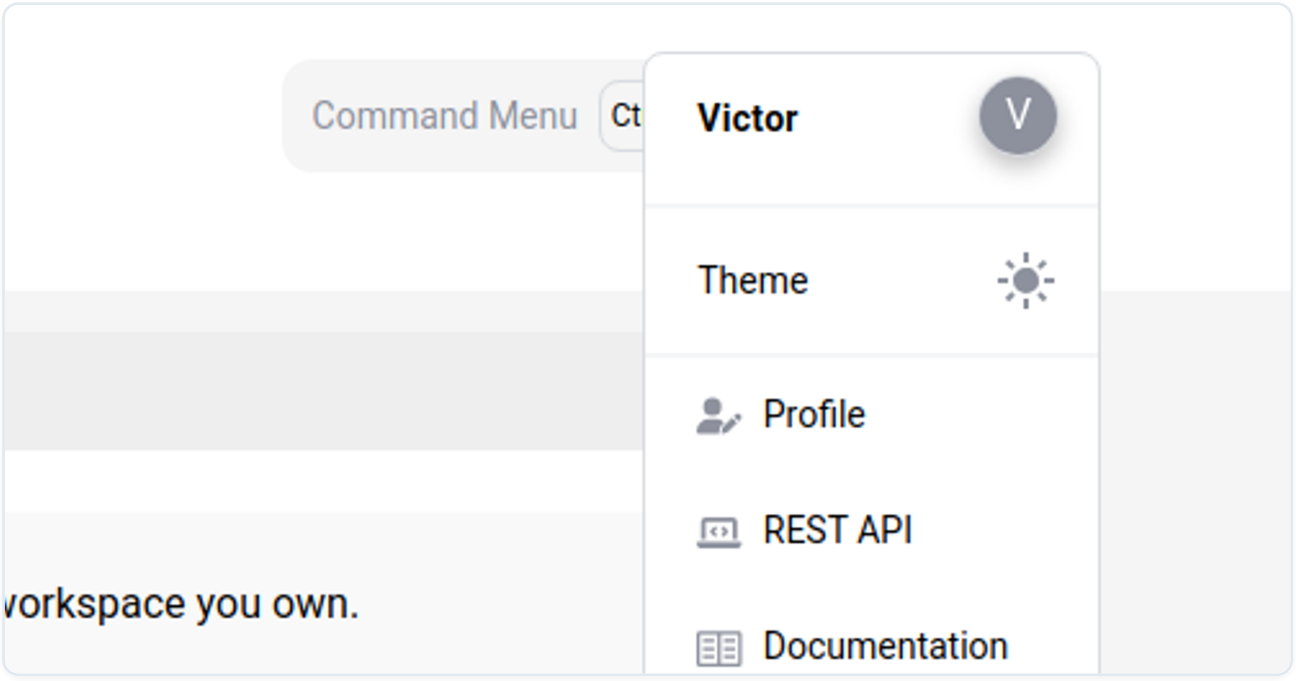
> Consejo:

> Tenga en cuenta que si definió un script de inicio para un espacio de trabajo determinado, este anulará el actual.



Tema

Hay dos temas de color para los paneles disponibles en el **Menú de perfil**. Puede alternar entre un tema **claro** y **oscuro** para la visualización de la Interfaz de Usuario (UI).



Idioma

Se puede seleccionar un idioma para la UI desde el pie de página. Los idiomas admitidos para la UI de la plataforma son:

- **Inglés**,
- **Francés**.

Información relacionada

- Integraciones
- Descripción general
- Seguridad
- Su perfil

Security

La página de **Seguridad** de su perfil es donde gestiona las claves, secretos y tokens vinculados a su cuenta de usuario, y donde revisa qué tiene acceso a su cuenta.

Gestionarlos en un solo lugar facilita ver qué existe, para qué sirve, y revocarlo o reemplazarlo.

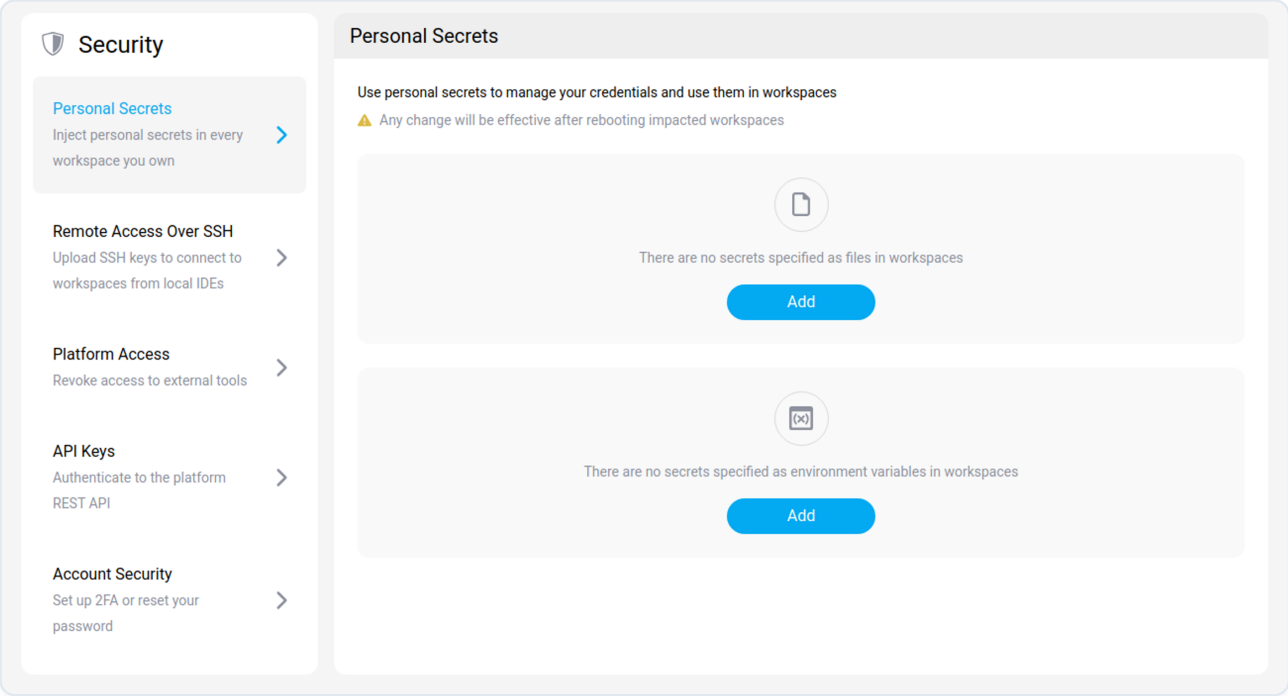
SECCIÓN	PARA QUÉ SIRVE	SE MUESTRA CUANDO
Secretos personales	Inyectar secretos personales en cada espacio de trabajo de su propiedad	Siempre
Acceso remoto a través de SSH	Subir claves SSH para conectarse a espacios de trabajo desde IDEs locales	SSH a los espacios de trabajo está habilitado para usted y permitido a nivel de plataforma
Acceso a la plataforma	Revocar acceso otorgado a herramientas externas	Siempre
Claves de API	Autenticarse en la API REST de SecurSpaces	La API REST está habilitada
Seguridad de la cuenta	Configurar la autenticación de dos factores o restablecer su contraseña	Tiene la autenticación de dos factores habilitada, o inicia sesión con una cuenta local en lugar de un proveedor de identidad

Nota:

> Las claves GPG no están en esta página. Las gestiona en Integración, junto con sus tokens de repositorio y su identidad SSH personal, porque se utilizan para firmar confirmaciones en su proveedor de Git.

Secretos personales

En **Secretos personales**, gestiona los secretos que se inyectan en cada espacio de trabajo de su propiedad. Puede añadir un secreto como archivo en el espacio de trabajo o como variable de entorno.



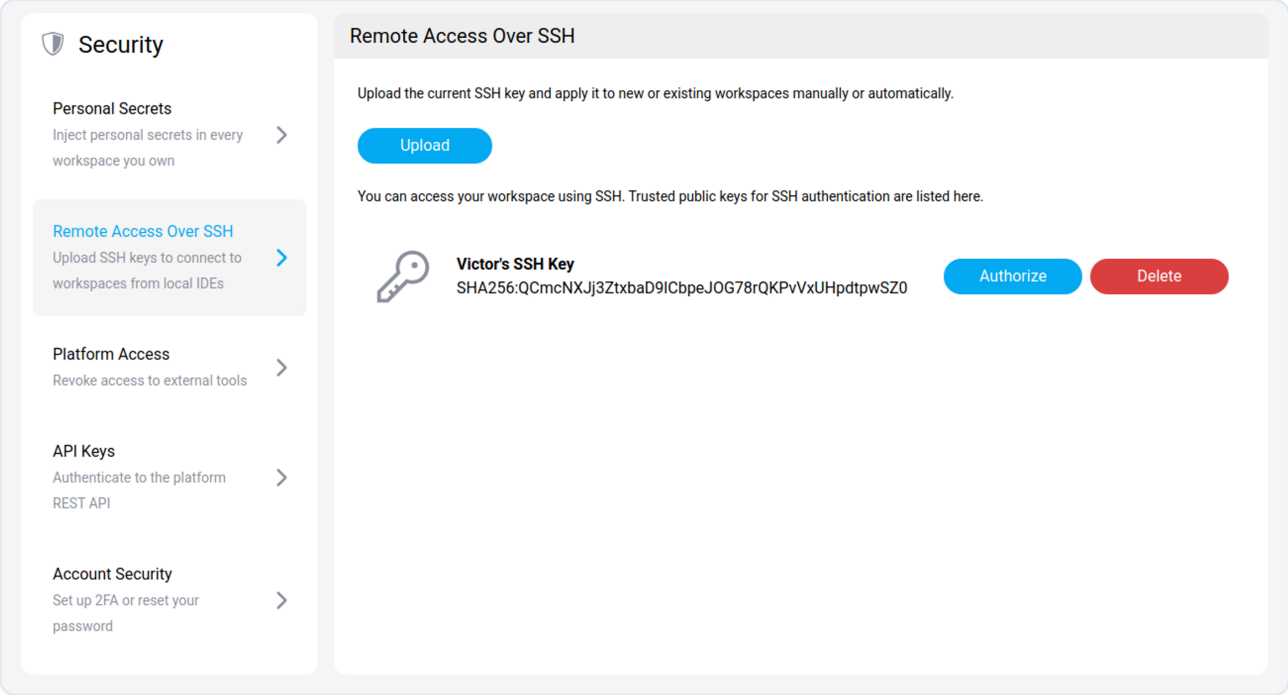
Acceso remoto a través de SSH

Las claves públicas de confianza para la autenticación SSH se enumeran aquí, cada una vinculada a su perfil. Suba una clave para conectarse a un espacio de trabajo desde un IDE local.

Un registro caduca después de un período establecido por el administrador de su plataforma, 7 días por defecto. Las integraciones de IDE de SecurSpaces lo renuevan por usted; con cualquier otro cliente SSH, debe volver a registrar la clave usted mismo. Consulte Caducidad y renovación de claves.

Ejecutar su IDE localmente a través de SSH le permite mantener su configuración local familiar mientras el código y el cómputo permanecen en el espacio de trabajo remoto. Para configurarlo, consulte Conectarse a través de SSH.

Esta sección aparece solo cuando SSH a los espacios de trabajo está habilitado para su cuenta y permitido a nivel de plataforma. Si no puede verla, pregunte a un administrador de plataforma si el desarrollo remoto a través de SSH está activado.



Acceso a la plataforma

Acceso a la plataforma enumera las herramientas externas a las que ha concedido acceso a su cuenta de SecurSpaces y le permite revocar dicho acceso.

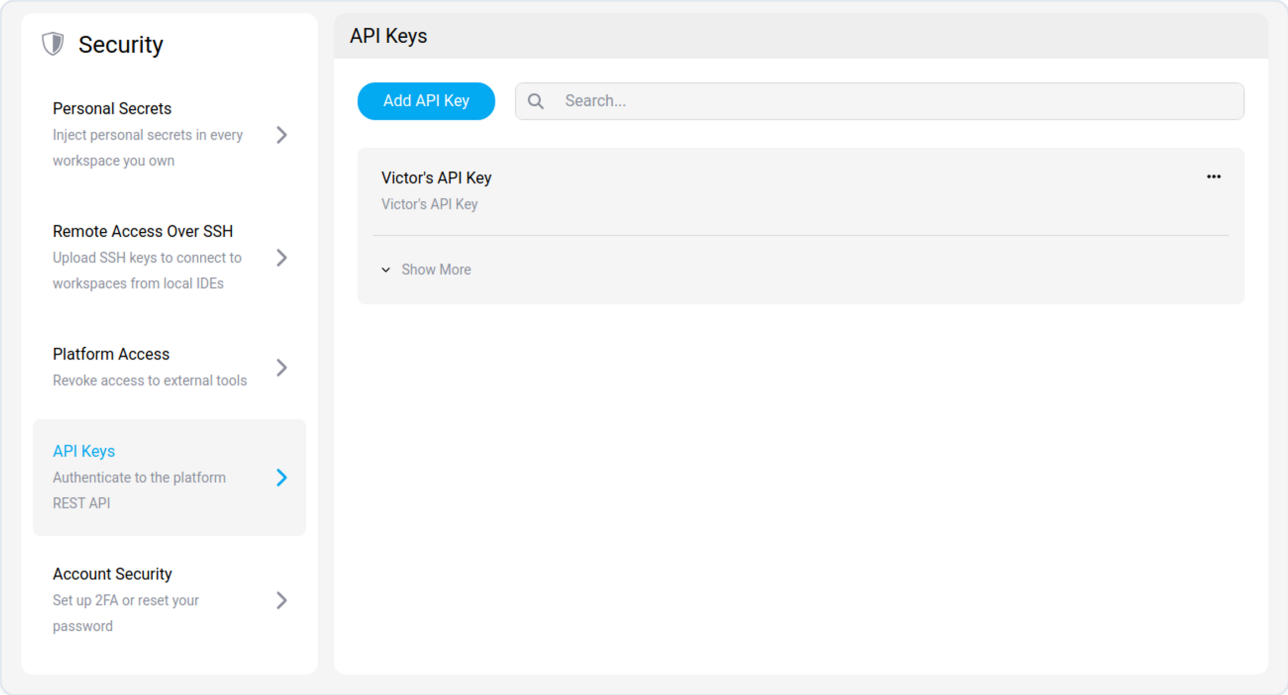
La extensión del IDE aparece aquí después de iniciar sesión desde un IDE local. Revocar una entrada finaliza el acceso de esa herramienta y debe autorizarse de nuevo antes de poder utilizarse.

Claves de API

Una **clave de API** le autentica en la API REST de SecurSpaces. Utilícela cuando un script o un sistema externo necesite llamar a la API en su nombre.

Una clave de API lleva su identidad, así que trátela como una contraseña: manténgala en secreto y revóquela aquí si está expuesta o ya no es necesaria.

Esta sección aparece solo cuando la API REST está habilitada para su cuenta.



Seguridad de la cuenta

Seguridad de la cuenta es donde configura la autenticación de dos factores o restablece su contraseña.

Aparece solo si ya tiene la autenticación de dos factores habilitada, o si inicia sesión con una cuenta local de SecurSpaces. Si su organización utiliza un proveedor de identidad como SAML u OIDC, su contraseña y la autenticación multifactor se gestionan allí en su lugar, y esta sección no se muestra.

Información relacionada

- Integración — tokens de repositorio, identidad SSH personal y claves GPG
- Conectar a través de SSH
- API REST

Persistent Docker

Información general

Docker persistente permite a los desarrolladores mantener las imágenes de Docker descargadas en el volumen persistente de su espacio de trabajo. Con la función habilitada, las imágenes que un desarrollador descarga dentro de un espacio de trabajo se almacenan en caché en `/home/`

`developer/` y permanecen disponibles después de que el espacio de trabajo se pause, reinicie o actualice.

Sin Docker persistente, la raíz de datos de Docker reside en el sistema de archivos raíz efímero del espacio de trabajo. Cada vez que se recrea el contenedor del espacio de trabajo —al pausar/reanudar, reiniciar o actualizar la imagen—, la caché de imágenes de Docker se descarta y cualquier imagen a la que hagan referencia las herramientas del desarrollador debe descargarse y descomprimirse de nuevo.

Para comprobar cuál se aplica a un espacio de trabajo, ejecuta `docker info` y busca **Docker Root Dir**. Una ruta bajo `/home/developer` significa que Docker persistente está activo para ti.

¿Qué problema resuelve?

Descargar imágenes en cada inicio del espacio de trabajo puede dominar el tiempo de arranque, especialmente cuando:

- El flujo de trabajo de un desarrollador depende de varias imágenes grandes (bases de datos, navegadores para pruebas de extremo a extremo, cadenas de herramientas de lenguaje, ejecutores de CI).
- Las imágenes tienen muchas capas y el espacio de trabajo está configurado con solo una o dos CPU, por lo que las capas solo se pueden descomprimir secuencialmente.
- El registro limita la tasa o restringe las descargas (por ejemplo, los límites de Docker Hub público por IP o por organización).
- El clúster tiene una salida limitada o medida al registro.

En entornos donde se descargan varias imágenes por sesión, el coste puede ser significativo: un espacio de trabajo que tarda segundos en reanudarse aún puede dejar al desarrollador esperando más de 20 minutos antes de que sus herramientas sean utilizables.

Docker persistente elimina el trabajo redundante de descarga y descompresión después de la primera vez que se utiliza una imagen. El espacio de trabajo en sí sigue iniciándose en la misma cantidad de tiempo; lo que mejora es el **tiempo hasta la productividad**, es decir, cuánto tiempo pasa hasta que las herramientas basadas en Docker del desarrollador están realmente listas.

> **Nota:**

> Docker persistente almacena en caché **imágenes**, no el estado del contenedor. Los datos escritos dentro de un contenedor en ejecución se descartan cuando se elimina el

> contenedor. Para persistir los datos producidos por un contenedor (un archivo de base de datos, estado de la aplicación, artefactos generados), monta un directorio bajo `/home/developer/` en el contenedor como un volumen de Docker. Consulta Qué persiste en un espacio de trabajo de SecurSpaces.

Cómo obtener acceso

Persistent Docker está restringido por un indicador de función de licencia. Por defecto, el indicador no está habilitado en las licencias de los clientes.

Para solicitar acceso:

1. Póngase en contacto con el Soporte de Citrix o con su equipo de cuentas y solicite que se habilite **Persistent Docker** en su licencia de Citrix SecurSpaces™.
2. Citrix habilita el indicador de función en el registro de licencia de su dominio.
3. Un administrador de plataforma en su entorno de SecurSpaces actualiza la licencia para que se detecte el nuevo indicador:
   - **Licencia en línea** — Abra la consola de administración de SecurSpaces, vaya a **Configuración del sistema** → **Licencia** y seleccione **Cargar nueva licencia** → **Licencia en línea**. La licencia actualizada incluye el indicador de función Persistent Docker.
   - **Licencia aislada (archivo)** — Citrix proporciona un nuevo archivo de licencia. Cárguelo en **Configuración del sistema** → **Licencia** → **Cargar nueva licencia**.

Después de la actualización de la licencia, **Persistent Docker** aparece como una nueva entrada en la lista de indicadores de función de la plataforma, junto con otras funciones restringidas, como el **Soporte de GPU**.

Configurar Persistent Docker en SecurSpaces

Una vez que el indicador de función sea visible en su entorno, un administrador de plataforma controla quién puede usarlo.

Habilitar el indicador de función

1. Inicie sesión en la consola de administración de SecurSpaces como **administrador de plataforma**.
2. Vaya a **Configuración del sistema** → **Funciones de la plataforma**.
3. Localice **Persistent Docker** en la lista de indicadores de función.

4. Elija el ámbito de implementación:
    - **Habilitado** — Todos los desarrolladores de la plataforma obtienen Persistent Docker.
    - **Habilitado para usuarios seleccionados** — Solo los usuarios, dominios o grupos que especifique obtienen Persistent Docker. Añada entradas en **Usuarios**, **Dominios** y **Grupos** según sea necesario.
5. Guarde la configuración.

Aplicar el cambio a los espacios de trabajo en ejecución

La característica se aplica al inicio del espacio de trabajo. Un desarrollador con un espacio de trabajo que ya estaba en ejecución cuando se habilitó la bandera debe hacer una de las siguientes acciones para empezar a almacenar imágenes en caché:

- Pausar y reanudar el espacio de trabajo, **o**
- Reiniciar el espacio de trabajo, **o**
- Actualizar el espacio de trabajo.

Los nuevos espacios de trabajo creados después de habilitar la bandera utilizan Persistent Docker automáticamente.

Planificar el uso adicional del volumen persistente

Persistent Docker almacena las capas de imágenes en el volumen persistente del espacio de trabajo. Dado que los desarrolladores suelen depender de múltiples imágenes —y a menudo de múltiples versiones de la misma imagen—, el volumen persistente se llena considerablemente más rápido que sin esta característica.

Antes de habilitar Persistent Docker de forma generalizada, revise las especificaciones de su espacio de trabajo:

1. Vaya a **Configuración del sistema** → **Especificaciones del espacio de trabajo**.
2. O bien:
    - Aumente el tamaño de disco predeterminado en las especificaciones utilizadas por los desarrolladores que obtendrán Persistent Docker, **o**
    - Habilite **Permitir a los usuarios aumentar el almacenamiento** en esas especificaciones para que los desarrolladores puedan ajustar el tamaño de su volumen persistente a medida que crece su caché de imágenes.

Si el volumen persistente de un desarrollador se llena, las extracciones de imágenes y otras operaciones del espacio de trabajo comenzarán a fallar. Planifique el margen de maniobra en consecuencia.

verificar que Docker persistente está activo

Un desarrollador puede confirmar que la caché persiste entre reinicios:

1. Abra un terminal del espacio de trabajo.
2. Extraiga o ejecute una imagen, por ejemplo:

   ```
   docker pull postgres:16

   docker images
   ```

3. Confirme que la imagen aparece en la lista mediante `docker images`.
4. Pause y reanude el espacio de trabajo.
5. Abra un terminal de nuevo y ejecute:

   ```
   docker images
   ```

   Resultado esperado: La imagen `postgres:16` sigue apareciendo en la lista sin necesidad de volver a extraerla.

Si la caché está vacía después de un reinicio, Docker persistente no está activo para ese desarrollador. Confirme con un administrador de la plataforma que la característica está habilitada y que el desarrollador está dentro del ámbito (usuario, dominio o grupo).

Cómo persistir datos de contenedores (volúmenes de Docker)

Docker persistente solo almacena imágenes en caché. Cualquier cosa que un contenedor escriba en su propio sistema de archivos se pierde cuando se elimina el contenedor. Este es el comportamiento estándar de Docker; SecurSpaces no lo cambia.

Para persistir los datos producidos por un contenedor, monte una carpeta de `/home/developer/` en el contenedor como un volumen. Por ejemplo, para ejecutar Postgres con su directorio de datos respaldado por su volumen persistente:

```
mkdir -p ~/postgres-data

docker run -d \

  --name pg \

  -e POSTGRES_PASSWORD=secret \

  -v ~/postgres-data:/var/lib/postgresql/data \

  postgres:16
```

Los archivos de la base de datos residen en `~/postgres-data`, que está en el volumen persistente, por lo que sobreviven a los reinicios del espacio de trabajo. Utilice el mismo patrón para cualquier otro contenedor con estado: identifique la ruta en la que escribe la aplicación y monte un directorio de `/home/developer/` en esa ruta.

Para una descripción completa de lo que persiste entre reinicios del espacio de trabajo, consulte Qué persiste en un espacio de trabajo de SecurSpaces.

Referencias

- Qué persiste en un espacio de trabajo de SecurSpaces
- Desarrollar en un espacio de trabajo
- Especificaciones del espacio de trabajo
- Imagen de espacio de trabajo personalizada

Run a graphical desktop in a workspace with the Debian GUI image

Algunos flujos de trabajo necesitan más que un IDE y un terminal basados en navegador. Cuando tienes que ejecutar herramientas basadas en GUI, diseñar aplicaciones o probar la interfaz gráfica de una aplicación, puedes usar la imagen de contenedor GUI de Debian de ejemplo proporcionada por Citrix Citrix SecurSpaces™. Esta imagen incluye un escritorio XFCE preconfigurado al que accedes directamente en tu navegador a través de noVNC.

Esta guía explica cómo hacer que la imagen GUI de Debian esté disponible en tu plataforma y cómo abrir su escritorio desde un espacio de trabajo.

Cómo funciona

La imagen GUI de Debian es una imagen CDE image (imagen de contenedor) estándar de SecurSpaces que añade:

- Un entorno de escritorio **XFCE**.
- Un servidor **TigerVNC** y el cliente **noVNC**, que transmite el escritorio a tu navegador a través del puerto **8081**.
- Un script de inicio, `/usr/bin/strong_network_startup/xstartup/initialize_workspace.sh`, que inicia el servidor VNC y la sesión de escritorio.

Expones el puerto 8081 a tu navegador usando un **Elemento de Acceso Personalizado** o una **Aplicación de Espacio de Trabajo**, y luego ejecutas el script de inicio para lanzar el escritorio.

Requisitos previos

Antes de empezar, asegúrate de tener:

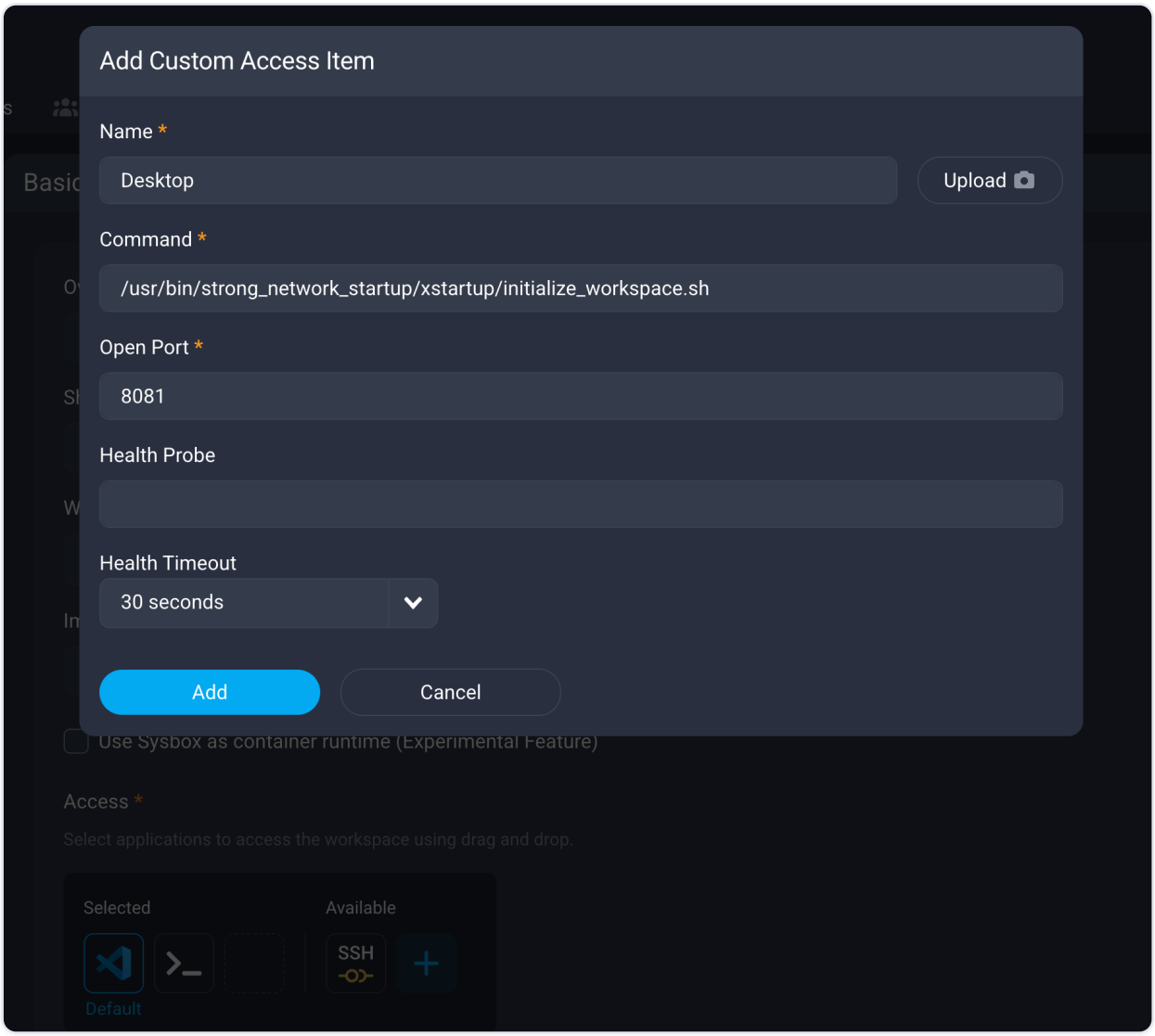
- La imagen GUI de Debian de ejemplo disponible para tu equipo. La imagen de referencia y `Dockerfile` se publican en el repositorio de imágenes de Citrix en GitHub. Compílala y súbela a un registro al que tu plataforma pueda acceder, o usa una imagen precompilada si tu administrador te proporciona una.
- La imagen añadida como imagen CDE image en los recursos de tu plataforma, organización o proyecto. Esta acción requiere que el permiso de Seguridad esté configurado en **Administrar**.
- Permiso para crear o editar un espacio de trabajo o plantilla de espacio de trabajo template que utilice la imagen.

Abrir el escritorio con un Elemento de Acceso Personalizado

Usa un Elemento de Acceso Personalizado cuando quieras que el escritorio aparezca como una opción de conexión de un solo clic en el espacio de trabajo, junto a VS Code y Terminal.

1. Cree o edite un espacio de trabajo que utilice la imagen GUI de Debian.
2. En el asistente del espacio de trabajo, vaya a **Información básica** y abra el menú **Acceso**.
3. Haga clic en **Añadir** para abrir el cuadro de diálogo **Añadir elemento de acceso personalizado** e introduzca lo siguiente:
   - **Nombre** — Un nombre para mostrar de su elección, por ejemplo `Desktop`.
   - **Puerto** — `8081`. Este es el puerto donde se ejecuta noVNC.

- **Comando** — `/usr/bin/strong_network_startup/xstartup/initialize_workspace.sh`



4. Guarde el asistente e inicie el espacio de trabajo.
5. Abra el escritorio haciendo clic en el elemento de acceso que creó.

Resultado esperado: El escritorio XFCE se abre en su navegador a través de noVNC.

Abrir el escritorio con una aplicación de espacio de trabajo

Utilice una aplicación de espacio de trabajo cuando prefiera iniciar el escritorio manualmente desde la terminal, o cuando desee reutilizar un flujo de trabajo existente basado en aplicaciones.

1. Cree un espacio de trabajo que utilice la imagen GUI de Debian.
2. Exponga el puerto **8081** como una aplicación de espacio de trabajo. Para obtener más detalles, consulte Crear una aplicación de espacio de trabajo.
3. Inicie el espacio de trabajo, abra la terminal y ejecute el script de inicio:

```
/usr/bin/strong_network_startup/xstartup/initialize_workspace.sh
```

4. Abra la aplicación del espacio de trabajo.

Resultado esperado: El escritorio XFCE se abre en la aplicación del espacio de trabajo.

Iniciar el escritorio automáticamente

Para evitar ejecutar el comando manualmente cada vez, automatice los pasos anteriores:

1. Añada el comando de inicio al script de inicio del espacio de trabajo para que el escritorio se inicie cada vez que se inicie el espacio de trabajo:

```
/usr/bin/strong_network_startup/xstartup/initialize_workspace.sh
```

2. Cree una plantilla de espacio de trabajo que utilice la imagen GUI de Debian y que ya exponga el puerto 8081 como una aplicación de espacio de trabajo.

Los espacios de trabajo creados a partir de esta plantilla se inician con el escritorio listo para usar, con ninguna configuración manual.

Solución de problemas

- **El escritorio no se carga** — Confirme que el puerto **8081** está expuesto (como un elemento de acceso personalizado o una aplicación de espacio de trabajo) y que el script de inicio se ha ejecutado. Con un elemento de acceso personalizado, el script se ejecuta automáticamente; con una aplicación de espacio de trabajo, ejecútelo manualmente a menos que forme parte del script de inicio.
- **Copiar y pegar del portapapeles no funciona** — La imagen instala `autocutsel` para la compatibilidad con el portapapeles. verificar que cualquier política de seguridad del portapapeles en el espacio de trabajo permite la acción que está intentando.
- **La imagen falla la validación al añadirla** — Una imagen CDE debe incluir un cliente SSH y los clientes Git y Git LFS, y debe tener un usuario `developer` con UID 1000. La imagen GUI de Debian de ejemplo ya cumple estos requisitos. Consulte Añadir una imagen CDE.

Install SecurSpaces as a desktop app

Citrix Secure Access con Chrome Enterprise Premium y SecurSpaces proporcionan un entorno de confianza cero y alto rendimiento para el desarrollo basado en la nube. Puede acceder a una

versión con todas las funciones de Visual Studio Code (VS Code) directamente desde su navegador web.

Para optimizar su flujo de trabajo, puede instalar la instancia de SecurSpaces como una aplicación web progresiva (PWA). Esto le permite ejecutar su entorno de desarrollo en una ventana dedicada e independiente en lugar de una pestaña del navegador, lo que proporciona una experiencia de escritorio nativa.

Arquitectura de las PWA de SecurSpaces

Cuando utiliza Google Chrome o Chrome Enterprise Premium, una aplicación web progresiva (PWA) actúa como un puente entre el sistema operativo local y el contenedor seguro de Citrix en la nube. A diferencia de un acceso directo de navegador estándar, una instancia de SecurSpaces instalada como PWA funciona como una aplicación independiente en la barra de tareas del sistema operativo y gestiona su propia lógica de ventanas.

La instalación de la instancia de SecurSpaces VS Code como PWA ofrece los siguientes beneficios:

- **Cambio de contexto reducido**: Separa los espacios de trabajo de desarrollo de la navegación web general.
- **Mayor espacio en pantalla**: Elimina los elementos de la interfaz de usuario del navegador, como la barra de direcciones y los marcadores, para maximizar el área de codificación.
- **Integración con el sistema**: Permite atajos de teclado nativos del sistema operativo (como **Alt+Tab** o **Cmd+Tab**) y mantiene el IDE activo incluso si cierra la ventana principal del navegador.

Instalar SecurSpaces como PWA

Siga estos pasos para crear un acceso directo de escritorio dedicado para su entorno SecurSpaces utilizando Google Chrome o Chrome Enterprise Premium.

1. **Acceda a su espacio de trabajo**. Navegue a la URL de SecurSpaces de su organización y lance su espacio de trabajo web de VS Code.
2. **Instale la aplicación**. En la barra de direcciones de Chrome (Omnibox), seleccione el icono de **Instalar** (el icono del monitor con una flecha hacia abajo) a la derecha de la URL.

> **Nota:**

> Alternativamente, seleccione el menú **Más** (tres puntos verticales), seleccione **Guardar y compartir**, y luego seleccione **Instalar página como aplicación**.

3. **Configure el nombre de la aplicación**. En el cuadro de diálogo, introduzca un nombre para la aplicación (por ejemplo, Engineering-Prod-SecurSpaces) para ayudar a distinguir entre múltiples entornos de proyecto.
4. **Iniciar y anclar la aplicación**. La instancia de SecurSpaces se abre en una ventana nueva y sin bordes. Para asegurar el acceso permanente, haga clic derecho en el icono de la barra de tareas de Windows o del Dock de macOS, y luego seleccione **Anclar**.

Seguridad para Chrome Enterprise Premium

Para organizaciones que utilizan **Chrome Enterprise Premium**, la funcionalidad de PWA sigue rigiéndose por la política corporativa. Los administradores de TI pueden realizar las siguientes tareas:

- Forzar la instalación de la PWA de SecurSpaces en las máquinas de los desarrolladores mediante la Política de Chrome.
- Aplicar reglas de Prevención de Pérdida de Datos (DLP) que persisten dentro de la ventana PWA independiente.
- Mantener el filtrado de URL para evitar que la PWA navegue a dominios externos no autorizados.

El uso de una PWA proporciona una experiencia de aplicación local mientras se mantienen los estándares de seguridad del entorno contenedorizado de Citrix.

Work from a virtual desktop

`Developer`

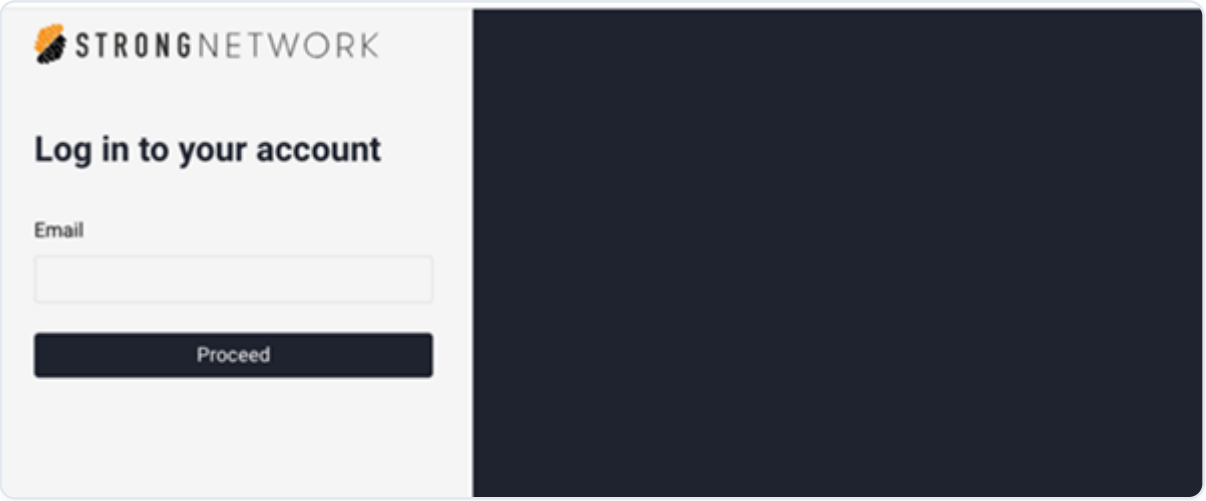
Citrix SecurSpaces™ es compatible con el **modo proxy**, que le permite seguir trabajando en un escritorio virtual existente en lugar de en un espacio de trabajo. Usted instala el Strong Agent en el VDA, y todo el acceso al código fuente se enruta a través de él.

El objetivo de esto son las credenciales. El agente utiliza las credenciales y claves de origen que ya posee la plataforma, por lo que nunca crea ni posee una clave SSH personal para acceder al repositorio, y se aplican las mismas reglas de acceso que se aplicarían dentro de un espacio de trabajo.

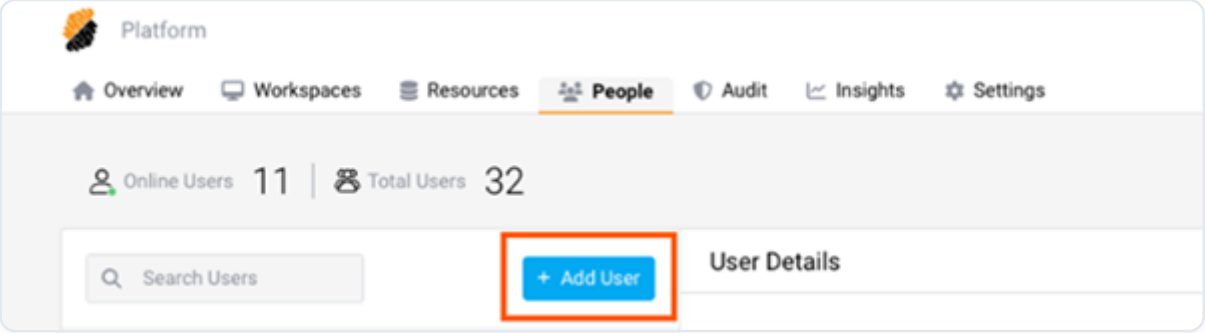
> **Nota:**
>
> Este procedimiento se aplica a VDA de Windows, VDA de Linux y VDA de Citrix para macOS.

Configurar su perfil

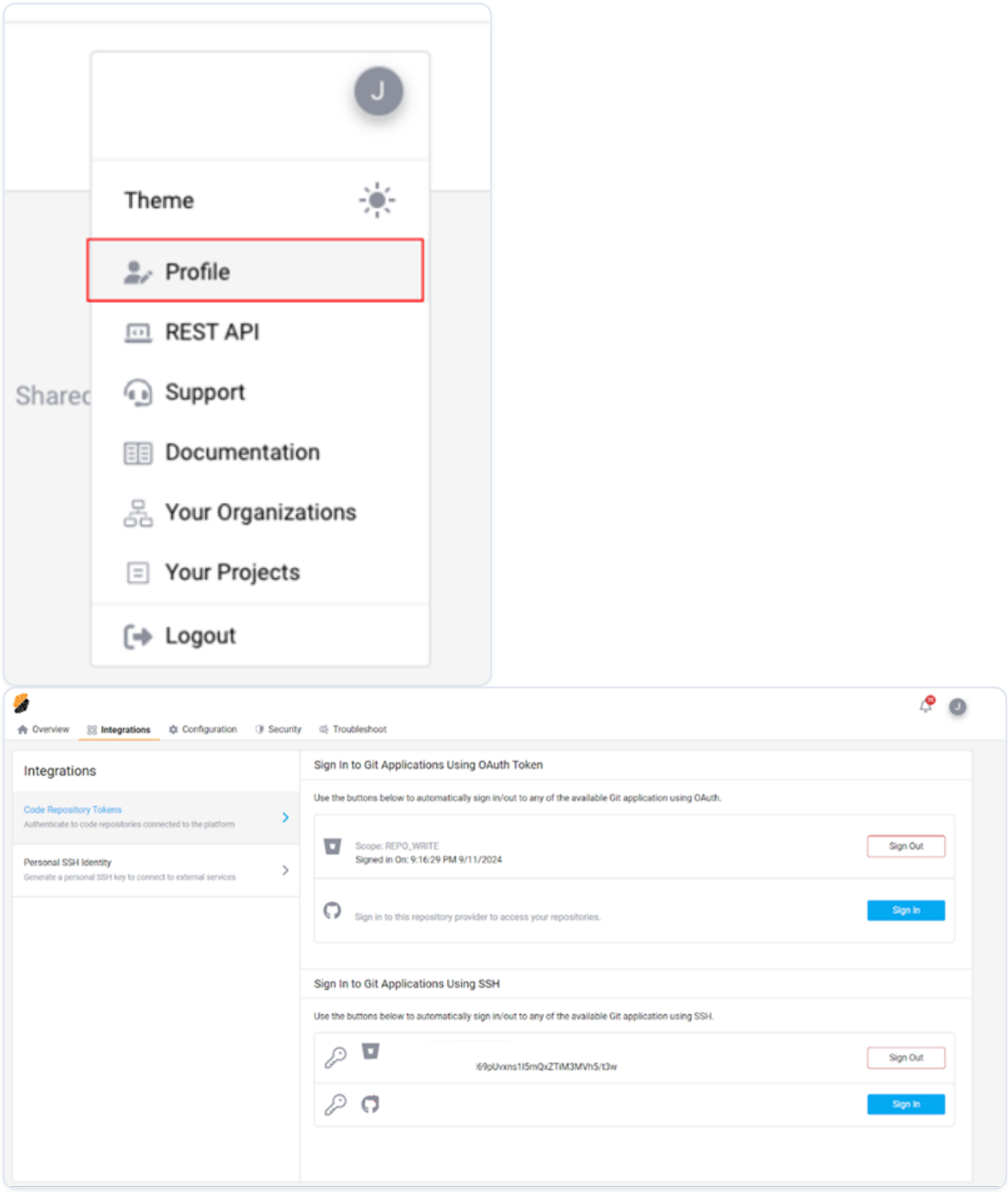
1. Si no ha utilizado el entorno nativo de la nube antes, active su cuenta de SecurSpaces con la URL de la instancia de SecurSpaces de su organización.



2. Pida al propietario de su proyecto que le añada a un proyecto.

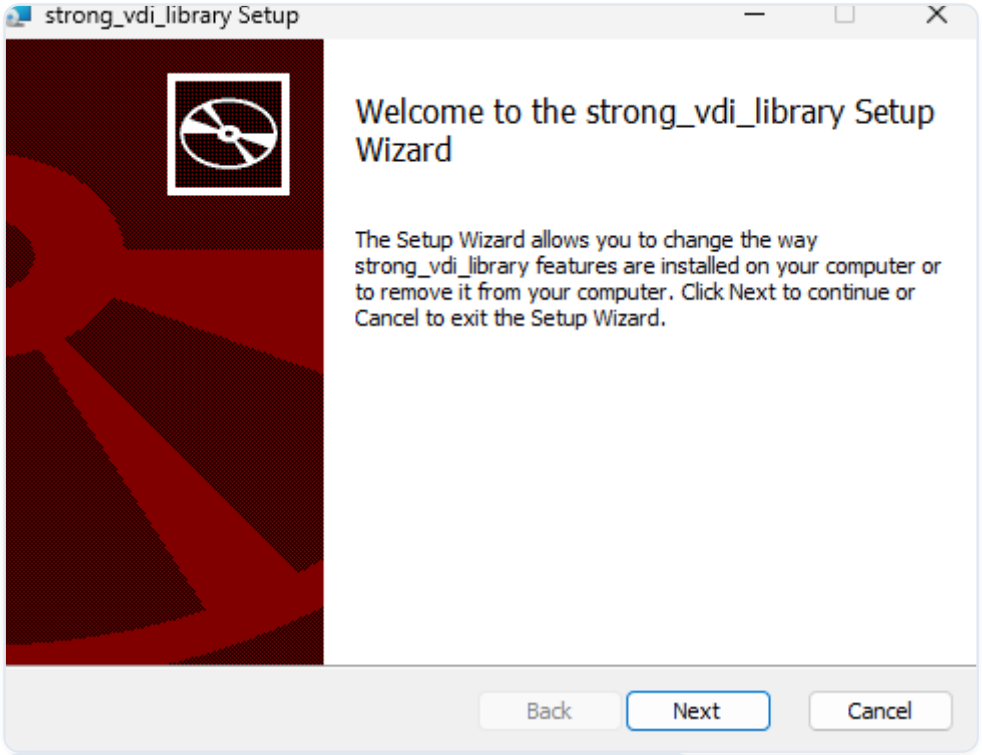


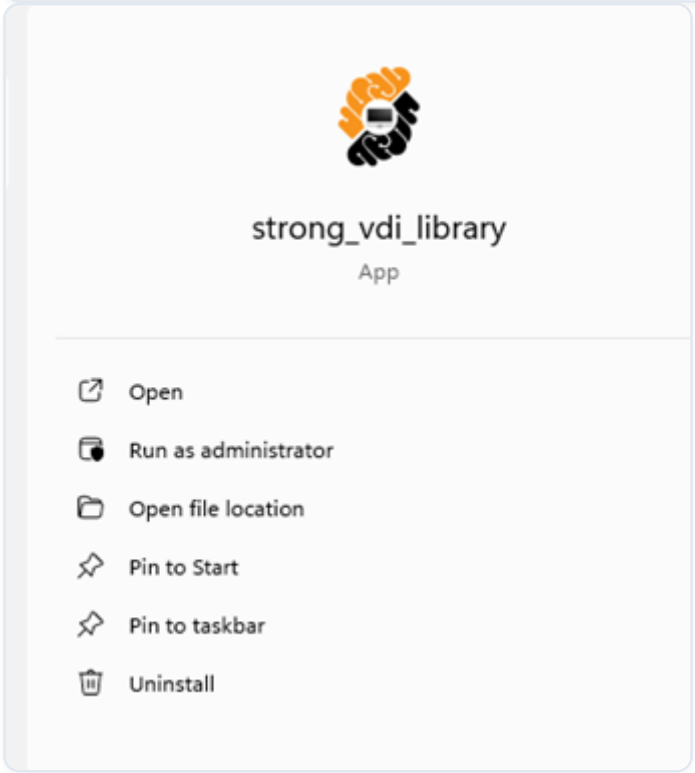
3. Configure su perfil para establecer el permiso de acceso al código fuente.



Instalar el agente

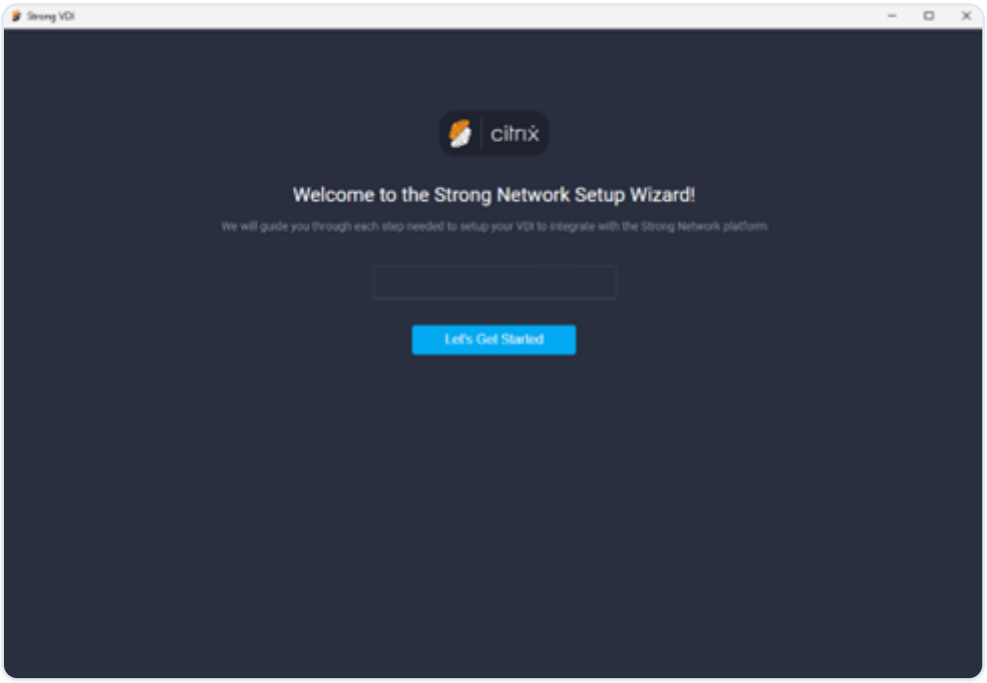
1. Instale el Strong Agent y, a continuación, ejecute la biblioteca Strong VDI.



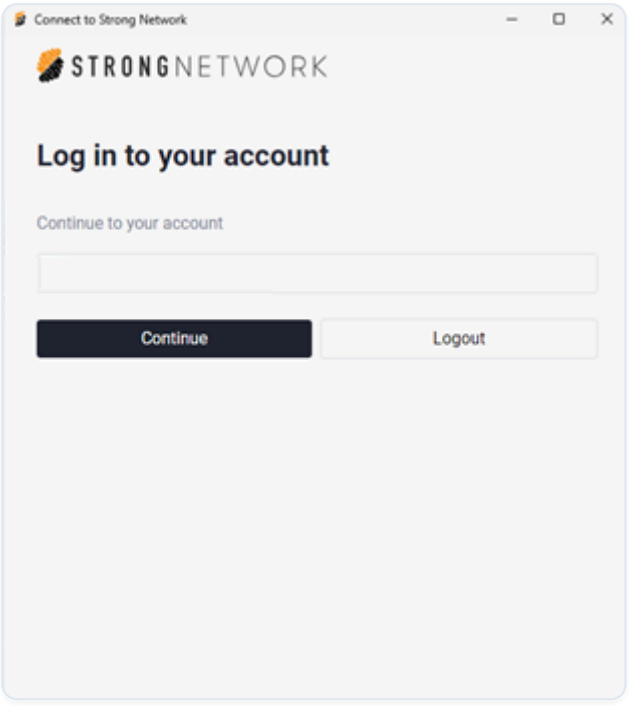


Configurar el agente

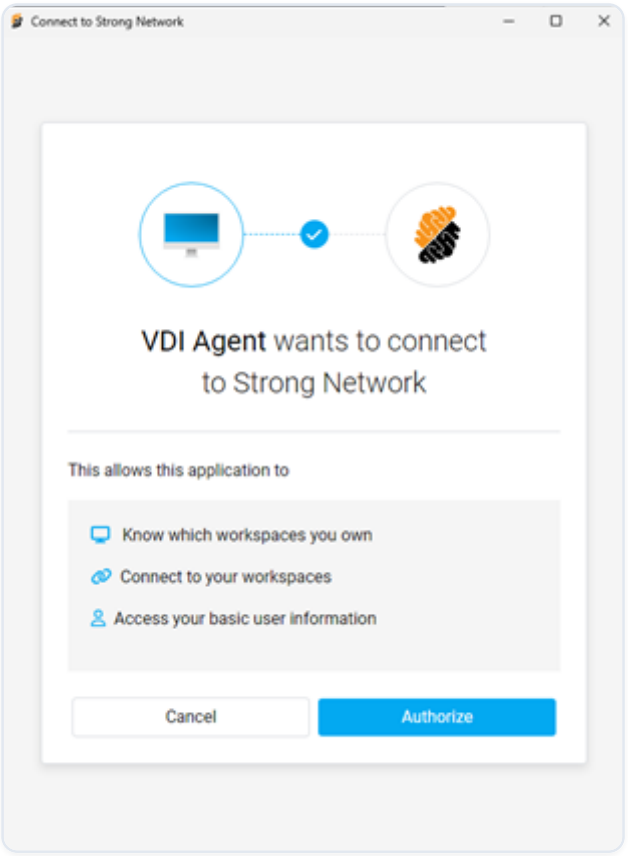
1. Ejecute el binario e introduzca la URL de su espacio de trabajo de SecurSpaces.



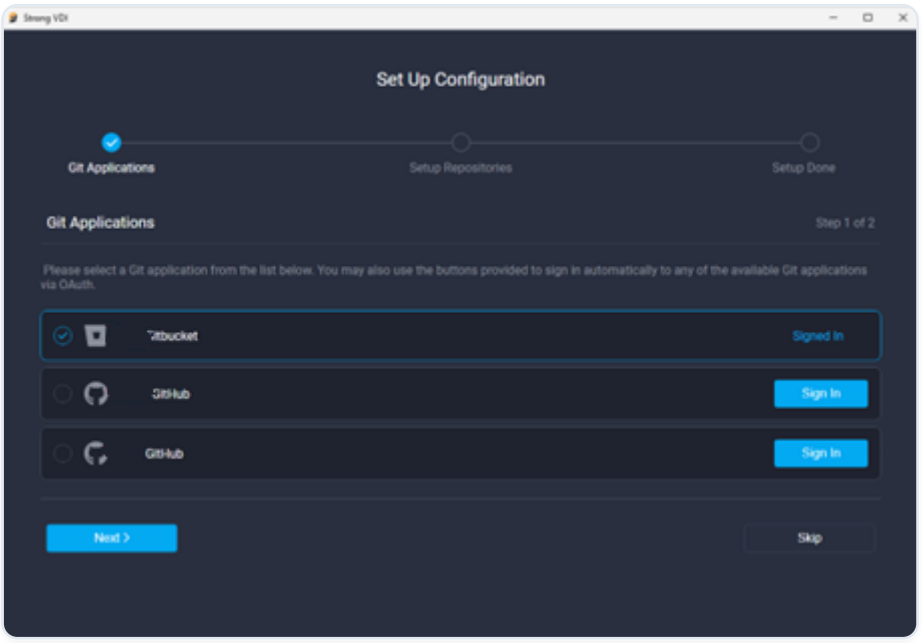
2. Seleccione **Empezar** e inicie sesión en su cuenta.



3. Autorice la conexión a SecurSpaces.



4. Configure el entorno y complete la configuración.



Ahora puede usar cualquier terminal para clonar su código fuente, y un IDE local como Visual Studio o Xcode para el trabajo diario. SecurSpaces gestiona las credenciales de forma centralizada en segundo plano.

Información relacionada

- Su perfil

- Conectarse a través de SSH
- Integración de Citrix DaaS

Give your AI assistant access to the documentation

Si utiliza un asistente de codificación de IA —GitHub Copilot, Claude Code, Cursor, Windsurf o un LLM autoalojado—, puede darle acceso a la documentación completa de Citrix SecurSpaces™ para que pueda responder con precisión a preguntas específicas de SecurSpaces y ayudarle con las tareas de SecurSpaces.

La documentación se sirve directamente desde su instancia de SecurSpaces, por lo que funciona de la misma manera en entornos aislados y conectados a Internet. Todas las recuperaciones de documentación permanecen en su red, y la documentación siempre coincide con su versión de SecurSpaces implementada.

Información general

La documentación se publica en un formato legible por IA basado en el estándar llms.txt. Dos archivos hacen esto posible:

- `llms.txt` — un índice estructurado de cada página de documentación, para que su asistente de IA pueda descubrir lo que está disponible y recuperar la página correcta.
- `llms-full.txt` — el corpus completo de documentación en un solo archivo, para su ingesta en una ventana de contexto o un sistema de generación aumentada por recuperación (RAG).

Qué fuente utilizar

Ambos archivos están disponibles desde dos ubicaciones. Prefiera la primera si tiene una implementación de SecurSpaces.

FUENTE	URL	ÚSELO CUANDO
Su instancia de SecurSpaces	`https://<your-securspaces-url>/docs/llms.txt`	Tiene acceso a una implementación. La documentación coincide con su versión implementada, las recuperaciones permanecen en su red y funciona en entornos aislados.

FUENTE	URL	ÚSELO CUANDO
La copia pública	`https://assets.sds.citrix.com/llms.txt`	No tiene un despliegue al que apuntar, o su herramienta no puede alcanzarlo. Siempre la documentación publicada más reciente, que puede estar por delante de su versión.

La copia pública indexa las mismas páginas en `docs.citrix.com`, por lo que necesita acceso a internet saliente. Utilice la copia alojada en la instancia siempre que pueda: no puede desviarse de la plataforma que está ejecutando.

Esta guía explica:

1. Verificar que la documentación está disponible desde su instancia de SecurSpaces.
2. Añadir contexto de SecurSpaces a su asistente de IA.
3. Probar que su asistente utiliza la documentación.

Antes de empezar

- Conozca la **URL de su instancia de SecurSpaces** — la URL que utiliza para iniciar sesión en la consola de SecurSpaces (por ejemplo, `https://sds.mycompany.internal`).
- Utilice un asistente de IA que admita indicaciones del sistema o instrucciones personalizadas.

Paso 1: verificar que la documentación está disponible

En su navegador, vaya a:

```
https://<your-securspaces-url>/docs/llms.txt
```

Debería ver una lista estructurada de páginas de documentación de SecurSpaces. Si esta página se carga, está listo para continuar.

Si no se carga, póngase en contacto con el administrador de su plataforma. Si no tiene una instancia de SecurSpaces a la que apuntar, utilice `https://assets.sds.citrix.com/llms.txt` en su lugar y sustituya esa URL dondequiera que esta guía se refiera a su instancia.

Paso 2: Añadir contexto de SecurSpaces a su asistente de IA

Añada el siguiente fragmento al mensaje del sistema o a las instrucciones personalizadas de su asistente de IA. Reemplace `<your-securspaces-url>` con la URL real de su instancia de SecurSpaces.

```
You have access to documentation for Citrix SecurSpaces, the cloud
development environment I work in. In SecurSpaces, my code, IDE, and
developer tools run in a remote, containerized workspace that I access
from a browser or over SSH — not on my local machine.

This workspace IS a SecurSpaces workspace. Treat any reference to "my/this
workspace," "my environment," "this machine/container," or my dev tooling
as referring to SecurSpaces — even when I don't say "SecurSpaces"
explicitly.



Documentation sources:

- Documentation index: https://<your-securspaces-url>/docs/llms.txt

- Full documentation corpus: https://<your-securspaces-url>/docs/llms-
full.txt



How to answer SecurSpaces questions:

- Fetch the index first to find relevant pages, then fetch the specific
page(s) for detailed answers. For a clearly SecurSpaces-related question,
prefer this documentation over general knowledge.

- Cite the specific doc page(s) you used (title or URL) so I can verify
the source. If you did not consult the docs for a SecurSpaces answer, say
so.

- SecurSpaces workspaces are ephemeral. When advising on installing tools
or changing the environment, check what persists and recommend an approach
that survives workspace restarts.
```

```
Accuracy and uncertainty:

- Base SecurSpaces-specific answers on the fetched documentation. Clearly
separate what the docs confirm from your own general knowledge or
inference.

- If the documentation does not cover the question, or covers it only

  partially, say so explicitly rather than filling the gap with
assumptions.

- Do not invent SecurSpaces features, configuration options, URLs, CLI
commands, API fields, or version numbers. If you are not certain a detail
is in the docs, state your uncertainty and point me to the docs index or
my platform administrator instead of guessing.

- This documentation matches my deployed SecurSpaces version. If your
general

  knowledge conflicts with it, the documentation wins. Flag any behavior
that may depend on version, configuration, or admin-controlled settings.

- If you cannot reach the documentation URLs, tell me the fetch failed and
do not answer SecurSpaces-specific questions from memory alone.
```

Dónde añadir este fragmento

HERRAMIENTA DE IA	DÓNDE AÑADIR
GitHub Copilot (VS Code)	Ajustes → Copilot → Instrucciones personalizadas, o `.github/copilot-instructions.md` en su repositorio
Claude Code	Añada a `CLAUDE.md` en la raíz de su proyecto, o `~/.claude/CLAUDE.md` para global
Cursor	Ajustes → Reglas para IA, o archivo `.cursorrules` en su repositorio
Windsurf	Ajustes → Cascada → Reglas

HERRAMIENTA DE IA	DÓNDE AÑADIR
LLM autoalojado (Ollama, etc.)	Directiva `SYSTEM` de Modelfile, o páselo como mensaje del sistema en su cliente

Paso 3: Pruébelo

Haz a tu asistente de IA una pregunta clara y específica de SecurSpaces, por ejemplo:

> "¿Cómo configuro una plantilla de espacio de trabajo en SecurSpaces?"

> El asistente debería recuperar la documentación y proporcionar una respuesta específica con terminología de SecurSpaces y pasos concretos.

Solución de problemas

SÍNTOMA	CAUSA POSIBLE	QUÉ HACER
`https://<your-securspaces-url>/docs/llms.txt` no carga	URL de instancia incorrecta, o el punto de conexión de la documentación no es accesible desde tu red	Confirma la URL que utilizas para iniciar sesión en la consola de SecurSpaces. Si sigue fallando, contacta con el administrador de tu plataforma.
El asistente responde con conocimientos generales en lugar de la documentación	Fragmento no aplicado, o la herramienta no recupera URLs automáticamente	Confirma que el fragmento está guardado en la ubicación correcta para tu herramienta. Pide al asistente que recupere primero el índice de la documentación.
El asistente informa que no puede acceder a las URLs de la documentación	Herramienta aislada (air-gapped) sin acceso a la red de la instancia de SecurSpaces	Asegúrese de que la herramienta de IA se ejecute donde pueda alcanzar la URL de su instancia de SecurSpaces, o use `llms-full.txt` como contexto pegado.

SÍNTOMA	CAUSA POSIBLE	QUÉ HACER
No tiene ninguna instancia de SecurSpaces a la que apuntar el asistente	Evaluando o trabajando fuera de una implementación	Use la copia pública en `https://assets.sds.citrix.com/llms.txt` y `https://assets.sds.citrix.com/llms-full.txt`.

Información relacionada

- Ejecutar agentes de codificación de IA en espacios de trabajo — cómo se rigen los agentes cuando se ejecutan dentro de un espacio de trabajo, y lo que su administrador configura para ellos

Troubleshooting

`Developer`

Empiece aquí cuando algo no funcione correctamente y no esté seguro de por qué. Cada síntoma a continuación apunta a la página que lo explica. Si ninguno de ellos coincide, las herramientas de diagnóstico de su perfil le indicarán si el problema es su espacio de trabajo, la red o la plataforma.

Muchos problemas en Citrix SecurSpaces™ no son fallos en absoluto: son políticas que funcionan según lo configurado. Un dominio bloqueado, un repositorio faltante o un espacio de trabajo que se pausa durante la noche son todos deliberados, y todos son corregidos por el propietario del proyecto o el administrador de la plataforma, no por usted. Saber cuál es cuál ahorra la mayor parte del tiempo.

Encuentre su síntoma

Iniciar y ejecutar un espacio de trabajo

SÍNTOMA	CAUSA PROBABLE	DÓNDE BUSCAR
El espacio de trabajo tarda minutos en iniciarse	El clúster está aprovisionando un nodo o extrayendo una imagen grande	Cuánto tarda en iniciarse un espacio de trabajo

SÍNTOMA	CAUSA PROBABLE	DÓNDE BUSCAR
El espacio de trabajo no se inicia o se detiene a mitad de camino	Una etapa de la secuencia de inicio está fallando	Qué sucede cuando se inicia un espacio de trabajo
El espacio de trabajo se detuvo mientras yo estaba ausente	La detección de inactividad lo pausó	Detección de inactividad del espacio de trabajo
Un trabajo largo se interrumpió durante la noche	Detección de inactividad de nuevo — solicita **Omitir programación**	Omitir programación
No puedo crear un espacio de trabajo	Un límite de proyecto o licencia, o tu rol	Roles y permisos
`No space left on device`	El disco del espacio de trabajo está lleno	Desarrollar en un espacio de trabajo
El error del espacio de trabajo menciona `OOMKilled`	Una tarea utilizó más memoria de la que permite el espacio de trabajo	El espacio de trabajo se queda sin memoria

Pérdida de trabajo

SÍNTOMA	CAUSA PROBABLE	DÓNDE BUSCAR
Los archivos desaparecen después de un reinicio	Solo algunas rutas sobreviven a un reinicio	Qué persiste en un espacio de trabajo
Los paquetes instalados desaparecen	Se instalaron fuera de la ruta persistente	Qué persiste en un espacio de trabajo
Las imágenes de Docker deben descargarse o reconstruirse después de cada reinicio	Docker persistente no está habilitado, por lo que la caché de imágenes no está en el volumen persistente	Docker persistente
El espacio de trabajo está ejecutando una imagen diferente a la que muestra la consola	Un cambio de imagen se aplica cuando el espacio de trabajo se reinicia	Crear un espacio de trabajo

SÍNTOMA	CAUSA PROBABLE	DÓNDE BUSCAR
Un archivo compartido cambió sin mi conocimiento	Los puntos de montaje son almacenamiento compartido en vivo	Límites de puntos de montaje

Acceder a elementos fuera del espacio de trabajo

SÍNTOMA	CAUSA PROBABLE	DÓNDE BUSCAR
Una descarga o instalación de paquete está bloqueada	La política de red restringe el tráfico saliente	Políticas de red
No puedo clonar ni enviar a un repositorio	El repositorio no está adjunto, o tu identidad de Git no está configurada	Integración
Una base de datos o un servicio interno no es accesible	El servicio no está adjunto, o el DNS está fallando	Conectar a servicios externos, luego Búsqueda DNS
`no signers found` o `no auth passed yet` al usar SSH o `git`	No hay ningún método SSH configurado para ese host	Conectar a servicios externos
Mi aplicación no es accesible desde el navegador	El puerto no está publicado	Compartir una aplicación en ejecución

Conexión

SÍNTOMA	CAUSA PROBABLE	DÓNDE BUSCAR
El IDE no se carga en el navegador	La conexión websocket está fallando	Herramienta de solución de problemas de WebSocket
Todo se siente lento	Puede que esté trabajando en una región distante	Comprobador de latencia de región
SSH desde mi IDE local falla	Configuración de clave, puerto o plataforma	Conectarse por SSH

SÍNTOMA	CAUSA PROBABLE	DÓNDE BUSCAR
El SSH que antes funcionaba es rechazado, y nada ha cambiado	La clave pública registrada ha caducado. Solo las integraciones IDE de SecurSpaces la renuevan automáticamente	Caducidad y renovación de la clave
Una sesión SSH o Remote-SSH se conecta y luego se cae	La sesión estuvo inactiva y un intermediario la cerró	Mantener una sesión activa
El terminal muestra caracteres extraños después de reconectar	Un programa a pantalla completa estaba ejecutándose cuando la conexión se cayó	Recuperar un terminal corrupto
Copiar y pegar no funciona	Una política de portapapeles se aplica al espacio de trabajo	Crear un espacio de trabajo
Arrastrar un archivo al IDE no hace nada	La transferencia de archivos está restringida	Pregunta a tu administrador de plataforma

Para problemas específicos de una tarea, la página que cubre la tarea también cubre sus fallos — consulta Desarrollar en un espacio de trabajo, Ejecutar un escritorio gráfico, y Dar acceso a tu asistente de IA.

Cuánto tarda en iniciarse un espacio de trabajo

Un inicio no es instantáneo, y uno lento no suele ser un fallo. Dos cosas predominan:

COSTE	POR QUÉ	CUÁNDO SE APLICA
Esperando un nodo	El clúster no tiene espacio y debe aprovisionar uno. El registro muestra mensajes de programación `0/4 nodes are available` repetidos mientras espera	Primer espacio de trabajo del día, o después de que el clúster se haya reducido

COSTE	POR QUÉ	CUÁNDO SE APLICA
Extrayendo la imagen	Una imagen de espacio de trabajo a menudo supera un gigabyte. El registro nombra cada imagen, su tamaño y cuánto tiempo tardó la extracción.	Primer uso de una imagen en ese nodo

Juntos, estos pueden tardar varios minutos. Una vez que la imagen está en el nodo y existe capacidad, los inicios posteriores son mucho más rápidos, y la preparación que sigue —configuración, scripts de inicio, clonación— suele ser cuestión de segundos.

Ambos costes pueden ser reducidos por un administrador de plataforma, por lo que los inicios consistentemente lentos merecen ser planteados en lugar de aceptarlos:

MITIGACIÓN	LO QUE ELIMINA
Nodos cálidos — un grupo de nodos mantenidos aprovisionados e inactivos	La espera a que el clúster se escale. Consulte Configuración de nodos cálidos
Imágenes en caché — una versión de imagen preextraída en los nodos del espacio de trabajo	La extracción de la imagen. Una imagen marcada como en caché muestra un indicador de **Imagen en caché** en la lista de imágenes

Muestre a su administrador de plataforma el registro que se describe a continuación: les indicará cuál de los dos le está costando realmente el tiempo.

Leer el registro de inicio

El registro no solo es visible mientras se inicia un espacio de trabajo. Puede abrirlo en cualquier momento:

1. En la página Espacios de trabajo, seleccione **Más acciones** (**...**) en el espacio de trabajo.
2. Seleccione **Registros**.

Se divide en dos fases, cada una mostrando su tiempo transcurrido, para que puedas ver dónde se fue el tiempo realmente en lugar de adivinar:

- **Configuración del contenedor** — programación, adjunción de volumen y extracción de imágenes. Aquí es donde un inicio prolongado casi siempre se produce.

- **Configuración del espacio de trabajo** — entorno, configuración, scripts de inicio, configuración del IDE y clonación del repositorio, con un tiempo asignado a cada paso.

Si un paso falló en lugar de simplemente ser lento, el registro es también donde aparece el error.

Qué sucede cuando se inicia un espacio de trabajo

Un espacio de trabajo que parece atascado suele estar pasando por una de estas etapas. El panel de progreso y el registro de inicio nombran la actual, lo que te indica dónde buscar:

ETAPA	QUÉ SIGNIFICA	SI SE DETIENE AQUÍ
Comprobando compatibilidad de la imagen	La imagen se está validando con la infraestructura del espacio de trabajo	La imagen puede no cumplir los requisitos. Consulta Requisitos de la imagen de contenedor
Creando imagen	La imagen del contenedor se está creando o extrayendo	Una imagen grande tarda más en el primer uso. Los fallos repetidos son un problema del registro o de la imagen; informa a tu propietario de proyecto
Configurando contenedor	El contenedor se está iniciando y el almacenamiento se está adjuntando	A menudo, un problema de recurso o punto de montaje
Configurando entorno	Los repositorios, secretos y servicios se están adjuntando	Un recurso al que no puedes acceder fallará aquí
Clonando repositorio del espacio de trabajo	Los repositorios adjuntos se están clonando	Verifica tu identidad de Git en Integración
Aplicando dot files	Tus dot files personales se están aplicando	Consulta Configuración
Aplicando archivos de configuración personalizados	Los archivos de configuración de tu perfil se están aplicando	Consulta Configuración

ETAPA	QUÉ SIGNIFICA	SI SE DETIENE AQUÍ
Ejecutando script de inicio del sistema	Se ejecuta el script de inicio definido en la plantilla	Un script fallido es un problema de la plantilla; informa a tu propietario de proyecto
Scripts de inicio del espacio de trabajo	Se ejecuta tu propio script de inicio	Comprueba tu script
Configurando la configuración del IDE	Se están aplicando la configuración y las extensiones del IDE	Consulta Configuración
Preparando el IDE para el lanzamiento	El IDE se está iniciando	Si nunca se completa, usa la Herramienta de solución de problemas de WebSocket

El espacio de trabajo se queda sin memoria

Si los detalles del error del espacio de trabajo incluyen `OOMKilled`, un proceso en el espacio de trabajo usó más memoria de la que permite la especificación del espacio de trabajo:

```
Workspace failure: CrashLoopBackOff. Reason: OOMKilled
```

Esto suele ocurrir después de una compilación, ejecución de prueba, instalación de paquete o tarea de herramientas asistidas por IA que necesitó brevemente más memoria de la esperada.

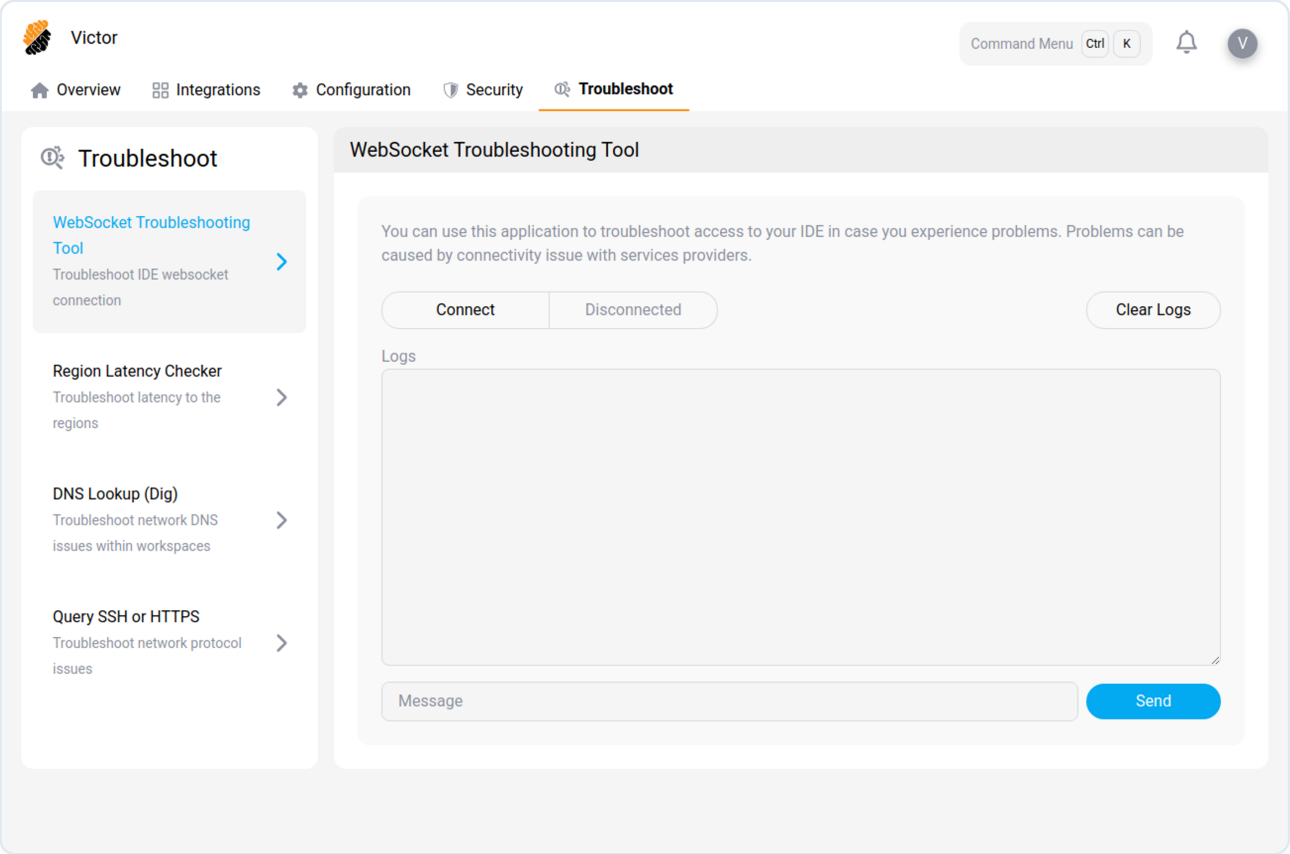
Para recuperar:

1. Vuelve a iniciar el espacio de trabajo y, a continuación, revisa lo que se estaba ejecutando cuando apareció el error.
2. Reduce la memoria que utiliza la tarea o ejecútala en pasos más pequeños.
3. Si la tarea necesita legítimamente más memoria, pide a tu propietario de proyecto una especificación con un límite de memoria superior. Si el espacio de trabajo proviene de una plantilla, la plantilla debe cambiarse en su lugar.
4. Reinicia el espacio de trabajo para que se aplique el nuevo límite.

Resultado esperado: El espacio de trabajo se inicia y la tarea se completa dentro de su límite de memoria.

Herramientas de diagnóstico

Tu perfil incluye cuatro herramientas para acotar un problema. Selecciona tu foto de perfil, selecciona **Perfil**, luego abre la pestaña **Solución de problemas**.



Herramienta de solución de problemas de WebSocket

Prueba la conexión WebSocket de la que depende el IDE en la nube. Selecciona **Conectar**, y la herramienta informará si la conexión se ha establecido y registrará lo que sucede. Puedes enviar un mensaje para confirmar que el tráfico pasa en ambas direcciones.

Úsala cuando el IDE no se cargue, o se caiga repetidamente, en el navegador. Un websocket que nunca se conecta suele significar que algo entre tú y la plataforma está cerrando la conexión — un proxy corporativo, una VPN, o una puerta de enlace de inspección TLS. Esa es información que necesita tu administrador de plataforma.

Comprobador de latencia de región

Informa el tiempo de ida y vuelta a cada región disponible. Úsalo cuando el IDE se sienta lento en lugar de roto.

Si una región distante es notablemente más rápida que la que estás utilizando, tu espacio de trabajo puede estar ejecutándose en el lugar equivocado. Las regiones que puedes usar las establece tu administrador.

Búsqueda DNS (Dig)

Resuelve un nombre de dominio desde dentro de un espacio de trabajo. Úselo cuando algo sea inalcanzable y no sepa si el nombre no se está resolviendo o si la conexión está siendo rechazada.

Si el nombre se resuelve pero la conexión sigue fallando, la causa suele ser la política de red en lugar de DNS.

Consultar SSH o HTTPS

Comprueba si un host es accesible a través de SSH o HTTPS desde el espacio de trabajo. Úselo después de la Búsqueda DNS, para separar un nombre que no se resuelve de un puerto que está bloqueado.

Cuándo escalar y qué incluir

Algunos problemas no puede solucionarlos usted mismo. Cualquier cosa que involucre la política de red, los recursos del espacio de trabajo, las plantillas, los repositorios adjuntos, el modo privilegiado o el programa de omisión es configurada por un propietario de proyecto o un administrador de plataforma.

Incluya lo siguiente, o la primera respuesta solo lo pedirá:

- El nombre del espacio de trabajo y el proyecto al que pertenece.
- La región, si su implementación tiene más de una.
- Lo que estaba haciendo y el mensaje exacto que vio.
- Cuándo ocurrió, con la zona horaria.
- A qué etapa llegó la secuencia de inicio, si el espacio de trabajo no se inició.
- La salida de la herramienta de diagnóstico relevante, si ejecutó una.

Información relacionada

- ¿Qué persiste en un espacio de trabajo?
- Detección de inactividad del espacio de trabajo
- Políticas de red
- Roles y permisos

Manage

Esta sección es para **propietarios de proyectos** y cualquier otra persona que gestione un proyecto en el día a día. Cubre cómo hacer que un equipo trabaje, darles lo que necesitan y establecer las reglas que seguirán sus espacios de trabajo.

La mayoría de las tareas aquí requieren el permiso de **Miembros**, **Recursos** o **Seguridad** a un nivel que su rol permita. Consulte Roles y permisos.

Poner un equipo a trabajar

TAREA	PÁGINA
Incorporar desarrolladores a la plataforma	Incorporar desarrolladores
Añadir y eliminar personas, y establecer sus roles	Personas
Comprender los roles y lo que permite cada permiso	Roles y permisos

Darles lo que necesitan

TAREA	PÁGINA
Dar a todos el mismo entorno inicial	Plantillas
Proporcionar imágenes de contenedor y cadenas de herramientas	Imágenes de espacio de trabajo
Adjuntar repositorios, secretos, almacenamiento y servicios	Recursos del proyecto
Configurar un proyecto para agentes de codificación de IA	Ejecutar agentes de codificación de IA en espacios de trabajo

Establecer las reglas

TAREA	PÁGINA
Renombrar un proyecto o recuperar uno eliminado	Configuración del proyecto y de la organización
Controlar el portapapeles, los límites, SSH y el tráfico de red	Política del espacio de trabajo
Permitir que los espacios de trabajo accedan a servicios externos a través de SSH	Habilitar SSH saliente

Información relacionada

- Administrar — configuración de toda la plataforma
- Conceptos

Onboard developers

`Project Owner`

Incorporar a alguien a un proyecto es una decisión seguida de una tarea breve. La decisión es si ellos crean sus propios espacios de trabajo o si usted crea uno para ellos. Todo lo demás se deriva de eso.

Esta página está escrita para la persona que realiza la incorporación. Para saber qué hace el desarrollador una vez que está dentro, consulte Primeros pasos.

Dos formas de incorporar a alguien

La diferencia es el permiso de **Espacios de trabajo** que conlleva el rol que asigne.

	AUTOSERVICIO	ASIGNADO
Rol	Desarrollador, Gerente o Propietario del proyecto	Invitado
Permiso de espacios de trabajo	Administrar personal o superior	Acceso

	AUTOSERVICIO	ASIGNADO
Quién crea el espacio de trabajo	El desarrollador, a partir de su plantilla	Tú, antes de que lleguen
¿Pueden cambiarlo?	Sí — ajustes y acceso a recursos	No — la configuración es fija
Adecuado para	Empleados y miembros del equipo a largo plazo	Contratistas, colaboradores externos, cualquier persona temporal
Tu esfuerzo	Configurar una plantilla una vez	Un espacio de trabajo por persona

El autoservicio es el caso normal. Elige asignado cuando necesites que el entorno sea exactamente lo que decidiste y que permanezca así, lo que suele implicar limitar lo que un externo puede alcanzar.

Ambos modelos pueden coexistir en un mismo proyecto. El rol es por persona, por lo que puedes tener diez desarrolladores de autoservicio y dos contratistas en espacios de trabajo fijos.

Antes de incorporar a nadie

Ten el proyecto listo primero, o tu primer desarrollador llegará a un entorno vacío. Consulta Configurar un proyecto para tu equipo, que cubre imágenes, repositorios, secretos y la plantilla de la que dependen ambos modelos.

Necesitas el permiso de **Miembros** configurado en **Gestionar** para añadir personas. Los roles predeterminados de Gestor y Propietario del proyecto ambos lo incluyen.

Incorporar a un desarrollador autónomo

1. Abrir **Personas** y seleccionar **Añadir nuevo usuario**.
2. Buscar al usuario y dejar el rol como **Desarrollador**, o elegir Administrador o Propietario del proyecto si van a dirigir parte del proyecto.
3. Seleccionar **Aplicar**.

Ahora pueden crear su propio espacio de trabajo a partir de su plantilla. No se requiere nada más de usted.

Incorporar a un invitado o contratista

1. Abrir **Personas** y seleccionar **Añadir nuevo usuario**.
2. Buscar al usuario y establecer el rol como **Invitado**.
3. Seleccionar **Crear un nuevo espacio de trabajo a partir de una plantilla o uno existente**, y elegir la plantilla que coincida con el trabajo.
4. Seleccionar **Establecer fecha de caducidad** y elegir cuándo finaliza su acceso.
5. Seleccionar **Aplicar**.

El espacio de trabajo se aprovisiona como parte de su adición, por lo que no hay un paso de asignación separado. Cuando inician sesión, el espacio de trabajo está esperando y su configuración es fija.

Establezca la fecha de caducidad incluso cuando espere que el compromiso se extienda. Una caducidad que debe renovarse deliberadamente es más segura que un acceso que persiste silenciosamente después de que alguien se haya marchado.

Consulte Añadir y eliminar usuarios para ver el diálogo completo, incluida la invitación a alguien que aún no está en la plataforma.

Lo que la plataforma envía por usted

Añadir un usuario a un proyecto activa un correo electrónico de **Te has unido a un nuevo proyecto** que contiene un enlace directo a el proyecto. Alguien completamente nuevo en la plataforma también recibe un correo electrónico de invitación.

Esto solo funciona si un administrador de la plataforma ha configurado una pasarela de correo electrónico. **Hasta que se configure una, la plataforma no envía nada en absoluto**, y su nuevo desarrollador estará esperando un mensaje que nunca llegará. Si no está seguro, consulte con su administrador de la plataforma antes de confiar en ello, o informe directamente a las personas de que han sido añadidas.

Consulte Notificaciones de correo electrónico de incorporación.

Qué hace el desarrollador a continuación

Diríjalos a Empezar. Un desarrollador autoasistido quiere Su primer espacio de trabajo; un invitado ya tiene uno, así que Configurar su cuenta es el mejor punto de partida.

Si prefiere entregar algo escrito para su propio equipo, adapte la plantilla de incorporación reutilizable, que puede rellenar con sus repositorios, herramientas y políticas.

Información relacionada

- Roles y permisos
- Personas
- Plantillas
- Configurar un proyecto para su equipo

Reusable template for SecurSpaces workspace onboarding

Información general

Utilice esta plantilla para incorporar desarrolladores a Citrix SecurSpaces™. Este marco proporciona una guía concisa y paso a paso para pasar del acceso inicial a una aplicación en ejecución. Puede personalizar y ampliar este documento con sus herramientas, repositorios y políticas específicos para ofrecer una experiencia de incorporación coherente y personalizada a su equipo.

Antes de empezar

Antes de empezar, asegúrese de que uno de los siguientes elementos esté disponible:

- Una plantilla de espacio de trabajo compartida por su equipo de TI o líder de equipo a través de un enlace o accesible a través de la interfaz de usuario de SecurSpaces.
- Acceso a la plantilla predeterminada de SecurSpaces desde el espacio de trabajo.

Si ninguna de las opciones está disponible, póngase en contacto con su líder de equipo antes de continuar.

Paso 1: Configure su perfil y lance un espacio de trabajo

Nota del administrador: En esta fase, los usuarios configurarán sus perfiles en la interfaz de usuario de SecurSpaces para acceder, crear y ejecutar rápidamente una aplicación. El entorno utiliza un terminal Linux estándar y Visual Studio Code. El objetivo es ejecutar la aplicación existente en el nuevo entorno lo antes posible para establecer prácticas familiares.

1. Configure su perfil

1. Inicie sesión en la **interfaz de usuario de la aplicación SecurSpaces**.
2. En su perfil,
    - Establezca su **zona horaria** y su **horario de trabajo** preferido.
    - Autentíquese con su proveedor de **Git** (GitHub, GitLab o Bitbucket).

2. Lance su espacio de trabajo

Elija una de las siguientes opciones:

- **Opción A:** Desde la interfaz de usuario de SecurSpaces, seleccione la flecha junto a **Crear espacio de trabajo** y, a continuación, seleccione **Desde plantilla**. Seleccione una **plantilla de espacio de trabajo** y, a continuación, seleccione **Iniciar**.
- **Opción B:** Si su repositorio de Git tiene un archivo con un enlace a un **espacio de trabajo** (normalmente readme.md), haga clic en **Abrir espacio de trabajo** directamente desde el README.md del proyecto.

3. Clone y compile su proyecto

1. Abra el espacio de trabajo utilizando la interfaz de VS Code basada en navegador o el terminal.
2. Clone su repositorio utilizando su comando estándar **git clone**.
3. Ejecute sus comandos de compilación habituales.
4. Compruebe que la extensión de VS Code para SecurSpaces está instalada y activa. Esta extensión le permite abrir y gestionar aplicaciones que se ejecutan en su espacio de trabajo.
5. Utilice la extensión para ejecutar su aplicación y previsualizarla usando la URL.

Habrá completado el Paso 1 cuando su aplicación esté en ejecución y sea accesible a través de una URL activa.

Paso 2: Configurar el acceso rápido

Nota del administrador: En esta fase, los usuarios configuran su método preferido para acceder a un espacio de trabajo: ya sea desde un icono de escritorio, a través de una aplicación web progresiva o utilizando una URL incrustada en una página web o de Markdown. Esto último se utiliza normalmente para iniciar un espacio de trabajo desde un repositorio de Git.

1. Cree un acceso directo de escritorio a su espacio de trabajo (abrir desde el IDE o el terminal)

Cree un acceso directo en el escritorio o en la barra de tareas para:

- La interfaz de usuario de SecurSpaces, o
- Un espacio de trabajo específico.

Esto permite un acceso instantáneo sin necesidad de navegar por marcadores o la interfaz de usuario de SecurSpaces.

2. Habilitar el inicio del repositorio Git

En la página de Espacio de trabajo, en **Plantilla**, copie el enlace de la plantilla de **Inicio rápido** para añadir un icono de **Abrir espacio de trabajo** al README.md de su repositorio, facilitando el lanzamiento de SecurSpaces directamente desde el repositorio.

Paso 3: Personalice la configuración de su perfil

Nota del administrador: En esta fase, los usuarios exploran las opciones de personalización del espacio de trabajo. Pueden configurar entornos en la interfaz de usuario de SecurSpaces a través del menú de perfil de usuario o editando la configuración del espacio de trabajo.

1. Persistir la configuración del shell

Usando el menú de perfil, añada sus archivos **.bashrc** o **.zshrc** para que se añadan automáticamente a su directorio de inicio cuando se cree un nuevo espacio de trabajo. Puede actualizar un espacio de trabajo existente utilizando la opción de actualización del menú del espacio de trabajo.

2. Añadir secretos y claves

Su perfil también le permite definir variables (por ejemplo, con secretos) y generar una clave SSH para que esté disponible en su espacio de trabajo:

- Variables de entorno personales
- Claves SSH – le permiten conectarse por SSH a un host utilizando una clave privada almacenada en el proxy de credenciales.

Esta configuración se puede actualizar en cualquier momento.

3. Precargar extensiones de VS Code

Usando el menú de perfil, configure sus extensiones preferidas de VS Code para que estén disponibles automáticamente cuando se inicie el espacio de trabajo.

Paso 4: (Opcional) Personalice la configuración de su espacio de trabajo

Nota del administrador: En esta fase, los usuarios modifican la configuración de su espacio de trabajo para optimizar el rendimiento y automatizar tareas repetitivas.

1. Ajustar los recursos de hardware

Actualice la configuración de CPU y memoria según las necesidades del proyecto, como compilaciones grandes o herramientas que consumen muchos recursos. Esta configuración se puede cambiar en cualquier momento.

2. Automatizar el inicio del espacio de trabajo

Usando el editor del espacio de trabajo, añada scripts previos o posteriores al inicio para instalar automáticamente herramientas o dependencias cuando el espacio de trabajo se inicie. Esta opción añade herramientas a una imagen base existente que no se pueden instalar en la carpeta de inicio (`./home/developer`). Para obtener más información sobre cómo se conservan los datos entre reinicios, consulte Mantener cambios persistentes en su espacio de trabajo.

3. Configurar la ejecución automática

Usando el editor del espacio de trabajo, puede configurar las aplicaciones que se ejecutan en su espacio de trabajo para que se inicien automáticamente al arrancar.

Obtener ayuda

Si su espacio de trabajo no se inicia, su compilación no se completa o su aplicación no se ejecuta como se esperaba, póngase en contacto con su jefe de equipo o con el canal de soporte de SecurSpaces.

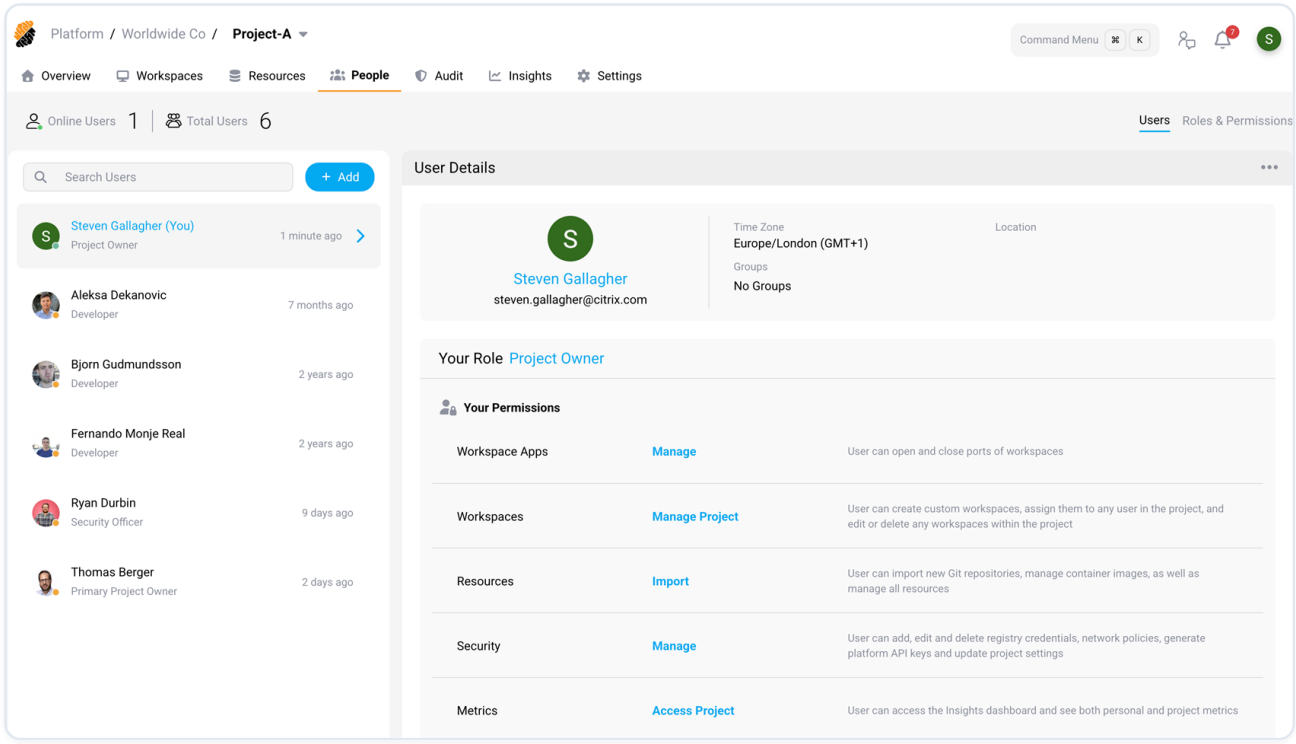
People page

La página Personas contiene información sobre los usuarios incorporados a un proyecto, una organización o la plataforma completa. Por lo tanto, cambiar de proyecto u organización actualiza la membresía en la tabla.

Puede ver el rol, los permisos y los detalles públicos de cada usuario en el panel Ver usuario.

Esta página proporciona funciones típicas de gestión de equipos a los usuarios con los permisos adecuados. El *propietario del proyecto* tiene permisos para actualizar los roles de los usuarios en el proyecto.

Además, el propietario del proyecto puede crear nuevos roles o actualizar los existentes desde el panel Gestión de permisos.



> **Información:**

> Un usuario normal puede ver todos los roles del proyecto y sus permisos, incluso sin tener el permiso Miembros configurado en **Gestionar**.

Contenido

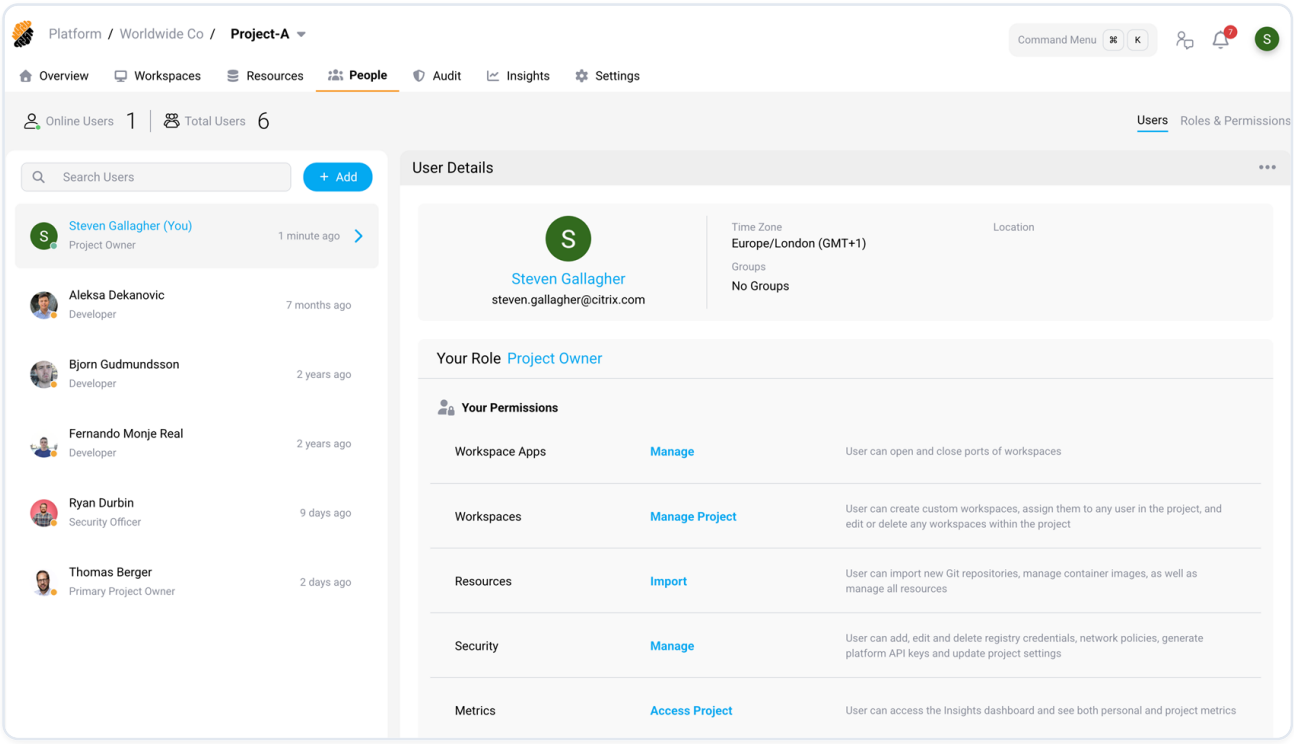
- Panel **Ver usuarios**.
- Panel **Control de acceso**.

Users

La página **Personas** muestra los usuarios en dos niveles: proyecto y plataforma. La información mostrada y las acciones disponibles varían según el nivel.

Vista a nivel de proyecto

A nivel de proyecto, la página **Personas** utiliza un diseño de panel dividido. El panel izquierdo enumera los miembros del proyecto y el panel derecho muestra los detalles del usuario seleccionado.



Lista de usuarios

El panel izquierdo muestra todos los miembros del proyecto, ordenados por actividad más reciente. Cada entrada muestra:

- Nombre de usuario y avatar
- Rol en el proyecto actual (por ejemplo, Propietario principal del proyecto, Desarrollador, oficial de seguridad)
- Marca de tiempo de la última actividad
- Indicador de estado en línea (para usuarios actualmente conectados)

Los recuentos resumidos de **Usuarios en línea** y **Usuarios totales** aparecen encima de la lista.

Utilice el campo **Buscar usuarios** encima de la lista de usuarios para filtrar por nombre. Esto reduce la lista mostrada sin cambiar la membresía real.

Panel de detalles del usuario

Seleccione un usuario de la lista para ver sus detalles en el panel derecho.

Información del perfil:

- Nombre y dirección de correo electrónico
- Zona horaria
- Ubicación (si la ha establecido el usuario)

- Pertenencias a grupos

Rol y permisos:

El panel muestra el rol actual del usuario en el proyecto y los permisos asociados. Cada categoría de permiso muestra el nombre de la categoría, el nivel de permiso y una descripción de lo que permite el nivel.

Para cambiar el rol de un usuario, seleccione **Cambiar rol**. Esto requiere que el permiso Miembros esté establecido en **Administrar**.

Menú Más acciones:

Seleccione el icono **...** en la parte superior derecha del panel Detalles del usuario para acceder a:

- **Más detalles** — Abre la página completa de detalles del usuario (la misma página que los detalles del usuario a nivel de plataforma descritos a continuación).
- **Eliminar usuario del proyecto** — Elimina al usuario del proyecto actual. Consulte Añadir y eliminar usuarios y grupos para obtener más detalles.

Pestañas

La página Personas a nivel de proyecto tiene dos pestañas en la esquina superior derecha:

- **Usuarios** — La lista de usuarios descrita anteriormente.
- **Roles y permisos** — Administrar roles del proyecto. Consulte Control de acceso para obtener más detalles.

Vista a nivel de plataforma

A nivel de plataforma, la página de **Personas** está disponible para los **oficiales de seguridad** y los **administradores de plataforma**. Muestra todos los usuarios registrados en la plataforma en una tabla.

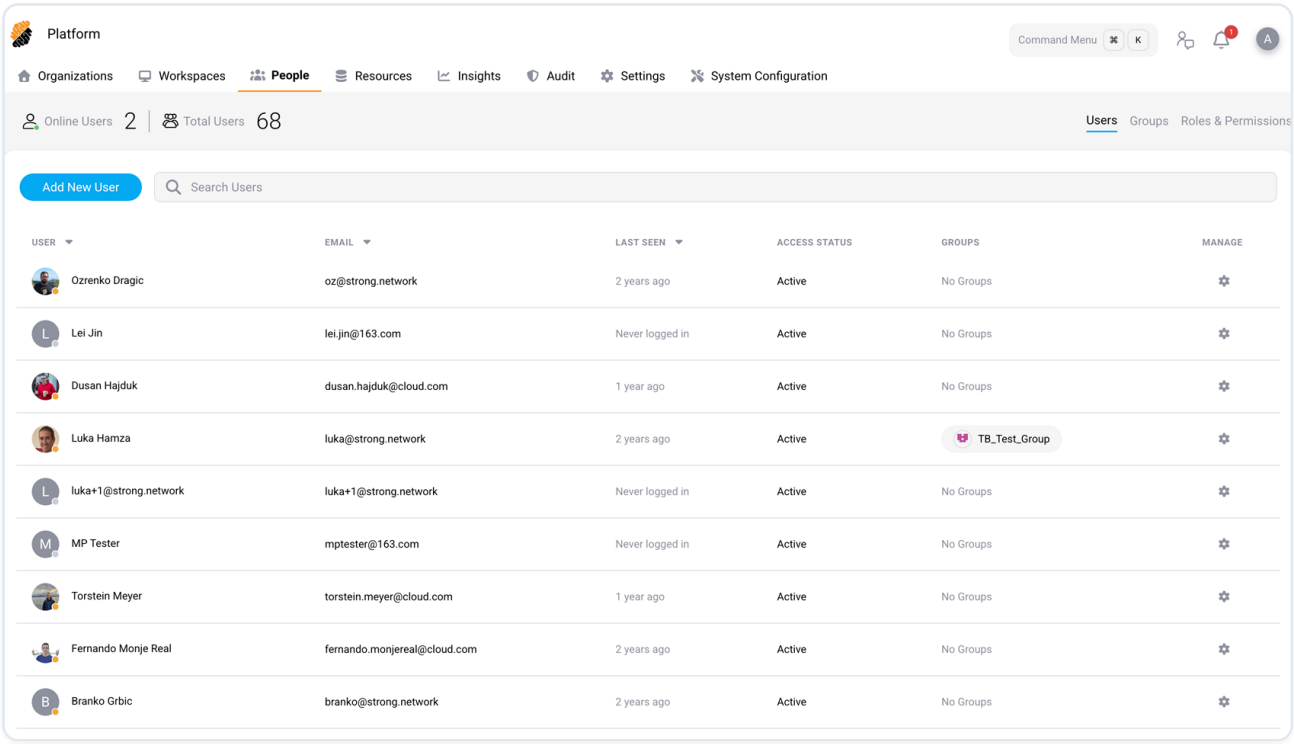


Tabla de usuarios

La tabla incluye las siguientes columnas:

COLUMNA	DESCRIPCIÓN
Usuario	Nombre y avatar. Ordenable.
Correo electrónico	Dirección de correo electrónico. Ordenable.
Última vez visto	Marca de tiempo de la actividad más reciente del usuario. Ordenable.
Estado de acceso	Indica si la cuenta del usuario está activa.
Grupos	Grupos a los que pertenece el usuario.
Gestionar	Icono de engranaje de configuración para acciones de gestión de usuarios.

Los recuentos resumidos de **Usuarios en línea** y **Usuarios totales** aparecen encima de la tabla. Utilice el campo **Buscar usuarios** para filtrar la lista.

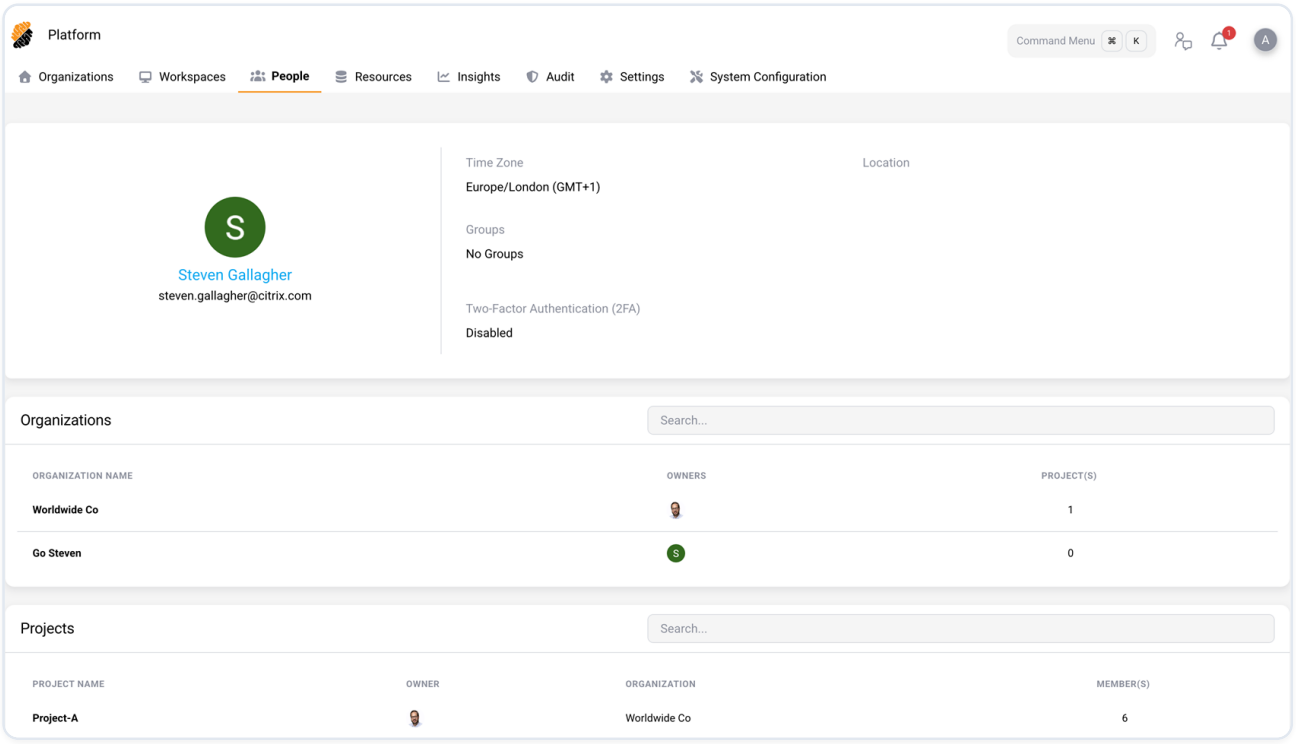
Pestañas

La página Personas a nivel de plataforma tiene tres pestañas:

- **Usuarios** — La tabla de usuarios descrita anteriormente.
- **Grupos** — Gestionar grupos a nivel de plataforma.
- **Roles y permisos** — Gestionar roles y permisos a nivel de plataforma.

Página de detalles del usuario

Seleccione una fila de usuario para abrir la página completa de detalles del usuario. Esta página proporciona una vista completa del acceso y la actividad del usuario en toda la plataforma.



Perfil:

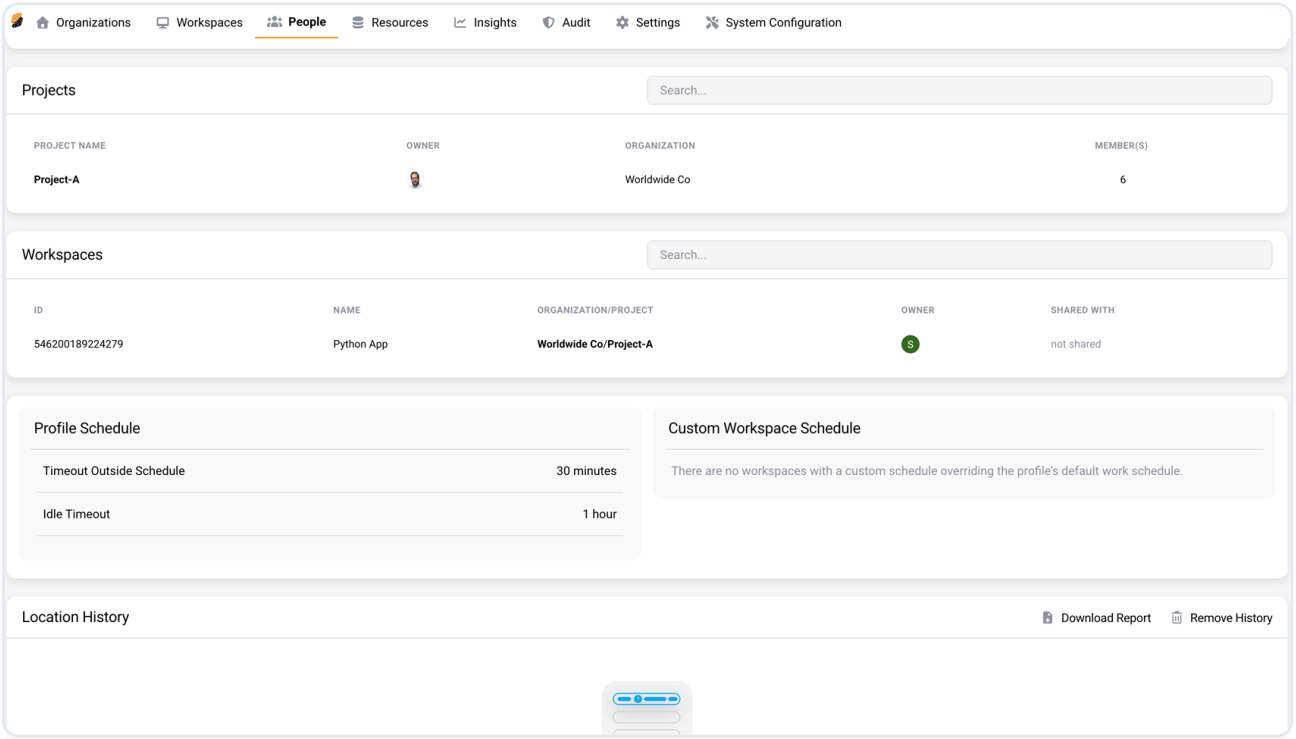
- Nombre, dirección de correo electrónico y avatar
- Zona horaria
- Ubicación
- Pertenencia a grupos
- Estado de la autenticación de dos factores (2FA)

Organizaciones:

Una tabla con capacidad de búsqueda que enumera todas las organizaciones a las que pertenece el usuario, con columnas para Nombre de la organización, Propietarios y número de Proyectos.

Proyectos:

Una tabla con capacidad de búsqueda que enumera todos los proyectos a los que el usuario puede acceder, con columnas para Nombre del proyecto, Propietario, Organización y número de Miembros.



Espacios de trabajo:

Una tabla con capacidad de búsqueda que enumera todos los espacios de trabajo propiedad del usuario o compartidos con él, con columnas para ID, Nombre, Organización/Proyecto, Propietario y Compartido con.

Programación del perfil:

Muestra la configuración de programación del usuario:

- Tiempo de espera fuera de la programación — cuánto tiempo permanece un espacio de trabajo en ejecución fuera del horario laboral del usuario antes de pausarse.
- Tiempo de espera de inactividad — cuánto tiempo permanece un espacio de trabajo en ejecución sin actividad antes de pausarse.

Programación personalizada del espacio de trabajo:

Enumera cualquier espacio de trabajo que tenga una programación personalizada que anule la programación de trabajo predeterminada del usuario.

Historial de ubicaciones:

Muestra el historial de ubicaciones de inicio de sesión del usuario. Incluye las acciones de **Descargar informe** y **Eliminar historial**.

Información relacionada

- Añadir y eliminar usuarios
- Roles y permisos
- Personas

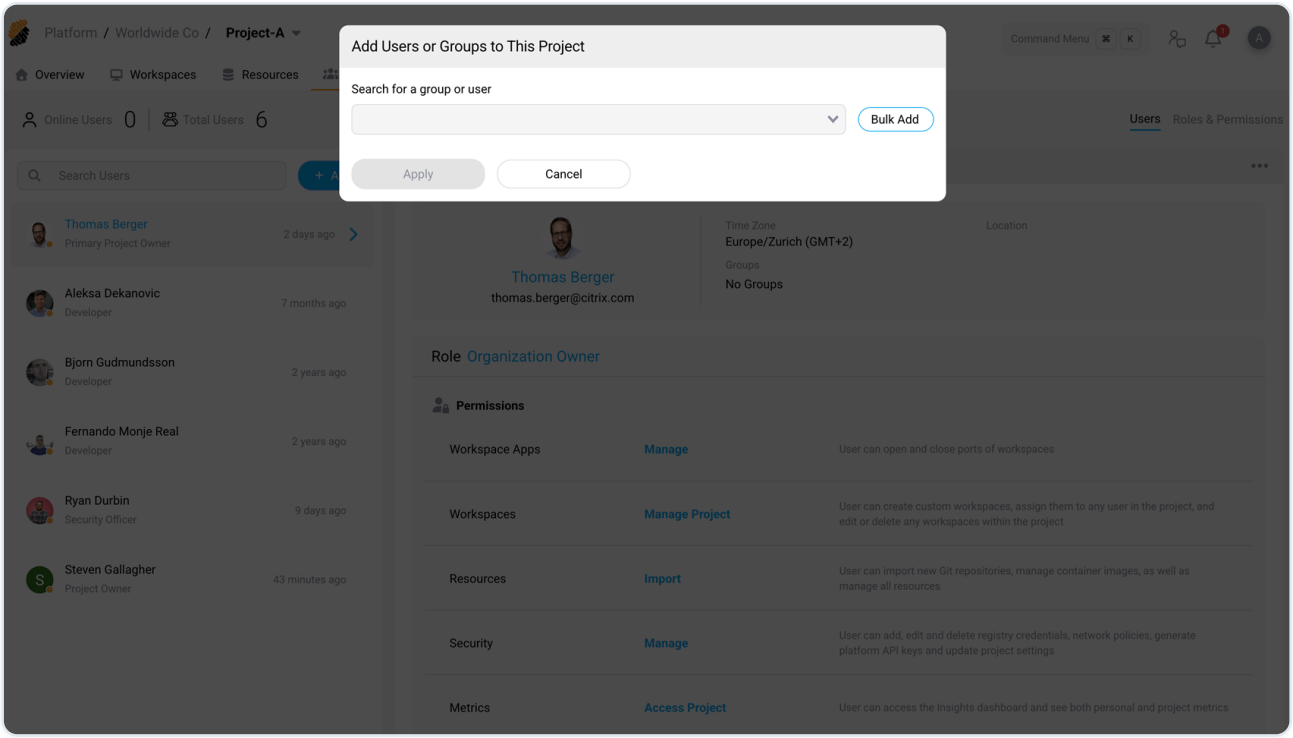
Add and remove users and groups

Esta página describe cómo añadir y eliminar usuarios y grupos en un proyecto. Estas acciones están disponibles en la página de **Personas** a nivel de proyecto y requieren que el permiso Miembros esté configurado en **Gestionar**.

Añadir usuarios o grupos a un proyecto

1. Navega a tu proyecto y selecciona **Personas** en la barra de navegación.
2. Selecciona **+ Añadir**.

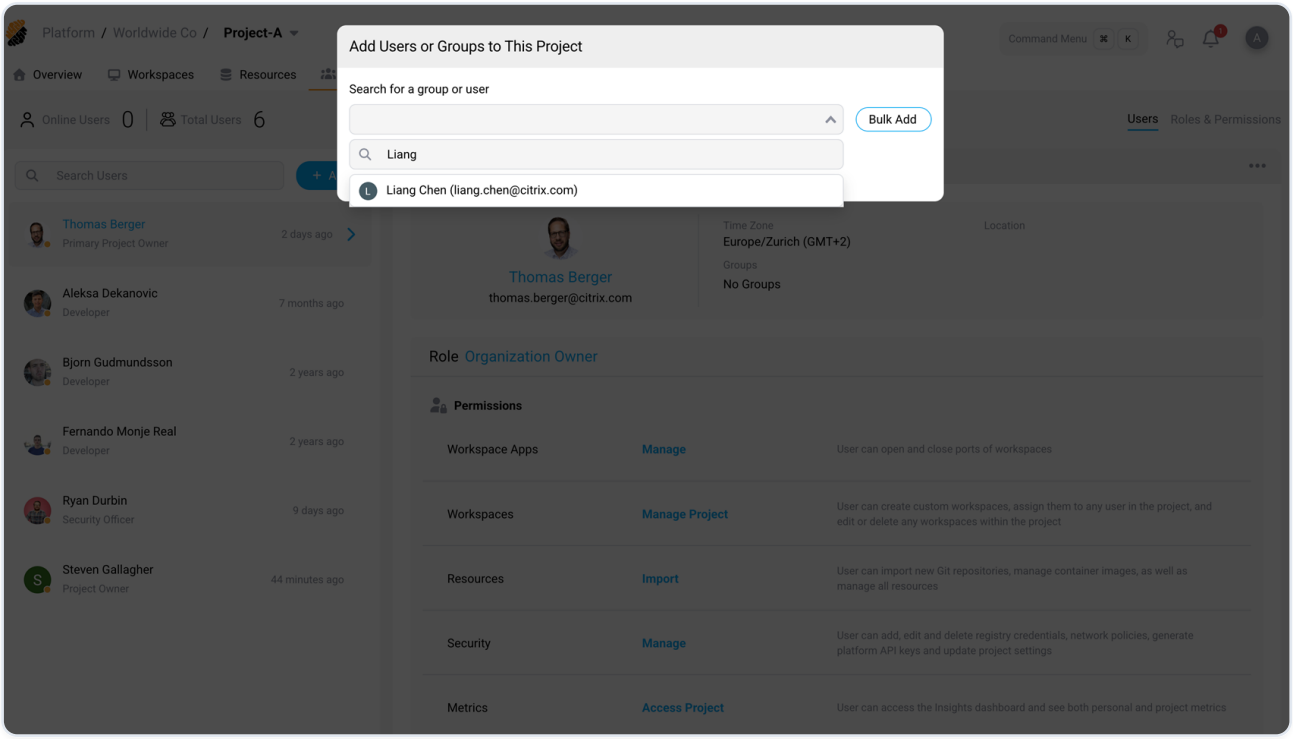
Se abre el modal **Añadir usuarios o grupos a este proyecto**.



Añadir un usuario por búsqueda

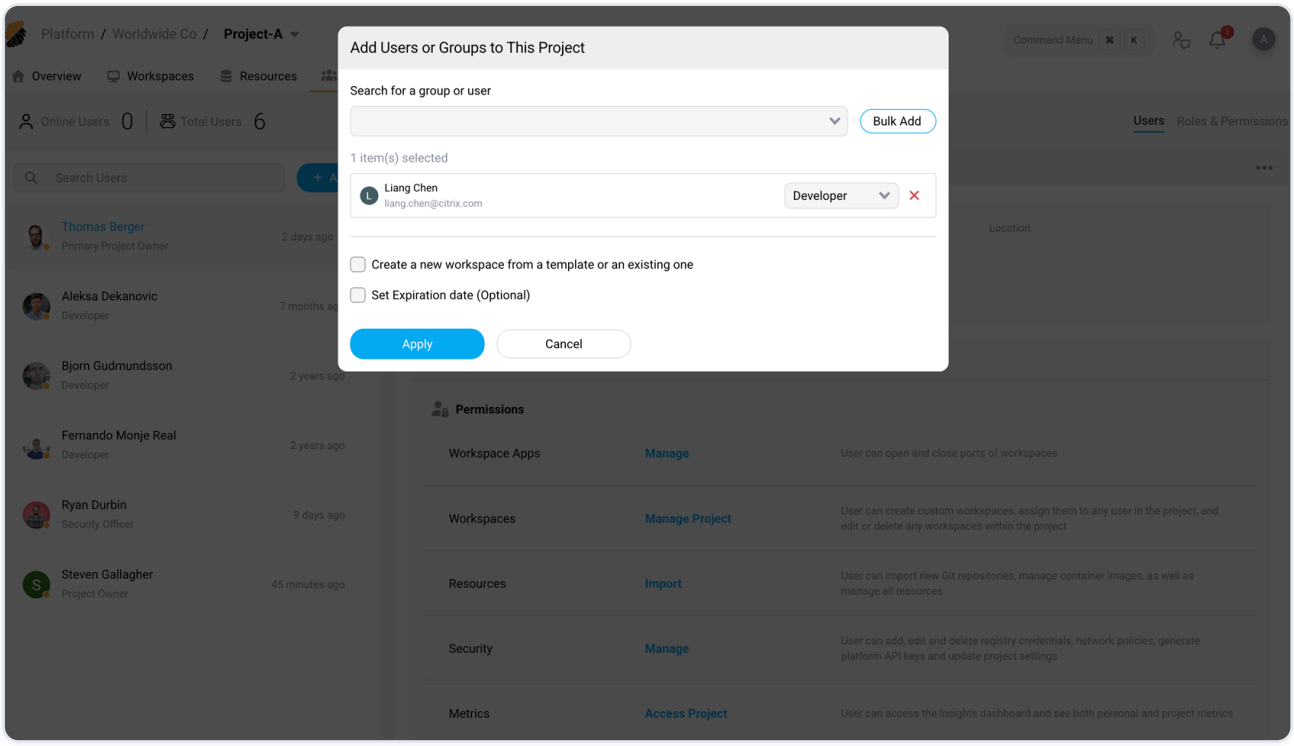
El desplegable de búsqueda muestra los usuarios de la plataforma que aún no son miembros del proyecto actual. Este es un campo de selección única; selecciona un usuario a la vez para evitar confusiones.

1. En el campo **Usuario o grupo**, empieza a escribir el nombre o la dirección de correo electrónico del usuario.
2. Selecciona el usuario de los resultados filtrados.



El usuario aparece en la lista de selección. Puedes:

- Cambiar su **rol** usando el desplegable junto al nombre del usuario (por defecto es Desarrollador).
- Marca **Crear un nuevo espacio de trabajo a partir de una plantilla o uno existente** para aprovisionar un espacio de trabajo durante la incorporación.
- Marca **Establecer fecha de caducidad (Opcional)** para establecer un límite de tiempo para el acceso del usuario al proyecto.
- Elimine al usuario de la lista seleccionando el botón **X**.



1. Seleccione **Aplicar** para añadir al usuario.

Invitar a un usuario que aún no está en la plataforma

El campo **Usuario o grupo** no se limita a personas que ya tienen una cuenta. También puede usarlo para invitar a alguien nuevo.

1. En el campo **Usuario o grupo**, escriba la dirección de correo electrónico completa de la persona.
2. Seleccione el icono de añadir (+).

Mientras escribe, y antes de que la dirección esté completa, el campo informa de que no se encontraron coincidencias y explica que introducir una dirección de correo electrónico completa le permite invitar a alguien. Una vez que la dirección es válida, el campo confirma que el usuario aún no está en la plataforma y le pide que seleccione el icono de añadir (+).

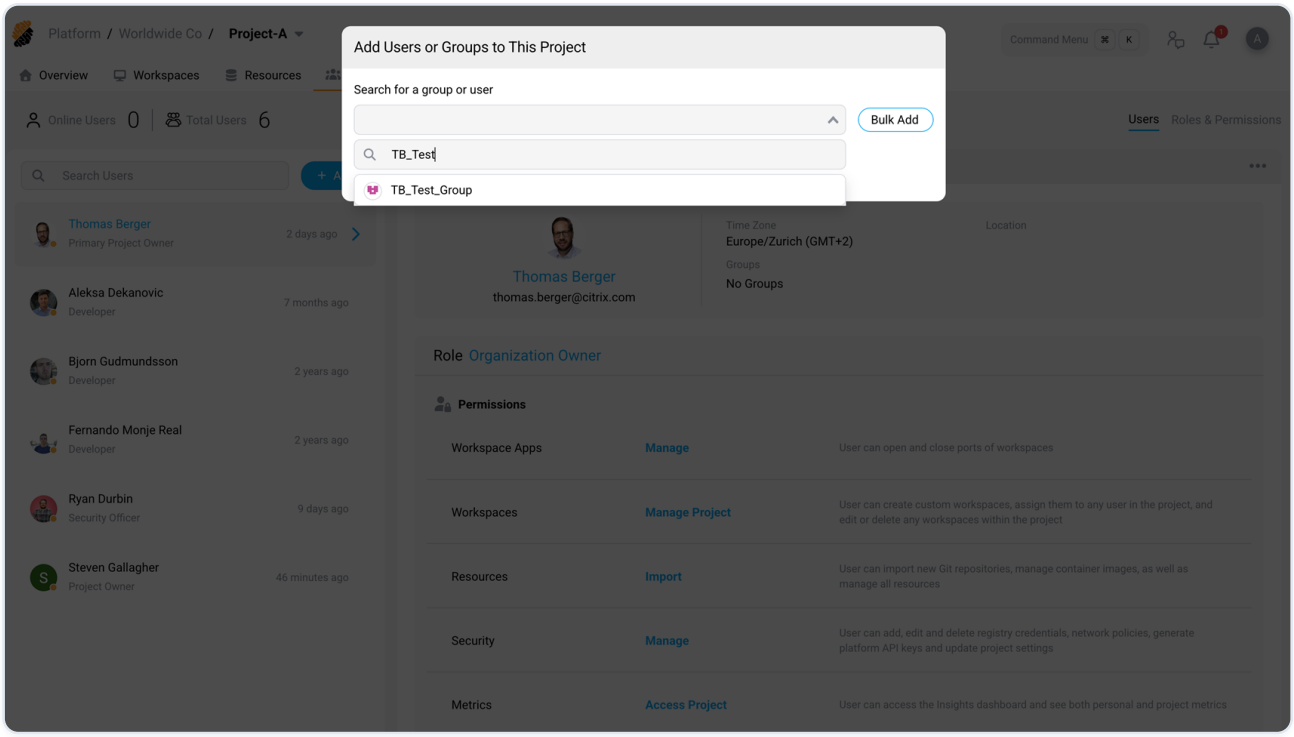
El usuario invitado aparece en la lista de selección, donde puede asignar un rol y las mismas opciones que a un usuario existente. Seleccione **Aplicar** para enviar la invitación.

> **Nota**
>
> Invitar a un usuario cuyo dominio de correo electrónico no está asociado con un proveedor de identidad configurado requiere que la función de registro de cuenta local esté habilitada. Consulte Añadir usuarios externos.

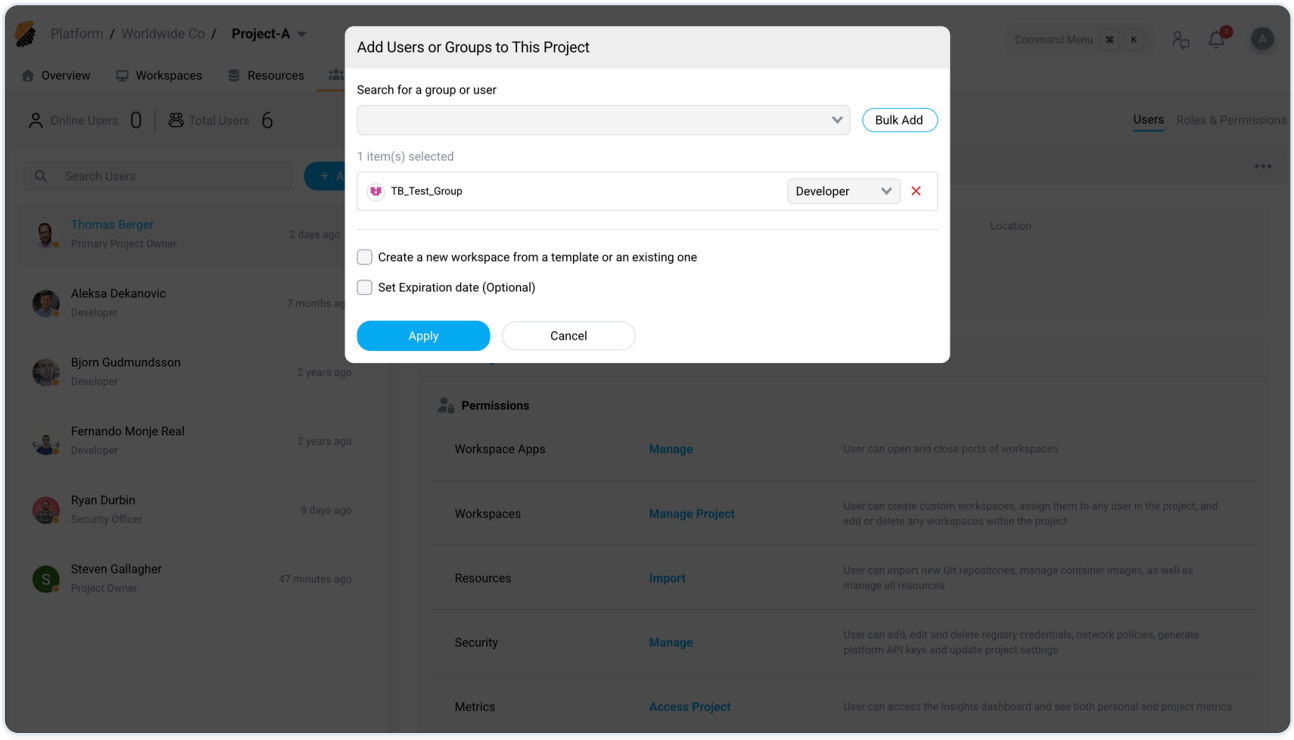
Añadir un grupo

Los grupos que existen en la plataforma se pueden añadir a un proyecto en el mismo modal.

1. En el campo **Usuario o grupo**, escriba el nombre del grupo.
2. Seleccione el grupo de los resultados filtrados. Los grupos se muestran con un icono de grupo.



El grupo aparece en la lista de selección con la misma asignación de rol y opciones que los usuarios individuales.

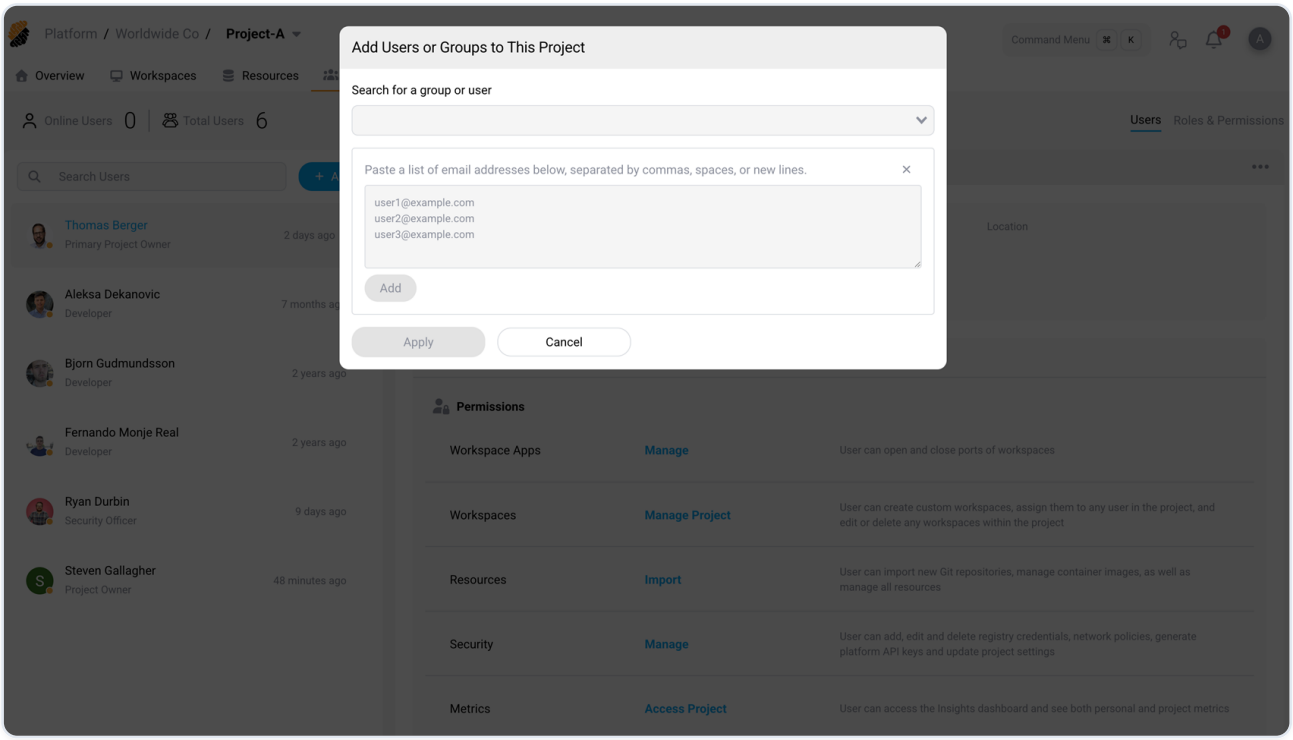


1. Seleccione **Aplicar** para añadir el grupo.

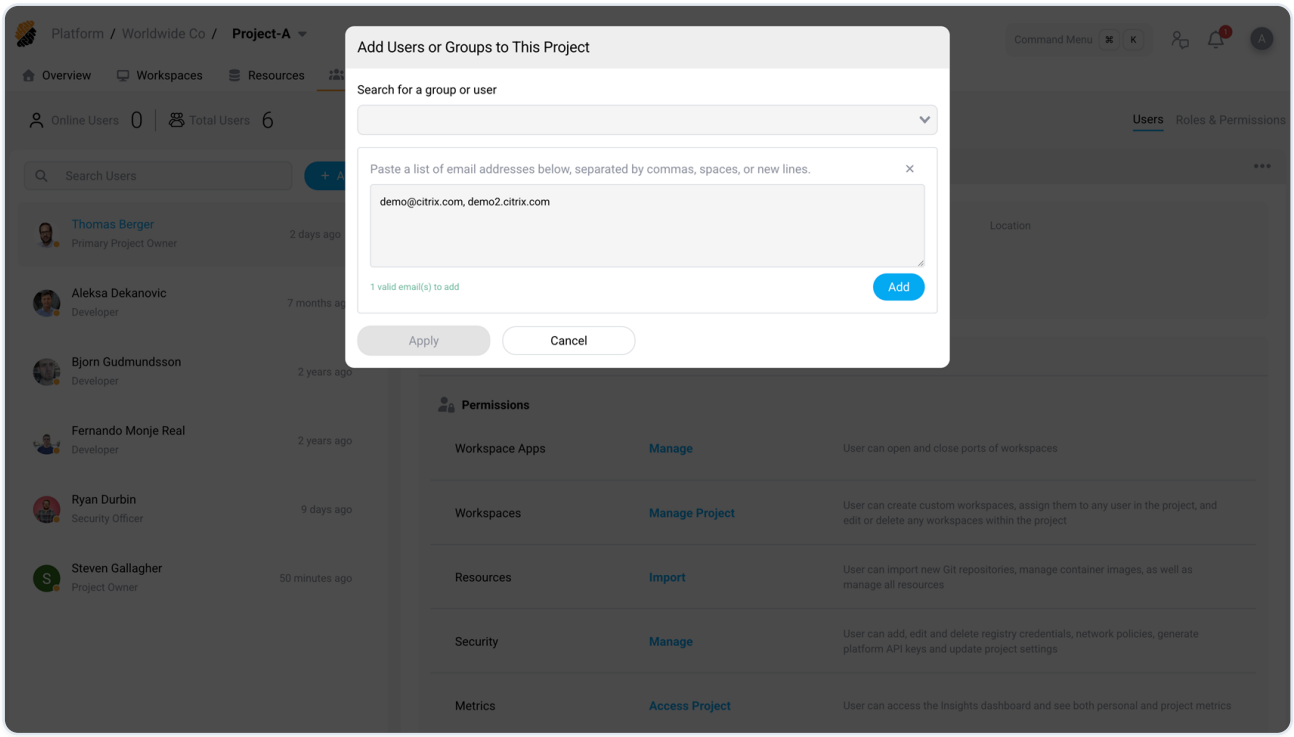
Añadir usuarios en bloque

Utilice la adición en bloque para incorporar a varios usuarios a la vez mediante su dirección de correo electrónico.

1. En el modal **Añadir usuarios o grupos a este proyecto**, seleccione **Añadir en bloque**.
2. Pegue una lista de direcciones de correo electrónico en el área de texto. Las comas, los espacios o los saltos de línea pueden separar las direcciones.



El sistema valida las direcciones a medida que escribe y muestra el número de correos electrónicos válidos.



1. Seleccione **Añadir**. El sistema valida las direcciones y añade los usuarios válidos a la lista de selección. Si alguna dirección no es válida, aparece un mensaje de error debajo del campo de entrada.
2. Asigne roles y configure opciones para los usuarios añadidos.
3. Seleccione **Aplicar** para completar la operación.

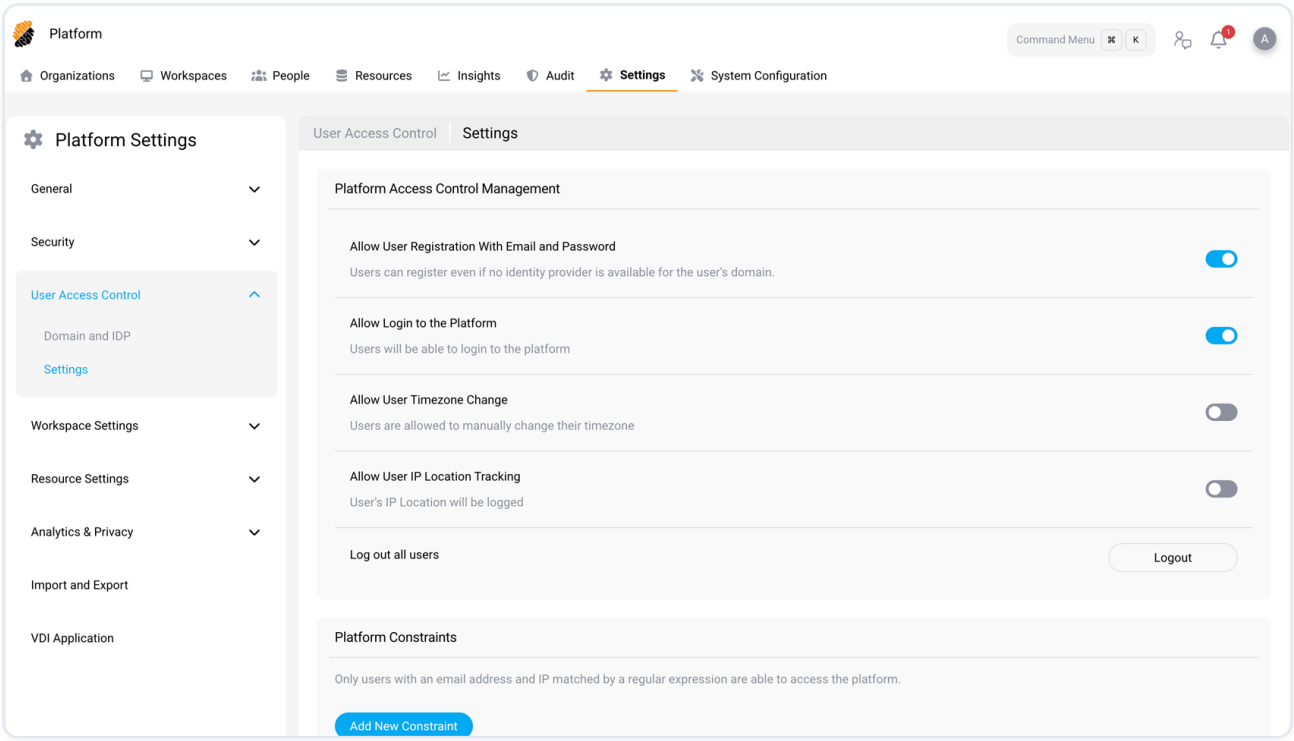
Añadir usuarios externos

Los usuarios externos son usuarios cuyo dominio de correo electrónico no está asociado con un proveedor de identidad (IdP) configurado. Añadir usuarios externos requiere una configuración a nivel de plataforma y sigue un flujo diferente al de añadir usuarios de plataforma existentes.

Habilitar el registro de cuentas locales

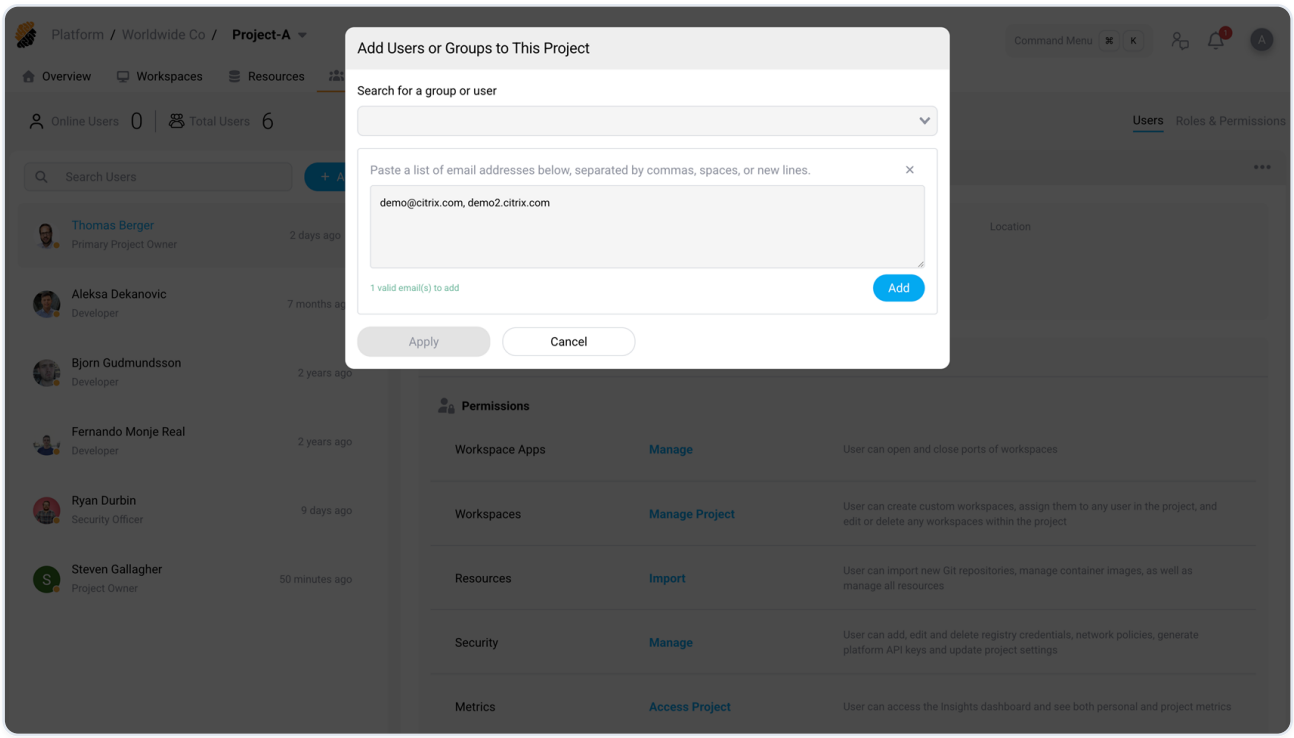
Antes de que se puedan añadir usuarios externos, un administrador de plataforma o un oficial de seguridad debe habilitar **Permitir el registro de usuarios con correo electrónico y contraseña** en **Plataforma > Configuración > Control de acceso de usuarios > Configuración**.

Cuando esta configuración está habilitada, Citrix SecurSpaces™ crea una cuenta local para los usuarios externos. El usuario puede iniciar sesión con correo electrónico y contraseña en lugar del IdP de la organización.



Añadir usuarios externos a un proyecto

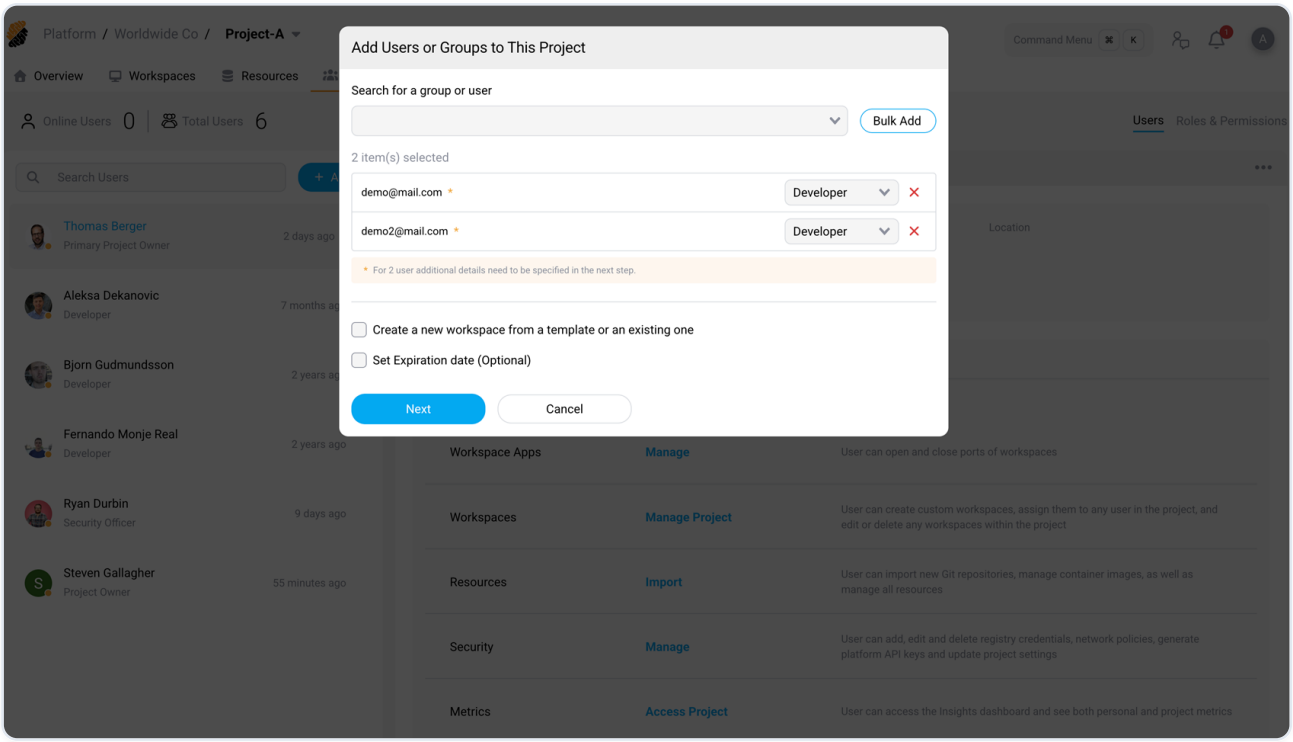
1. Abra la ventana modal **Añadir usuarios o grupos a este proyecto** (consulte Añadir usuarios o grupos a un proyecto).
2. Seleccione **Añadir en bloque** y pegue las direcciones de correo electrónico externas.



1. Seleccione **Añadir**. Los usuarios externos aparecen en la lista de selección marcados con un asterisco (*****) junto a su dirección de correo electrónico. Un aviso indica: "Para *N* usuarios, se deben especificar detalles adicionales en el siguiente paso."

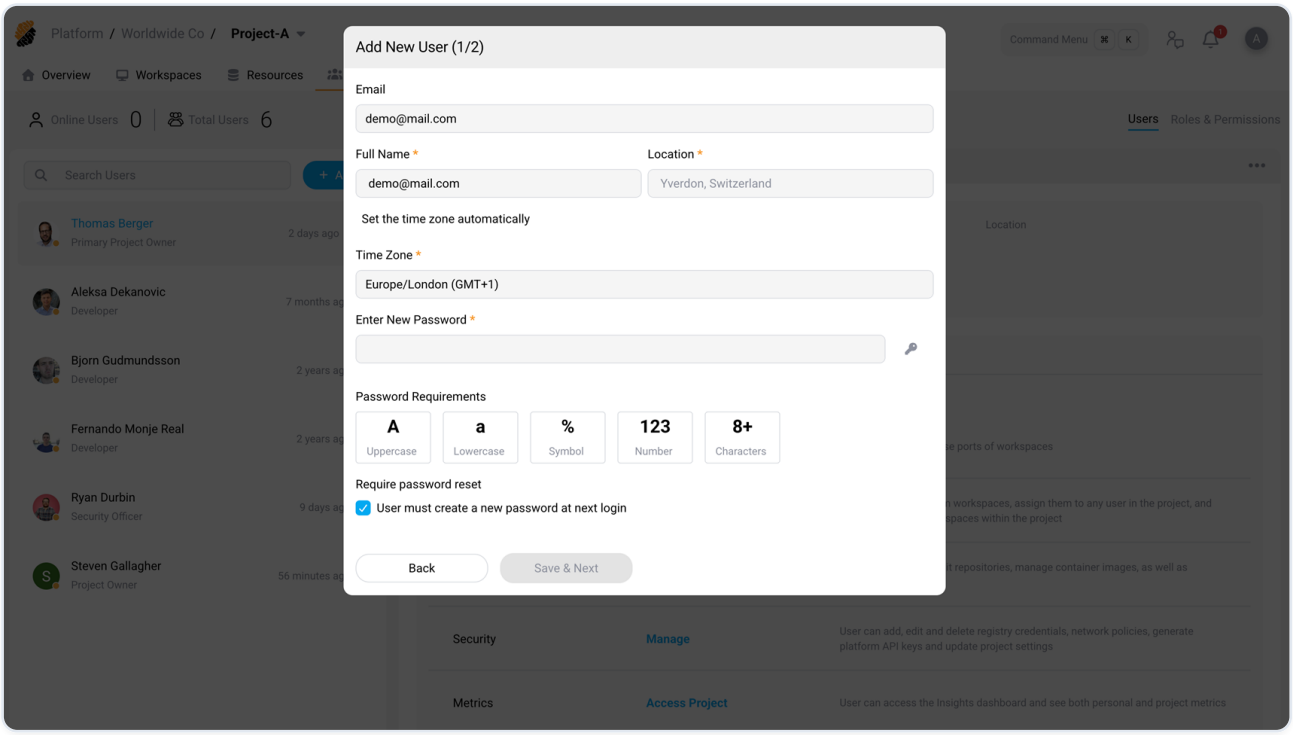
2. Asigne roles y configure las opciones según sea necesario.

El botón **Aplicar** cambia a **Siguiente** cuando hay usuarios externos.

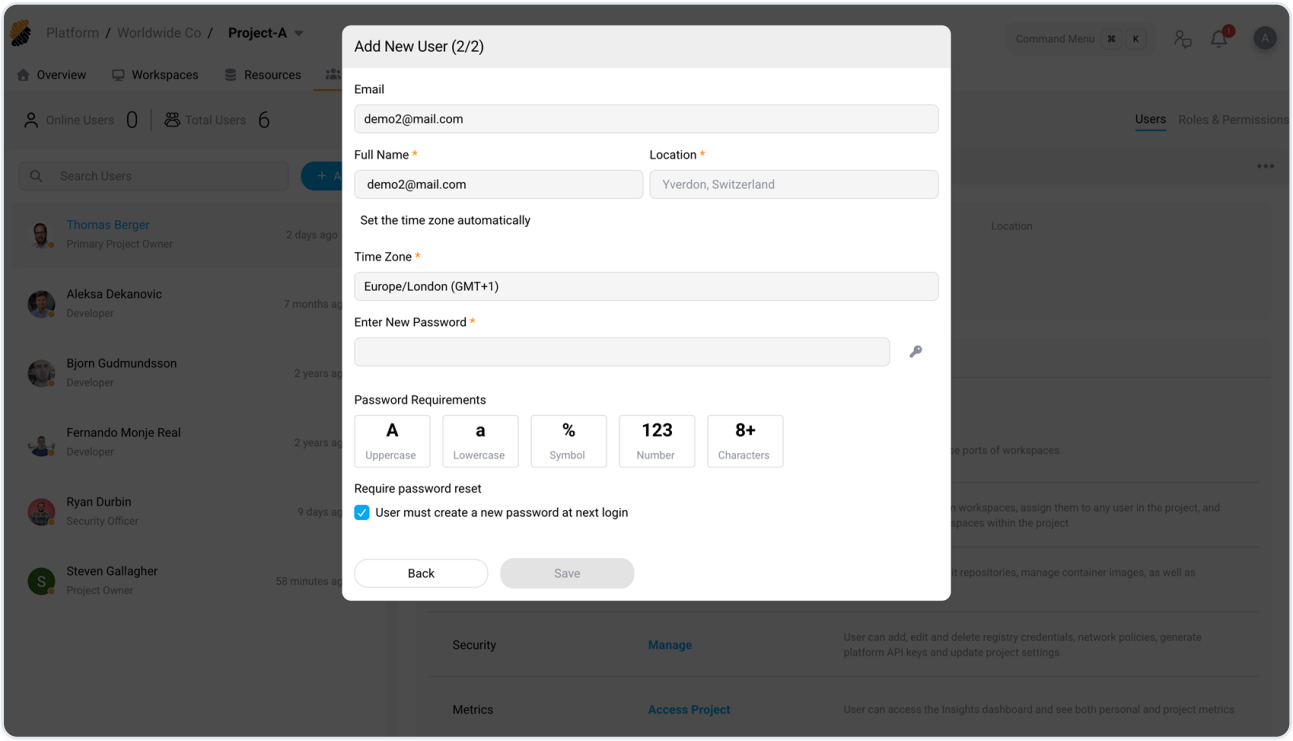


1. Seleccione **Siguiente**. SecurSpaces muestra un formulario de **Añadir nuevo usuario** para cada usuario externo. El formulario muestra un contador de pasos (por ejemplo, "1/2") y requiere:

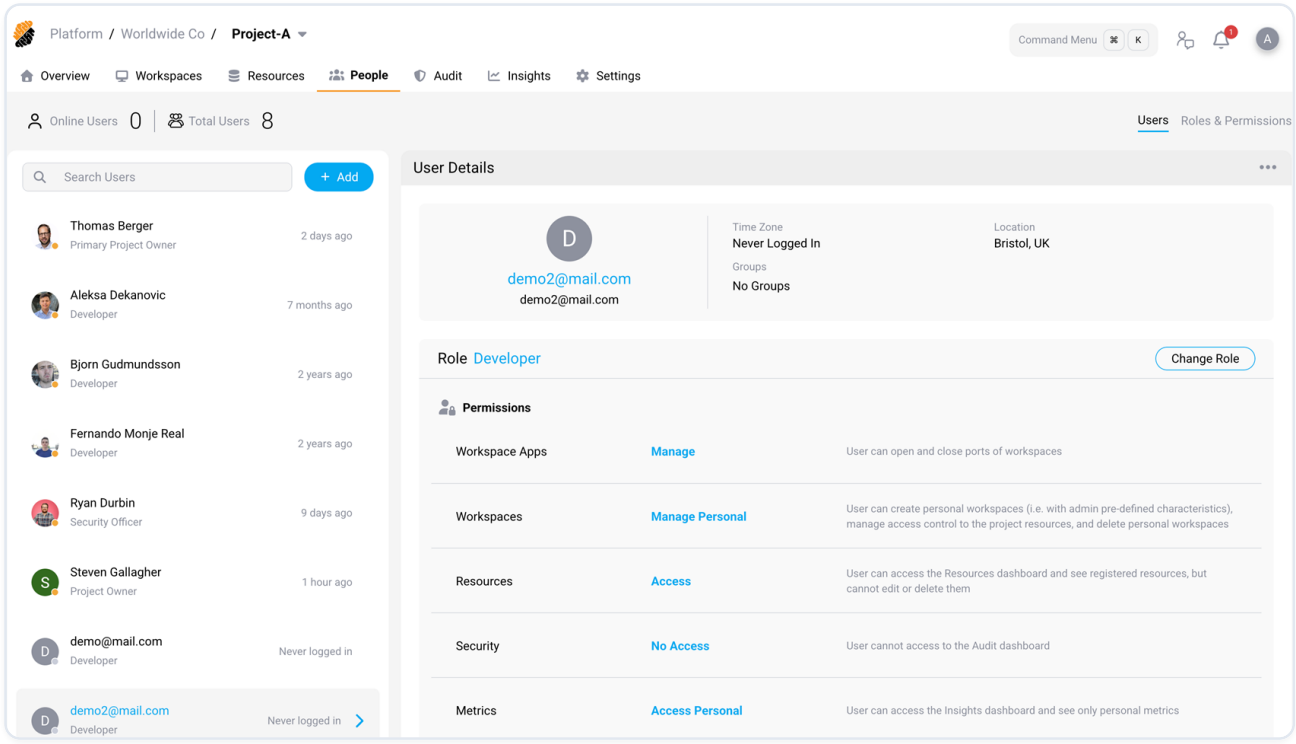
- **Nombre completo** — prellenado con la dirección de correo electrónico; editable.
- **Ubicación** — obligatorio.
- **Zona horaria** — se rellena automáticamente según la ubicación.
- **Contraseña** — debe cumplir los requisitos mostrados (mayúsculas, minúsculas, símbolo, número, más de 8 caracteres).
- **Repetir nueva contraseña** — debe coincidir con la contraseña.
- **Requerir restablecimiento de contraseña** — marcado por defecto. Cuando está habilitado, el usuario debe crear una nueva contraseña en el siguiente inicio de sesión.



1. Seleccione **Guardar y siguiente** para pasar al siguiente usuario externo. Para el último usuario del lote, el botón cambia a **Guardar**.

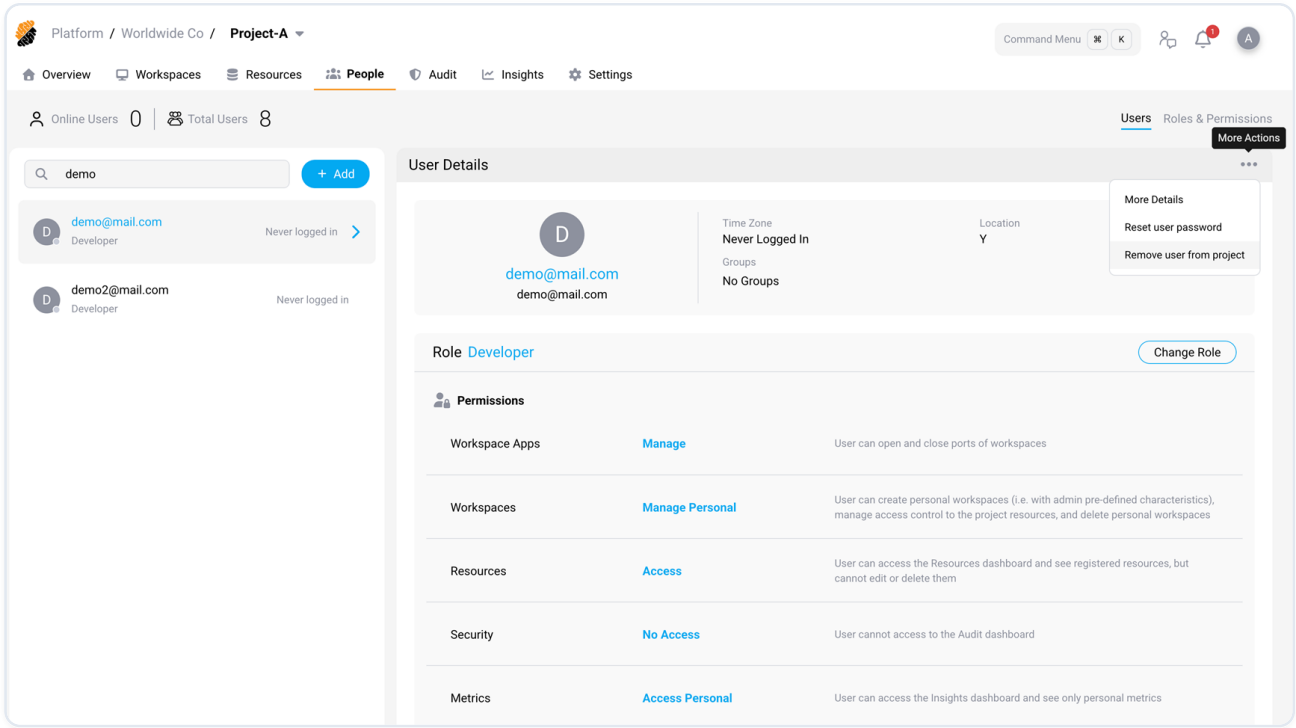


Después de guardar todos los usuarios externos, SecurSpaces crea cuentas locales y añade los usuarios al proyecto. Hasta que un usuario externo inicie sesión por primera vez, el usuario aparece en la lista de miembros del proyecto con el estado "Nunca ha iniciado sesión".

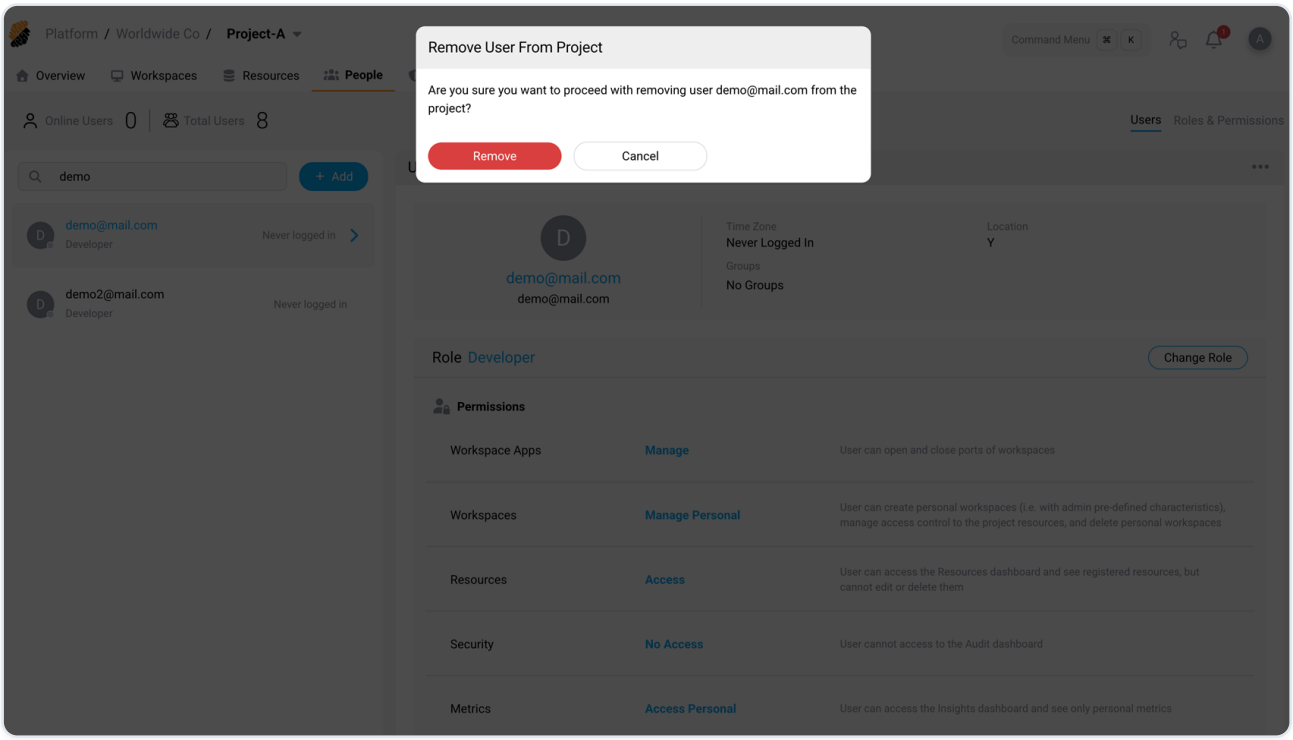


Eliminar un usuario de un proyecto

1. En la página **Personas**, seleccione un usuario de la lista de usuarios.
2. En el panel **Detalles del usuario**, seleccione el menú **...** (Más acciones) en la parte superior derecha.
3. Seleccione **Eliminar usuario del proyecto**.



Un cuadro de diálogo de confirmación le pide que confirme la eliminación.



Si el usuario posee espacios de trabajo en el proyecto, el cuadro de diálogo advierte que al eliminar al usuario se eliminarán esos espacios de trabajo. Puede anular la selección de espacios de trabajo individuales para conservarlos antes de confirmar.

1. Seleccione **Eliminar** para confirmar.

El usuario pierde el acceso al proyecto y a todos los recursos asociados. El usuario permanece en la base de datos de la plataforma. Para eliminar completamente a un usuario de la plataforma, un administrador de la plataforma o un oficial de seguridad debe eliminar al usuario de la página Personas a nivel de plataforma.

Permisos

ACCIÓN	PERMISO REQUERIDO
Añadir usuarios o grupos a un proyecto	Miembros – Administrar
Eliminar un usuario de un proyecto	Miembros – Administrar
Cambiar el rol de un usuario	Miembros – Administrar
Ver miembros del proyecto	Miembros – Acceso

Información relacionada

- Roles y permisos

- Usuarios
- Personas

Roles and permissions

El acceso en Citrix SecurSpaces™ se concede a través de **roles**. Un rol es un conjunto de permisos con nombre, y cada miembro de un proyecto tiene uno. Los roles están vinculados al proyecto, por lo que la misma persona puede tener diferentes roles en diferentes proyectos.

Esta página es la referencia de lo que permite cada rol y permiso. Otros artículos enlazan aquí en lugar de repetirlo.

Los roles y permisos se muestran en la página Personas. Un propietario de proyecto puede crear roles o cambiar los existentes desde el panel de control de acceso.

> **Advertencia:**

> Los roles deciden quién puede acceder a su código fuente, secretos y configuraciones de seguridad. Asígnelos según el principio de mínimo privilegio.

Por qué una característica está oculta

SecurSpaces oculta lo que su rol no puede usar en lugar de mostrarlo deshabilitado. Si una página, botón o entrada de menú descrita en esta documentación no está presente, la razón habitual es que su rol no tiene el permiso para ello.

Algunas características también están ocultas por razones no relacionadas con su rol, como que una configuración de plataforma esté desactivada o que una integración opcional no esté configurada. El artículo de cada característica indica cuál se aplica.

Para ver sus propios permisos, abra la página Personas y consulte su rol.

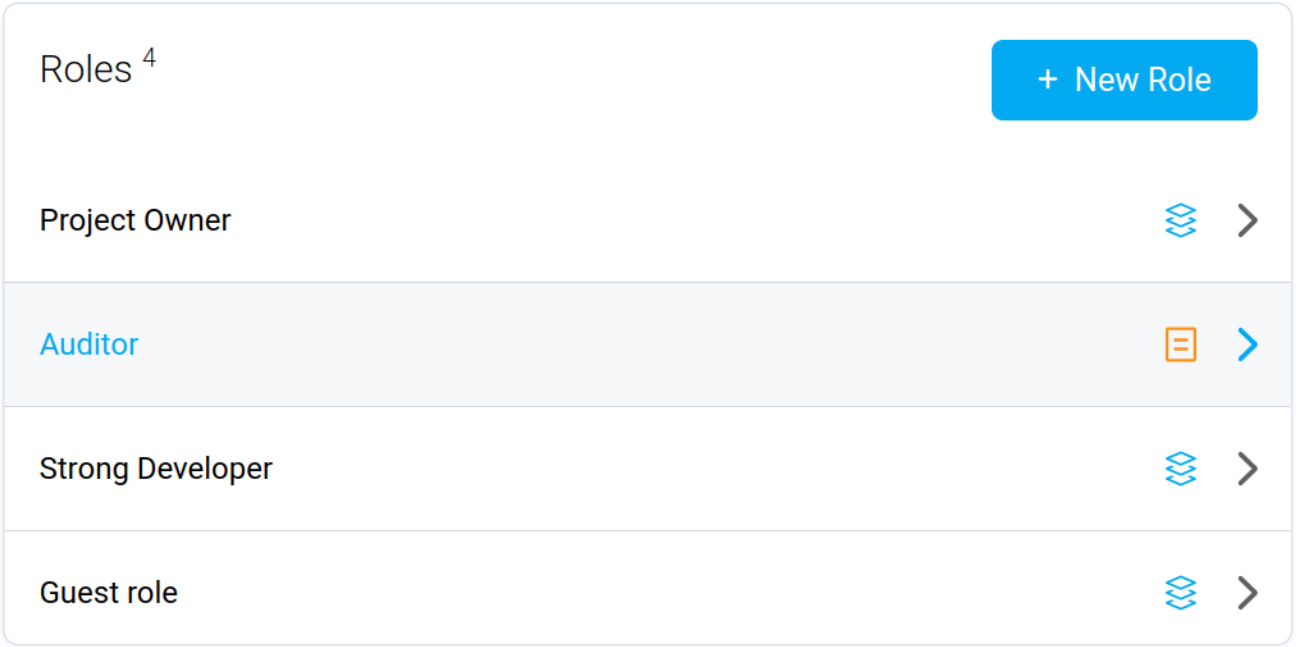
Roles predeterminados

Un nuevo proyecto tiene cuatro roles.

ROL	DESTINADO A
Invitado	Alguien que necesita ver un proyecto sin cambiar nada

ROL	DESTINADO A
Desarrollador	Desarrollo diario en sus propios espacios de trabajo
Administrador	Gestión del proyecto: sus espacios de trabajo, recursos y miembros
Propietario del proyecto	Gestión del proyecto y su configuración de seguridad

Un propietario de proyecto difiere de un gestor de dos maneras. Un gestor no tiene permiso de **Seguridad**, por lo que las políticas de red, las credenciales de registro, las claves API de la plataforma y la configuración del proyecto están fuera de su alcance. Un gestor tampoco puede gestionar roles, por lo que no puede crear ni editar roles, ni transferir la propiedad. Un gestor aún puede gestionar espacios de trabajo, recursos y miembros.



Qué incluye cada rol predeterminado

PERMISO	INVITADO	DESARROLLADOR	ADMINISTRADOR	PROPIETARIO DEL PROYECTO
Aplicaciones del espacio de trabajo	Gestionar	Gestionar	Gestionar	Gestionar

PERMISO	INVITADO	DESARROLLADOR	ADMINISTRADOR	PROPIETARIO DEL PROYECTO
Espacios de trabajo	Acceso	Gestionar personal	Gestionar proyecto	Gestionar proyecto
Recursos	Acceso	Acceso	Importar	Importar
Recursos regulados	No	Sí	Sí	Sí
Recursos confidenciales	No	Sí	Sí	Sí
Métricas	Sin acceso	Acceso personal	Acceso al proyecto	Acceso al proyecto
Miembros	Sin acceso	Acceso	Gestionar	Gestionar
Seguridad	Sin acceso	Sin acceso	Sin acceso	Gestionar
Gestionar roles y permisos	No	No	No	Sí

Nota:

Un administrador de plataforma puede deshabilitar el rol predefinido de **Propietario del proyecto** y nombrar un reemplazo, por lo que una implementación puede diferir de esta tabla. Un rol deshabilitado no puede asignarse a nadie, aunque los miembros que ya lo tienen lo conservan. Consulta el panel de control de acceso de tu proyecto.

Permisos

Un rol establece un nivel para cada uno de los seis permisos, más tres configuraciones separadas y una casilla de verificación que permite la gestión de roles.

Aplicaciones del espacio de trabajo

Controla el acceso a las aplicaciones que se ejecutan dentro de los espacios de trabajo.

NIVEL	EL USUARIO PUEDE
Sin acceso	No abrir puertos del espacio de trabajo para ver aplicaciones, ni ver aplicaciones compartidas por otros
Acceso	Ver aplicaciones compartidas con ellos por otros usuarios
Gestionar	Abrir y cerrar puertos en los espacios de trabajo

Espacios de trabajo

Controla lo que el usuario puede hacer con los espacios de trabajo.

NIVEL	EL USUARIO PUEDE
Sin acceso	No acceder a los espacios de trabajo
Acceso	Usar los espacios de trabajo que se les han asignado, pero no editar propiedades, cambiar el acceso a los recursos ni eliminarlos
Administrar personal	Crear espacios de trabajo personales con características predefinidas por un administrador, administrar el acceso a los recursos del proyecto y eliminar sus propios espacios de trabajo
Administrar proyecto	Crear espacios de trabajo personalizados, asignarlos a cualquier persona del proyecto y editar o eliminar cualquier espacio de trabajo del proyecto

Recursos

Controla el panel de Recursos: repositorios, secretos, servicios conectados, depósitos de datos y puntos de montaje.

NIVEL	EL USUARIO PUEDE
Sin acceso	No abrir el panel de Recursos

NIVEL	EL USUARIO PUEDE
Acceso	Ver los recursos registrados, pero no editarlos ni eliminarlos
Gestionar	Ver, editar y eliminar repositorios de proyectos, secretos, servicios externos y depósitos de datos
Importar	Todo lo que permite Gestionar, además de importar repositorios Git, imágenes de contenedor y aplicaciones conectadas SAML

Seguridad

Controla el panel de Auditoría y la configuración de seguridad del proyecto.

NIVEL	EL USUARIO PUEDE
Sin acceso	No abrir el panel de Auditoría
Acceso	Abrir el panel de Auditoría y ver las políticas de red, pero no añadirlas, editarlas ni eliminarlas
Gestionar	Añadir, editar y eliminar credenciales de registro y políticas de red, generar claves API de plataforma y actualizar la configuración del proyecto

Métricas

Controla el panel de Insights.

NIVEL	EL USUARIO PUEDE
Sin acceso	No abrir el panel de Insights
Acceso personal	Ver sus propias métricas
Acceso al proyecto	Ver sus propias métricas y las del proyecto

Miembros

Controla el panel de Personas.

NIVEL	EL USUARIO PUEDE
Sin acceso	No abrir el panel de Personas
Acceso	Ver miembros del proyecto
Gestionar	Añadir y eliminar miembros del proyecto, y asignar o cambiar sus roles, hasta el nivel del rol que el propio usuario posee

Gestionar roles y permisos

Una casilla de verificación al pie del editor de roles en lugar de un nivel en una escala, etiquetada como **El usuario puede gestionar roles y permisos de otros usuarios (habilitar todos los permisos)**. Permite la administración del proyecto: crear, editar y eliminar roles, transferir la propiedad del proyecto y restaurar espacios de trabajo eliminados.

CONFIGURACIÓN	EL USUARIO PUEDE
El usuario puede gestionar roles y permisos de otros usuarios	Crear, editar y eliminar roles, transferir la propiedad del proyecto y restaurar espacios de trabajo eliminados

Solo el rol de **Propietario del proyecto** lo tiene seleccionado por defecto. Está separado del permiso de **Miembros**: un gestor puede añadir miembros y establecer sus roles, pero no puede crear ni editar los roles por sí mismo.

> **Importante:**

> Al seleccionar esta casilla, también se elevan todos los demás permisos del rol a su nivel más alto, que es lo que "habilitar todos los permisos" en la etiqueta significa. Las aplicaciones de espacio de trabajo, los espacios de trabajo, los recursos, la seguridad, las métricas y los miembros se mueven a su máximo, y las configuraciones reguladas y confidenciales se activan. Desmarcar la casilla de nuevo restaura los niveles que tenía el rol antes. Trátelo como si concediera todo en el proyecto, no solo la gestión de roles.

Configuraciones separadas

Estos son interruptores en el rol en lugar de niveles en una escala.

CONFIGURACIÓN	EFECTO
Recursos regulados	El rol puede acceder a recursos marcados como regulados, lo que significa que están sujetos a una regulación
Recursos confidenciales	El rol puede acceder a recursos marcados como confidenciales, como la propiedad intelectual
Requerir plantillas para la creación de espacios de trabajo	El rol solo puede crear espacios de trabajo a partir de una plantilla. La creación de un espacio de trabajo personalizado o la copia de uno existente están bloqueadas.

Límites en la delegación de acceso

Un usuario con el permiso de **Miembros** establecido en **Administrar** puede incorporar personas al proyecto y asignarles sus roles, pero no usar eso para escalar. Se aplican cuatro reglas, y la plataforma las aplica todas.

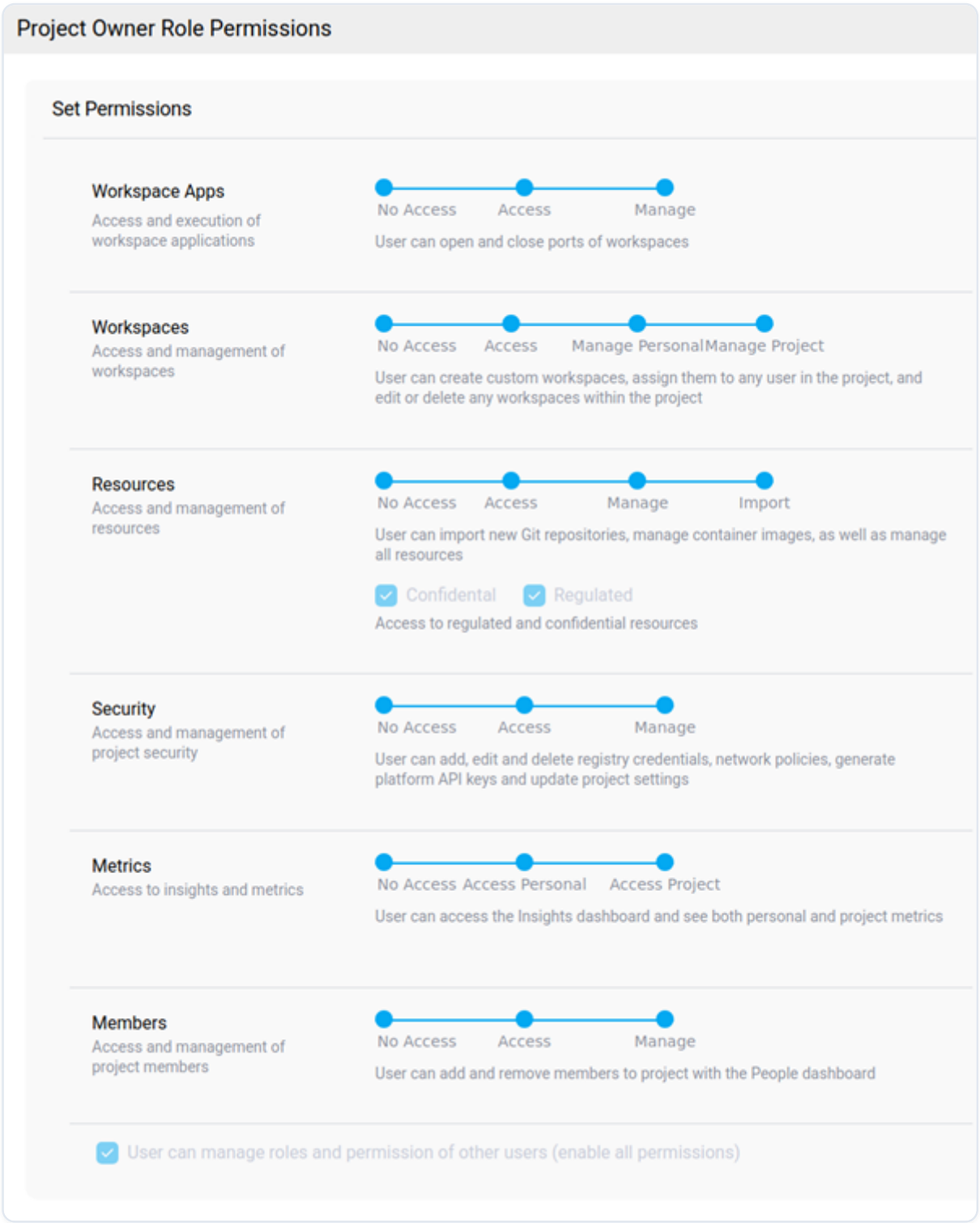
- **No puede otorgar un rol superior al suyo.** Cuando asigna un rol, se compara con su propio rol en ese proyecto, permiso por permiso. Si el rol que está asignando es superior en cualquier permiso individual —incluida la gestión de roles y las configuraciones reguladas y confidenciales—, la asignación se deniega, incluso si es inferior en todos los demás.
- **El límite se aplica al rol que otorga, no a la persona sobre la que actúa.** Le impide crear a alguien más poderoso que usted. No le impide actuar sobre un miembro que ya tiene más poder que usted: un gestor de miembros aún puede cambiar el rol de un gestor a uno inferior o eliminarlo del proyecto.
- **No puedes cambiar tu propio rol** y no puedes eliminarte de un proyecto.
- **No puedes eliminar al propietario del proyecto.** La propiedad debe transferirse primero, lo que requiere la casilla de verificación de gestión de roles.

> **Nota:**
>
> Estos límites se aplican a los roles del proyecto. Un administrador de plataforma, un oficial de seguridad o el propietario de la organización del proyecto no están sujetos a ellos.

Crear un rol

Requiere un rol con **El usuario puede gestionar roles y permisos de otros usuarios** seleccionado, que es el que tiene el rol de **Propietario del proyecto**. Un gestor no puede crear ni editar roles: la gestión de roles es independiente del permiso de **Miembros** que rige la adición y eliminación de miembros.

Abre el panel de control de acceso desde la página Personas, añade un rol, nómbralo y establece cada permiso. Un rol creado a nivel de proyecto solo está disponible en ese proyecto.



Información relacionada

- Personas
- Roles de plataforma
- Panel de auditoría
- Políticas de red
- Recursos del proyecto

Projects and organizations

Configuración general para un proyecto y para la organización que lo contiene, y las ventanas de recuperación que se aplican cuando se elimina cualquiera de ellos.

Para saber qué son los proyectos y las organizaciones y cómo se relacionan, consulte Proyectos y Organizaciones.

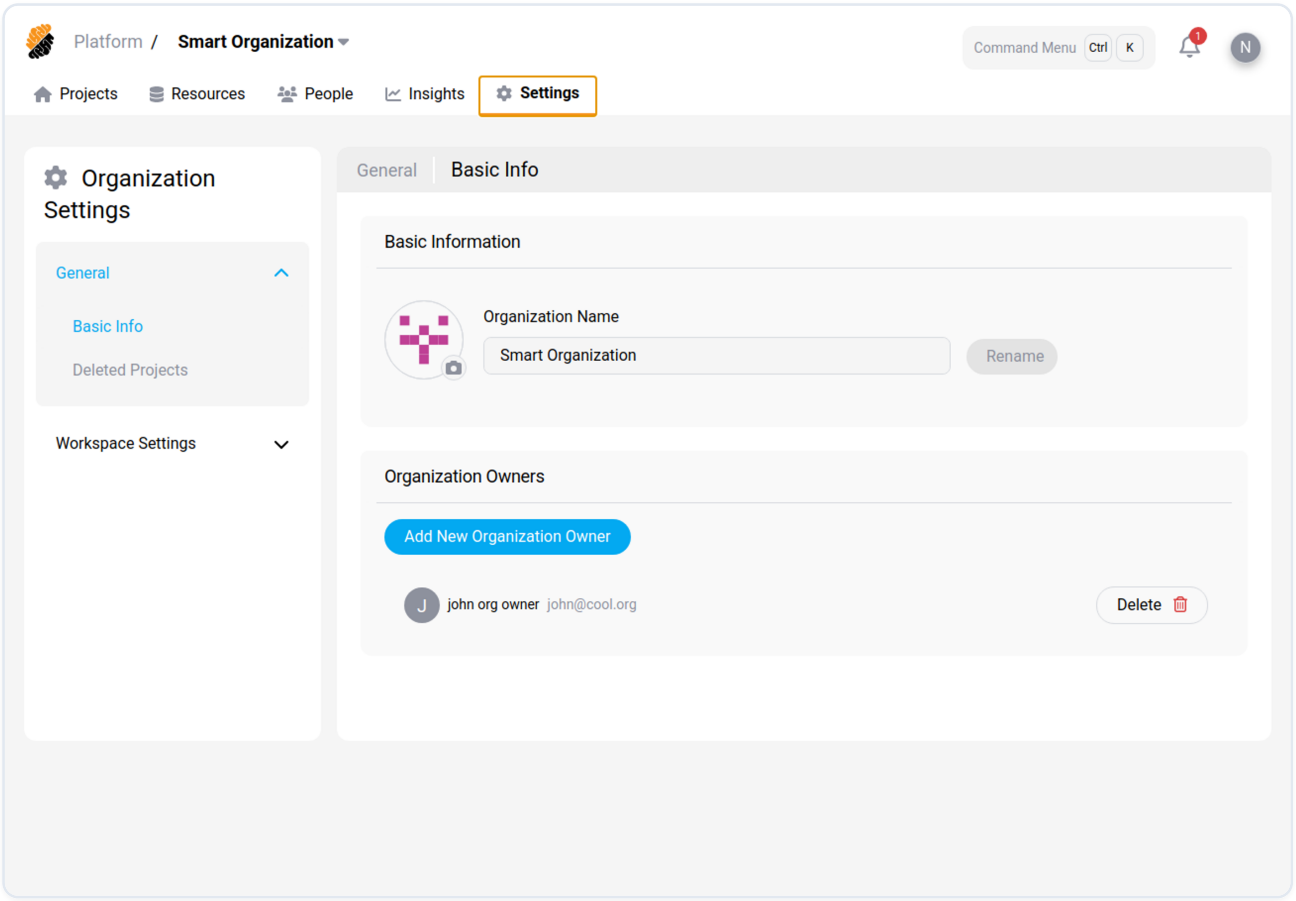
Ubicación de cada configuración

CONFIGURACIÓN	ORGANIZACIÓN	PROYECTO
Renombrar	sí	sí
Recuperar un proyecto eliminado	sí	—
Recuperar un espacio de trabajo eliminado	—	sí
Política del espacio de trabajo, incluyendo la configuración de seguridad y red	Política del espacio de trabajo de la organización	Política del espacio de trabajo

La configuración de la organización se aplica a cada proyecto dentro de la organización, por lo que es el lugar para estandarizar la configuración en lugar de repetirla proyecto por proyecto.

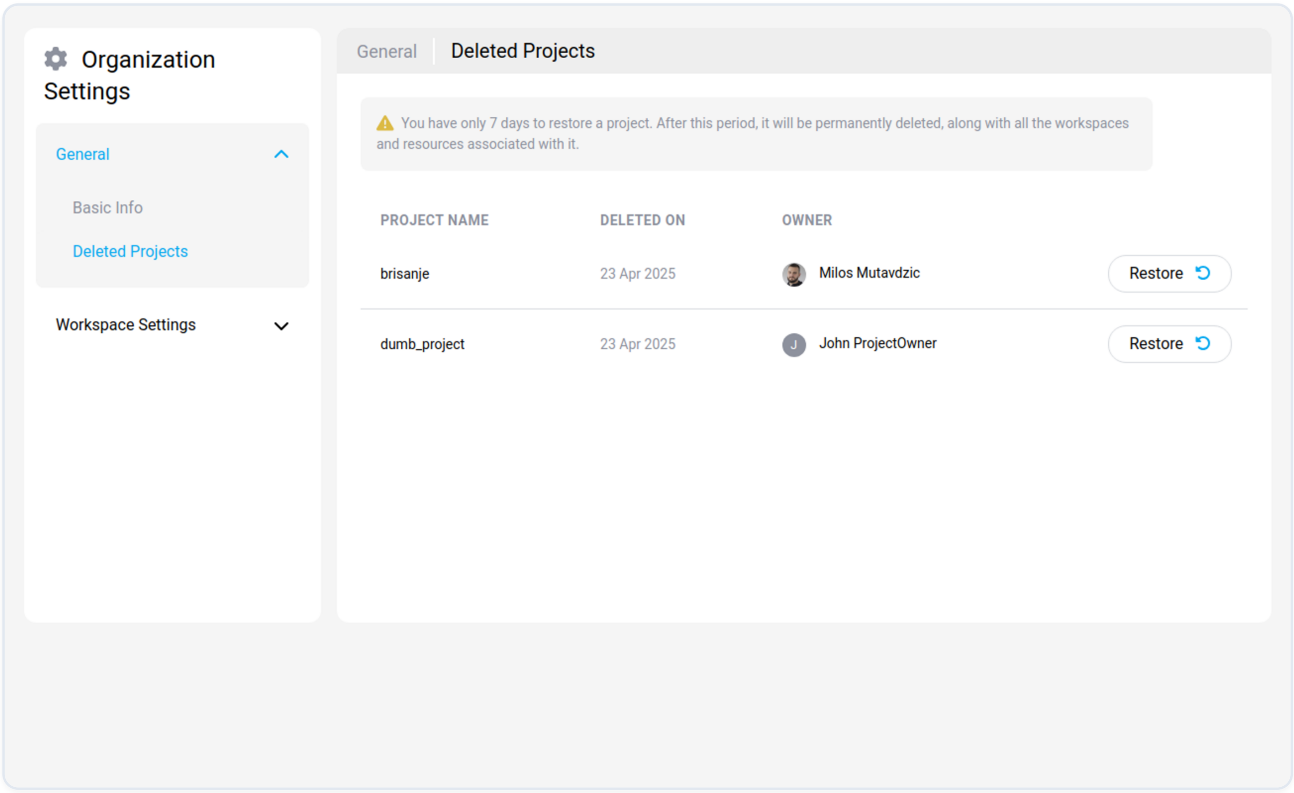
Configuración de la organización

La configuración de la organización es el punto de control para cada proyecto de la organización. Definir una configuración aquí proporciona una base consistente que cada proyecto nuevo y existente adopta.



Recuperar un proyecto eliminado

Un proyecto eliminado puede restaurarse durante **7 días**. Después de ese período, se elimina permanentemente, junto con sus espacios de trabajo, secretos, imágenes, repositorios y otros recursos.

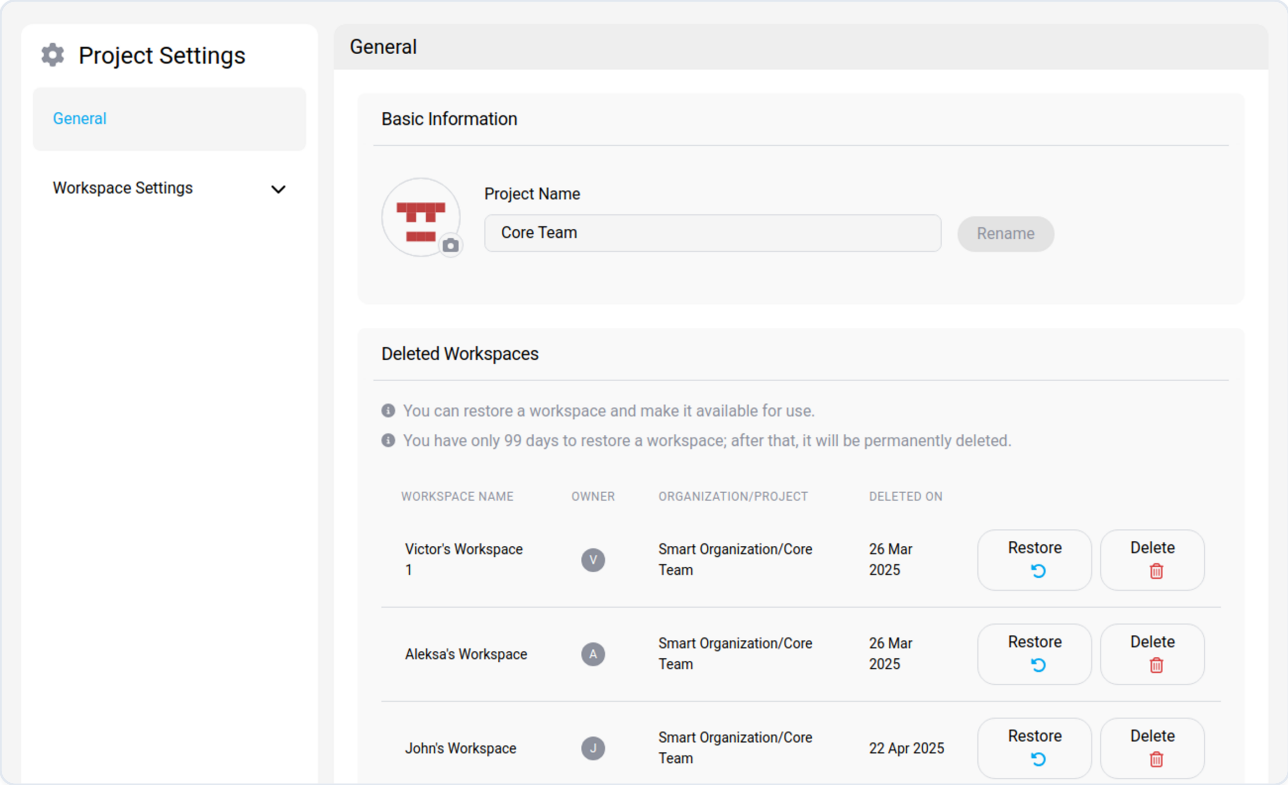


Nota:

La limpieza se ejecuta según un cronograma y no en el momento exacto en que se cierra la ventana, por lo que un proyecto puede permanecer visible un poco más allá de los 7 días. No confíe en el tiempo adicional.

Configuración del proyecto

En **Información básica** puede cambiar el nombre del proyecto.



Recuperar un espacio de trabajo eliminado

Un espacio de trabajo eliminado se puede restaurar durante un período que establezca el administrador de la plataforma, de **1 a 99 días**. Después de ese período, se elimina permanentemente.

El período de retención se configura a nivel de plataforma en Política de espacio de trabajo, no por proyecto.

> **Nota:**
>
> Un punto de montaje no se puede eliminar mientras un espacio de trabajo eliminado en la papelera de reciclaje todavía lo esté utilizando, porque ese espacio de trabajo aún se puede restaurar. Consulte Límites y comportamiento del punto de montaje.

Información relacionada

- Proyectos
- Organizaciones
- Política de espacio de trabajo
- Incorporar desarrolladores

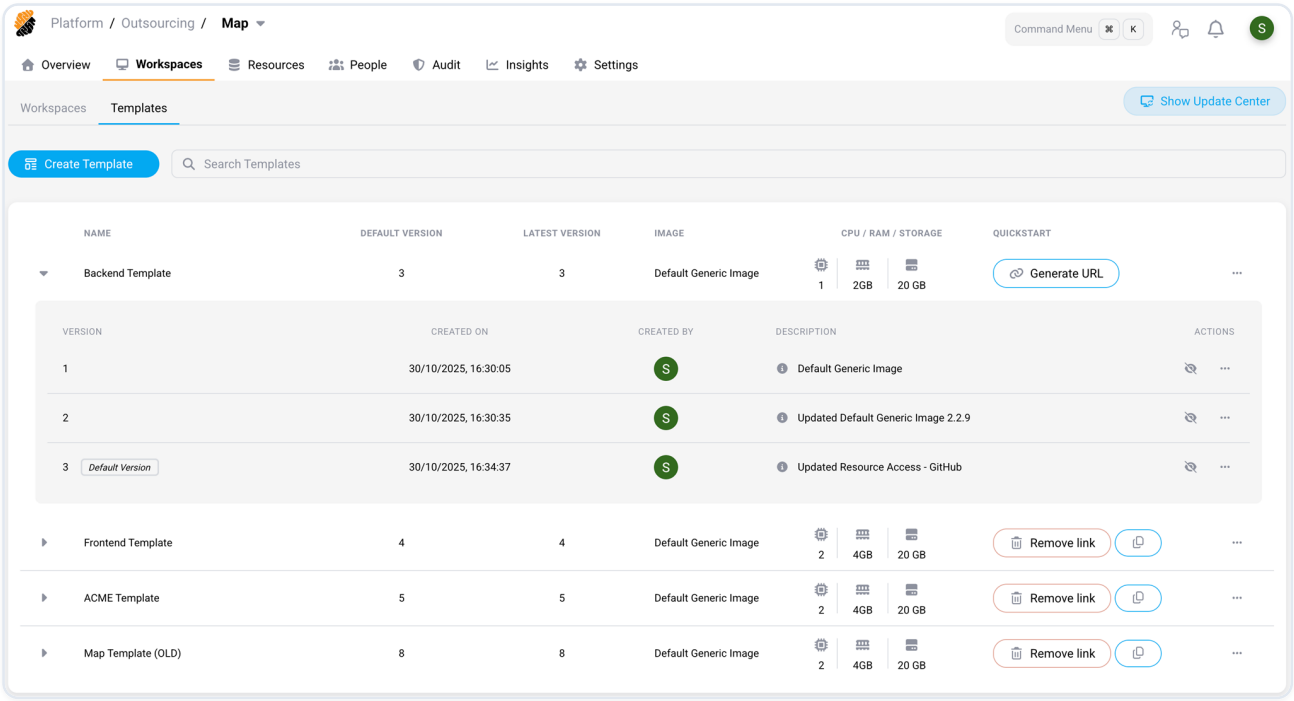
Templates

Las **plantillas** de espacio de trabajo ayudan a agilizar la incorporación de proyectos al eliminar la necesidad de una configuración manual del espacio de trabajo. Cada plantilla define todos los parámetros de configuración necesarios, incluida la configuración del espacio de trabajo, los repositorios, los secretos, los scripts de inicio y las políticas de seguridad, lo que garantiza la coherencia en todos los espacios de trabajo dentro de un proyecto. Utilice la función de inicio rápido para crear un nuevo espacio de trabajo con un solo clic desde una fuente externa, como un repositorio de código o un portal de ingeniería.

- Ver plantillas
- Plantilla integrada
- Crear una plantilla
- Crear una nueva versión de una plantilla
- Rastrear qué versión de plantilla utiliza un espacio de trabajo
- Actualizar un espacio de trabajo a la versión de plantilla predeterminada
- Archivar una plantilla
- Inicio rápido
- Duplicar una plantilla

Ver plantillas

Las plantillas se muestran en la sección **Plantillas** de la página de espacios de trabajo. Cada plantilla puede tener varias versiones, que son visibles al expandir el icono de chevron en el lado izquierdo de la pantalla.



Una plantilla se define por las siguientes características:

- **Información básica**: Nombre, imagen de contenedor, configuración de CPU/RAM/ Almacenamiento y descripción.
- **Nivel de clasificación**: Confidencial o regulado.
- **Configuración del espacio de trabajo**: Todos los demás elementos que describen un espacio de trabajo.

Plantilla integrada

Cada nuevo proyecto incluye una plantilla integrada. Se proporciona como un punto de partida funcional en lugar de un conjunto completo, por lo que la mayoría de los equipos crean sus propias plantillas a partir de ella o de una imagen personalizada.

NOMBRE	IMAGEN	CPU / RAM / ALMACENAMIENTO	DESCRIPCIÓN
Plantilla de VSCode monitorizada	Imagen genérica predeterminada	2 CPU / 4 GB / 20 GB	Crea un contenedor Ubuntu completamente actualizado con tráfico y portapapeles monitorizados.

La plantilla se crea con la política de red **Monitorizar tráfico (predeterminada)** aplicada. Para ver las otras políticas disponibles para un proyecto, consulte Políticas de red.

Más imágenes para crear plantillas

Citrix publica Dockerfiles de ejemplo e imágenes precompiladas que puede usar o adaptar:

- strong-network/images en GitHub — Dockerfiles y scripts de compilación, incluyendo la imagen base genérica y variantes específicas de lenguaje y de escritorio.
- strongnetwork en Docker Hub — imágenes precompiladas a las que puedes hacer referencia directamente.

Para que uno esté disponible para tu proyecto, consulta Imágenes de contenedor.

Crear una plantilla

Requiere el permiso Espacios de trabajo establecido en **Gestionar proyecto**.

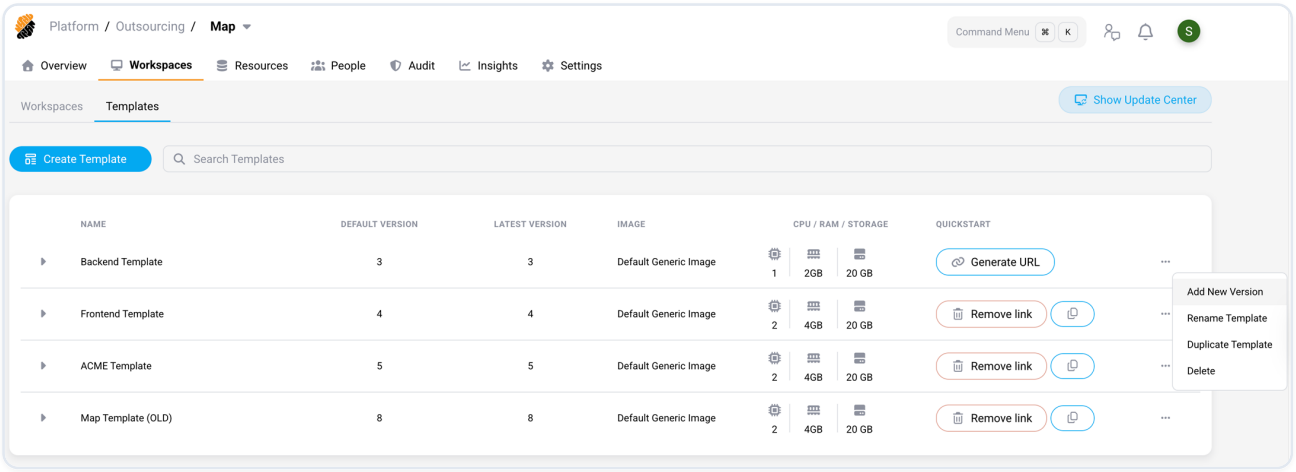
En la Página de espacios de trabajo, en la sección **Plantillas**, puedes crear una plantilla haciendo clic en el botón **Crear plantilla**. Seguirías los mismos pasos que durante la configuración inicial de un espacio de trabajo.

> **Nota**

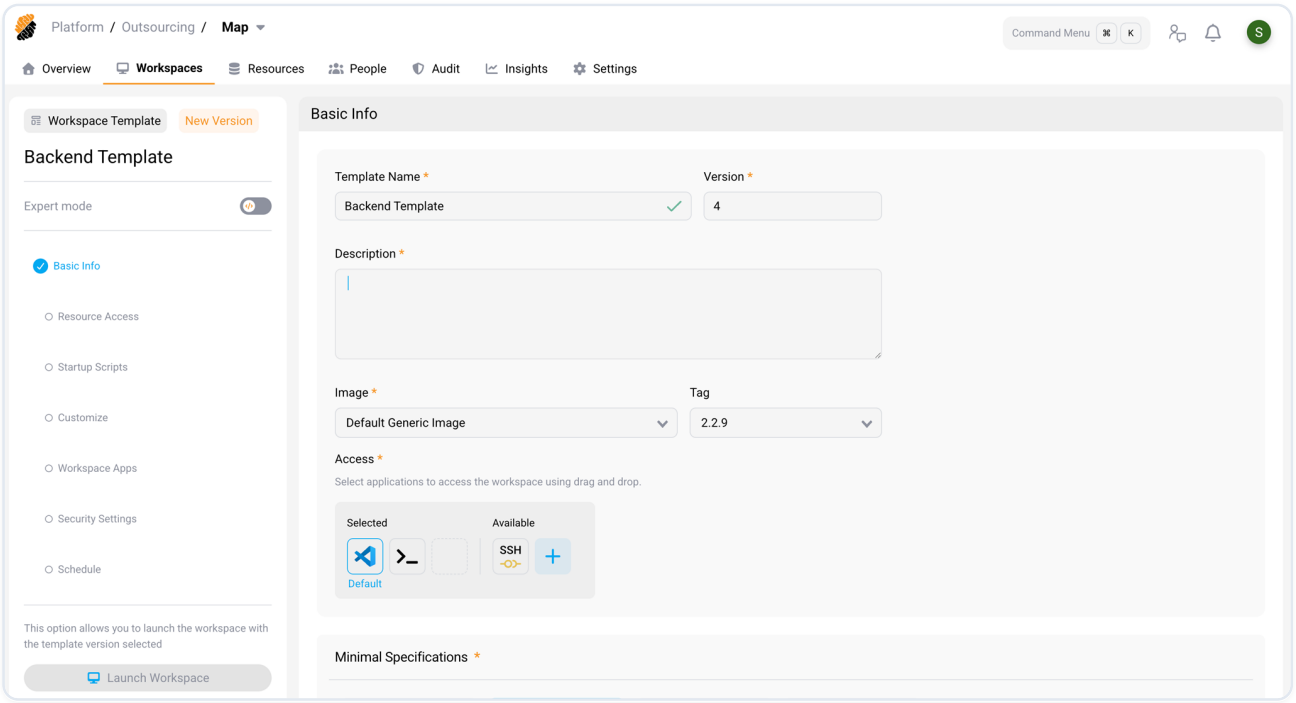
> Los puntos de montaje solo son compatibles en la región principal, pero el editor de plantillas te permite adjuntar uno independientemente de la región en la que trabaje el proyecto. Por lo tanto, una plantilla que contenga un punto de montaje solo es utilizable en la región principal: los espacios de trabajo iniciados desde ella en cualquier otra región no pueden usar ese almacenamiento. Cuando un desarrollador crea un espacio de trabajo a partir de dicha plantilla en el proyecto, el selector de región se bloquea a la región principal. Consulta Puntos de montaje en plantillas de espacio de trabajo.

Crear una nueva versión de una plantilla

Las versiones de plantilla te permiten ajustar la configuración de una plantilla programáticamente. Se puede crear una nueva versión haciendo clic en el botón "**...**" a la derecha de una plantilla y seleccionando **Añadir nueva versión**.



Esto abre la misma interfaz de usuario de configuración que para crear un nuevo espacio de trabajo o plantilla, pero con todas las configuraciones actuales, especificadas en la versión más reciente de la plantilla, cargadas.

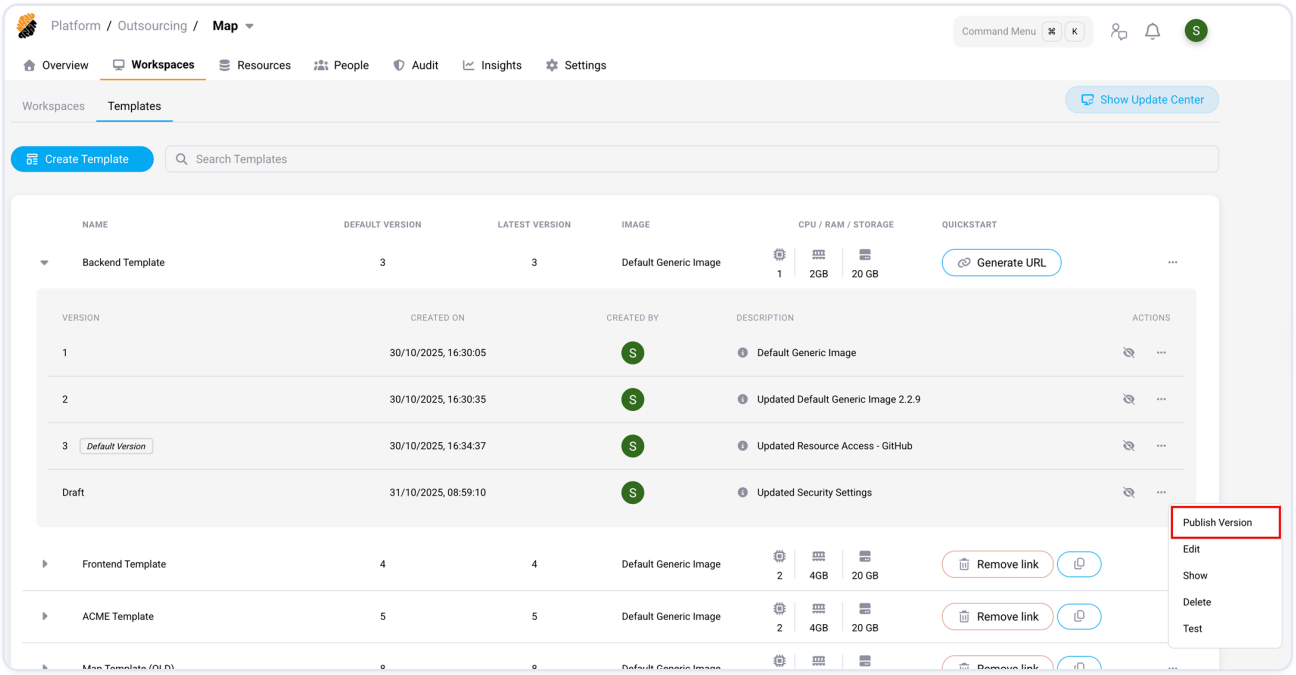


Después de realizar los cambios necesarios, puedes guardar la nueva versión como borrador, lo que permite modificaciones posteriores, o guardarla como una versión final de plantilla de inmediato, la cual no se podrá cambiar después.

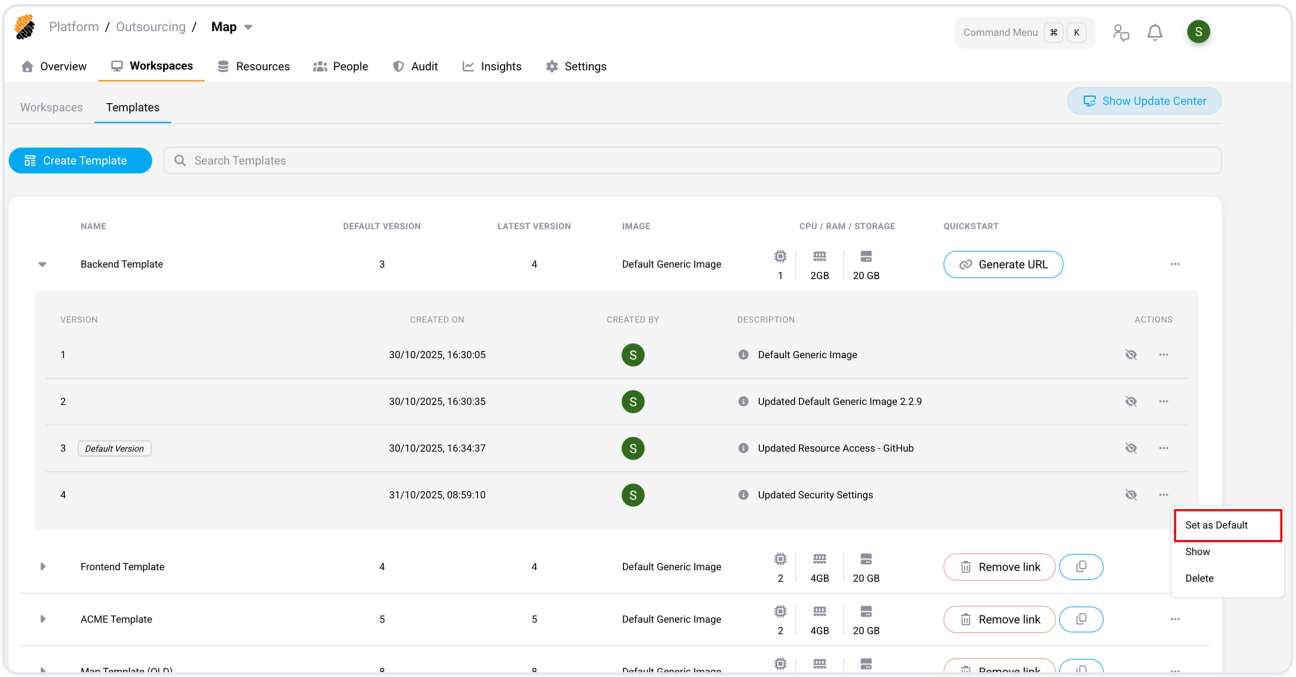
Una versión borrador o nueva de plantilla se puede probar de las siguientes maneras:

- Seleccionar **Iniciar espacio de trabajo** directamente dentro del editor de plantillas.
- Hacer clic en el botón "**...**" a la derecha de una plantilla y seleccionar **Probar**.
- Seleccionarlo manualmente de la lista de versiones en el asistente **Crear espacio de trabajo a partir de plantilla**.

Después de finalizar una versión borrador, se puede publicar como una nueva versión de plantilla haciendo clic en el botón "**...**" a la derecha de una plantilla y seleccionando **Publicar versión**.



Para asegurar que la nueva versión de la plantilla se seleccione automáticamente para los espacios de trabajo recién creados, haga clic en el botón "**...**" a la derecha de una plantilla y seleccione **Establecer como predeterminada**.



Nota

> Una versión de plantilla no se puede eliminar mientras algún Workspace la siga utilizando, y una plantilla no se puede eliminar mientras alguna de sus versiones esté en uso. Para retirar una plantilla que todavía está en uso, consulte Archivar una plantilla.

Rastrear qué versión de plantilla utiliza un espacio de trabajo

Cada Workspace registra la plantilla y la versión de plantilla a partir de la cual fue creado. Esto le permite ver qué Workspaces aún ejecutan una configuración anterior, para que pueda actualizarlos a su estándar actual.

> **Nota**
>
> El seguimiento de versiones se aplica a los Workspaces creados a partir de una plantilla. Los Workspaces creados antes de que se introdujera esta característica, y los Workspaces creados con el asistente simple **Crear Workspace** en lugar de a partir de una plantilla, no tienen una versión registrada y se listan como **sin versión**.

Indicadores de estado de la versión

En la sección **Plantillas** de la Página de Workspaces, cada nombre de plantilla muestra un contador para cada grupo de Workspaces que no está alineado con la versión predeterminada:

- **En pruebas** — Espacios de trabajo creados a partir de una versión borrador.
- **Obsoleto** — Espacios de trabajo creados a partir de una versión publicada que ya no es la versión predeterminada.
- **Sin versión** — Espacios de trabajo que no tienen una versión de plantilla registrada.

Los espacios de trabajo que ya utilizan la versión predeterminada cumplen las normas y no se contabilizan.

Seleccione cualquier contador para expandir la plantilla y abrir la ventana de **Espacios de trabajo asociados**.

Revisar y exportar espacios de trabajo asociados

La ventana **Espacios de trabajo asociados** enumera todos los espacios de trabajo que utilizan la plantilla, agrupados por la versión de plantilla a partir de la cual se creó. Ábrala seleccionando un

contador de estado, seleccionando **Espacios de trabajo asociados** en la plantilla expandida o seleccionando el recuento asociado en una fila de versión.

1. Expanda una fila de versión para listar los espacios de trabajo individuales y sus propietarios.
2. Seleccione espacios de trabajo individuales o utilice la casilla de verificación de nivel de versión para seleccionar todos los espacios de trabajo de esa versión.
3. Seleccione **Exportar como CSV**.

Resultado esperado: Se descarga un archivo CSV con las columnas **Nombre del espacio de trabajo**, **Propietario**, **Correo electrónico del propietario** y **Versión de la plantilla**. Las versiones borrador se exportan como `Draft` y los espacios de trabajo sin versión registrada se exportan como `Unversioned`.

> **Nota**
>
> Revisar y exportar espacios de trabajo asociados requiere permiso para gestionar plantillas de espacios de trabajo. Los desarrolladores pueden crear espacios de trabajo a partir de una plantilla, pero no pueden abrir esta ventana.

Actualizar un espacio de trabajo a la versión de plantilla predeterminada

Cuando se establece una nueva versión predeterminada, los espacios de trabajo existentes continúan ejecutando la versión a partir de la cual se crearon. Cada espacio de trabajo afectado muestra un indicador de actualización en la plataforma, y la actualización se aplica a un espacio de trabajo a la vez. El propietario del espacio de trabajo elige cuándo aplicarla.

Una actualización puede ser aplicada por el propietario del espacio de trabajo, o en su nombre por un propietario de proyecto, administrador de plataforma, propietario de organización o oficial de seguridad.

> **Advertencia**
>
> Aplicar una actualización reinicia el Espacio de trabajo y **reemplaza** la configuración del Espacio de trabajo con la configuración definida en la versión de plantilla predeterminada. Los datos persistentes, como el directorio de inicio y el código fuente, se conservan. Los cambios de configuración realizados en el Espacio de trabajo después de su creación, como un repositorio o secreto añadido, se pierden. Esta acción no se puede deshacer.

> Una actualización nunca reduce el disco de un Espacio de trabajo. Si el disco del Espacio de trabajo es más grande de lo que requiere la nueva versión de la plantilla —porque se expandió después de la creación del Espacio de trabajo—, el Espacio de trabajo mantiene su tamaño actual. Un disco más grande en la nueva versión se aplica como de costumbre.

Aplicar una actualización

1. En la tarjeta del Espacio de trabajo, seleccione el icono de actualización en el encabezado de la tarjeta, o seleccione **Actualizar** en el menú "**...**".
2. Revise los detalles de la actualización. Cuando el Espacio de trabajo se creó a partir de una versión publicada, la ventana muestra la versión actual y la nueva junto con una lista de **Cambios de configuración** de los repositorios, secretos, depósitos de datos, puntos de montaje, servicios conectados, imágenes, política de red, y script de inicio que se añaden o eliminan.
3. Seleccione **Actualizar**.

Resultado esperado: El Espacio de trabajo se reinicia con la nueva versión y el indicador de actualización desaparece.

> **Nota**

> Para un Espacio de trabajo sin una versión de plantilla registrada, la ventana confirma a qué versión está alineado el Espacio de trabajo, pero no enumera los cambios de configuración individuales.

Actualizar antes de editar

Un Espacio de trabajo que está desactualizado respecto a la versión de plantilla predeterminada debe actualizarse antes de que su configuración pueda ser editada. Cuando edita un Espacio de trabajo de este tipo, se abre una ventana de **Por favor, actualice su Espacio de trabajo** en lugar de la página de edición. Esto se aplica al editar desde la tarjeta del Espacio de trabajo, desde la pestaña **Espacios de trabajo** de su perfil, desde la lista de Espacios de trabajo del proyecto y al importar una configuración de IDE.

Seleccione **Actualizar** para aplicar la actualización y continuar a la página de edición.

Archivar una plantilla

Archive una plantilla cuando ya no deba usarse para nuevos Espacios de trabajo, pero aún tenga Espacios de trabajo asociados a ella. El archivado es la alternativa a eliminar una plantilla que todavía está en uso.

Para archivar una plantilla, seleccione el botón "**...**" a la derecha de una plantilla y seleccione **Archivar**.

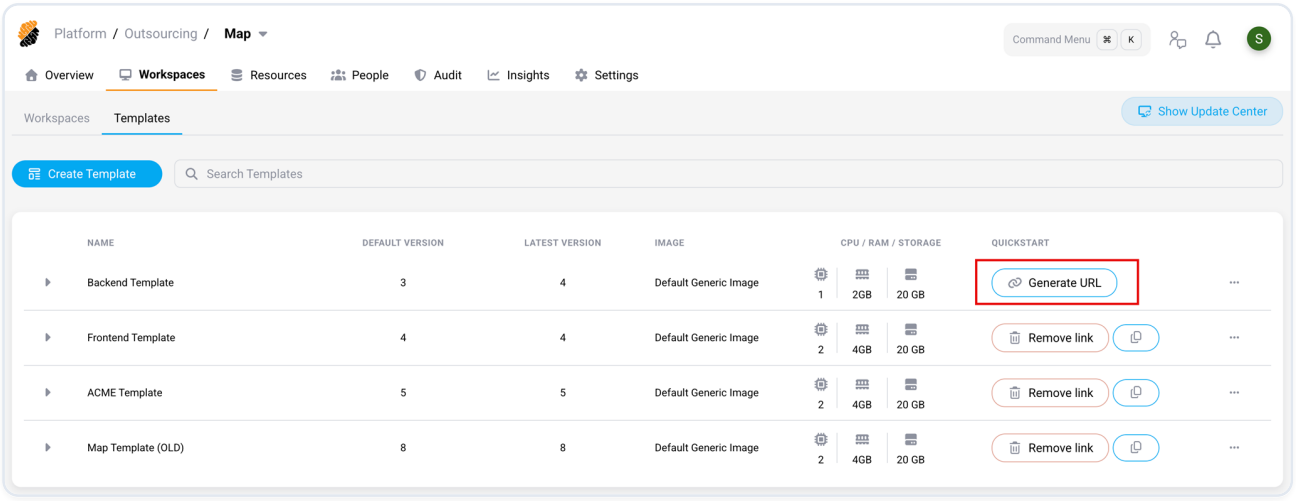
Resultado esperado: La plantilla se marca con una insignia de **Archivado** y ya no se puede seleccionar al crear un Espacio de trabajo, incluso a través de un enlace de inicio rápido. Los Espacios de trabajo existentes creados a partir de la plantilla no se ven afectados y aún se pueden actualizar a una versión de la plantilla.

Las plantillas archivadas están ocultas por defecto. Utilice el filtro de archivado en la sección **Plantillas** para mostrarlas u ocultarlas. Para que una plantilla archivada vuelva a estar disponible, seleccione el botón "**...**" y seleccione **Restaurar**.

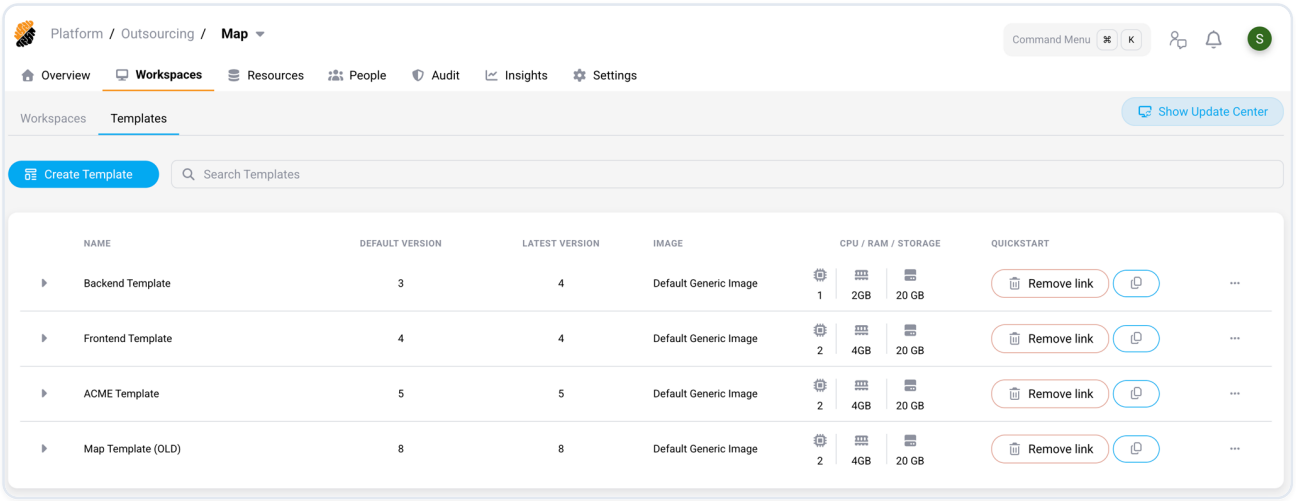
Inicio rápido

La funcionalidad de inicio rápido permite a los desarrolladores crear un nuevo espacio de trabajo con un solo clic desde un repositorio de código, un portal de ingeniería o cualquier otra ubicación fuera de Citrix SecurSpaces™.

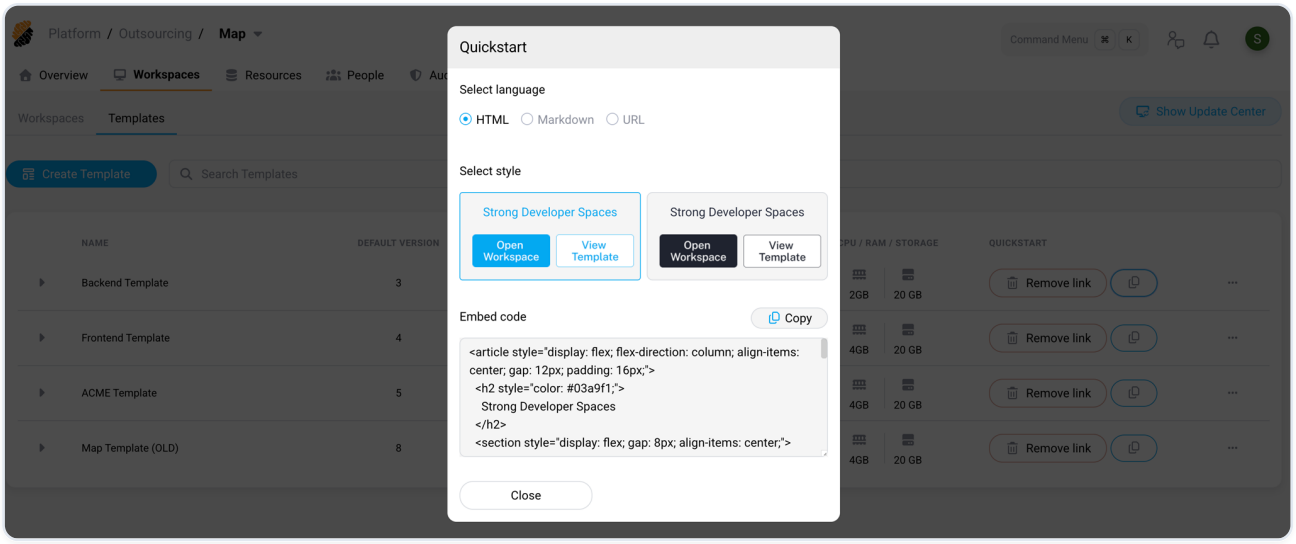
Cree un enlace de inicio rápido haciendo clic en el botón **Generar URL** a la derecha de una plantilla.



Luego haga clic en el icono **Copiar**.

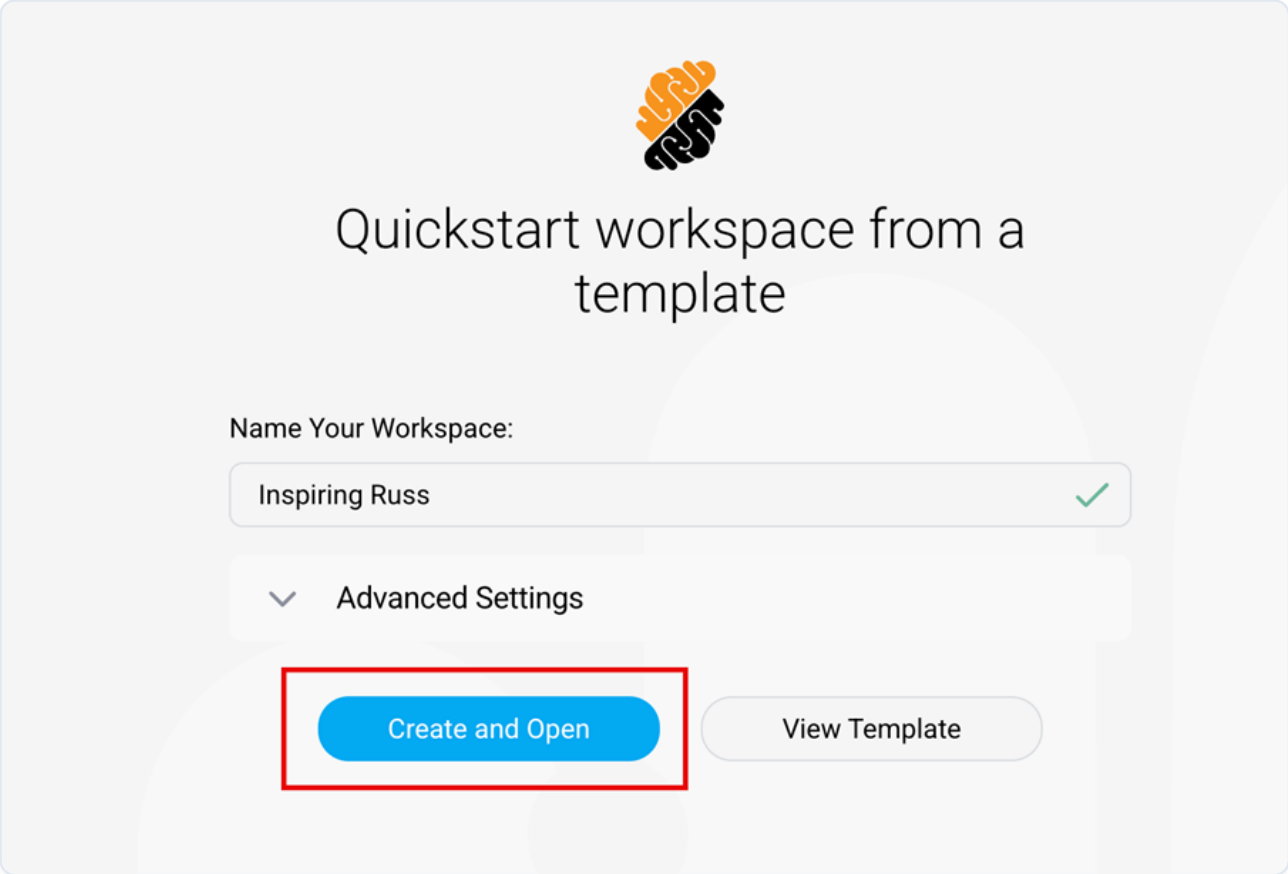


Seleccione cualquiera de las opciones disponibles.

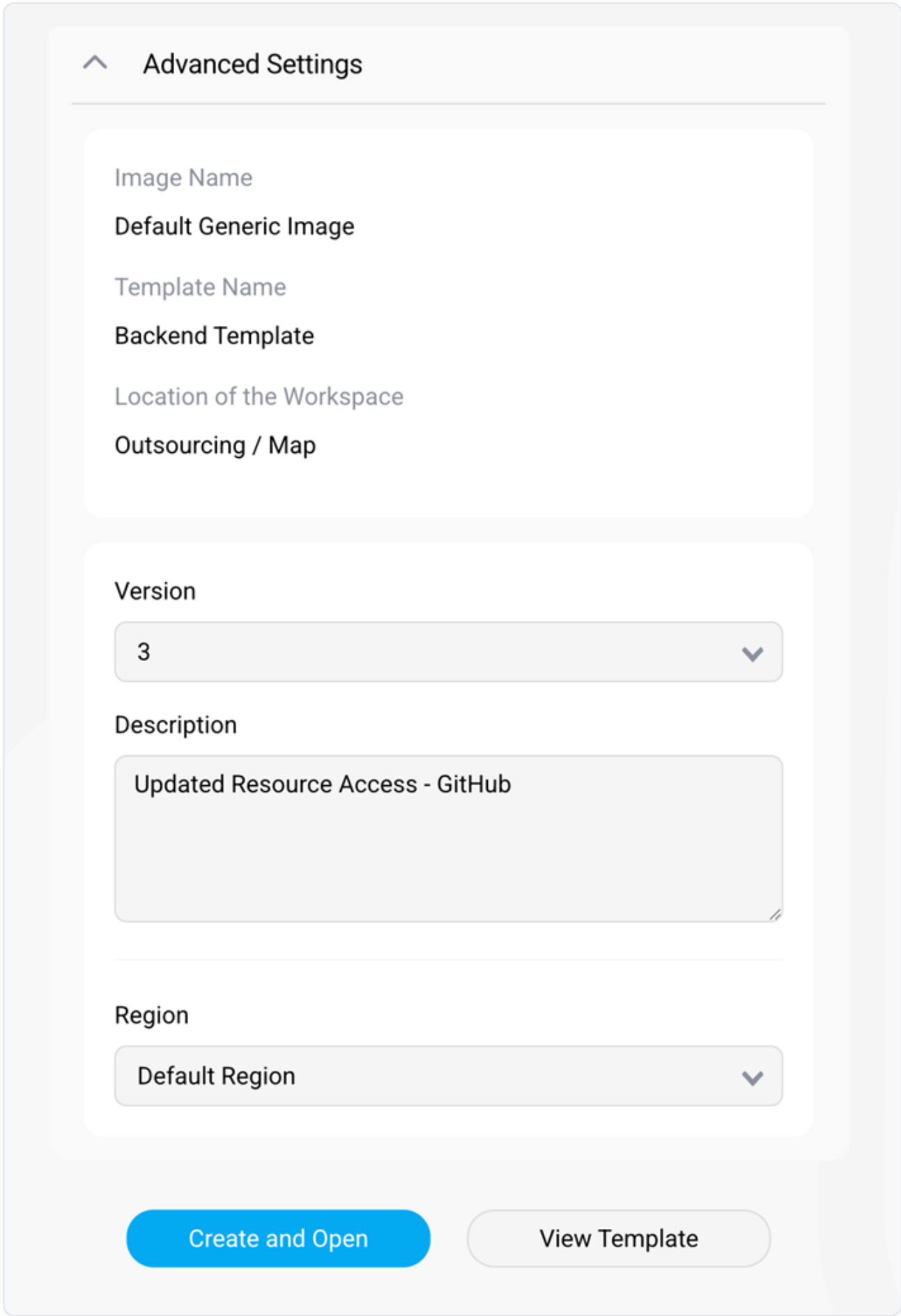


Cuando un usuario accede a la URL de inicio rápido, SecurSpaces inicia la creación de un nuevo espacio de trabajo, a menos que el usuario ya tenga un espacio de trabajo basado en esta plantilla en particular. En este caso, el usuario será redirigido automáticamente al espacio de trabajo correspondiente.

Cuando se necesita crear un nuevo espacio de trabajo, el usuario puede configurar el nombre del espacio de trabajo y finalizar el flujo de creación, seleccionando **Crear y abrir**.



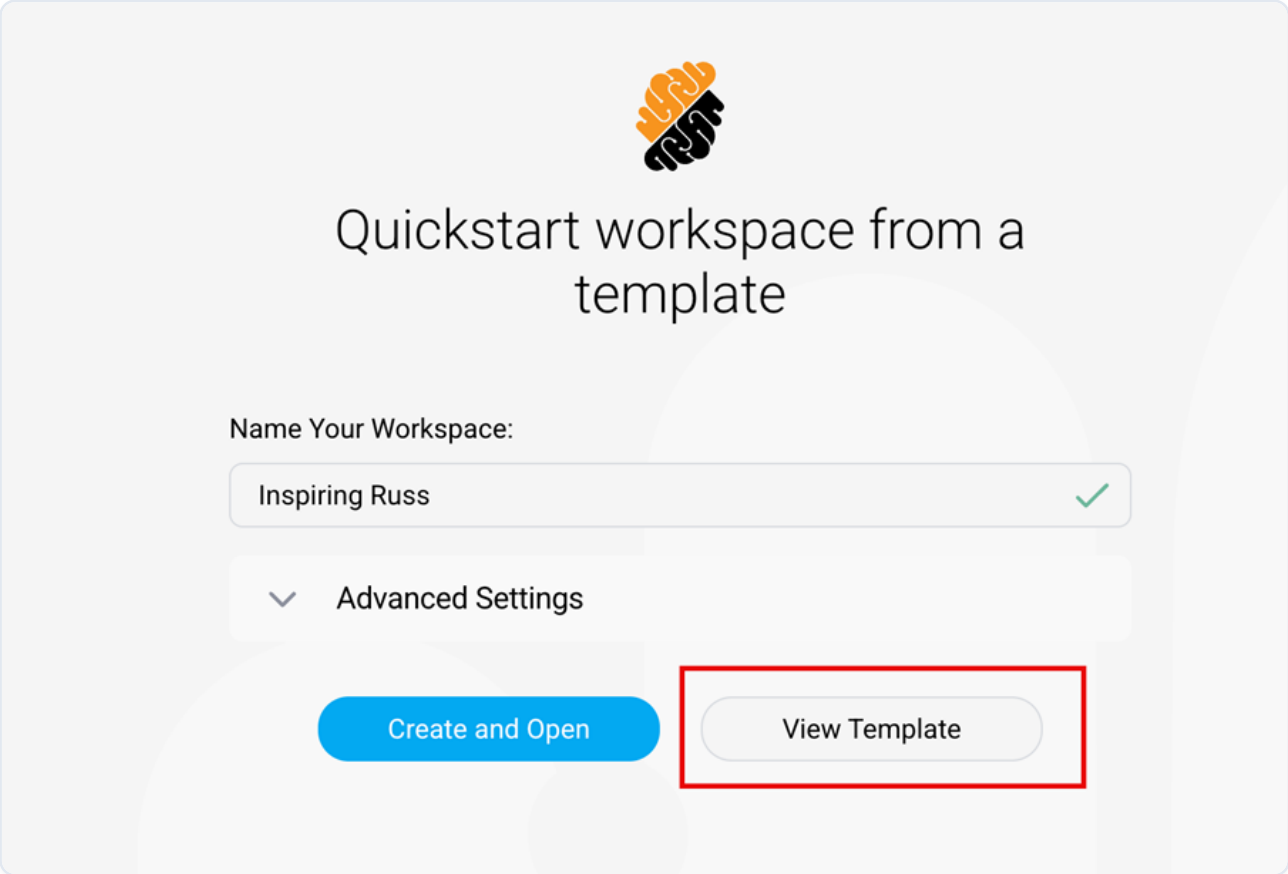
A través del menú de **Configuración avanzada**, se pueden verificar los detalles de configuración, como la plantilla base o el proyecto SecurSpaces relacionado, y se pueden configurar la versión de la plantilla, así como la región de despliegue.


Advanced Settings
Image Name
Default Generic Image
Template Name
Backend Template
Location of the Workspace
Outsourcing / Map
Version
3
Description
Updated Resource Access - GitHub
Region
Default Region
Create and Open
View Template

Advertencia

La región de despliegue que se ofrece aquí no se verifica con los puntos de montaje de la plantilla. Si la plantilla incluye un punto de montaje y selecciona una región diferente a la principal, el Espacio de trabajo se crea en esa región con el punto de montaje adjunto, pero no puede usar ese almacenamiento. Deje la región configurada como la región principal cuando la plantilla incluya un punto de montaje.

El botón **Ver plantilla** abre el editor de plantillas de espacio de trabajo para la versión seleccionada, para verificar más detalles de configuración.



Automatizar enlaces de inicio rápido con la API REST

También puede gestionar los enlaces de inicio rápido a través de la API REST. Utilice la API cuando necesite publicar enlaces de lanzamiento de plantillas en un portal de desarrolladores, un archivo README de repositorio o un flujo de trabajo de incorporación interno.

La API de enlaces de inicio rápido puede:

- Habilitar un enlace de inicio rápido para una plantilla de espacio de trabajo.

- Devolver la URL sin formato, la URL de la plantilla de vista y los fragmentos de inserción de Markdown o HTML generados.
- Generar fragmentos de inserción claros u oscuros.
- Revocar un enlace de inicio rápido cuando ya no deba utilizarse.

Para obtener detalles del punto final, consulte API REST.

Incluir elementos de acceso personalizados en las plantillas

Las plantillas de espacio de trabajo pueden incluir Elementos de acceso personalizado. Utilice los Elementos de acceso personalizado para proporcionar acceso con un solo clic a herramientas o servicios que se ejecutan dentro de los espacios de trabajo creados a partir de la plantilla.

Los Elementos de acceso personalizado se pueden gestionar en la configuración de la plantilla del espacio de trabajo o a través de la API REST. Cada elemento define un nombre para mostrar, un puerto, un comando y configuraciones opcionales de comprobación de estado.

Para obtener detalles sobre los puntos finales, consulte API REST.

Duplicar una plantilla

Una plantilla de espacio de trabajo se puede duplicar haciendo clic en el botón "**...**" a la derecha de una plantilla y seleccionando **Duplicar**. Esto permite crear rápidamente nuevas configuraciones basadas en plantillas existentes.

Información relacionada

- Ejecutar agentes de codificación de IA en espacios de trabajo — lo que necesita una plantilla cuando los agentes se ejecutan en ella
- Imágenes de espacio de trabajo

Build and manage custom workspace images for SecurSpaces

Si bien las imágenes estándar ofrecen un inicio rápido, el uso de imágenes de espacio de trabajo personalizadas dentro de Citrix SecurSpaces™ garantiza que su entorno de desarrollo se adapte a las necesidades de su organización, manteniendo al mismo tiempo un estricto cumplimiento.

Ventajas de las imágenes personalizadas

- **Experiencia de desarrollador personalizada:** Preinstale tiempos de ejecución específicos del proyecto (Node, Python, Go) y utilidades CLI (kubectl, terraform). Puede preconfigurar los

ajustes de red internos, los certificados CA, las extensiones IDE y los alias de shell para que el espacio de trabajo esté listo inmediatamente después del lanzamiento.

- **Gobernanza estandarizada:** Asegúrese de que cada contenedor siga los estándares internos, incluidas las distribuciones de SO aprobadas y reforzadas, y la procedencia del software de repositorios de confianza.
- **Seguridad proactiva:** Integre las imágenes en su ciclo de vida de gestión de vulnerabilidades. Active compilaciones automatizadas para rotar las imágenes cuando se detecte una CVE y reduzca la superficie de ataque eliminando paquetes innecesarios.

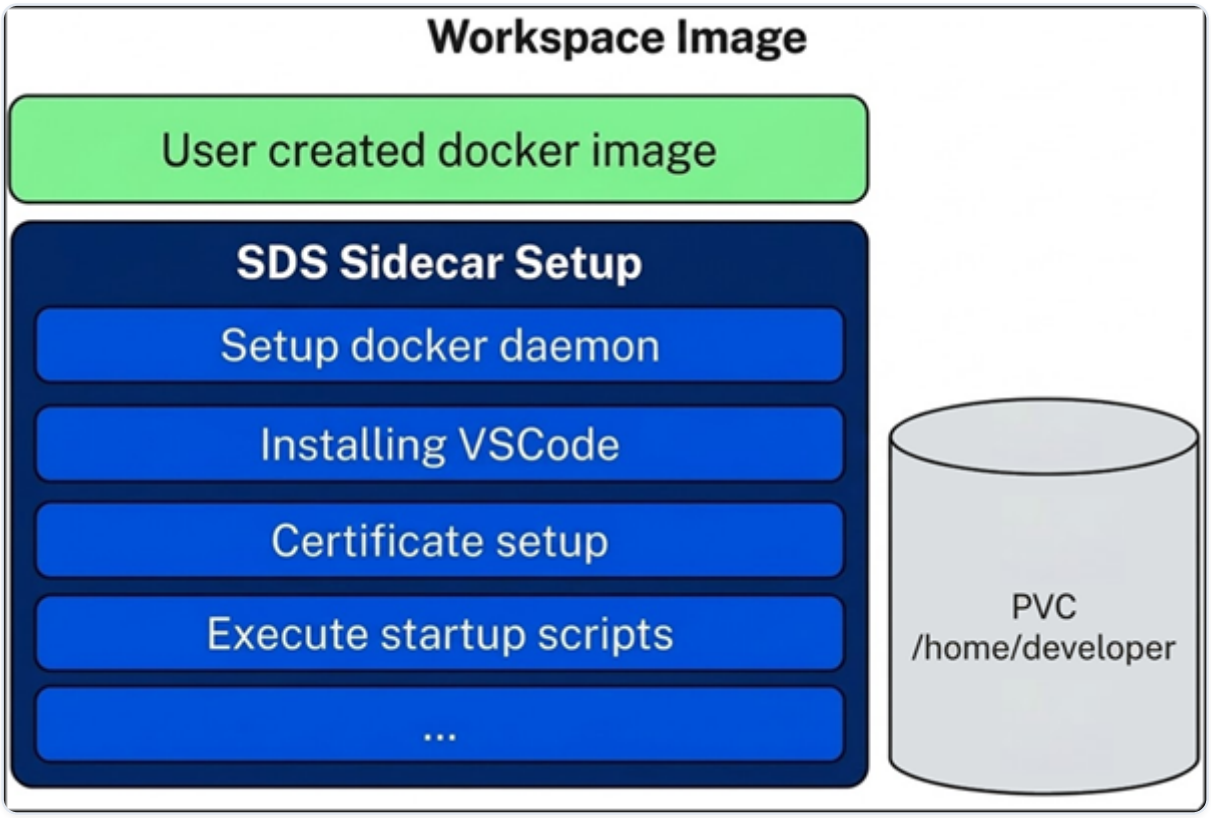
Arquitectura

Arquitectura de tiempo de ejecución

En la plataforma SecurSpaces, un espacio de trabajo se ejecuta dentro de un Pod de Kubernetes. Existe una relación uno a uno entre un espacio de trabajo y un Pod para garantizar el aislamiento a nivel de contenedor.

El tiempo de ejecución del espacio de trabajo consta de tres capas principales:

- **El contenedor del espacio de trabajo:** El entorno de ejecución que contiene sus compiladores, depuradores y herramientas.
- **Almacenamiento persistente:** Un volumen persistente (PV) montado en el directorio de inicio del usuario (`/home/developer`). Esto garantiza que el código, las configuraciones locales y el historial de shell persistan si el Pod se reinicia.
- **Sidecars de plataforma:** Contenedores auxiliares gestionados por la plataforma SecurSpaces que proporcionan características como scripts de inicio y soporte para Docker-in-Docker.



Arquitectura de imagen en capas

Recomendamos una arquitectura de imagen multicapa para equilibrar la gobernanza centralizada con la autonomía del desarrollador:

- **Imagen base:** Un sistema operativo reforzado proporcionado por el departamento de TI corporativo. Incluye certificados de CA empresariales y configuraciones de seguridad básicas.
- **Imagen de la organización:** Propiedad del equipo de la plataforma SecurSpaces. Contiene las dependencias principales de SecurSpaces, herramientas de desarrollo comunes y configuraciones de proxy globales.
- **Imagen de proyecto:** Propiedad de los equipos de aplicaciones. Incluye tiempos de ejecución específicos (por ejemplo, JDK 17, Node 20) y dependencias específicas del proyecto.

Comprender la persistencia

En un espacio de trabajo de SecurSpaces, solo el directorio `/home/developer` es persistente. Cuando un espacio de trabajo se reinicia, cualquier cambio en el sistema de archivos raíz (`/etc`, `/usr`, `/var`) se descarta.

> **Importante:**

> El volumen persistente se monta en tiempo de ejecución. Cualquier archivo colocado en `/home/developer` durante la fase `docker build` será sobrescrito por el volumen persistente una vez que se inicie el espacio de trabajo.

Patrones de diseño de persistencia

- Binarios: Instale los binarios en directorios del sistema como `/usr/local/bin` durante la compilación de Docker.
- Datos y configuración local: Configure las herramientas para almacenar registros, caché y complementos en `/home/developer`.
- Configuración global: Use `/etc/` para la configuración global de herramientas para que sirva como respaldo.

Persistencia no estándar

Las herramientas que instalan binarios dinámicamente en el directorio de inicio (por ejemplo, `conda`, `nvs`, `gcloud CLI`) deben tratarse como Datos Locales. Use scripts de inicio para asegurar que estas configuraciones se restauren o inicialicen después de que se monte el volumen persistente.

Configuración automatizada con scripts de inicio

Scripts gestionados por la plataforma

Gestionados a través de la interfaz de usuario de SecurSpaces, estos scripts se ejecutan cada vez que se inicia un espacio de trabajo.

- **Scripts de prearranque:** Se ejecutan durante la fase inicial de inicialización del contenedor.
- **Scripts de postarranque:** Se ejecutan después de que los servicios del espacio de trabajo estén activos.
- **Idempotencia:** Dado que se ejecutan en cada inicio, asegúrese de que los scripts comprueben las configuraciones existentes:

```
if [ ! -f "/home/developer/.my_tool_config" ]; then

    echo "Initializing configuration..."

fi
```

Scripts incrustados en la imagen

Ideales para prácticas DevOps estrictas, estos scripts se almacenan en la imagen de Docker y se ejecutan solo una vez durante la creación inicial del espacio de trabajo.

- **Directorio de destino:** `/usr/bin/strong_network_startup/`
- **Permisos:** El usuario `developer` debe tener permisos de ejecución.
- **Nomenclatura:** Los scripts se ejecutan en orden alfabético. Use prefijos numéricos (por ejemplo, `01_setup.sh`).

Los archivos sin el bit de ejecución se omiten silenciosamente, así que establezca el modo al copiar el script. Un script que falla registra un error y los scripts restantes siguen ejecutándose.

Preinstalar extensiones de VS Code

El ejemplo de imagen base crea `/usr/bin/strong_network_startup/vscode_extensions`. Ese directorio no es parte del mecanismo de scripts de inicio: es donde la plataforma busca extensiones para instalar en el IDE en la nube.

Coloque los archivos `.vsix` allí y se instalarán la primera vez que un espacio de trabajo se inicie desde la imagen. Así es como se envía un conjunto de extensiones estándar con una imagen de proyecto, en lugar de pedir a cada desarrollador que instale las mismas extensiones manualmente.

```
COPY --chown=developer:developer extensions/*.vsix /usr/bin/
strong_network_startup/vscode_extensions/
```

Para usar un directorio diferente, establezca la variable de entorno `VSCODE_EXTENSION_INSTALL_DIR` en el espacio de trabajo. Cuando no está configurada, la plataforma usa la ruta anterior.

Crear una imagen en la plataforma

Si su equipo solo necesita algunas adiciones a una imagen existente, SecurSpaces puede construir la imagen derivada para usted, sin un Dockerfile o una canalización. Consulte Crear una imagen a partir de una existente.

Mejores prácticas de seguridad

Gestión de secretos

Nunca incruste credenciales (claves SSH, tokens de API) directamente en una imagen de Docker. SecurSpaces proporciona una inyección segura en tiempo de ejecución:

- **Variables de entorno:** Ideales para claves de API y nombres de usuario.
- **Montajes de archivos:** Los secretos se montan en la carpeta `/secrets/`. Preferido para archivos de licencia y claves criptográficas.

Integraciones de terceros

Siempre prefiera las integraciones de plataforma nativas (por ejemplo, JFrog Artifactory, proveedores de Git) en lugar de la inyección manual de secretos. SecurSpaces gestiona la capa de autenticación automáticamente, por lo que no necesita gestionar manualmente los archivos `.npmrc`, `.gi` o `.docker/config.json` en su imagen.

Requisitos del sistema

Las imágenes personalizadas deben cumplir los requisitos de imagen de contenedor de SecurSpaces: paquetes principales, paquetes por distribución y por arquitectura, y la cuenta `developer` UID 1000. Consulte Requisitos de imagen de contenedor.

Cree su primera imagen base

Filosofía de diseño

- **Completitud sobre minimalismo:** A diferencia de las imágenes de producción, las imágenes de espacio de trabajo deben priorizar la experiencia del desarrollador incluyendo todos los compiladores, encabezados y bibliotecas `-dev` necesarios.
- **Omitir compilaciones de varias etapas:** Mantenga las herramientas instaladas durante el proceso de compilación disponibles para el desarrollador.
- **Anulaciones de orquestación:** SecurSpaces anula `ENTRYPOINT` y `CMD` para iniciar servicios de plataforma. Utilice scripts de inicio para la lógica de inicialización.

Ejemplo de Ubuntu 24.04

```
FROM ubuntu:24.04
```

```
# 1. Install SecurSpaces core requirements


RUN apt-get update && apt-get install -y --no-install-recommends \
    curl bash tar git git-lfs openssh-client sudo \
    && apt-get clean && rm -rf /var/lib/apt/lists/*


# 2. Create developer user (Repurposing default 'ubuntu' user for 24.04)


RUN usermod -l developer -d /home/developer -m ubuntu && \
    groupmod -n developer ubuntu


# 3. Setup startup directory


RUN mkdir -p /usr/bin/strong_network_startup/vscode_extensions && \
    chown -R developer:developer /usr/bin/strong_network_startup && \
    chmod u+rwx /usr/bin/strong_network_startup


# 4. Run as the developer user, in the developer home directory


USER 1000
WORKDIR /home/developer
```

Cuando se añade la imagen, SecurSpaces la prueba antes de que cualquiera pueda usarla. Consulte Cómo la plataforma comprueba una imagen.

Instalar un certificado de CA privado

Si su organización ejecuta su propia autoridad de certificación, añada el certificado raíz al almacén de confianza del sistema en el momento de la compilación. Sin él, `git`, `curl` y los gestores de paquetes dentro del espacio de trabajo no podrán verificar los hosts internos.

```
COPY internal-ca.crt /usr/local/share/ca-certificates/internal-ca.crt

RUN update-ca-certificates
```

En Red Hat y CentOS, copie en `/etc/pki/ca-trust/source/anchors/` y ejecute `update-ca-trust` en su lugar.

Esto es independiente del certificado que SecurSpaces inyecta cuando se adjunta una política de red a un espacio de trabajo, lo cual la plataforma gestiona por usted. Consulte Certificados cuando se adjunta una política de red.

Algunas herramientas incluyen su propio paquete de CA e ignoran el almacén del sistema. Esas necesitan apuntar a su certificado por separado, normalmente a través de una variable de entorno.

Habilitar el acceso de root

Para conceder privilegios de sudo al usuario desarrollador, añada lo siguiente a su Dockerfile:

```
RUN apt-get update && apt-get install -y sudo && rm -rf /var/lib/apt/
lists/*



# Grant passwordless sudo



RUN echo "developer ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers.d/developer &&
\

    chmod 0440 /etc/sudoers.d/developer
```

> **Nota:**

> Para aumentar la seguridad, puede incluir en la lista blanca herramientas específicas en lugar de conceder acceso completo: `developer ALL=(ALL) NOPASSWD: /usr/bin/apt-get, /usr/bin/systemctl`

Usar Docker dentro de un espacio de trabajo

Los espacios de trabajo pueden construir y ejecutar contenedores. Un demonio de Docker se ejecuta como un sidecar en el Pod del espacio de trabajo y su socket se expone al espacio de trabajo en `/var/run/docker.sock`, por lo que **solo necesita el cliente de Docker en su imagen, no el demonio**.

```
# Install the Docker CLI, Buildx, and Compose from the official static builds.

# Pin the versions your organization has approved rather than tracking latest.

ARG DOCKER_VERSION=27.3.1

RUN curl -fsSL "https://download.docker.com/linux/static/stable/x86_64/docker-${DOCKER_VERSION}.tgz" \

      -o /tmp/docker.tgz && \

    tar -C /tmp -xzf /tmp/docker.tgz && \

    mv /tmp/docker/docker /usr/local/bin/ && \

    rm -rf /tmp/docker /tmp/docker.tgz
```

Instale la CLI en un directorio del sistema como `/usr/local/bin`, no en `/home/developer`, para que sobreviva a un reinicio. Consulte Comprensión de la persistencia.

Qué se le permite hacer al espacio de trabajo

En la configuración predeterminada sin root, el socket no lleva directamente al demonio. Es un proxy que inspecciona cada solicitud y rechaza cualquier cosa que pudiera romper el aislamiento

del espacio de trabajo. Las compilaciones ordinarias y `docker run` funcionan normalmente; se rechazan los siguientes:

RECHAZADO	EJEMPLOS
Contenedores privilegiados	`--privileged`
Espacios de nombres del host	`--pid=host`, `--network=host`, `--ipc=host`, `--uts=host`
Capacidades añadidas más allá de las predeterminadas de Docker	`--cap-add=SYS_ADMIN`, `--cap-add=ALL`
Opciones de seguridad relajadas	`--security-opt apparmor=unconfined`, `seccomp=unconfined`, `no-new-privileges=false`
Acceso a dispositivos del host	`--device`
Padre de cgroup personalizado	`--cgroup-parent`
Montajes de enlace desde fuera del espacio de trabajo	Solo `/home/developer`, `/tmp` y `/var/run/docker.sock` están permitidos como orígenes

Una solicitud rechazada falla con un mensaje que nombra la restricción, por ejemplo `privileged containers are not allowed`. Los volúmenes con nombre no se ven afectados.

> **Nota:**

> **Root Docker in Docker** es un indicador de característica de la plataforma. Cuando un administrador de plataforma lo activa, el socket alcanza el demonio directamente y estas restricciones ya no se aplican. El indicador se puede configurar para todos, o para usuarios y grupos seleccionados, por lo que puede estar activado para algunos desarrolladores y no para otros. Consulte Activar o desactivar características.

Ejemplos publicados por Citrix

En lugar de empezar desde cero, puede adaptar una imagen que Citrix ya construye:

- strong-network/images en GitHub — los Dockerfiles y scripts de compilación detrás de las imágenes suministradas, incluyendo variantes base, genéricas, específicas de idioma y GUI. El repositorio tiene un makefile, por lo que `make base_image` o `make all` los compila localmente.
- strongnetwork en Docker Hub — las mismas imágenes, precompiladas, que puede referenciar directamente o usar como una línea `FROM`.

Información relacionada

- Requisitos de la imagen de contenedor — lo que una imagen debe proporcionar y la comprobación que debe pasar
- Ejecutar agentes de codificación de IA en espacios de trabajo — empaquetar herramientas de agente para que estén presentes al inicio del espacio de trabajo
- Plantillas
- Almacenamiento en caché de imágenes

Container images

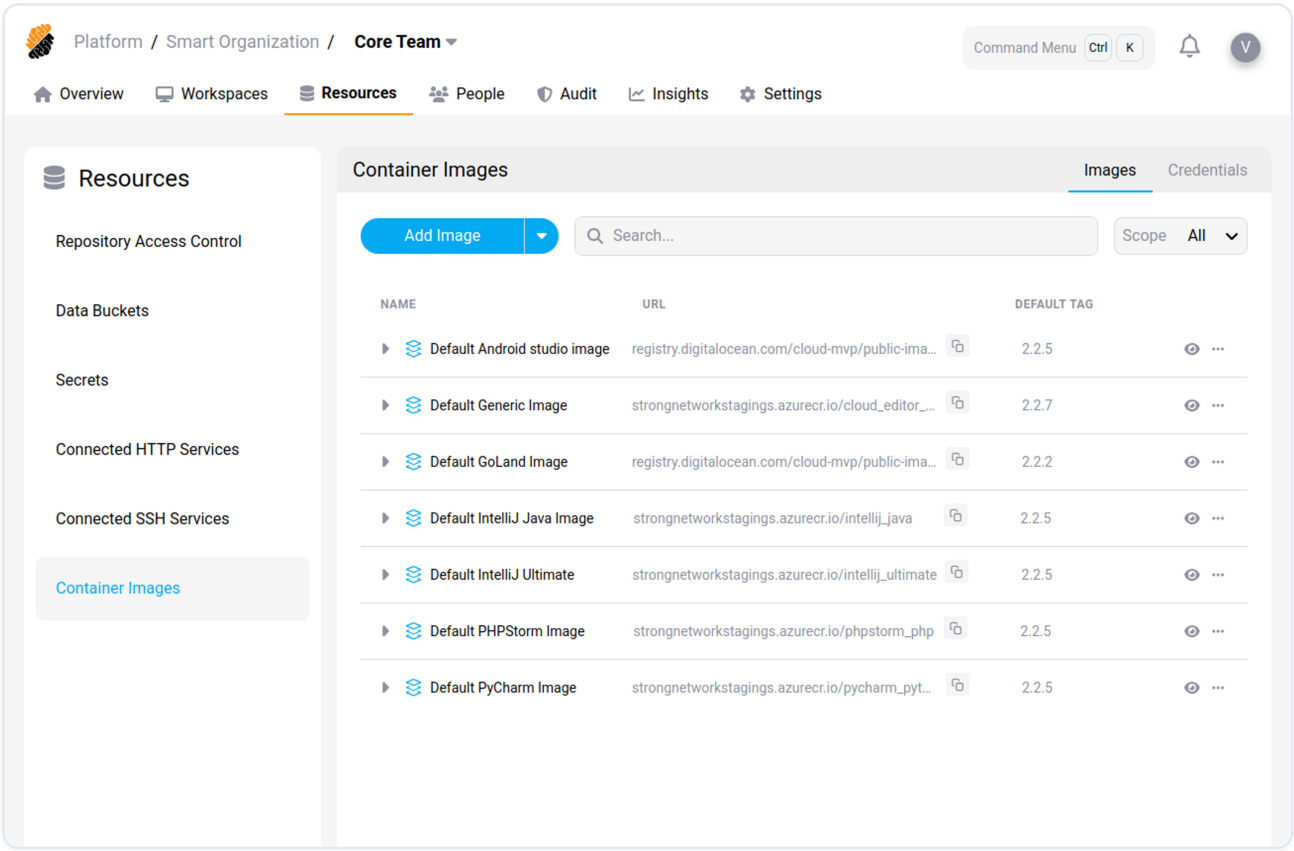
Las imágenes de contenedor o también los Entornos de Desarrollo en la Nube (CDE) se utilizan para definir la configuración de un entorno de desarrollo. Normalmente, los CDE definen todas las dependencias de software necesarias para construir la aplicación deseada una vez implementada. Los usuarios crean espacios de trabajo con dicha imagen como "plantilla" y comienzan a contribuir código al proyecto dentro de este contexto.

Las imágenes CDE se importan de un registro como parte de los recursos disponibles para los usuarios en la plataforma. Los registros pueden ser públicos o privados. Para los registros privados, debe proporcionar credenciales para autenticarse correctamente antes de importar la imagen. Los registros públicos, por definición, no necesitan credenciales.

- Ver imágenes CDE
- Añadir una imagen CDE
- Ver credenciales de registro
- Añadir una credencial de registro
- Actualizar una credencial de registro

Ver imágenes CDE

El panel muestra las imágenes CDE disponibles en el proyecto. Puede buscar una o filtrar las utilizadas en los espacios de trabajo.



Una imagen CDE se define por las siguientes características:

- **Información básica**: Nombre, ámbito de uso (plataforma, organización o proyecto), URL y etiqueta.
- **Nivel de clase**: Esta opción define la visibilidad de la imagen CDE en función de los permisos del usuario.
- **Información del activo**: Esta opción permite proporcionar una descripción del CDE.

Al hacer clic en una imagen CDE, puede ver una lista de las versiones del CDE seguida de detalles básicos como la fecha de importación y el estado.

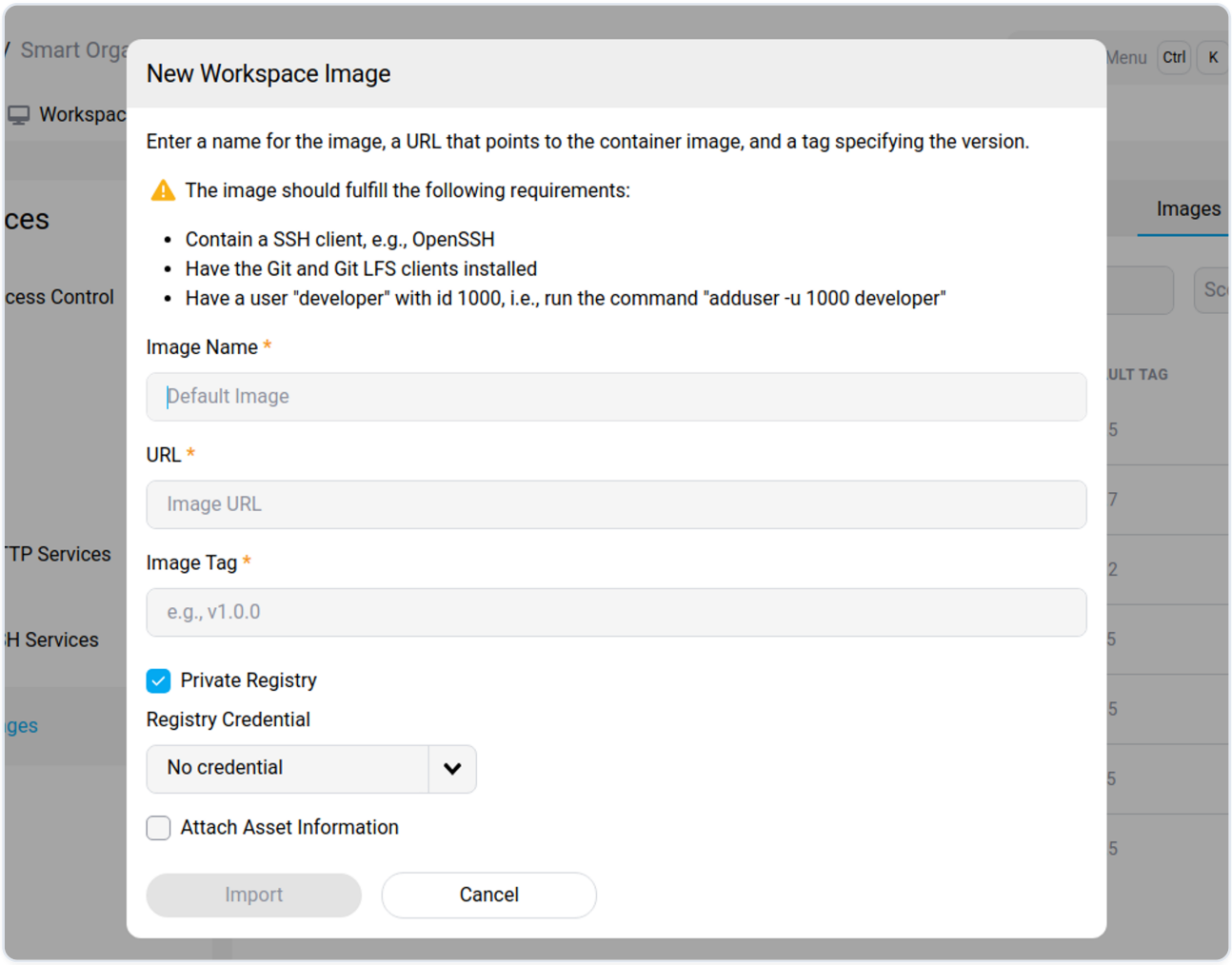
Añadir una imagen CDE

Requiere el conjunto de permisos Recursos para **Importar**.

Seleccione **Añadir imagen**. El formulario se abre como **Nueva imagen de espacio de trabajo** y solicita:

1. **URL**, la ruta completa a la imagen, en el formato `<registry>/<namespace>/<repository>:<tag>`.
2. **Nombre de la imagen**, un nombre para identificar la imagen.
3. **Etiqueta de imagen**, por ejemplo `v1.0.0`.

4. **Registro privado** (opcional), la credencial utilizada para acceder a un registro privado.
5. **Adjuntar información de activos** (opcional), una descripción de la imagen.



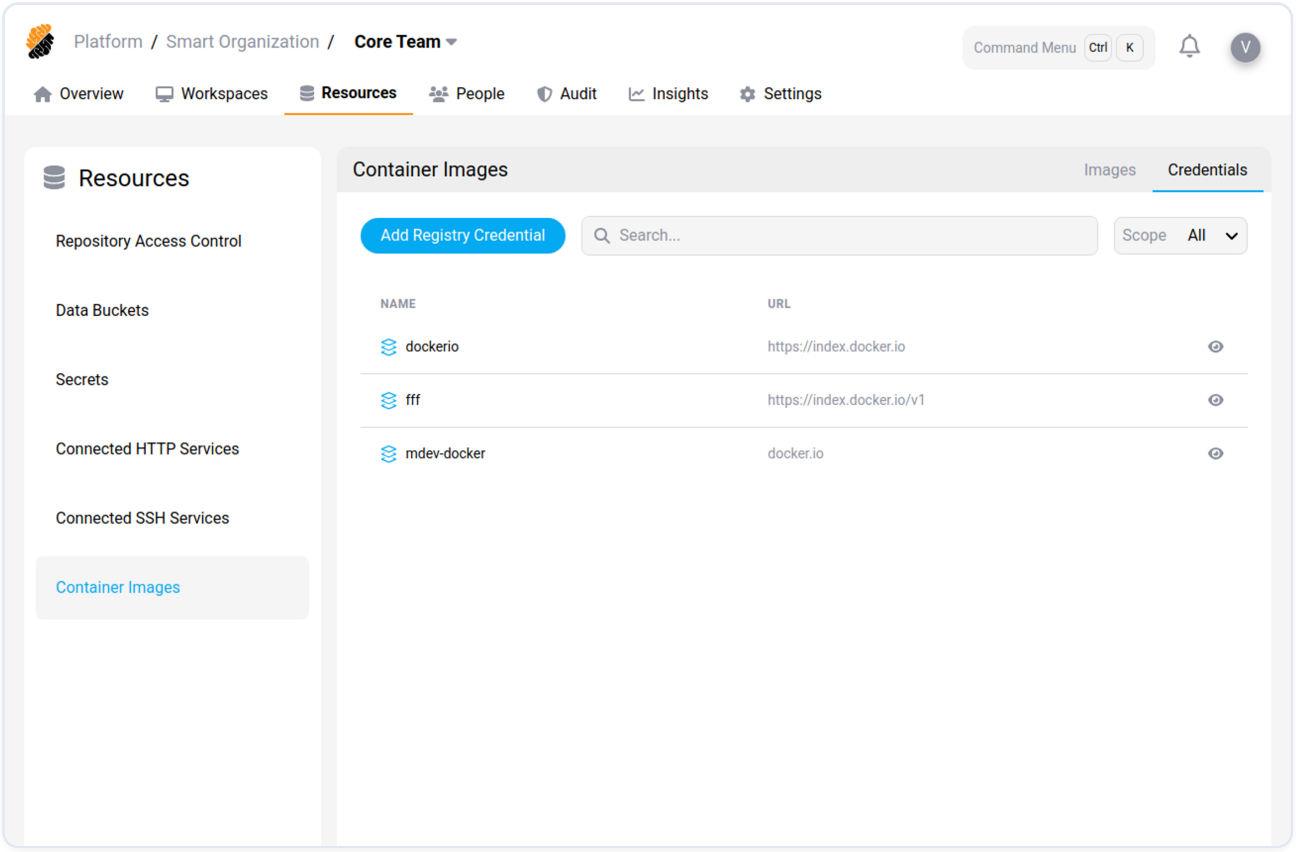
Advertencia

La imagen debe cumplir los requisitos de imagen de contenedor de SecurSpaces antes de poder utilizarse para un espacio de trabajo. Como mínimo, necesita un cliente SSH, Git y Git LFS, y un usuario llamado `developer` con UID 1000. Para ver la lista completa, consulte Requisitos de imagen de contenedor.

Puede editar o eliminar una imagen CDE haciendo clic en el icono "**...**" junto a su nivel de clase.

Ver credenciales de registro

Para mostrar las credenciales utilizadas en el proyecto, haga clic en el botón "**Credenciales**" en la parte superior derecha del panel. Puede buscar una o filtrar las utilizadas en los espacios de trabajo.



Una credencial de registro se define por las siguientes características:

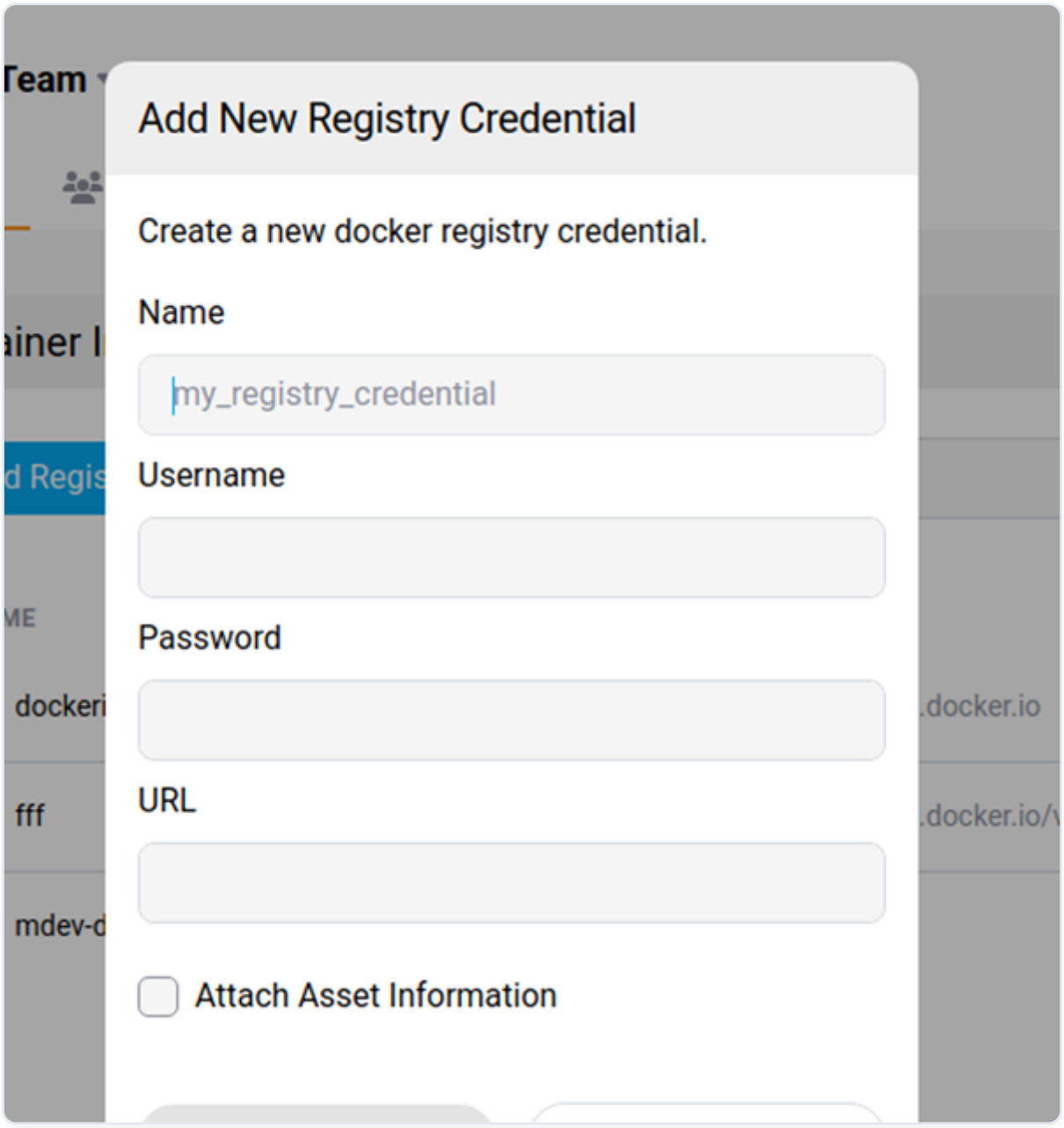
1. **Nombre**,
2. **Ámbito** y
3. una **URL**.

Por motivos de seguridad, ninguna credencial se expone directamente ni está disponible para consulta.

Añadir una credencial de registro

Requiere el permiso de **Seguridad** establecido en **Administrar**.

Puede añadir una credencial de registro pulsando el botón "**Añadir credencial de registro**".

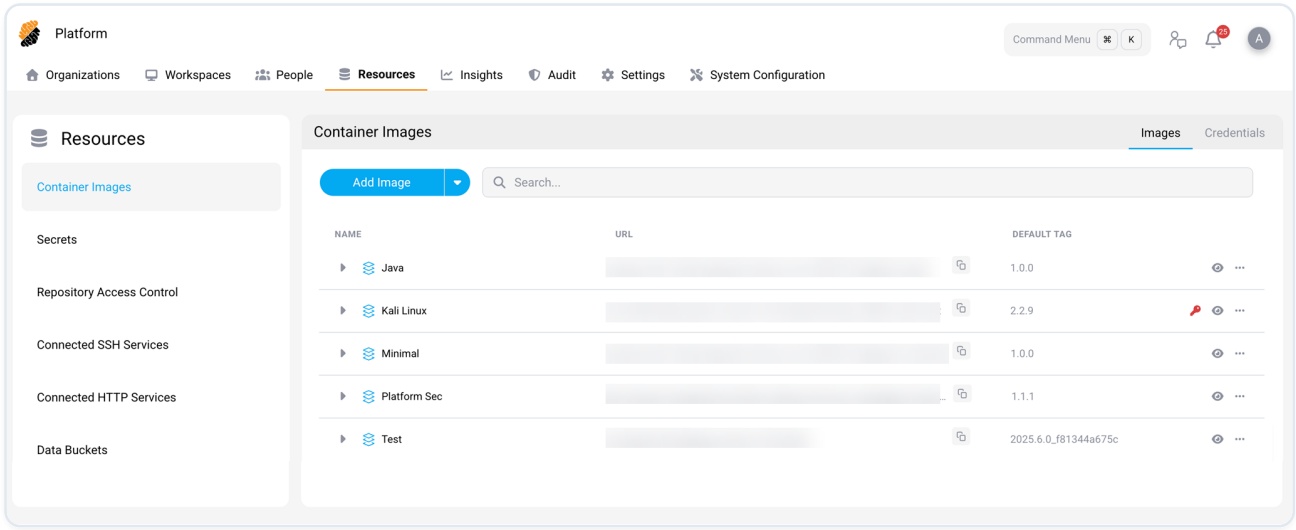


Deberá introducir la siguiente información:

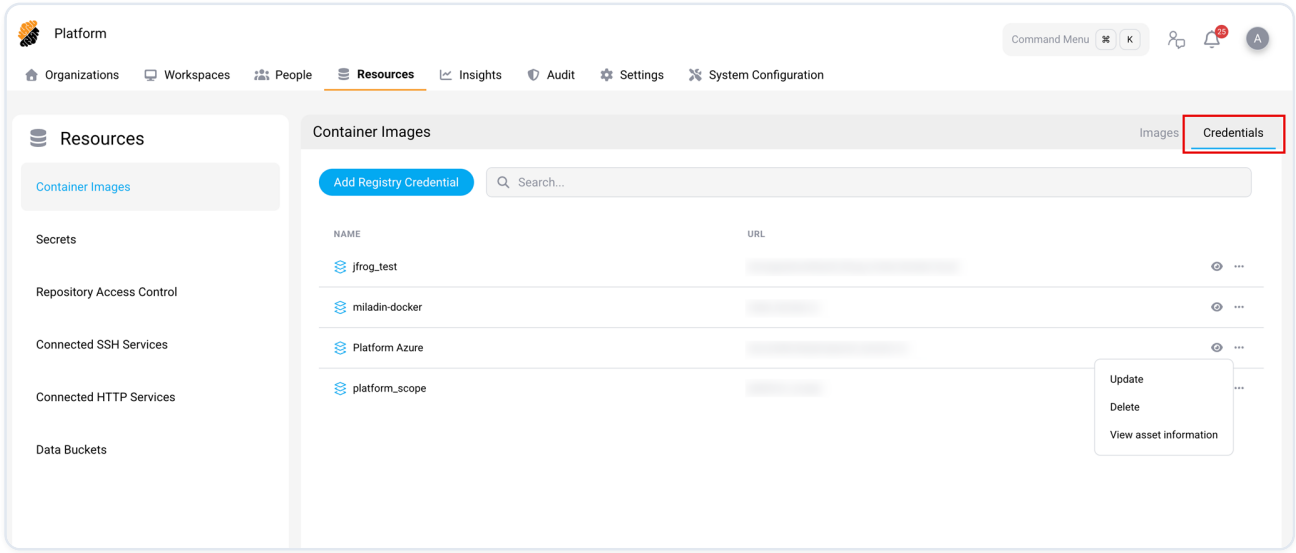
1. **Nombre**, para identificar las credenciales cuando sea necesario durante el registro de una imagen CDE,
2. **Nombre de usuario**:, y
3. **Contraseña**:, como valores de credencial, y una
4. **URL**: donde se realiza la autenticación.
5. **Información del activo**, una descripción de la credencial de registro.

Actualizar una credencial de registro

Cuando una credencial de registro deja de ser válida, se mostrará un icono de llave roja junto a la imagen de contenedor relacionada, como se muestra en la captura de pantalla a continuación.



Pase el ratón sobre el icono para ver el nombre de la credencial, luego cambie a la vista de **Credenciales** haciendo clic en la pestaña correspondiente en la esquina superior derecha. Encuentre la credencial que se identificó anteriormente en la lista de credenciales almacenadas y haga clic en el botón "**...**" de la derecha. Seleccione **Actualizar** para actualizar la información de la credencial.



Información relacionada

- Crear una imagen a partir de una existente
- Administrar cadenas de herramientas con Mise
- Administrar cadenas de herramientas con Nix
- Administrar cadenas de herramientas del espacio de trabajo
- Actualizar una imagen de contenedor existente
- Imágenes del espacio de trabajo

Update an existing container image

Descripción general

Este artículo se centra en el flujo de trabajo de la plataforma para actualizar una imagen de contenedor existente, de modo que los equipos puedan reutilizar una cadena de herramientas coherente y preconfigurada en todos los espacios de trabajo. Para la gestión diaria de la persistencia del software, consulte Cómo mantener cambios persistentes en su espacio de trabajo.

Por qué es importante la persistencia

Las imágenes de contenedor definen la configuración base de un entorno de desarrollo. Los usuarios crean espacios de trabajo a partir de una imagen como un *plano*, lo que ayuda a prevenir la desviación del entorno y acelera la incorporación.

Contexto: persistencia y scripts de inicio

En SecurSpaces, solo los datos en `/home/developer` son persistentes por defecto. Los cambios fuera de ese directorio (por ejemplo, instalaciones de paquetes a nivel de SO) no persisten entre los reinicios del espacio de trabajo.

La mejor práctica es mantener las herramientas compartidas (por ejemplo, entre un equipo, un proyecto, etc.) en una imagen base del espacio de trabajo, para que los equipos obtengan una cadena de herramientas coherente en todos los espacios de trabajo. Utilice los scripts de inicio solo para personalizaciones individuales, por ejemplo, específicas del usuario.

Para obtener detalles sobre el modelo de persistencia de los espacios de trabajo y cómo hacer que las instalaciones posteriores sean persistentes, consulte Cómo mantener cambios persistentes en su espacio de trabajo.

Administrar imágenes de contenedor (Recursos → Imágenes de contenedor)

> **Permiso:**

> Para añadir una imagen de espacio de trabajo, necesita que el permiso Recursos esté configurado en **Importar**.

> Las imágenes se importan desde un registro (público o privado). Los registros privados requieren credenciales; los registros públicos no.

Ver imágenes de contenedor

El panel **Imágenes de contenedor** (en **Recursos** → **Imágenes de contenedor**) muestra las imágenes disponibles en el ámbito seleccionado (proyecto, organización o plataforma). Puede buscar imágenes o filtrar las que se utilizan actualmente en los espacios de trabajo.

Añadir una imagen de contenedor

Para añadir una imagen:

1. Vaya a **Recursos** → **Imágenes de contenedor** para su proyecto.
2. Puede añadir imágenes de contenedor a nivel de proyecto, organización o plataforma (según sus permisos)
3. Seleccione **Añadir imagen**.
4. Proporcione la **URL**, el **Nombre de la imagen** y la **Etiqueta de la imagen**. Opcionalmente, configure el **Registro privado** y **Adjuntar información de activos**.

> **Advertencia:**

> Para conocer los requisitos de la imagen, consulte Requisitos de la imagen de contenedor.

(Opcional) Imágenes de ejemplo

Si desea ejemplos de imágenes de espacio de trabajo, Citrix publica tanto Dockerfiles como imágenes precompiladas:

- strong-network/images en GitHub — Dockerfiles y scripts de compilación que puede adaptar.
- strongnetwork en Docker Hub — imágenes precompiladas a las que puede hacer referencia directamente.

Haga que un entorno sea persistente para su equipo

Hay dos formas comunes de estandarizar las herramientas para un equipo:

Opción 1: Crear una nueva imagen de espacio de trabajo (donde sea compatible)

En las implementaciones de productos, Citrix SecurSpaces™ puede transformar un script de inicio en una nueva imagen de espacio de trabajo automáticamente cuando sea necesario. La disponibilidad de las funciones puede variar entre entornos.

Opción 2: Iniciar desde una imagen existente y estandarizar la configuración con scripts de inicio

Utilice esta opción cuando desee una base fiable y solo necesite aplicar la configuración o instalaciones más pequeñas al iniciar el espacio de trabajo. Los scripts de inicio pueden ejecutarse antes o después del inicio, dependiendo de si el espacio de trabajo debe esperar por ellos.

Puntos a considerar

- Solo `/home/developer` es persistente entre los reinicios del espacio de trabajo. Planifique las instalaciones en consecuencia (imagen, herramientas de espacio de usuario o script de inicio).
- Requisitos previos de la imagen: verificar SSH, GIT, GIT LFS y UID de desarrollador 1000 antes de compartir una imagen ampliamente.
- Gobernanza: considere restringir los registros permitidos y configurar los registros privados de forma centralizada (Restricciones de URL de imagen y Crear registro de imagen).

Referencias

- Mantener cambios persistentes en su espacio de trabajo
- Imágenes de contenedor
- Crear un espacio de trabajo
- Configuración de recursos (Restricciones de URL de imagen, Crear registro de imagen)
- Repositorio de imágenes de ejemplo en GitHub
- Imágenes precompiladas en Docker Hub

Preguntas frecuentes

- ¿Por qué desaparecieron mis herramientas instaladas después de un reinicio?

  Solo `/home/developer` es persistente. Cualquier otra cosa instalada debe integrarse en la imagen o volver a aplicarse al inicio.

- ¿Cuál es la forma más rápida de incorporar a un equipo?

  Proporcione una imagen de espacio de trabajo que incluya la cadena de herramientas compartida y mantenga solo la configuración dinámica en los scripts de inicio.

- ¿Cuándo debo usar post-start?

Use post-start para tareas pesadas, de modo que el espacio de trabajo esté disponible rápidamente mientras la configuración continúa en segundo plano.

Información relacionada

- Imágenes de contenedor
- Crear una imagen a partir de una existente
- Administrar cadenas de herramientas con Mise
- Administrar cadenas de herramientas con Nix
- Administrar cadenas de herramientas del espacio de trabajo
- Imágenes de espacio de trabajo

Create an image from an existing one

Requiere el conjunto de permisos Recursos para **Importar**.

La mayoría de los equipos necesitan una imagen estándar con algunas adiciones: un tiempo de ejecución de lenguaje, una CLI interna, un certificado. Mantener un Dockerfile y una canalización de compilación para eso es un trabajo desproporcionado.

Crear imagen a partir de existente lo hace en la plataforma. Usted elige una imagen base, proporciona un script bash, y Citrix SecurSpaces™ crea una nueva imagen con su script como la capa `RUN` final del Dockerfile, y luego la envía a su registro. El resultado aparece como una imagen de contenedor ordinaria que cualquier espacio de trabajo o plantilla puede usar.

Antes de empezar

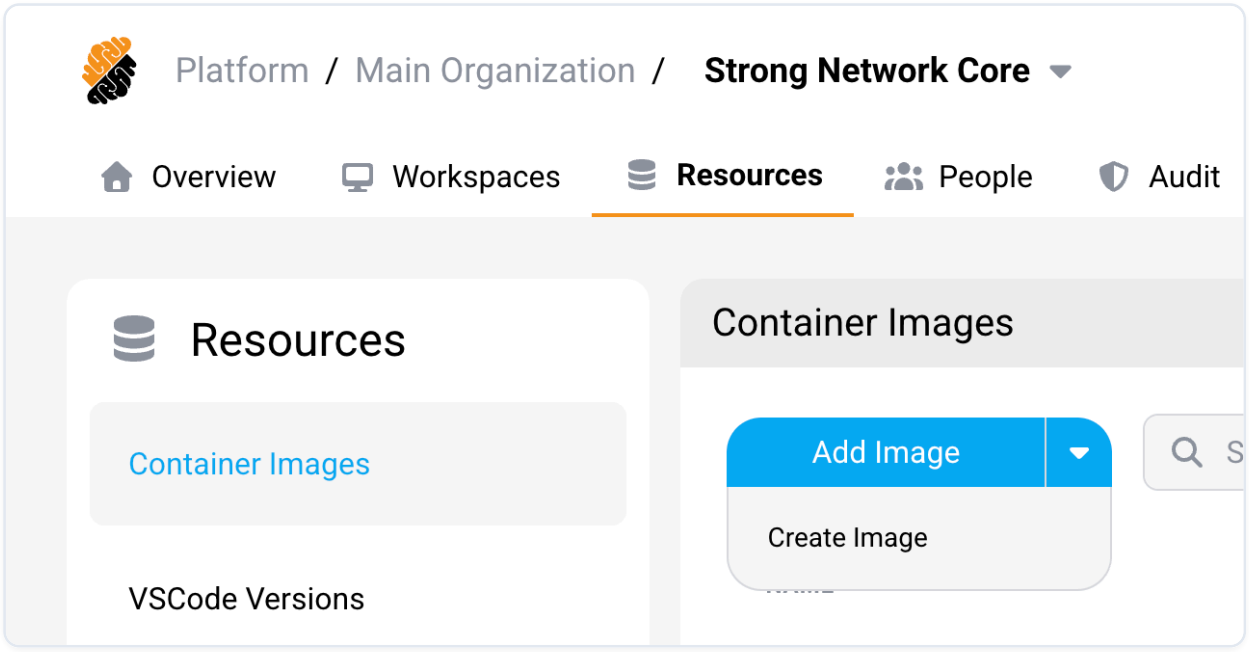
La opción solo aparece cuando un administrador de la plataforma ha configurado un **registro de destino**, que es el registro al que se envían las imágenes creadas en la plataforma. Hasta entonces, **Agregar imagen** es un botón simple sin menú desplegable.

Si no ve **Crear imagen**, falta esa configuración. Consulte Acceso al registro.

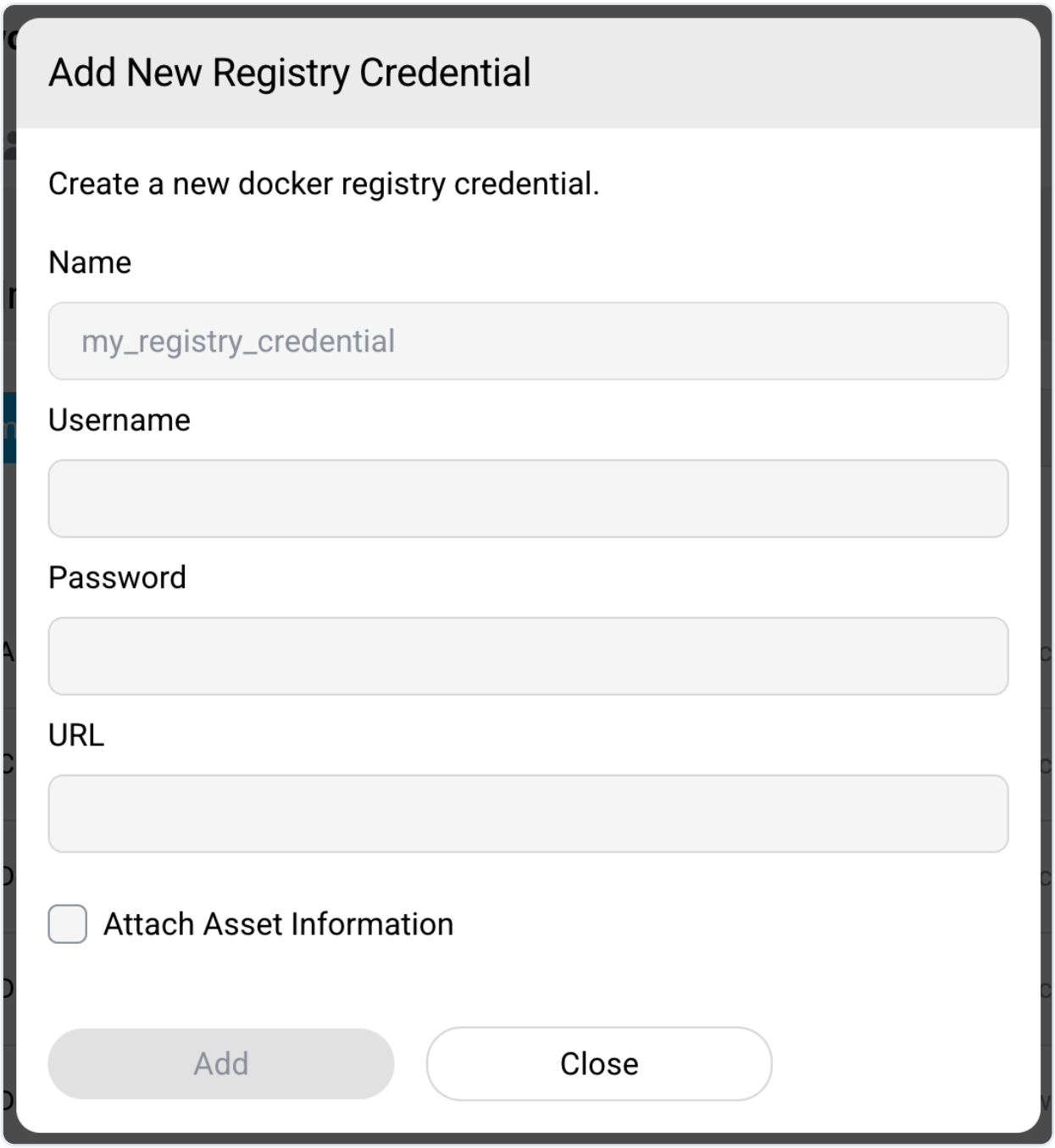
También necesita una **credencial de registro cuya URL coincida con el registro de destino**. La compilación se envía con ella, y los espacios de trabajo extraen la imagen final con ella. Si ninguna credencial coincide, el modal lo indica y **Confirmar** permanece deshabilitado.

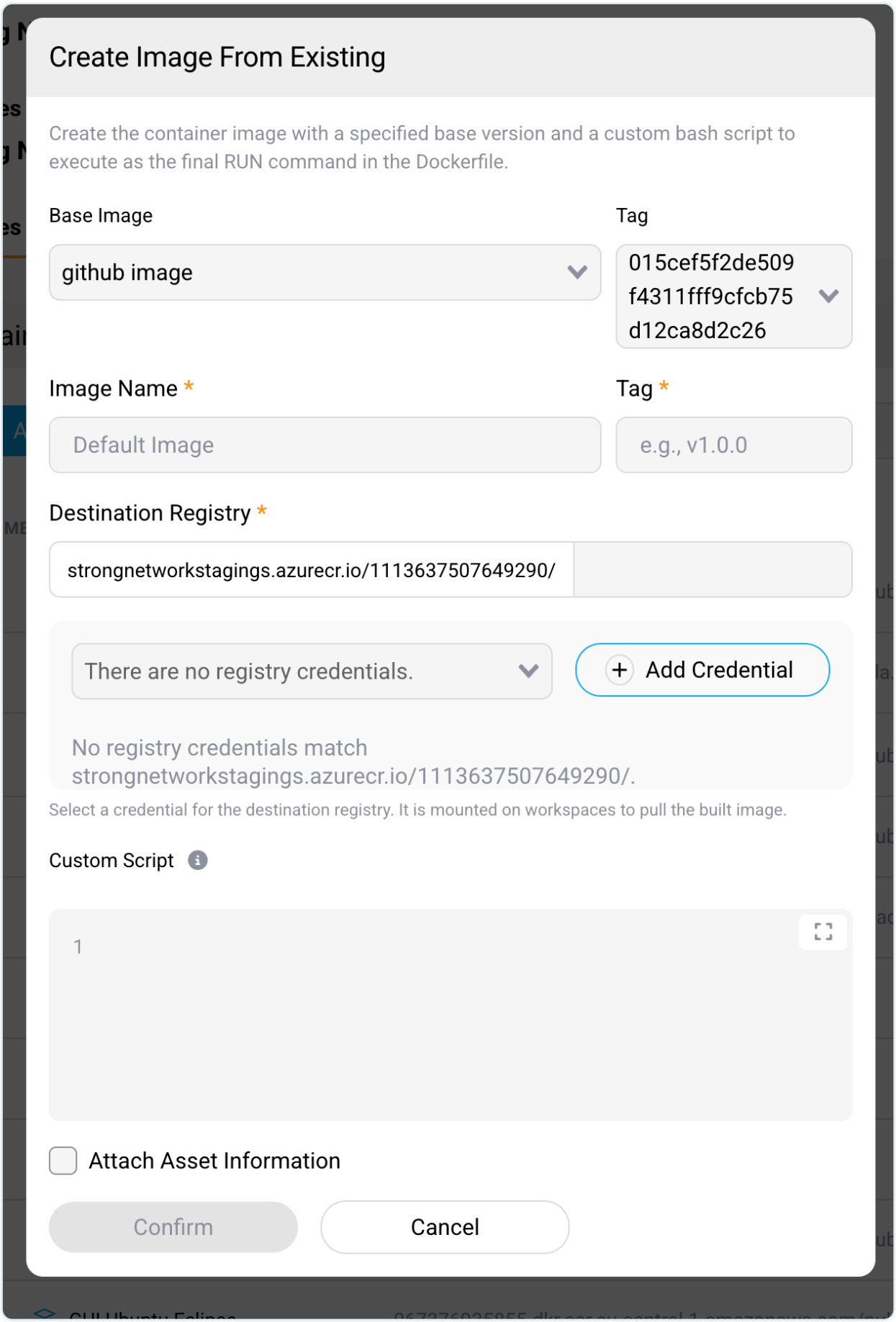
Crear la imagen

1. Abra **Recursos > Imágenes de contenedor**.
2. Seleccione la flecha junto a **Agregar imagen** y, a continuación, seleccione **Crear imagen**.



3. Elija la **Imagen base** y la **Etiqueta** sobre las que compilar.
4. Introduzca el **Nombre de la imagen** y la **Etiqueta** para la imagen que está creando, por ejemplo `v1.0.0`.
5. Compruebe el **Registro de destino**. Se rellena a partir de la configuración de la plataforma.
6. Seleccione una **credencial de registro** para ese registro. Si la lista está vacía, seleccione **Agregar credencial** y proporcione un nombre, nombre de usuario, contraseña y la URL del registro.


Add New Registry Credential
Create a new docker registry credential.
Name
my_registry_credential
Username
Password
URL
Attach Asset Information
Add
Close


Create Image From Existing
Create the container image with a specified base version and a custom bash script to execute as the final RUN command in the Dockerfile.
Base Image
github image
Tag
015cef5f2de509
f4311fff9cfcb75
d12ca8d2c26
Image Name *
Default Image
Tag *
e.g., v1.0.0
Destination Registry *
strongnetworkstagings.azurecr.io/1113637507649290/
There are no registry credentials.
Add Credential
No registry credentials match strongnetworkstagings.azurecr.io/1113637507649290/.
Select a credential for the destination registry. It is mounted on workspaces to pull the built image.
Custom Script
1
Attach Asset Information
Confirm
Cancel

7. Introduzca su **Script personalizado**. Se ejecuta como el último comando `RUN` en el Dockerfile generado.
8. Seleccione **Confirmar**.

La compilación se ejecuta en el clúster. Cuando finaliza, la imagen aparece junto con sus otras imágenes de contenedor.

Escribir el script

El script es una única capa `RUN` añadida a la imagen base, por lo que se aplican las reglas habituales de Dockerfile:

- Se ejecuta como parte de la compilación, no al inicio del espacio de trabajo. Todo lo que instala se integra en la imagen.
- Se ejecuta de forma no interactiva. Los comandos que solicitan entrada se colgarán hasta que expire el plazo de compilación.
- Solo persisten los cambios en el sistema de archivos. Las variables de entorno establecidas con `export` no sobreviven a la capa.
- La imagen base debe seguir cumpliendo los requisitos de la imagen de contenedor después de que se haya ejecutado su script; en particular, el usuario `developer` con UID 1000, y los clientes SSH, Git y Git LFS clientes.

Mantenga el script con lo que realmente comparte el equipo. Un paso específico del espacio de trabajo pertenece a un script de inicio, que se ejecuta al inicio y se puede cambiar sin necesidad de reconstruir.

Límites de compilación

Las compilaciones se ejecutan como un trabajo de Kubernetes con límites fijos. Una compilación que los exceda fallará en lugar de degradar el clúster:

LÍMITE	PREDETERMINADO
CPU	500m solicitados, 2 núcleos máximo
Memoria	1 GiB solicitado, 4 GiB máximo
Tiempo real	30 minutos
Reintentos	Ninguno — se informa de una compilación fallida, nunca se reintenta

Una compilación grande o un script que descarga una gran cantidad de datos puede exceder el límite de memoria o el plazo. Si eso ocurre, mueva el trabajo pesado a una imagen base construida por su propia canalización, y use esta característica para la capa delgada superior.

Un administrador de plataforma puede aumentar estos límites con `imageBuilderSpecification` en los valores de Helm, que acepta `cpuRequest`, `cpuLimit`, `memoryRequest`, `memoryLimit` y `deadlineSeconds`. Los límites se aumentan para que coincidan con las solicitudes si están configurados a un valor inferior.

Cómo se aísla la compilación

Su script es código arbitrario y se ejecuta en el clúster. SecurSpaces lo compila en un entorno aislado (sandbox) en lugar de en un demonio de Docker:

- La compilación ejecuta **BuildKit sin privilegios de root** dentro de un espacio de nombres de usuario, como un usuario no root.
- El contenedor no tiene privilegios, descarta todas las capacidades de Linux y el propio proceso de compilación no posee ninguna.
- Los límites de CPU y memoria significan que un script descontrolado se detiene en lugar de agotar el nodo.
- El trabajo nunca se reintenta, por lo que un script colgado no puede reiniciarse indefinidamente, y se limpia después de que finaliza.

Por eso la función está restringida a una configuración a nivel de plataforma en lugar de estar disponible por defecto: activarla permite a los miembros del proyecto ejecutar código en tiempo de compilación en su clúster, dentro de ese entorno aislado.

Crear una imagen a partir de un espacio de trabajo

La misma compilación está disponible al editar un espacio de trabajo, en **Scripts de inicio**, como **crear una imagen personalizada basada en la imagen actual del espacio de trabajo, extendida con scripts de inicio seleccionados**. Úselo para promover scripts de inicio que se hayan integrado en la imagen, para que ya no se ejecuten en cada inicio.

Esa ruta requiere además que la imagen del espacio de trabajo tenga una credencial de registro adjunta.

Información relacionada

- Imágenes de contenedor
- Imágenes de espacio de trabajo

- Requisitos de imagen de contenedor
- Acceso al registro

Manage workspace toolchains

Un gestor de cadenas de herramientas permite a cada proyecto declarar los tiempos de ejecución de lenguaje y las herramientas que necesita en un archivo en su propio repositorio, de modo que una imagen de contenedor base sirve a muchos equipos. Citrix SecurSpaces™ documenta dos:

- Mise
- Nix

Ninguno está integrado en la plataforma. Ambos son herramientas comunes que se instalan en una imagen base, y ambos funcionan debido al mismo comportamiento de la plataforma, descrito a continuación.

Elija entre Mise y Nix

	MISE	NIX
Archivo de configuración	`mise.toml`	`flake.nix`
Primer inicio típico	10–60 segundos	30–120 segundos
Qué persiste por defecto	Las herramientas se instalan bajo `/home/developer`, que persiste	El almacén de Nix está en `/nix`, que **no** persiste a menos que añadas un volumen
Reproducibilidad	Versiones de herramientas fijadas	Cierres de dependencias completamente fijados a través de `flake.lock`
Curva de aprendizaje	Baja. Familiar para cualquiera que haya usado `asdf` o `nvm`.	Más alta. Requiere aprender el lenguaje Nix.

Elige **Mise** cuando quieras versiones de herramientas por proyecto con una configuración mínima, y tus equipos se sientan cómodos fijando versiones en un archivo simple.

Elige **Nix** cuando necesites entornos reproducibles bit a bit y estés preparado para configurar un volumen persistente para `/nix` e invertir en el lenguaje Nix.

Comportamiento de la plataforma en el que ambos se basan

Solo `/home/developer` persiste

El contenedor del espacio de trabajo se recrea a partir de su imagen en cada inicio. `/home/developer` es un volumen persistente y sobrevive; todo lo demás no. Consulta Qué persiste en un espacio de trabajo de SecurSpaces.

Esto es lo que hace que un gestor de cadenas de herramientas sea práctico: las herramientas se descargan una vez y permanecen en los inicios posteriores.

Los archivos escritos durante la construcción de la imagen están ocultos

Un volumen persistente está vacío cuando se crea por primera vez, y montarlo oculta cualquier cosa que la construcción de la imagen haya escrito en esa ruta. Por lo tanto, instalar herramientas en `/home/developer` en un Dockerfile no tiene ningún efecto en tiempo de ejecución.

Instale en una ruta del sistema como `/usr/local`, y use un script de primer inicio para cualquier cosa que deba residir en el directorio de inicio.

Scripts de primer inicio

Los scripts en `/usr/bin/strong_network_startup/` de la imagen se ejecutan una vez, en el primer inicio, después de que `/home/developer` exista.

La plataforma registra que se han ejecutado creando `/home/developer/.strong_network_init`. Dado que ese marcador reside en el volumen persistente, los scripts se ejecutan de nuevo para cualquier espacio de trabajo con un nuevo volumen, y de nuevo si se elimina el marcador.

Estos son distintos de los scripts de inicio configurados en la consola, que se ejecutan en **cada** inicio. Consulte Scripts de inicio.

Certificados cuando se adjunta una política de red

Cuando un espacio de trabajo tiene una política de red adjunta, su tráfico saliente se enruta a través del proxy de salida de SecurSpaces, y el certificado del proxy se añade al almacén de confianza del sistema en `/etc/ssl/certs/ca-certificates.crt`.

La plataforma también configura varios ecosistemas que mantienen su propio almacén de confianza:

ECOSISTEMA	CONFIGURADO
el npm	`cafile`
el pip	`global.cert`
el yarn	`strict-ssl` deshabilitado
Node.js	`NODE_EXTRA_CA_CERTS`
Python `requests`	`REQUESTS_CA_BUNDLE`
Java	El certificado se importa en el almacén de claves de JDK
VS Code	`http.proxyStrictSSL` deshabilitado

Las herramientas que leen el almacén de confianza del sistema, incluyendo Mise y Nix, funcionan sin configuración adicional. Una herramienta que incluye su propio paquete de CA e ignora el almacén del sistema debe apuntar al certificado proxy explícitamente.

Consulte Políticas de red.

Escenario de ejemplo

Ambos ejemplos prácticos utilizan el mismo proyecto, una aplicación web que requiere:

- Node.js 22, el entorno de ejecución de la aplicación
- Python 3.13, para scripts de compilación y herramientas
- Terraform 1.x, para la gestión de infraestructura
- jq, para el procesamiento de JSON

Información relacionada

- Gestionar cadenas de herramientas de espacio de trabajo con Mise
- Gestionar cadenas de herramientas de espacio de trabajo con Nix
- Qué persiste en un espacio de trabajo de SecurSpaces
- Imágenes de espacio de trabajo
- Plantillas de espacio de trabajo

Manage workspace toolchains with Mise

En lugar de construir y mantener imágenes de contenedor separadas para cada equipo, puede usar Mise-en-Place (Mise) para definir cadenas de herramientas específicas del proyecto sobre una única imagen base. Mise es un gestor de versiones de herramientas de desarrollo políglota que permite a cada equipo declarar sus lenguajes, tiempos de ejecución y herramientas CLI requeridos en un archivo de configuración `mise.toml` que reside en el repositorio junto con el código.

¿Por qué usar Mise?

Mise simplifica la forma en que su organización gestiona las cadenas de herramientas de desarrollo en Citrix SecurSpaces™. Ofrece varios beneficios en comparación con el mantenimiento de múltiples imágenes de contenedor:

- **Menos imágenes que mantener.** Use una imagen base en toda su organización y permita que los equipos definan sus necesidades de herramientas por proyecto.
- **Incorporación más rápida.** Los desarrolladores clonan un repositorio y las herramientas se instalan automáticamente, sin configuración manual ni documentación obsoleta.
- **Entornos con control de versiones.** Las definiciones de la cadena de herramientas residen en Git, por lo que los cambios pasan por solicitudes de extracción y revisión de código como cualquier otro cambio de código.
- **Reinicios de espacio de trabajo más rápidos.** Debido a que los espacios de trabajo persisten el directorio `/home/developer`, las herramientas instaladas sobreviven entre sesiones. Después del primer inicio, los inicios posteriores se activan en menos de un segundo.
- **Autoservicio para desarrolladores.** Los equipos actualizan su propia cadena de herramientas sin solicitar una nueva imagen de contenedor al equipo de la plataforma.
- **Coherencia en todo el equipo.** Cada desarrollador de un proyecto obtiene las mismas versiones de herramientas, lo que reduce los problemas de "funciona en mi máquina".
- **No se requiere root para cambios en el tiempo de ejecución.** Los desarrolladores instalan o actualizan los tiempos de ejecución de lenguajes en su propio directorio de inicio, por lo que desaparecen los puntos de fricción comunes como los errores de permiso `npm install -g` o la contaminación del Python del sistema `pip`. La imagen base permanece inmutable.
- **Menos proliferación de imágenes.** En lugar de mantener una imagen separada para cada combinación de tiempos de ejecución (Python 3.10 + Node 18, Python 3.12 + Node 20, y así sucesivamente), una única imagen políglota permite a los desarrolladores elegir versiones por proyecto, lo que reduce el número de imágenes que construye, escanea y almacena.

Cómo funciona en SecurSpaces

El enfoque general sigue este patrón:

1. Su equipo de plataforma crea una única imagen de contenedor base con Mise preinstalado.
2. Cada equipo confirma un archivo de configuración `mise.toml` en su repositorio.
3. Cuando un desarrollador inicia un espacio de trabajo, Mise lee la configuración e instala las herramientas declaradas.
4. Dado que `/home/developer` persiste a través de los reinicios del espacio de trabajo, las herramientas instaladas permanecen disponibles en los inicios posteriores sin necesidad de volver a descargarlas.

Qué sucede en el primer inicio frente a los inicios posteriores

PRIMER INICIO DEL ESPACIO DE TRABAJO	INICIOS POSTERIORES
Descarga e instala las herramientas declaradas (normalmente de 10 a 60 segundos, dependiendo del número de herramientas)	Detecta las herramientas ya presentes; se activa instantáneamente (en menos de 1 segundo)

Escenario de ejemplo

Los ejemplos de esta guía utilizan un proyecto de aplicación web que requiere la siguiente cadena de herramientas:

- Node.js 22 (tiempo de ejecución de la aplicación)
- Python 3.13 (scripts de compilación y herramientas)
- Terraform 1.x (gestión de infraestructura)
- jq (procesamiento de JSON)

Configurar una imagen base de contenedor

Comience con la imagen genérica del repositorio de imágenes de SecurSpaces. Esta imagen se basa en Ubuntu 24.04 e incluye utilidades de desarrollo comunes como Git, Docker, kubectl y CLIs de la nube. Extienda esta imagen instalando Mise en tiempo de compilación. Esto asegura que Mise esté disponible inmediatamente cuando se inicia un espacio de trabajo, sin que los desarrolladores tengan que instalarlo ellos mismos. Cree un Dockerfile que extienda la imagen genérica:

```
FROM strongnetwork/generic:latest



USER root



# Install Mise for all users

RUN curl https://mise.run | MISE_INSTALL_PATH=/usr/local/bin/mise sh



# Add a first-start script that configures Mise for the developer user.

# Scripts in /usr/bin/strong_network_startup/ run automatically on first

# workspace start, after /home/developer has been created.

COPY setup-mise.sh /usr/bin/strong_network_startup/setup-mise.sh

RUN chmod +x /usr/bin/strong_network_startup/setup-mise.sh



USER 1000

WORKDIR /home/developer
```

Cree `setup-mise.sh` junto a su Dockerfile:

```
#!/bin/bash

# setup-mise.sh — runs once on first workspace start

# At this point /home/developer exists and is writable.



if ! grep -q 'mise activate' /home/developer/.bashrc 2>/dev/null; then
```

```
  echo 'eval "$(mise activate bash)"' >> /home/developer/.bashrc

fi
```

¿Por qué no escribir en `.bashrc` en el Dockerfile? El directorio `/home/developer` no existe durante las fases iniciales de inicio de un nuevo espacio de trabajo. Se crea más tarde en el flujo de inicio. Los scripts colocados en `/usr/bin/strong_network_startup/` se ejecutan después de que `/home/developer` esté disponible, por lo que pueden escribir en él de forma segura. Mise instala herramientas en `~/.local/share/mise/installs/` por defecto. Debido a que esta ruta está dentro de `/home/developer`, todas las herramientas instaladas persisten a través de los reinicios del espacio de trabajo.

Reforzar la instalación de Mise para producción

El patrón `curl https://mise.run | sh` anterior es conveniente para empezar, pero la mayoría de los entornos de producción querrán controles de cadena de suministro más estrictos. Dos cambios convierten la imagen base en una instalación de Mise lista para producción:

1. Reemplace el instalador remoto con una descarga fija de su propio registro de artefactos.
2. Aplique la configuración de Mise a nivel de sistema (réplicas de registro, proxy, complementos permitidos) en `/etc/mise/config.toml` para que se apliquen a cada desarrollador.

Instalar Mise desde un registro de artefactos interno

Evite ejecutar scripts de instalador remoto en el momento de la construcción de la imagen. En su lugar, replique la versión de Mise en su registro de artefactos interno (por ejemplo, JFrog Artifactory) y descárguela durante la construcción con una solicitud autenticada y con versión fija. Utilice secretos de construcción de BuildKit para que el token del registro nunca termine en una capa de imagen.

Cree un script de instalación reforzado junto a su Dockerfile:

```
#!/bin/bash

# install-mise.sh — downloads a pinned Mise release from JFrog Artifactory

set -euo pipefail



MISE_URL="https://artifactory.example.com/artifactory/generic-local/mise/
```

```
v${MISE_VERSION}"

INSTALL_PATH="/usr/local/bin/mise"



# Resolve the architecture-specific asset name

case "$(uname -m)" in

  x86_64)  MISE_ARCH="x64" ;;

  aarch64) MISE_ARCH="arm64" ;;

  *) echo "Unsupported architecture: $(uname -m)"; exit 1 ;;

esac

FILENAME="mise-v${MISE_VERSION}-linux-${MISE_ARCH}.tar.gz"



# Download and verify

curl -fsSL -H "Authorization: Bearer ${JF_TOKEN}" \

  "${MISE_URL}/${FILENAME}" -o /tmp/mise.tar.gz

curl -fsSL -H "Authorization: Bearer ${JF_TOKEN}" \

  "${MISE_URL}/${FILENAME}.sha256" -o /tmp/mise.tar.gz.sha256

(cd /tmp && sha256sum -c mise.tar.gz.sha256)



tar -xzf /tmp/mise.tar.gz -C /usr/local/bin --strip-components=1 bin/mise

chmod +x "${INSTALL_PATH}"

rm /tmp/mise.tar.gz /tmp/mise.tar.gz.sha256
```

Luego, llame al script desde el Dockerfile, pasando el token del registro como un secreto de construcción:

```
ARG MISE_VERSION=2026.2.20



USER root



COPY install-mise.sh /tmp/install-mise.sh

COPY mise-config.toml /etc/mise/config.toml



RUN --mount=type=secret,id=jfrog_token \

    JF_TOKEN="$(cat /run/secrets/jfrog_token)" \

    MISE_VERSION="${MISE_VERSION}" \

    bash /tmp/install-mise.sh && \

    rm /tmp/install-mise.sh



RUN echo 'eval "$(mise activate bash)"' >> /etc/bash.bashrc
```

Construya la imagen con el secreto vinculado desde su entorno de CI, por ejemplo:

```
DOCKER_BUILDKIT=1 docker build \

  --secret id=jfrog_token,env=JFROG_TOKEN \

  -t your-registry/sds-base:latest .
```

El token está disponible solo para el paso `RUN` que lo monta y nunca se escribe en una capa de imagen.

Aplicar la configuración de Mise a nivel de sistema

La configuración que debe aplicarse a cada desarrollador —réplicas de registro, un proxy interno, una lista blanca de complementos— pertenece a `/etc/mise/config.toml`. Debido a que el archivo reside en la capa del contenedor, no puede ser sobrescrito por cambios dentro de `/home/developer`, y se vuelve a aplicar en cada inicio del espacio de trabajo.

Una configuración mínima que apunta Mise a réplicas internas:

```
[settings]

# Rewrite outbound download URLs to your internal mirror

url_replacements = { "github.com" = "artifactory.example.com/github-
mirror" }



[settings.node]

mirror_url = "https://artifactory.example.com/artifactory/nodejs-dist"



[settings.python]

# Resolve Python builds from your internal mirror of python-build-
standalone

mirror_url = "https://artifactory.example.com/artifactory/python-build-
standalone"
```

Los desarrolladores aún pueden añadir sus propios `mise.toml` por proyecto, pero no pueden eludir las restricciones de espejo, proxy o plugin a nivel de sistema definidas aquí. Para ver la lista completa de configuraciones disponibles, consulte la referencia de configuración de Mise.

Habilitar Mise en espacios de trabajo existentes

El enfoque de imagen de contenedor anterior funciona para los nuevos espacios de trabajo creados a partir de la imagen actualizada. Para los espacios de trabajo existentes que ya están en ejecución, utilice un script de inicio del espacio de trabajo en su lugar. Configure un script de inicio en la consola de SecurSpaces (en las propiedades del espacio de trabajo o como parte de la

plantilla del espacio de trabajo). El script comprueba si Mise ya está configurado y solo ejecuta la instalación si es necesario:

```
#!/bin/bash

# Workspace startup script — configure in the SecurSpaces console or
workspace template



# Install Mise if not already present

if ! command -v mise &> /dev/null; then

  curl https://mise.run | MISE_INSTALL_PATH=/home/developer/.local/bin/
mise sh

fi



# Activate Mise in the shell if not already configured

if ! grep -q 'mise activate' /home/developer/.bashrc 2>/dev/null; then

  echo 'eval "$(mise activate bash)"' >> /home/developer/.bashrc

fi



# Source Mise for the current script session

eval "$(mise activate bash)"



# Install project tools if a mise.toml exists

if [ -f /home/developer/project/mise.toml ]; then

  cd /home/developer/project
```

```
  mise install

fi
```

Dado que este script comprueba las instalaciones existentes antes de actuar, es seguro ejecutarlo en cada inicio del espacio de trabajo. En un espacio de trabajo ya configurado, se completa en menos de un segundo.

Defina la cadena de herramientas de su proyecto

Una vez que su imagen base incluya Mise, cada equipo define su cadena de herramientas en un archivo `mise.toml` en la raíz de su repositorio:

```
[tools]

node = "22"

python = "3.13"

terraform = "1"

jq = "latest"
```

Cuando un desarrollador abre un espacio de trabajo y navega al directorio del proyecto, Mise instala automáticamente las versiones de herramientas especificadas y las añade al `PATH` del shell.

Instalar herramientas al iniciar el espacio de trabajo

Si desea que las herramientas estén preinstaladas antes de que el desarrollador abra un terminal, añada `mise install` a su script de inicio del espacio de trabajo (consulte Habilitar Mise en espacios de trabajo existentes para ver el patrón de script completo). El comando esencial es:

```
cd /home/developer/project

mise install
```

En el primer inicio, esto descarga e instala todas las herramientas declaradas. En los inicios posteriores, Mise detecta que las herramientas ya están presentes y se completa en menos de un segundo.

Usar variables de entorno y tareas

Mise también gestiona las variables de entorno y las tareas del proyecto. Añádalas al mismo `mise.toml`:

```
[tools]

node = "22"

python = "3.13"

terraform = "1"

jq = "latest"



[env]

NODE_ENV = "development"

AWS_REGION = "eu-west-1"



[tasks]

dev = "npm run dev"

test = "npm test"

lint = "npm run lint && terraform validate"
```

Los desarrolladores pueden ejecutar `mise run dev` o `mise run test` y las herramientas y variables de entorno correctas se cargarán automáticamente. Para obtener todos los detalles sobre la configuración de Mise, consulte la documentación de Mise.

Preinstalar herramientas en el momento de la creación de la imagen

El flujo de trabajo predeterminado de Mise instala las herramientas en `/home/developer/.local/share/mise/installs/` la primera vez que se inicia un espacio de trabajo. Esto mantiene la imagen base pequeña, pero significa que los desarrolladores esperan la

descarga en el primer inicio y el espacio de trabajo necesita acceso a la red a un registro (o un espejo interno) en ese momento.

Si quieres que un tiempo de ejecución específico esté disponible inmediatamente en el primer inicio —por ejemplo, porque tu equipo siempre usa Node 22, o porque tus espacios de trabajo tienen egreso restringido—, integra la herramienta en la imagen durante el tiempo de compilación.

Instalar herramientas globalmente en un directorio de datos compartido de Mise

Establece `MISE_DATA_DIR` a una ruta del sistema (como `/usr/share/mise`) durante la compilación y crea un enlace simbólico del binario resultante en `/usr/bin`. Esto hace que el tiempo de ejecución esté disponible para cada desarrollador de inmediato, sin consumir espacio en el volumen persistente:

```
USER root



# Install Node 22 globally into /usr/share/mise and expose it on PATH

RUN MISE_DATA_DIR=/usr/share/mise mise use -g node@22 && \

    ln -s "$(MISE_DATA_DIR=/usr/share/mise mise which node)" /usr/bin/node
```

La herramienta instalada de esta manera reside en la capa del contenedor, por lo que está disponible inmediatamente en cada inicio del espacio de trabajo sin necesidad de descarga. Los desarrolladores aún pueden añadir su propio `mise.toml` por proyecto para superponer versiones adicionales o diferentes — Mise resuelve primero las herramientas con ámbito de proyecto desde `~/.local/share/mise/installs/` y recurre al directorio compartido.

Este patrón es la elección correcta cuando:

- Una versión específica del tiempo de ejecución es obligatoria para el equipo y no debería necesitar ser descargada de nuevo.
- El egreso del espacio de trabajo está restringido y no puedes confiar en que `mise install` tenga éxito en tiempo de ejecución.
- Quieres un rendimiento predecible en el primer inicio, independientemente de la latencia del registro.

Preinstalar con un script de primer inicio (carga diferida)

Si prefieres mantener la imagen base pequeña pero aun así evitar pedir a los desarrolladores que instalen herramientas manualmente, usa un script de primer inicio que ejecute `mise use --global` para el tiempo de ejecución requerido. La descarga ocurre una vez, en el primer inicio, y persiste en `/home/developer` para los inicios posteriores.

Coloca el script en `/usr/bin/strong_network_startup/` en tu imagen:

```
#!/bin/bash

# /usr/bin/strong_network_startup/install-node.sh — runs once, on first start

mise use --global node@22
```

```
COPY --chmod=755 install-node.sh /usr/bin/strong_network_startup/install-node.sh
```

Esto mantiene la imagen pequeña, pero aún requiere acceso a la red a un registro de Mise (o a tu espejo interno) en el primer inicio.

Comprender la persistencia del espacio de trabajo

Mise instala herramientas en `/home/developer`, que persiste a través de los reinicios, por lo que las herramientas se descargan una sola vez.

RUTA	PERSISTE
`/home/developer/.local/share/mise/installs/`	Sí. Binarios de herramientas.
`/home/developer/.local/share/mise/`	Sí. Metadatos y shims de herramientas.
`/home/developer/.cache/mise/`	Sí. Caché de descarga.
`/usr/local/bin/mise`	Parte de la capa de la imagen, siempre presente
Paquetes instalados con `apt-get` en tiempo de ejecución	No

El primer inicio siempre descarga herramientas, porque el volumen persistente está vacío y oculta cualquier cosa que la imagen de compilación escribió en esa ruta. Para acortarlo, aloje un espejo binario interno y fije las versiones en lugar de usar `latest`, lo que evita una búsqueda de la versión más reciente.

Para el modelo de persistencia completo, consulte Administrar cadenas de herramientas del espacio de trabajo y Qué persiste en un espacio de trabajo de SecurSpaces.

Consideraciones de red y seguridad

Mise descarga binarios de registros externos en tiempo de ejecución. Si su implementación de SecurSpaces aplica controles de egreso, permita el acceso a los siguientes dominios:

- `mise.run` — instalador
- `github.com` y `api.github.com` — descargas de herramientas y resolución de versiones
- `nodejs.org`, `python.org` y registros ascendentes similares según las herramientas utilizadas

Alternativamente, configure espejos internos para estos registros y apunte Mise a sus URL internas. Consulte Reforzar la instalación de Mise para producción para ver un ejemplo que replica el propio Mise y aplica configuraciones de espejo a nivel de sistema, y la documentación de configuración de Mise para obtener detalles sobre cómo configurar registros personalizados.

> **Nota:**
>
> Cuando un espacio de trabajo tiene una política de red adjunta, su tráfico se enruta a través del servicio de proxy de SecurSpaces y el certificado del proxy se añade al almacén de confianza del sistema. Ambas herramientas leen ese almacén, por lo que no se necesita ninguna configuración de certificado adicional. Consulte Certificados cuando se adjunta una política de red.

Próximos pasos

- Documentación de Mise — referencia completa para la gestión de herramientas, tareas y variables de entorno
- Repositorio de imágenes de espacio de trabajo de SecurSpaces — imágenes de contenedor base y genéricas para SecurSpaces

- Plantillas de espacio de trabajo — configure scripts de inicio y ajustes de recursos en sus plantillas de espacio de trabajo
- Administrar cadenas de herramientas del espacio de trabajo — elección entre Mise y Nix, y el comportamiento de la plataforma en el que ambos se basan

Información relacionada

- Imágenes de contenedor
- Crear una imagen a partir de una existente
- Administrar cadenas de herramientas con Nix
- Administrar cadenas de herramientas del espacio de trabajo
- Actualizar una imagen de contenedor existente
- Imágenes del espacio de trabajo

Manage workspace toolchains with Nix

En lugar de construir y mantener imágenes de contenedor separadas para cada equipo, puede usar Nix Package Manager (Nix) para definir cadenas de herramientas específicas del proyecto sobre una única imagen base. Nix es un gestor de paquetes puramente funcional que permite a cada equipo declarar sus lenguajes, tiempos de ejecución y paquetes de sistema requeridos en un archivo de configuración `flake.nix` que reside en el repositorio junto con el código.

¿Por qué usar Nix?

Nix simplifica la forma en que su organización gestiona las cadenas de herramientas de desarrollo en Citrix SecurSpaces™. Ofrece varios beneficios sobre el mantenimiento de múltiples imágenes de contenedor:

- **Menos imágenes que mantener.** Use una imagen base en toda su organización y permita que los equipos definan sus necesidades de herramientas por proyecto.
- **Incorporación más rápida.** Los desarrolladores clonan un repositorio y las herramientas se instalan automáticamente, sin configuración manual ni documentación obsoleta.
- **Entornos con control de versiones.** Las definiciones de la cadena de herramientas residen en Git, por lo que los cambios pasan por solicitudes de extracción y revisión de código como cualquier otro cambio de código.
- **Reinicios de espacio de trabajo más rápidos.** Con un almacén Nix persistente, los paquetes instalados sobreviven entre sesiones. Después del primer inicio, los inicios posteriores se activan en menos de un segundo.

- **Autoservicio para desarrolladores.** Los equipos actualizan su propia cadena de herramientas sin solicitar una nueva imagen de contenedor al equipo de plataforma.
- **Consistencia en todo el equipo.** Cada desarrollador de un proyecto obtiene las mismas versiones de herramientas, lo que reduce los problemas de "funciona en mi máquina".
- **Compilaciones reproducibles.** Nix garantiza que si un paquete se compila en una máquina, se compila de forma idéntica en otra: los paquetes están aislados e identificados por hashes criptográficos de todo su grafo de dependencias.

Cómo funciona en SecurSpaces

El enfoque general sigue este patrón:

1. Su equipo de plataforma crea una única imagen de contenedor base con Nix preinstalado.
2. Cada equipo confirma un archivo de configuración `flake.nix` en su repositorio.
3. Cuando un desarrollador inicia un espacio de trabajo, Nix lee la configuración y descarga los paquetes declarados.
4. Con un almacén Nix persistente, los paquetes instalados permanecen disponibles en los arranques posteriores sin necesidad de volver a descargarlos.

¿Qué ocurre en el primer arranque frente a los arranques posteriores?

PRIMER ARRANQUE DEL ESPACIO DE TRABAJO	ARRANQUES POSTERIORES
Descarga los cierres de paquetes de la caché binaria (normalmente de 30 a 120 segundos, dependiendo del número de paquetes)	Paquetes ya en el almacén; se activa al instante (en menos de 1 segundo)

> **Importante:**
>
> Esto asume que has configurado la persistencia para el almacén Nix. Sin ella, Nix vuelve a descargar los paquetes en cada reinicio. Consulta Configurar la persistencia para Nix para ver las opciones de configuración.

Escenario de ejemplo

Los ejemplos de esta guía utilizan un proyecto de aplicación web que requiere la siguiente cadena de herramientas:

- Node.js 22 (tiempo de ejecución de la aplicación)
- Python 3.13 (scripts de compilación y herramientas)
- Terraform 1.x (gestión de infraestructura)
- jq (procesamiento de JSON)

Configurar una imagen de contenedor base

Comience con la imagen genérica del repositorio de imágenes de SecurSpaces. Esta imagen se basa en Ubuntu 24.04 e incluye utilidades de desarrollo comunes como Git, Docker, kubectl y CLIs de la nube.

Extienda esta imagen instalando Nix en tiempo de compilación. Esto asegura que Nix esté disponible inmediatamente cuando se inicia un espacio de trabajo, sin que los desarrolladores tengan que instalarlo ellos mismos.

Cree un Dockerfile que extienda la imagen genérica:

```
FROM strongnetwork/generic:latest



USER root



# Install Nix in single-user mode (installs to /nix)

RUN curl -L https://nixos.org/nix/install | sh -s -- --no-daemon



# Add a first-start script that configures Nix for the developer user.

# Scripts in /usr/bin/strong_network_startup/ run automatically on first

# workspace start, after /home/developer has been created.

COPY setup-nix.sh /usr/bin/strong_network_startup/setup-nix.sh

RUN chmod +x /usr/bin/strong_network_startup/setup-nix.sh
```

```
USER 1000

WORKDIR /home/developer
```

Cree `setup-nix.sh` junto a su Dockerfile:

```
#!/bin/bash

# setup-nix.sh — runs once on first workspace start

# At this point /home/developer exists and is writable.



if ! grep -q 'nix-profile' /home/developer/.bashrc 2>/dev/null; then

  echo '. /nix/var/nix/profiles/default/etc/profile.d/nix.sh' >> /home/
developer/.bashrc

fi
```

¿Por qué no escribir en `.bashrc` en el Dockerfile? El directorio `/home/developer` no existe durante las fases iniciales de inicio de un nuevo espacio de trabajo. Se crea más tarde en el flujo de inicio. Los scripts colocados en `/usr/bin/strong_network_startup/` se ejecutan después de que `/home/developer` esté disponible, por lo que pueden escribir en él de forma segura.

Habilitar Nix en espacios de trabajo existentes

El enfoque de imagen de contenedor anterior funciona para nuevos espacios de trabajo creados a partir de la imagen actualizada. Para los espacios de trabajo existentes que ya están en ejecución, utilice un script de inicio de espacio de trabajo en su lugar. Configure un script de inicio en la consola de SecurSpaces (en las propiedades del espacio de trabajo o como parte de la plantilla del espacio de trabajo). El script comprueba si Nix ya está configurado y solo ejecuta la instalación si es necesario:

```
#!/bin/bash

# Workspace startup script — configure in the SecurSpaces console or
workspace template
```

```
# Install Nix if not already present
if [ ! -d /nix ]; then
  curl -L https://nixos.org/nix/install | sh -s -- --no-daemon
fi

# Activate Nix in the shell if not already configured
if ! grep -q 'nix-profile' /home/developer/.bashrc 2>/dev/null; then
  echo '. /nix/var/nix/profiles/default/etc/profile.d/nix.sh' >> /home/
developer/.bashrc
fi

# Source Nix for the current script session
. /nix/var/nix/profiles/default/etc/profile.d/nix.sh

# Build the development environment if a flake.nix exists
if [ -f /home/developer/project/flake.nix ]; then
  cd /home/developer/project
  nix develop --command true
fi
```

Dado que este script comprueba las instalaciones existentes antes de actuar, es seguro ejecutarlo en cada inicio de espacio de trabajo. En un espacio de trabajo ya configurado, se completa en menos de un segundo.

Defina su cadena de herramientas de proyecto

Una vez que su imagen base incluye Nix, cada equipo define su entorno en un archivo `flake.nix` en la raíz de su repositorio:

```
{
  description = "Web application development environment";

  inputs = {
    nixpkgs.url = "github:NixOS/nixpkgs/nixos-unstable";
  };

  outputs = { self, nixpkgs }:
    let
      system = "x86_64-linux";
      pkgs = nixpkgs.legacyPackages.${system};
    in
    {
      devShells.${system}.default = pkgs.mkShell {
        packages = [
          pkgs.nodejs_22
          pkgs.python313
          pkgs.terraform
          pkgs.jq
```

```
        ];


        shellHook = ''
          export NODE_ENV="development"
          export AWS_REGION="eu-west-1"
        '';
      };
    };
}
```

Los desarrolladores entran en el entorno ejecutando `nix develop` desde el directorio del proyecto. Esto activa los paquetes declarados y establece las variables de entorno especificadas.

Instalar paquetes al iniciar el espacio de trabajo

Si desea que los paquetes se descarguen previamente antes de que el desarrollador abra un terminal, añada `nix develop --command true` a su script de inicio del espacio de trabajo (consulte Habilitar Nix en espacios de trabajo existentes para ver el patrón de script completo). El comando esencial es:

```
cd /home/developer/project

nix develop --command true
```

Esto construye y almacena en caché el entorno de desarrollo sin entrar en un nuevo shell. Los desarrolladores luego ejecutan `nix develop` de forma interactiva cuando están listos para trabajar.

Alternativamente, use direnv con la extensión nix-direnv para activar el entorno automáticamente al entrar en el directorio del proyecto.

Configurar la persistencia para Nix

Por defecto, Nix instala los paquetes en `/nix/store/`, que está fuera del directorio persistente `/home/developer`. Sin configuración adicional, Nix vuelve a descargar todos los paquetes en cada reinicio del espacio de trabajo.

Tienes tres opciones para hacer que los paquetes de Nix persistan:

1. **Añadir un volumen persistente en `/nix` (recomendado).** En tu plantilla de espacio de trabajo, configura un volumen persistente adicional montado en `/nix`. Este es el enfoque más sencillo y funciona con sustitutos estándar de Nix como `cache.nixos.org`.
2. **Usar un almacén local en el directorio de inicio.** Configura Nix para que use una ruta de almacén dentro del directorio de inicio persistente. Esto requiere soporte de espacio de nombres de usuario en el contenedor:

   ```
   nix develop --store /home/developer/.nix-store
   ```

   > **Nota:**
   >
   > Un almacén reubicado no puede usar la caché binaria predeterminada sin configuración adicional. Consulta el manual de Nix sobre almacenes locales para obtener más detalles.

3. **Usar nix-portable.** Un único binario que opera completamente dentro de `$HOME` sin requerir un montaje `/nix` a nivel de sistema. Consulta el repositorio de nix-portable para obtener instrucciones de configuración.

Comprender la persistencia del espacio de trabajo

Nix difiere de la mayoría de los gestores de cadenas de herramientas aquí: su almacén reside en `/nix`, fuera del directorio de inicio persistente. Sin un volumen persistente en `/nix`, los paquetes se vuelven a descargar en cada reinicio. Consulta Configurar la persistencia para Nix.

RUTA	PERSISTE
`/home/developer/.bashrc`	Sí. Activación del shell.
`/home/developer/.nix-profile/`	Sí. Enlaces simbólicos a los paquetes activos.
`/nix/store/`	Solo con un volumen persistente en `/nix`

RUTA	PERSISTE
`/nix/var/`	Solo con un volumen persistente en `/nix`
Paquetes instalados con `apt-get` en tiempo de ejecución	No

El primer inicio siempre descarga paquetes, porque ambos volúmenes están vacíos al crearse y ocultan cualquier cosa que la compilación de la imagen haya escrito en esas rutas. Para acortarlo, ejecute una caché binaria de Nix como sustituto, y bloquee `flake.lock` a un commit específico de nixpkgs para que una actualización del canal ascendente no desencadene descargas inesperadas.

Para el modelo de persistencia completo, consulte Administrar cadenas de herramientas del espacio de trabajo y Qué persiste en un espacio de trabajo de SecurSpaces.

Consideraciones de red y seguridad

Nix descarga binarios de registros externos en tiempo de ejecución. Si su implementación de SecurSpaces aplica controles de salida, permita el acceso a los siguientes dominios:

- `cache.nixos.org` — caché binaria oficial
- `github.com` — entradas de flake y descargas de código fuente
- `channels.nixos.org` — metadatos del canal

Alternativamente, configure una caché binaria interna y apunte Nix a sus URL internas. Consulte la referencia de configuración de Nix para obtener detalles sobre cómo configurar sustitutos personalizados.

> **Nota:**

> Cuando un espacio de trabajo tiene una política de red adjunta, su tráfico se enruta a través del servicio proxy de SecurSpaces y el certificado proxy se añade al almacén de confianza del sistema. Ambas herramientas leen ese almacén, por lo que no se necesita ninguna configuración de certificado adicional. Consulte Certificados cuando se adjunta una política de red.

Próximos pasos

- Documentación de Nix — guías y referencia para flakes, paquetes y shells de desarrollo de Nix
- Búsqueda de Nixpkgs — busca entre los más de 120.000 paquetes Nix disponibles
- Repositorio de imágenes de espacio de trabajo de SecurSpaces — imágenes de contenedor base y genéricas para SecurSpaces
- Plantillas de espacio de trabajo — configure scripts de inicio y ajustes de recursos en sus plantillas de espacio de trabajo
- Administrar cadenas de herramientas del espacio de trabajo — elección entre Mise y Nix, y el comportamiento de la plataforma en el que ambos se basan

Información relacionada

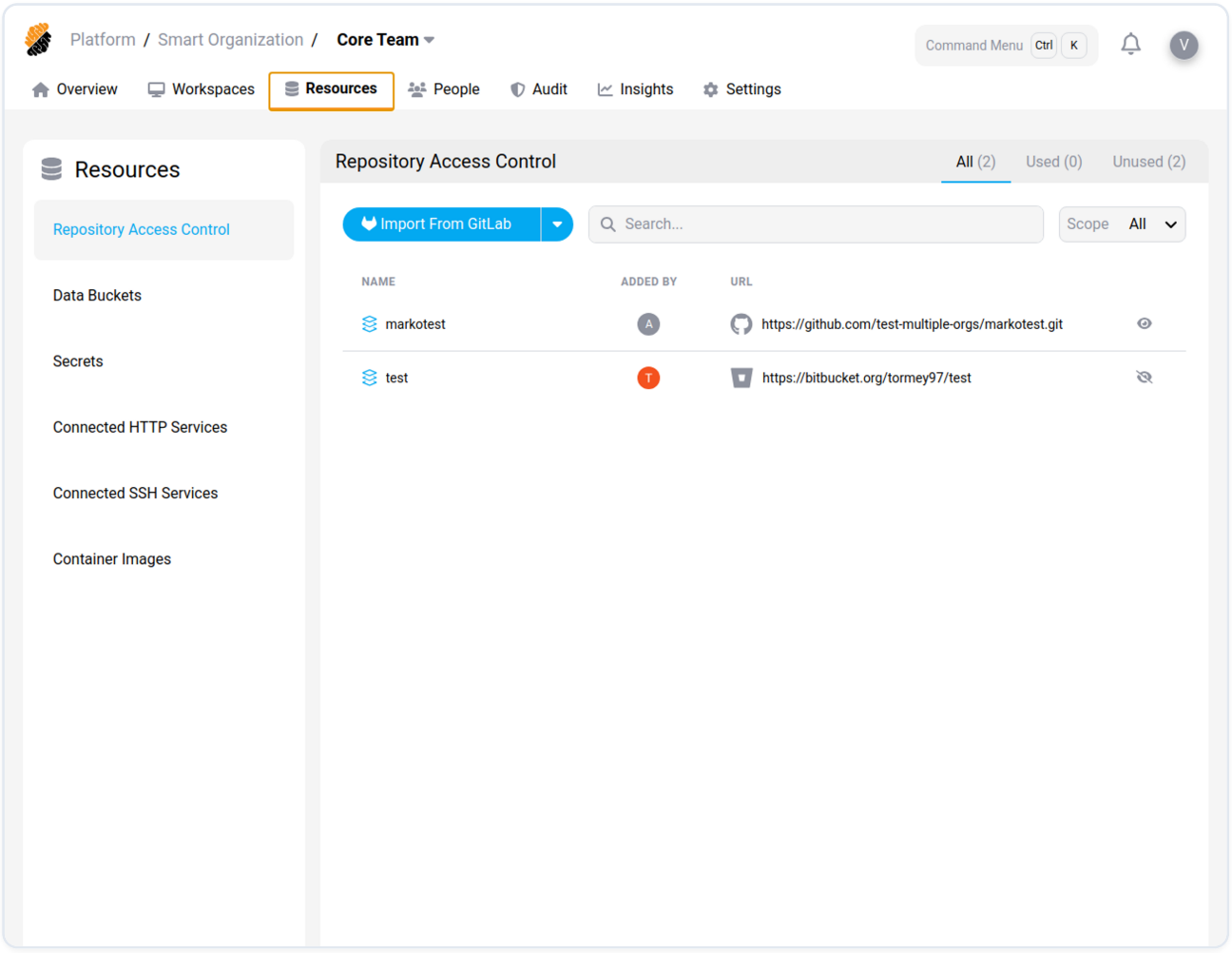
- Imágenes de contenedor
- Crear una imagen a partir de una existente
- Administrar cadenas de herramientas con Mise
- Administrar cadenas de herramientas del espacio de trabajo
- Actualizar una imagen de contenedor existente
- Imágenes de espacio de trabajo

Project resources

En la página de recursos, puede ver y gestionar los diferentes recursos utilizados en el proyecto.

Los recursos se utilizan para definir propiedades del espacio de trabajo, como la configuración de contenedores y las políticas de red, o la información disponible para los usuarios para el desarrollo como repositorios de código, depósitos de datos, secretos y servicios. Los recursos se gestionan en tres niveles de granularidad según el ámbito de uso previsto: plataforma, organización y proyecto.

Los recursos se adjuntan a un espacio de trabajo durante el proceso de configuración y actualización. Cuando los recursos son accesibles para los usuarios, este proceso es un medio para definir una política de control de acceso de grano fino para cada espacio de trabajo individual.



Contenido

- Control de acceso al repositorio
- Depósitos de datos
- Secretos
- Servicios HTTP conectados
- Servicios SSH conectados
- Imágenes de contenedor

Code repositories

Importar un repositorio en un proyecto es lo que permite a un desarrollador clonar y enviar sin tener credenciales propias. Citrix SecurSpaces™ inyecta las credenciales en tiempo de ejecución, a través del proxy, para que el dispositivo del desarrollador nunca necesite acceso Git a su código fuente.

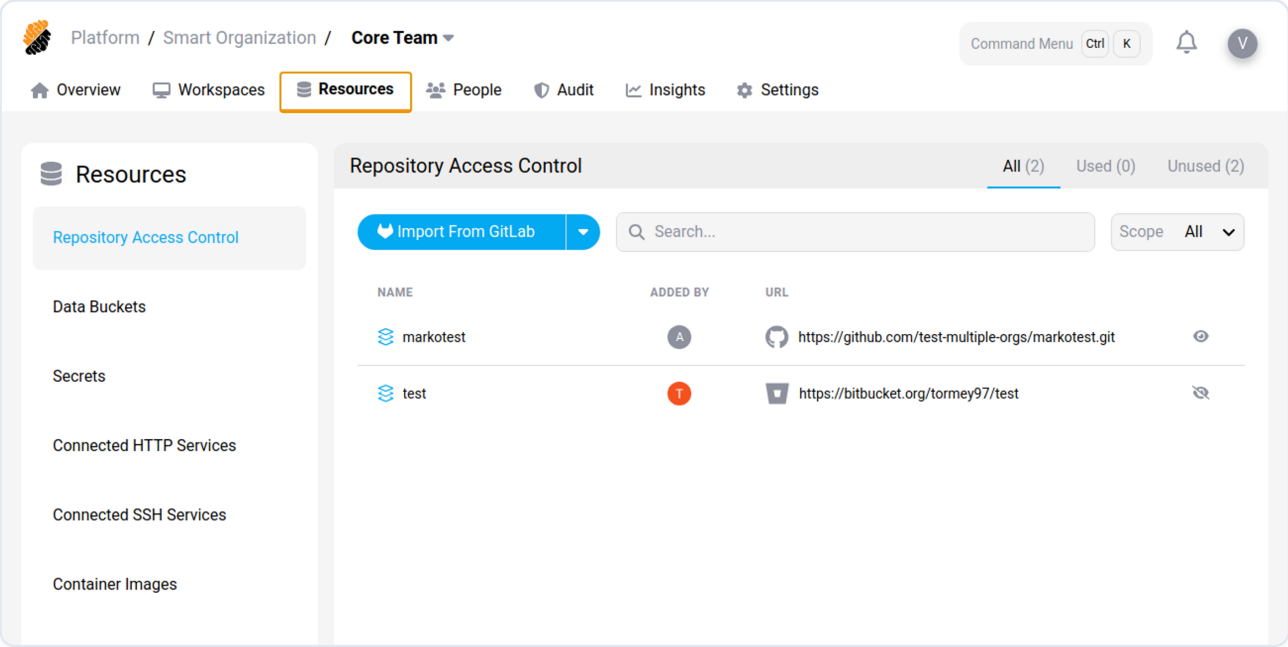
Los repositorios están basados en Git. Se importan de un proveedor que su administrador de plataforma ya ha conectado, o se añaden manualmente por URL.

PROVEEDOR	COMPATIBLE
GitHub	Gestionado y autoalojado
GitLab	Gestionado y autoalojado
Bitbucket	Nube y servidor
Azure DevOps	Gestionado
Cualquier otro host de Git	Por URL, introducido manualmente

Si el proveedor que necesita no se ofrece al importar, es que aún no se ha conectado a nivel de plataforma. Consulte Repositorios de código para saber qué implica y pregunte a su administrador de plataforma.

Ver repositorios

Los repositorios importados en el proyecto se listan en una tabla. Puede buscar o filtrar por los espacios de trabajo que los utilizan.



Un registro de repositorio contiene:

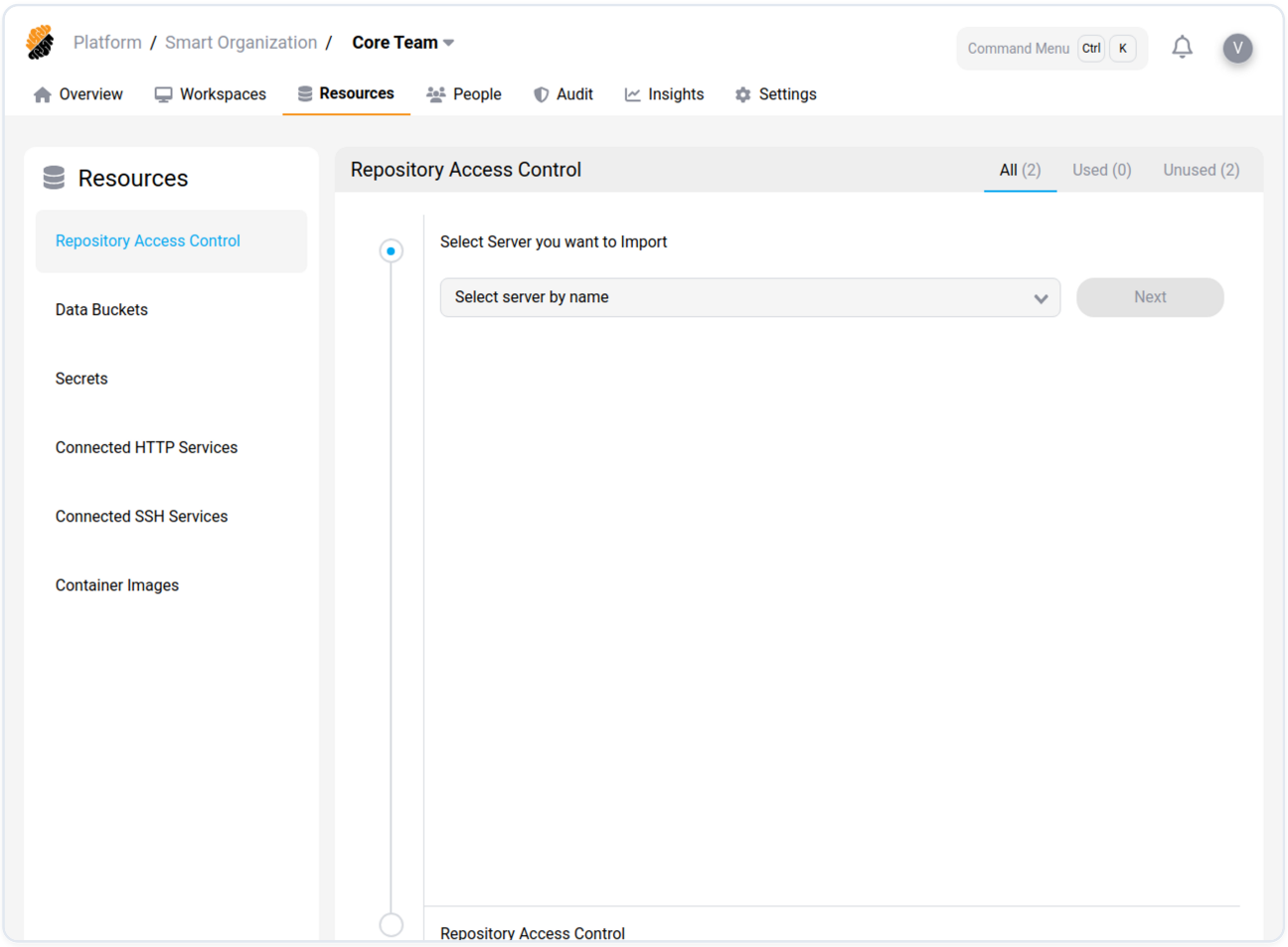
- **Información básica** — nombre, ámbito (plataforma, organización o proyecto), quién lo añadió, el proveedor de Git y la URL.
- **Nivel de clase** — la visibilidad del repositorio, evaluada según los permisos de cada usuario.
- **Información del activo** — una descripción.

El ámbito es importante aquí. Un repositorio importado a nivel de plataforma u organización está disponible para los proyectos que se encuentran debajo, así que compruebe lo que ya tiene antes de importar su propia copia.

Importar un repositorio

Requiere el permiso Recursos configurado en **Importar**.

1. Seleccione **Importar repositorio**.
2. Seleccione el proveedor.
3. La aplicación Git conectada se escanea en busca de repositorios. Seleccione el que desea importar.



La importación registra el repositorio con el proyecto. No copia ningún código: el repositorio permanece donde está, y los espacios de trabajo lo alcanzan a través de la plataforma.

Información relacionada

- Recursos del proyecto
- Repositorios de código (configuración de la plataforma)
- Configurar un proyecto para su equipo

- Roles y permisos

Secrets

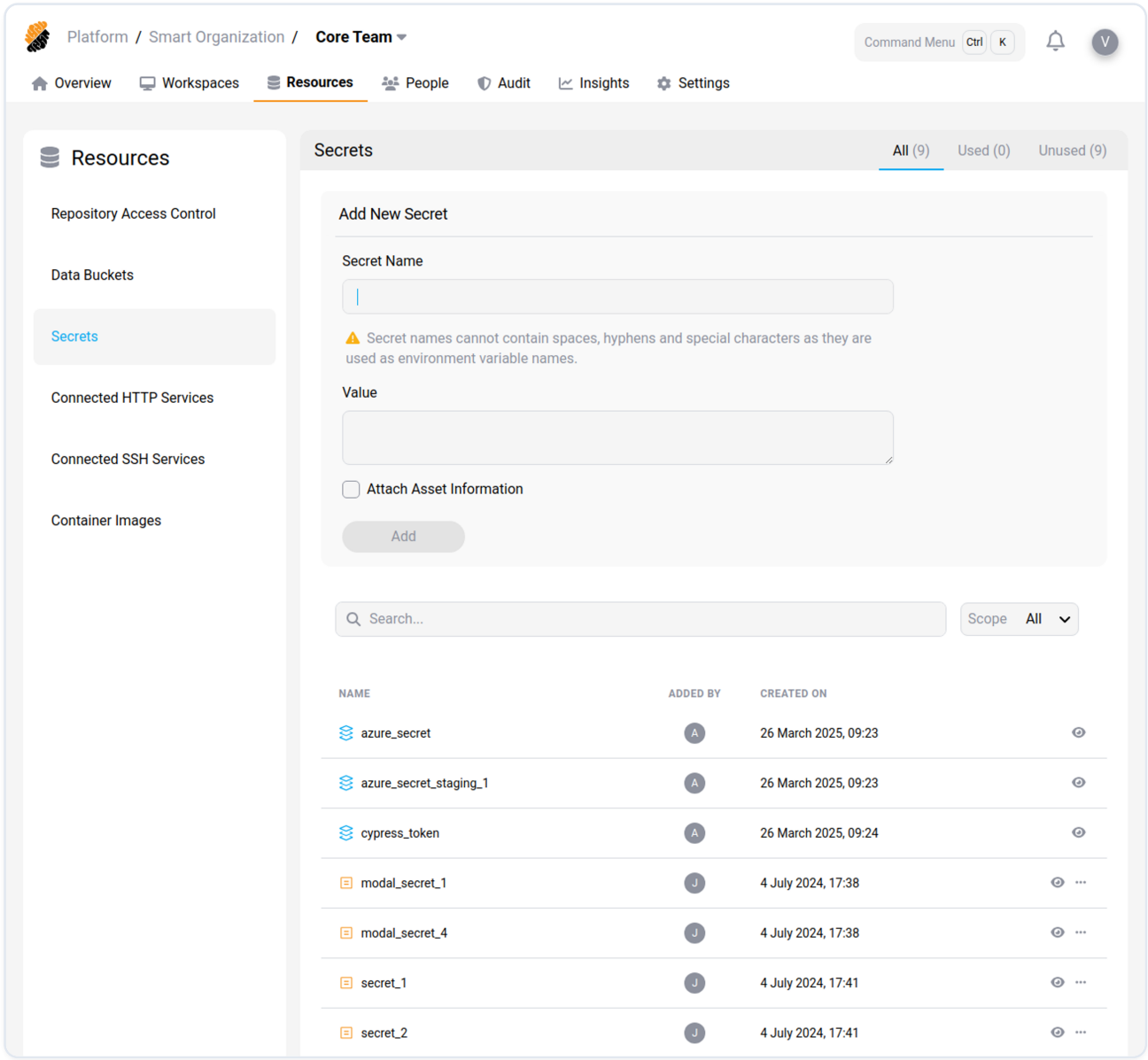
La gestión de secretos permite a los desarrolladores almacenar de forma segura datos sensibles como contraseñas, claves y tokens, en un entorno protegido con capacidades de control de acceso.

Generalmente, el término "secreto" se refiere a cualquier credencial necesaria (por ejemplo, claves criptográficas, tokens y contraseñas) para autenticarse con un servicio durante el proceso de desarrollo. El almacenamiento de secretos es un servicio que puede ser proporcionado por la plataforma o por un mecanismo externo. Una vez registrados en la plataforma, los secretos adjuntos a espacios de trabajo están disponibles en el sistema de archivos del contenedor como variables de entorno o archivos. Esta sección explica cómo la plataforma gestiona los secretos, pero tenga en cuenta que su plataforma podría utilizar un servicio externo para ese propósito.

- Ver secretos
- Añadir un nuevo secreto

Ver secretos

Los secretos utilizados en la organización o proyecto se muestran en una tabla. Puede buscar uno o filtrar los utilizados en los espacios de trabajo.



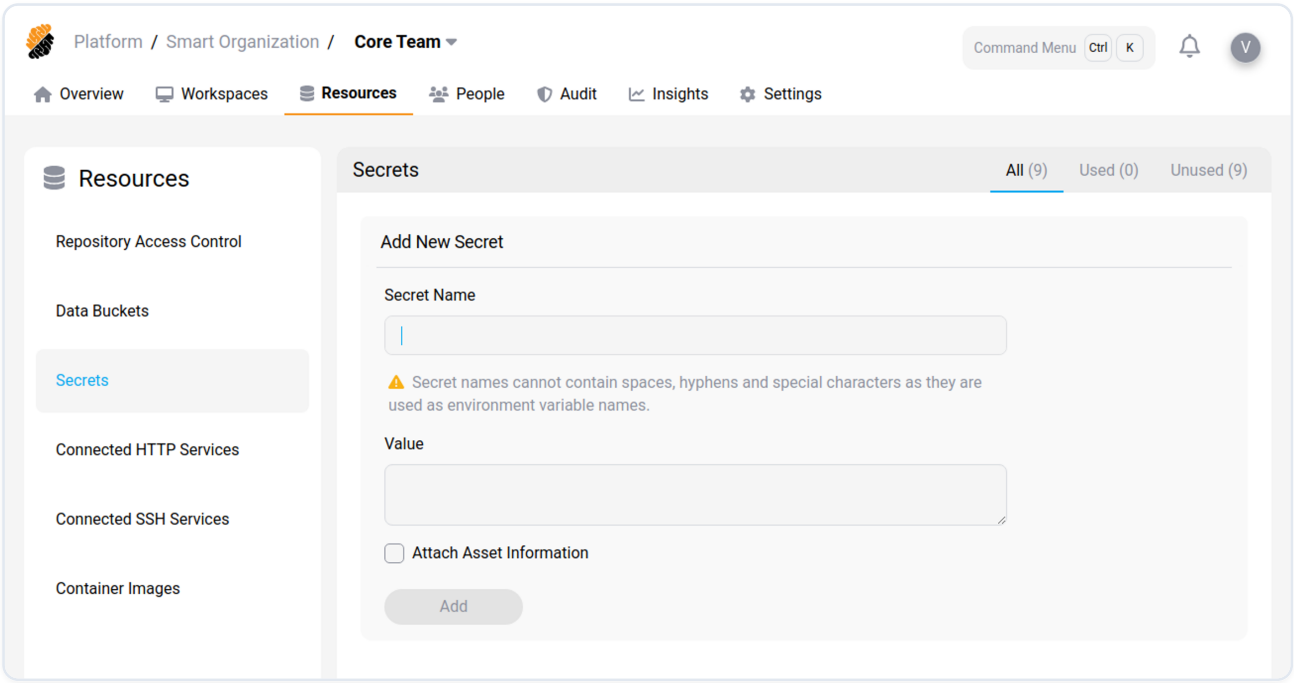
Un secreto se define por las siguientes características:

- **Información básica**: Información como el nombre, el usuario que lo añadió, el ámbito de uso (plataforma, organización o proyecto).
- **Nivel de clase**: Esta opción define la visibilidad del secreto en función de los permisos del usuario.
- **Información del activo**: Esta opción permite proporcionar una descripción del secreto.

Añadir un nuevo secreto

Requiere que el permiso Recursos esté configurado en **Gestionar**.

Puede crear un secreto en la parte superior de la **Página de secretos**.



Deberá introducir la siguiente información:

1. **Nombre**, un nombre para identificar el secreto,
2. **Valor**:, es decir, el valor del secreto, y una
3. **Información del activo**, una descripción del secreto.

Información relacionada

- Repositorios de código
- Servicios HTTP conectados
- Servicios SSH conectados
- Cubos de datos
- Elegir entre cubos de datos y puntos de montaje
- Recursos del proyecto

Data buckets

Un **Cubo de datos** se utiliza para el almacenamiento general y no estructurado de datos en línea. Básicamente, es una carpeta en formato S3 que se usa comúnmente para almacenar y acceder grandes conjuntos de datos. La mayoría de los proveedores de la nube ofrecen cubos de datos S3 como un mecanismo general de almacenamiento de datos. La plataforma es compatible con cubos de proveedores como Azure, Google y Amazon Web Services. Son particularmente populares para aplicaciones de Ciencia de Datos.

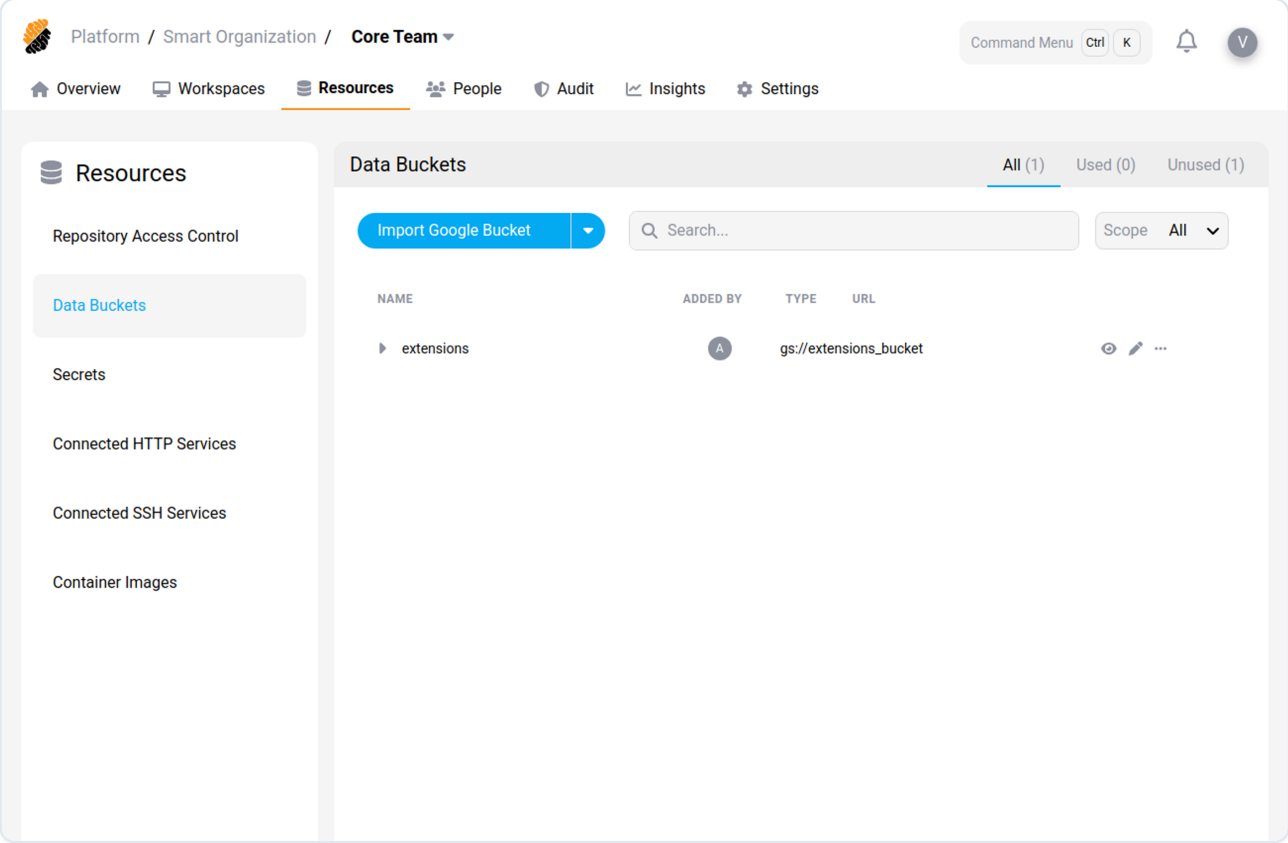
Los Cubos de datos le permiten usar sus conjuntos de datos externos dentro de un espacio de trabajo. Un cubo de datos adjunto a un espacio de trabajo se monta automáticamente como una carpeta en el sistema de archivos del contenedor.

En cuanto a los otros tipos de recursos, los cubos de datos se importan primero a la plataforma para que estén disponibles al crear o actualizar la configuración de un espacio de trabajo.

- Ver Cubos de datos
- Importar un Cubo de datos

Ver Cubos de datos

Se muestran los Cubos de datos utilizados en el proyecto. Puede filtrar los que están en uso.



Un Cubo de datos se define por las siguientes características:

- **Información básica**: Información como el nombre, el usuario que lo añadió, el proveedor de servicios (Google, Amazon o Microsoft) y la URL.
- **Nivel de clase**: Esta opción define la visibilidad del contenedor según los permisos del usuario.
- **Permisos**: Esta opción le permite definir el acceso a un cubo de datos como de lectura o de lectura y escritura.
- **Información del activo**: Esta opción permite proporcionar una descripción del cubo de datos.

La plataforma proporciona un mecanismo para crear versiones de cubos. Se crea una nueva versión cuando se cargan datos a un cubo desde un espacio de trabajo (con acceso de escritura). Al hacer clic en un cubo, puede ver una lista de versiones seguida de detalles básicos (fecha de creación, tamaño, estado, conexiones), así como su contenido haciendo clic en el *icono del libro*.

Para cargar datos desde un espacio de trabajo, el espacio de trabajo ya debe estar adjunto al Cubo de datos y debe tener acceso de escritura. Si el espacio de trabajo no está adjunto o tiene acceso de solo lectura, elija otro espacio de trabajo o actualice el acceso a los recursos del espacio de trabajo antes de cargar.

Importar un cubo de datos

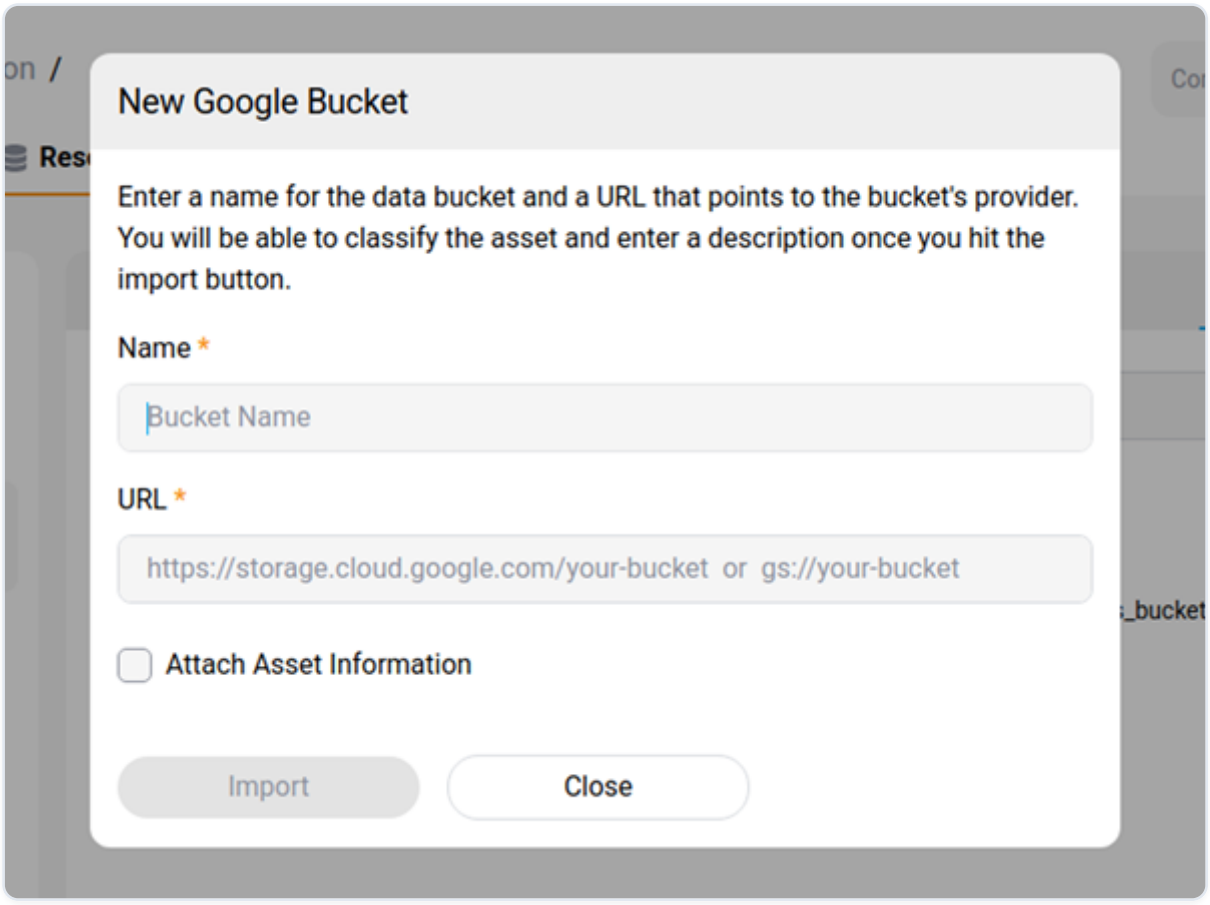
Requiere el conjunto de permisos Recursos establecido en **Gestionar**.

El botón de importación nombra al proveedor que utilizará, por lo que se lee **Importar cubo de Google**, **Importar cubo de Amazon**, o **Importar cubo de Microsoft**. Seleccione el proveedor que coincida con su cubo antes de importar.

El formulario se abre como **Nuevo cubo de Google**, **Nuevo cubo de Amazon** o **Nuevo cubo de Microsoft**, y solicita:

1. **Nombre**, un nombre para identificar el cubo de datos.
2. **URL**, que apunta a la ubicación de almacenamiento del proveedor de la nube.
3. **Adjuntar información del activo** (opcional), una descripción del cubo.

Seleccione **Importar** para guardarlo.



Información

Al importar cubos de Amazon, debe especificar su región para optimizar el rendimiento del acceso a los datos.

Información relacionada

- Repositorios de código
- Servicios HTTP conectados
- Servicios SSH conectados
- Elegir entre cubos de datos y puntos de montaje
- Puntos de montaje
- Recursos del proyecto

Mount points

Un **Punto de Montaje** conecta el almacenamiento externo basado en archivos directamente a un sistema de archivos de espacio de trabajo. A diferencia de los Cubos de Datos, que crean instantáneas puntuales que se replican en el clúster, los Puntos de Montaje proporcionan acceso en vivo al almacenamiento. Los cambios realizados dentro del espacio de trabajo son inmediatamente visibles para otros espacios de trabajo que comparten el mismo Punto de Montaje, lo que permite la colaboración en tiempo real en archivos y conjuntos de datos compartidos.

Los Puntos de Montaje son útiles cuando los equipos necesitan:

- Compartir grandes conjuntos de datos (por ejemplo, datos de entrenamiento de ML o artefactos de modelos) sin duplicarlos en los espacios de trabajo.
- Colaborar en tiempo real en archivos compartidos sin un flujo de trabajo manual de instantánea y publicación.
- Acceder a terabytes de datos al instante, sin esperar la replicación.

> **Nota**

> Los Puntos de Montaje solo están disponibles cuando un administrador de la plataforma ha habilitado la función en **Configuración del sistema > Integraciones > Almacenamiento de puntos de montaje**. Consulte Habilitar Puntos de Montaje para obtener más detalles.

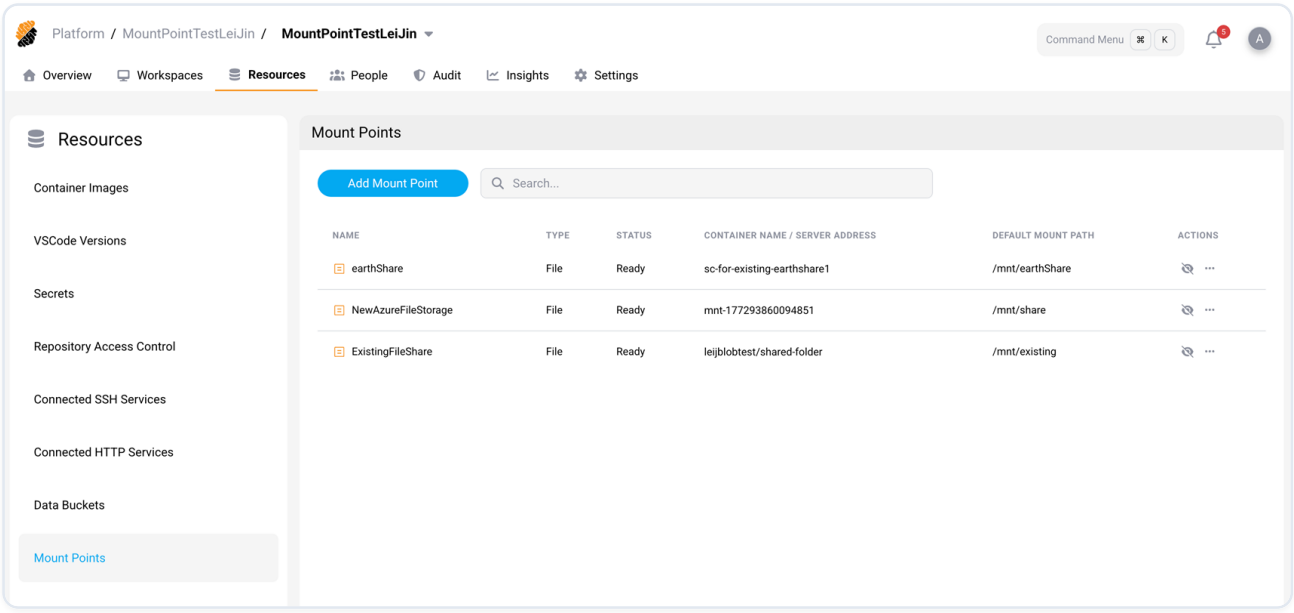
> **Nota**

> Los Puntos de Montaje no son compatibles en configuraciones multirregión.

- Ver Puntos de Montaje
- Añadir un Punto de Montaje
- Adjuntar un Punto de Montaje a un espacio de trabajo

Ver Puntos de Montaje

Los Puntos de Montaje configurados para el proyecto actual se muestran en la página **Recursos > Puntos de Montaje**.



Cada punto de montaje muestra la siguiente información:

- **Nombre** — Una etiqueta descriptiva para el punto de montaje.
- **Tipo** — El tipo de almacenamiento. Un punto de montaje de Azure lee **Archivo** o **Blob**. Un punto de montaje de AWS lee el servicio de respaldo que utiliza, **Amazon EFS** o **Archivos de Amazon S3**.
- **Estado** — El estado actual del punto de montaje. Consulte Estados del punto de montaje.
- **Identificador de almacenamiento** — El almacenamiento detrás del punto de montaje. Para Azure, es la cuenta de almacenamiento y el recurso compartido de archivos, o el nombre del contenedor o volumen. Para AWS, es el nombre del volumen que un administrador de plataforma publicó, o los identificadores del sistema de archivos y del punto de acceso.
- **Ruta de montaje predeterminada** — La ruta del sistema de archivos donde se monta el recurso compartido dentro del espacio de trabajo (por ejemplo, `/mnt/shared-data`).
- **Acciones** — Ver detalles o gestionar el punto de montaje.

Estados del punto de montaje

ESTADO	QUÉ SIGNIFICA
Creando	El punto de montaje ha sido aceptado y la configuración ha comenzado.
Aprovisionando	Se está aprovisionando el almacenamiento y la plataforma está esperando que el volumen se vincule.

ESTADO	QUÉ SIGNIFICA
Listo	El volumen está vinculado. El punto de montaje se puede adjuntar a un espacio de trabajo.
Actualizando	Se está aplicando una edición.
Eliminando	Se está eliminando el punto de montaje.
Error	El aprovisionamiento o la adjunción fallaron, o se agotó el tiempo de espera. Elimine el punto de montaje y créelo de nuevo.

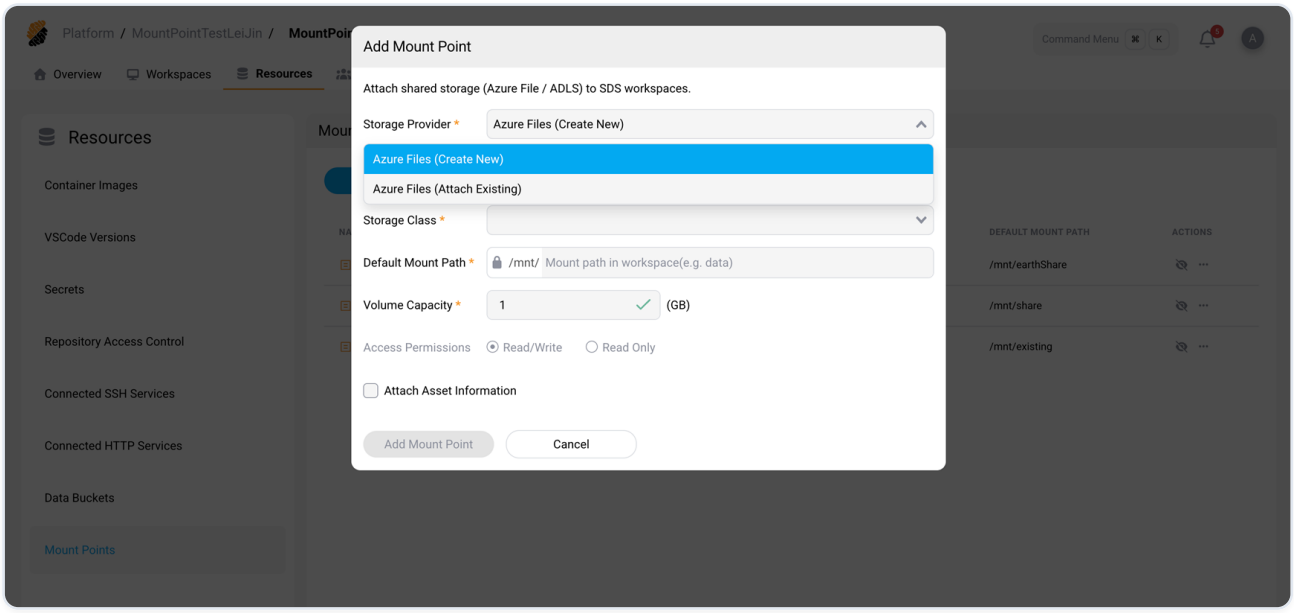
Un punto de montaje solo se puede editar mientras está en estado **Listo**. En cualquier otro estado, la acción **Editar** no está disponible, y una edición enviada para él es rechazada con un mensaje de que el punto de montaje no está listo.

> **Nota**
>
> Para un punto de montaje de AWS, **Listo** significa que el volumen está vinculado. No significa que el volumen haya sido montado. Consulte Solucionar problemas de puntos de montaje de AWS.

Añadir un punto de montaje

Requiere que el conjunto de permisos Recursos esté configurado en **Administrar**.

Para añadir un punto de montaje, seleccione **Añadir punto de montaje** en la página **Recursos > Puntos de montaje**.

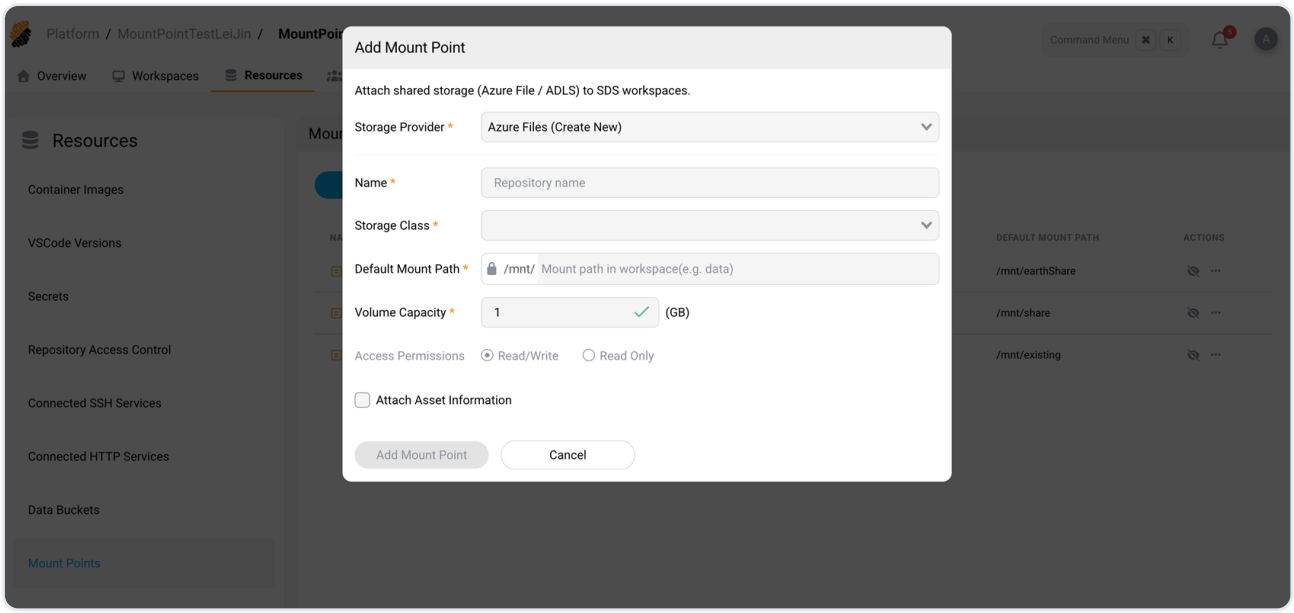


Primero, seleccione un **Proveedor de almacenamiento** del menú desplegable. El menú desplegable solo muestra las entradas para la nube en la que se ejecuta su implementación, por lo que un clúster de AWS ofrece las entradas de AWS y un clúster de Azure ofrece las entradas de Azure.

- **Azure Files (Create New)** — Aprovisiona un nuevo recurso compartido de archivos de Azure.
- **Azure Files (Attach Existing)** — Se conecta a un recurso compartido de archivos de Azure existente.
- **AWS Files (Create New)** — Aprovisiona nuevo almacenamiento compartido respaldado por AWS a partir de una clase de almacenamiento elegible.
- **Archivos de AWS (Adjuntar existentes)** — Se conecta al almacenamiento existente de Amazon Elastic File System (EFS) o Amazon S3 Files preparado por su equipo de infraestructura.

Azure Files (Crear nuevo)

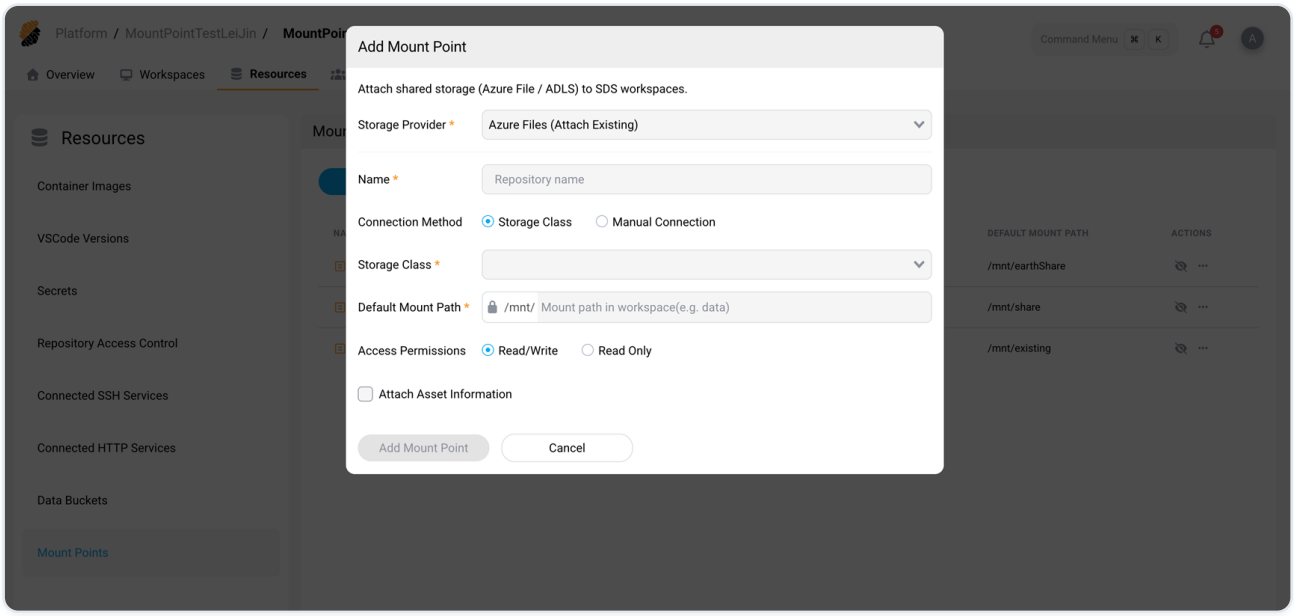
Proporcione la siguiente información:



1. **Nombre** — Un nombre descriptivo para identificar el punto de montaje.
2. **Clase de almacenamiento** — Seleccione una clase de almacenamiento de entre las opciones disponibles.
3. **Ruta de montaje predeterminada** — La ruta donde se monta el recurso compartido dentro del sistema de archivos del espacio de trabajo. La ruta tiene el prefijo `/mnt/` (por ejemplo, al introducir `data` se obtiene `/mnt/data`).
4. **Capacidad del volumen** — El tamaño del recurso compartido de archivos en GB.
5. **Permisos de acceso** — Fijo en **Lectura/Escritura** para un recurso compartido recién aprovisionado. El control se muestra, pero no se puede cambiar. Elija acceso de solo lectura por espacio de trabajo al adjuntar el punto de montaje.
6. **Adjuntar información del activo** (opcional) — Añada metadatos para clasificar el punto de montaje.

Azure Files (Adjuntar existente)

Al adjuntar un recurso compartido de archivos de Azure existente, proporcione un **Nombre** y seleccione un **Método de conexión**. Los dos métodos se ofrecen como un par de opciones, y cada uno solicita un conjunto de campos diferente.



- **Clase de almacenamiento** — Seleccione una clase de almacenamiento de archivos de Azure elegible. Utilice este método cuando un administrador de la plataforma ya haya preparado una clase de almacenamiento para el recurso compartido.
- **Conexión manual** — Introduzca los detalles de almacenamiento directamente. Los tres campos son obligatorios:
  - **Cuenta de almacenamiento** — El nombre de la cuenta de almacenamiento de Azure que contiene el recurso compartido.
  - **Clave de acceso** — La clave de acceso de la cuenta de almacenamiento.
  - **Nombre del recurso compartido de archivos** — El nombre del recurso compartido de archivos a montar.

Luego configure la **Ruta de montaje predeterminada** y seleccione **Lectura/Escritura** o **Solo lectura** en **Permisos de acceso**. El método de conexión y sus campos se fijan una vez que se crea el punto de montaje.

Archivos de AWS (Crear nuevo)

Al crear un nuevo punto de montaje respaldado por AWS, seleccione una clase de almacenamiento que represente Amazon EFS o Archivos de Amazon S3. La clase de almacenamiento determina el servicio de respaldo y debe ser configurada por un administrador antes de que los propietarios del proyecto puedan usarla.

Proporcione la siguiente información:

1. **Nombre** — Un nombre descriptivo para identificar el punto de montaje.

2. **Clase de almacenamiento** — Seleccione una clase de almacenamiento de Amazon EFS o Archivos de Amazon S3 elegible.
3. **Ruta de montaje predeterminada** — La ruta donde se monta el almacenamiento dentro del sistema de archivos del espacio de trabajo. La ruta tiene el prefijo `/mnt/`.
4. **Permisos de acceso** — Fijos en **Lectura/Escritura** para un punto de montaje recién aprovisionado. El control se muestra pero no se puede cambiar, y no se puede cambiar más tarde editando el punto de montaje. Elija acceso de solo lectura por espacio de trabajo cuando adjunte el punto de montaje, si los usuarios no deben modificar los datos compartidos desde ese espacio de trabajo.
5. **Adjuntar información de activo** (opcional) — Añada metadatos para clasificar el punto de montaje.

No hay tamaño que establecer. Amazon EFS y Amazon S3 Files son elásticos, por lo que un punto de montaje de AWS no tiene capacidad aprovisionada y ninguna cuota de tamaño por punto de montaje. Consulte Límites y comportamiento de los puntos de montaje.

> **Nota**
>
> Un nuevo punto de montaje de AWS muestra **Creando**, y luego **Aprovisionando**, durante un máximo de tres minutos mientras AWS crea el punto de acceso y el volumen se vincula. Esa espera es normal y no significa que el punto de montaje haya fallado. Para saber qué garantiza y qué no garantiza **Listo**, consulte Solucionar problemas de puntos de montaje de AWS.

Archivos de AWS (Adjuntar existente)

Utilice la opción de adjuntar existente cuando un equipo de infraestructura ya haya creado el almacenamiento que el proyecto debe usar. Hay dos formas de identificar ese almacenamiento, y cuál de ellas vea dependerá de cómo esté configurada la plataforma.

Seleccionar un volumen existente. Cada implementación ofrece este método, y a menos que un administrador de la plataforma haya habilitado el segundo, es el único método disponible. El formulario muestra una lista de **Volúmenes** que contiene los volúmenes que un administrador de la plataforma ha publicado en su proyecto, en su organización o en toda la implementación. Proporcione la siguiente información:

1. **Nombre** — Un nombre descriptivo para identificar el punto de montaje.
2. **Volumen** — Seleccione un volumen publicado por su nombre.

3. **Ruta de montaje predeterminada** — La ruta donde el almacenamiento se monta dentro del sistema de archivos del espacio de trabajo.
4. **Permisos de acceso** — Seleccione **Lectura/Escritura** o **Solo lectura**.

Si el volumen que espera no aparece en la lista, pida a su administrador de la plataforma que lo revise. Un volumen se ofrece solo al ámbito que nombra su etiqueta, y un volumen que un punto de montaje eliminado liberó debe restablecerse antes de que pueda ser adjuntado de nuevo. Consulte Crear un PersistentVolume para adjuntar existente.

Introducir detalles del sistema de archivos. Un administrador de la plataforma puede permitir adicionalmente que la plataforma construya el volumen a partir de las coordenadas de AWS que usted introduzca. Este método está desactivado por defecto. Cuando está habilitado, una opción de **Método de adjuntar** aparece encima del formulario, ofreciendo **Seleccionar un volumen existente** e **Introducir detalles del sistema de archivos**. Cuando no está habilitado, no hay opción que elegir y solo se muestra la lista de volúmenes. Al elegir **Introducir detalles del sistema de archivos** se solicita:

1. **Nombre** — Un nombre descriptivo para identificar el punto de montaje.
2. **Backend de almacenamiento** — Seleccione **Amazon EFS** o **Amazon S3 Files**.
3. **ID del sistema de archivos** — El identificador del sistema de archivos de AWS, que comienza con `fs-`.
4. **ID de punto de acceso** — El identificador del punto de acceso, que comienza con `fsap-`. Este campo es obligatorio para tanto Amazon EFS como Amazon S3 Files.
5. **Subruta** (opcional) — Monta un directorio específico dentro del almacenamiento de respaldo.
6. **Ruta de montaje predeterminada** — La ruta donde el almacenamiento se monta dentro del sistema de archivos del espacio de trabajo.
7. **Permisos de acceso** — Seleccione **Lectura/Escritura** o **Solo lectura**.

Los administradores y los oficiales de seguridad ven un control adicional en este formulario: una casilla de verificación **Montar todo el sistema de archivos (sin punto de acceso)**. Al seleccionarla, se oculta el campo **ID de punto de acceso** y se monta la raíz del sistema de archivos, de modo que un espacio de trabajo ve los datos de cada proyecto en ese sistema de archivos y no hay aislamiento por proyecto. Se rechaza en un sistema de archivos que ya respalda los puntos de montaje creados por la plataforma. En ese caso, desmarque la casilla de verificación y nombre un punto de acceso específico en su lugar. Los propietarios de proyectos no ven esta casilla de verificación.

> **Importante**
>
> Amazon EFS y Amazon S3 Files se montan a través de NFS, y ambos necesitan la opción de montaje `tls` para que ese tráfico se encripte. Una clase de almacenamiento o volumen que no lo incluya no se ofrece, y un intento de adjuntarlo se rechaza en lugar de montarse sin cifrar. Si una clase de almacenamiento, volumen o punto de acceso que espera no está disponible, pida a su administrador de plataforma que revise la configuración de almacenamiento del punto de montaje de AWS.

> Las clases de almacenamiento de AWS y los sistemas de archivos existentes son preparados por su administrador de plataforma fuera de la plataforma. Si faltan las opciones de AWS, o si no se ofrece un sistema de archivos existente que espera, consulte Preparar el almacenamiento de AWS para puntos de montaje.

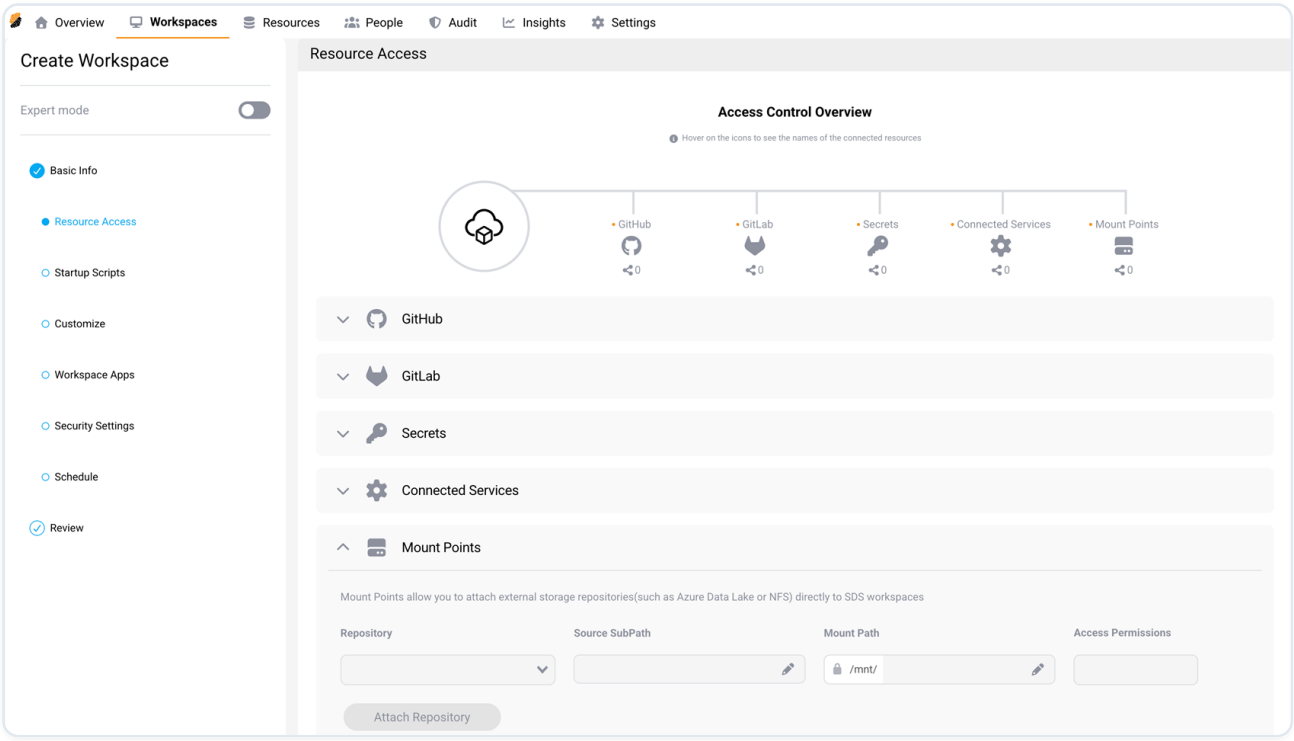
> **Nota**
>
> La eliminación de un punto de montaje se bloquea mientras lo utilice un espacio de trabajo activo, una plantilla de espacio de trabajo o un espacio de trabajo eliminado que aún pueda restaurarse. Desvincúlelo de cada uno de ellos primero.

> La edición no se ve afectada por el uso. Un punto de montaje se puede editar siempre que esté **Listo**, independientemente de cuántos espacios de trabajo lo utilicen, y no se puede editar en ningún otro estado. Un punto de montaje con errores o aún en proceso de aprovisionamiento tiene que eliminarse y crearse de nuevo en lugar de corregirse.

Adjuntar un punto de montaje a un espacio de trabajo

Puede adjuntar uno o más puntos de montaje a un espacio de trabajo durante la creación del espacio de trabajo o al crear una plantilla de espacio de trabajo.

Los puntos de montaje aparecen en el paso **Acceso a recursos** junto con otros tipos de recursos como GitHub, GitLab, Secretos y Servicios conectados.



Al adjuntar un punto de montaje:

1. Expanda la sección **Puntos de montaje** en el paso Acceso a recursos.
2. Seleccione un punto de montaje en el menú desplegable **Repositorio**.
3. Opcionalmente, especifique una **Subruta de origen** para montar un subdirectorio específico del recurso compartido de archivos.
4. Revise o personalice la **Ruta de montaje** — la ubicación en el sistema de archivos del espacio de trabajo donde el recurso compartido es accesible. La ruta tiene el prefijo `/mnt/`.
5. Seleccione **Lectura/Escritura** o **Solo lectura** en **Permisos de acceso**. Aquí es donde elige cómo el Punto de Montaje se comporta en este espacio de trabajo. El menú desplegable comienza con la configuración propia del Punto de Montaje, que es Lectura/Escritura para cada Punto de Montaje creado con **Crear nuevo**, y es el único lugar para hacer que un adjunto sea de solo lectura.
6. Seleccione **Adjuntar repositorio** para añadir el punto de montaje al espacio de trabajo.

Los puntos de montaje adjuntos se enumeran en **Repositorios configurados** debajo del formulario de adjuntos.

> **Importante**

Cada punto de montaje en un espacio de trabajo debe usar una ruta de montaje única. Si se detecta un conflicto de ruta, el sistema muestra un error e impide que se cree el espacio de trabajo hasta que se resuelva el conflicto.

Nota

Los puntos de montaje solo se pueden añadir en la región principal. Si el espacio de trabajo está configurado para una región no principal, la sección Puntos de montaje se deshabilita.

Puntos de montaje en plantillas de espacio de trabajo

Cuando crea o actualiza una plantilla de espacio de trabajo, puede preconfigurar puntos de montaje de la misma manera que durante la creación del espacio de trabajo. Los espacios de trabajo creados a partir de la plantilla heredan automáticamente los puntos de montaje configurados y sus rutas de montaje.

Los desarrolladores que crean un espacio de trabajo a partir de una plantilla aún pueden personalizar la ruta de montaje para cada punto de montaje adjunto antes de iniciar el espacio de trabajo.

Nota

El editor de plantillas no está cubierto por la restricción de región principal. Permite adjuntar un punto de montaje a cualquier región a la que se dirija la plantilla, por lo que se puede guardar una plantilla que contenga almacenamiento que los espacios de trabajo fuera de la región principal no pueden usar. No trate esto como una forma compatible de usar puntos de montaje en una región secundaria. Consulte Límites y comportamiento de los puntos de montaje.

Información relacionada

- Repositorios de código
- Servicios HTTP conectados
- Servicios SSH conectados
- Cubos de datos
- Elegir entre cubos de datos y puntos de montaje

- Límites y comportamiento de los puntos de montaje
- Recursos del proyecto

Connected HTTP services

Servicios HTTP conectados consisten en servicios utilizados para la implementación de aplicaciones de software. Estos servicios suelen proporcionar funciones, datos o acceso de host a través de API sobre el protocolo de red HTTP.

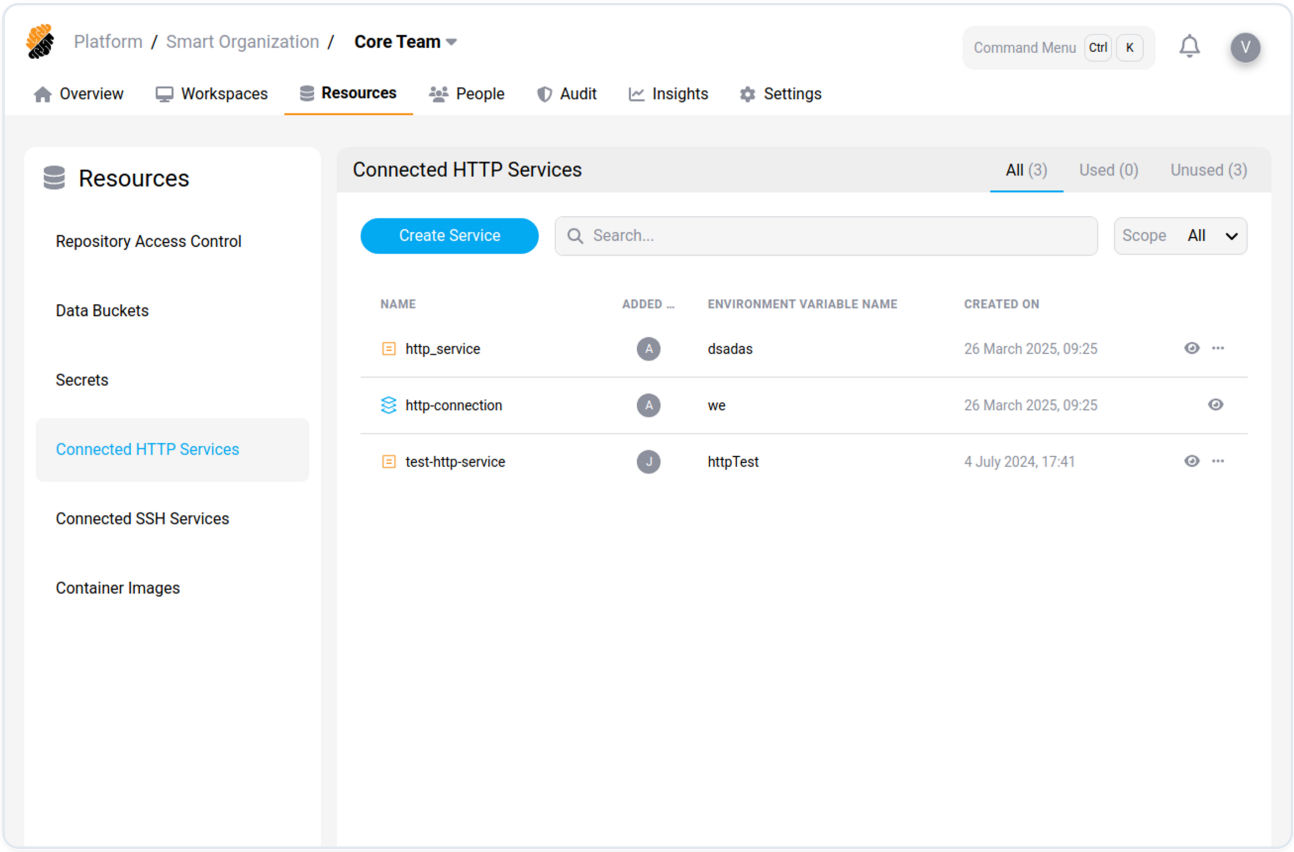
> **Consejo**

> La naturaleza y el protocolo de los servicios que se pueden adjuntar a los espacios de trabajo dependen de la implementación de su plataforma.

> Como ocurre con otros tipos de recursos, los servicios HTTP se adjuntan a los espacios de trabajo durante la creación o la actualización de la configuración del espacio de trabajo.

- Ver servicios HTTP conectados
- Añadir un servicio HTTP

Ver servicios HTTP conectados



Los servicios HTTP conectados se definen por las siguientes características:

- **Información básica**: Nombre, ámbito de uso (plataforma, organización o proyecto), URL y etiqueta.
- **Nivel de clase**: Esta opción define la visibilidad del servicio según los permisos del usuario.
- **Información del activo**: Esta opción permite proporcionar una descripción del contenedor.
- **Nombre de la variable de entorno**: permite el acceso al servicio nombrando una variable de entorno.

Añadir un servicio HTTP

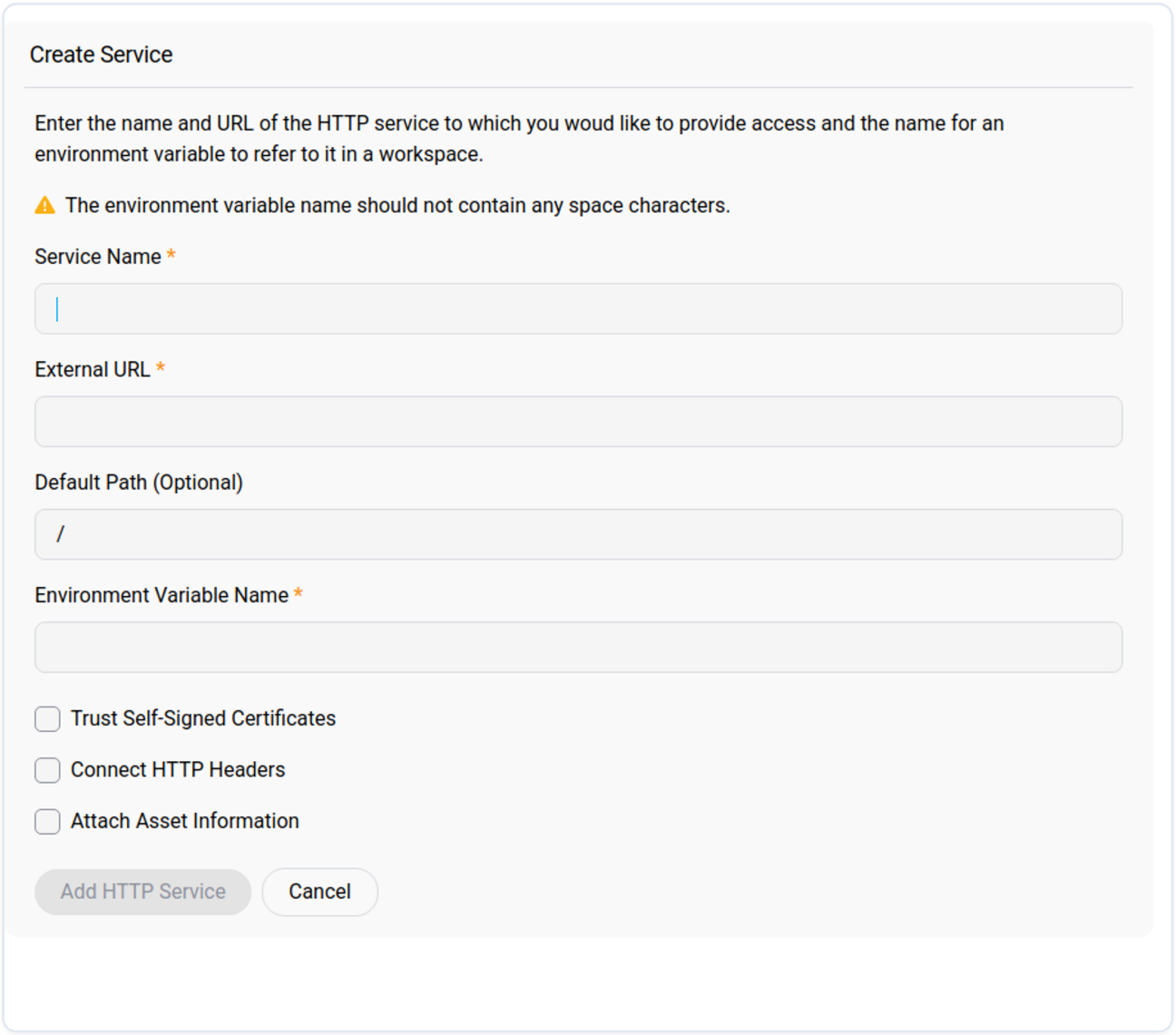
Requiere el permiso Recursos establecido en **Administrar**.

Seleccione **Crear servicio**, y luego proporcione:

1. **Nombre del servicio**, un nombre para identificar el servicio.
2. **URL externa**, que apunta a la ubicación del servicio.
3. **Ruta predeterminada (opcional)**, que se añade a la URL cuando se llama al servicio.
4. **Nombre de la variable de entorno**, utilizado para nombrar el servicio dentro del entorno del espacio de trabajo. No debe contener espacios ni caracteres especiales.

5. **Confiar en certificados autofirmados**, si el servicio presenta un certificado que no es de confianza pública.
6. **Conectar encabezados HTTP**, utilizado para pasar datos de autenticación cuando el servicio lo requiere. Puede añadir autenticación de acceso básico o encabezados personalizados.
7. **Adjuntar información del activo**, utilizado para proporcionar una descripción del servicio.

Seleccione **Añadir servicio HTTP** para guardarlo.



Información relacionada

- Repositorios de código
- Servicios SSH conectados
- Cubos de datos
- Elegir entre cubos de datos y puntos de montaje

- Puntos de montaje
- Recursos del proyecto

Connected SSH services

Servicios SSH conectados consisten en servicios utilizados para la implementación de aplicaciones de software. Estos servicios suelen proporcionar funciones, datos o acceso de host a través de API sobre el protocolo de red SSH. Para permitir que los usuarios se conecten a los servicios SSH, debe configurar el servicio SSH como un recurso de proyecto o los usuarios deben configurar una identidad SSH personal en la configuración de su perfil.

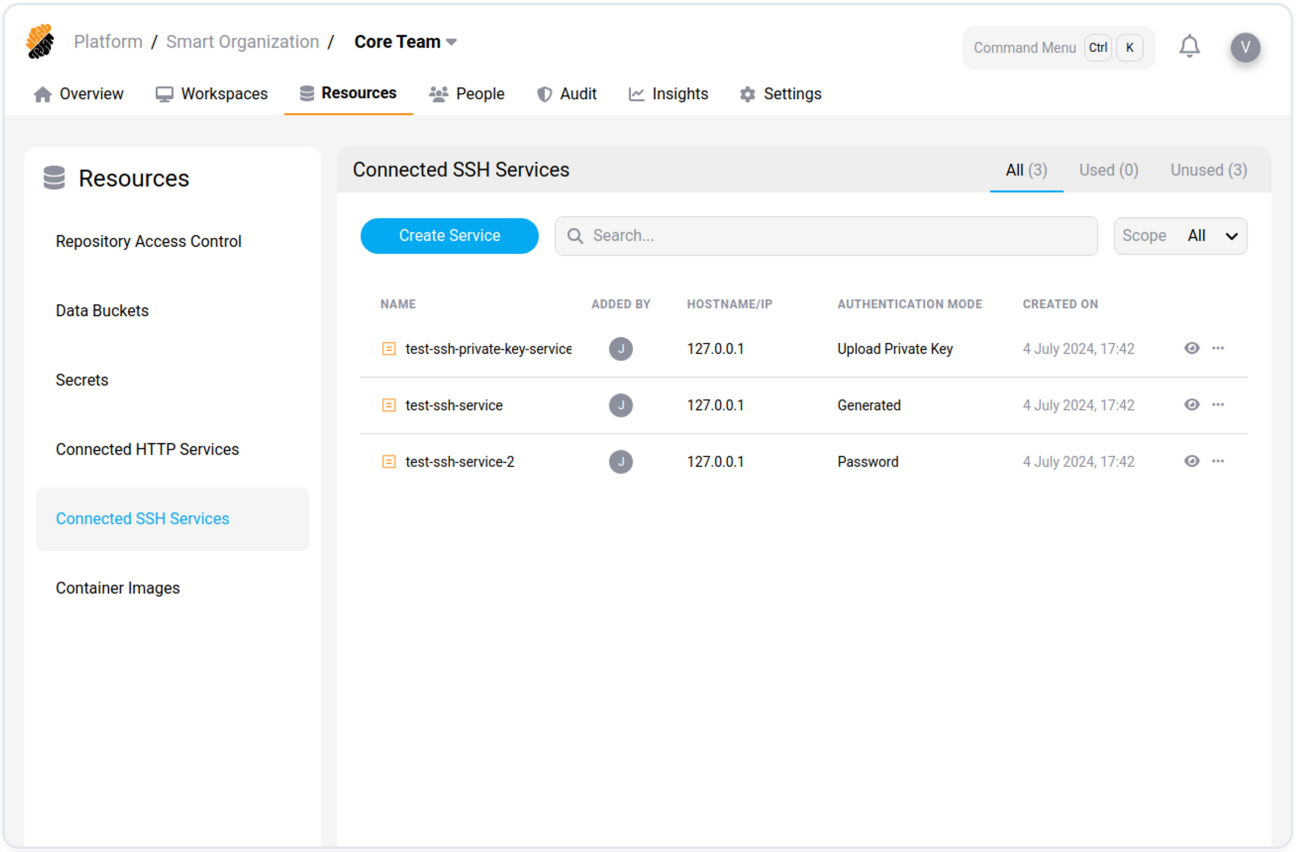
> **Consejo**

> La naturaleza y el protocolo de los servicios que se pueden adjuntar a espacios de trabajo dependen de la implementación de su plataforma.

> Al igual que con otros tipos de recursos, los servicios SSH se adjuntan a los espacios de trabajo cuando se crea el espacio de trabajo o cuando se actualizan sus configuraciones. Para el paso de adjuntar y la opción alternativa, consulte Habilitar SSH saliente.

- Ver servicios SSH conectados
- Agregar un servicio SSH

Ver servicios SSH conectados



Los servicios SSH conectados se definen por las siguientes características:

- **Información básica**: nombre y ámbito de uso (plataforma, organización o proyecto).
- **Nivel de clase**: define la visibilidad del servicio, según los permisos del usuario.
- **Información de activos adjuntos**: le permite proporcionar una descripción del servicio.
- **Nombre de host o dirección IP**: la dirección del host SSH.
- **Método de autenticación**: el mecanismo utilizado para autenticarse con el servicio.

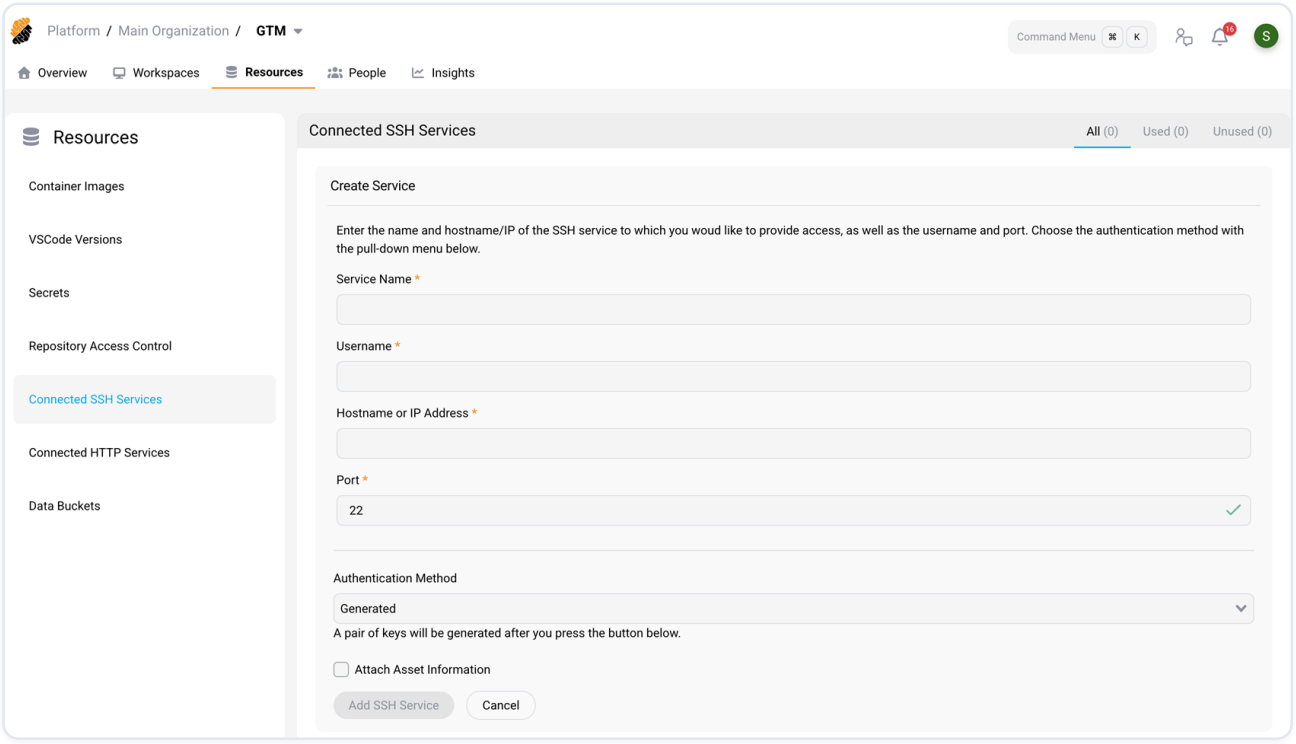
Agregar un servicio SSH

Requiere que el permiso **Recursos** esté establecido en **Administrar**.

Seleccione **Crear servicio** y, a continuación, introduzca:

1. **Nombre del servicio**, un nombre para identificar el host. No debe contener espacios ni letras mayúsculas.
2. **Nombre de usuario**, el nombre de usuario utilizado para acceder al host.
3. **Nombre de host o dirección IP**, que apunta a la ubicación del host.
4. **Puerto**, el puerto en el que escucha el servicio SSH.

5. **Método de autenticación**, un método de autenticación para acceder al servicio, y elija uno de los métodos:
    - "Generado": Se generará un par de claves al añadir el servicio SSH.
    - "Cargar clave privada": Cargue la clave privada que se utilizará para autenticarle en el servicio SSH.
    - "Contraseña": Inserte la contraseña asociada a su nombre de usuario SSH introducido previamente.
6. **Información del activo**, una descripción del servicio.



Información relacionada

- Habilitar SSH saliente
- Conectarse a servidores y servicios externos a través de SSH

Choose between data buckets and mount points

Citrix SecurSpaces™ proporciona dos mecanismos para hacer que los datos externos estén disponibles dentro de espacios de trabajo: **Data Buckets** y **Mount Points**. Ambos permiten a los equipos compartir conjuntos de datos, archivos y artefactos entre espacios de trabajo dentro de un proyecto, pero difieren en cómo se almacenan, sincronizan y acceden a los datos.

Esta guía explica cómo funciona cada opción y cuándo usarla.

De un vistazo

	DATA BUCKETS	MOUNT POINTS
Cómo llegan los datos al espacio de trabajo	Instantánea copiada al clúster	Conexión en vivo al almacenamiento externo
Colaboración en tiempo real	No — los cambios requieren un ciclo de publicación manual	Sí — los cambios son inmediatamente visibles para todos los espacios de trabajo conectados
Duplicación de datos	Sí — cada instantánea se replica en el clúster	No — los datos permanecen en el almacenamiento externo
Control de versiones	Integrado — se crea una nueva versión cada vez que se publican datos desde un espacio de trabajo	No integrado — use el control de versiones de almacenamiento externo si es necesario
Proveedores de almacenamiento compatibles	Amazon S3, Azure Blob Storage, Google Cloud Storage	Amazon EFS, Amazon S3 Files, Azure File Storage
Configuración necesaria	Importar un cubo (propietario del proyecto)	El administrador de la plataforma habilita la función; el propietario del proyecto crea Puntos de montaje
Ideal para	Experimentos reproducibles, conjuntos de datos versionados, referencias puntuales	Grandes conjuntos de datos compartidos, colaboración en tiempo real, datos a escala de terabytes

Cubos de datos

Un Cubo de datos conecta una ubicación de almacenamiento externa compatible con S3 a la plataforma. Cuando un Cubo de datos se adjunta a un espacio de trabajo, la plataforma crea una **instantánea de un momento dado** del contenido del cubo y la replica en el clúster. La instantánea se monta como una carpeta en el sistema de archivos del espacio de trabajo.

Cómo funciona

1. Un propietario de proyecto importa un Cubo de datos proporcionando un nombre, una URL de cubo y un proveedor de almacenamiento.
2. Un desarrollador adjunta el Data Bucket a un espacio de trabajo durante la creación del espacio de trabajo.
3. La plataforma replica el contenido del bucket en el clúster y monta la instantánea como una carpeta.
4. Si el desarrollador modifica datos en un bucket de lectura-escritura y publica los cambios, la plataforma crea una nueva versión de la instantánea.

Cuándo usar Data Buckets

- **La reproducibilidad importa.** Cada instantánea tiene versiones para que pueda volver a un estado conocido de los datos en cualquier momento.
- **Los conjuntos de datos son de tamaño pequeño a moderado.** Las instantáneas duplican los datos en el clúster, por lo que el tiempo de replicación y el uso del disco escalan con el tamaño del conjunto de datos.
- **Se prefiere el aislamiento.** Cada espacio de trabajo obtiene su propia copia de los datos. Los cambios en un espacio de trabajo no afectan a otros hasta que se publican explícitamente.

Limitaciones

- La replicación puede tardar mucho tiempo para conjuntos de datos grandes.
- Las instantáneas consumen espacio en disco del clúster proporcional al tamaño de los datos.
- Los cambios no se comparten en tiempo real; otros usuarios solo ven las actualizaciones después de que se publica una nueva versión.

Puntos de montaje

Un Punto de montaje conecta el almacenamiento externo basado en archivos directamente al sistema de archivos del espacio de trabajo sin copiar datos al clúster. El espacio de trabajo lee y escribe en el almacenamiento externo en tiempo real.

Cómo funciona

1. Un administrador de la plataforma habilita los tipos de almacenamiento de Puntos de montaje en **Configuración del sistema > Integraciones**.

2. Un propietario de proyecto crea un punto de montaje especificando el proveedor de almacenamiento, los detalles de conexión, la ruta de montaje predeterminada y los permisos de acceso.
3. Un desarrollador adjunta el punto de montaje durante la creación del espacio de trabajo. La ruta de montaje se puede personalizar y se puede especificar una subruta de origen para montar un subdirectorio específico.
4. El almacenamiento externo se monta en la ruta especificada (por ejemplo, `/mnt/shared-data`). Todos los espacios de trabajo conectados al mismo punto de montaje ven los mismos archivos en tiempo real.

Cuándo usar puntos de montaje

- **Colaboración en tiempo real.** Varios desarrolladores necesitan leer o escribir archivos compartidos simultáneamente, y los cambios deben ser visibles de inmediato.
- **Grandes conjuntos de datos.** Los datos son demasiado grandes para replicarse de manera eficiente: terabytes de datos de entrenamiento de ML, artefactos de modelos o resultados de experimentos compartidos.
- **Evitar la duplicación de datos.** Desea reducir el uso del disco del clúster manteniendo los datos en el almacenamiento externo en lugar de copiarlos en el clúster.

Limitaciones

- Requiere que un administrador de plataforma habilite la función antes de que los propietarios de proyectos puedan crear puntos de montaje.
- Sin control de versiones integrado: si necesita instantáneas de un momento dado, adminístrelas en el proveedor de almacenamiento externo.
- Un proveedor de nube por clúster. Si están presentes las clases de almacenamiento de puntos de montaje de AWS y Azure, el proveedor no se puede resolver y la función se retira. Consulte Preparar el almacenamiento de AWS para puntos de montaje.
- No compatible con configuraciones multirregión.

Cómo elegir entre los dos

Utilice las siguientes preguntas para guiar su decisión:

1. **¿Necesitan varios desarrolladores ver los cambios de los demás en tiempo real?** Sí → Puntos de montaje. Los cubos de datos requieren un ciclo de publicación manual para compartir actualizaciones.

2. **¿Necesita un control de versiones integrado para reproducir estados anteriores de los datos?** Sí → Data Buckets. Cada publicación crea una instantánea versionada. Mount Points no versionan los datos automáticamente.
3. **¿Es el conjunto de datos muy grande (cientos de GB o más)?** Sí → Mount Points. Evitan el coste de tiempo y disco de replicar los datos en el clúster.
4. **¿Necesita que cada desarrollador trabaje en una copia aislada de los datos?** Sí → Data Buckets. Cada espacio de trabajo tiene su propia instantánea, independiente de otros espacios de trabajo.
5. **¿Qué proveedor de almacenamiento está utilizando?** Data Buckets es compatible con Amazon S3, Azure Blob Storage y Google Cloud Storage. Mount Points es compatible con Amazon EFS, Amazon S3 Files y Azure File storage. Para la ruta de AWS, consulte Preparar el almacenamiento de AWS para Mount Points.

Ambas opciones se pueden utilizar dentro del mismo proyecto. Por ejemplo, un equipo podría usar un Mount Point para un directorio compartido de datos de entrenamiento y un Data Bucket para los resultados de experimentos versionados.

Temas relacionados

- Data Buckets
- Mount Points
- Habilitar el almacenamiento de Mount Point
- Crear un espacio de trabajo

Información relacionada

- Repositorios de código
- Servicios HTTP conectados
- Servicios SSH conectados
- Data buckets
- Puntos de montaje
- Recursos del proyecto

Enable outbound SSH

Por defecto, el servicio de proxy de SecurSpaces bloquea las conexiones SSH salientes desde los espacios de trabajo. Hasta que habilite una de las dos opciones siguientes, un desarrollador que intente acceder a un host externo a través de SSH tendrá la conexión cerrada.

Esta página es para propietarios de proyectos y oficiales de seguridad. Para el lado del desarrollador —generar una clave, registrarla y conectarse—, consulte Conectarse a servidores y servicios externos a través de SSH.

Elija una opción

CONSIDERACIÓN	IDENTIDAD SSH PERSONAL	SERVICIOS SSH CONECTADOS
Ideal para	Desarrolladores individuales que necesitan su propia clave, por ejemplo, para autenticarse con Azure DevOps o GitHub	Equipos donde varias personas se conectan al mismo servicio SSH
Quién lo configura	Usted habilita el interruptor; cada desarrollador genera y registra su propia clave	Usted crea el recurso de servicio y lo adjunta a los espacios de trabajo; los desarrolladores se conectan sin necesidad de configuración adicional
Propiedad de la clave	Cada usuario es propietario de su clave	La plataforma o un administrador posee la clave
Esfuerzo de registro	Cada usuario registra su clave pública en cada servicio de destino	Registrado una vez, y todos los que usan el espacio de trabajo se conectan
Alcance	Nivel de usuario, en todos los espacios de trabajo donde el interruptor está activado	Nivel de recurso, adjunto por espacio de trabajo o plantilla
Mejor ajuste	Acceso a cuentas y servicios personales	Infraestructura compartida como servidores de compilación, máquinas

CONSIDERACIÓN	IDENTIDAD SSH PERSONAL	SERVICIOS SSH CONECTADOS
		virtuales de ensayo e instancias en la nube

Opción 1: Habilitar identidad SSH personal

Requiere que el permiso de **Seguridad** esté configurado en **Administrar**, que poseen los propietarios de proyectos y los oficiales de seguridad.

Con la identidad SSH personal, la plataforma genera y guarda un par de claves para cada usuario. La clave privada se aplica cuando el desarrollador se conecta y nunca se expone dentro del espacio de trabajo.

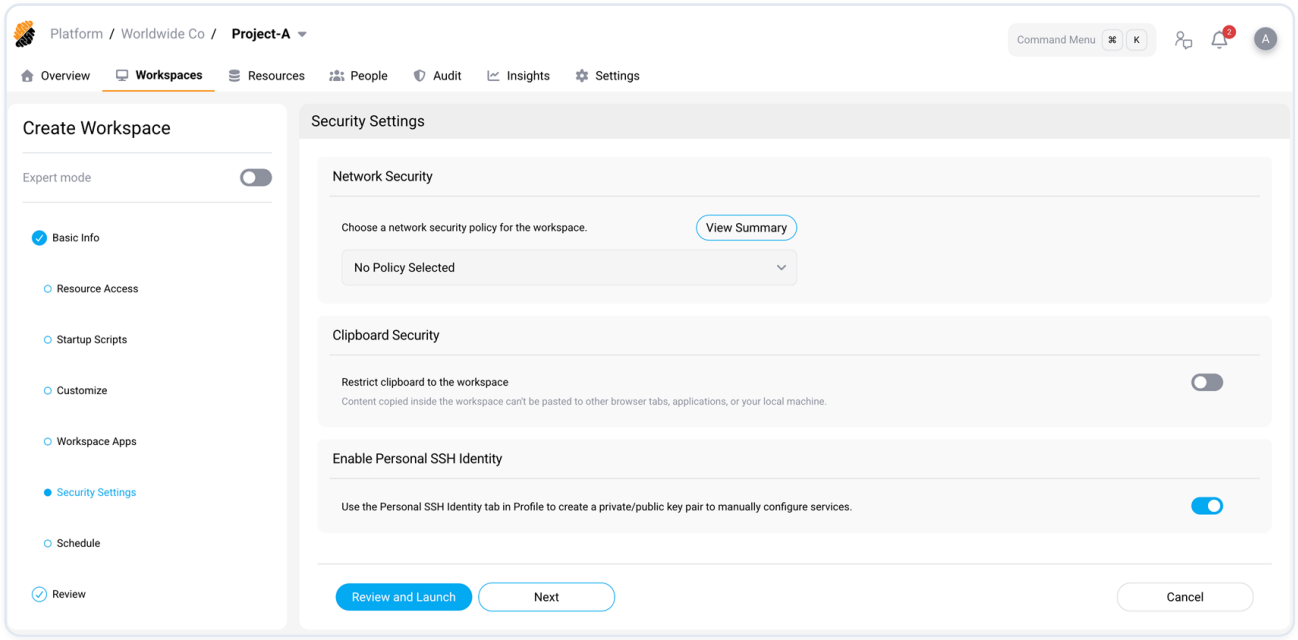
Puede habilitar la configuración en un solo espacio de trabajo o en una plantilla para que cada espacio de trabajo creado a partir de ella herede la configuración.

En un espacio de trabajo

1. Vaya a la pestaña **Espacios de trabajo** del proyecto.
2. Crear o editar un espacio de trabajo.
3. En el panel izquierdo, selecciona **Configuración de seguridad**.
4. Activa **Habilitar identidad SSH personal**.
5. Selecciona **Revisar y lanzar**, o **Siguiente**, para guardar.

En una plantilla de espacio de trabajo

1. Ve a la pestaña **Espacios de trabajo** del proyecto y selecciona la vista **Plantillas**.
2. Crea o edita una plantilla.
3. En **Configuración de seguridad**, activa **Habilitar identidad SSH personal**.
4. Guarda la plantilla.



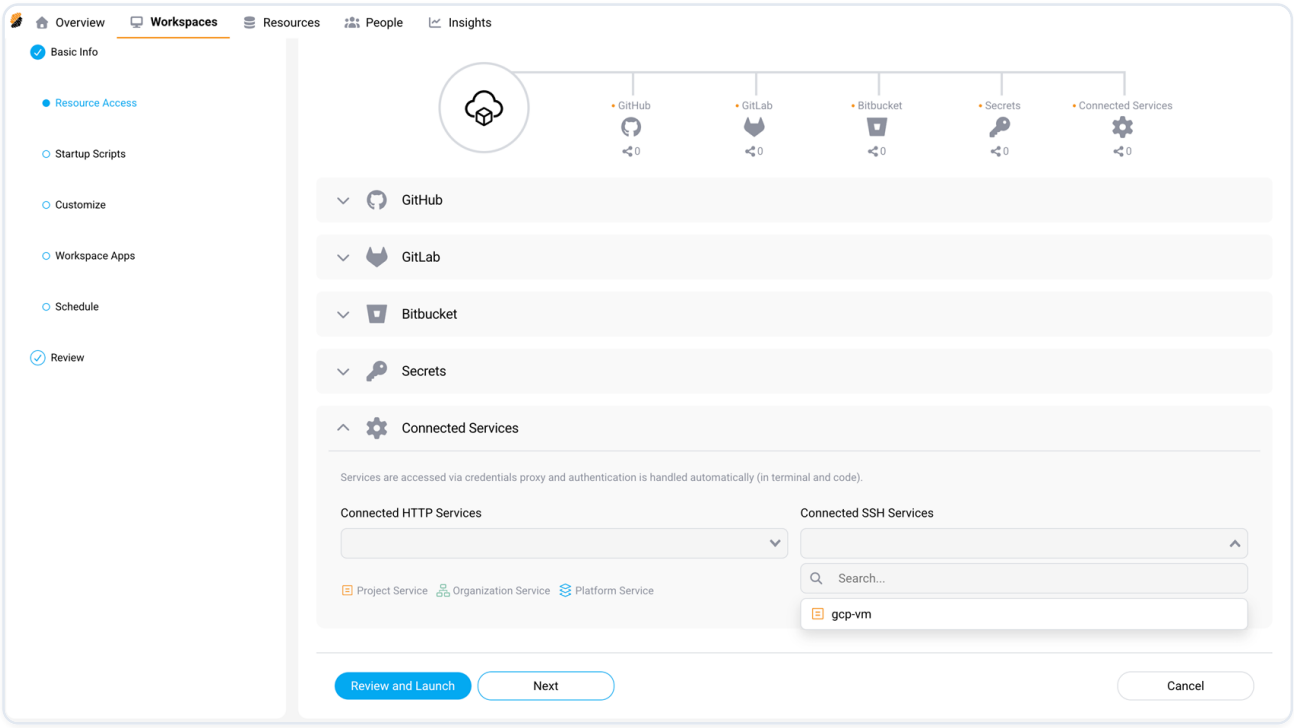
Ahora se permite SSH saliente desde ese espacio de trabajo. Cada desarrollador genera su propia clave en su perfil y registra la clave pública en el servicio de destino. Consulta Identidad SSH personal.

Opción 2: Adjuntar un servicio SSH conectado

La creación del servicio requiere que el permiso de **Recursos** esté configurado en **Administrar**.

Un servicio SSH conectado define un host de destino una vez, con sus credenciales, y lo comparte entre espacios de trabajo. Los desarrolladores se conectan con `ssh <service-name>` y nunca manejan una clave.

1. Crea el servicio como un recurso del proyecto. Para el formulario y sus campos, consulta Servicios SSH conectados.
2. Adjúntalo a un espacio de trabajo:
    a. Crea o edita un espacio de trabajo.
    b. En el panel izquierdo, selecciona **Acceso a recursos**.
    c. En **Servicios conectados**, abre la lista **Servicios SSH conectados**.
    d. Selecciona tu servicio.
    e. Selecciona **Revisar y lanzar**, o **Siguiente**, para guardar.



Información relacionada

- Conectarse a servidores y servicios externos a través de SSH
- Servicios SSH conectados
- Políticas de red

SecurSpaces Flex workspace templates

Este artículo describe las plantillas de espacio de trabajo en Citrix SecurSpaces™ Flex: qué son, cómo funcionan y cómo crearlas y gestionarlas. Para conocer las opciones de tamaño del espacio de trabajo y el consumo de créditos, póngase en contacto con su equipo de ventas de Citrix.

¿Qué es una plantilla de espacio de trabajo?

Una plantilla de espacio de trabajo es el artefacto de implementación principal en Citrix SecurSpaces Flex. Define el entorno que recibe un desarrollador cuando inicia un espacio de trabajo.

Una plantilla de espacio de trabajo incluye:

- **Imagen de contenedor** — La imagen base de contenedor Linux con herramientas, tiempos de ejecución y configuración preinstalados.
- **Herramientas preinstaladas** — Lenguajes, SDK, CLI y herramientas de desarrollo integrados en la imagen.

- **Límites de recursos** — Máximo de vCPU y RAM que el espacio de trabajo puede consumir (separado del perfil de tamaño del espacio de trabajo; utilizado para establecer límites estrictos dentro de un nivel de cómputo).
- **Controles de acceso** — Qué usuarios o grupos de usuarios pueden iniciar espacios de trabajo desde esta plantilla.
- **Scripts de inicio** — Scripts que se ejecutan al inicializar el espacio de trabajo: clonar repositorios, configurar archivos de configuración (dot files), montar secretos o ejecutar comandos de configuración.

Qué posee el cliente

El cliente posee y aloja la imagen de contenedor. Citrix no proporciona ni gestiona el contenido de la imagen de contenedor. El cliente es responsable de:

- Crear y mantener la imagen de contenedor.
- Alojar la imagen en un registro de contenedores accesible desde el plano de ejecución de Citrix SecurSpaces (por ejemplo, Azure Container Registry, Docker Hub o un registro privado).
- Aplicar parches y actualizar la imagen según sea necesario.

Citrix escanea la imagen de contenedor en busca de vulnerabilidades conocidas cuando se inicia un espacio de trabajo. Los resultados del escaneo se muestran al administrador en la consola de Citrix SecurSpaces.

Tamaño y plantilla desacoplados

El tamaño del espacio de trabajo y la plantilla del espacio de trabajo se configuran de forma independiente. Una única plantilla se puede emparejar con cualquier tamaño de espacio de trabajo (Ligero, Mediano o Pesado) bajo demanda. Esto significa:

- No necesita una plantilla separada por nivel de computación.
- Los desarrolladores pueden cambiar los tamaños de los espacios de trabajo sin necesidad de una nueva plantilla.
- Los equipos de ingeniería de plataforma pueden estandarizar en un número reducido de plantillas y dejar que el tamaño del espacio de trabajo varíe según la carga de trabajo.

Crear una plantilla de espacio de trabajo

Para crear una plantilla de espacio de trabajo, debe tener el rol de **Administrador** en la consola de Citrix SecurSpaces.

1. Inicie sesión en su entorno de SecurSpaces en la URL de acceso de su organización (por ejemplo, `https://yourcompany.flex.sds.citrix.com`).
2. Vaya a **Administración** > **Plantillas de espacio de trabajo**.
3. Seleccione **Crear plantilla**.
4. Complete la configuración de la plantilla:

CAMPO	DESCRIPCIÓN
Nombre	Un nombre descriptivo para la plantilla (por ejemplo, `backend-java-21` o `data-platform`).
Descripción	Opcional. Una breve descripción que se muestra a los administradores.
Imagen de contenedor	La referencia completa de la imagen, incluyendo el registro, el nombre de la imagen y la etiqueta (por ejemplo, `myregistry.azurecr.io/dev-image:latest`).
Límites de recursos	Opcional. Límites máximos de vCPU y RAM para los espacios de trabajo creados a partir de esta plantilla.
Script de inicio	Opcional. Un script de shell que se ejecuta al inicializar el espacio de trabajo.
Acceso	Los usuarios o grupos con permiso para iniciar espacios de trabajo desde esta plantilla.

5. Seleccione **Guardar** para crear la plantilla.

La plantilla ya está disponible para la creación de espacios de trabajo y aparece en la página **Plantillas de espacios de trabajo**.

Tamaños de espacio de trabajo gestionados

En las implementaciones de Flex, los tamaños de los espacios de trabajo se gestionan por separado de las plantillas de espacios de trabajo. Citrix publica los niveles de tamaño disponibles,

y cada nivel puede tener una versión actual, versiones anteriores compatibles y versiones retiradas. Esto mantiene los valores de CPU, memoria, almacenamiento y clase de almacenamiento alineados con el catálogo de servicios de Flex.

Los administradores aún pueden controlar dónde está disponible un nivel de tamaño. Pueden asignar o eliminar un nivel para una organización o proyecto, y pueden actualizar los espacios de trabajo existentes a la versión actual del mismo nivel. No pueden crear, editar ni eliminar las definiciones de nivel gestionadas por Citrix.

Cuando hay una versión más reciente de un nivel disponible, los espacios de trabajo afectados muestran un aviso de actualización. La actualización mantiene el espacio de trabajo en el mismo nivel y aplica la versión actual del nivel. Las versiones de nivel retiradas no están disponibles para nuevos espacios de trabajo, pero los espacios de trabajo existentes permanecen visibles para que puedan ser revisados y actualizados.

Cuando un administrador habilita o deshabilita un nivel gestionado, o aplica una actualización masiva para mover espacios de trabajo a la versión actual de un nivel, SecurSpaces registra la acción exitosa en el registro de auditoría. La entrada de auditoría incluye quién realizó la acción, cuándo ocurrió y el resultado, como el estado del nivel o el número de espacios de trabajo actualizados.

Actualizar una plantilla de espacio de trabajo

La actualización de una plantilla cambia la configuración de los nuevos espacios de trabajo creados a partir de ella. Los espacios de trabajo existentes en ejecución no se ven afectados hasta que se reinician.

1. Ve a **Administración** > **Plantillas de espacio de trabajo**.
2. Selecciona la plantilla que quieres actualizar.
3. Edita los campos relevantes.
4. Selecciona **Guardar**.

> **Nota:**
>
> Si actualizas la etiqueta de la imagen del contenedor (por ejemplo, de `v1.0` a `v1.1`), los nuevos espacios de trabajo usarán la imagen actualizada. Los desarrolladores con espacios de trabajo en ejecución deben detener y reiniciar su espacio de trabajo para que se aplique la nueva imagen.

Control de versiones de plantillas

Las plantillas de espacio de trabajo admiten el control de versiones. Cada versión guardada de una plantilla se registra. Los administradores pueden:

- Ver el historial de versiones de una plantilla.
- Revertir a una versión anterior si una nueva imagen o configuración causa problemas.

Eliminar una plantilla de espacio de trabajo

Eliminar una plantilla la quita de la lista de plantillas disponibles. Los espacios de trabajo existentes en ejecución que se crearon a partir de la plantilla eliminada seguirán ejecutándose hasta que se detengan.

1. Vaya a **Administración** > **Plantillas de espacio de trabajo**.
2. Seleccione la plantilla que desea eliminar.
3. Seleccione **Eliminar**.
4. Confirme la eliminación en el cuadro de diálogo.

Más información

- Descripción general de SecurSpaces Flex — el punto de partida para toda la documentación de Flex
- Consumo de créditos de Platform Flex
- Conexiones de red
- Descripción general de la seguridad técnica
- Plantillas de espacio de trabajo en Citrix SecurSpaces (autohospedado) — para conceptos de plantillas de espacio de trabajo que se aplican a ambos modelos de implementación

Deploy

Esta sección es para el equipo que implementa SecurSpaces en su propia infraestructura. SecurSpaces es alojado por el cliente: se ejecuta en un clúster de Kubernetes que usted proporciona y controla.

Consulte Requisitos del sistema y Destinos de red antes de empezar. El segundo es más importante para entornos aislados o con cortafuegos.

Instalar

TAREA	PÁGINA
Implementar un entorno de evaluación de una sola VM	Implementar un entorno de evaluación
Instalar con la CLI	Instalar con la CLI de Strong Installer
Implementar en Amazon EKS	Amazon EKS
Implementar en Azure AKS	Azure AKS
Implementar en Red Hat OpenShift	Red Hat OpenShift

Configurar el entorno

TAREA	PÁGINA
Configurar el controlador de entrada	Ingress
Permitir conexiones SSH a los espacios de trabajo	Reenvío TCP SSH
Usar una base de datos externa	Base de datos externa
Enrutar a través de un proxy externo	Proxy externo

TAREA	PÁGINA
Ejecutar espacios de trabajo en más de una región	Varias regiones
Proporcionar GPU a los espacios de trabajo	Espacios de trabajo habilitados para GPU en AKS

Mantenerlo actualizado

TAREA	PÁGINA
Actualizar una implementación existente	Actualizar

Información relacionada

- Administrar — configuración después de la instalación
- Límites de confianza — lo que usted posee

Deploy an evaluation environment

La VM de 1 clic ejecuta toda la plataforma Citrix SecurSpaces™ en una única máquina virtual (VM). Úsela para una prueba de concepto (POC) o una demostración. La preparación de la VM es la parte que difiere entre plataformas; la instalación, validación y los pasos de gestión son los mismos.

> **Nota:**
>
> La VM de 1 clic no está diseñada para uso en producción y no se puede actualizar ni migrar a una instalación de producción. Para producción, consulte Implementar en un clúster.

La secuencia de implementación

1. **Prepare la VM.** Utilice la página correspondiente a su plataforma en la tabla siguiente. En la nube, el instalador crea la VM por usted.
2. **Instale SecurSpaces.** Consulte Implementar en la nube o Instalar en una VM local.
3. **Valide la implementación.** Consulte Validar la implementación.

4. **Administre el entorno.** Consulte Administrar el entorno de evaluación.

Elija su plataforma

PLATAFORMA	PÁGINA	NOTAS
AWS, Azure o Google Cloud	Implementar en la nube	El instalador crea la VM, DNS y TLS
Citrix XenServer®	Preparar una VM de XenServer	Invitado Ubuntu creado en XenCenter
Microsoft Hyper-V	Preparar una VM de Hyper-V	Invitado Ubuntu en un PC con Windows
Otros hipervisores o metal desnudo	Instalar en una VM local	Cualquier host que cumpla los requisitos

Antes de empezar

- Compruebe los requisitos del host en Requisitos del sistema.
- Elija una capacidad de máquina. Consulte Dimensionamiento.
- Tenga lista una dirección de correo electrónico de administrador.

Para saber cómo funciona la VM de 1 clic, consulte La VM de 1 clic.

Siguiente paso

Elija su plataforma:

- Implementar en la nube
- Preparar una VM de XenServer
- Preparar una VM de Hyper-V
- Instalar en una VM local, para otros hipervisores y hardware sin sistema operativo

Información relacionada

- Implementar en un clúster
- Licencias

Deploy in the cloud

Esta página despliega la VM 1-Click de Citrix SecurSpaces™ en AWS, Azure o Google Cloud. El instalador crea la VM, instala la plataforma y configura los certificados DNS y TLS.

Requisitos previos

- Docker en su máquina local.
- Credenciales para AWS, Azure o Google Cloud, con los permisos en Permisos de la nube.
- En AWS o Google Cloud, acceso de entrada a los puertos en Abrir los puertos requeridos.
- Una dirección de correo electrónico de administrador.
- Una capacidad de máquina. Consulte Dimensionamiento.

Abrir los puertos requeridos

La VM necesita tres puertos de entrada:

PUERTO	UTILIZADO PARA
443	La consola de SecurSpaces y el IDE en la nube, a través de HTTPS
2222	Conexiones SSH desde IDEs locales a espacios de trabajo
22	Acceso SSH a la propia VM, para administración

Lo que tiene que hacer depende del proveedor de la nube.

Azure. No se necesita ninguna acción. El instalador crea un grupo de seguridad de red que permite los tres puertos desde cualquier dirección.

AWS. Abra los puertos usted mismo. El instalador no crea un grupo de seguridad, por lo que la VM utiliza el grupo de seguridad predeterminado de su VPC predeterminada, que no permite el tráfico entrante desde internet. Antes de la implementación, agregue reglas de entrada para los puertos TCP 443, 2222 y 22 a ese grupo de seguridad.

GCP. Abra los puertos usted mismo. El instalador no crea reglas de firewall. Coloca la VM en la red `default` con la etiqueta de red `https-server`. Antes de la implementación, cree reglas de

firewall en la red `default` que permitan los puertos TCP 443, 2222 y 22 a las instancias con la etiqueta `https-server`.

> **Advertencia:**
>
> Permita estos puertos solo desde las direcciones desde las que se conectan sus evaluadores, en lugar de desde cualquier dirección. En Azure, las reglas que crea el instalador permiten cualquier dirección; restrinja su origen después de la implementación si su política de seguridad lo requiere.

Permisos en la nube

El instalador se implementa con la identidad de la nube con la que inicia sesión cuando solicita las credenciales de la nube. Esa identidad necesita permiso para crear la VM y los recursos que la rodean. Lo que necesita depende del proveedor de la nube.

Abrir los puertos en Abrir los puertos requeridos en AWS o GCP es un paso manual y separado. Quien lo haga necesita permiso para cambiar el grupo de seguridad o crear reglas de firewall, lo cual no incluyen los permisos a continuación.

Azure

Inicie sesión con una cuenta de usuario o un principal de servicio. Necesita permiso para crear la VM, su red y un equilibrador de carga.

El instalador solicita un grupo de recursos y sugiere `strong-network-demo-rg`. Si el grupo de recursos ya existe, el instalador lo utiliza. Si no existe, el instalador lo crea. El alcance que conceda depende de eso:

GRUPO DE RECURSOS	CONCEDER EL ROL EN
Ya existe	El grupo de recursos
Creado por el instalador	La suscripción

Para evitar conceder un rol a toda la suscripción, cree primero el grupo de recursos usted mismo y concédale el rol.

Elija una de las siguientes opciones.

Rol integrado. Asigne **Colaborador** en el ámbito de la tabla. Esta es la opción más sencilla.

Roles integrados más específicos. Asigne tanto **Colaborador de máquina virtual** como **Colaborador de red** en ese ámbito. El instalador no crea ninguna cuenta de almacenamiento, por lo que no se necesita ningún rol de almacenamiento.

Rol personalizado. Para obtener los permisos mínimos, cree un rol personalizado con estas acciones y asígnelo en ese ámbito. Reemplace `{subscription-id}` con su ID de suscripción:

```
{

    "Name": "SecurSpaces 1-Click VM deployer",

    "IsCustom": true,

    "Description": "Deploy a SecurSpaces 1-Click VM",

    "Actions": [

        "Microsoft.Compute/virtualMachines/*",

        "Microsoft.Compute/disks/*",

        "Microsoft.Compute/virtualMachines/extensions/*",

        "Microsoft.Network/virtualNetworks/*",

        "Microsoft.Network/publicIPAddresses/*",

        "Microsoft.Network/networkInterfaces/*",

        "Microsoft.Network/networkSecurityGroups/*",

        "Microsoft.Network/loadBalancers/*",

        "Microsoft.Resources/resourceGroups/*",

        "Microsoft.Resources/subscriptions/resourceGroups/read"

    ],

    "NotActions": [],

    "DataActions": [],
```

```
    "NotDataActions": [],

    "AssignableScopes": ["/subscriptions/{subscription-id}"]

}
```

Por ejemplo, para asignar los roles integrados más específicos a una entidad de servicio en un grupo de recursos existente:

```
az role assignment create \

  --assignee <service-principal-id> \

  --role "Virtual Machine Contributor" \

  --scope "/subscriptions/<subscription-id>/resourceGroups/<resource-
group-name>"



az role assignment create \

  --assignee <service-principal-id> \

  --role "Network Contributor" \

  --scope "/subscriptions/<subscription-id>/resourceGroups/<resource-
group-name>"
```

AWS

La identidad necesita permiso para crear una instancia EC2, un par de claves y una dirección IP elástica. El instalador no crea ningún grupo de seguridad ni adjunta ningún rol de IAM a la VM, por lo que no se necesitan permisos de grupo de seguridad ni de IAM para ello.

Elija una de las siguientes opciones.

Política administrada. Adjunte **AmazonEC2FullAccess**. Esta es la opción más sencilla.

Política personalizada. Para los permisos mínimos, adjunte una política con estas acciones:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeImages",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateKeyPair",
                "ec2:DeleteKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:AllocateAddress",
                "ec2:ReleaseAddress",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeAddresses",
                "ec2:CreateTags",
```

```
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": "*"
        }
    ]
}
```

GCP

La identidad necesita permiso para crear una instancia de Compute Engine y una dirección IP externa estática en el proyecto que seleccione. El instalador no adjunta ninguna cuenta de servicio a la VM, por lo que no se necesitan permisos de cuenta de servicio.

El instalador también enumera sus proyectos para que pueda elegir uno, y comprueba que la API de Compute Engine esté habilitada en él. Si la API no está habilitada, el instalador intenta habilitarla.

Elija una de las siguientes opciones.

Roles predefinidos. Conceda **Compute Admin** (`roles/compute.admin`). Esta es la opción más sencilla. Para un acceso más restringido, conceda **Compute Instance Admin (v1)** (`roles/compute.instanceAdmin.v1`) y **Compute Network User** (`roles/compute.networkUser`) en su lugar.

Rol personalizado. Para los permisos mínimos, cree un rol con estos permisos:

```
{

    "title": "SecurSpaces 1-Click VM deployer",

    "description": "Deploy a SecurSpaces 1-Click VM on GCP",

    "stage": "GA",

    "includedPermissions": [

        "compute.instances.create",

        "compute.instances.delete",

        "compute.instances.get",

        "compute.instances.list",

        "compute.instances.setMetadata",

        "compute.instances.setTags",

        "compute.instances.start",

        "compute.instances.stop",

        "compute.addresses.create",

        "compute.addresses.delete",

        "compute.addresses.get",

        "compute.addresses.list",

        "compute.addresses.use",

        "compute.disks.create",

        "compute.disks.delete",

        "compute.disks.get",

        "compute.disks.list",
```

```
        "compute.disks.use",
        "compute.images.get",
        "compute.images.list",
        "compute.images.useReadOnly",
        "compute.zones.get",
        "compute.zones.list",
        "compute.regions.get",
        "compute.regions.list",
        "compute.machineTypes.get",
        "compute.machineTypes.list",
        "compute.networks.get",
        "compute.subnetworks.use",
        "compute.subnetworks.useExternalIp",
        "resourcemanager.projects.get",
        "serviceusage.services.list"
    ]
}
```

Sea cual sea la opción que elija, la identidad también necesita `serviceusage.services.list`, para que el instalador pueda confirmar que la API de Compute Engine está habilitada. Sin ella, el instalador no puede saber que la API está habilitada y sigue pidiéndole que la habilite. Si la API aún no está habilitada, habilítela usted mismo antes de la implementación, o conceda `serviceusage.services.enable` para que el instalador pueda hacerlo.

Ejecutar el instalador

1. Cree un directorio para los archivos de implementación y ejecute el instalador en él:

```
mkdir -p ~/sds-cloud-deployment

cd ~/sds-cloud-deployment

docker run -it --rm -v ${PWD}:/strong-network/shared strongnetwork/
strong_installer:<version>
```

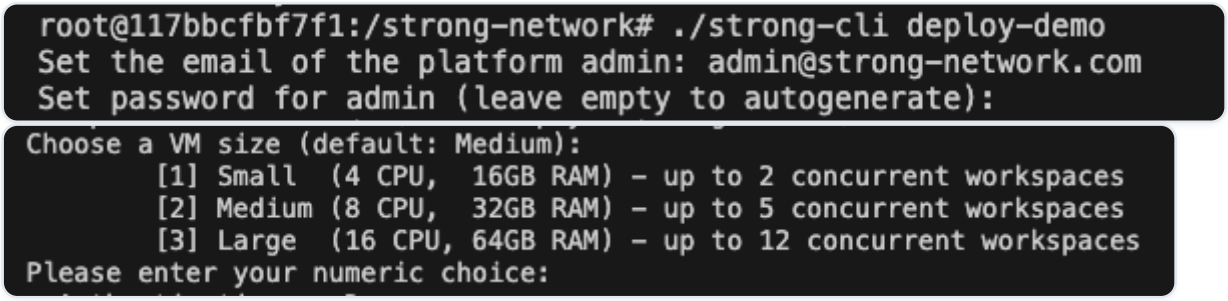
   Sustituya `<version>` por la versión a implementar, por ejemplo `2026.9.4`.

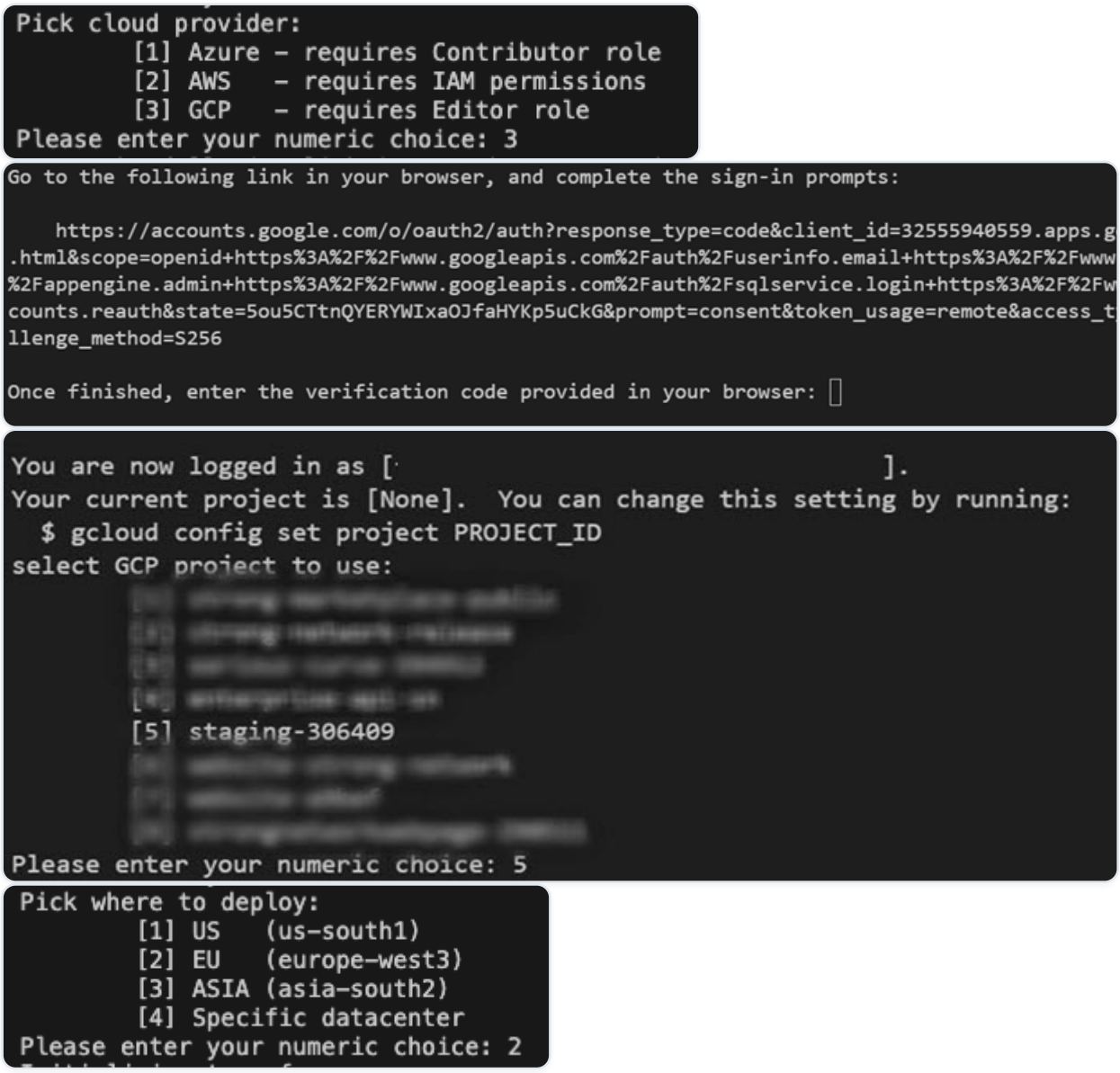
2. En el mensaje `sds-cli`, introduzca:

```
deploy-demo
```

3. Complete las indicaciones:

MENSAJE	INTRODUZCA
Credenciales de administrador	Dirección de correo electrónico y contraseña
Tamaño de la VM	Capacidad de su máquina
Proveedor de la nube	AWS, Azure o GCP
Credenciales de la nube	Su identidad en la nube. Para GCP, seleccione un proyecto de la lista.
Región	EE. UU., UE o Asia, o un centro de datos específico





4. Espere a que el instalador termine. Anote la URL de la plataforma y las credenciales de administrador que muestra.

> **Precaución:**
>
> La salida del instalador y el directorio de despliegue contienen credenciales y el estado de la nube. Guárdelos de forma privada y conserve el directorio: lo necesitará para eliminar los recursos de la nube.

> La VM está en ejecución y la URL de la plataforma está disponible.

Siguiente paso

Continúe con Validar el despliegue.

Prepare a XenServer VM

Esta página crea la VM de Ubuntu en Citrix XenServer® donde está instalado Citrix SecurSpaces™. Cuando la VM esté lista, continúe con Instalar en una VM local.

Requisitos previos

- Un host XenServer administrado con XenCenter, con recursos libres para la capacidad de su máquina. Consulte Dimensionamiento.
- Una ISO de Ubuntu 22.04 o 24.04 Desktop en un repositorio de almacenamiento.
- Una red virtual con acceso a Internet saliente a la que puedan acceder los dispositivos cliente.

Crear la VM

1. En XenCenter, seleccione **Nueva VM** y elija la ISO de Ubuntu Desktop como origen de instalación.
2. Asigne vCPU, memoria y disco para la capacidad de su máquina.
3. Conecte la interfaz de red a la red virtual.
4. Instale Ubuntu Desktop. Cree una cuenta de usuario con permisos `sudo`.

Preparar el invitado

En un terminal de la VM:

1. Instale y habilite SSH:

```
sudo apt update

sudo apt install -y openssh-server

sudo systemctl enable --now ssh
```

2. Anote la dirección IP de la VM:

```
hostname -I
```

3. Para mantener un punto de restauración limpio, tome una instantánea de la VM en XenCenter.

La VM está en ejecución, limpia y accesible.

Solución de problemas

PROBLEMA	RESOLUCIÓN
La comprobación AVX falla en el invitado	La CPU del host de XenServer no es compatible con AVX. Utilice un host compatible.
Los dispositivos cliente no pueden acceder a la VM	Conecte la VM a una red a la que los dispositivos cliente puedan enrutar.

Siguiente paso

Continúe con Instalar en una VM local.

Prepare a Hyper-V VM

Esta página crea la VM de Ubuntu en Microsoft Hyper-V donde se instala Citrix SecurSpaces™. El host de Windows puede también ejecutar el instalador. Cuando la VM esté lista, continúe con Instalar en una VM local.

Requisitos previos

- Una edición de Windows con Hyper-V habilitado, por ejemplo, Windows 11 Pro.
- Suficiente memoria libre en el host para una asignación fija que coincida con la capacidad de su máquina. Consulte Dimensionamiento.
- Espacio libre en disco para el disco virtual y los puntos de control.
- Una ISO de Ubuntu 22.04 o 24.04 Desktop de versiones de Ubuntu.
- Para ejecutar el instalador en el host de Windows: Docker Desktop ejecutando contenedores Linux.

Crear la VM

1. En el **Administrador de Hyper-V**, seleccione su host local.
2. Seleccione **Nuevo** > **Máquina virtual** e introduzca un nombre, por ejemplo `SecurSpaces-Lab`.
3. Seleccione **Generación 2**.
4. Establezca la **Memoria de inicio** en la memoria para la capacidad de su máquina, por ejemplo `16384` MB para Pequeña. Desactive **Usar memoria dinámica para esta máquina virtual**.

5. Conecte el adaptador de red a **Conmutador predeterminado**. Para acceder a la consola desde otros dispositivos, conéctelo a un conmutador virtual externo en su lugar.
6. Cree un disco duro virtual para la capacidad de su máquina, por ejemplo, 200 GB para Pequeña.
7. Seleccione la ISO de Ubuntu Desktop como imagen de arranque y finalice el asistente.
8. Abra la **Configuración** de la VM:
    - En **Procesador**, establezca el número de procesadores virtuales para la capacidad de su máquina, por ejemplo, 4 para Pequeña.
    - En **Seguridad**, mantenga seleccionada la opción **Habilitar arranque seguro** y seleccione la plantilla **Autoridad de certificación UEFI de Microsoft**.
9. Inicie la VM, seleccione **Conectar** e instale Ubuntu Desktop. Cree una cuenta de usuario con permisos `sudo`.
10. Apague la VM, retire la ISO de la unidad de DVD y vuelva a iniciar la VM.

> **Consejo:**
>
> Eliminar una VM en Hyper-V no elimina su VHDX. Cuando repita la instalación, cree un nuevo disco virtual.

Preparar el invitado

En un terminal de la VM:

1. Instale y habilite SSH y curl:

```
sudo apt update

sudo apt install -y openssh-server curl

sudo systemctl enable --now ssh
```

2. Instale las herramientas de Hyper-V para el kernel en ejecución e inicie el demonio KVP, para que Hyper-V informe la dirección IP de la VM:

```
sudo apt install -y "linux-cloud-tools-$(uname -r)"

sudo udevadm control --reload-rules

sudo udevadm trigger --action=add --subsystem-match=misc

sudo systemctl enable --now hv-kvp-daemon
```

3. Evite que la VM se suspenda cuando esté inactiva:

```
sudo systemctl mask sleep.target suspend.target hibernate.target
hybrid-sleep.target
```

4. Anote la dirección IP de la VM:

```
hostname -I
```

5. Desde PowerShell en el host de Windows, compruebe que puede conectarse:

```
ssh <user>@<vm-ip>
```

6. Para mantener un punto de restauración limpio, apague la VM y cree un punto de control.

La VM está en ejecución, limpia y accesible.

Ejecutar pasos posteriores desde Windows

Cuando ejecute el instalador en el host de Windows, use estos comandos de PowerShell en los pasos posteriores.

1. Ejecutar el instalador:

```
New-Item -ItemType Directory -Path
"$env:USERPROFILE\SecurSpacesInstaller"

Set-Location "$env:USERPROFILE\SecurSpacesInstaller"

docker run --rm -it `

  --mount "type=bind,source=$($PWD.Path),target=/strong-network/shared"
`
```

```
  strongnetwork/strong_installer:<version>
```

2. Copiar el script de despliegue a la VM:

```
scp .\deploy.sh <user>@<vm-ip>:~/deploy.sh
```

3. Comprobar DNS y HTTPS:

```
Resolve-DnsName <name>.try.sds.citrix.com

curl.exe --head https://<name>.try.sds.citrix.com/
```

4. Después de un reinicio, compruebe el estado y la dirección IP de la VM, en PowerShell como administrador:

```
Get-VM -Name SecurSpaces-Lab

Get-VMNetworkAdapter -VMName SecurSpaces-Lab | Select-Object
-ExpandProperty IPAddresses
```

Solución de problemas

PROBLEMA	RESOLUCIÓN
La VM no se inicia, con el error `0x800705AA`	Hyper-V no puede asignar la memoria. Libere memoria en el host cerrando aplicaciones u otras VM.
Hyper-V no muestra ninguna dirección IP para la VM	Instale `linux-cloud-tools-$(uname -r)` e inicie `hv-kvp-daemon`. El paquete genérico `linux-cloud-tools-virtual` puede coincidir con un kernel diferente.
La comprobación AVX falla en el invitado	La CPU del host no soporta AVX. Utilice un host compatible.
El contenedor del instalador no se inicia	Asegúrese de que Docker Desktop esté ejecutando contenedores Linux y pueda acceder a Docker Hub.

PROBLEMA	RESOLUCIÓN
La URL de la plataforma se resuelve a la dirección incorrecta	La dirección de la VM en el Conmutador predeterminado ha cambiado. Compare `hostname -I` con el registro DNS.
Otros dispositivos no pueden acceder a la consola	El Conmutador predeterminado solo es accesible desde el host de Windows. Utilice un conmutador virtual externo.

Siguiente paso

Continúe con Instalar en una VM local.

Install on a local VM

Esta página instala Citrix SecurSpaces™ en una VM o host Ubuntu que haya preparado. Ejecuta el instalador en una máquina separada, el host del instalador. Genera un script de implementación que se ejecuta en el host de destino.

Para preparar una VM primero, consulte Preparar una VM de XenServer o Preparar una VM de Hyper-V.

Requisitos previos

- Un host de destino que cumpla los requisitos de VM de 1 clic, sin Docker, Kubernetes ni K3s instalados.
- Un host de instalador con Docker, acceso HTTPS saliente a Docker Hub y 20 GB de espacio libre en disco.
- Una dirección de correo electrónico de administrador.
- Una capacidad de máquina. Consulte Dimensionamiento.

Comprobar el host de destino

1. En el host de destino, ejecute:

```
cat /etc/os-release

grep -o 'avx[^ ]*' /proc/cpuinfo | head -1

free -h
```

```
df -h /

hostname -I
```

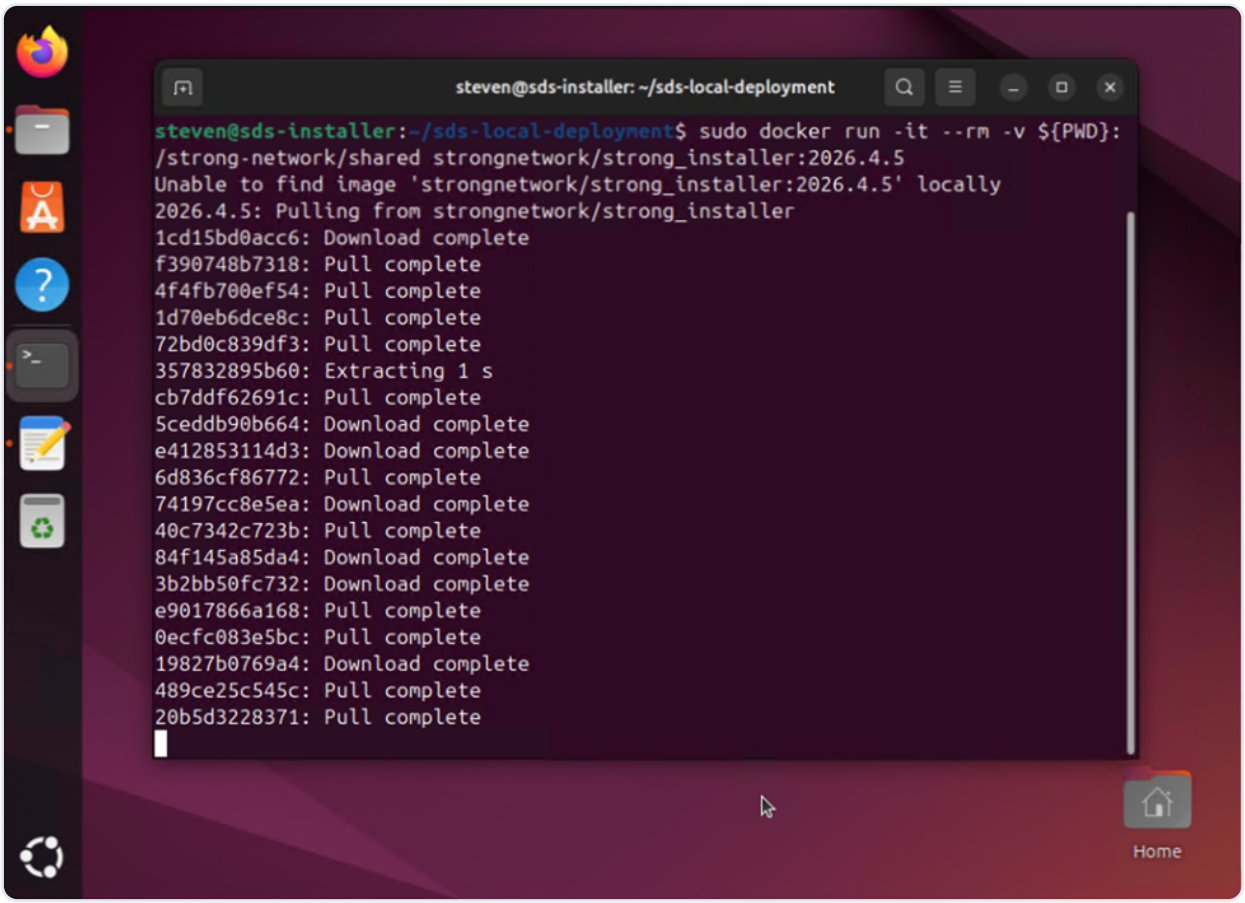
2. Compruebe que:
   - El sistema operativo es Ubuntu 22.04 o 24.04.
   - El comando AVX devuelve una salida. Si no lo hace, utilice un host diferente.
   - La memoria y el disco coinciden con la capacidad de su máquina.
3. Anote la dirección IP que utilizarán los dispositivos cliente.

Ejecutar el instalador

1. En el host del instalador, cree un directorio privado y ejecute el instalador en él:

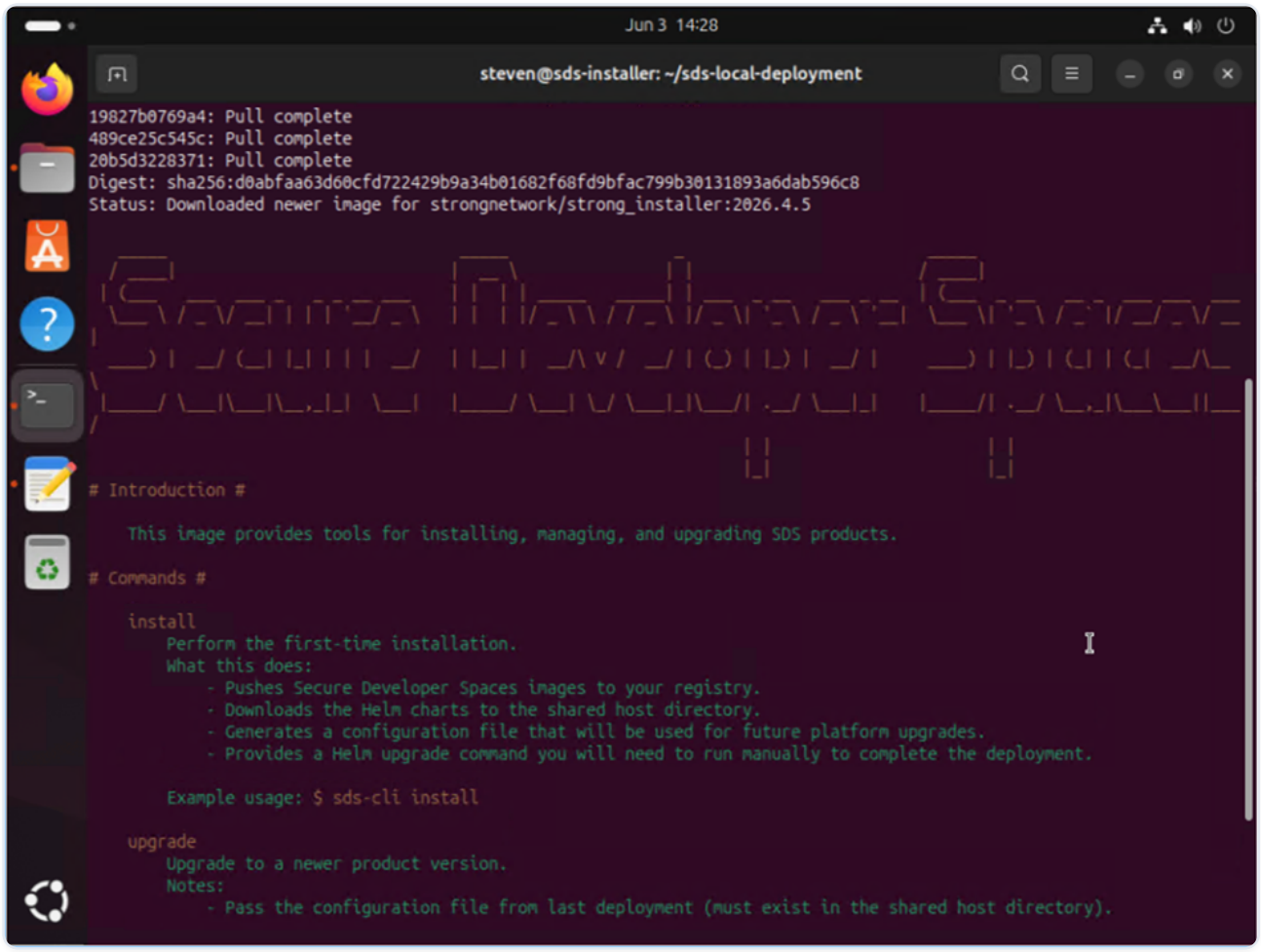
```
mkdir -p ~/sds-local-deployment

cd ~/sds-local-deployment

docker run -it --rm -v ${PWD}:/strong-network/shared strongnetwork/
strong_installer:<version>
```

   Sustituya `<version>` por la versión a implementar, por ejemplo, `2026.9.4`. En Windows, consulte Ejecutar pasos posteriores desde Windows.



2. Si el instalador ofrece una versión más reciente, seleccione **No** para permanecer en la versión que eligió.

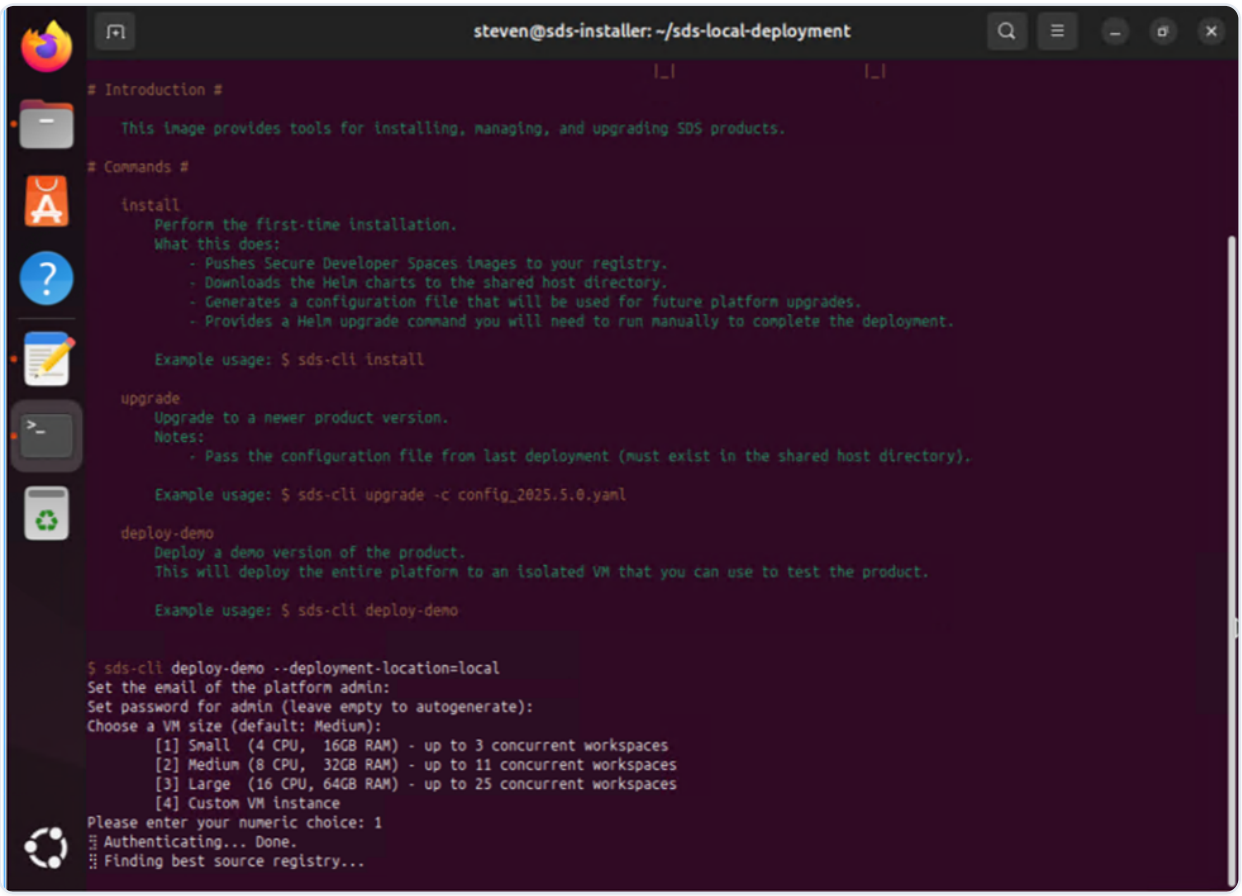
Se abre el indicador `sds-cli`. Solo acepta subcomandos de la CLI de SecurSpaces. Consulte CLI de SDS.



Generar el script de implementación

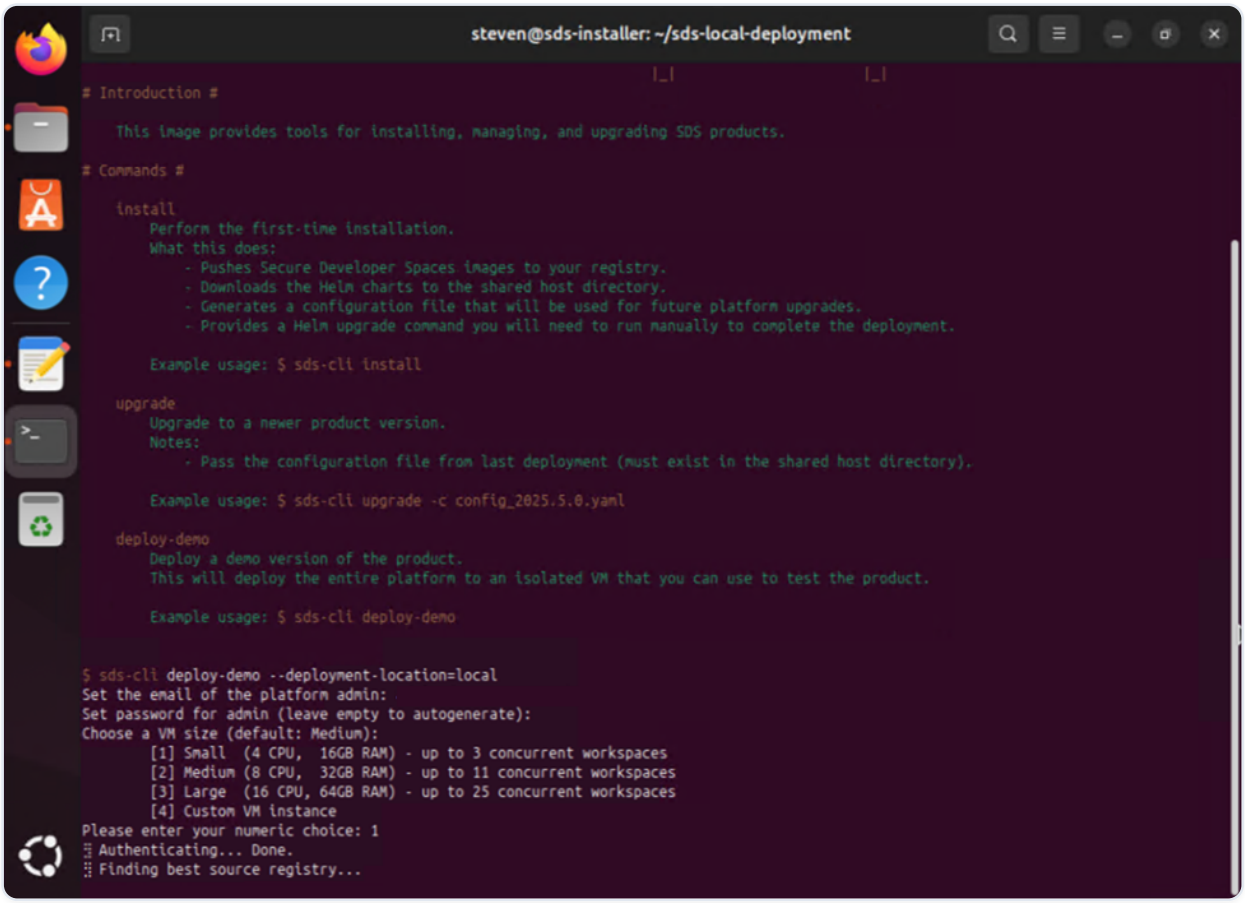
1. En el indicador `sds-cli`, introduzca este comando en una sola línea:

```
deploy-demo --deployment-location=local
```



2. Complete las solicitudes:

SOLICITUD	INTRODUZCA
Correo electrónico del administrador	La dirección con la que inicia sesión
Contraseña del administrador	Una contraseña segura, o dejar en blanco para generar una
Capacidad de la máquina	La capacidad que coincide con el host de destino. El valor predeterminado es Medio.
Región	**1** EE. UU., **2** UE o **3** Asia



3. En **Script de implementación local generado**, copie el script desde `#!/bin/bash` hasta, pero sin incluir, la línea separadora.
4. Guárdelo en el host del instalador como `deploy.sh`, en UTF-8 sin BOM y con terminaciones de línea LF.
5. Anote la URL asignada, por ejemplo `<name>.try.sds.citrix.com`, y las credenciales de administrador.

> **Precaución:**
>
> El script y la salida del instalador contienen secretos. Guárdelos de forma privada.

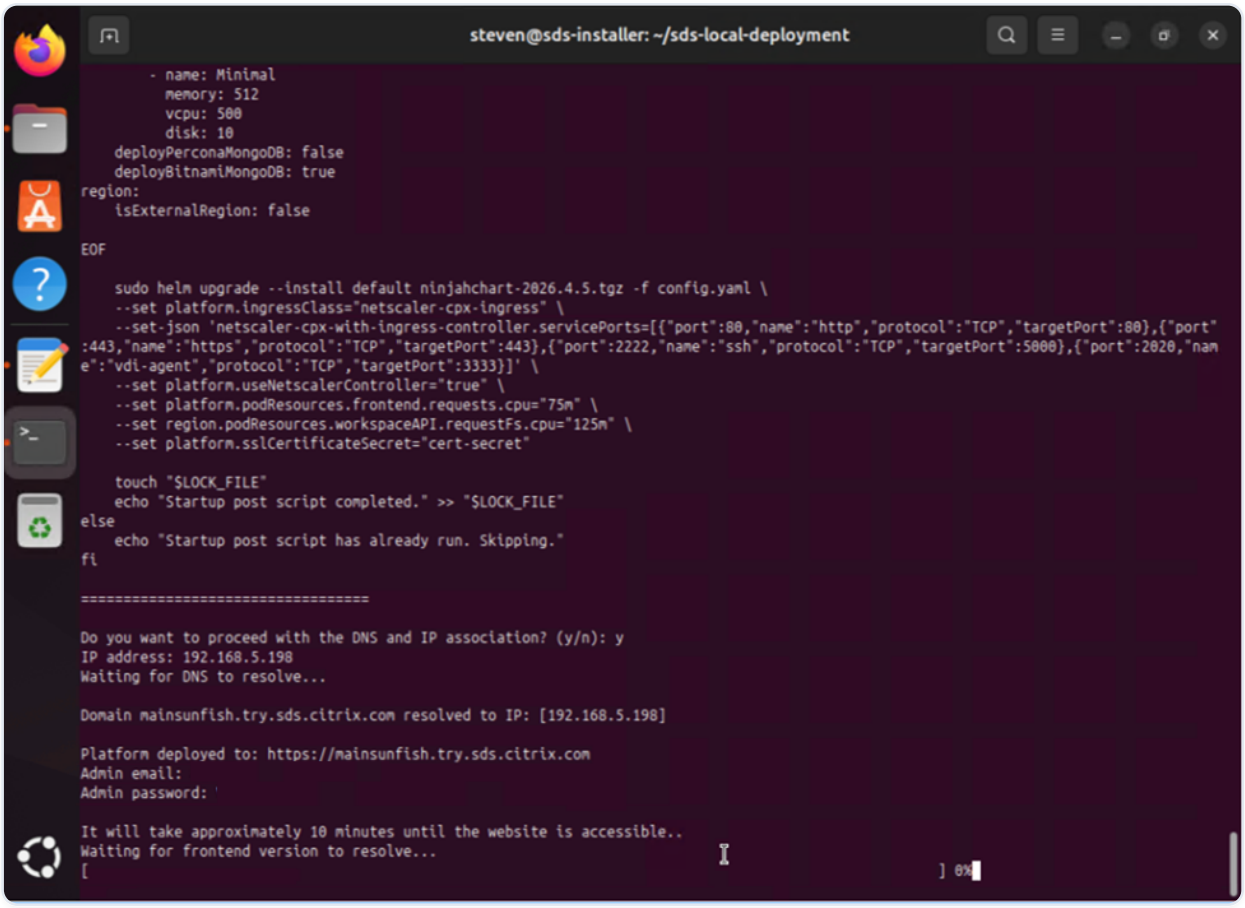
> Deje el instalador abierto para el siguiente paso.

Asociar la dirección IP con DNS

> **Importante:**

> Complete este paso en el plazo de 1 hora desde la generación del script. Puede ejecutar el script al mismo tiempo.

1. Cuando el instalador pregunte si desea continuar con la asociación de DNS e IP, introduzca `y`.
2. Introduzca la dirección IP del host de destino.

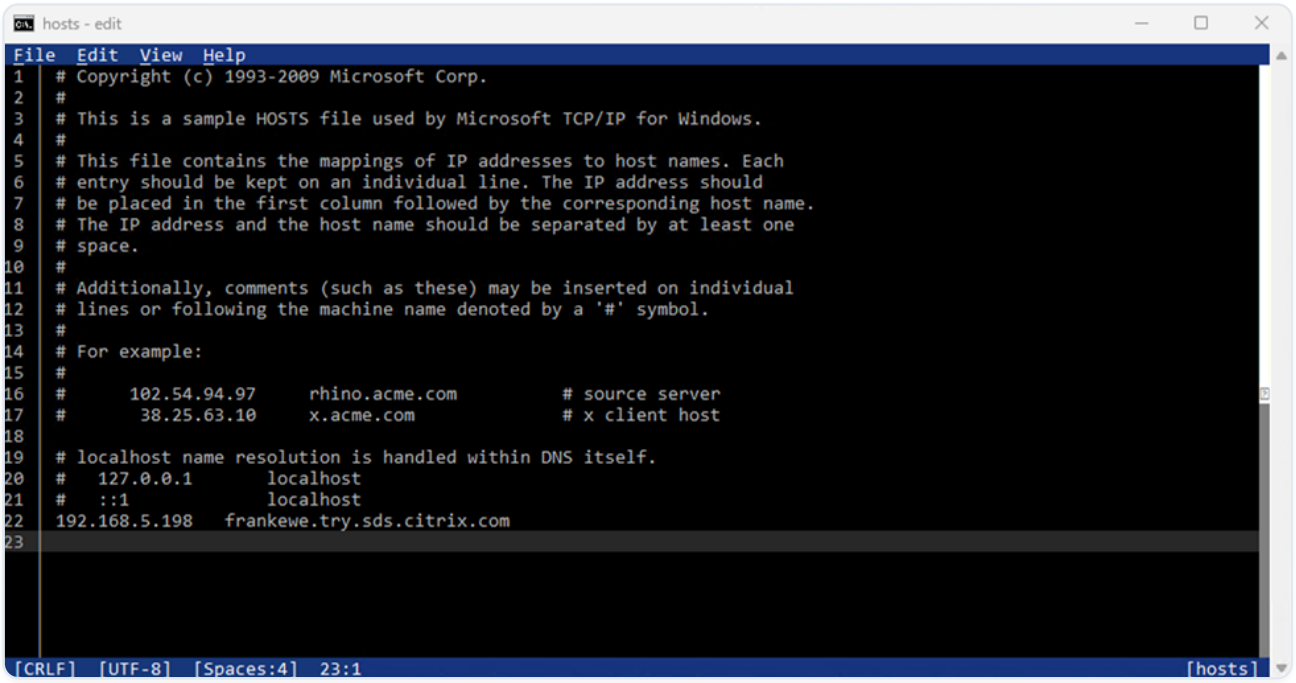


3. Desde un dispositivo cliente, compruebe que el nombre de host asignado se resuelve en esa dirección:

```
nslookup <name>.try.sds.citrix.com
```

Si los dispositivos cliente no pueden resolver el nombre de host, añada un registro a su servidor DNS o añada esta línea al archivo hosts en cada dispositivo cliente:

```
<host-ip>  <name>.try.sds.citrix.com
```



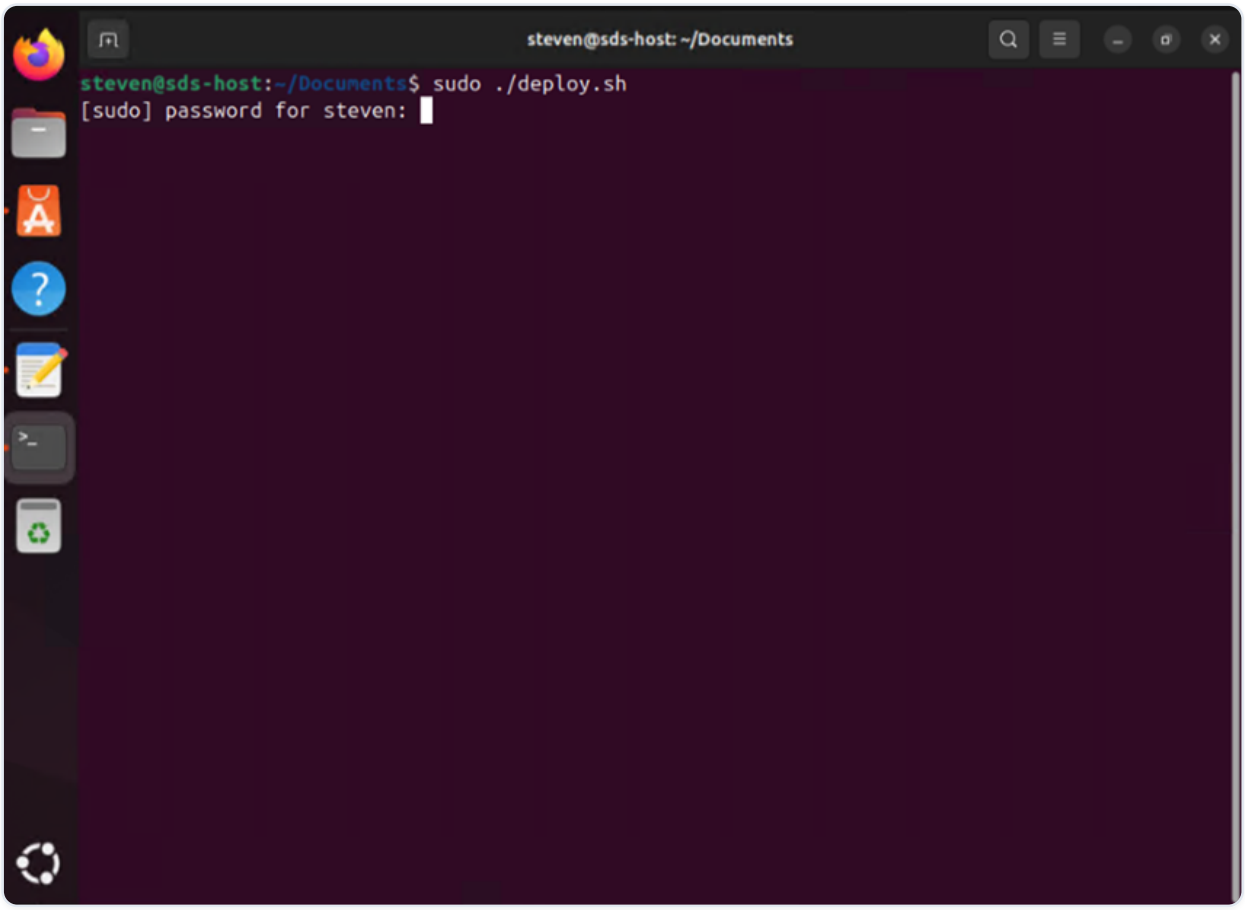
Ejecutar el script de despliegue

1. Copie `deploy.sh` al host de destino y conéctese a él:

```
scp deploy.sh <user>@<host-ip>:~/deploy.sh

ssh <user>@<host-ip>
```

2. En el host de destino, restrinja los permisos del archivo y ejecútelo:

```
chmod 600 ~/deploy.sh

sudo sh -c 'umask 077; exec bash ~/deploy.sh'
```



3. Cuando el script termine, compruebe el clúster:

```
sudo kubectl get nodes

sudo kubectl get pods -A
```

Espere hasta que el nodo esté `Ready` y cada pod muestre todos sus contenedores listos en la columna **READY**.

Esperar la inicialización

Un trabajo en segundo plano aplica la licencia de evaluación y crea datos de muestra una vez que finaliza el script.

1. Busque el trabajo y siga su registro:

```
sudo kubectl get jobs

sudo kubectl logs job/<job-name>
```

2. Espere `One Click VM Demo Data Successfully Initialized.` en el registro.

Precaución:

Hasta que finalice la inicialización, el asistente de configuración puede mostrar un paso de **Licencia** con **Community** seleccionado. No seleccione Community. Espere y luego recargue la página.

Solución de problemas

PROBLEMA	RESOLUCIÓN
El contenedor del instalador no se inicia	Asegúrese de que Docker esté en ejecución y pueda acceder a Docker Hub.
`unknown command` en el indicador `sds-cli`	Introduzca el subcomando en una sola línea, sin `sds-cli`, una ruta o caracteres de continuación de línea.
El script falla inmediatamente	Asegúrese de que `deploy.sh` contenga solo el script, comience con `#!/bin/bash` y use finales de línea LF sin BOM.
El script falla más tarde	El host de destino no está limpio. Restaure una instantánea limpia o reinstale Ubuntu, luego ejecute el script de nuevo.
La URL de la plataforma no se resuelve	Compruebe el registro DNS o el archivo hosts. Si ha pasado más de 1 hora, ejecute el instalador de nuevo para generar un nuevo script.

Siguiente paso

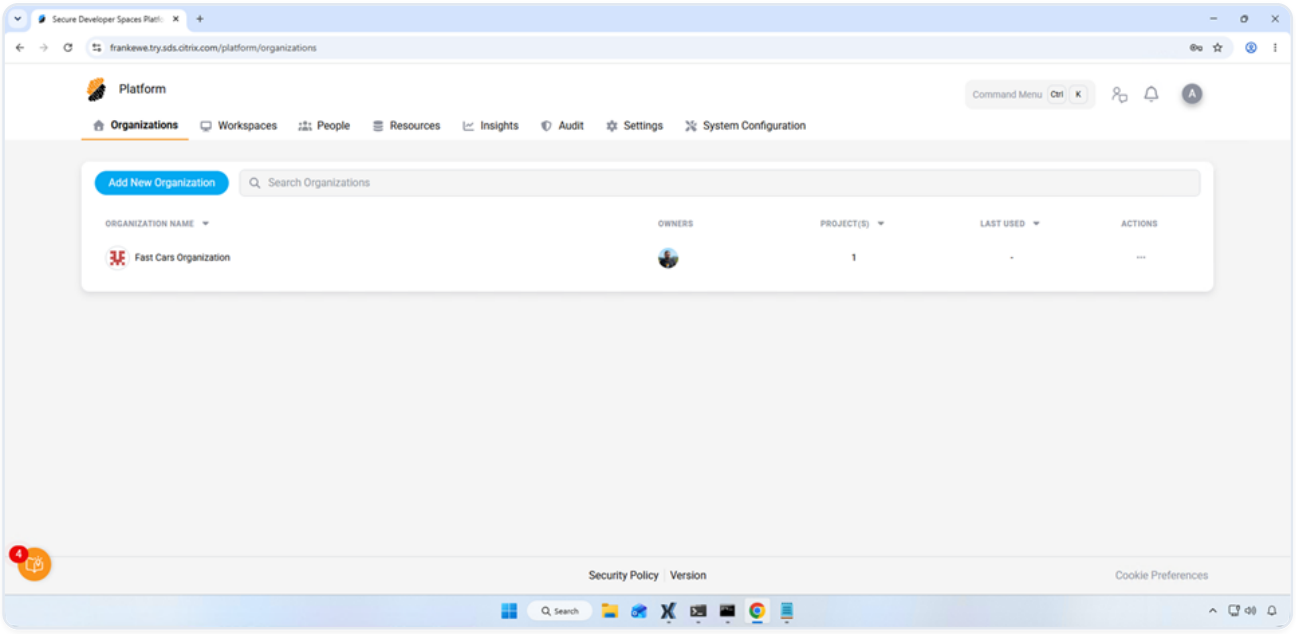
Continúe con Validar la implementación.

Validate the deployment

Esta página comprueba que un nuevo entorno de evaluación de Citrix SecurSpaces™ funciona, tanto para implementaciones en la nube como locales.

Iniciar sesión

1. En un navegador, vaya a `https://<name>.try.sds.citrix.com`. Utilice el nombre de host, no la dirección IP.
2. Introduzca el correo electrónico del administrador, seleccione **Continuar** e introduzca la contraseña del administrador del instalador.



Si el inicio de sesión falla con "nombre de usuario o contraseña no válidos", espere 5 minutos y vuelva a intentarlo.

Complete el asistente de configuración

1. En **Registrar dominio de inicio de sesión**, seleccione **Omitir**. Para usar su proveedor de identidades en su lugar, consulte Proveedores de identidades.
2. En **Aplicaciones de repositorio de código**, seleccione **Omitir**. Para conectar un proveedor más tarde, consulte Repositorios de código.
3. En **Organización**, introduzca un nombre de organización y un nombre de proyecto, por ejemplo `Test Lab` y `Hello SecurSpaces`, y seleccione **Finalizar**.

Comprobar la licencia

Vaya a **Plataforma** > **Configuración del sistema** > **Licencia**, y compruebe el tipo de licencia, los límites y la fecha de caducidad. La licencia de evaluación es válida durante 6 meses, y el certificado TLS durante 90 días. Consulte Licencias.

Crear un espacio de trabajo

1. En su proyecto, seleccione **Crear su primer espacio de trabajo**.

2. Seleccione **Crear espacio de trabajo personalizado**.
3. En **Información básica**, introduzca:

CONFIGURACIÓN	VALOR
Nombre	`hello-securspaces`
Propietario	Su usuario
Imagen del espacio de trabajo	Imagen genérica predeterminada
Región	Región predeterminada
Recursos	Mínimo

4. Seleccione **Revisar y lanzar**, y luego **Lanzar**.
5. Espere a que el estado cambie a **En ejecución**.

Ejecutar código

1. En la columna **Acceso**, selecciona el icono de VS Code. Si el navegador bloquea la ventana, permite las ventanas emergentes para la URL de la consola URL.
2. Si el IDE pregunta si confiar en `/home/developer`, selecciona **Administrar** > **Confiar**.
3. Abre un terminal y ejecuta:

```
mkdir -p ~/hello-securspaces

cd ~/hello-securspaces

printf 'print("Hello from Citrix SecurSpaces!")\n' > hello.py

python3 hello.py

sha256sum hello.py
```

4. Comprueba que la salida es `Hello from Citrix SecurSpaces!` y anota la suma de verificación.

Comprobar que los archivos persisten

1. En la página **Espacios de trabajo**, abre el menú de acciones del espacio de trabajo, selecciona **Pausar** y espera a que aparezca **Pausado**.
2. Selecciona **Ejecutar** y espera a que aparezca **En ejecución**.
3. Vuelve a abrir el IDE y ejecuta:

```
python3 ~/hello-securspaces/hello.py

sha256sum ~/hello-securspaces/hello.py
```

4. Comprueba que la salida y la suma de verificación son las mismas que antes.

La implementación funciona.

Siguiente paso

Continúa con Administrar el entorno de evaluación.

Para aprender SecurSpaces como desarrollador, sigue Tu primer espacio de trabajo.

Manage the evaluation environment

Esta página se aplica a entornos de evaluación de Citrix SecurSpaces™ en la nube y locales. Para problemas específicos de la plataforma, consulte la sección de solución de problemas de la página de su plataforma.

Reiniciar la VM

1. Apague o reinicie la VM desde el sistema operativo, por ejemplo con `sudo reboot`.
2. Para una VM local, compruebe que su dirección IP no haya cambiado. Si lo ha hecho, actualice el registro DNS o el archivo de hosts.
3. Conéctese a la VM y espere hasta que el nodo y cada pod estén listos:

```
sudo kubectl get nodes

sudo kubectl get pods -A
```

   Esto puede tardar varios minutos. No reinstale mientras se inician los servicios.
4. Si un espacio de trabajo muestra **Error**, seleccione **Pausar**, espere a que aparezca **Pausado** y seleccione **Ejecutar**.

Solución de problemas

PROBLEMA	RESOLUCIÓN
El asistente de configuración muestra **Licencia** con **Comunidad** seleccionada	La inicialización no ha finalizado. Espere y, a continuación, recargue la página. No seleccione Comunidad.
El inicio de sesión falla justo después de la implementación	Los servicios aún se están iniciando. Espere 5 minutos y vuelva a intentarlo.
La URL de la plataforma se resuelve en la dirección incorrecta	La dirección IP de la VM cambió. Actualice el registro DNS o el archivo de hosts.
Un espacio de trabajo muestra **Error** después de un reinicio	Espere hasta que todos los pods estén listos, luego pause y ejecute el espacio de trabajo.
El navegador informa un error de certificado después de 90 días	El certificado TLS ha caducado. Es válido por 90 días.
La consola informa una licencia caducada después de 6 meses	La licencia de evaluación ha caducado. Compruebe **Platform** > **System Configuration** > **License**.

Eliminar el entorno

1. Guarde cualquier nota, resultado o captura de pantalla que necesite.
2. Elimine la plataforma:
   - **Nube:** elimine los recursos que creó el instalador.
   - **Local:** en el host de destino, ejecute `sudo /usr/local/bin/k3s-uninstall.sh`, o elimine la VM. En Hyper-V, también elimine el archivo VHDX y los puntos de control.
3. Elimine cualquier registro DNS o entrada de archivo de hosts que haya añadido.
4. En el host del instalador, elimine el script de implementación, la salida del instalador y el directorio de implementación.

Información relacionada

- Implementar un entorno de evaluación
- Implementar en un clúster

Deploy to a cluster

Citrix SecurSpaces™ se ejecuta en cualquier clúster compatible con Kubernetes, incluido OpenShift. La preparación de ese clúster es la parte que difiere entre plataformas; todo lo demás es igual.

> **Nota**

> Esta página es para una implementación de producción. **Si solo necesita evaluar SecurSpaces, no necesita ningún clúster** — la VM de 1 clic ejecuta toda la plataforma en una única máquina virtual, y es la ruta más rápida para obtener un entorno de trabajo para una prueba de concepto o una demostración. Consulte Implementar un entorno de evaluación. No está destinada para uso en producción.

La secuencia de implementación

1. **Prepare su infraestructura** — un clúster de Kubernetes, un registro de contenedores y una base de datos MongoDB. Esto es específico de la plataforma; utilice la página correspondiente a su plataforma a continuación.
2. Instalar con la CLI de Strong Installer — extraiga el gráfico de Helm, envíe las imágenes a su registro y cree el archivo de configuración.
3. Implementar en el clúster — instale el controlador de entrada, cargue el secreto TLS y aplique el gráfico de Helm.
4. **Configure la plataforma** — identidad, repositorios y acceso. Consulte la tabla al final de la página de instalación.

> **Importante:**

> Cada implementación necesita un controlador de entrada, y el gráfico instala uno para usted solo si utiliza NetScaler CPX. Decida qué controlador va a utilizar antes de empezar, porque afecta al clúster que construya y a cómo se expone el SSH del espacio de trabajo. Consulte Ingress.

Elija su plataforma

PLATAFORMA	PÁGINA	NOTAS
Amazon EKS	Amazon EKS	EKS, ECR y MongoDB Atlas
Azure AKS	Azure AKS	AKS, ACR y MongoDB Atlas o Cosmos DB
Google GKE	Google GKE	GKE Standard, Artifact Registry y MongoDB Atlas. Autopilot no es compatible
Red Hat OpenShift	Red Hat OpenShift	Guía autónoma, incluyendo la política de ruta comodín específica de OpenShift
Nutanix Kubernetes Platform	Nutanix Kubernetes Platform	NKP 2.17 o posterior, con ingress de NetScaler CPX

Los clústeres autoalojados y otras distribuciones gestionadas siguen la misma secuencia: crear el clúster, proporcionar un registro y una base de datos, luego instalar. Consulte Requisitos del sistema para las versiones de Kubernetes compatibles y el dimensionamiento.

Antes de empezar

REQUISITO	DETALLE
Dominios	Un dominio de host y un subdominio comodín para soporte de proxy como `*.proxy.example.com`
TLS	Certificados para ambos dominios
Base de datos	MongoDB, alojada o en clúster. Consulte La base de datos de SecurSpaces
Registro	Un registro de contenedores que usted controla, al que el instalador envía imágenes
Dimensionamiento	Grupos de nodos para los niveles de servicio y espacio de trabajo. Consulte Dimensionamiento

REQUISITO	DETALLE
Licencia	Una licencia de SecurSpaces. Consulte Licencias

Para una evaluación en lugar de una implementación de producción, la VM de 1 clic es considerablemente más rápida. Consulte Implementar un entorno de evaluación.

Información relacionada

- Arquitectura
- Requisitos del sistema
- NGINX
- Varias regiones
- Actualización

Amazon EKS

Esta página prepara la infraestructura de AWS que Citrix SecurSpaces™ necesita: un clúster de Kubernetes para ejecutar, un registro de contenedores desde el que extraer imágenes y una base de datos MongoDB para almacenar el estado de la plataforma.

Cuando haya terminado, continúe con Instalar con la CLI de Strong Installer, que es la misma para todas las plataformas.

Requisitos previos

- Una cuenta de AWS con permisos para crear recursos de EKS, ECR y redes.
- Una suscripción a MongoDB Atlas.
- Dos nombres de dominio: uno normal como `example.com`, y un subdominio comodín para soporte de proxy como `*.proxy.example.com`.
- Certificados TLS para esos dominios.
- Un proveedor de identidades, como Okta, si tiene la intención de usar SAML.
- Un controlador de entrada, o una decisión sobre cuál usar. SecurSpaces no puede servir tráfico sin uno, y solo NetScaler CPX es implementado por el gráfico. Consulte Entrada.

Para el dimensionamiento y las versiones compatibles, consulte Requisitos del sistema.

Instale las siguientes herramientas:

- Interfaz de línea de comandos de AWS
- eksctl
- kubectl

Crear un clúster de EKS

1. Configure la AWS CLI con sus credenciales:

   ```
   aws configure
   ```

   Introduzca su ID de clave de acceso de AWS, clave de acceso secreta, región predeterminada y formato de salida cuando se le solicite.

El tamaño de referencia para unos 500 desarrolladores es de dos nodos de servicio `m7i.2xlarge` (8 vCPU, 32 GiB) y un grupo de espacios de trabajo de autoescalado de `m7i.4xlarge` (16 vCPU, 64 GiB). Consulte Dimensionamiento.

1. Cree el clúster:

   ```
   eksctl create cluster \

     --name $MY_EKS_CLUSTER_NAME \

     --region $AWS_REGION \

     --nodegroup-name standard-nodes \

     --node-type m7i.2xlarge \

     --nodes 2 \

     --nodes-min 2 \

     --nodes-max 4 \

     --managed
   ```

2. Añada un grupo de nodos para espacios de trabajo, con autoescalado. Los espacios de trabajo son la parte elástica de la implementación, así que dé a este grupo espacio para crecer:

```
eksctl create nodegroup \
  --cluster $MY_EKS_CLUSTER_NAME \
  --region $AWS_REGION \
  --name workspace-nodes \
  --node-type m7i.4xlarge \
  --nodes 2 \
  --nodes-min 2 \
  --nodes-max 10 \
  --managed
```

3. verificar la conexión:

```
kubectl get nodes
```

Cree un registro de Amazon ECR

SecurSpaces extrae sus imágenes de servicio y sus imágenes de espacio de trabajo de un registro que usted controla. El instalador las envía allí en la siguiente etapa.

1. Cree un repositorio para las imágenes de la plataforma:

```
aws ecr create-repository \
  --repository-name strong-network \
  --image-scanning-configuration scanOnPush=true
```

2. Cree un repositorio para las imágenes de espacio de trabajo:

```
aws ecr create-repository \
  --repository-name ws-images \
```

```
  --image-scanning-configuration scanOnPush=true
```

3. Autentique Docker en el registro:

```
aws ecr get-login-password --region $AWS_REGION | docker login --
username AWS --password-stdin $AWS_ACCOUNT_ID.dkr.ecr.
$AWS_REGION.amazonaws.com
```

4. Para una implementación multirregión, configure la replicación entre regiones:

```
aws ecr put-replication-configuration \

  --replication-configuration '{"rules":[{"destinations":
[{"region":"us-west-2","registryId":"$AWS_ACCOUNT_ID"}]}]}'
```

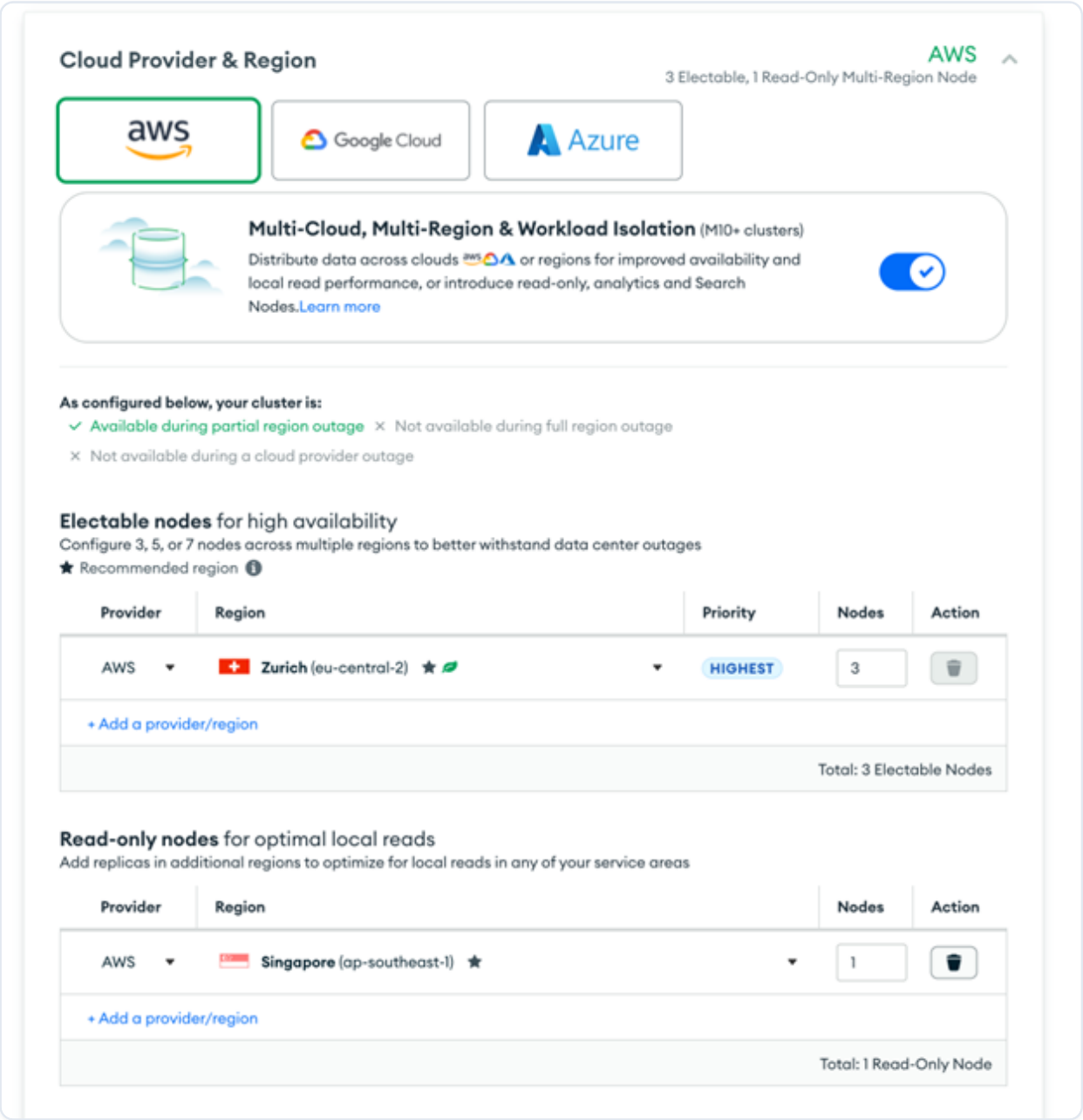
Cree una base de datos MongoDB

SecurSpaces almacena el estado de su plataforma en MongoDB. Para saber qué contiene y qué tamaño se espera que alcance, consulte La base de datos de SecurSpaces.

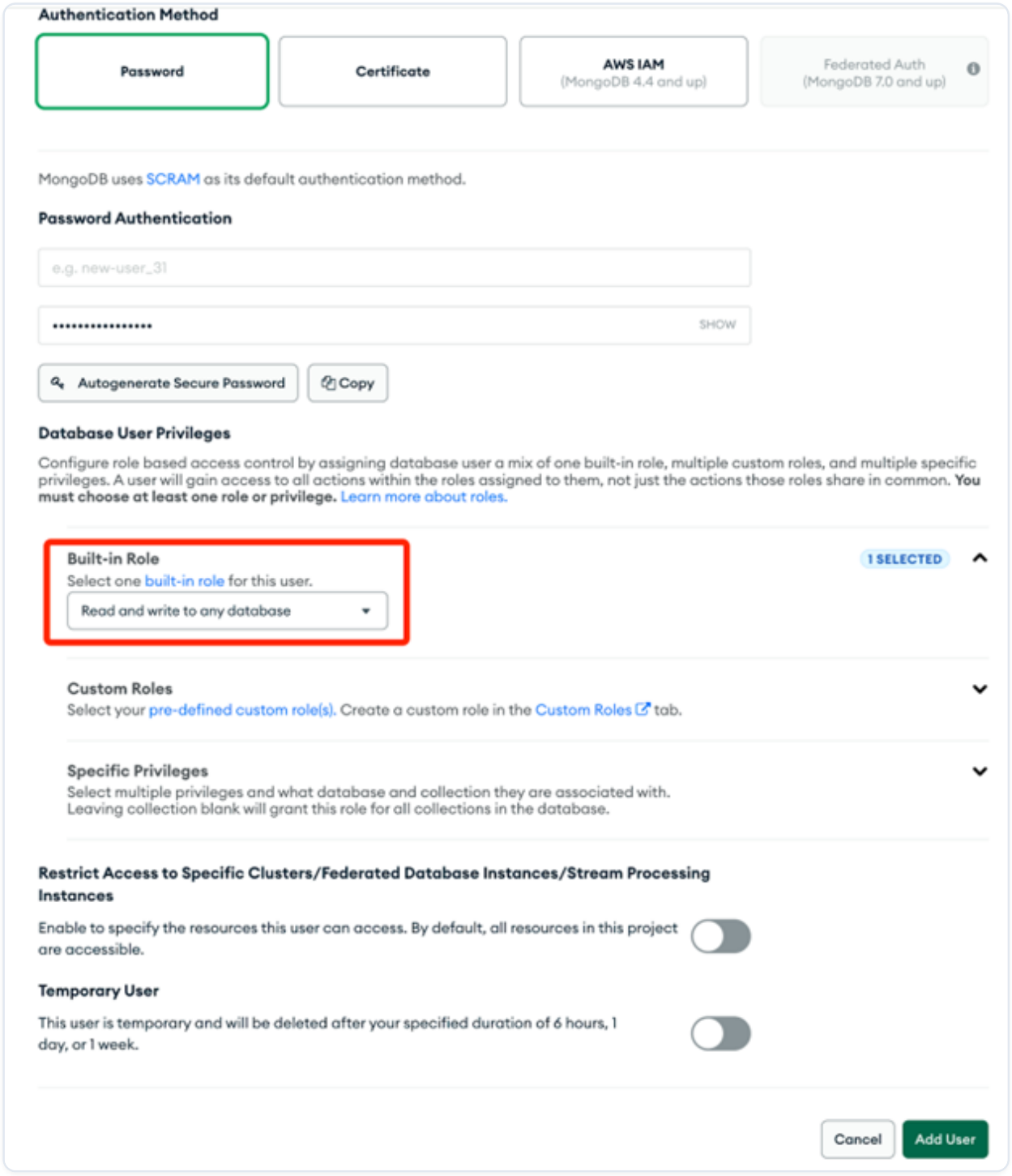
1. En MongoDB Atlas, abra la página de la base de datos y seleccione **Crear**.

2. Configure la implementación y seleccione **Crear implementación**:

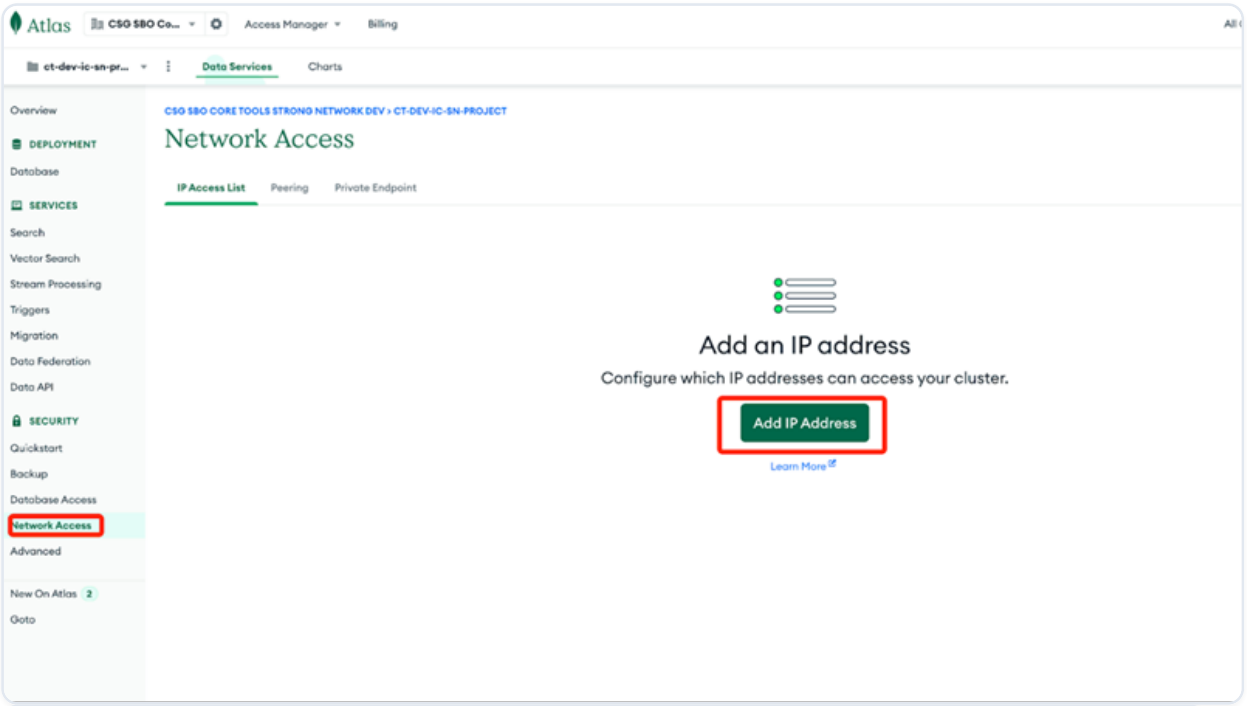
   - Seleccione **AWS** como proveedor de la nube.
   - Elija la misma región que el clúster de EKS.
   - Seleccione el nivel M10 con autoescalado.

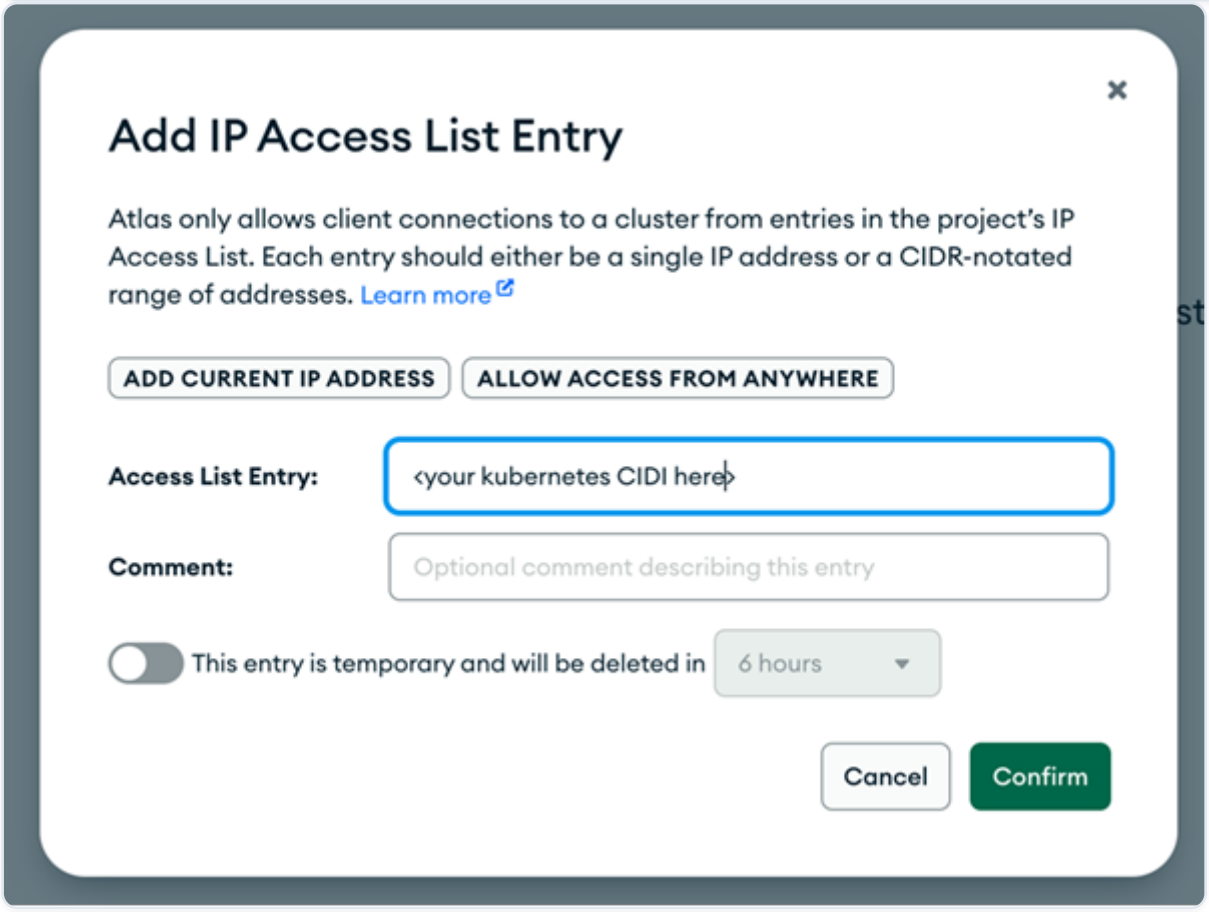


3. En la página **Acceso a la base de datos**, añada un usuario.



4. En la página **Acceso a la red**, permita que su clúster de EKS acceda a la base de datos. Añada los bloques CIDR para la VPC del clúster, o empareje la VPC con Atlas, que es la opción más segura.





También puede ejecutar MongoDB dentro del clúster en lugar de usar Atlas. Consulte Configurar una base de datos externa.

Siguiente paso

Su infraestructura de AWS está lista. Continúe con Instalar con la CLI de Strong Installer.

Durante esa instalación también configuró el controlador de entrada. Si no ha elegido uno, hágalo primero — consulte Ingress.

Información relacionada

- Despliegue de Kubernetes
- Requisitos del sistema
- Ingress
- Espacios de trabajo habilitados para GPU

Azure AKS

Esta página prepara la infraestructura de Azure que Citrix SecurSpaces™ necesita: un clúster de Kubernetes para ejecutarse, un registro de contenedores para extraer imágenes, y una base de datos MongoDB para almacenar el estado de la plataforma.

Cuando haya terminado, continúe con Instalar con la CLI de Strong Installer, que es la misma para todas las plataformas.

Requisitos previos

- Una suscripción de Azure con permisos para crear recursos de AKS, ACR y redes.
- Una suscripción a MongoDB Atlas o Azure Cosmos DB para MongoDB.
- Dos nombres de dominio: uno normal como `example.com`, y un subdominio comodín para soporte de proxy como `*.proxy.example.com`.
- Certificados TLS para esos dominios.
- Un proveedor de identidades, como Okta, si tiene la intención de usar SAML.
- Un controlador de entrada, o una decisión sobre cuál usar. SecurSpaces no puede servir tráfico sin uno, y solo NetScaler CPX es implementado por el gráfico. Consulte Entrada.

Para conocer el tamaño y las versiones compatibles, consulte Requisitos del sistema.

Instale las siguientes herramientas:

- CLI de Azure
- kubectl

Crear un clúster de AKS

1. Cree un grupo de recursos. Este es el contenedor lógico para la implementación, y su ubicación determina dónde se ejecutan los recursos cuando no se especifica uno:

   ```
   az group create --name $MY_RESOURCE_GROUP_NAME --location $REGION
   ```

2. Crear el clúster. El siguiente ejemplo crea un clúster con una identidad administrada asignada por el sistema:

   ```
   az aks create \

     --resource-group $MY_RESOURCE_GROUP_NAME \

     --name $MY_AKS_CLUSTER_NAME \

     --node-count 1 \

     --generate-ssh-keys
   ```

   El ejemplo crea un único nodo. Ajuste el tamaño del clúster a la carga esperada: el tamaño de referencia para aproximadamente 500 desarrolladores es de dos nodos de servicio `Standard_D8as_v6` (8 vCPU, 32 GiB) y un grupo de espacios de trabajo de autoescalado de `Standard_D16as_v6` (16 vCPU, 64 GiB). Consulte Dimensionamiento.

3. Descargue las credenciales y apunte `kubectl` al clúster:

   ```
   az aks get-credentials --resource-group $MY_RESOURCE_GROUP_NAME --name
   $MY_AKS_CLUSTER_NAME
   ```

4. verificar la conexión:

   ```
   kubectl get nodes
   ```

Crear un Azure Container Registry

SecurSpaces extrae sus imágenes de servicio y sus imágenes de espacio de trabajo de un registro que usted controla. El instalador las envía allí en la siguiente etapa.

1. Cree el registro. El nombre debe ser único dentro de Azure y contener entre 5 y 50 caracteres alfanuméricos en minúsculas:

```
az acr create --resource-group myResourceGroup --name
mycontainerregistry --sku Basic
```

2. Cree un principal de servicio con el rol `AcrOwner`. El comando devuelve `appId`, `displayName`, `password` y `tenant`:

```
acr_resource_id=$(az acr show --name <acr-name> --query id --output
tsv)

az ad sp create-for-rbac --name <service-principal-name> --role
AcrOwner --scopes ${acr_resource_id} --sdk-auth
```

3. verificar el principal de servicio iniciando sesión en el registro:

```
docker login <acr-name>.azurecr.io --username <service-principal-id>
```

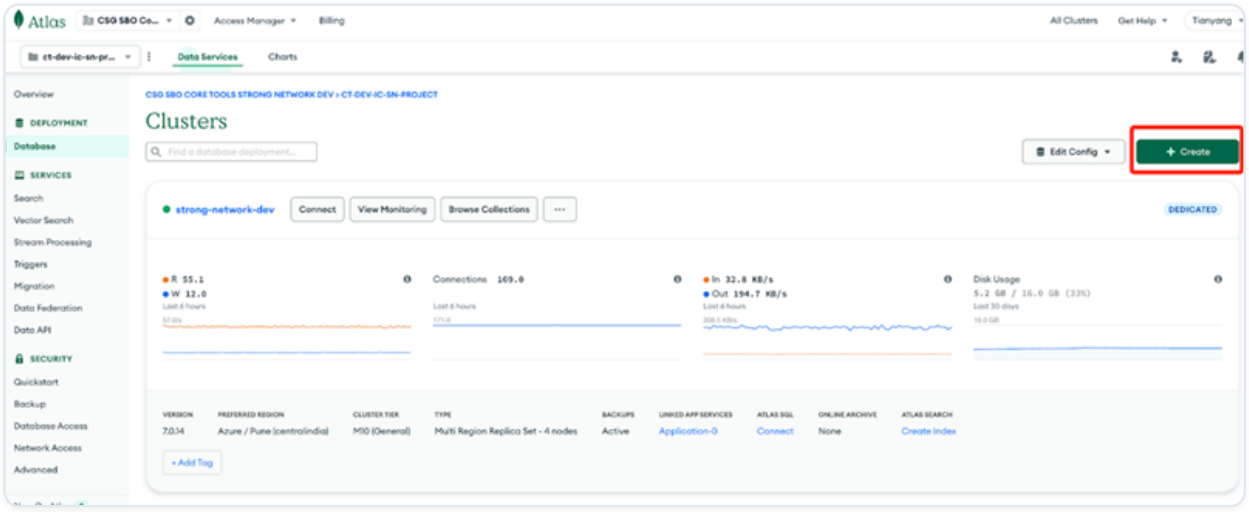
4. Adjunte el registro al clúster, para que AKS pueda extraer de ACR sin credenciales adicionales:

```
az aks update --name myAKSCluster --resource-group myResourceGroup --
attach-acr <acr-name>
```

Crear una base de datos MongoDB

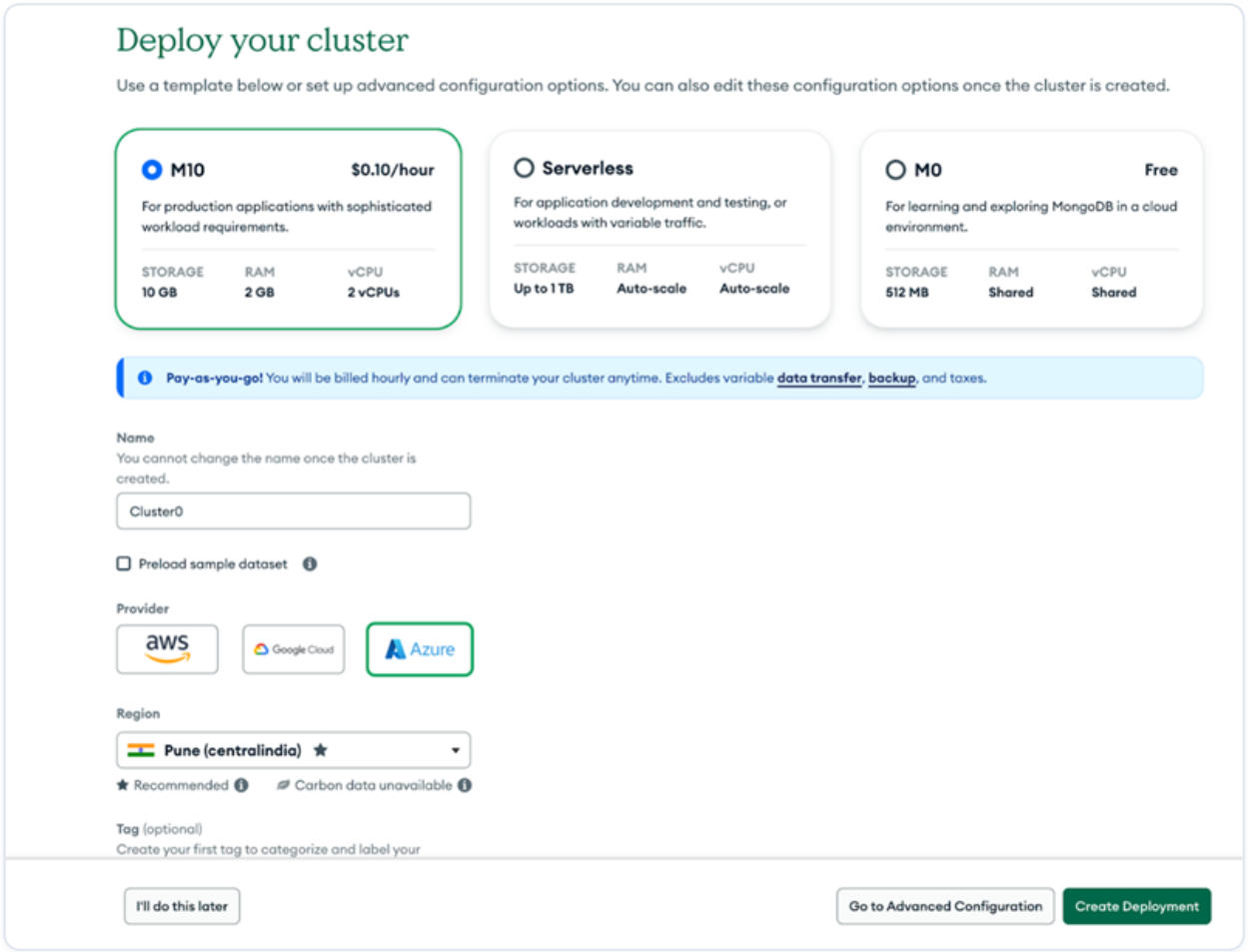
SecurSpaces almacena el estado de su plataforma en MongoDB. Para saber qué contiene y cuánto se espera que crezca, consulte La base de datos de SecurSpaces.

1. En MongoDB Atlas, abra la página de la base de datos y seleccione **Crear**.

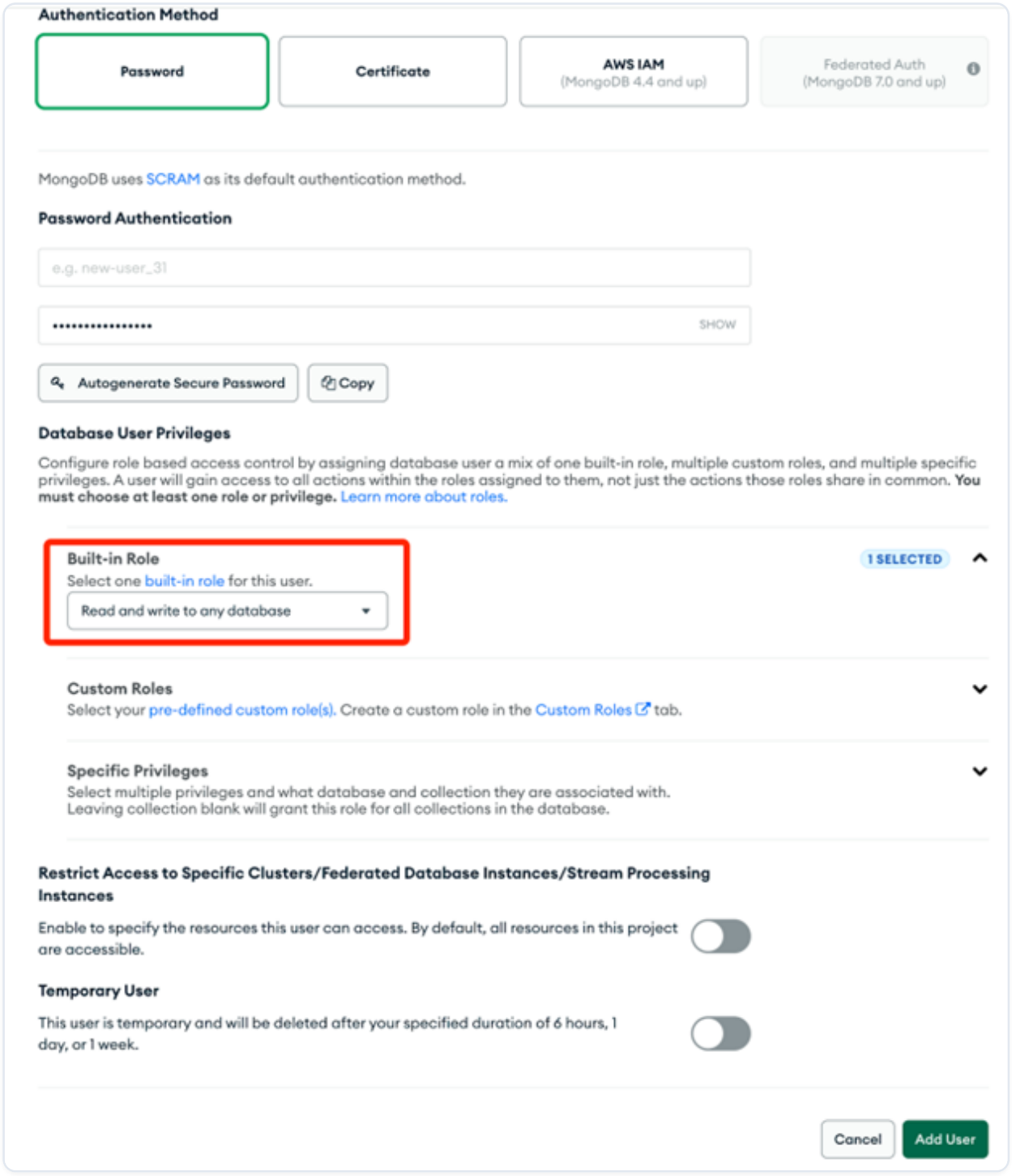


2. Configure la implementación y seleccione **Crear implementación**:

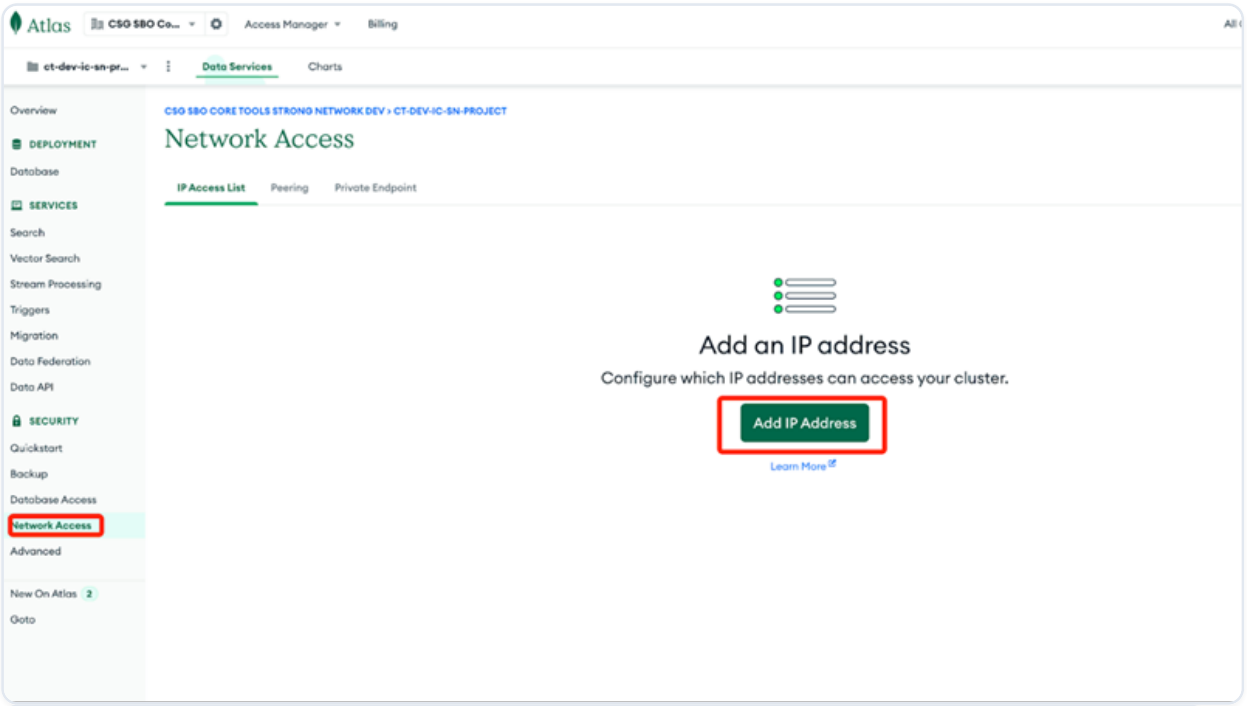
   - Seleccione **Azure** como proveedor de la nube.
   - Elija la misma región que el clúster de AKS.
   - Seleccione el nivel M10 con autoescalado.

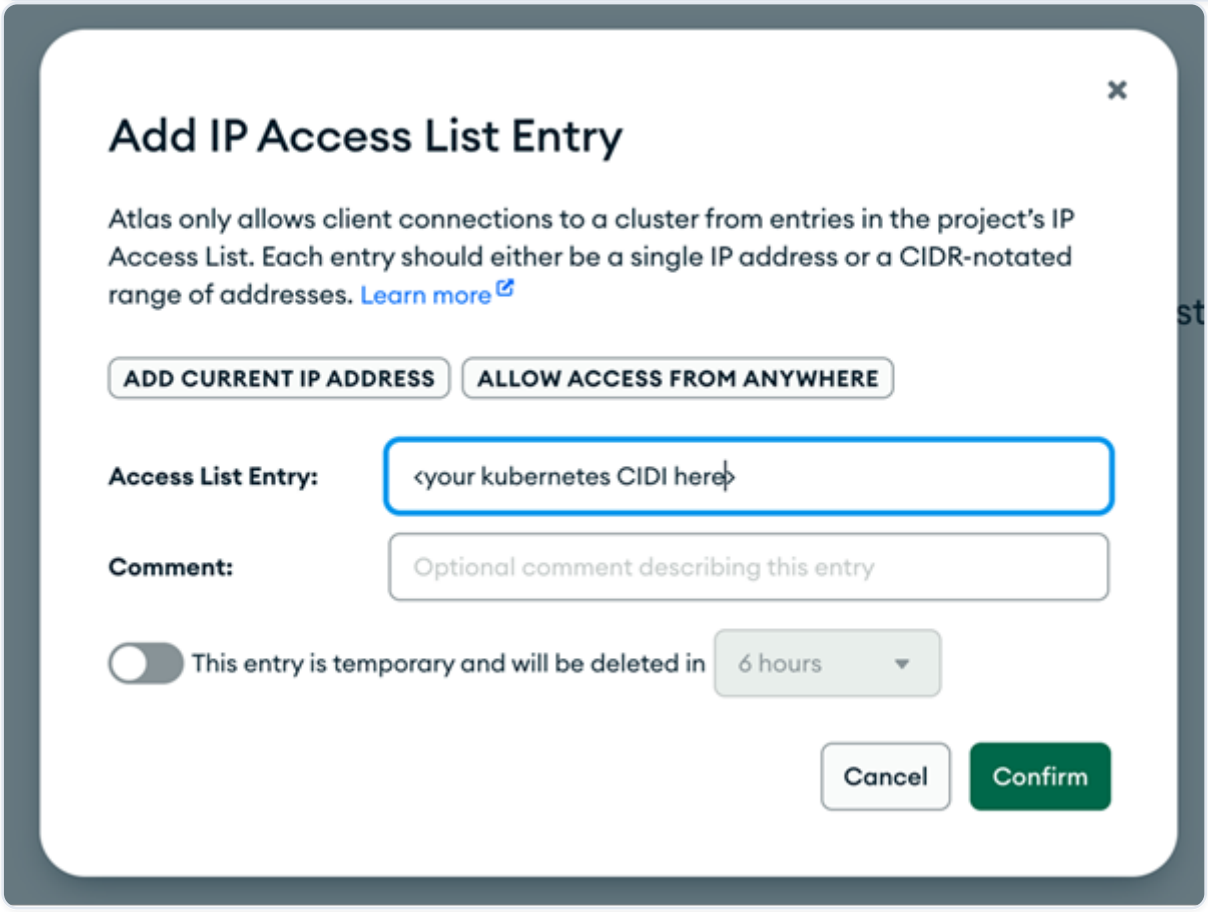


3. En la página de **Acceso a la base de datos**, añada un usuario.



4. En la página de **Acceso a la red**, permita que su clúster de AKS acceda a la base de datos. Añada los rangos de IP de salida del clúster, o utilice puntos de conexión privados, que es la opción más segura.





También puede ejecutar MongoDB dentro del clúster en lugar de utilizar un servicio alojado. Consulte Configurar una base de datos externa.

Siguiente paso

Su infraestructura de Azure está lista. Continúe con Instalar con la CLI de Strong Installer.

Durante esa instalación también configuró el controlador de entrada. Si no ha elegido uno, hágalo primero — consulte Ingress.

Información relacionada

- Despliegue de Kubernetes
- Requisitos del sistema
- Ingress
- Espacios de trabajo habilitados para GPU en AKS

Google GKE

Esta página prepara la infraestructura de Google Cloud que Citrix SecurSpaces™ necesita: un clúster de Kubernetes para ejecutarse, un registro de contenedores desde el que extraer imágenes y una base de datos MongoDB para almacenar el estado de la plataforma.

Cuando haya terminado, continúe con Instalar con la CLI de Strong Installer, que es la misma para todas las plataformas.

> **Importante:**

> **Utilice GKE Standard, no GKE Autopilot.** SecurSpaces no se instala en clústeres Autopilot; la instalación falla. Autopilot es el modo predeterminado al crear un clúster en la consola de Google Cloud, así que seleccione Standard explícitamente.

> **NetScaler CPX no funciona actualmente en GKE.** Este es un problema conocido, se está trabajando en una solución y aún no hay fecha. Póngase en contacto con Citrix para conocer el estado actual antes de planificar una implementación que dependa de él, y utilice una de estas opciones en su lugar:

> - NGINX — el sustituto más cercano, y la opción que esta documentación cubre por completo
> - Kubernetes Gateway API — compatible con el gráfico, con la configuración específica de GKE descrita a continuación

Requisitos previos

- Un proyecto de Google Cloud con permisos para crear recursos de GKE, Artifact Registry y redes.
- Una suscripción a MongoDB Atlas si utiliza Atlas, o un plan para implementar Percona MongoDB interno.
- Dos nombres de dominio: uno normal como `example.com`, y un subdominio comodín para soporte de proxy como `*.proxy.example.com`.
- Certificados TLS para esos dominios.
- Un proveedor de identidades, como Okta, si tiene la intención de usar SAML.
- Un controlador de entrada, o una decisión sobre cuál usar. SecurSpaces no puede servir tráfico sin uno, y solo NetScaler CPX es implementado por el gráfico. Consulte Entrada.

Para conocer el tamaño y las versiones compatibles, consulte Requisitos del sistema y Dimensionamiento.

Instale las siguientes herramientas:

- Google Cloud CLI
- kubectl

Crear un clúster de GKE

1. Inicie sesión y seleccione su proyecto:

```
gcloud auth login

gcloud config set project $PROJECT_ID
```

El tamaño de referencia para unos 500 desarrolladores es de dos nodos de servicio `n2-standard-8` (8 vCPU, 32 GiB) y un grupo de espacios de trabajo con autoescalado de `n2-standard-16` (16 vCPU, 64 GiB). Consulte Dimensionamiento.

1. Cree un clúster estándar con un grupo de nodos para los servicios de la plataforma:

```
gcloud container clusters create $CLUSTER_NAME \

  --project $PROJECT_ID \

  --region $REGION \
```

```
  --num-nodes 2 \

  --machine-type n2-standard-8 \

  --enable-ip-alias
```

`gcloud container clusters create` produce un clúster estándar. Autopilot requiere el comando separado `create-auto`, que no debe usarse.

2. Añada un grupo de nodos para espacios de trabajo, con autoescalado. Los espacios de trabajo son la parte elástica de la implementación, así que dé a este grupo espacio para crecer:

```
gcloud container node-pools create workspace-nodes \

  --cluster $CLUSTER_NAME \

  --project $PROJECT_ID \

  --region $REGION \

  --machine-type n2-standard-16 \

  --num-nodes 2 \

  --enable-autoscaling \

  --min-nodes 2 \

  --max-nodes 10
```

3. Obtenga las credenciales del clúster y verificar la conexión:

```
gcloud container clusters get-credentials $CLUSTER_NAME --project
$PROJECT_ID --region $REGION

kubectl get nodes
```

El instalador ejecuta este comando por usted durante una actualización, utilizando el nombre del clúster, el proyecto y la región en su archivo de configuración.

Crear un repositorio de Artifact Registry

SecurSpaces extrae sus imágenes de servicio y sus imágenes de espacio de trabajo de un registro que usted controla. El instalador las envía allí en la siguiente etapa.

1. Habilite la API y cree un repositorio para las imágenes de la plataforma:

```
gcloud services enable artifactregistry.googleapis.com --project
$PROJECT_ID



gcloud artifacts repositories create strong-network \

  --repository-format=docker \

  --location=$REGION \

  --project=$PROJECT_ID
```

2. Cree un repositorio para las imágenes de espacio de trabajo:

```
gcloud artifacts repositories create ws-images \

  --repository-format=docker \

  --location=$REGION \

  --project=$PROJECT_ID
```

3. Autenticar Docker en el registro:

```
gcloud auth configure-docker $REGION-docker.pkg.dev
```

El instalador reconoce una URL de Artifact Registry o Container Registry —cualquier cosa que contenga `docker.pkg.dev` o `gcr.io` — y se autentica en ella con la CLI de Google Cloud. Puede iniciar sesión como una cuenta de usuario o proporcionar una clave de cuenta de servicio con `--service-account-file-path`, que es la opción habitual para una pipeline. Consulte Referencia de la CLI de SDS.

Crear una base de datos MongoDB

SecurSpaces almacena el estado de su plataforma en MongoDB. Para saber qué contiene y cuánto se espera que crezca, consulte La base de datos de SecurSpaces.

MongoDB Atlas

1. En MongoDB Atlas, abra la página de la base de datos y seleccione **Crear**.
2. Configure la implementación y seleccione **Crear implementación**:
   - Seleccione **Google Cloud** como proveedor de la nube.
   - Elija la misma región que el clúster de GKE.
   - Seleccione el nivel M10 con autoescalado.
3. Cree un usuario de base de datos y anote el nombre de usuario y la contraseña. El instalador los solicitará.
4. Permita el acceso desde las direcciones de salida de su clúster en **Acceso a la red**.
5. Copie la cadena de conexión de **Conectar > Controladores**.

Percona MongoDB interno con copias de seguridad de GCS sin clave

Para ejecutar MongoDB dentro de GKE, seleccione Percona durante la instalación (`platform.deployPerconaMongoDB` sin establecer o `true`). El gráfico actualizado implementa Percona Operator 1.23.0, MongoDB 7.0.37-20 y PBM 2.15.0.

Para copias de seguridad sin clave en Google Cloud Storage:

- Habilite la federación de identidades de carga de trabajo para GKE y el servidor de metadatos de GKE en los grupos de nodos que ejecutan los pods de la base de datos y del operador.
- Cree un bucket de copia de seguridad y conceda acceso directamente a las cuentas de servicio de Kubernetes de la base de datos y del operador. El operador también necesita acceso para la limpieza de retención.
- Configure `perconaServerMongoDB.serviceAccount` y `perconaServerMongoDB.backup` en los valores de Helm. Utilice el almacenamiento nativo `gcs` sin `credentialsSecret`; no se necesita ninguna clave JSON de cuenta de servicio ni clave HMAC.

Las copias de seguridad están deshabilitadas por defecto. Para comandos de configuración, programaciones, PITR, retención y verificación, consulte Identidad de carga de trabajo de GCS.

Para una implementación existente de SDS 2026.9, primero ejecute el script de actualización de Percona proporcionado por el instalador para alcanzar la versión 1.22.0 y aplicar los CRD 1.23, luego ejecute Helm para completar el paso a la versión 1.23.0. Consulte Actualización.

Si utiliza la API de Gateway de Kubernetes

GKE necesita una configuración adicional cuando SecurSpaces utiliza recursos de la API de Gateway en lugar de recursos de Ingress. Establezca ambas en su archivo de configuración:

```
platform:
  useGatewayAPI: true
  gatewayAPI:
    gatewayClassName: <your-gateway-class>
    enableHealthCheckPolicy: true
```

`enableHealthCheckPolicy` crea los recursos `networking.gke.io/v1` HealthCheckPolicy que GKE requiere para verificar el estado de los backends. Se aplica solo a GKE.

La mayoría de las implementaciones utilizan un controlador de entrada en su lugar. Consulte Ingress.

Siguiente paso

Su infraestructura de Google Cloud está lista. Continúe con Instalar con la CLI de Strong Installer.

Durante esa instalación, también configurará el controlador de entrada. Si no ha elegido uno, hágalo primero — consulte Ingress.

Información relacionada

- Plataformas de Kubernetes
- Requisitos del sistema
- Dimensionamiento
- Ingress

Deploy SecurSpaces on Red Hat OpenShift

La plataforma Citrix SecurSpaces™ proporciona un entorno de desarrollo en la nube seguro y productivo que se puede implementar en nubes públicas, privadas y servidores autoalojados. También funciona en modos completamente aislados (air-gapped), como en entornos de alta seguridad. El propósito principal de la plataforma SecurSpaces es proporcionar entornos de desarrollo en la nube (CDE) seguros que aumenten la productividad del desarrollador al tiempo que garantizan la seguridad a nivel empresarial. Permite a las organizaciones optimizar el aprovisionamiento y la gestión de entornos de codificación, mejorando la eficiencia y la colaboración entre equipos internos y externos. Al centralizar los recursos de desarrollo e integrar funciones de seguridad automatizadas, la plataforma reduce el riesgo de fugas de datos y robo de propiedad intelectual, lo que permite un trabajo remoto seguro y respalda las prácticas de DevSecOps. Específicamente, los escenarios de uso típicos abarcan la eficiencia de TI, la productividad del desarrollador y la gobernanza del proceso de desarrollo. Esta guía de implementación proporciona los pasos para implementar SecurSpaces en un clúster de Red Hat OpenShift existente. Los CDE se pueden acceder a través de entornos de desarrollo integrados (IDE) en la nube o locales, ofreciendo un entorno seguro y aislado para los desarrolladores.

Esta guía cubre la preparación de un clúster de OpenShift y la instalación de la plataforma SecurSpaces en él. A diferencia de las páginas de EKS y AKS, es autónoma, porque el modelo de rutas y contexto de seguridad de OpenShift cambia varios de los pasos de instalación.

Una vez que la plataforma esté en funcionamiento, consulte Kubernetes para saber qué configurar a continuación.

Requisitos previos

La implementación de la plataforma CDE de SecurSpaces tiene los siguientes requisitos previos:

- Registro de contenedores al que tenga permisos de inserción (push)
- Un clúster de OpenShift en funcionamiento
- Herramientas básicas para trabajar con ese clúster de OpenShift: **oc** y **kubectl** Ya debería estar autenticado tanto en **oc** como en **kubectl** con su clúster de OpenShift.

Pasos de implementación

Obtener una licencia de la plataforma SecurSpaces

Necesita una licencia válida para usar la plataforma SecurSpaces. Póngase en contacto con su ATS o arquitecto de soluciones para solicitar que se le emita una. Para emitir una licencia, solo necesitamos saber qué URL se utilizará para acceder a la plataforma SecurSpaces. En el caso de

OpenShift, primero necesitamos averiguar el dominio del clúster, lo que podemos hacer fácilmente de dos maneras:

1. Desde la URL de la consola web: El dominio del clúster forma parte de la dirección de la consola web de OpenShift. Si accede a la consola en `https://console-OpenShift-console.apps.cluster.example.com`, entonces su dominio de clúster es `apps.cluster.example.com`
2. Usando la CLI de OpenShift (oc):

   ```
   oc get ingresses.config/cluster -o jsonpath='{.spec.domain}'
   ```

   - Obtendrá una salida como: `apps.sm9kda46je6e9a9c7b.swedencentral.aroapp.io`
   - Una vez que tenga el dominio del clúster, el dominio final de la plataforma SecurSpaces tendrá el formato: `sn.<cluster-domain>`
   - En nuestro caso, se verá así: `sn.apps.<CLUSTER_ID>.<REGION>.aroapp.io`

Ahora que tenemos el dominio, lo registraremos con el servidor de licencias de SecurSpaces.

Compruebe la política de comodines de su clúster de OpenShift

Para poder crear y usar espacios de trabajo en la plataforma SecurSpaces, que tienen rutas dinámicas, debe asegurarse de que la política de comodines del enrutamiento de su clúster de OpenShift esté configurada como **WildcardsAllowed**.

Para ello, puede seguir estos pasos:

- Averigüe el nombre de su controlador de entrada ejecutando:

```
oc get ingresscontroller -n openshift-ingress-operator -o
jsonpath='{.items[*].metadata.name}'
```

- Si realizó una instalación predeterminada de un clúster de OpenShift y no ha cambiado ninguna de las configuraciones, lo más probable es que el nombre sea default.
- Compruebe si su controlador de entrada ya tiene una política WildcardsAllowed configurada, utilizando el nombre del controlador obtenido en el paso anterior. En nuestro caso, es default, por lo que el comando se ve así:

```
oc get ingresscontroller default -n openshift-ingress-operator -o
jsonpath='{.spec.routeAdmission.wildcardPolicy}'
```

- Si la salida es WildcardsAllowed, entonces todo está configurado y puede pasar al siguiente paso de la guía.
- Si la salida está vacía, significa que necesitamos configurar la política manualmente. Esto se puede hacer editando la configuración de ese controlador de entrada en particular (llamado default) ejecutando:

```
oc patch ingresscontroller default -n openshift-ingress-operator --
type=merge -p '{"spec":{"routeAdmission":
{"wildcardPolicy":"WildcardsAllowed"}}}'
```

- Ahora puede verificar que el comando anterior fue exitoso ejecutando y obteniendo **WildcardsAllowed** como respuesta:

```
oc get ingresscontroller default -n openshift-ingress-operator -o
jsonpath='{.spec.routeAdmission.wildcardPolicy}'
```

- Si desea ver la configuración completa del controlador de entrada, puede ejecutar:

```
oc get ingresscontroller default -n openshift-ingress-operator -o yaml
```

Puede encontrar más información sobre el tema de los controladores de entrada y las políticas de comodines en particular en: https://docs.redhat.com/en/documentation/OpenShift_container_platform/4.18/html/operator_apis/ingresscontroller-operator-OpenShift-io-v1#spec-routeadmission

Cree un espacio de nombres de Kubernetes para su implementación

Seleccione el nombre del espacio de nombres que desea utilizar para la implementación de SecurSpaces. Se recomienda no reutilizar espacios de nombres existentes para implementar nuestra plataforma. Para esta guía, usaremos el nombre SecurSpaces.

- Primero, debe comprobar si ese espacio de nombres ya existe ejecutando:

```
kubectl get namespaces | grep strong-network
```

- Si no existe, puede crearlo ejecutando:

```
kubectl create namespace strong-network
```

Ejecutar el instalador de SecurSpaces

Puede iniciar el proceso de instalación ejecutando el siguiente comando desde la consola de su dispositivo:

```
docker run -it --rm -v ${PWD}:/strong-network/shared strongnetwork/
strong_installer:2026.9.4
```

Una vez ejecutado esto y descargada y ejecutada la imagen del instalador, puede ejecutar el instalador. El instalador creará un archivo de configuración que deberá utilizarse para actualizar el producto en el futuro. También descargará el gráfico de Helm en el directorio del host compartido y enviará las imágenes de SecurSpaces a su registro de contenedores.

Dado que proporcionamos un gran número de imágenes de espacio de trabajo precompiladas por defecto, que ocupan una cantidad significativa de espacio, puede reducir el número de imágenes que extraemos o enviamos editando la lista de imágenes de espacio de trabajo que extraeremos o enviaremos, o no descargándolas en absoluto. Esto también podría ser útil si usted (el cliente) planea usar sus propias imágenes de espacio de trabajo, por lo que no necesitará las precompiladas de SecurSpaces.

En caso de que solo necesite imágenes de espacio de trabajo específicas pero no quiera descargar el resto, puede editar el archivo **workspace_images.txt** y eliminar las que no necesite.

Entonces puede ejecutar:

```
sds-cli install
```

Tendrá que pasar por un asistente que le ayudará a crear el archivo de configuración YAML.

El ejemplo siguiente se capturó en una versión anterior. El instalador actual hace menos preguntas — ya no solicita el dominio del espacio de trabajo, la clave de cifrado de la base de datos, el secreto JWT, las afinidades de nodo o la autenticación de dos factores — y nombra el gráfico y el archivo de configuración según la versión que instale.

```
Enter the main domain of the platform (e.g, strong-network.example.com):
`sn.apps.<CLUSTER_ID>.<REGION>.aroapp.io`

The default domain used to access workspaces is:
proxy.sn.apps.<CLUSTER_ID>.<REGION>.aroapp.io`

Do you want to change it? (y/n): n
```

```
Set the email of the platform admin: admin:admin@example.com

Set password for admin (leave empty to autogenerate):

Define the base64 database encryption key (leave empty to autogenerate):

Define the JWT secret (leave empty to autogenerate):

Do you want to enable node affinities for workspaces and strong network
services? (y/n): n

Use two-factor authentication for users? (y/n): n

Installing version 2025.5.0...
```

En caso de que reciba un error en la terminal como el siguiente: `Failed to fetch access token with error: permission denied, try using a service account...`

Esto significa que su dominio no está registrado correctamente en el servidor de licencias de SecurSpaces y, por lo tanto, no podemos generar automáticamente el token de acceso para nuestro registro de contenedores.

Si no encontró ningún problema durante el asistente, todo su asistente se verá como la salida siguiente.

```
root@0f7ca7f89e78:/strong-network# sds-cli install

Enter the main domain of the platform (e.g, strong-network.example.com):
sn.apps.<CLUSTER_ID>.<REGION>.aroapp.io

The default domain used to access workspaces is:
proxy.sn.apps.<CLUSTER_ID>.<REGION>.aroapp.io

Do you want to change it? (y/n): n

Set the email of the platform admin: admin:admin@example.com

Set password for admin (leave empty to autogenerate):

Define the base64 database encryption key (leave empty to autogenerate):
```

```
Define the JWT secret (leave empty to autogenerate):

Do you want to enable node affinities for workspaces and Citrix Secure
Developer Spaces services? (y/n): n

Use two-factor authentication for users? (y/n): n

Installing version 2026.4.5...

⣿ Authenticating... Done.

⣿ Finding best source registry... Selected EU region.

Pulling helm chart version 2026.4.5..

File ninjahchart-2026.4.5.tgz downloaded to /strong-network/shared/
ninjahchart-2026.4.5.tgz

Destination Registry URL:<YOUR_REGISTRY>.azurecr.io

Detected Azure Registry Type..

Select Type For Authentication:

        [1] User Account

        [2] Service Principal

Please Enter Your Numeric Choice: 2

Enter service principal ID: <YOUR_SERVICE_PRINCIPAL_ID>

Enter service principal password: Authentication successful.

src: europe-docker.pkg.dev/strong-network-release/images/frontend:2026.4.5

dst: http://<YOUR_REGISTRY>.azurecr.io/frontend:2026.4.5

Getting image source signatures

Copying blob fb6ab0edbcbd done   |

Copying blob ab9385d5595c done   |
```

```
Copying blob 0c1c1add5fb1 done   |

Copying blob 4f4fb700ef54 skipped: already exists

Copying config 3564c26c52 done   |

Writing manifest to image destination

⣿ Finishing up... Done.

Run your deployment like this:

    helm upgrade --install \\

            --namespace default \\

            --create-namespace \\

            -f "./config_2026.4.4.yaml" \\

            release ./ninjahchart-2026.4.5.tgz

root@0f7ca7f89e78:/strong-network#`
```

Añadir secretos del registro de Docker a Kubernetes

Las imágenes de Docker para la propia plataforma SecurSpaces y, posteriormente, para las imágenes de espacio de trabajo deben alojarse en una ubicación adecuada. Por eso necesita proporcionar su registro de contenedores (o Artifactory), porque el instalador de SecurSpaces extraerá las imágenes del Artifactory GCP privado de SecurSpaces y las enviará a su registro. Es probable que el registro de contenedores de SecurSpaces no sea público, y por eso necesita autenticarse con él. Las credenciales para esta autenticación deben estar presentes durante la instalación de la plataforma SecurSpaces para que las imágenes puedan extraerse para cada uno de los pods de servicio de SecurSpaces. Una vez que tenga las credenciales listas, puede añadirlas ejecutando:

```
kubectl create secret docker-registry acr-secret   --namespace=strong-
network   --docker-server=<YOUR_REGISTRY>.azurecr.io    --docker-
username=<YOUR_SERVICE_PRINCIPAL_ID>-token   --docker-
password=<YOUR_REGISTRY_PASSWORD>
```

Esto crea un nuevo secreto de registro de Docker llamado **'acr-secret'** en el espacio de nombres **'strong-network'**.

Puede verificar que el secreto se ha añadido correctamente ejecutando:

```
`kubectl get secrets | grep acr-secret`
```

Ahora debe editar manualmente la configuración YAML que obtuvo como resultado de ejecutar el instalador de Strong y añadir la siguiente línea en la sección de la plataforma:
`imagePullSecrets: acr-secret`

Establecer restricciones de contexto de seguridad adecuadas

Dado que el modelo de seguridad de OpenShift difiere del modelo de seguridad estándar de Kubernetes, debe aplicar políticas adicionales; de lo contrario, los servicios o espacios de trabajo de SecurSpaces no se iniciarán correctamente. Debe establecer políticas tanto para las implementaciones de servicios como para los espacios de trabajo que se crearán en la plataforma.

ESTABLECER POLÍTICAS PARA LAS CUENTAS DE SERVICIO DE LOS SERVICIOS DE LA PLATAFORMA

Ejecute las siguientes instrucciones:

```
oc adm policy -n strong-network add-scc-to-user privileged -z release-
central-service

oc adm policy -n strong-network add-scc-to-user privileged -z release-
coordinator

oc adm policy -n strong-network add-scc-to-user privileged -z release-
proxy

oc adm policy -n strong-network add-scc-to-user privileged -z release-
workspace-api

oc adm policy -n strong-network add-scc-to-user privileged -z release-
mongodb

oc adm policy -n strong-network add-scc-to-user privileged -z release-
frontend
```

```
oc adm policy -n strong-network add-scc-to-user privileged -z release-
cron-service-account
```

Esto añadirá los permisos elevados a todas las cuentas de servicio de los servicios de la plataforma que utiliza SecurSpaces.

El indicador `-z` indica que lo que sigue es un nombre de cuenta de servicio, por ejemplo, release-proxy.

Crear una nueva cuenta de servicio, su política y asignarla

Cree un archivo llamado **workspaces-policy.yaml**:

```
apiVersion: security.openshift.io/v1

kind: SecurityContextConstraints

metadata:

  annotations:

    kubernetes.io/description: anyuid provides all features of the
restricted SCC

      but allows users to run with any UID and any GID.

  creationTimestamp: "2024-08-07T12:25:28Z"

  generation: 1

  name: strongnetwork-scc

  resourceVersion: "998061"

  uid:

allowHostDirVolumePlugin: false

allowHostIPC: false

allowHostNetwork: false
```

```
allowHostPID: false

allowHostPorts: false

allowPrivilegeEscalation: true

allowPrivilegedContainer: true

allowedCapabilities:

- NET_ADMIN

- NET_RAW

defaultAddCapabilities: null

fsGroup:

  type: RunAsAny

groups:

- system:cluster-admins

priority: 10

readOnlyRootFilesystem: false

requiredDropCapabilities:

- MKNOD

runAsUser:

  type: RunAsAny

seLinuxContext:

  type: MustRunAs

supplementalGroups:

  type: RunAsAny
```

```
users: []

volumes:

- configMap

- downwardAPI

- emptyDir

- persistentVolumeClaim

- projected

- secret
```

Aplíquelo ejecutando:

```
kubectl apply -f workspaces-policy.yaml
```

Ahora debe comprobar si ya existe una cuenta de servicio llamada **statefulset-sa**:

```
oc get serviceaccounts | grep statefulset-sa
```

La cuenta de servicio ya existe

Si la cuenta de servicio ya existe, puede comprobar si ya tiene asignadas las **strongnetwork-scc SecurityContextConstraints**. Puede hacerlo ejecutando:

```
`oc get rolebindings,clusterrolebindings --all-namespaces -o wide | grep
statefulset-sa`
```

Puede esperar obtener una salida como la siguiente, lo que significaría que está utilizando un **strongnetwork-scc**: Si este es el caso, no necesita realizar ningún paso adicional con respecto a la cuenta de servicio y sus políticas.

La cuenta de servicio no existe

Si la cuenta de servicio no existe, debe crear una y asignarle la política **strongnetwork-scc**:

```
oc create serviceaccount statefulset-sa -n strong-network

oc adm policy add-scc-to-user strongnetwork-scc -z statefulset-sa
```

Edición de la configuración YAML

Finalmente, debe editar manualmente la configuración YAML que obtuvo como resultado de ejecutar el instalador de Strong. Debe añadir las siguientes líneas en la sección platform:

```
useOpenShift: true
```

Debe añadir las siguientes líneas en la sección region:

```
clusterConfig:

        privilegedWorkspaces: true

        customServiceAccount: statefulset-sa
```

YAML final

Después de todas las ediciones realizadas en los pasos anteriores, la configuración YAML debería verse así:

```
mongodb:

    auth:

        replicaSetKey: <MONGODB_REPLICA_SET_KEY>

        password: <MONGODB_PASSWORD>

        rootPassword: <MONGODB_ROOT_PASSWORD>

platform:

    imageTag: 2026.9.4

    dockerRegistry: <YOUR_REGISTRY>.azurecr.io/

    workspaceRegistry: <YOUR_REGISTRY>.azurecr.io/ws-images/
```

```
    publicRegistryLatestTag: 2.3.9

    sidecarTag: 2026.9.4

    hostName: sn.apps.<CLUSTER_ID>.<REGION>.aroapp.io

    centralProxyHostname: proxy.sn.apps.<CLUSTER_ID>.<REGION>.aroapp.io

    userAdminEmail: admin@example.com

    userAdminPassword: <ADMIN_PASSWORD>

    secretKeyReposB64: <BASE64_ENCRYPTION_KEY>

    jwtSecret: <JWT_SECRET>

    sslCertificateSecret: ""

    sslCertificateSecretProxy: ""

    twoFaDisabled: true

    useOpenShift: true

    imagePullSecrets: acr-secret

region:

    clusterConfig:

        privilegedWorkspaces: true

        customServiceAccount: statefulset-sa
```

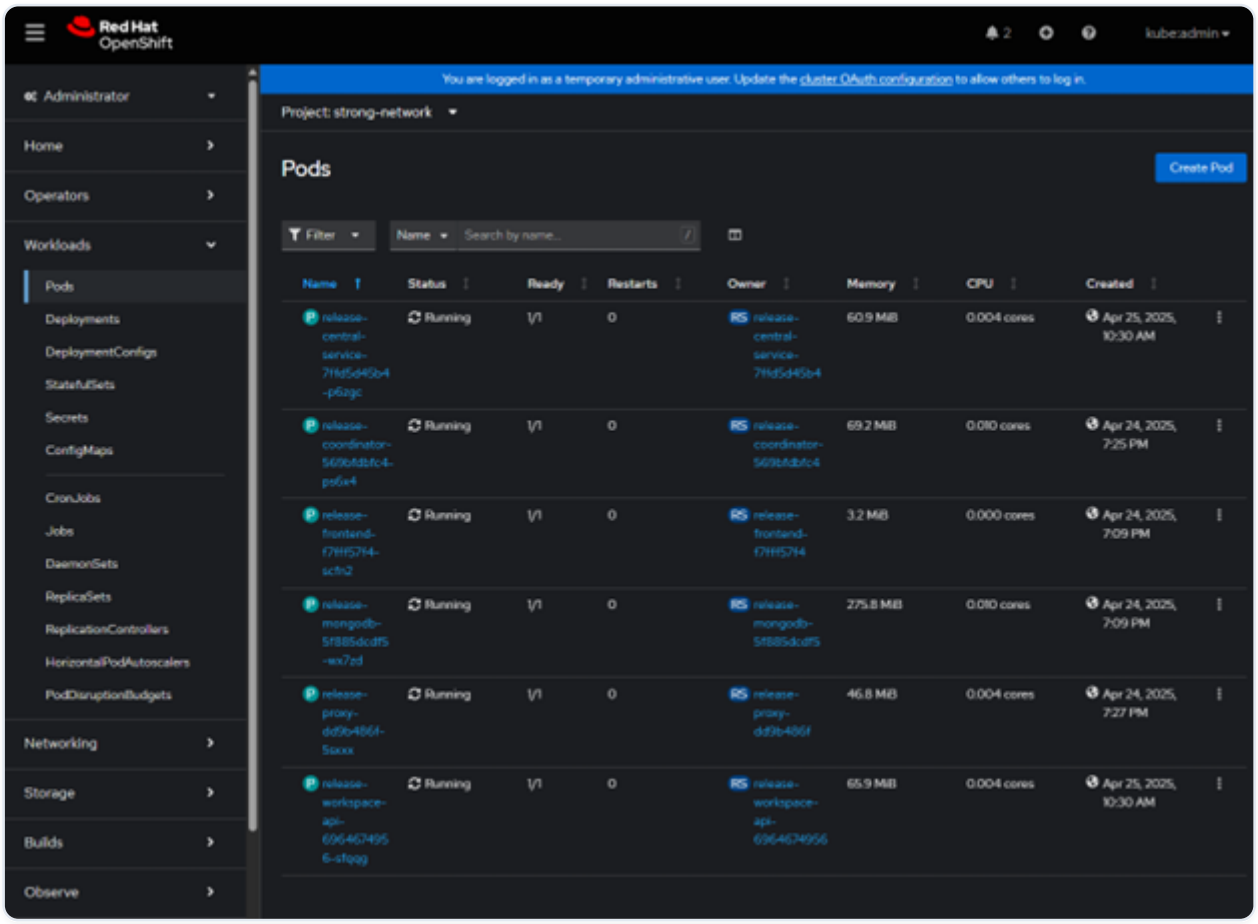
Despliegue

Ahora lo que queda es ejecutar el helm upgrade y desplegar la aplicación:

```
helm upgrade --install \\

            --namespace strong-network \\
```

```
        -f "./config_2026.9.4.yaml" \\

        release ./ninjahchart-2026.9.4.tgz
```

La terminal se congelará durante unos segundos mientras el despliegue está en curso. Ahora puede ir a la consola de OpenShift y a **Workloads -> Pods** y verificar que todos los pods se están ejecutando correctamente:



Si hay un problema con un pod en particular, haga clic en ese pod y revise sus Logs/Events. Cuando todo esté correcto con todos los pods, puede proceder a iniciar sesión en la plataforma en la URL definida por el valor **hostName** en el YAML, utilizando **userAdminEmail** y **userAdminPassword** del YAML.

Después de crear la organización y el proyecto iniciales, puede intentar crear un espacio de trabajo y ver si se despliega correctamente. Si el espacio de trabajo no se despliega correctamente, examine los registros del Pod/StatefulSet relevante, como se explicó anteriormente.

Nutanix Kubernetes Platform

Citrix SecurSpaces™ se ejecuta en la plataforma Nutanix Kubernetes (NKP). Esta página cubre lo específico de NKP: los requisitos previos del clúster, las etiquetas de nodo, el certificado y la configuración de entrada que necesita el gráfico.

Todo lo demás es la instalación estándar. Cuando haya terminado aquí, continúe con Instalar con la CLI de Strong Installer.

Nutanix publica una guía completa de principio a fin como nota técnica de soluciones, que es útil para el lado NKP de la implementación: Citrix Secure Developer Spaces en Nutanix Kubernetes Platform.

> **Importante:**

> La nota técnica de Nutanix se escribió para SecurSpaces `2025.10.13` y no se ha revisado desde entonces. Su etiqueta de imagen del instalador, el nombre del archivo del gráfico y el comando CLI están desactualizados; utiliza `strong-cli`, que ahora es `sds-cli`. Úsela para los pasos específicos de NKP y siga la documentación de SecurSpaces para la instalación en sí.

Requisitos previos

- NKP 2.17 o posterior, implementado como un clúster autogestionado o de carga de trabajo.
- Una dirección IP libre en el rango del balanceador de carga del servicio de Kubernetes, para el balanceador de carga de SecurSpaces.
- Un kubeconfig con acceso privilegiado al clúster.
- Tres nombres de dominio:

PROPÓSITO	EJEMPLO
Principal	`sds.example.com`
Proxy	`proxy.sds.example.com`
Subdominio comodín	`*.proxy.sds.example.com`

- Un certificado TLS cuyos Nombres Alternativos del Sujeto cubran los tres dominios.

- Una licencia de plataforma de SecurSpaces.

Para las versiones de Kubernetes compatibles y la planificación de capacidad, consulte Requisitos del sistema y Dimensionamiento.

Crear el espacio de nombres

```
kubectl create namespace strong-network
```

Etiquetar los nodos

SecurSpaces separa los nodos de servicio de los nodos de espacio de trabajo. Etiquételos para que el gráfico pueda programar cada tipo de pod en el grupo correcto:

```
kubectl label nodes <service-node-name> strong.network/type=service

kubectl label nodes <workspace-node-name> strong.network/type=workspace
```

Para saber cuántos nodos de cada tipo aprovisionar, consulte Dimensionamiento.

Instalar el certificado

Almacene el certificado y su clave privada como un secreto TLS en el espacio de nombres:

```
kubectl create secret tls sds-example-com-cert \

  --key=/path/to/private_key.pem \

  --cert=/path/to/cert.pem \

  -n strong-network
```

Si utiliza cert-manager, solicite el certificado en su lugar. Este ejemplo emite un certificado autofirmado, que es adecuado para pruebas pero no para producción:

```
apiVersion: cert-manager.io/v1

kind: Certificate

metadata:

  name: sds-example-com-cert
```

```
  namespace: strong-network
spec:
  secretName: sds-example-com-cert
  issuerRef:
    name: selfsigned-issuer
    kind: ClusterIssuer
  dnsNames:
    - sds.example.com
    - proxy.sds.example.com
    - "*.proxy.sds.example.com"
```

Configurar el gráfico para NKP

Ejecute el instalador como se describe en Instalar con la CLI de Strong Installer. Seleccione **Percona MongoDB** cuando el instalador pregunte por el tipo de base de datos, a menos que esté utilizando una base de datos externa.

Luego, añada los valores específicos de NKP al archivo de configuración generado. NKP incluye NetScaler CPX como su controlador de entrada, por lo que el gráfico necesita que se le indique que emita anotaciones de entrada de NetScaler:

```
platform:
  useNetscalerController: true
  ingressClass: netscaler-cpx-ingress
  sslCertificateSecret: sds-example-com-cert
```

`ingressClass` debe coincidir con la clase que su controlador NetScaler CPX realmente observa. El valor predeterminado del gráfico es `netscaler-cpx-ingress`; confirme el suyo con `kubectl get ingressclass` y establezca ambos lados con el mismo valor.

Nota:

Si su versión del gráfico requiere que la afinidad de nodo se active explícitamente, también establezca `platform.enableNodeAffinity: true`. Las etiquetas de nodo anteriores no tienen efecto a menos que la afinidad esté habilitada. La nota técnica de Nutanix marca esto como requerido para `2025.10.13`.

Implementar

```
helm upgrade --install \

    --namespace strong-network \

    --create-namespace \

    -f ./config_<version>.yaml \

    release ./ninjachart-<version>.tgz
```

Compruebe que la plataforma se haya iniciado:

```
kubectl get pods -n strong-network

kubectl get ingress -n strong-network
```

Luego abra `https://sds.example.com/login` e inicie sesión con la cuenta de administrador que configuró durante la instalación.

Información relacionada

- Plataformas de Kubernetes
- Instalar con la CLI de Strong Installer
- Requisitos del sistema
- Dimensionamiento

Install with the Strong Installer CLI

La CLI de Strong Installer (`sds-cli`) le ayuda a instalar, actualizar y gestionar las implementaciones de Citrix SecurSpaces™. Ejecuta la CLI desde el contenedor de Strong Installer.

Información general

Utilice este artículo para:

- Instalar SecurSpaces por primera vez.
- Actualizar una implementación existente.
- Enviar imágenes de contenedor a su registro.

Requisitos previos

Antes de empezar, asegúrese de tener:

- Docker instalado y en ejecución en su máquina local.
- Credenciales para su registro de contenedores.
- Acceso a la red a Docker Hub y a su registro de destino.
- Suficiente espacio en disco para descargar y enviar imágenes de contenedor.

Ejecutar Strong Installer

Strong Installer está disponible como un contenedor de Docker en Docker Hub. Ejecute este comando para iniciarlo:

```
docker run -it --rm -v ${PWD}:/strong-network/shared \

    strongnetwork/strong_installer:2026.9.4
```

Nota:

`${PWD}` monta su directorio actual en `/strong-network/shared` dentro del contenedor. Strong Installer guarda los archivos de configuración y los gráficos de Helm en esta ubicación.

Instalar SecurSpaces

Antes de empezar

Asegúrese de tener:

- La URL del registro de contenedores de destino.
- Credenciales de autenticación para su registro.
- Las versiones de servicio y espacio de trabajo que desea instalar.

Pasos de instalación

1. Inicie el contenedor de Strong Installer:

   ```
   docker run -it --rm -v ${PWD}:/strong-network/shared \

       strongnetwork/strong_installer:2026.9.4
   ```

2. Ejecute el comando de instalación:

   ```
   sds-cli install
   ```

   Opcional: Especifique las versiones de servicio y espacio de trabajo con indicadores:

   ```
   sds-cli install -v 2026.9.4 -w 2.3.9
   ```

3. Introduzca los valores de configuración iniciales cuando se le solicite.
4. Siga las indicaciones para autenticarse en su proveedor de nube o registro.
5. Introduzca la URL completa del registro de destino.
6. Espere mientras la CLI crea el archivo de configuración y envía las imágenes a su registro.

Autenticación del registro

Strong Installer detecta el tipo de registro a partir de la URL y solicita las credenciales adecuadas. Para el tipo de credencial que espera cada registro, y para las marcas que las proporcionan de forma no interactiva, consulte Referencia de la CLI de SDS.

> **Importante:**

> Después de autenticarse, el archivo del gráfico de Helm se descarga en su directorio compartido. Proteja este archivo inmediatamente, ya que contiene la configuración de su implementación.

Implementar en el clúster

La instalación envía las imágenes y escribe el archivo de configuración. La implementación aplica esa configuración a su clúster de Kubernetes. Prepare el clúster primero; consulte Kubernetes para su plataforma.

Antes de empezar

Asegúrese de tener:

- Un clúster de Kubernetes preparado, con `kubectl` apuntando a él.
- Un controlador de entrada. El `ingressClass` predeterminado del gráfico es `nginx`, pero se recomienda NetScaler CPX porque el gráfico lo implementa y configura por usted. Consulte Entrada.
- Un certificado TLS y una clave para su dominio de host.
- El gráfico de Helm y el archivo de configuración producidos en el paso de instalación.

Instalar un controlador de entrada

SecurSpaces no comenzará a servir tráfico sin uno. A menos que esté utilizando NetScaler CPX, que el gráfico implementa por usted, instale y configure el controlador antes de aplicar el gráfico.

- NGINX — instale con Helm y luego aplique los valores de ConfigMap recomendados
- NetScaler CPX — desplegado por el gráfico, sin instalación separada
- Ingress — si aún no ha elegido un controlador todavía

Cualquiera que use, `platform.ingressClass` en su archivo de configuración debe coincidir con la clase que el controlador realmente observa. Confírmelo con `kubectl get ingressclass`.

Cargar el secreto TLS

La configuración de entrada de SecurSpaces hace referencia a un secreto TLS. Créelo antes de la implementación:

```
kubectl create secret tls my-ssl-secret --cert=path/to/tls.crt --key=path/
to/tls.key
```

Implementar el gráfico

```
helm upgrade --install my_release ninjahchart-${SN_VERSION}.tgz -f
config.yml
```

verificar la implementación

Liste los pods en ejecución:

```
kubectl get pods
```

La salida se parece a lo siguiente:

```
pod/release-central-service-7794bf97db     1/1 Running 0 3h24m

pod/release-central-service-55f74bb5d      1/1 Running 0 3h24m

pod/release-mongodb-869ddfb7c-7q58h        1/1 Running 0 3h24m

pod/release-coordinator-7f9c4c95bd5fd      1/1 Running 0 3h24m

pod/release-proxy-569859ddb9-748jj         1/1 Running 0 3h24m

pod/release-frontend-7b4b8b97d4-67d2k      1/1 Running 0 3h24m

pod/release-workspace-api-74cb48675c-9x4v8 1/1 Running 0 3h24m
```

Luego, navegue a la URL de su implementación e inicie sesión con las credenciales de administrador establecidas en sus valores de Helm.

Qué configurar a continuación

TAREA	PÁGINA
Conectar un proveedor de identidad	Identidad y acceso
Conectar repositorios de código	Repositorios de código

TAREA	PÁGINA
Permitir acceso SSH a los espacios de trabajo	Reenvío TCP de SSH
Añadir una región	Múltiples regiones
Crear su primer proyecto y equipo	Configurar un proyecto para su equipo

Actualizar una implementación existente

Antes de empezar

Asegúrese de tener:

- El archivo de configuración de su implementación anterior, por ejemplo, `config_2026.9.0.yaml`.
- Acceso al mismo registro de contenedores utilizado en la implementación original.
- Una copia de seguridad reciente de la base de datos. Para Percona interno, revise el procedimiento de actualización paso a paso.

Procedimiento

1. Inicie el contenedor de Strong Installer con la versión de lanzamiento objetivo:

```
docker run -it --rm -v ${PWD}:/strong-network/shared \

    strongnetwork/strong_installer:<target-version>
```

2. Ejecute el comando de actualización con su archivo de configuración existente:

```
sds-cli upgrade -c config_2026.9.0.yaml
```

3. Espere a que la CLI descargue el chart, actualice la configuración y envíe las imágenes. Para los despliegues de Percona (`platform.deployPerconaMongoDB` sin establecer o `true`), también copia el kit de actualización en `/strong-network/shared/percona-upgrade/` e imprime las instrucciones del script. No se añaden nuevas indicaciones de Percona a la CLI; al volver a ejecutarlo, se reemplaza el kit con los scripts de la versión del instalador.

4. Al actualizar de SDS 2026.9 al chart con Percona Operator 1.23.0, ejecute el kit desde el directorio compartido antes de Helm. Reemplace el espacio de nombres, la versión y la versión del chart con sus valores:

   ```
   ./percona-upgrade/upgrade-percona.sh default release ./ninjahchart-<version>.tgz
   ```

   El script solicita `yes`, realiza una copia de seguridad, actualiza a través de 1.21.2 y 1.22.0, y aplica los CRD 1.23. Helm 3 no actualiza los CRD existentes. Consulte Actualización para conocer los requisitos previos, las pausas de escritura y los comandos de recuperación. Omita este paso para MongoDB externo.

5. Ejecute el comando Helm impreso por el instalador y luego valide la plataforma. Para Percona, esto completa la migración al operador 1.23.0, MongoDB 7.0.37-20 y PBM 2.15.0. Helm bloquea un despliegue de Percona existente que no ha alcanzado la versión 1.22 o carece de los CRD 1.23 requeridos.

Actualización sin un archivo de configuración

Si no tiene el archivo de configuración original, ejecute la actualización con la bandera `--ignore-config`:

```
sds-cli upgrade --ignore-config
```

La CLI solicita cada valor que de otro modo leería del archivo de configuración, incluidos el dominio del host y la URL del registro de destino, y no escribe un nuevo archivo de configuración. Consulte Actualización sin un archivo de configuración.

> **Advertencia:**
>
> Si actualiza sin un archivo de configuración, debe introducir todos los parámetros de despliegue manualmente. Utilice esta opción solo si el archivo de configuración no está disponible.

Actualización automatizada

Para pipelines de CI/CD u otros despliegues automatizados, puede ejecutar la etapa de actualización del instalador con un solo comando. Aplique el comando Helm impreso después.

Para la migración a Percona 1.23, primero complete el paso del script de Percona anterior; el script requiere confirmación.

Ejemplo: Google Artifact Registry

```
docker run -it --rm -v ${PWD}:/strong-network/shared \

    strongnetwork/strong_installer:2026.9.4 \

    upgrade \

    -c config_2026.9.0.yaml \

    --source-registry-region eu \

    --service-account-file-path shared/your-service-account.json
```

La URL del registro de destino se lee del archivo de configuración pasado con `-c`. No hay ninguna bandera para configurar la.

Banderas

Para la lista completa de indicadores, incluyendo los indicadores de autenticación específicos del registro para Google Artifact Registry, Amazon ECR, Azure Container Registry y el inicio de sesión genérico de Docker, consulte referencia de la CLI de SDS.

> **Consejo:**
>
> Utilice `--use-docker-login` con `--registry-username` y `--registry-password` para omitir las solicitudes de autenticación del proveedor de la nube. Esto es útil para las canalizaciones de CI/CD que no admiten solicitudes interactivas.

Solo enviar imágenes

Para enviar imágenes de contenedor sin ejecutar una instalación o actualización completa, utilice el comando `push-images`.

Procedimiento

1. Inicie el contenedor de Strong Installer:

```
docker run -it --rm -v ${PWD}:/strong-network/shared \

    strongnetwork/strong_installer:2026.9.4
```

2. Ejecute el comando `push-images`:

```
sds-cli push-images \

    --source-registry-region eu \

    -c config.yaml \

    --verbose
```

Enviar imágenes con inicio de sesión de Docker (no interactivo)

Para las canalizaciones de CI/CD, utilice la bandera `--use-docker-login` para omitir las solicitudes de autenticación en la nube:

```
sds-cli push-images \

    --source-registry-region eu \

    --use-docker-login \

    --registry-username "your-username" \

    --registry-password "your-password" \

    -c config.yaml
```

Banderas

Para la lista completa de indicadores `push-images`, incluyendo las opciones de omisión, consulte referencia de la CLI de SDS.

Solución de problemas

Solicitudes de autenticación en CI/CD

PROBLEMA	RESOLUCIÓN
La CLI le pide que elija un método de autenticación incluso cuando se proporcionan las credenciales.	Utilice `--use-docker-login` con `--registry-username` y `--registry-password` para omitir la autenticación del proveedor de la nube.

```
sds-cli push-images \

    --use-docker-login \

    --registry-username "$USERNAME" \

    --registry-password "$PASSWORD" \

    ...
```

Permiso denegado de Docker

PROBLEMA	RESOLUCIÓN
Errores de permiso denegado al ejecutar comandos de Docker	Asegúrese de que su usuario esté añadido al grupo `docker`, o anteponga el comando con `sudo`.

Fallos al subir imágenes

PROBLEMA	RESOLUCIÓN
Las imágenes no se pueden subir al registro de destino.	verificar que sus credenciales de registro son correctas.
	Asegúrese de que el registro de destino existe y es accesible.
	Compruebe la conectividad de red tanto a los registros de origen como de destino.

PROBLEMA	RESOLUCIÓN
	Utilice `--verbose` para mensajes de error detallados.

Información relacionada

- Referencia de la CLI de SDS
- Actualización
- Requisitos

Ingress

Cada despliegue de Citrix SecurSpaces™ necesita un controlador de entrada delante. La plataforma termina TLS en la entrada, y el tráfico del espacio de trabajo —incluidas las conexiones WebSocket para el IDE en la nube y, opcionalmente, SSH— pasa a través de él.

Controladores compatibles

CONTROLADOR	DESPLEGADO POR EL GRÁFICO DE SECURSPACES	CONFIGURACIÓN NECESARIA
NetScaler CPX (recomendado)	Sí	Ninguna. Consulte NetScaler CPX
NGINX	No	Valores de ajuste y configuración manual para SSH
HAProxy	No	Establecer la clase de entrada
API de puerta de enlace de Kubernetes	No	Establezca una clase de pasarela en lugar de usar recursos Ingress
Istio	No	Haga coincidir su pasarela y la configuración manual para SSH. Consulte Istio

NetScaler CPX es la opción recomendada, y la única que el gráfico de SecurSpaces puede implementar y configurar por usted. Si no tiene ninguna preferencia existente, úselo.

> **Importante:**

> **NetScaler CPX no funciona actualmente en Google GKE.** Este es un problema conocido con una solución en curso y aún sin fecha. En GKE, use NGINX o la API de Gateway de Kubernetes, y contacte a Citrix para conocer el estado actual. Consulte Google GKE.

Qué afecta la elección

Dos cosas difieren significativamente entre los controladores.

Manejo de WebSocket y HTTP/2. El IDE en la nube mantiene una conexión WebSocket mientras un espacio de trabajo esté abierto. Un controlador que cierra las conexiones inactivas demasiado pronto, o que almacena en búfer las respuestas de forma agresiva, produce desconexiones que parecen fallos de la plataforma. Con NetScaler CPX, el gráfico aplica los perfiles correctos por sí mismo. Con NGINX, los configura manualmente — consulte NGINX.

Acceso SSH a los espacios de trabajo. SSH necesita una ruta TCP a través del ingress, en un puerto diferente al 443.

- Con **NetScaler CPX**, el gráfico crea el ingress SSH y el puerto de servicio por usted. Nada que hacer.
- Con **NGINX**, usted crea un ConfigMap, parchea la implementación del controlador y expone el puerto usted mismo. Consulte SSH TCP forwarding with NGINX.
- Con **Istio**, el gráfico no crea ningún ingress SSH. Usted expone TCP a la API del espacio de trabajo usted mismo, como con NGINX. Consulte Istio.

Esa diferencia es la principal razón práctica para preferir NetScaler CPX.

Selección de un controlador

El controlador se elige en el archivo de configuración que genera el instalador, antes de ejecutar Helm. Consulte Instalar con la CLI de Strong Installer.

CONFIGURACIÓN	PROPÓSITO
`platform.ingressClass`	La clase de entrada que su controlador observa
`platform.useNetscalerController`	Implementar y configurar NetScaler CPX
`platform.useNginxController`	Aplicar anotaciones de entrada específicas de NGINX
`platform.useHAProxyController`	Aplicar anotaciones de entrada específicas de HAProxy
`platform.useGatewayAPI`	Usar recursos de la API de Gateway en lugar de recursos de Ingress
`platform.useIstio`	Utilice los recursos de Istio Gateway y VirtualService en lugar de los recursos de Ingress
`platform.istio.gatewayNamespace`	Espacio de nombres donde se ejecuta la carga de trabajo del gateway de entrada de Istio
`platform.istio.gatewaySelector`	Etiquetas que seleccionan la carga de trabajo del gateway de entrada de Istio

Establezca el indicador de anotación que coincida con su controlador. `ingressClass` debe coincidir con la clase que el controlador realmente observa; confírmelo con `kubectl get ingressclass` en lugar de asumir el valor predeterminado.

Información relacionada

- NetScaler CPX
- NGINX
- Istio
- Reenvío TCP SSH con NGINX
- Requisitos del sistema

NetScaler CPX

NetScaler CPX es el controlador de entrada recomendado para Citrix SecurSpaces™, y el único que el gráfico Helm de SecurSpaces despliega por usted.

Funciona de inmediato. El gráfico instala NetScaler CPX, lo conecta a la plataforma y aplica la configuración que SecurSpaces necesita. No tiene que configurar el controlador por separado.

> **Importante:**
>
> **NetScaler CPX no funciona actualmente en Google GKE.** Este es un problema conocido con una solución en curso y sin fecha aún. En GKE, use NGINX o la API de Kubernetes Gateway, y contacte con Citrix para conocer el estado actual. Otras plataformas no se ven afectadas.

Qué configura el gráfico

Comprender lo que ya está gestionado le evita tener que repetirlo manualmente.

ÁREA	LO QUE OBTIENE
El controlador	NetScaler CPX se instala como parte de la versión de SecurSpaces, con su licencia aceptada y expuesta a través de un servicio LoadBalancer
Puertos	80 y 443 para la plataforma, más un puerto para SSH a los espacios de trabajo y uno para el agente VDI
Gestión de conexiones	Perfiles HTTP y TCP con WebSocket y HTTP/2 habilitados, que es lo que el IDE en la nube necesita para mantener una sesión abierta
Seguridad del backend	Autenticación de cliente en el frontend, y TLS al frontend y a los servicios centrales
SSH a los espacios de trabajo	Un ingreso SSH dedicado, creado automáticamente, enrutado al servicio de espacio de trabajo a través de TCP

El ingreso SSH es la diferencia que vale la pena conocer. Con otros controladores, usted mismo construye esa ruta.

Seleccionarlo

NetScaler CPX se elige en el archivo de configuración que genera el instalador:

```
platform:

  useNetscalerController: true

  ingressClass: netscaler-cpx-ingress

  sslCertificateSecret: <your-tls-secret>
```

`ingressClass` debe coincidir con la clase que el controlador observa. `netscaler-cpx-ingress` es el valor que usa el gráfico; si cambia uno, cambie ambos.

`sslCertificateSecret` nombra un secreto TLS en el espacio de nombres de la versión, que cubre su dominio de plataforma, su dominio de proxy y el subdominio de proxy comodín. Consulte Instalar con la CLI de Strong Installer.

verificar

Después de que se implementa la versión:

```
kubectl get pods -n strong-network

kubectl get ingress -n strong-network

kubectl get svc -n strong-network
```

Debería ver el pod CPX en ejecución, una dirección externa en el servicio LoadBalancer y un ingreso para la plataforma junto con uno para SSH.

Si la dirección del LoadBalancer permanece pendiente, su clúster no tiene un proveedor de balanceador de carga o no tiene una dirección libre en su rango. Ese es un problema a nivel de clúster, no de SecurSpaces.

Uso de un NetScaler existente

Si ya ejecuta NetScaler delante de su clúster, apunte SecurSpaces a él en lugar de dejar que el gráfico despliegue CPX: omita `useNetscalerController` y establezca `ingressClass` en la clase que observa su controlador existente. El gráfico sigue aplicando las anotaciones específicas de NetScaler cuando el nombre de la clase comienza con `netscaler`.

Información relacionada

- Documentación de NetScaler CPX — la documentación del producto para el propio CPX, incluyendo escalado, licencias y configuración avanzada
- Ingress
- Instalar con la CLI de Strong Installer
- Requisitos del sistema

NGINX

Estos valores se aplican al controlador **ingress-nginx**. Si utiliza NetScaler CPX, el gráfico de SecurSpaces aplica los perfiles equivalentes por sí mismo y no hay nada que ajustar. Consulte NetScaler CPX.

Citrix SecurSpaces™ gestiona conexiones de larga duración: el IDE en la nube, las sesiones SSH y las aplicaciones de espacio de trabajo mantienen un socket abierto durante toda la sesión de trabajo. La configuración predeterminada de ingress-nginx está ajustada para tráfico de solicitud/respuesta corto, por lo que se recomiendan los siguientes valores para una implementación de SecurSpaces.

Instalar el controlador

SecurSpaces no instala NGINX por usted. El clúster necesita un controlador ingress-nginx antes de implementar el gráfico de Helm.

Muchos servicios gestionados de Kubernetes tienen una forma recomendada de hacerlo; consulte primero la guía de implementación de ingress-nginx de su proveedor de la nube. Si su proveedor no aparece en la lista, instálelo con Helm:

```
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx

helm repo update

helm install --namespace nginx --create-namespace ingress-nginx ingress-
```

```
nginx/ingress-nginx \

  --set controller.service.type=LoadBalancer
```

En AWS, añada la anotación que aprovisiona un equilibrador de carga de red:

```
--set controller.service.annotations."service\.beta\.kubernetes\.io/aws-load-balancer-type"="nlb"
```

Confirme la clase de entrada que supervisa el controlador y utilice ese valor para `platform.ingressClass` en su configuración de SecurSpaces:

```
kubectl get ingressclass
```

Ajustar el controlador

Aplique los siguientes valores antes de poner la plataforma en uso. En la práctica, no son opcionales: los valores predeterminados producen sesiones de Cloud IDE interrumpidas en condiciones de trabajo normales.

Existe un ConfigMap predeterminado en el espacio de nombres `ingress-nginx`, normalmente llamado `ingress-nginx-controller`. El nombre varía según cómo se haya instalado el controlador de entrada.

```
kubectl edit configmap ingress-nginx-controller
```

Valores recomendados

```
apiVersion: v1

data:

  allow-snippet-annotations: "true"

  enable-brotli: "true"

  keep-alive: 120s

  keep-alive-requests: "10000"
```

```
  use-gzip: "true"

  use-http2: "true"

kind: ConfigMap
```

VALOR	EFECTO
`allow-snippet-annotations`	Controla si el controlador respeta las anotaciones de fragmentos. Consulte la nota a continuación: esta tiene consecuencias más allá del rendimiento.
`enable-brotli`	Comprime las respuestas con Brotli cuando el cliente lo soporta.
`keep-alive`	Mantiene una conexión upstream inactiva abierta durante 120 segundos en lugar de los 75 predeterminados.
`keep-alive-requests`	Permite 10.000 solicitudes por conexión keep-alive en lugar de las 1.000 predeterminadas, lo cual es importante para las sesiones largas que crea el IDE en la nube.
`use-gzip`	Comprime las respuestas para clientes que no soportan Brotli.
`use-http2`	Sirve HTTP/2 a los clientes que lo soportan.

Acerca de `allow-snippet-annotations`

El gráfico Helm de SecurSpaces lee este valor del ConfigMap cuando se renderiza y se comporta de manera diferente dependiendo de lo que encuentre:

- **`"true"`** — el gráfico añade su propia anotación `server-snippet` al ingress, que instala páginas de error de SecurSpaces para HTTP 400, 401, 403, 404, 405, 408 y 413.
- **`"false"`** — el gráfico omite esa anotación. La plataforma sigue funcionando, pero esas respuestas recurren a las páginas de error predeterminadas del controlador de ingress.

Si establece `platform.nginxConfig` o `platform.nginxConfigSubdomain` en sus valores de Helm, el gráfico emite una anotación `configuration-snippet`, que el controlador solo respeta cuando `allow-snippet-annotations` es `"true"`.

> **Nota:**
>
> Las anotaciones de fragmentos permiten a cualquier usuario que pueda crear un objeto Ingress inyectar la configuración de NGINX. Las versiones recientes de ingress-nginx establecen esto por defecto en `"false"` por esa razón. Configurar esto en `"true"` es una compensación entre las páginas de error de SecurSpaces y esa exposición. Si la política de su clúster prohíbe las anotaciones de fragmentos, déjelo en `"false"` — la plataforma es completamente funcional de cualquier manera.

Información relacionada

- Reenvío TCP SSH
- Instalar con la CLI de Strong Installer
- Puertos y protocolos

Istio

Utilice Istio cuando un estándar de clúster requiera que el tráfico de la plataforma entre a través de una puerta de enlace de entrada de Istio. Cuando lo habilita, el gráfico de Citrix SecurSpaces™ renderiza recursos de Istio Gateway, VirtualService y DestinationRule en lugar de recursos de Kubernetes Ingress.

SecurSpaces no instala Istio. Instale la puerta de enlace de entrada de Istio y confirme que está en ejecución antes de implementar el gráfico.

> **Importante:**
>
> El gráfico no crea ninguna entrada SSH cuando Istio está habilitado. Si sus desarrolladores se conectan a los espacios de trabajo a través de SSH, debe construir esa ruta usted mismo. Consulte SSH a espacios de trabajo.

Antes de empezar

Asegúrese de tener:

- **Istio 1.22 o posterior.** El gráfico utiliza la API estable `networking.istio.io/v1`.
- **Una puerta de enlace de entrada de Istio ya en ejecución** en el clúster.
- **Permiso para crear recursos en el espacio de nombres de la puerta de enlace.** El gráfico crea un Secret que contiene la autoridad de certificación de servicios internos allí, junto con las DestinationRules que seleccionan la carga de trabajo de la puerta de enlace. Istio resuelve ambos en el espacio de nombres de la puerta de enlace en lugar del espacio de nombres de la versión.
- **Las etiquetas que identifican su carga de trabajo de puerta de enlace.** Confírmelas en lugar de asumir las predeterminadas:

  ```
  kubectl get pods -n <gateway-namespace> --show-labels
  ```

Seleccionar Istio

Istio se elige en el archivo de configuración que genera el instalador, antes de ejecutar Helm:

```
platform:

  useIstio: true

  istio:

    gatewayNamespace: istio-system

    gatewaySelector:

      istio: ingressgateway

  sslCertificateSecret: <your-tls-secret>
```

VALOR	LO QUE ESTABLECE
`platform.useIstio`	Renderiza recursos de Istio en lugar de recursos de Ingress

VALOR	LO QUE ESTABLECE
`platform.istio.gatewayNamespace`	El espacio de nombres donde se ejecuta la carga de trabajo del gateway de entrada de Istio
`platform.istio.gatewaySelector`	Las etiquetas que seleccionan la carga de trabajo del gateway de entrada de Istio

Los valores predeterminados mostrados anteriormente coinciden con un gateway instalado con `istioctl install`. `platform.ingressClass` y los indicadores específicos del controlador se ignoran mientras `useIstio` está activado.

Distribuciones de Istio gestionadas

Las distribuciones gestionadas etiquetan su gateway de forma diferente y lo ejecutan en su propio espacio de nombres. El complemento de Istio de Azure Kubernetes Service, por ejemplo, necesita:

```
platform:
  useIstio: true
  istio:
    gatewayNamespace: aks-istio-ingress
    gatewaySelector:
      istio: aks-istio-ingressgateway-external
```

Qué crea el gráfico

RECURSO	QUÉ HACE
Gateway para el host de la plataforma	Sirve HTTP en el puerto 80 con una redirección a HTTPS, y HTTPS en el puerto 443
Gateway para subdominios de espacio de trabajo	Sirve el nombre de host del proxy y su subdominio comodín

RECURSO	QUÉ HACE
VirtualService para el host de la plataforma	Enruta cada ruta de la plataforma al servicio que la atiende
VirtualService para los subdominios del espacio de trabajo	Enruta los subdominios a la API del espacio de trabajo, y el coordinador al coordinador
DestinationRules, en el espacio de nombres de la puerta de enlace	Reorigina TLS a cada servicio y verificar el certificado
Secreto de la autoridad de certificación de servicios	Otorga a la puerta de enlace la autoridad contra la que verifica esos servicios

En el host de la plataforma, el gráfico enruta las rutas gRPC-Web, SCIM, OAuth, SAML y REST al servicio central, las rutas de espacio de trabajo y navegador a la API del espacio de trabajo, y todo lo demás al frontend.

El TLS público termina en la puerta de enlace de entrada de Istio. La puerta de enlace abre entonces una segunda conexión TLS a los servicios de SecurSpaces, para que el tráfico permanezca cifrado en su camino a través del clúster.

En una región externa, el gráfico expone solo la API del espacio de trabajo, en el propio host de API de esa región.

SecurSpaces permanece fuera de la malla

Los pods de servicio de SecurSpaces optan por no participar en la inyección de sidecar de Istio. Los servicios ya cifran el tráfico entre ellos con la autoridad de certificación de servicios interna, y mantenerlos fuera de la ruta de datos significa que la política de malla de todo el clúster no los rige.

Esto es importante si su malla aplica cualquiera de los siguientes, porque de lo contrario ambos romperían la plataforma:

- Un `outboundTrafficPolicy` de `REGISTRY_ONLY`, lo que bloquearía las llamadas salientes a proveedores de Git, proveedores de identidad y registros de contenedores.
- Una política de denegación por defecto `AuthorizationPolicy`, que bloquearía las llamadas entre los servicios de SecurSpaces.

El gateway de entrada sigue enrutando a los servicios a través de las DestinationRules que crea el gráfico.

SSH a los espacios de trabajo

Los recursos de Istio que crea el gráfico solo admiten HTTP y HTTPS. A diferencia de NetScaler CPX™, que crea una entrada SSH y el puerto de servicio por usted, Istio le deja ese camino a usted.

Para ofrecer SSH, exponga el tráfico TCP al servicio de API del espacio de trabajo en el puerto 2222 a través de su gateway, luego habilite SSH a nivel de plataforma, organización, proyecto y espacio de trabajo. Los pasos del lado de la plataforma son los mismos independientemente del controlador que utilice; consulte Reenvío TCP SSH, y comience en **Habilitar acceso SSH en la plataforma**.

verificar

Después de desplegar la versión, confirme que los recursos existen y que el gateway tiene una dirección externa:

```
kubectl get gateway,virtualservice -n strong-network

kubectl get destinationrule -n <gateway-namespace>

kubectl get svc -n <gateway-namespace>
```

Resultado esperado: dos Gateways y dos VirtualServices en el espacio de nombres de la versión, una DestinationRule para cada servicio de SecurSpaces en el espacio de nombres del gateway, y una dirección externa en el servicio del gateway.

Si el host de la plataforma devuelve un 503, el gateway coincide con el recurso Gateway pero no puede alcanzar un servicio. Compruebe que las DestinationRules se hayan desplegado en el espacio de nombres del gateway y que su selector de carga de trabajo coincida con las etiquetas del gateway.

Información relacionada

- Entrada
- Reenvío TCP SSH
- Instalar con la CLI de Strong Installer
- Puertos y protocolos

SSH TCP forwarding with NGINX

Esta guía describe cómo configurar la plataforma SecurSpaces para habilitar el acceso SSH a los Workspaces. El acceso SSH permite a los desarrolladores conectarse de forma segura al sistema de archivos remoto de un espacio de trabajo y utilizar funciones de IDE remoto en herramientas como Visual Studio Code, JetBrains Gateway, Cursor o Windsurf.

> **Nota:**
>
> La configuración de entrada en esta página es para **NGINX**. Si utiliza NetScaler CPX, el gráfico de SecurSpaces crea la entrada SSH y el puerto de servicio por usted, por lo que puede saltar a Habilitar acceso SSH en la plataforma. Consulte NetScaler CPX.

> Al utilizar distribuciones de Kubernetes como MicroK8s, reemplace la aplicación de despliegue con un `DaemonSet`.

Información general

La función de acceso SSH es opcional y debe habilitarse en varios niveles:

- Plataforma
- Organización
- Proyecto
- Espacio de trabajo individual

Esta guía explica:

1. Configurar el balanceador de carga de nginx para reenviar solicitudes TCP para el acceso SSH.
2. Habilitar el acceso SSH en la configuración de la plataforma, la organización y el proyecto.
3. Usar SSH para conectarse a los Workspaces.

Configurar NGINX para el acceso SSH

El balanceador de carga nginx debe configurarse para gestionar las solicitudes SSH. Este es un proceso relativamente rápido. Deberá:

1. Crear un ConfigMap llamado ssh-mapping en el espacio de nombres nginx que mapee el puerto SSH al puerto SSH del servicio de espacio de trabajo SN (designado 12345)

2. Editar el DeploymentApp del controlador de entrada nginx para que aplique el nuevo ConfigMap en la bandera –tcp-services-configmap.
3. Exponer el puerto 12345 en el Servicio del controlador de entrada nginx.

Crear un ConfigMap

Para crear el ConfigMap, primero cambie al espacio de nombres del controlador nginx; por defecto, debería llamarse nginx. Luego, simplemente ejecute el comando para crear el ConfigMap:

```
kubectl create configmap ssh-mapping
```

Edite el campo de datos del ConfigMap para incluir un mapeo del puerto SSH a la API del espacio de trabajo de su versión (está escuchando en el puerto 2222, que está codificado, por favor no cambie este valor). Para hacer esto, edite el mapa de configuración:

```
kubectl edit configmap ssh-mapping
```

Actualice el campo `data`:

```
apiVersion: v1

data:

  "12345": default/release-workspace-api:2222

kind: ConfigMap
```

Importante:

El puerto `2222` está codificado en la API del espacio de trabajo. No cambie este valor.

Actualizar el despliegue del controlador de entrada NGINX

Edite el DeploymentApp del despliegue del controlador de entrada nginx para incluir el argumento `--tcp-services-configmap`:

```
kubectl edit deployment ingress-nginx-controller
```

Añada lo siguiente a los Argumentos del controlador (bajo el encabezado Args):

```
spec:

--tcp-services-configmap=$(POD_NAMESPACE)/ssh-mapping
```

Exponer puerto en el servicio

Exponga el puerto en el servicio del controlador nginx. Añada la siguiente entrada bajo el campo de puertos del servicio:

```
kubectl edit svc nginx-ingress-controller
```

```
Ports:

appProtocol: http

      name: http

      nodePort: 30875

      port: 80

      protocol: TCP

      targetPort: http

appProtocol: https

      name: https

      nodePort: 31800

      port: 443

      protocol: TCP

      targetPort: https

name: ssh

      port: 12345
```

```
    protocol: TCP

    targetPort: 12345
```

Una vez completado, las solicitudes TCP al puerto `12345` se reenviarán al servicio del espacio de trabajo.

Habilitar el acceso SSH en la plataforma

El acceso SSH debe habilitarse individualmente en los niveles de plataforma, organización y proyecto.

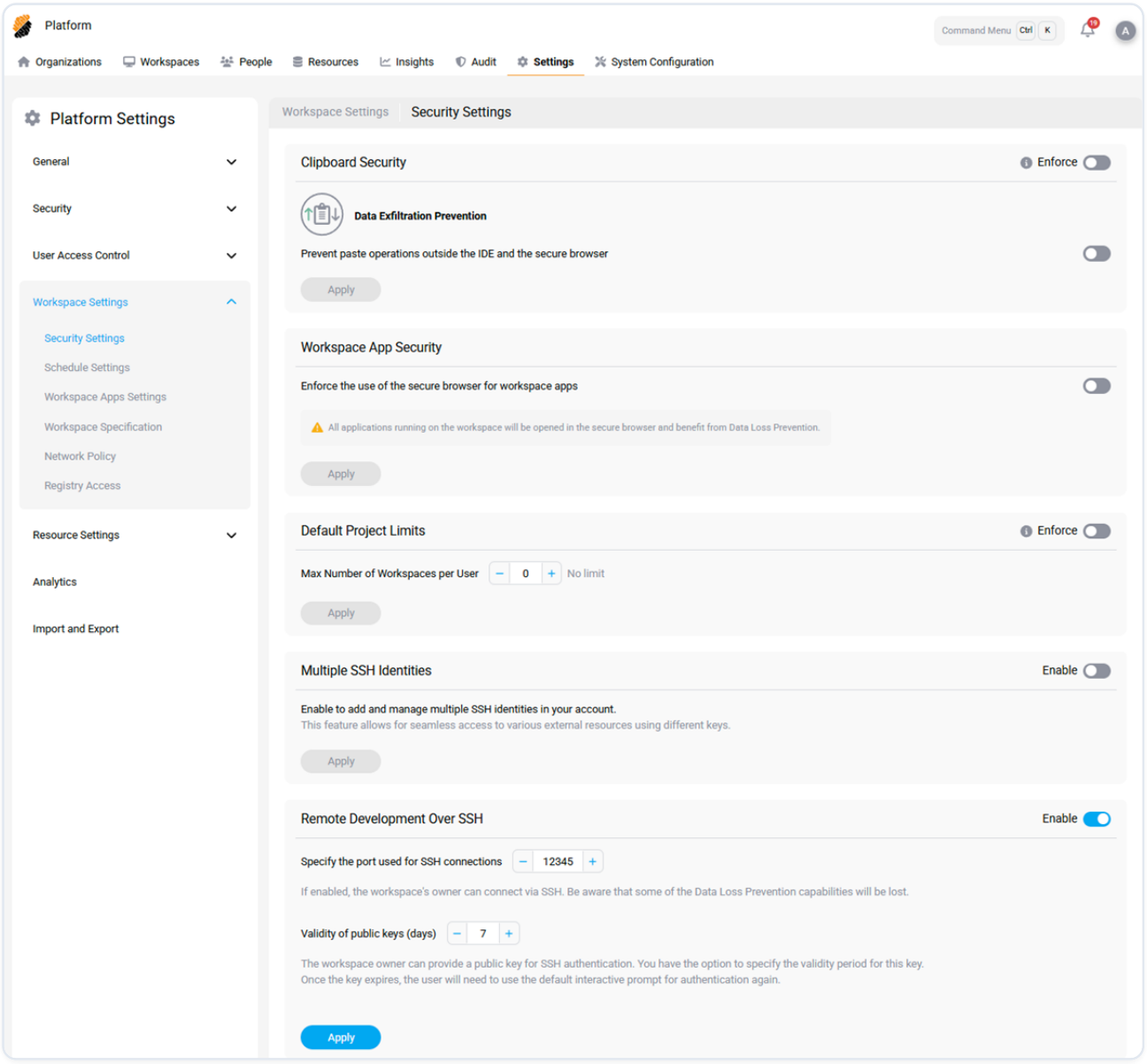
Nivel de plataforma

> **Rol requerido**: Administrador o responsable de seguridad

> Para habilitar la función, navegue a la página de Configuración de la plataforma del espacio de trabajo:

Descripción general de la plataforma → Configuración → Configuración del espacio de trabajo → Configuración de seguridad

- Localice la sección **Desarrollo remoto a través de SSH**.
- Active la función **activada**.
- Asegúrese de que el puerto SSH coincida con el puerto expuesto en el balanceador de carga de nginx (`12345`).



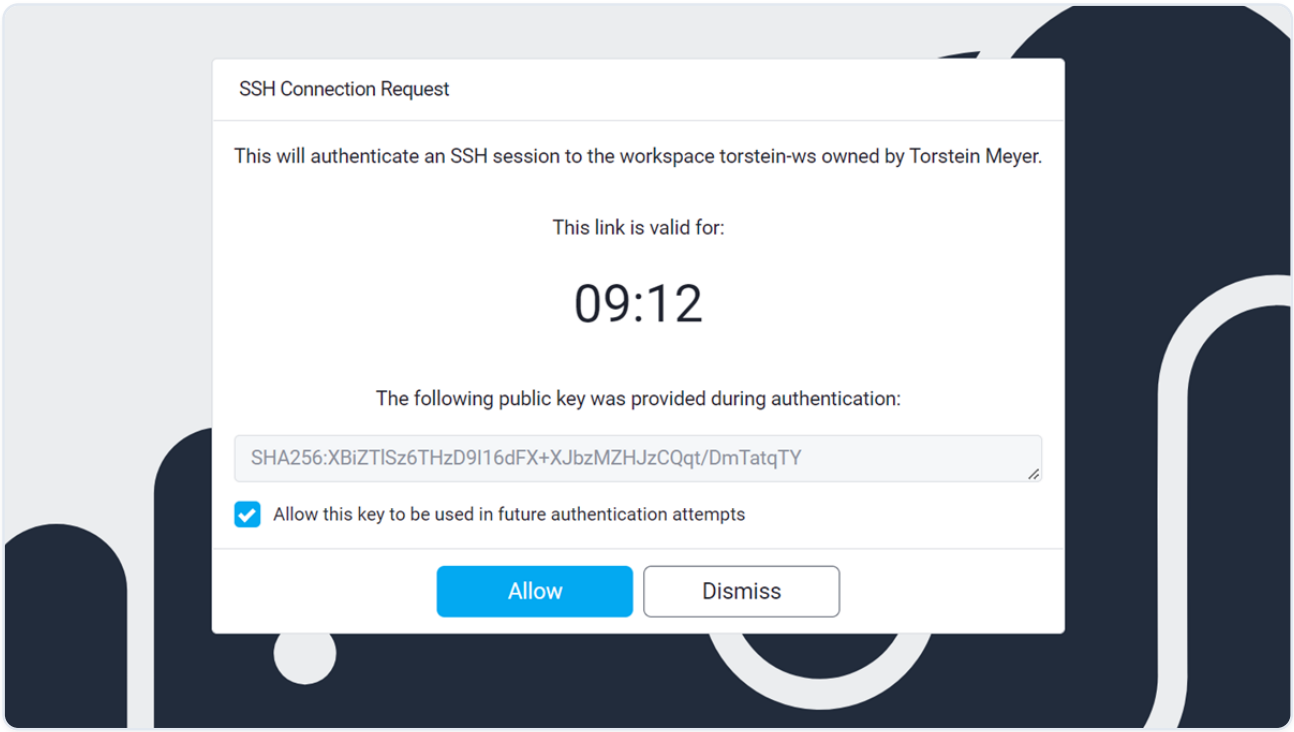
El administrador también puede configurar el **período de validez** para las claves públicas utilizadas en la autenticación con el espacio de trabajo.

Al conectarse a un espacio de trabajo con SSH, se le mostrará al usuario el siguiente mensaje:

```
C:\Users\torstein>ssh ws-53748696236688@ssh.proxy.cloudcoder.network
you need to approve the SSH connection request on the platform. Access the following URL to proceed:
https://cloudcoder.network/ssh_to_workspace_approval/ebf75f3273c1de91b41097cd7b1f56c12b3bc43e336ec072008d7419b5fc1edf
```

Al abrir el enlace proporcionado, llegarán a la siguiente página:

Desde aquí, el usuario puede permitir o descartar la solicitud. Además, el usuario puede optar por permitir que la clave pública proporcionada durante el proceso de autenticación omita la visualización del mensaje en futuros intentos de autenticación. Esta clave solo será válida por un período de tiempo determinado, que es configurable por el administrador a través de la configuración de validez de las claves públicas.



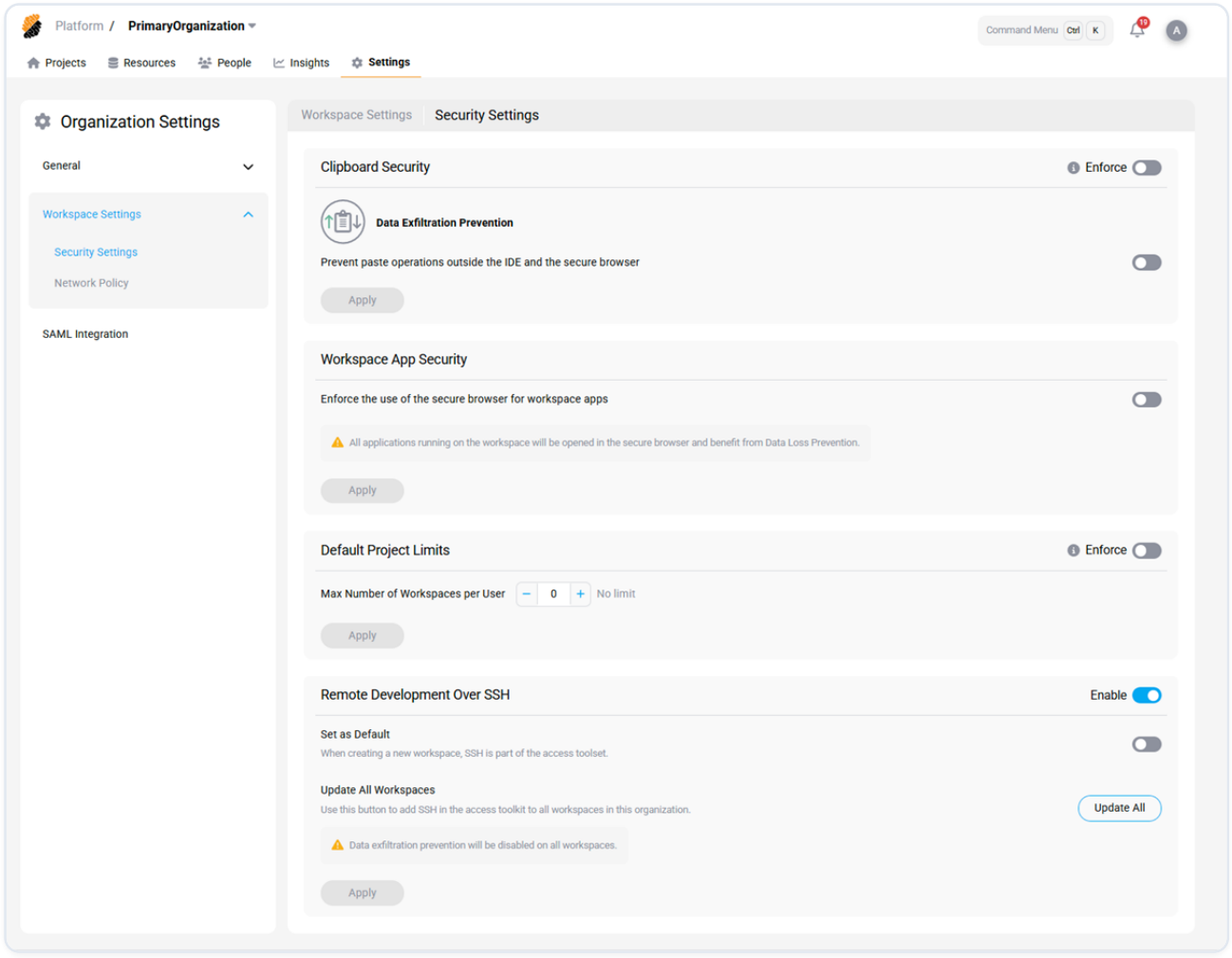
Nivel de organización

Rol requerido: Propietario de la organización o Administrador

Para habilitar la función, navegue a la página de Configuración de seguridad del espacio de trabajo:

Resumen de la organización → Configuración → Configuración del espacio de trabajo → Configuración de seguridad

- Active **Desarrollo remoto a través de SSH** para habilitar.

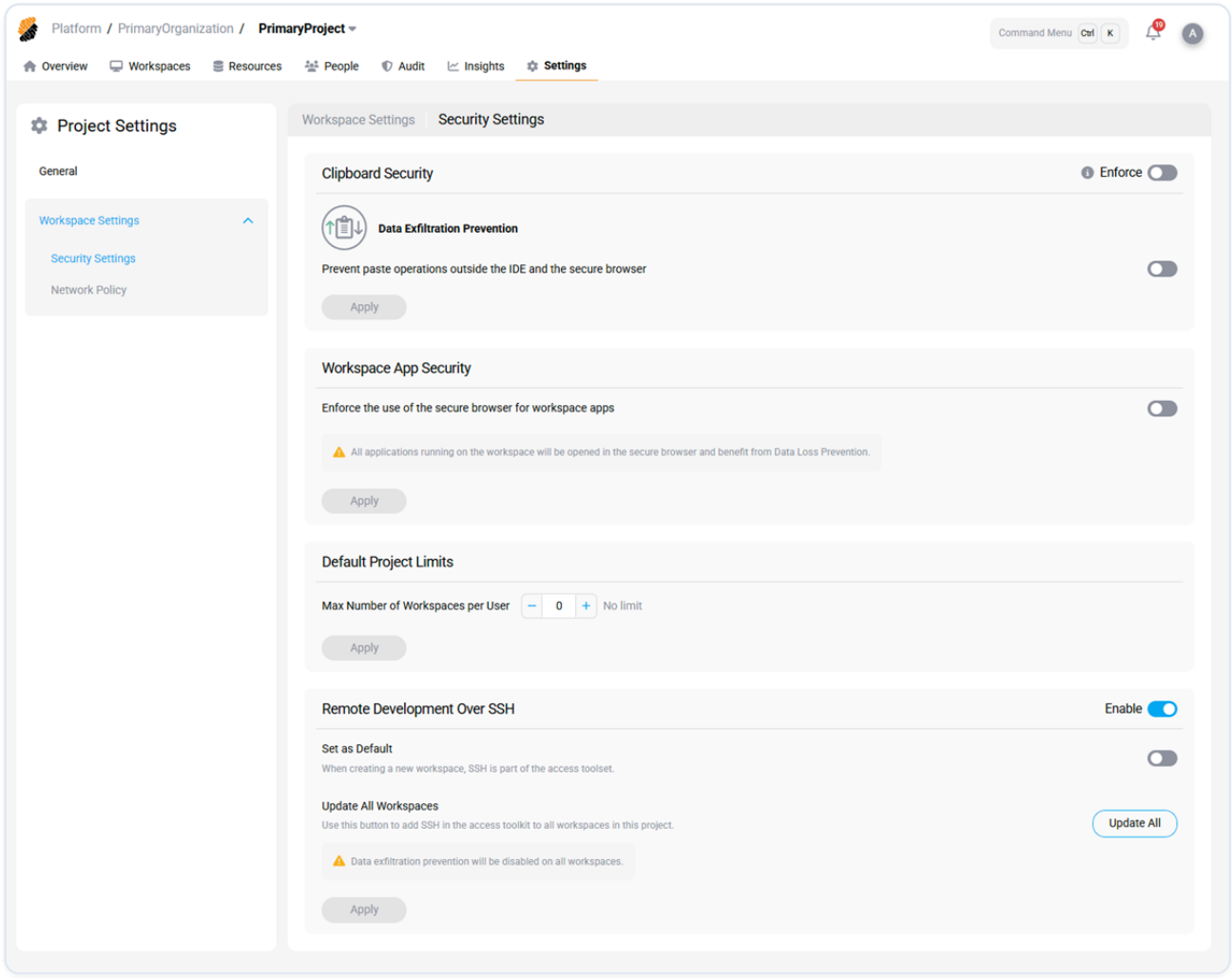


Nivel de proyecto

> **Rol requerido**: Propietario del proyecto o Administrador

> Para habilitar la función, navegue a la página de Configuración de seguridad del espacio de trabajo: **Resumen del proyecto → Configuración → Configuración del espacio de trabajo → Configuración de seguridad**

- Active **Desarrollo remoto a través de SSH** para habilitar.
- Opcionalmente:
  - Habilite SSH como parte del elemento de acceso predeterminado para nuevos espacios de trabajo.
  - Actualice todos los espacios de trabajo existentes para incluir acceso SSH.



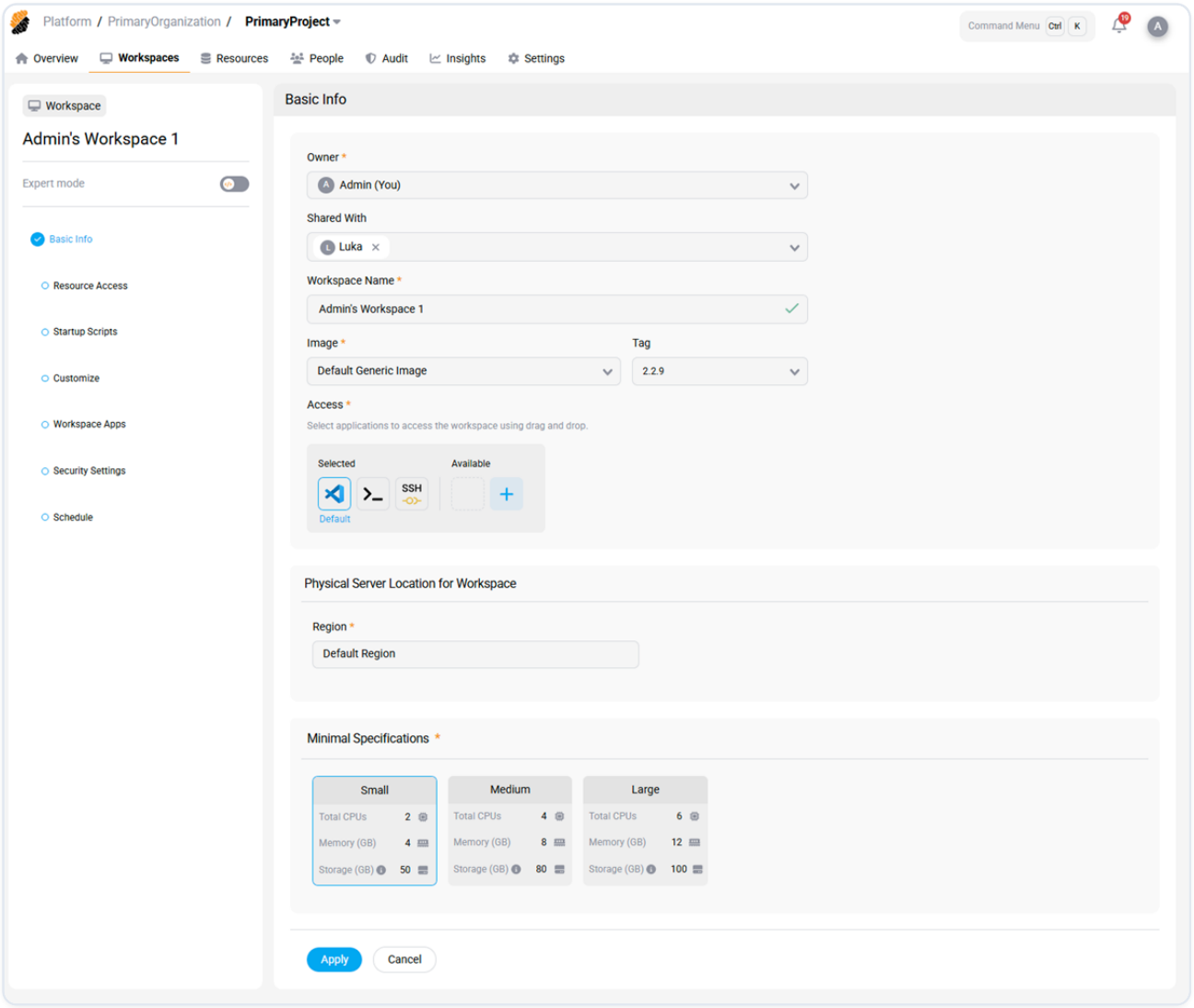
Usar SSH para conectarse a espacios de trabajo

Una vez habilitado, los desarrolladores pueden conectarse a los Workspaces en ejecución a través de SSH.

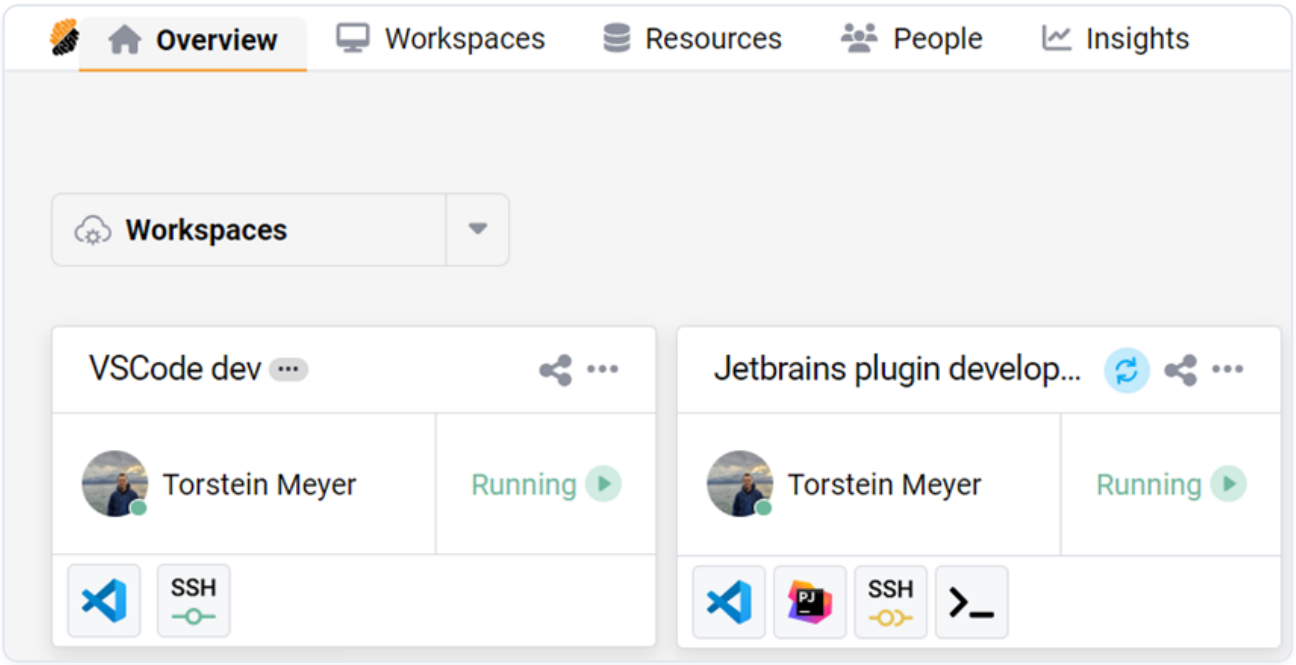
Habilitar SSH en Workspaces individuales

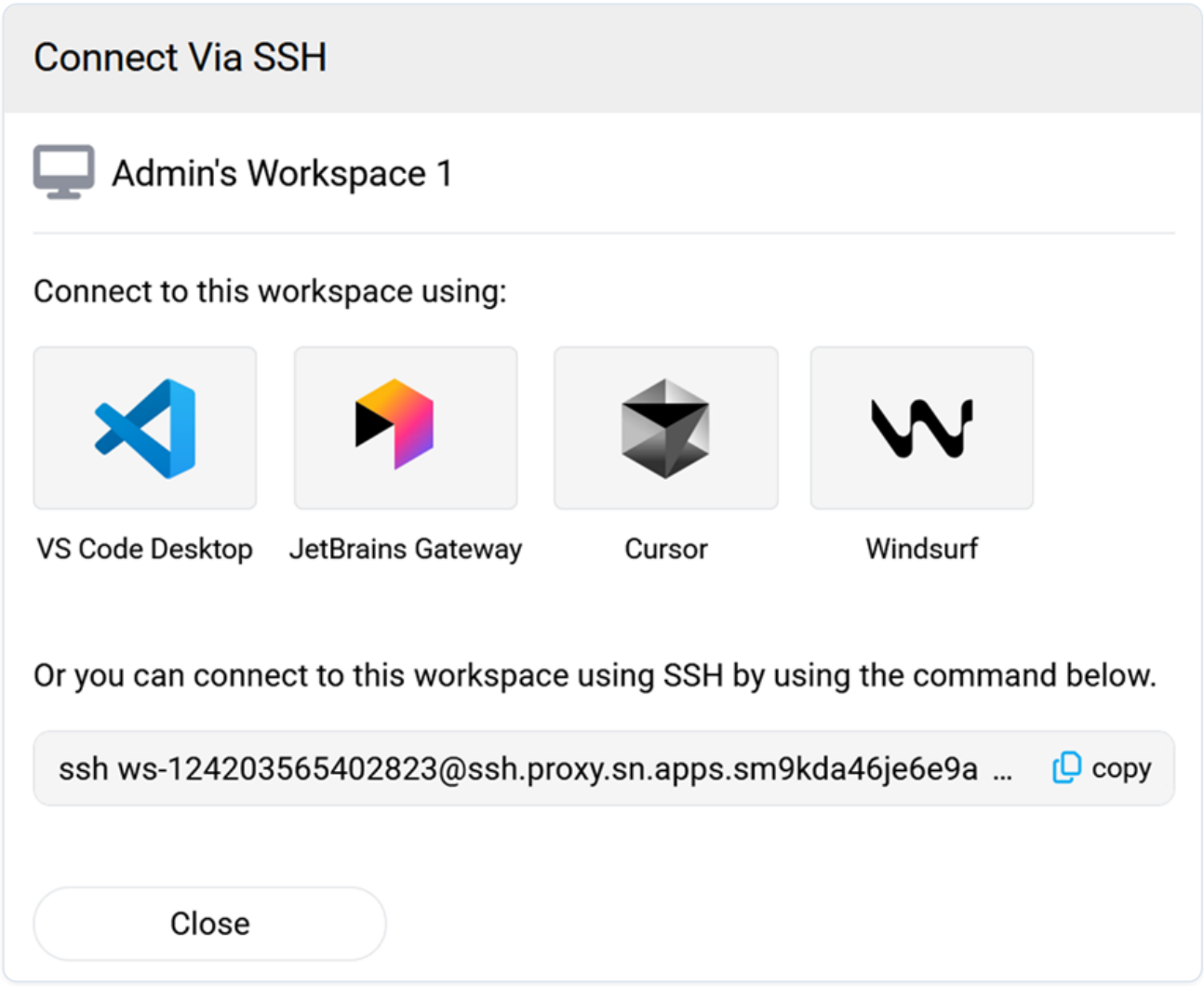
Con la función SSH habilitada, los desarrolladores de la plataforma pueden utilizarla. Como medida de seguridad adicional, la función también se puede habilitar o deshabilitar en cada Workspace específico. Por defecto, SSH está deshabilitado en los Workspaces individuales. Para habilitarlo:

- Editar el Workspace.
- En la página de **Información básica**, en **Acceso**, arrastre el icono de **SSH** de *Disponible* a *Seleccionado*.
- Haga clic en **Aplicar**.



En los workspaces con SSH habilitado, el propietario del workspace podrá acceder a él mediante SSH cuando el workspace esté en estado de ejecución. Para ello, primero abra el modal Conectar a través de SSH haciendo clic en el icono de SSH en la tarjeta del workspace:



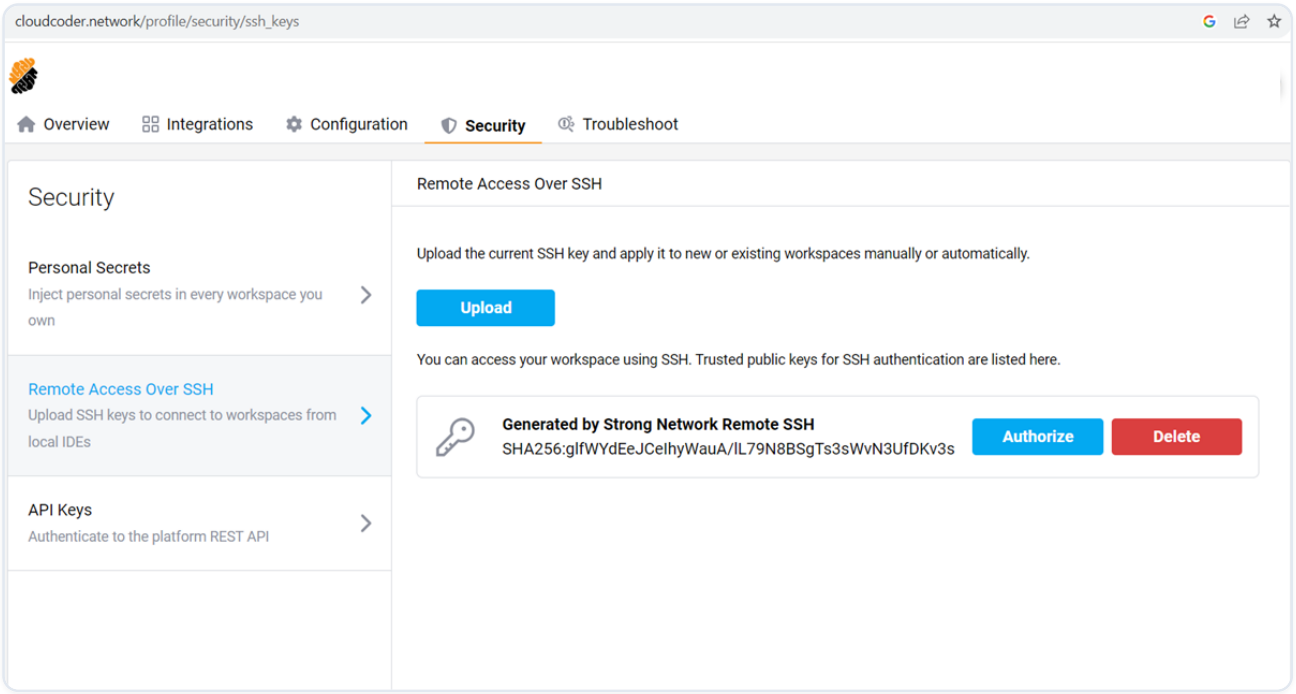


Esto abrirá el modal **Conectar a través de SSH**. Aquí el usuario puede conectarse directamente a sus editores locales de VS Code Desktop y/o JetBrains Gateway, o copiar el comando SSH en el formato:

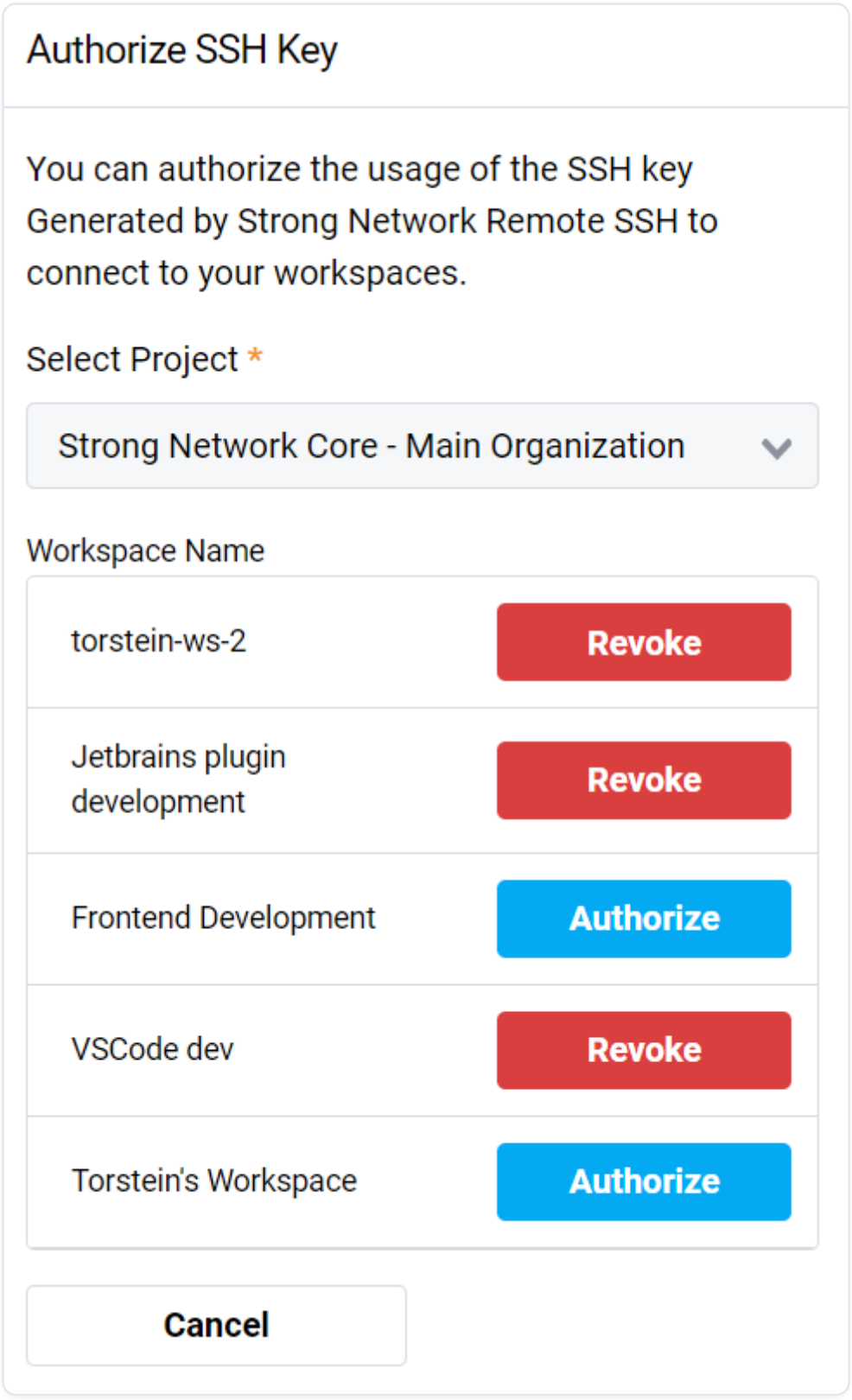
```
ssh ws-{id}.ssh.proxy.{domain} -p {port}
```

Luego puede usar este comando para acceder al workspace como lo haría con cualquier servidor SSH ordinario.

El usuario puede autenticarse utilizando una clave pública. Para ello, la clave pública debe cargarse en la plataforma y autorizarse para su uso en el workspace. La carga de la clave se puede realizar en la página de perfil:



Al hacer clic en **Autorizar**, el usuario podrá especificar el acceso de la clave a workspaces específicos:



SSH al espacio de trabajo con IDEs locales

Esta característica se puede usar con VS Code Remote Development y/o Jetbrains Gateway para usar un IDE en su máquina local pero el sistema de archivos en la máquina remota.

External database

Puede configurar SecurSpaces para autenticarse en una implementación externa de MongoDB con certificados X.509 en lugar de credenciales de nombre de usuario y contraseña. Utilice esta opción para implementaciones que requieran autenticación basada en certificados, como entornos de MongoDB Atlas gestionados por equipos de seguridad empresariales.

Requisitos previos

- Una implementación externa de MongoDB que admita `MONGODB-X509`
- Un usuario de base de datos MongoDB X.509 cuyo nombre distinguido coincida con el asunto del certificado de cliente
- Un certificado de cliente y una clave privada en formato PEM
- El paquete de la autoridad de certificación si su implementación de MongoDB utiliza una autoridad de certificación privada
- Acceso para actualizar los valores de Helm de SecurSpaces y ejecutar `helm upgrade`

Configurar la autenticación X.509 con valores de certificado en línea

Codifique los archivos de certificado en Base64 y añádalos a `platform.externalMongodb.auth`:

```
platform:

  externalMongodb:

    hostName: "cluster.example.mongodb.net"

    protocol: "mongodb+srv"

    additionalParameters: "retryWrites=true&w=majority"

    authMechanism: "MONGODB-X509"

    auth:

      database: "strong-network"

      caCertPemB64: "<base64-ca-certificate>"

      certPemB64: "<base64-client-certificate>"
```

```
      certKeyPemB64: "<base64-client-private-key>"
```

Si su implementación de MongoDB utiliza una autoridad de certificación de confianza pública, puede omitir `caCertPemB64`. SecurSpaces utilizará entonces el grupo de certificados del sistema.

Configurar la autenticación X.509 con un Secret de Kubernetes existente

Si ya gestiona el material del certificado en Kubernetes, haga referencia al Secret y a los nombres de las claves:

```
platform:

  externalMongodb:

    hostName: "cluster.example.mongodb.net"

    protocol: "mongodb+srv"

    additionalParameters: "retryWrites=true&w=majority"

    authMechanism: "MONGODB-X509"

    auth:

      database: "strong-network"

      existingSecret: "sds-mongodb-x509"

      existingSecretKeys:

        caCert: "ca.pem"

        cert: "tls.crt"

        certKey: "tls.key"
```

El Secret debe existir en el espacio de nombres de la implementación de SecurSpaces antes de aplicar la actualización de Helm.

Aplicar la configuración

1. Actualice su archivo de valores de Helm de SecurSpaces.
2. Confirme que el host, el protocolo y los parámetros adicionales de MongoDB externo coinciden con su implementación de MongoDB.
3. Ejecute su comando estándar `helm upgrade`.
4. Confirme que los servicios de SecurSpaces se inician correctamente y pueden conectarse a la implementación externa de MongoDB.

Después de la actualización, SecurSpaces se conecta a la implementación externa de MongoDB utilizando el certificado de cliente X.509 configurado.

Información relacionada

- La base de datos de SecurSpaces
- Dimensionamiento de la base de datos
- Realizar una copia de seguridad de la base de datos

External proxy configuration

Muchos entornos empresariales requieren que todo el tráfico saliente HTTP/HTTPS fluya a través de un proxy corporativo — para filtrado de salida, inspección TLS o registro de cumplimiento. SecurSpaces soporta esto de forma nativa a través de un único bloque de valores de Helm: `platform.externalProxy`.

Cuando se configura, **todo el tráfico saliente tanto de los servicios de la plataforma Citrix SecurSpaces™ como de los espacios de trabajo de los desarrolladores** se enruta a través del proxy especificado. SecurSpaces gestiona la configuración del proxy automáticamente dentro de los espacios de trabajo — inyecta las variables de entorno estándar `HTTP_PROXY`, `HTTPS_PROXY` y `NO_PROXY`, y la mayoría de las herramientas CLI (`curl`, `git`, `apt`, `pip`, `npm`, tiempos de ejecución de lenguajes) las respetan por defecto.

> **Nota:**
>
> Esta página trata sobre el enrutamiento del tráfico de SecurSpaces a través del proxy de salida **de su organización**. No trata sobre el servicio de proxy de SecurSpaces, que es un componente interno de la plataforma por el que pasa cada conexión del espacio de trabajo y

> que no necesita configuración. Consulte Cómo funciona el servicio de proxy de SecurSpaces.

Bloque de configuración

La configuración se encuentra bajo `platform.externalProxy` en su archivo de valores de Helm:

```
platform:

  externalProxy:

    httpsProxyUrl: ""

    httpProxyUrl: ""

    certificate: ""

    noProxyList: ""
```

Si omite el bloque `externalProxy` por completo, el tráfico fluye directamente desde el clúster sin un proxy.

Campos

`httpsProxyUrl`

La URL del proxy utilizada para el tráfico HTTPS. Formato: `http://host:port` o `https://host:port` (el *protocolo del propio proxy*, no el tráfico que se está proxyficando).

Si `httpsProxyUrl` está configurado pero `httpProxyUrl` no lo está, el tráfico HTTPS utiliza este valor, y el tráfico HTTP también recurre a él.

`httpProxyUrl`

La URL del proxy utilizada para el tráfico HTTP. Mismo formato que el anterior.

Si `httpProxyUrl` está configurado pero `httpsProxyUrl` no lo está, el tráfico HTTP utiliza este valor, y el tráfico HTTPS recurre a él.

En la mayoría de las configuraciones corporativas, un único proxy maneja ambos protocolos, por lo que es común configurar solo uno de los dos y confiar en la alternativa. Configure ambos explícitamente solo si su entorno utiliza proxies diferentes para HTTP y HTTPS.

`certificate`

Si su proxy realiza inspección TLS (a veces llamada intercepción TLS, proxy man-in-the-middle o "break-and-inspect"), presenta su propio certificado a los clientes en lugar del del servidor de origen. Para confiar en él, proporcione aquí el certificado de CA del proxy.

El certificado debe estar **codificado en PEM** y luego **codificado en base64** antes de ser colocado en el archivo de valores. Genere el valor con:

```
base64 -w 0 < proxy-ca.pem
```

(o `base64 -i proxy-ca.pem` en macOS). Pegue la cadena resultante de una sola línea como valor.

Si necesita confiar en **múltiples certificados** (por ejemplo, una CA raíz más una intermedia, o varios proxies en diferentes regiones), concatene todos los bloques PEM en un solo archivo *antes* de la codificación base64. Cada certificado debe mantener sus marcadores completos `-----BEGIN CERTIFICATE-----` / `-----END CERTIFICATE-----`:

```
cat root-ca.pem intermediate-ca.pem proxy-ca.pem > combined.pem

base64 -w 0 < combined.pem
```

El orden no importa para la evaluación de la confianza: todos los certificados del paquete se añaden al almacén de confianza.

Cuando se establece, el certificado se añade al almacén de confianza de cada contenedor de servicio de SecurSpaces y de cada contenedor de espacio de trabajo, de modo que las llamadas HTTPS a través del proxy se validan correctamente sin necesidad de configuración por aplicación.

Déjelo vacío si su proxy no realiza inspección TLS o utiliza un certificado de confianza pública.

`noProxyList`

Una lista separada por comas de hosts, dominios y direcciones IP que omiten el proxy. Utilícela para servicios internos a los que el proxy no puede llegar o que no necesitan inspección: su

servidor Git interno, un registro de contenedores privado, espejos de paquetes internos, la API de Kubernetes, etc.

Reglas de formato:

- Separado por comas, **sin espacios** entre las entradas
- Un punto inicial (`.example.com`) coincide con el dominio y todos sus subdominios
- Un nombre de host simple (`example.com`) coincide solo con ese host
- Se admiten direcciones IP (`192.168.1.10`) y rangos CIDR (`10.0.0.0/8`)
- Los puertos se pueden añadir con dos puntos (`example.com:8443`)

El tráfico dentro del clúster (cualquier cosa que se resuelva en una dirección `cluster.local` o una IP de pod/servicio) ya está excluido y no es necesario listarlo aquí.

Ejemplo práctico

Una implementación corporativa típica con un proxy de inspección TLS en `proxy.corp.example.com:8080`, un servidor Git interno y un registro privado:

```
platform:

  externalProxy:

    httpsProxyUrl: "http://proxy.corp.example.com:8080"

    httpProxyUrl: "http://proxy.corp.example.com:8080"

    certificate:
"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURxRENDQXBDZ0F3SUJBZ0lVRkV4..."

    noProxyList:
".corp.example.com,git.internal,registry.internal,10.0.0.0/8"
```

Lo que esto hace:

- Todo el tráfico HTTP y HTTPS saliente de los servicios y espacios de trabajo de SecurSpaces se enruta a través de `proxy.corp.example.com:8080`.
- El certificado de CA del proxy es de confianza en todas partes, por lo que la inspección TLS funciona sin errores de certificado.

- Cualquier cosa bajo `*.corp.example.com`, además de los dos nombres de host internos y el rango privado `10.0.0.0/8`, omite el proxy y se conecta directamente.

Aplicar cambios

SecurSpaces lee `platform.externalProxy` al iniciar el pod. Después de actualizar los valores y ejecutar `helm upgrade`, los servicios adoptan la nueva configuración cuando sus pods se reinician. Los pods de espacio de trabajo existentes continúan usando la configuración de proxy con la que se iniciaron; reinicie el espacio de trabajo para aplicar los cambios.

Solución de problemas

Errores de certificado (`x509: certificate signed by unknown authority`, `SSL_ERROR_BAD_CERT_DOMAIN`): El proxy realiza la inspección TLS, pero `certificate` no está configurado o contiene la CA incorrecta. verificar con `openssl s_client -connect <any-https-host>:443 -proxy proxy.corp.example.com:8080` desde dentro de un espacio de trabajo y compruebe qué certificado se presenta.

Hosts internos inalcanzables: Falta una entrada `noProxyList`. La coincidencia de subdominios requiere el punto inicial.

Errores de decodificación Base64 en el momento de la implementación: El valor `certificate` debe ser una sola línea sin saltos de línea incrustados. Vuelva a ejecutar `base64 -w 0` para aplanarlo.

Deploy SecurSpaces in multiple regions

Esta guía describe cómo implementar Citrix SecurSpaces™ en varios clústeres o regiones de Kubernetes. Una configuración multirregión mejora la experiencia del desarrollador al reducir la latencia y mejorar el rendimiento al dirigir a los usuarios al clúster regional más cercano.

Concepto principal

Una implementación multirregión consta de:

- **Implementación principal (central)** – Aloja la base de datos y los servicios principales.
- **Implementaciones regionales** – Implementaciones sin estado que se conectan a la base de datos y los servicios de la implementación principal.

Para garantizar un funcionamiento sin problemas, los valores de configuración críticos (especialmente los secretos para la autenticación y el cifrado) deben sincronizarse desde la

implementación principal a cada implementación regional. Esta sincronización se realiza copiando valores específicos de la implementación principal de Helm al gráfico de Helm regional.

Cómo implementar en regiones adicionales

Al igual que la implementación principal, las regiones se gestionan mediante gráficos de Helm.

Aunque los gráficos de Helm regionales son similares a los de la implementación principal, la principal diferencia es que varios valores que normalmente se **generan automáticamente durante la primera implementación** deben **copiarse manualmente** de la implementación principal a los gráficos de Helm regionales.

Estos valores incluyen:

- Credenciales de autenticación de la base de datos y parámetros de conexión
- Secretos para firmar cookies y tokens
- Secretos para cifrar valores almacenados

Rellenar los gráficos de Helm

1. Copie los valores de la sección `platform` de la implementación principal.

   2\. Añada una sección `region` y establezca `isExternalRegion` en `true`.

Ejemplo `values.yaml`:

```
platform:

  imageTag: ""                # Image tag for services

  hostName: ""                # Main domain used to access the platform,
e.g. strong-network.example.com

  centralProxyHostname: ""    # Wildcard domain for workspaces, e.g.
proxy.strong-network.example.com

  jwtSecret: ""               # Use the same jwtSecret as in the main
deployment

  secretKeyReposB64: ""       # Example: openssl rand -base64 16

  # Include all other values from the primary deployment's platform
section
```

```
  # ...
region:
  isExternalRegion: true      # For regional deployments, set this to true
```

Nota:

Cuando `isExternalRegion` se establece en `true`, establezca `platform.internalMongodb` en `false`.

Campos obligatorios y sus asignaciones

Los siguientes campos deben coincidir entre las implementaciones principal y regional:

NOMBRE DEL CAMPO	DESCRIPCIÓN
hostName	Nombre de dominio de la implementación (utilizado por usuarios y API).
centralProxyHostname	Subdominio del espacio de trabajo de la implementación principal (normalmente `proxy.<hostName>`)
jwtSecret	Secreto para firmar tokens y cookies.
secretKeyReposB64	Secreto para cifrar valores.

Recuperar secretos de la implementación principal

Ejecute los siguientes comandos en el espacio de nombres del **clúster de implementación principal** para extraer los valores requeridos.

Obtenga el valor `hostName`

```
kubectl get secrets strong-network-secret -o yaml
```

Copie el valor `hostName` de la salida.

Obtenga el valor `secretKeyReposB64`

```
kubectl get secrets strong-network-secret -o yaml
```

Copie el valor `secretKeyReposB64`, luego **descodifíquelo en base64** antes de pegarlo en los gráficos Helm regionales.

Por ejemplo:

```
echo "<base64-encoded-value>" | base64 --decode
```

Pasos siguientes

- verificar que todos los secretos y valores de configuración requeridos estén sincronizados entre las implementaciones principal y regional.
- Implemente el gráfico Helm para el clúster regional.
- Confirme que los desarrolladores pueden conectarse a la implementación regional más cercana con una latencia mínima.

GPU-enabled workspaces on AKS

Esta guía explica cómo habilitar y validar espacios de trabajo Citrix SecurSpaces™ habilitados para GPU en un clúster de Azure Kubernetes Service (AKS) utilizando GPU NVIDIA.

Requisitos previos

Antes de empezar, asegúrese de tener lo siguiente:

- Un clúster de AKS con permisos para gestionar grupos de nodos y desplegar complementos de Kubernetes
- Un grupo de nodos compatible con GPU (tamaño de VM de ejemplo: **Standard_NC24ads_A100_v4**)
- Acceso a la CLI de Kubernetes (**kubectl**)
- Una opción de plantilla/especificación de espacio de trabajo que pueda solicitar GPU (por ejemplo, **GPUs: 1**)

Añadir un grupo de nodos GPU

Cree o escale un grupo de nodos GPU en AKS utilizando el portal de Azure, la CLI de Azure o Infraestructura como Código (IaC). Una vez que los nodos estén listos, confirme que se han unido al clúster:

```
kubectl get nodes -o wide
```

Instalar el complemento de dispositivo NVIDIA

Debe desplegar el complemento de dispositivo NVIDIA como un DaemonSet para permitir que el clúster se comunique con el hardware de la GPU.

1. Desplegar el complemento:

```
kubectl create -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/v0.17.1/deployments/static/nvidia-device-plugin.yml
```

1. Realice la verificar de que el complemento se está ejecutando:

```
kubectl -n kube-system get ds nvidia-device-plugin-daemonset

kubectl -n kube-system get pods -l name=nvidia-device-plugin-ds -o wide
```

1. Confirme que el recurso de GPU es anunciado por el nodo. Reemplace <GPU_NODE_NAME> con el nombre específico de su nodo:

```
kubectl describe node <GPU_NODE_NAME> | grep -E "nvidia.com/gpu|Capacity|Allocatable" -n
```

Resultado esperado: El nodo muestra `nvidia.com/gpu` en **Capacity/Allocatable**.

Reservar nodos GPU para cargas de trabajo GPU (Recomendado)

Para asegurar que los nodos GPU se reserven para tareas específicas, aplique etiquetas y taints.

Etiquetar nodos GPU para la programación de espacios de trabajo

Aplique una etiqueta al nodo para la programación de espacios de trabajo:

```
kubectl label node <GPU_NODE_NAME> strong.network/type=workspace
```

Aplicar taints a los nodos GPU para evitar cargas de trabajo que no sean GPU

Aplique un taint para evitar que las cargas de trabajo que no sean GPU se programen en estos nodos:

```
kubectl taint node <GPU_NODE_NAME> nvidia.com/gpu=present:NoSchedule
```

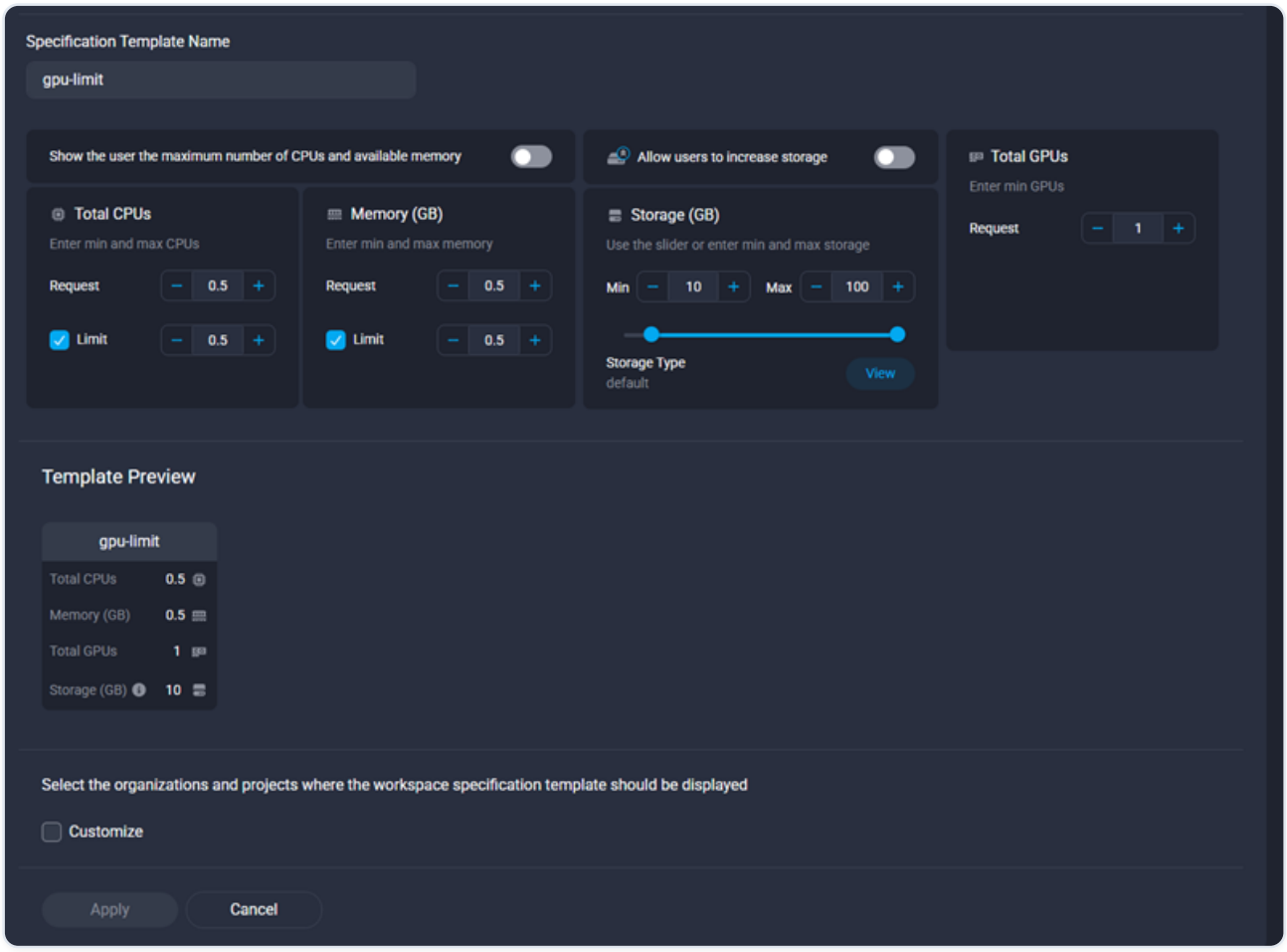
NOTA:

Los pods de espacio de trabajo habilitados para GPU deben incluir una tolerancia coincidente para que puedan programarse en estos nodos.

Crear una plantilla de espacio de trabajo SecurSpaces habilitada para GPU

En su portal de administración, cree o actualice una plantilla de espacio de trabajo que solicite recursos de GPU. Asegúrese de configurar:

- GPU: 1 (o el valor requerido para su carga de trabajo).
- Límites de recursos: Tamaño de CPU, memoria y disco apropiado para las tareas de GPU.



Crear el espacio de trabajo SecurSpaces

Seleccione su plantilla habilitada para GPU para crear un nuevo espacio de trabajo.

Validar la asignación de GPU (Kubernetes)

Una vez implementado el espacio de trabajo, verificar que la GPU está correctamente asignada y accesible.

Confirmar que el pod del espacio de trabajo se está ejecutando en un nodo GPU

verificar que el pod del espacio de trabajo se está ejecutando en un nodo GPU designado:

```
kubectl get pod <workspace-pod> -n <namespace> -o wide
```

Resultado esperado:

- **Estado**: `Running`
- **Nodo**: Nodo con capacidad de GPU.

Confirmar que la GPU es solicitada por el contenedor de la carga de trabajo

```
kubectl describe pod <workspace-pod> -n <namespace>
```

Resultado esperado:

- El contenedor principal del espacio de trabajo incluye nvidia.com/gpu: 1 en solicitudes/límites
- El pod tiene la tolerancia necesaria (si los nodos GPU están contaminados)

Validar el acceso a la GPU dentro del espacio de trabajo de SecurSpaces

Desde el terminal del contenedor del espacio de trabajo de SecurSpaces, ejecute:

```
nvidia-smi
```

Resultado esperado:

- Se muestran los detalles de la GPU NVIDIA (modelo, versión del controlador, utilización).

```
developer@ws-245925371265100-0:~$ nvidia-smi
Tue Mar  3 10:58:04 2026
+-----------------------------------------------------------------------------------------+
| NVIDIA-SMI 580.95.05              Driver Version: 580.95.05      CUDA Version: 13.0     |
+-----------------------------------------+------------------------+----------------------+
| GPU  Name                 Persistence-M | Bus-Id          Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf          Pwr:Usage/Cap |           Memory-Usage | GPU-Util  Compute M. |
|                                         |                        |               MIG M. |
|=========================================+========================+======================|
|   0  NVIDIA A100 80GB PCIe          Off |   00000001:00:00.0 Off |                    0 |
| N/A   34C    P0             43W /  300W |       0MiB /  81920MiB |      0%      Default |
|                                         |                        |             Disabled |
+-----------------------------------------+------------------------+----------------------+

+-----------------------------------------------------------------------------------------+
| Processes:                                                                              |
|  GPU   GI   CI              PID   Type   Process name                        GPU Memory |
|        ID   ID                                                               Usage      |
|=========================================================================================|
|  No running processes found                                                             |
+-----------------------------------------------------------------------------------------+
developer@ws-245925371265100-0:~$
developer@ws-245925371265100-0:~$
developer@ws-245925371265100-0:~$ lspci | grep -i vga
bash: lspci: command not found
developer@ws-245925371265100-0:~$ nvidia-smi -q

==============NVSMI LOG==============

Timestamp                                 : Tue Mar  3 10:58:45 2026
Driver Version                            : 580.95.05
CUDA Version                              : 13.0

Attached GPUs                             : 1
GPU 00000001:00:00.0
    Product Name                          : NVIDIA A100 80GB PCIe
    Product Brand                         : NVIDIA
    Product Architecture                  : Ampere
    Display Mode                          : Requested functionality has been deprecated
    Display Attached                      : Yes
    Display Active                        : Disabled
    Persistence Mode                      : Disabled
    Addressing Mode                       : None
    MIG Mode
```

Solución de problemas

Kubernetes no detecta las GPU

Si el complemento del dispositivo se está ejecutando pero la capacidad de la GPU no es visible en los nodos (común después de cambios en el grupo de nodos), reinicie el tiempo de ejecución del nodo y vuelva a implementar el complemento:

```
kubectl debug <GPU_NODE_NAME> -it --image=ubuntu -- chroot /host systemctl
restart containerd

kubectl delete daemonset -n kube-system nvidia-device-plugin-daemonset

kubectl create -f https://raw.githubusercontent.com/NVIDIA/k8s-device-
plugin/v0.17.1/deployments/static/nvidia-device-plugin.yml
```

Luego, vuelva a verificar la capacidad del nodo:

```
kubectl describe node <GPU_NODE_NAME> | grep -E "nvidia.com/gpu|Capacity|
Allocatable" -n
```

Problemas comunes

PROBLEMA	CAUSA POTENCIAL
Pod pendiente: “Insufficient nvidia.com/gpu”	No hay suficientes GPU libres en el grupo de nodos, o el pod está solicitando más GPU de las esperadas.
El pod se programa, pero nvidia-smi falla	El controlador/complemento del dispositivo no funciona correctamente, o la imagen del contenedor carece de las herramientas NVIDIA necesarias.
El pod no se programará en nodos GPU	Los nodos GPU están contaminados pero el pod carece de la tolerancia requerida, o los selectores/afinidad de nodos impiden la programación.
Los recursos de GPU no son visibles dentro del contenedor	El complemento de dispositivo NVIDIA no se está ejecutando correctamente, o la imagen del contenedor carece de las bibliotecas NVIDIA necesarias.

Upgrade

Actualice SecurSpaces ejecutando el instalador basado en Docker, preparando la base de datos interna si usa Percona, y aplicando el comando Helm impreso por el instalador.

Para una actualización de SDS 2026.9 al gráfico con Percona Operator 1.23.0, ejecute el script de actualización de Percona suministrado **antes** de Helm. Percona admite actualizaciones de operador de una versión menor a la vez. El script lleva la base de datos a través de 1.21.2 y 1.22.0; Helm completa la actualización a 1.23.0.

Las implementaciones que utilizan MongoDB externo siguen el flujo habitual del instalador y Helm sin el paso de Percona.

Requisitos previos

Antes de iniciar la actualización, asegúrese de lo siguiente:

- Una copia de seguridad reciente de la base de datos de configuración de SecurSpaces. Consulte Realizar copia de seguridad de la base de datos.
- Acceso al terminal con Docker instalado.
- El directorio de trabajo actual `${PWD}` contiene el archivo de configuración correcto para su implementación existente.
- Permisos necesarios para ejecutar Docker y aplicar actualizaciones de Helm a su clúster.
- El contexto de Kubernetes está configurado correctamente.
- Para Percona interno, `kubectl` y permiso para aplicar definiciones de recursos personalizados (CRD) con ámbito de clúster, actualizar el Deployment del operador y el recurso personalizado de la base de datos, y acceder a los pods de la base de datos para la copia de seguridad.
- Espacio en el directorio de trabajo para el archivo `mongodump` escrito por el script de actualización.
- Solo el operador de Percona previsto supervisa esta base de datos. Compruebe si hay otros operadores supervisando todos los espacios de nombres.

Ejecutar el instalador

Inicie el instalador para la versión de destino. Reemplace `<target-version>` con la versión del instalador que suministra el gráfico con Percona Operator 1.23.0:

```
docker run -it --rm -v ${PWD}:/strong-network/shared \

  strongnetwork/strong_installer:<target-version>
```

Nota:

`${PWD}` se refiere a su directorio de trabajo actual. Este directorio debe contener el archivo de configuración utilizado en su implementación actual.

Ejecutar el comando de actualización

Una vez dentro del contenedor Docker, ejecute el comando de actualización utilizando su archivo de configuración existente:

```
sds-cli upgrade -c config_<your-current-version>.yaml
```

Ejemplo:

```
sds-cli upgrade -c config_2026.9.0.yaml
```

El instalador descarga el nuevo chart, actualiza la configuración, imprime el comando `helm upgrade --install ... release` habitual y envía las imágenes. No hay nuevas preguntas de Percona en `sds-cli upgrade`.

Si `platform.deployPerconaMongoDB` no está configurado o `true`, también copia el kit de actualización de Percona en `/strong-network/shared/percona-upgrade/` e imprime las instrucciones de actualización, restauración y eliminación de copias de seguridad. El kit contiene tres scripts y los CRD para 1.21.2 y 1.22.0. Una nueva ejecución reemplaza esta copia para que los scripts coincidan con la versión del instalador. El directorio está disponible como `./percona-upgrade/` en el host a través del montaje del directorio compartido.

Para MongoDB externo (`platform.deployPerconaMongoDB: false`), el kit y las instrucciones de Percona se omiten.

Preparar Percona MongoDB interno para 1.23

Ejecute este paso después de que `sds-cli upgrade` finalice y antes del comando Helm impreso. Utilice un terminal con acceso al clúster y trabaje desde el directorio compartido que contiene el chart y `percona-upgrade/`.

El script toma el espacio de nombres, el nombre de la versión de Helm y la ruta del archivo del gráfico, en ese orden:

```
./percona-upgrade/upgrade-percona.sh <namespace> <release> ./ninjahchart-<version>.tgz
```

Para el espacio de nombres `default` y la versión `release`:

```
./percona-upgrade/upgrade-percona.sh default release ./ninjahchart-<version>.tgz
```

El script:

1. Sale con "nada que hacer" si la base de datos ya está en 1.23.
2. Comprueba que el gráfico proporcionado contiene los CRD 1.23.
3. Le pide que introduzca `yes`, espera a que la base de datos esté `ready`, y escribe una copia de seguridad `mongodump` en el directorio actual. Conserve este archivo hasta que haya validado la plataforma.
4. Actualiza a través de las versiones intermedias que se indican a continuación. En cada paso, aplica los CRD de esa versión, establece la imagen del operador, parchea el recurso personalizado de la base de datos (`crVersion`, imagen de MongoDB e imagen de PBM), y espera a `ready` con cada pod de la base de datos en la nueva imagen.
5. Aplica los CRD 1.23 del gráfico y escala el operador antiguo a `0`, listo para que Helm inicie la versión 1.23.0.

ETAPA	OPERADOR Y BASE DE DATOS `CRVERSION`	VERSIÓN DE LA IMAGEN DE MONGODB
Implementación inicial (SDS 2026.9)	1.20.1	7.0.26-14
Primer paso del script	1.21.2	7.0.28-15
Segundo paso del script	1.22.0	7.0.30-16
Actualización final de Helm	1.23.0	7.0.37-20

Los CRD deben aplicarse fuera de Helm. Helm 3 no actualiza los CRD existentes. La ejecución del script realiza estas actualizaciones explícitas de CRD, incluidos los CRD 1.23 necesarios antes de la actualización final de Helm.

Cada paso de la versión es un reinicio gradual. Espere una pausa de escritura de hasta unos 15 segundos por paso; planifique la ventana de actualización en consecuencia.

Aplicar la actualización de Helm

Una vez que el script de Percona se complete correctamente, ejecute el comando de Helm impreso por el instalador. Para MongoDB externo, ejecútelo directamente después de que el instalador finalice.

Helm inicia Percona Operator 1.23.0, que mueve la base de datos a `crVersion: 1.23.0`, MongoDB `7.0.37-20`, y PBM `2.15.0`.

El gráfico bloquea una implementación de Percona existente que no ha alcanzado la versión 1.22 o carece de los CRD 1.23 requeridos. Una implementación 1.23 ya actualizada puede someterse a actualizaciones posteriores de Helm.

Verificación posterior a la actualización

Una vez aplicada la actualización de Helm:

- verificar que todos los pods están en ejecución y en buen estado:

```
kubectl get pods -n <your-namespace>
```

- Compruebe la disponibilidad del servicio y los registros:

```
kubectl logs <pod-name> -n <your-namespace>
```

- Confirme que la versión de la plataforma se ha actualizado correctamente.
- Para Percona, confirme que la base de datos es `ready`, `crVersion` es `1.23.0`, y que los pods de la base de datos usan MongoDB `7.0.37-20` y PBM `2.15.0`:

```
kubectl get psmdb <release>-psmdb-db -n <namespace>

kubectl get psmdb <release>-psmdb-db -n <namespace> -o yaml

kubectl get pods -n <namespace> -o wide
```

- Inicie sesión como administrador de la plataforma y confirme que las organizaciones, los proyectos y los servicios están disponibles.
- Si las copias de seguridad están habilitadas, confirme que se siguen completando y que se conservan la configuración de almacenamiento, programación y PITR . Para copias de seguridad de GCS sin clave, consulte Realizar copia de seguridad de la base de datos.

Limpiar o restaurar la copia de seguridad de la actualización

Después de la validación de la plataforma, elimine la copia de seguridad de la actualización del directorio donde ejecutó el script:

```
./percona-upgrade/delete-percona-backup.sh
```

Si necesita recuperar los datos, utilice el script de restauración con el archivo creado durante la actualización:

```
./percona-upgrade/restore-percona-backup.sh default release
<backup>.archive.gz
```

Sustituya `default` y `release` por su espacio de nombres y la versión de Helm. Esto restaura **solo los datos**; no degrada el operador, los CRD, MongoDB o PBM. Siga las instrucciones de quiescencia y validación en Restaurar la base de datos.

Solución de problemas

Helm bloquea la actualización de Percona

Ejecutar Helm antes de preparar Percona puede producir el siguiente error (ajustado aquí para facilitar la lectura):

```
Error: UPGRADE FAILED: execution error at (ninjahchart/templates/percona-
instance.yaml:14:4):

The Percona MongoDB database protein-psmdb-db is on operator version
1.20.1 with CRDs unknown.

This chart needs it on 1.22 or later with CRDs 1.23:

run percona-upgrade/upgrade-percona.sh from the SDS installer first.
```

Ejecute `upgrade-percona.sh` con el espacio de nombres, la versión y el nuevo gráfico correctos, luego vuelva a ejecutar el comando Helm . No omita las versiones intermedias del operador ni las actualizaciones explícitas de CRD.

Operadores de Percona en conflicto

Si la base de datos no se establece en la versión esperada o no está lista, compruebe si otro operador de Percona supervisa el mismo espacio de nombres, incluidos los operadores configurados para supervisar todos los espacios de nombres. Un operador sobrante puede reconciliar la base de datos a una configuración en conflicto. Identifique y escale el operador no deseado a `0` antes de continuar.

Otros problemas de actualización

Si encuentra problemas durante la actualización:

- Revise la salida del instalador en busca de mensajes de error.
- Asegúrese de que su archivo de configuración coincide con el formato esperado.
- Compruebe los registros de Docker y Kubernetes para obtener contexto adicional.

Administer

Esta sección está dirigida a **administradores de plataforma** que ejecutan Citrix SecurSpaces™ para toda la organización. Cubre todo lo que se configura una vez y se aplica en todas partes: quién puede iniciar sesión, qué pueden hacer los espacios de trabajo, qué sistemas externos están conectados y cómo se licencia y supervisa la plataforma.

La mayoría de las tareas aquí requieren derechos de administrador de plataforma. Algunas áreas sensibles a la seguridad necesitan el rol de oficial de seguridad.

Si está configurando la plataforma por primera vez, instálela primero — consulte Implementar.

Empiece aquí

TAREA	PÁGINA
Encuentre la configuración a nivel de plataforma y lo que cubre cada área	Configuración del sistema
Cargar una licencia y activar las funciones de la plataforma	Licencias
Administrar la configuración de la plataforma como código	Proveedor de Terraform
Permitir agentes de codificación de IA de forma segura	Ejecutar agentes de codificación de IA en espacios de trabajo

Incorporación de personas

TAREA	PÁGINA
Conectar un proveedor de identidades y sincronizar usuarios	Identidad y acceso
Conceder roles de toda la plataforma, como el de oficial de seguridad	Roles de la plataforma

TAREA	PÁGINA
Controlar quién puede acceder a la plataforma	Control de acceso de usuarios

Establecer las reglas

TAREA	PÁGINA
Configurar opciones y valores predeterminados de toda la plataforma	Configuración de la plataforma
Establecer lo que los espacios de trabajo pueden hacer	Política de espacio de trabajo
Controlar cuándo los espacios de trabajo se pausan y se eliminan	Ciclo de vida del espacio de trabajo y detección de inactividad
Restringir el movimiento de datos y aplicar opciones de seguridad	Configuración de seguridad

Conexión de otros sistemas

TAREA	PÁGINA
Conectar repositorios, registros y herramientas de terceros	Integraciones
Proporcionar acceso al registro y versiones de IDE	Recursos de la plataforma
Preparar el almacenamiento para los puntos de montaje	Almacenamiento

Ejecución de la plataforma

TAREA	PÁGINA
Revisar licencias, análisis y uso	Operaciones

TAREA	PÁGINA
Dimensionar, hacer copias de seguridad y restaurar la base de datos	La base de datos de SecurSpaces
Revisar eventos de auditoría y reenviarlos a un SIEM	Auditoría
Ver cómo se asignan y consumen los recursos	Perspectivas
Servir espacios de trabajo desde más de una región	Regiones

System configuration

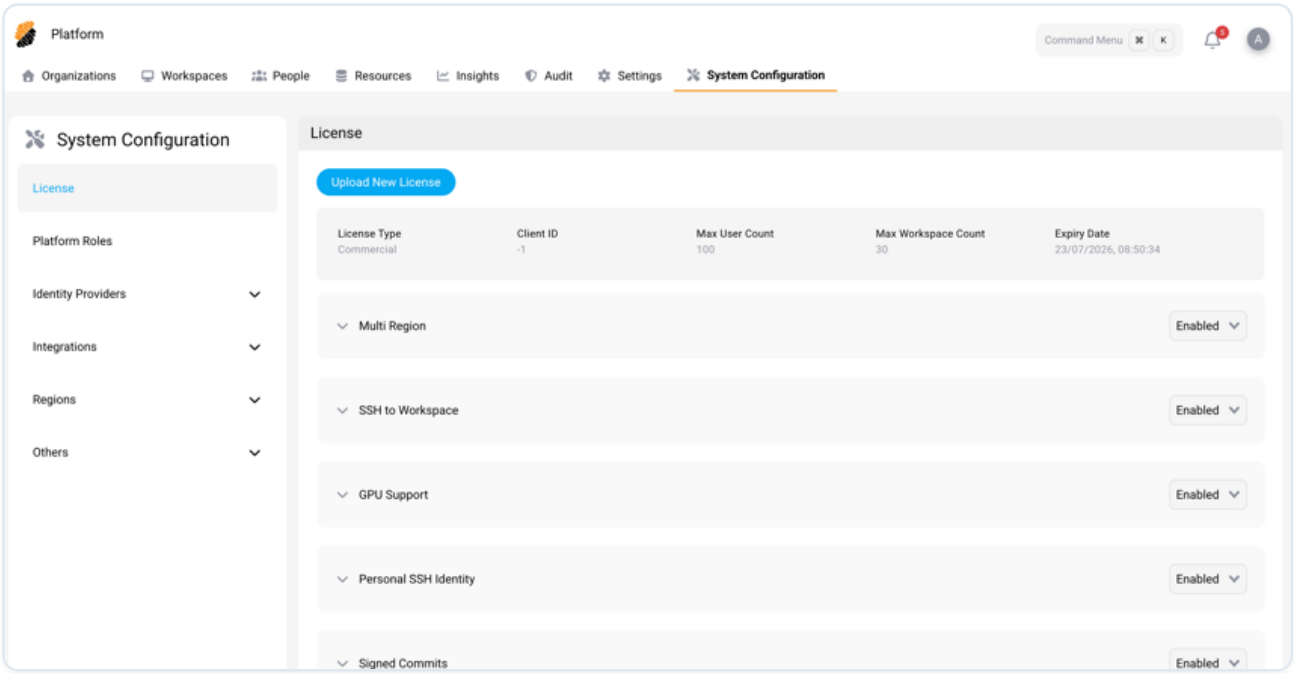
La **Configuración del sistema** es donde se gestiona Citrix SecurSpaces™ a nivel de plataforma. Desde un único lugar, puede gestionar su licencia y sus funciones, asignar roles de plataforma, conectar proveedores de identidad, activar integraciones, configurar regiones y ajustar algunas otras opciones de toda la plataforma.

> **Nota:**
>
> Solo los administradores de la plataforma pueden abrir la Configuración del sistema. Es independiente de la **Configuración de la plataforma**, que abarca otras opciones de toda la plataforma, como la configuración general, la configuración de seguridad y los análisis.

Abrir la Configuración del sistema

Inicie sesión como administrador de la plataforma y seleccione **Configuración del sistema** en la barra de navegación superior. Se abre en la página **Licencia**.

Para ir directamente, vaya a `https://<your-sds-hostname>/platform/system_configuration`.



Áreas de configuración

La navegación izquierda agrupa todo en estas áreas:

ÁREA	QUÉ SE HACE AQUÍ
Licencia	Cargue su licencia, revise lo que cubre y active o desactive las funciones de la plataforma.
Roles de plataforma	Asigne a usuarios y grupos roles de toda la plataforma, como el de oficial de seguridad.
Proveedores de identidad	Conecte proveedores de OAuth, SAML y SCIM para que los usuarios inicien sesión y se sincronicen automáticamente.
Integraciones	Conecte repositorios de código, aplicaciones de terceros, almacenamiento y Citrix DaaS™.
Regiones	Agregue regiones y nodos cálidos para implementaciones multirregión.
Otros	Configure la puerta de enlace de correo electrónico, el contacto de violación de datos, la clave del servidor SSH, los términos de servicio y las etiquetas de proyecto.

Información relacionada

- Roles de plataforma
- Configuración de la plataforma
- Roles y permisos

Terraform provider

Citrix SecurSpaces™ publica un proveedor de Terraform para que la configuración de la plataforma se pueda gestionar como código en lugar de a través de la consola. Es útil cuando se crean proyectos y plantillas repetidamente, cuando la configuración debe revisarse antes de aplicarse, o cuando una auditoría necesita un registro de quién cambió qué.

El proveedor gestiona objetos de la plataforma. No implementa la plataforma en sí misma; para ello, consulte Instalar con la CLI de Strong Installer.

Qué gestiona

RECURSO	GESTIONA
`strong_user`	Usuarios de la plataforma
`strong_organization`	Organizaciones y su propietario
`strong_project`	Proyectos, su propietario y sus miembros
`strong_user_group`	Grupos de usuarios y su pertenencia
`strong_workspace_template`	Plantillas de espacio de trabajo, incluidas especificaciones, imágenes, scripts, secretos, aplicaciones y configuraciones de seguridad

Obtener el proveedor

El proveedor se distribuye a través de su implementación de SecurSpaces en lugar del Registro público de Terraform, por lo que lo descarga con el mismo contenedor de instalador que utiliza para las actualizaciones. El acceso está vinculado a su derecho de plataforma.

1. Ejecute el contenedor del instalador como se describe en Instalar con la CLI de Strong Installer.
2. Obtenga el proveedor:

```
sds-cli get-terraform -d <your-sds-hostname>
```

La versión más reciente se descarga en el directorio compartido. Añada `-v <version>` para seleccionar una específica, o `--verbose` para listar primero las disponibles.

3. Instálelo donde Terraform busca proveedores locales y márquelo como ejecutable:

```
mkdir -p ~/.terraform.d/plugins/strong.network/strong-network/strong/
<version>/linux_amd64/

cp terraform-provider-strong-<version> \

  ~/.terraform.d/plugins/strong.network/strong-network/strong/
<version>/linux_amd64/terraform-provider-strong

chmod +x ~/.terraform.d/plugins/strong.network/strong-network/strong/
<version>/linux_amd64/terraform-provider-strong
```

Nota:

Dado que el proveedor se instala desde el sistema de archivos en lugar de un registro, `terraform init` no verificar una suma de comprobación para él. Obténgalo a través de `sds-cli` en lugar de copiarlo entre máquinas, y mantenga la versión que implementó registrada con el resto de su código de infraestructura.

Configurar el proveedor

Declare el proveedor y apúntelo a su implementación:

```
terraform {

  required_providers {

    strong = {

      source  = "strong.network/strong-network/strong"

      version = "<version>"
```

```
    }
  }
}


provider "strong" {
  api_token      = var.api_token
  deployment_url = var.deployment_url
}
```

ARGUMENTO	OBLIGATORIO	DESCRIPCIÓN
`api_token`	Sí	Una clave API de plataforma. Cree una en **Perfil > Seguridad > Claves API**
`deployment_url`	Sí	La URL de su implementación de SecurSpaces

El token está marcado como sensible por el proveedor, por lo que Terraform no lo imprime. Suminístrelo a través de una variable o del entorno en lugar de escribirlo en un archivo, y concédale solo los permisos que la configuración necesita — consulte Roles y permisos.

Recursos

`strong_user`

ARGUMENTO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`email`	cadena	Sí	La dirección de correo electrónico del usuario

ARGUMENTO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`user_type`	entero	Sí	`1` para un administrador, `3` para un desarrollador
`identity_provider`	entero	Sí	El proveedor de identidad, como valor numérico. `1` Google, `2` Microsoft, `3` SAML, `7` OIDC genérico, `0` ninguno
`full_name`	cadena	No	El nombre completo del usuario

`strong_organization`

ARGUMENTO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`name`	cadena	Sí	El nombre de la organización
`owner_id`	cadena	Sí	El ID de usuario o el correo electrónico del propietario

`strong_project`

ARGUMENTO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`name`	cadena	Sí	El nombre del proyecto
`owner_id`	cadena	Sí	El ID de usuario o correo electrónico del propietario

ARGUMENTO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`organization_id`	cadena	Sí	La organización a la que pertenece el proyecto
`member`	lista de bloques	No	Miembros del proyecto. Cada bloque toma `id` y `role`

`strong_user_group`

ARGUMENTO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`name`	cadena	Sí	El nombre del grupo
`description`	cadena	No	Una descripción del grupo
`members`	conjunto de cadenas	No	ID de usuario en el grupo

`strong_workspace_template`

El recurso más grande. Cubre lo que una plantilla define en la consola, incluyendo:

- **Identidad y alcance** — `name`, `project_id`, `version`, `description`, `region_id`
- **Imagen** — `workspace_image` con `id` y `tag`
- **Recursos** — `workspace_specs` con `cpu`, `memory` y `disk`
- **Inicio** — `before_startup_script`, `after_startup_script`, `default_folder`
- **Secretos** — `injected_secrets_as_env`, `injected_secrets_as_file` y equivalentes locales que toman `secret_name` y `content`
- **Aplicaciones** — `workspace_apps` con `port`, `name` y `use_https`
- **Seguridad** — `policy_ids` para políticas de red, `apps_security`, `personal_ssh_identity`, `workspace_access_items`
- **Portapapeles** — `clipboard_settings`, que cubre `monitor`, `clipboard_restricted`, restricciones de pegado, límites de caracteres y `enable_supervised_copy`
- **Programación** — `workspace_schedule`, `timeout_outside_schedule`, `idle_timeout`

Para saber qué hace cada configuración, consulte Plantillas de espacio de trabajo.

Ejemplo

Creación de una organización, un proyecto dentro de ella y un grupo:

```
resource "strong_user" "lead" {

  email             = "team-lead@example.com"

  user_type         = 3

  full_name         = "Team Lead"

  identity_provider = 3

}



resource "strong_organization" "engineering" {

  name     = "engineering"

  owner_id = strong_user.lead.id

}



resource "strong_project" "platform" {

  name            = "platform-services"

  owner_id        = strong_user.lead.id

  organization_id = strong_organization.engineering.id

}



resource "strong_user_group" "reviewers" {
```

```
  name        = "reviewers"
  description = "Engineers who review platform changes"
  members     = [strong_user.lead.id]
}
```

Aplícalo de la forma habitual:

```
terraform init
terraform plan
terraform apply
```

Cada recurso admite la importación, para que puedas incorporar objetos que ya existen bajo la gestión de Terraform con `terraform import`.

Información relacionada

- Referencia de la CLI de SDS
- API
- Plantillas de espacio de trabajo
- Roles y permisos

Run AI coding agents in workspaces

Los desarrolladores ejecutan cada vez más agentes de codificación de IA que editan archivos, ejecutan comandos, instalan paquetes y llaman a servicios externos en su nombre. Un agente que hace eso en un portátil está en gran medida sin gobernar. Ejecutarlo dentro de un espacio de trabajo de Citrix SecurSpaces™ le aplica los mismos controles que ya se aplican al desarrollador.

Los agentes se utilizan de dos maneras, y la diferencia determina cuánto de esta página se aplica a usted:

MODO	QUÉ ASPECTO TIENE
Asistido	Un desarrollador abre su espacio de trabajo en el IDE en la nube o en un IDE local y ejecuta un agente desde dentro, observando lo que hace
No asistido	Una canalización o un orquestador crea un espacio de trabajo, un agente se ejecuta por sí solo y el resultado se recopila posteriormente

El uso asistido es donde la mayoría de los equipos comienzan y no necesita ninguna configuración especial: el espacio de trabajo que un desarrollador ya tiene aplica sus controles al agente automáticamente. Las ejecuciones desatendidas requieren más decisiones, y la mayor parte de esta página trata sobre ellas.

Esta página es para administradores de plataforma. Cubre lo que un agente puede alcanzar, cómo evitar que las ejecuciones concurrentes colisionen, cuánto cuesta y lo que se puede ver después.

Por qué un espacio de trabajo es el límite adecuado

Un agente hereda el entorno en el que se ejecuta. En un punto final, eso significa las credenciales del desarrollador, todo su sistema de archivos y acceso a la red sin restricciones.

En un espacio de trabajo, el límite ya está establecido:

- **Las credenciales se gestionan, no se retienen.** Las credenciales de repositorio y servicio se inyectan en tiempo de ejecución y permanecen en la plataforma. Un agente las utiliza sin poder leerlas y sin que lleguen nunca al punto final.
- **La salida está controlada por políticas.** Un agente solo llega a los destinos que permite la política de red del espacio de trabajo, por lo que un agente que decida obtener un paquete de un host inesperado no podrá hacerlo.
- **El sistema de archivos está delimitado.** El agente ve el espacio de trabajo, no la máquina del desarrollador.
- **Todo está auditado.** La actividad del agente produce los mismos eventos de auditoría que la actividad del desarrollador.

Agentes asistidos

Un desarrollador ejecuta un agente dentro del espacio de trabajo de la misma manera que lo haría en un portátil: abre el espacio de trabajo, inicia Copilot, Claude Code, Cursor, o lo que el equipo utilice, y trabaja junto a él. Ambos métodos de conexión lo admiten: el IDE en la nube en una pestaña del navegador, o un IDE local conectado a través de SSH. Consulta Elige cómo conectarte.

No se requiere nada adicional para gobernarlo. El agente se ejecuta como el usuario del espacio de trabajo, por lo que hereda la política de red, las credenciales intermediadas, el rol y las reglas del portapapeles que ya se aplican a ese desarrollador, y su tráfico de IA se atribuye como cualquier otro. Un administrador decide esos controles una vez, en la plantilla; el desarrollador no puede optar por participar ni por no participar.

Hay dos cosas que vale la pena configurar para que los desarrolladores no estén luchando contra el entorno:

- **Las herramientas del agente pertenecen a la imagen o a un** script de inicio, no a la configuración manual de cada desarrollador. Los agentes CLI instalados en una ruta del sistema, y las extensiones de VS Code suministradas como archivos `.vsix`, están disponibles en el momento en que se inicia un espacio de trabajo. Consulta Administrar imágenes de espacio de trabajo.
- **El punto de conexión del modelo debe ser accesible.** Un agente que no puede alcanzar a su proveedor falla de maneras que parecen un espacio de trabajo roto. Incluye el punto de conexión en la política de red, o enrútalo a través de la puerta de enlace.

> **Nota:**
>
> Los controles de protección de datos son más débiles cuando un desarrollador conecta un IDE local a través de SSH que cuando utiliza el IDE en la nube, porque el contenido sale de la sesión del navegador. Cuando eso importa, gobiérnalo por política. Consulta Controles por capas.

Agentes no asistidos

El resto de esta sección se refiere a ejecuciones que nadie está observando. Si tus desarrolladores solo usan agentes de forma interactiva, los controles anteriores ya están haciendo su trabajo.

Aislar una ejecución de otra

Los agentes que se ejecutan en paralelo y comparten un directorio de trabajo interfieren entre sí: ediciones en conflicto, puertos en colisión y cambios de dependencia realizados para una tarea que rompen otra.

Asigna a cada ejecución concurrente su propio espacio de trabajo. Un espacio de trabajo es un contenedor con su propio sistema de archivos, su propio espacio de procesos y su propia identidad de red, por lo que dos ejecuciones no pueden colisionar.

Cree cada uno a partir de una plantilla de espacio de trabajo, de modo que la imagen, los recursos, las credenciales, los scripts y la política se definan una sola vez y cada ejecución comience de forma idéntica.

Las plantillas se pueden gestionar como código con el proveedor de Terraform. El proveedor gestiona plantillas, proyectos, usuarios, grupos y organizaciones; no crea espacios de trabajo individuales, por lo que la creación por ejecución utiliza la API o la interfaz de usuario.

La API REST crea espacios de trabajo cuando una canalización o un orquestador realiza el desencadenamiento:

PUNTO FINAL	PROPÓSITO
`POST /v1/projects/{project_id}/workspaces/template`	Crear un espacio de trabajo a partir de una plantilla
`POST /v1/projects/{project_id}/workspaces`	Crear un espacio de trabajo a partir de una especificación explícita
`POST /v1/projects/{project_id}/workspaces/{ws_id}/state`	Iniciar o pausar un espacio de trabajo existente
`DELETE` en el espacio de trabajo	Descartar la ejecución

Establezca el estado al crear para que el espacio de trabajo se inicie en ejecución en lugar de pausado, y elimínelo cuando la ejecución finalice.

> **Nota:**

> El aislamiento es por espacio de trabajo, no por sesión dentro de uno. Dos agentes en el mismo espacio de trabajo comparten un sistema de archivos y interferirán. Si la concurrencia importa, cree un espacio de trabajo para cada ejecución.

Iniciar el agente dentro del espacio de trabajo

Crear un espacio de trabajo no ejecuta nada. SecurSpaces no tiene una API para ejecutar un comando en un espacio de trabajo en ejecución, por lo que el agente debe iniciarse desde dentro. Hay dos maneras de organizar esto para una ejecución a la que nadie asiste.

Un script de inicio. Un espacio de trabajo ejecuta un script de pre-inicio antes de que se inicie el IDE y un script de post-inicio una vez que el espacio de trabajo está listo. Coloque la invocación del agente en el script de post-inicio y el espacio de trabajo comenzará la ejecución por sí mismo, sin un disparador externo. Esta es la opción a utilizar para ejecuciones desatendidas. Reserve el script de pre-inicio para la preparación de la que depende el agente, no para el agente en sí, porque un fallo allí puede impedir que el espacio de trabajo se inicie por completo.

Los scripts de inicio se pueden configurar en tres niveles, y para las cargas de trabajo de los agentes, dos de ellos son importantes:

NIVEL	EFECTO
Plantilla	Cada espacio de trabajo creado a partir de la plantilla ejecuta el mismo script. Úselo cuando las ejecuciones sean similares
Espacio de trabajo	El script se establece en el espacio de trabajo individual en el momento de la creación. Úselo cuando cada ejecución necesite un comando diferente

El nivel de espacio de trabajo es lo que permite a un orquestador variar el trabajo por ejecución. Crear un espacio de trabajo a partir de una plantilla hereda el script de la plantilla, mientras que crear uno a partir de una especificación explícita acepta un script de inicio en la solicitud, de modo que el llamador puede proporcionar el comando para esa ejecución sin mantener una plantilla para cada variación.

Para saber cómo configurarlos, consulte Dónde configurar los scripts de inicio.

SSH. Recupere los detalles de conexión del espacio de trabajo de la API, conéctese y ejecute el comando. Utilice esto cuando el orquestador necesite decidir qué ejecutar después de que exista el espacio de trabajo, o para recopilar resultados cuando la ejecución finalice. Consulte Conectarse a través de SSH.

Una ejecución impulsada por un pipeline, por lo tanto, se ve así: cree el espacio de trabajo con un script de post-inicio que inicie el agente, deje que la ejecución continúe, recopile el resultado, elimine el espacio de trabajo.

> **Importante:**
>
> Los scripts de inicio se ejecutan en cada inicio de espacio de trabajo, no solo en el primero. Si la detección de inactividad pausa un espacio de trabajo y este se reanuda más tarde, el script posterior al inicio se ejecuta de nuevo. Haga que el script sea idempotente, o haga que compruebe si la ejecución ya ha finalizado, para que al reanudar un espacio de trabajo no se inicie el trabajo silenciosamente por segunda vez.

Decida a qué puede acceder un agente

Un agente está tan restringido como el espacio de trabajo en el que se ejecuta, así que incorpore la restricción en la plantilla en lugar de confiar en el comportamiento del agente.

Salida de red. Adjunte una política de red que permita solo los destinos que el trabajo necesita — sus repositorios, su registro de artefactos, su punto final de modelo. Un agente no puede exfiltrar datos a un host que la política no permita, independientemente de lo que se le pida que haga.

Credenciales. Utilice recursos del proyecto en lugar de secretos personales para las cargas de trabajo del agente, de modo que la credencial pertenezca al proyecto y pueda rotarse o revocarse sin afectar la cuenta de una persona. Asigne al espacio de trabajo solo los recursos que esa tarea requiera.

Permisos. El espacio de trabajo se ejecuta como un usuario con un rol. Asigne a los espacios de trabajo del agente un rol con los permisos más restringidos que funcionen — consulte Roles y permisos.

Protección de datos. Los controles del portapapeles y de la aplicación del espacio de trabajo se aplican a una sesión de agente como lo hacen a una sesión de desarrollador. Consulte Controles por capas.

Controle lo que cuesta

Las ejecuciones de agentes consumen recursos de cómputo de manera diferente a las personas. Son intermitentes, pueden ejecutarse sin supervisión y un bucle que no termina mantendrá un espacio de trabajo ocupado indefinidamente. Un agente supervisado está limitado por la propia sesión del desarrollador, por lo que esta sección es más relevante para las ejecuciones sin supervisión — con la excepción del gasto de tokens, que se aplica a ambos.

- **Detección de inactividad** pausa un espacio de trabajo que deja de usarse, lo cual es la principal protección contra una ejecución olvidada que genere facturación durante la noche. Consulte Ciclo de vida del espacio de trabajo y detección de inactividad.
- **Especificaciones del espacio de trabajo** limitan la CPU, la memoria y el disco por ejecución. Dimensione las plantillas de agente deliberadamente; un agente no necesita la estación de trabajo completa de un desarrollador.
- **Concurrencia** es lo que impulsa el recuento de nodos, no el número de espacios de trabajo existentes. Consulte Dimensionamiento.

> **Importante:**
>
> Un agente que se ejecuta sin supervisión no se pausará a sí mismo. La detección de inactividad es lo que impide que una ejecución abandonada consuma un nodo hasta que alguien se dé cuenta, así que confirme que está habilitada antes de permitir ejecuciones sin supervisión.

Vea lo que sucedió

Dos fuentes, que responden a diferentes preguntas.

Auditoría registra lo que el agente hizo en la plataforma: inicio y detención del espacio de trabajo, acceso a recursos, eventos de portapapeles y transferencia, y actividad de red monitorizada. Consulte Auditoría.

AI Gateway registra lo que el agente gastó. Cuando el tráfico de IA se enruta a través de una pasarela, SecurSpaces etiqueta cada solicitud con el usuario, proyecto y espacio de trabajo de origen, para que el consumo de tokens pueda atribuirse en lugar de llegar como una única factura no atribuida. Consulte Configurar el enrutamiento de AI Gateway.

Esa atribución es lo que hace que el uso del agente sea manejable: sin ella, solo conocería el total y nada más.

Un punto de partida viable

Si los desarrolladores están ejecutando agentes de forma interactiva, ya ha recorrido la mayor parte del camino. Confirme tres cosas en las plantillas que utilizan:

1. La política de red permite el punto de conexión del modelo, así como sus repositorios y registro.
2. Las herramientas del agente están en la imagen o en un script de inicio, en lugar de que cada desarrollador las instale.
3. El tráfico de IA se enruta a través de la pasarela, para que el consumo se atribuya en lugar de ser anónimo.

Para ejecuciones desatendidas, añada:

1. Una plantilla para ejecuciones de agentes, con una especificación que se ajuste a la carga de trabajo en lugar de al escritorio de un desarrollador.
2. Credenciales con ámbito de proyecto, y no más de lo que la tarea requiere.
3. Detección de inactividad confirmada como habilitada, para que una ejecución abandonada no retenga un nodo.
4. La invocación del agente en un script posterior al inicio, escrito para ser seguro si el espacio de trabajo se reanuda.
5. Un espacio de trabajo por ejecución concurrente, eliminado cuando la ejecución finaliza.

Empiece con una población pequeña y un equipo. La plantilla es lo que hay que hacer bien — una vez que lo esté, cada ejecución la hereda.

Información relacionada

- Dar acceso a la documentación a su asistente de IA
- Configurar el enrutamiento de AI Gateway
- Políticas de red
- Plantillas
- Dimensionamiento
- Conectarse a través de SSH
- Qué persiste en un espacio de trabajo
- API REST

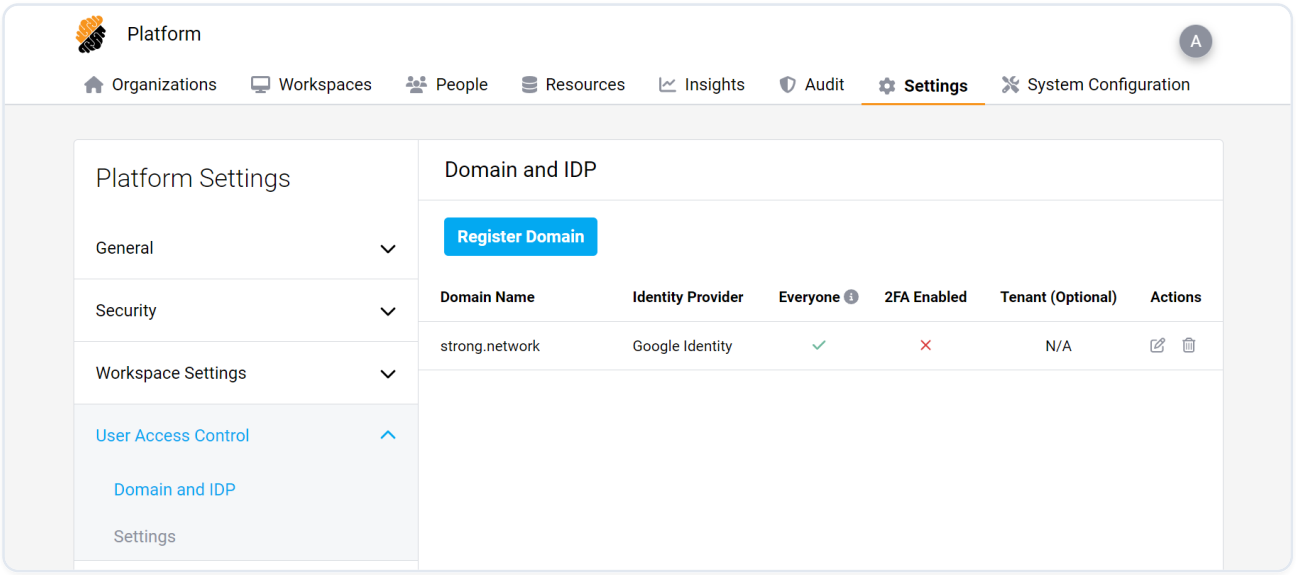
Configure platform login

Configurar inicio de sesión para usuarios

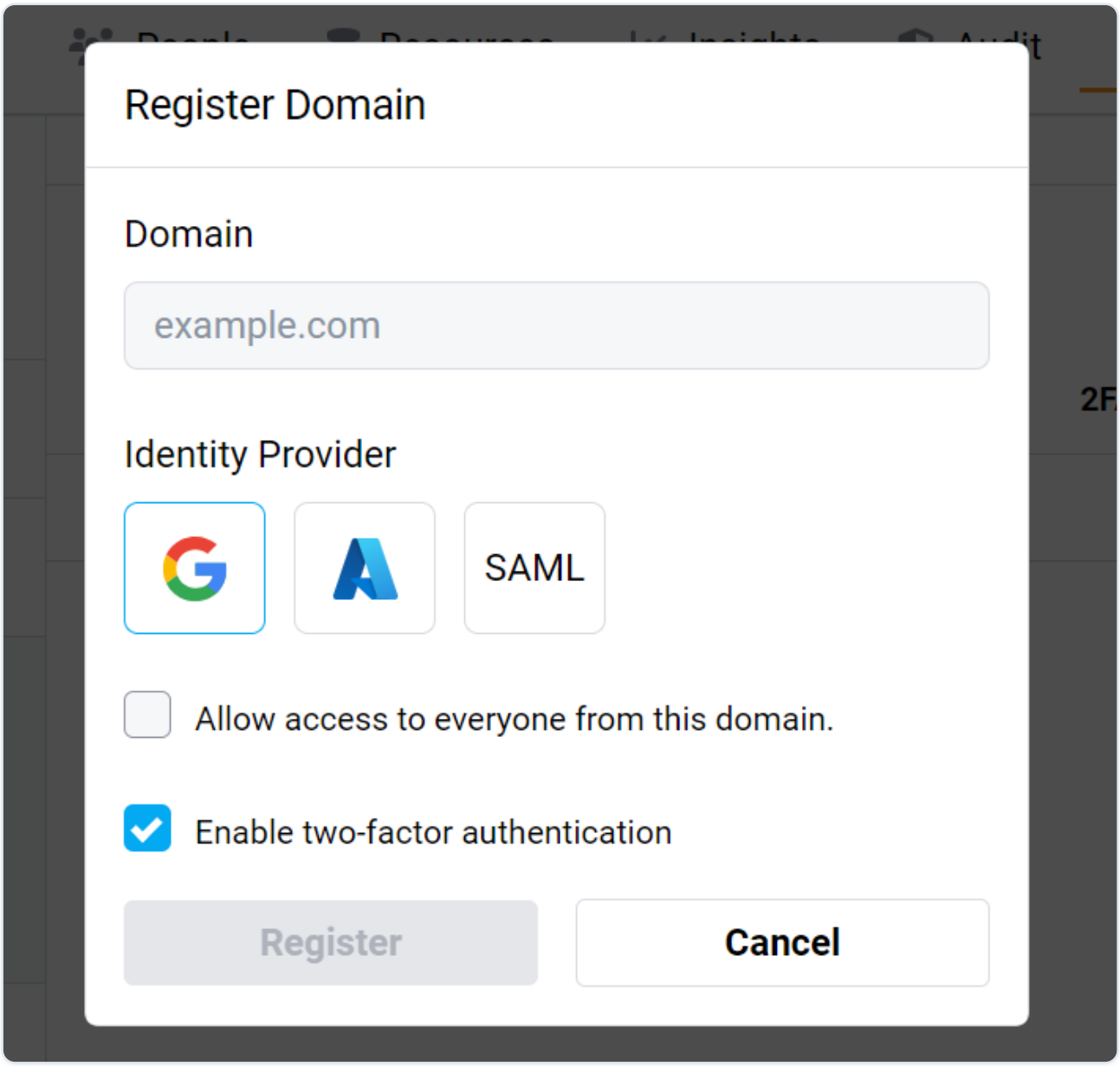
Hay cinco formas en que los usuarios pueden iniciar sesión en la plataforma:

- Proveedor de Google OAuth
- Proveedor de Microsoft OAuth (Azure)
- SAML
- OpenID Connect
- Nombre de usuario y contraseña

Después de configurar el Proveedor de Identidad elegido (cualquiera de las primeras 4 opciones), se puede usar para autenticar usuarios de dominios específicos. Estos se pueden configurar en Control de Acceso de Usuario, en el submenú “Dominio e IDP”.



Si se añade un dominio, significa que al añadir un usuario a la plataforma, ese usuario se autenticará utilizando el Proveedor de Identidad elegido.



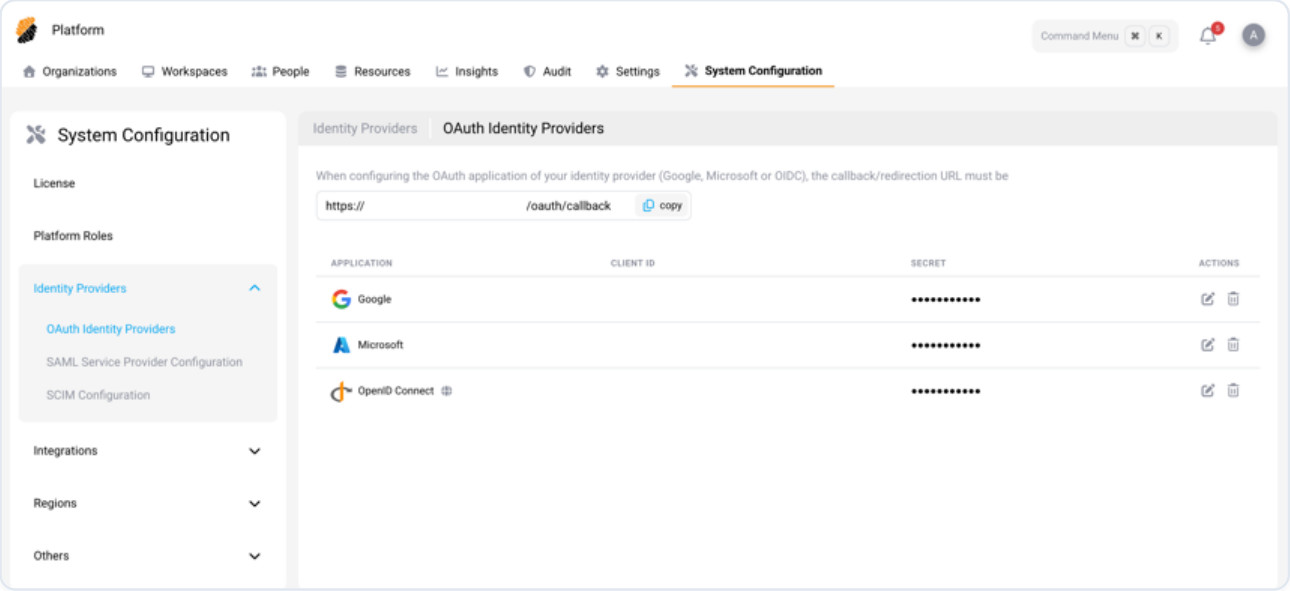
En este menú, puede optar por marcar “Permitir acceso a todos desde este dominio”, lo que creará cuentas de usuario sobre la marcha, sin necesidad de crear la cuenta de antemano. Esto se denomina aprovisionamiento Just-in-Time. Este nuevo usuario no tendrá ninguna organización o proyecto asignado.

También puede habilitar la autenticación de dos factores, que utilizará OTP en cualquier usuario del dominio especificado. Si se desea la autenticación de dos factores, recomendamos configurarla en su Proveedor de Identidad o en la plataforma para evitar pedir al usuario que realice el proceso dos veces.

Identity providers

Permita que sus usuarios inicien sesión con las cuentas que ya tienen y mantenga su lista de usuarios sincronizada automáticamente. En **Proveedores de identidades**, conecte Citrix SecurSpaces™ a los sistemas de identidad de su organización.

Encuentre esta configuración en **Configuración del sistema > Proveedores de identidades**.



Puede configurar tres tipos de proveedor:

- Proveedores de identidades OAuth
- Configuración del proveedor de servicios SAML
- Configuración de SCIM

Proveedores de identidades OAuth

Elija los proveedores OAuth con los que sus usuarios inician sesión, como Google, Microsoft (Azure) o cualquier proveedor de OpenID Connect.

Para configurar uno, siga la guía correspondiente:

- Google OAuth
- Microsoft OAuth
- OpenID Connect

Configuración del proveedor de servicios SAML

Conecte SecurSpaces a su proveedor de identidades SAML para que los usuarios se autentiquen a través de él. Cargue los metadatos de su proveedor desde una URL o un archivo XML, y la plataforma se encargará del resto.

Para obtener instrucciones paso a paso, consulte SAML.

Configuración de SCIM

Mantenga a los usuarios y grupos actualizados sin trabajo manual. Con SCIM, su proveedor de identidad añade y elimina usuarios por usted. Genere un token de autorización aquí y luego déselo a su proveedor de SCIM para vincular ambos.

Para obtener instrucciones paso a paso, consulte SCIM.

Información relacionada

- Configurar el inicio de sesión de la plataforma
- Configuración del sistema

Platform roles

La mayoría del acceso en Citrix SecurSpaces™ se concede a través de roles de proyecto, que se aplican dentro de un único proyecto. Los **roles de plataforma** son diferentes: se aplican en toda la plataforma, independientemente de la organización o el proyecto al que pertenezca la persona.

Los roles de plataforma se asignan en Configuración del sistema, en **Roles de plataforma**. Solo un administrador de plataforma puede abrir esa página.

Roles disponibles

ROL	QUÉ CONCEDE
Oficial de seguridad	Acceso a áreas sensibles a la seguridad, como análisis del sistema y datos de auditoría. Solo un administrador de plataforma puede asignar o eliminar este rol.
Oficial de privacidad de datos	Nombra al contacto para las responsabilidades de privacidad de datos en la plataforma.

El rol de oficial de seguridad también conlleva privilegios que los roles de proyecto no pueden conceder. Por ejemplo, un oficial de seguridad puede activar **Omitir programación** para un espacio de trabajo, de modo que siga ejecutándose en lugar de pausarse cuando esté inactivo. Consulte Detección de inactividad del espacio de trabajo.

Asignar un rol de plataforma

1. Inicie sesión como administrador de plataforma y abra **Configuración del sistema**.
2. Seleccione **Roles de plataforma**.

3. Seleccione el rol que desea asignar.
4. Busque un usuario o grupo y añádalos.

Eliminar un rol de plataforma

1. Abra **Configuración del sistema > Roles de plataforma**.
2. Seleccione el rol y, a continuación, seleccione el usuario o grupo.
3. Confirme la eliminación.

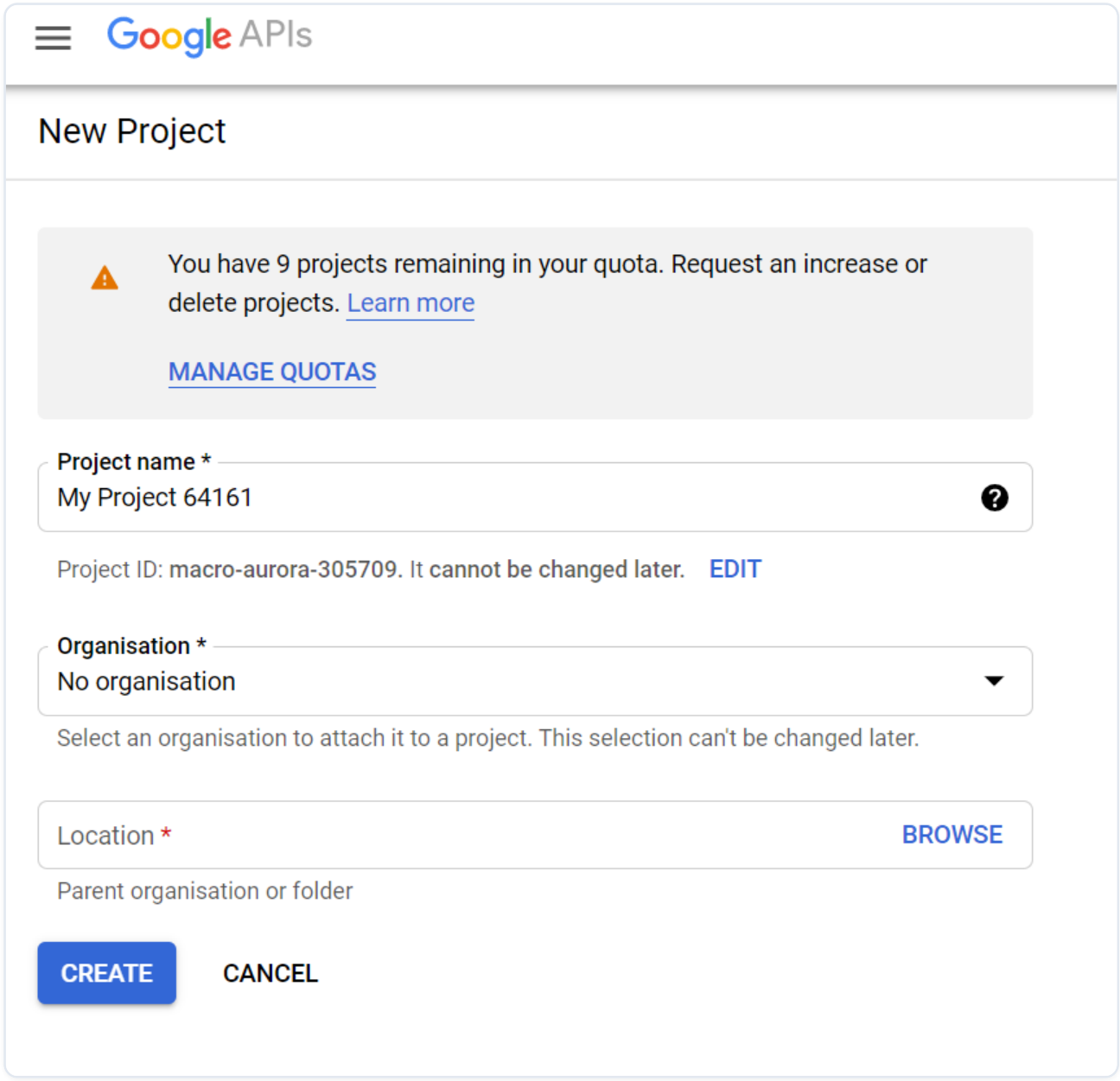
Información relacionada

- Configuración del sistema
- Roles y permisos
- Control de acceso de usuario

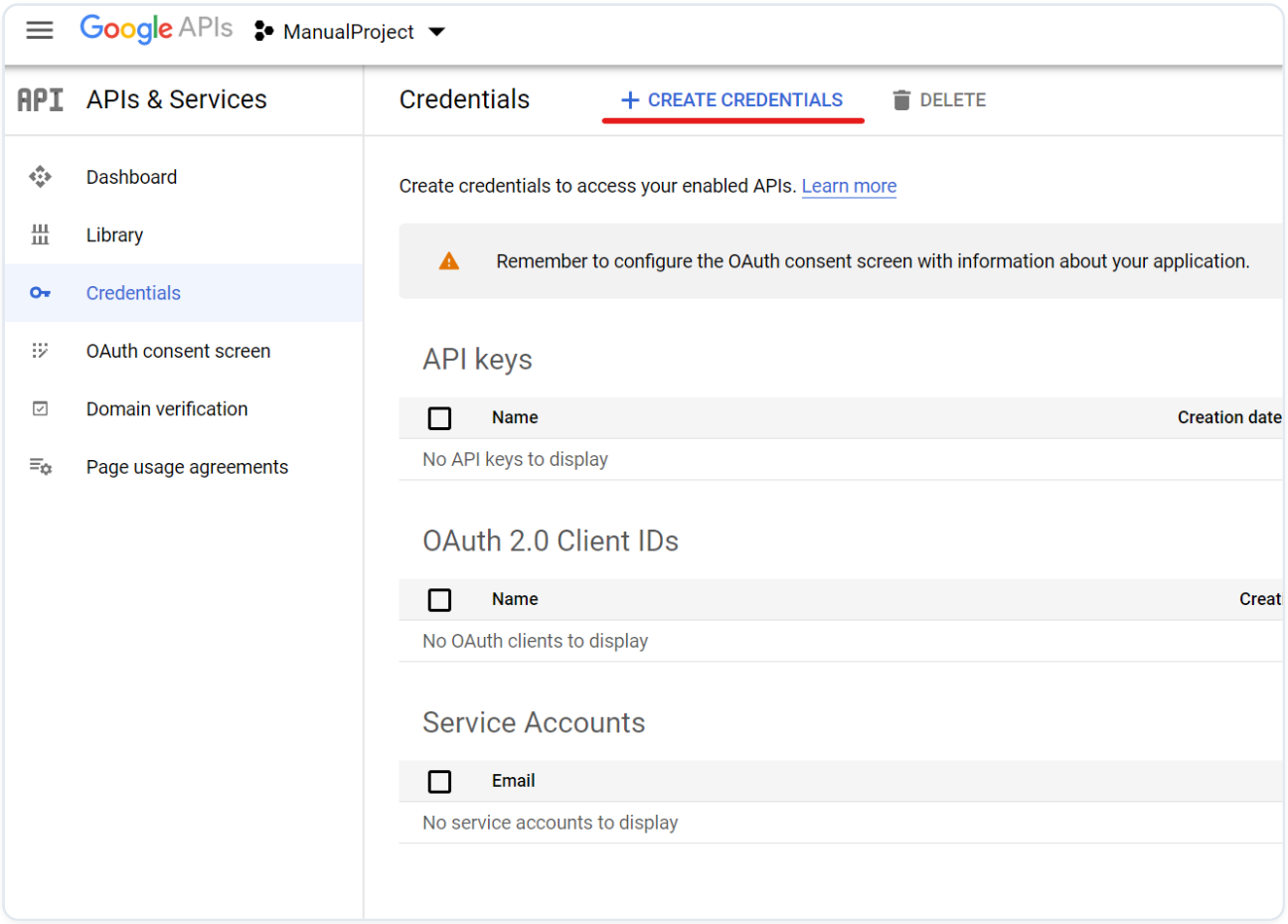
Google OAuth

Para crear un cliente OAuth para usar Google como proveedor de identidad, siga estos pasos para obtener el ID de cliente OAuth y el secreto requeridos en la configuración de la plataforma:

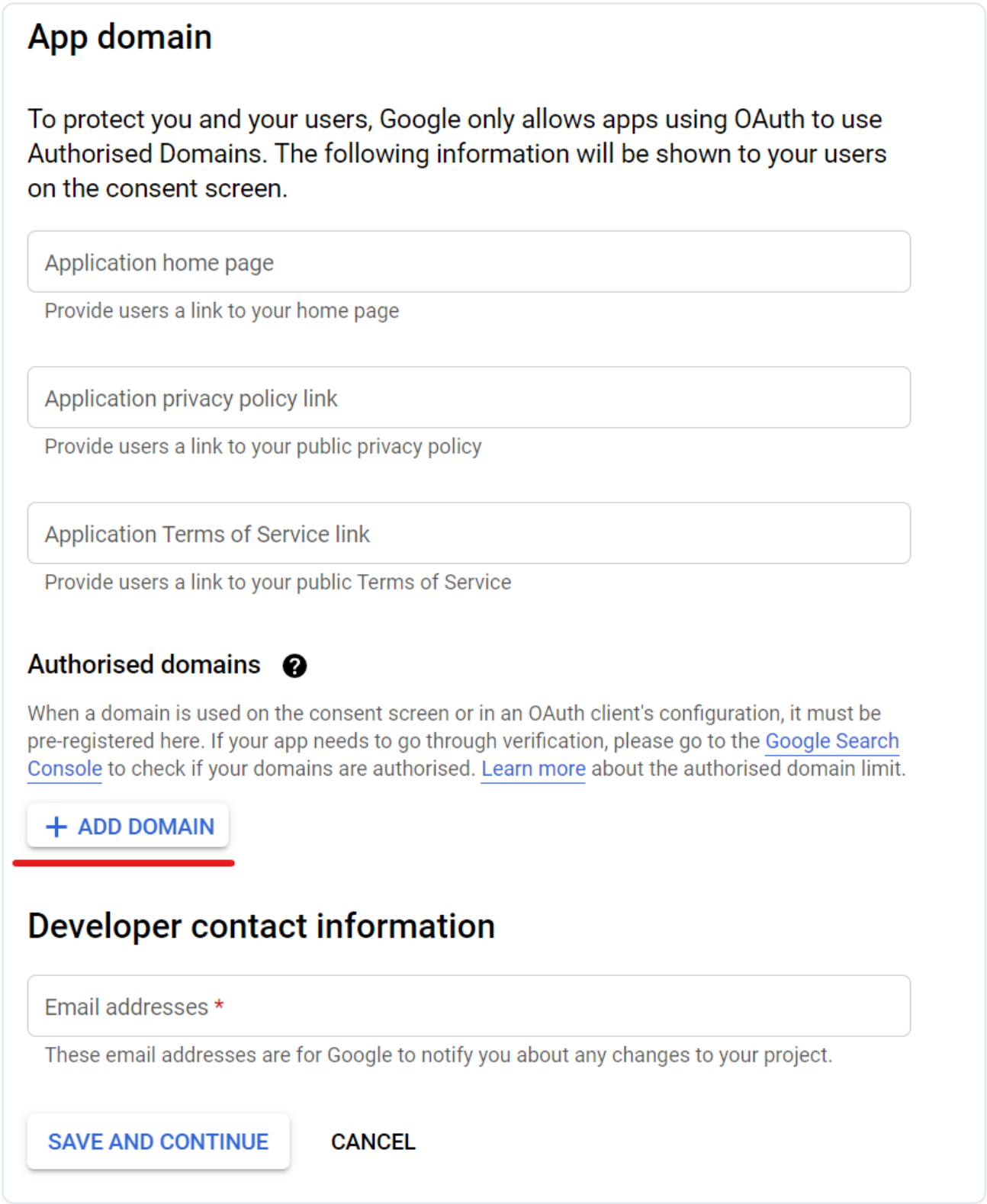
- Vaya a la Consola de API de Google y cree un nuevo proyecto (o use uno existente). El nombre del proyecto, la organización y la ubicación quedan a su discreción.



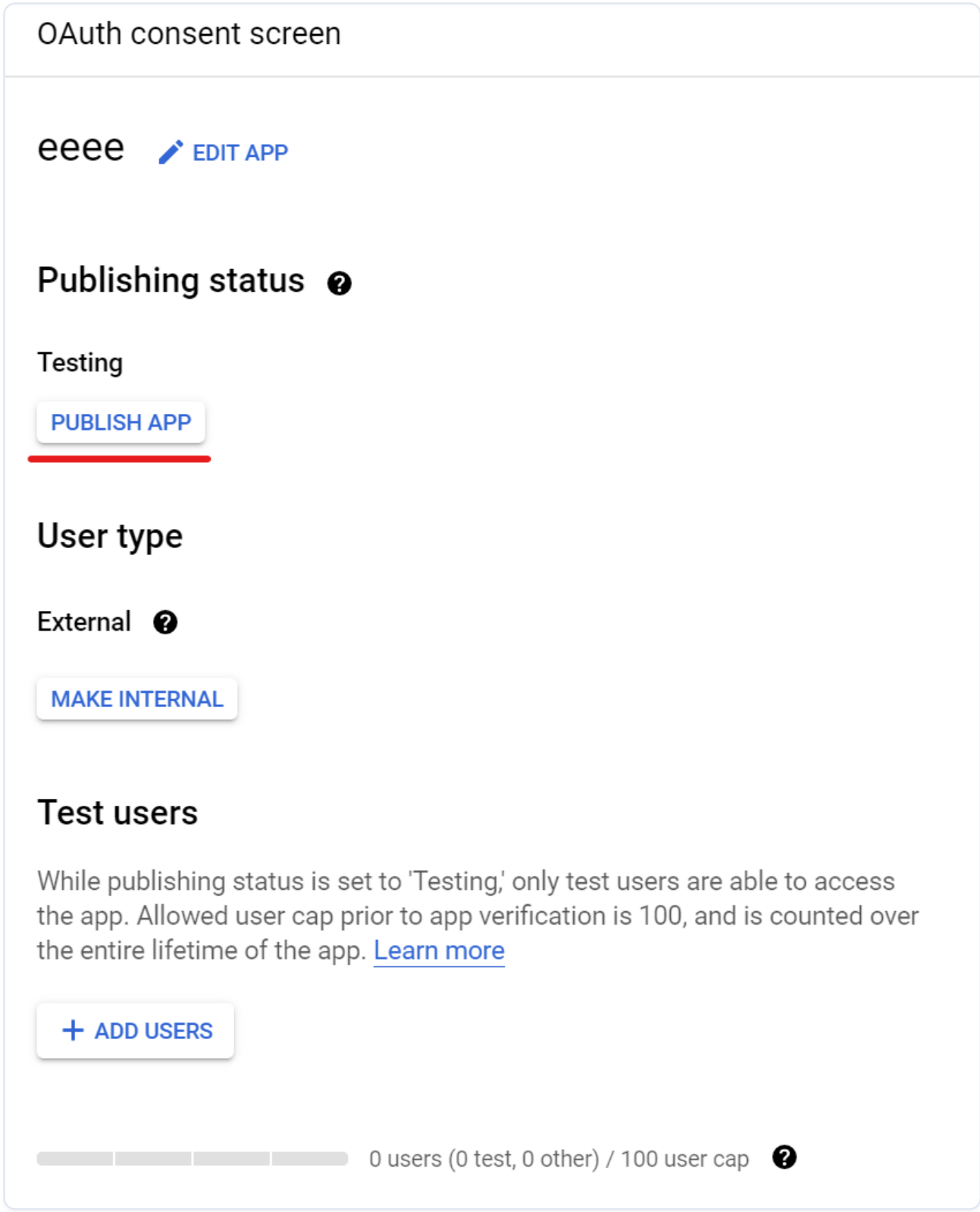
- Dentro del proyecto, haga clic en “+ Crear credenciales” y seleccione “ID de cliente OAuth” del submenú.



- Se le presentará una advertencia para configurar primero una pantalla de consentimiento de OAuth. Haga clic en ella. Seleccione una pantalla de consentimiento externa y haga clic en crear. Rellene los campos a su discreción. El nombre de la aplicación será visible para los usuarios que intenten iniciar sesión en la plataforma.

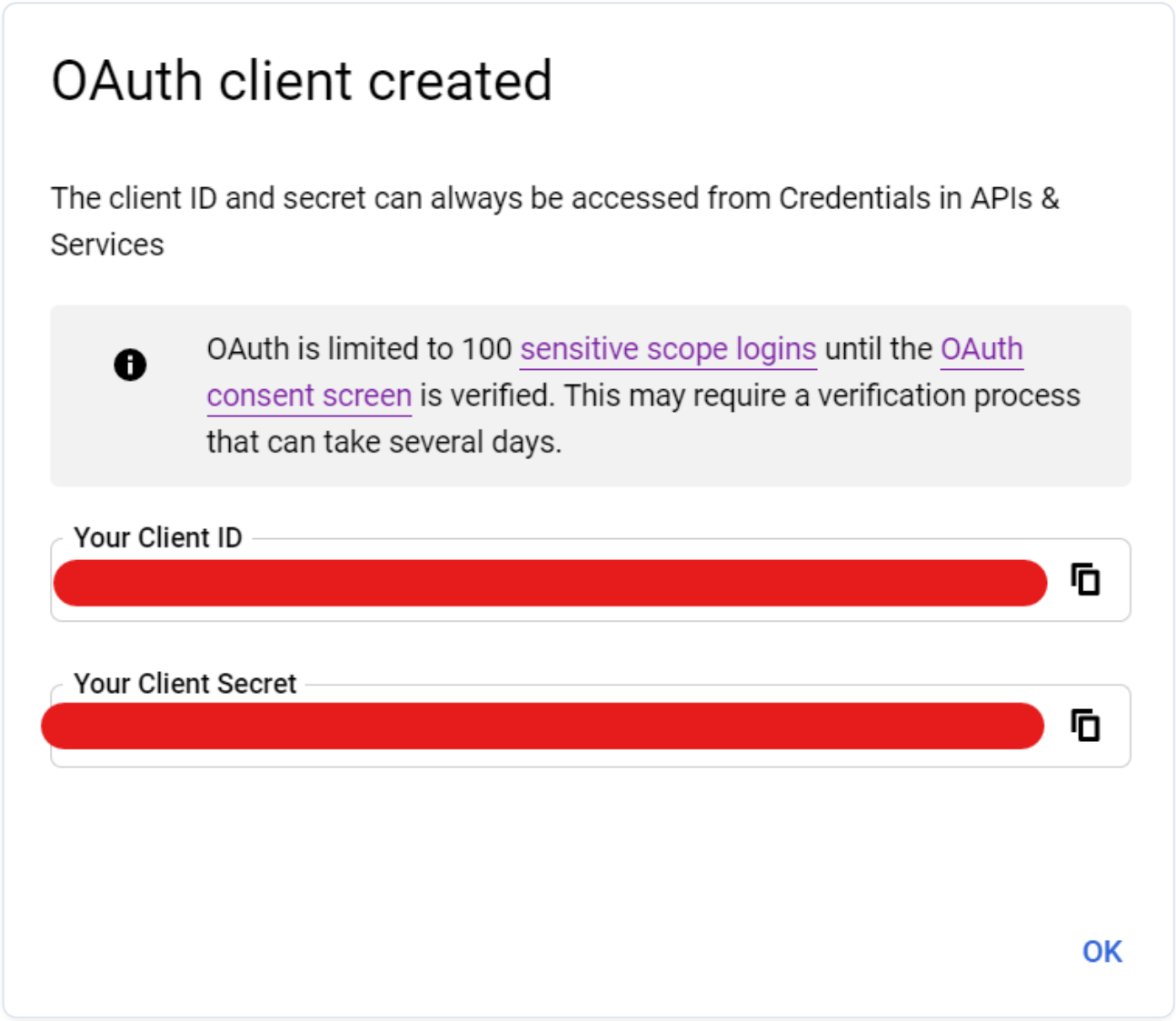


- En el dominio autorizado, especifique el dominio en el que está desplegada la plataforma.
- Haga clic en “Guardar y continuar” en los siguientes menús sin añadir nada hasta llegar a la página de resumen, luego haga clic en “Volver al panel de control”.
- Haga clic en “Publicar aplicación”.



- Vuelva a la página de Credenciales y cree las credenciales para un ID de cliente OAuth.
- En esta página, establezca el tipo de aplicación en “Aplicación web”. El nombre queda a su discreción.

- En “Orígenes de JavaScript autorizados”, especifique el nombre de dominio en el que está desplegada la plataforma. En “URI de redireccionamiento autorizadas”, introduzca la URL de redireccionamiento, similar a:
  - `https://example.com/oauth/callback`
  - Donde “example.com” debe establecerse como el nombre de dominio adecuado.
- Haga clic en “Crear” y anote el ID de cliente y el Secreto para la configuración de la plataforma.



Información relacionada

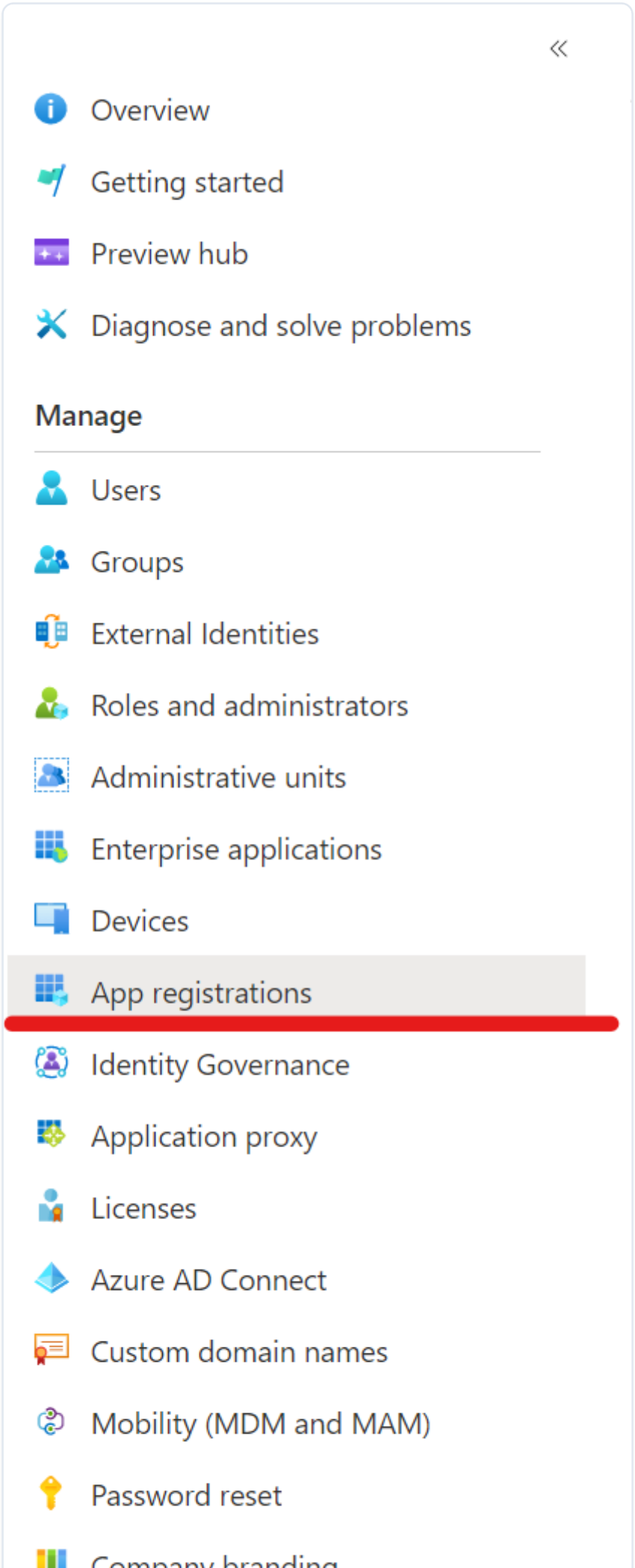
- Microsoft Entra
- OpenID Connect
- Roles de la plataforma
- Proveedores de identidad

- SAML
- Identidad y acceso

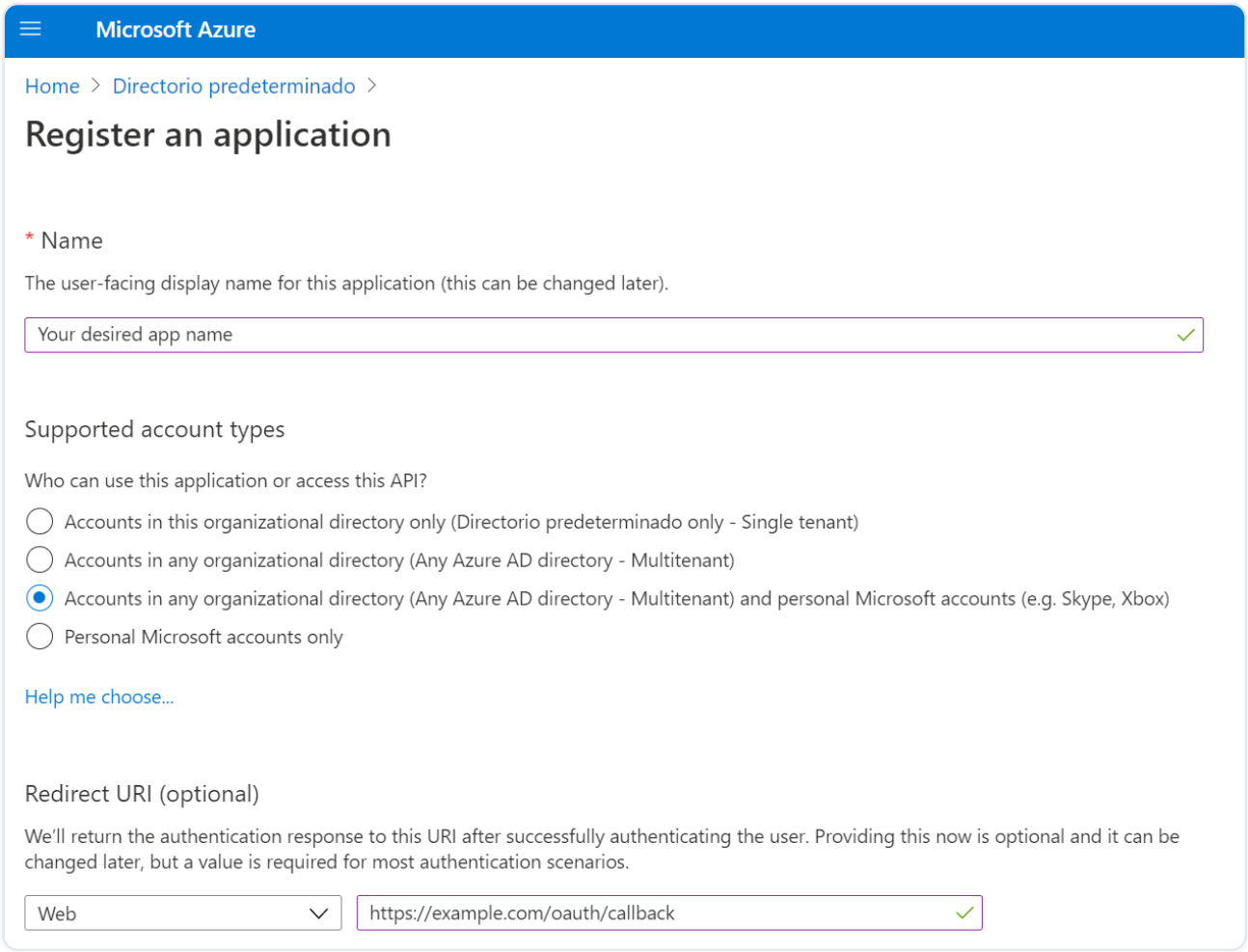
Microsoft Entra

La plataforma admite la integración con Azure Active Directory para iniciar sesión con su cuenta de Microsoft Azure. Para configurarlo:

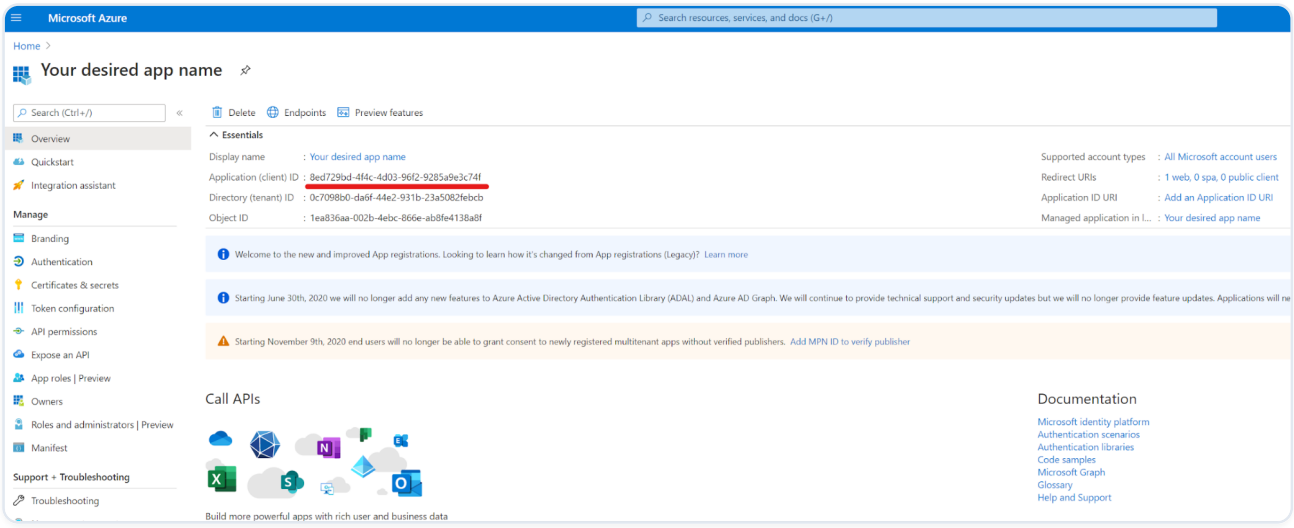
- Vaya al portal de Microsoft Azure.
- Navegue hasta Azure Active Directory.


Overview
Getting started
Preview hub
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset

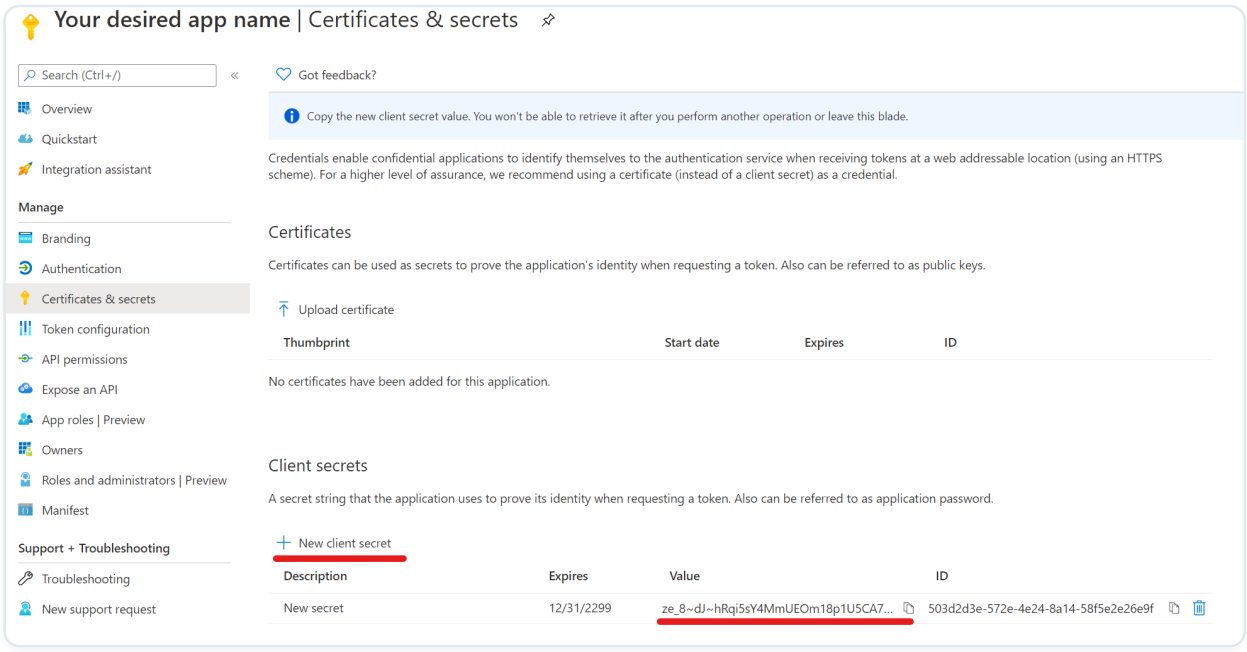
- Haga clic en «Registros de aplicaciones» y luego en «Nuevo registro». Configure lo siguiente:
- **Nombre de la aplicación:** Elija un nombre que será visible públicamente para los usuarios que inicien sesión en la plataforma.
- **Tipos de cuenta admitidos:** Recomendamos seleccionar «Cuentas en cualquier directorio organizacional (cualquier directorio de Azure AD - Multitenant) y cuentas personales de Microsoft (por ejemplo, Skype, Xbox)» para permitir que los usuarios registrados inicien sesión con sus cuentas de dominio público.
- **URI de redirección:** Establezca el selector en «Web» e introduzca un URI similar a `https://example.com/oauth/callback`.



- Haga clic en «Registrar» en la parte inferior.
- En la siguiente página, anote el ID de cliente de OAuth para la configuración de la plataforma.



- Para obtener el secreto, vaya a «Certificados y secretos» de la aplicación recién creada y haga clic en «Nuevo secreto de cliente». Introduzca este secreto en la configuración de la plataforma para completar la configuración.



Cierre de sesión único (SLO) para Microsoft Azure

Para habilitar el cierre de sesión único para el flujo OIDC con Azure, configure lo siguiente:

- Para cerrar la sesión de los usuarios de Microsoft cuando cierren la sesión de la plataforma Citrix SecurSpaces™, añada otra URL en la sección URI de redirección con solo el nombre de dominio utilizado por la plataforma SecurSpaces. Esta URL se utiliza para redirigir a los usuarios de vuelta después de que cierren la sesión de sus cuentas de Microsoft.
- Añada la declaración opcional llamada “login_hint” al token de ID:
- Vaya a “Configuración de tokens” y haga clic en “Añadir declaración opcional”.
- Seleccione ID como tipo de token y luego seleccione “login_hint”.

- Para cerrar la sesión del usuario de la plataforma SecurSpaces cuando cierre la sesión de su cuenta de Microsoft, añada la declaración opcional llamada “sid” al tipo de token de ID.
- Añada una URL de cierre de sesión en el menú “Autenticación” con la estructura `https://[domain_name]/auth/logout`, donde `domain_name` es el dominio bajo el cual tiene la plataforma SecurSpaces. Microsoft llamará a este punto final cuando un usuario cierre la sesión para también cerrar la sesión del usuario de la plataforma SecurSpaces.

Información relacionada

- Google OAuth
- OpenID Connect
- Roles de la plataforma
- Proveedores de identidad
- SAML
- Identidad y acceso

Connect an OpenID Connect provider

Esta plataforma es compatible con la integración de OpenID Connect para el inicio de sesión.

Registro de la aplicación

- Vaya al portal para desarrolladores del proveedor de OpenID.
- Navegue a la sección Aplicaciones o Clientes.
- Haga clic en «Crear nueva aplicación» o equivalente. Configure lo siguiente:
- **Nombre de la aplicación**: Elija un nombre que se mostrará a los usuarios que inicien sesión.
- **Tipo de aplicación**: Seleccione «Aplicación web».
- **URI de redirección**: Añada el siguiente URI para gestionar las redirecciones de inicio de sesión: `https://example.com/oauth/callback`
- **URI de redirección de cierre de sesión**: Añada el siguiente URI para gestionar las redirecciones de cierre de sesión: `https://example.com/auth/logout`
- Guarde la aplicación.

Anote el ID de cliente y el secreto de cliente generados durante este proceso. Estos serán necesarios para la configuración de la plataforma.

Configuración de ámbitos y reclamaciones

En la sección Ámbitos o Permisos de su aplicación, asegúrese de que se incluyan los siguientes ámbitos:

- `openid`
- `email`
- `profile`
- Cualquier ámbito adicional que requiera su plataforma.

Configure las reclamaciones si es necesario. Las reclamaciones comunes incluyen:

- `sub`: Identificador único para el usuario.
- `email`: Dirección de correo electrónico del usuario.
- `name`: Nombre completo del usuario.
- `preferred_username`: Nombre de usuario o alias.

Habilitar el cierre de sesión único (SLO)

Para habilitar el cierre de sesión único (SLO) para OpenID Connect:

Vaya a la sección de Configuración avanzada o Configuración de cierre de sesión.

Habilite el cierre de sesión único si es compatible con el proveedor.

Añada la URI de redirección de cierre de sesión configurada anteriormente:

`https://example.com/auth/logout`

Opcionalmente, añada las siguientes reclamaciones al token de ID:

- `sid`: Identificador de sesión.
- `logout_hint`: Proporciona contexto para cerrar sesión.

Información relacionada

- Google OAuth
- Microsoft Entra
- Roles de la plataforma
- Proveedores de identidad
- SAML

- Identidad y acceso

SAML

Citrix SecurSpaces™ actúa como proveedor de servicios SAML 2.0. Cualquier proveedor de identidades conforme funciona — Okta, Microsoft Entra ID, Ping, ADFS y otros — porque la configuración es un intercambio de metadatos en lugar de algo específico del proveedor.

Configurarlo es una tarea de dos partes: el proveedor de identidades necesita conocer SecurSpaces, y SecurSpaces necesita conocer al proveedor de identidades.

Configurar el proveedor de identidades

Cree una aplicación SAML en su proveedor de identidades con los siguientes valores, donde `<your-sds-hostname>` es el dominio en el que está implementada su plataforma:

CONFIGURACIÓN	VALOR
URL de inicio de sesión único (URL del servicio de consumidor de aserciones)	`https://<your-sds-hostname>/saml/acs`
URI de audiencia (URL de metadatos del proveedor de servicios)	`https://<your-sds-hostname>/saml/metadata`

Si su proveedor de identidades prefiere importar metadatos en lugar de introducir los valores manualmente, SecurSpaces publica sus propios metadatos de proveedor de servicios. Utilice **Descargar metadatos** en la página de configuración de SAML.

Atributos

El proveedor de identidades debe enviar estos atributos en la aserción:

ATRIBUTO	TIPO	¿QUÉ HACE?
`email`	**Obligatorio**	El correo electrónico con el que el usuario está registrado en la plataforma. Sin él, la conexión no funciona.
`displayName`	Recomendado	El nombre que se muestra para el usuario en toda la plataforma. Cuando está

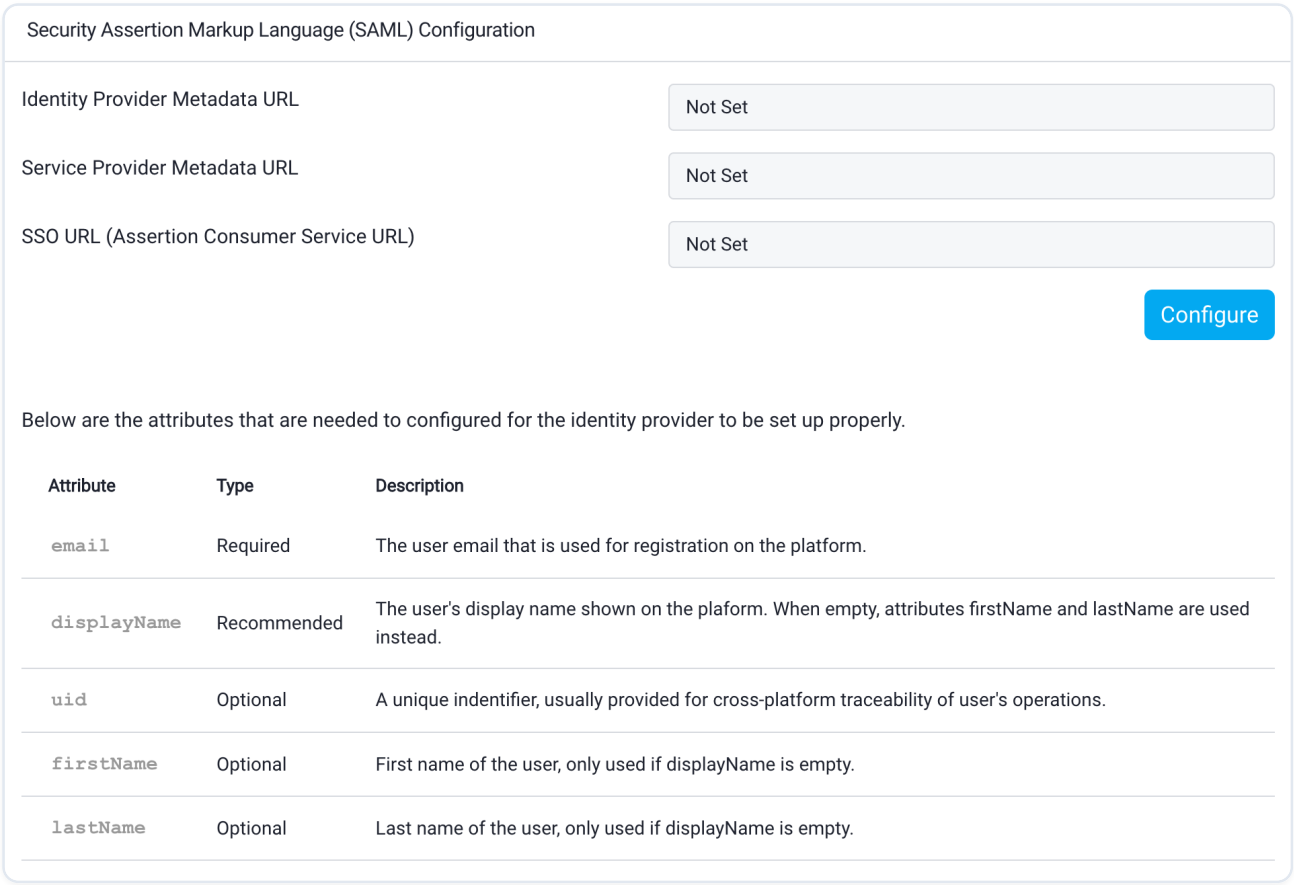
ATRIBUTO	TIPO	¿QUÉ HACE?
		vacío, se usan `firstName` y `lastName` en su lugar.
`firstName`	Opcional	Se usa solo cuando `displayName` está vacío.
`lastName`	Opcional	Se usa solo cuando `displayName` está vacío.
`uid`	Opcional	Un identificador único, normalmente proporcionado para que las acciones de un usuario puedan rastrearse en todos los sistemas.

Envíe `displayName` si puede. Sin él, la plataforma ensambla un nombre a partir de `firstName` y `lastName`, y si estos también están ausentes, los usuarios se identifican por su dirección de correo electrónico en toda la consola y el registro de auditoría.

Enviar `uid` merece la pena siempre que los datos de auditoría se correlacionen con otros sistemas, porque las direcciones de correo electrónico cambian y un identificador estable no.

Configurar SecurSpaces

1. Inicie sesión como administrador de la plataforma.
2. Vaya a **System Configuration > SAML Service Provider Configuration**, o navegue hasta `https://<your-sds-hostname>/platform/system_configuration/saml_sp`.
3. Seleccione **Configure**.
4. Proporcione los metadatos del proveedor de identidad, ya sea como una **Identity Provider Metadata URL** o cargando su archivo de metadatos XML.



Una URL de metadatos es la mejor opción si su proveedor de identidad ofrece una, porque las rotaciones de certificados se detectan automáticamente en lugar de tener que volver a cargar el archivo.

Información relacionada

- Proveedores de identidad
- SCIM — aprovisionamiento automático de usuarios
- Control de acceso de usuarios
- Roles de plataforma

SCIM configuration

La plataforma Citrix SecurSpaces™ se adhiere a la especificación del Sistema para la Gestión de Identidades entre Dominios (SCIM) 2.0. Utilice SCIM para el aprovisionamiento, sincronización y desaprovisionamiento automático de usuarios y grupos. La plataforma SecurSpaces es compatible con los puntos finales `/Users` y `/Groups`.

- Utilice el punto final `/Users` para crear, actualizar, eliminar y recuperar usuarios. Las respuestas de usuario incluyen membresías de grupo directas en el atributo de solo lectura `groups` cuando el usuario pertenece a uno o más grupos.

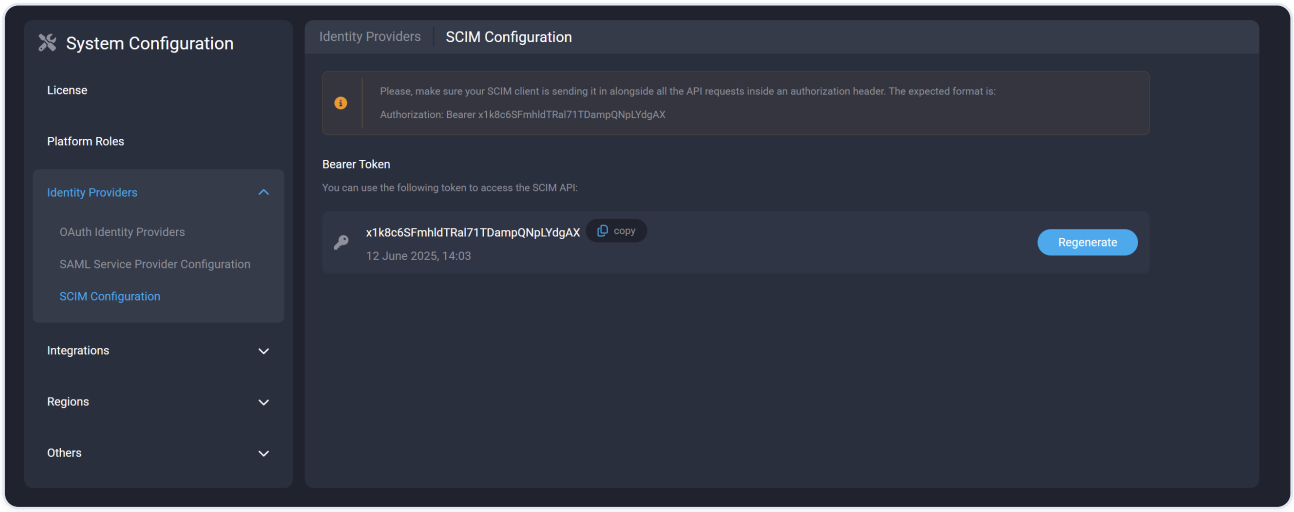
- Utilice el punto final `/Groups` para crear, actualizar, eliminar y recuperar grupos. Las respuestas de la lista de grupos incluyen a los miembros del grupo, de modo que los proveedores de identidad pueden validar las membresías sin solicitar cada grupo por separado.

Cuando su proveedor de identidad envía campos de nombre SCIM separados, SecurSpaces asigna `name.givenName` y `name.familyName` al nombre y apellido del usuario. Si el proveedor envía `name.formatted`, SecurSpaces utiliza ese valor formateado como el nombre para mostrar del usuario.

Configurar el proveedor SCIM

Se requiere un token para autorizar las solicitudes entre su proveedor SCIM y la plataforma SecurSpaces. Como administrador, puede obtener el token en **Configuración del sistema > Proveedores de identidad > Configuración SCIM**.

`https://<your-sds-hostname>/system_configuration/identity_providers/scim`



Asegúrese de que su proveedor SCIM incluya este token en todas las solicitudes de API, utilizando el siguiente formato de encabezado de autorización:

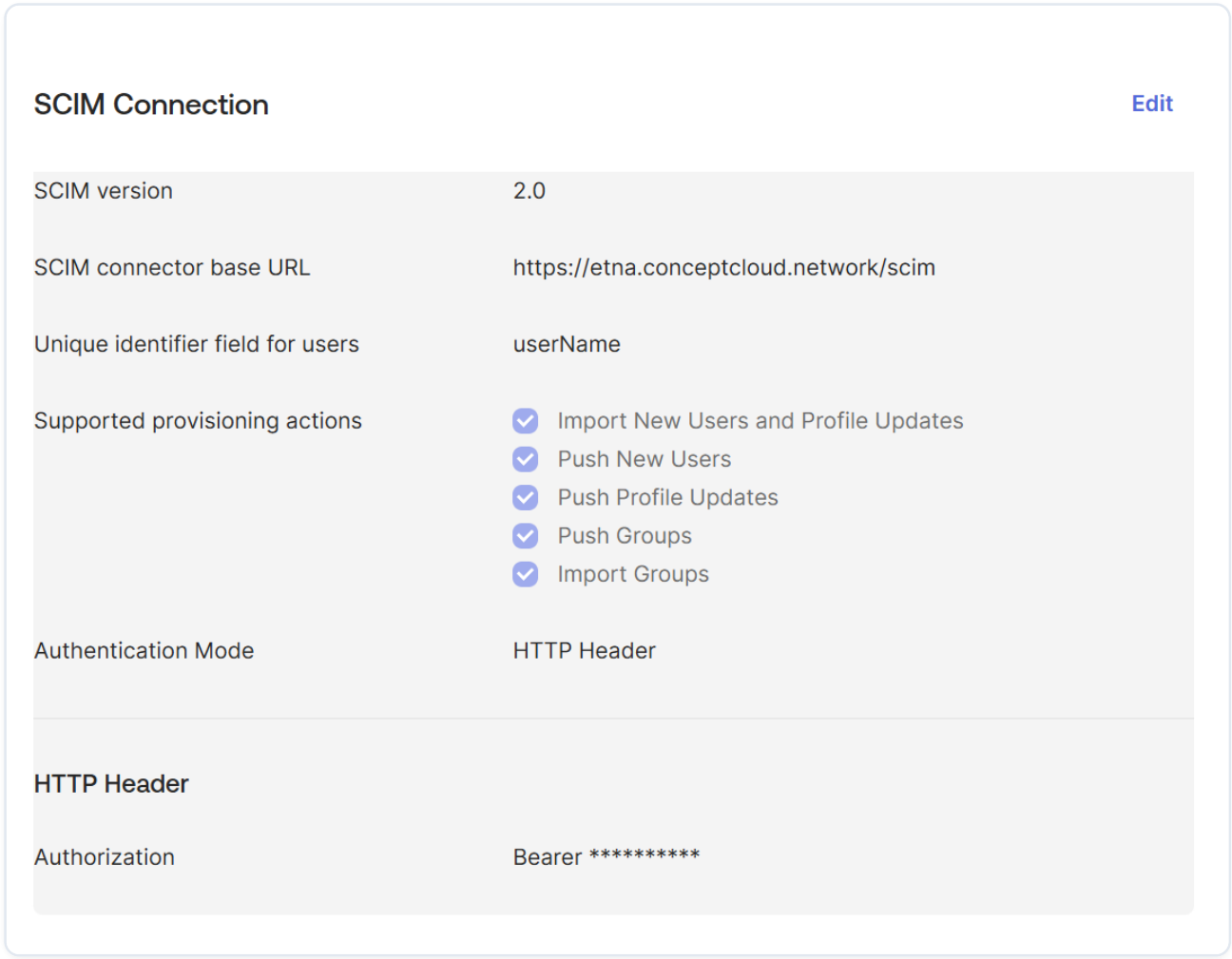
`Authorization: Bearer <scim-token>`

Okta

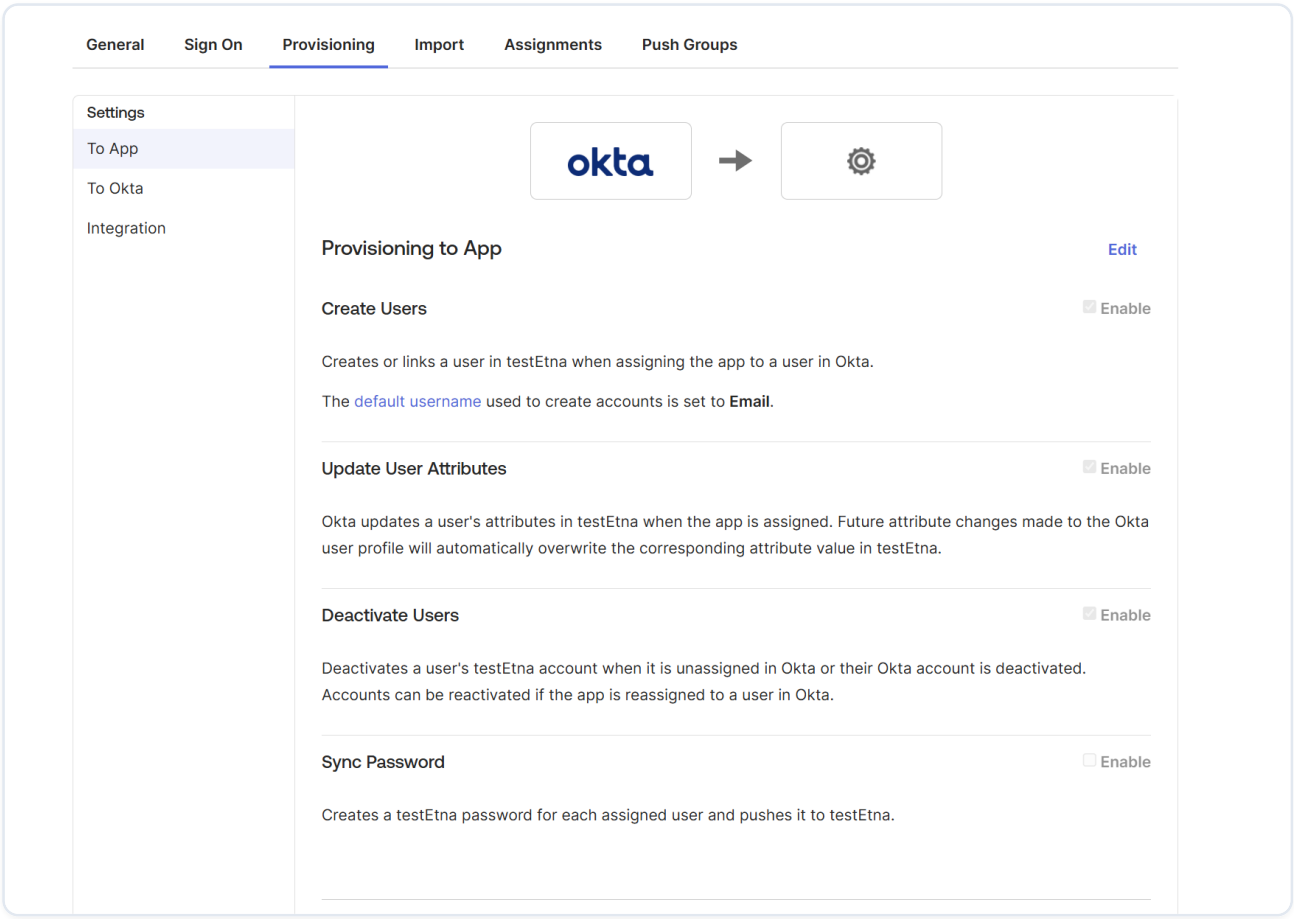
Para usar Okta, configure estos campos:

- **URL base del conector SCIM:** `https://<your-sds-hostname>/scim`
- **Campo de identificador único para usuarios:** `userName`

La configuración es similar a este ejemplo:



En usuarios, habilite las opciones que coincidan con su flujo de trabajo de aprovisionamiento:

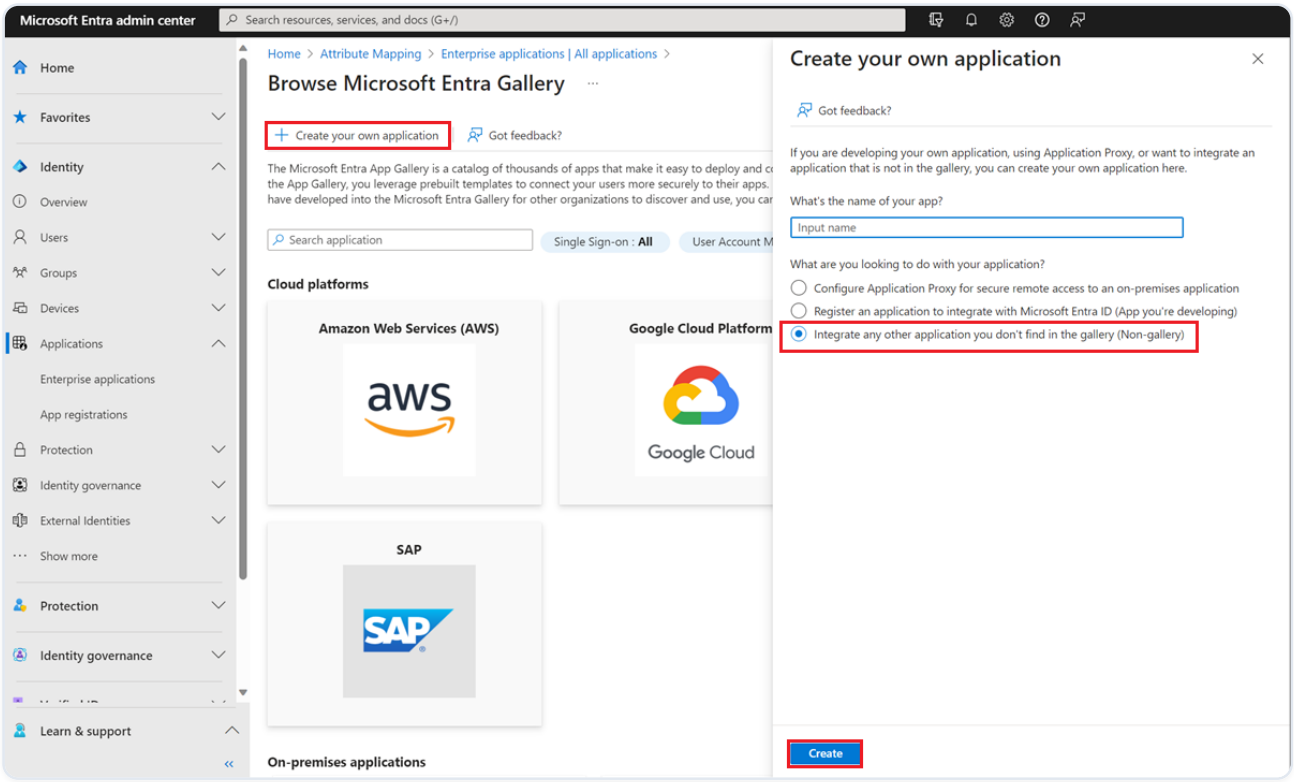


Microsoft Entra

Para usar Microsoft Entra, configure una aplicación empresarial personalizada dentro de su inquilino de Microsoft Entra.

AGREGAR UNA APLICACIÓN EMPRESARIAL

1. Inicie sesión en el centro de administración de Microsoft Entra con al menos permisos de **Administrador de aplicaciones en la nube**.
2. Vaya a **Identidad > Aplicaciones > Aplicaciones empresariales > Todas las aplicaciones**.
3. Seleccione **+ Nueva aplicación**.
4. Seleccione **Crear su propia aplicación**.
5. Introduzca un nombre de aplicación único y seleccione **Integrar cualquier otra aplicación que no encuentre en la galería**.
6. Seleccione **Crear**.



CONFIGURAR EL APROVISIONAMIENTO

Una vez creada la aplicación, siga estos pasos para configurar la conexión SCIM:

1. Vaya a **Identidad > Aplicaciones > Aplicaciones empresariales**, y seleccione su aplicación recién creada.
2. En **Administrar**, seleccione **Aprovisionamiento**.
3. Seleccione **+ Nueva configuración**.
4. Para **Seleccionar método de autenticación**, seleccione la opción de token de portador compatible.
5. Para **URL de inquilino**, introduzca la URL de su punto final SCIM. Por ejemplo, `https://<your-sds-hostname>/scim`.
6. Para **Token secreto**, introduzca el token de portador proporcionado por SecurSpaces.
7. Seleccione **Probar conexión**.
8. Seleccione **Guardar**.

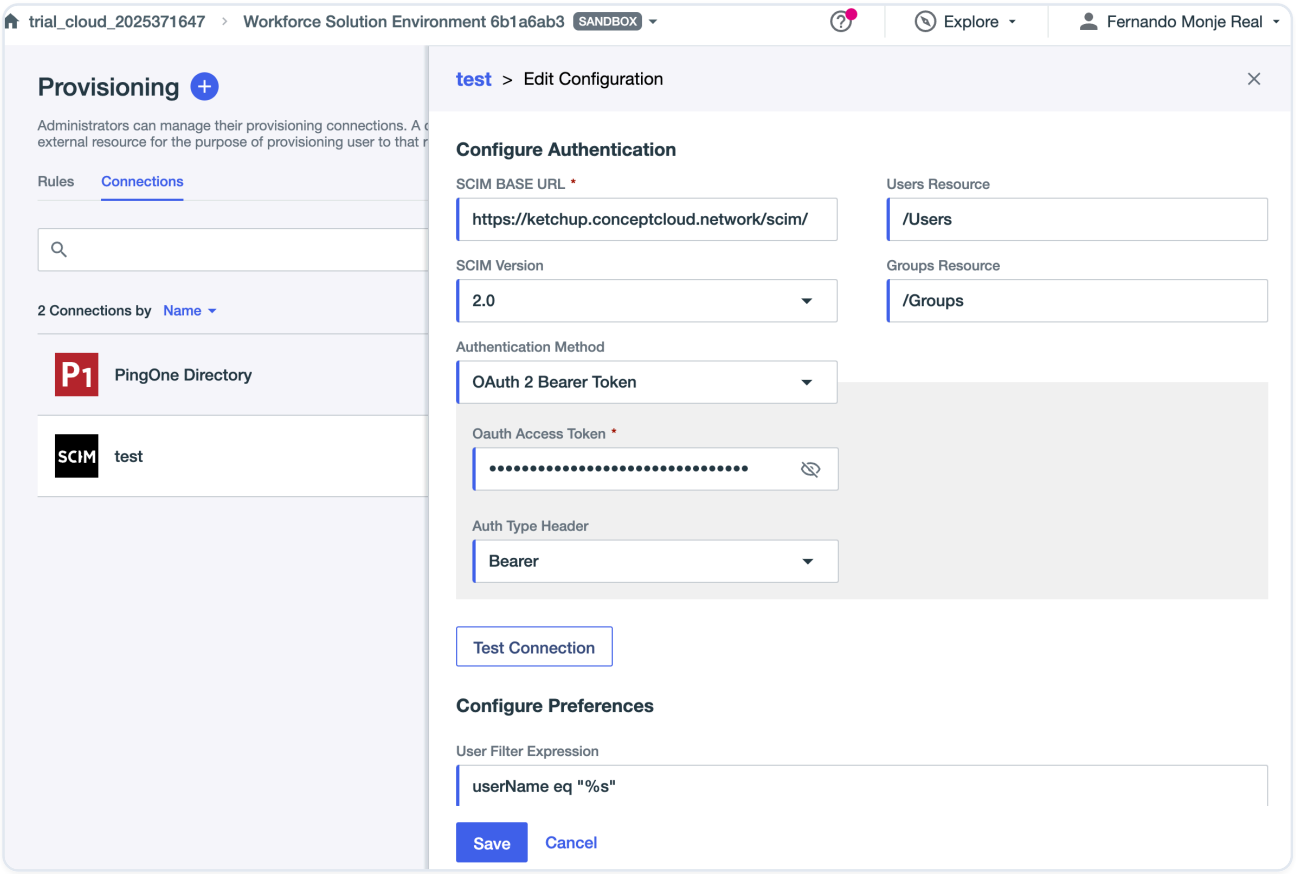
> **Nota:**
>
> Puede que se requiera una conexión de prueba exitosa para continuar.

PingOne

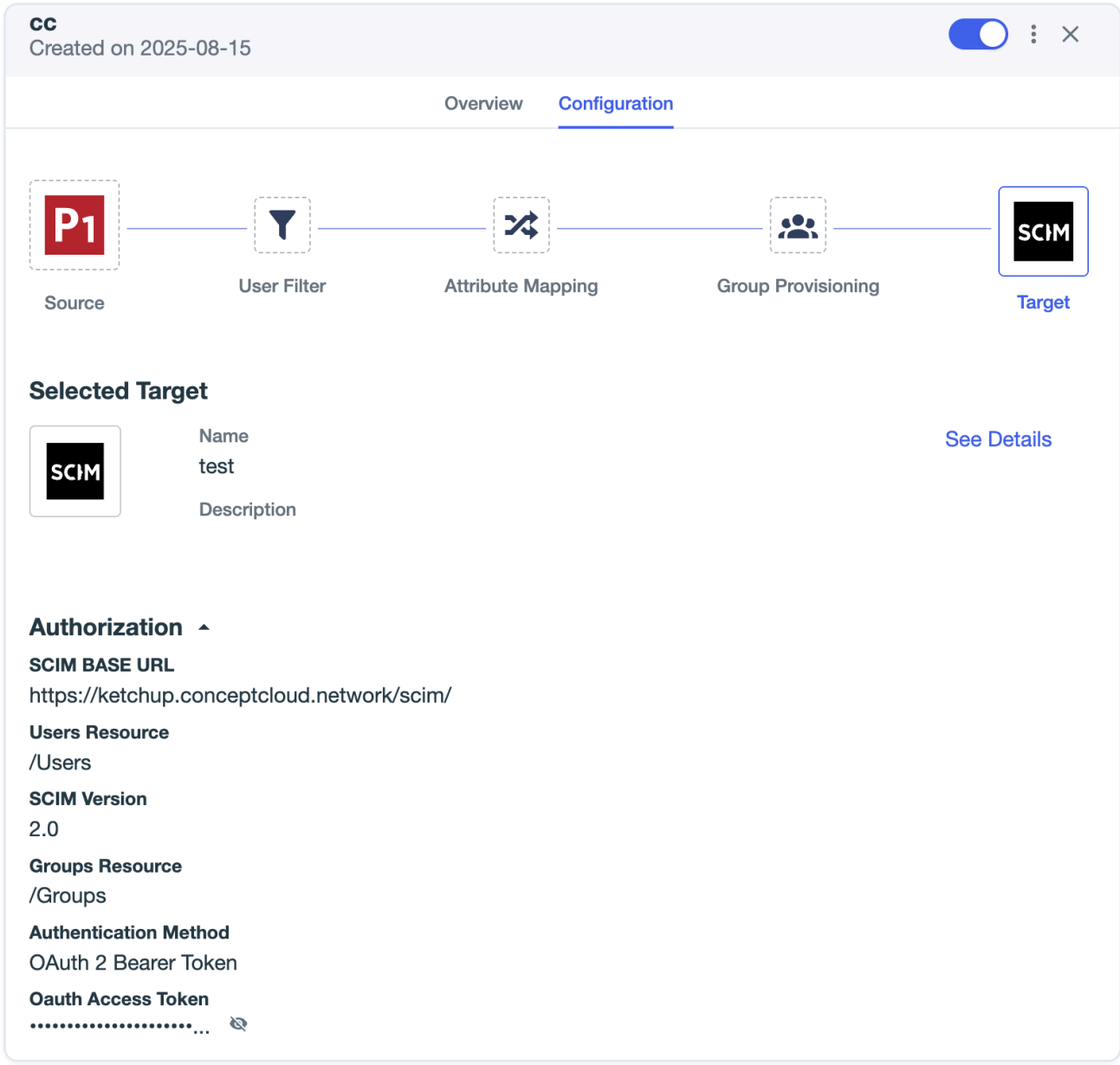
Para usar PingOne, configure estos campos:

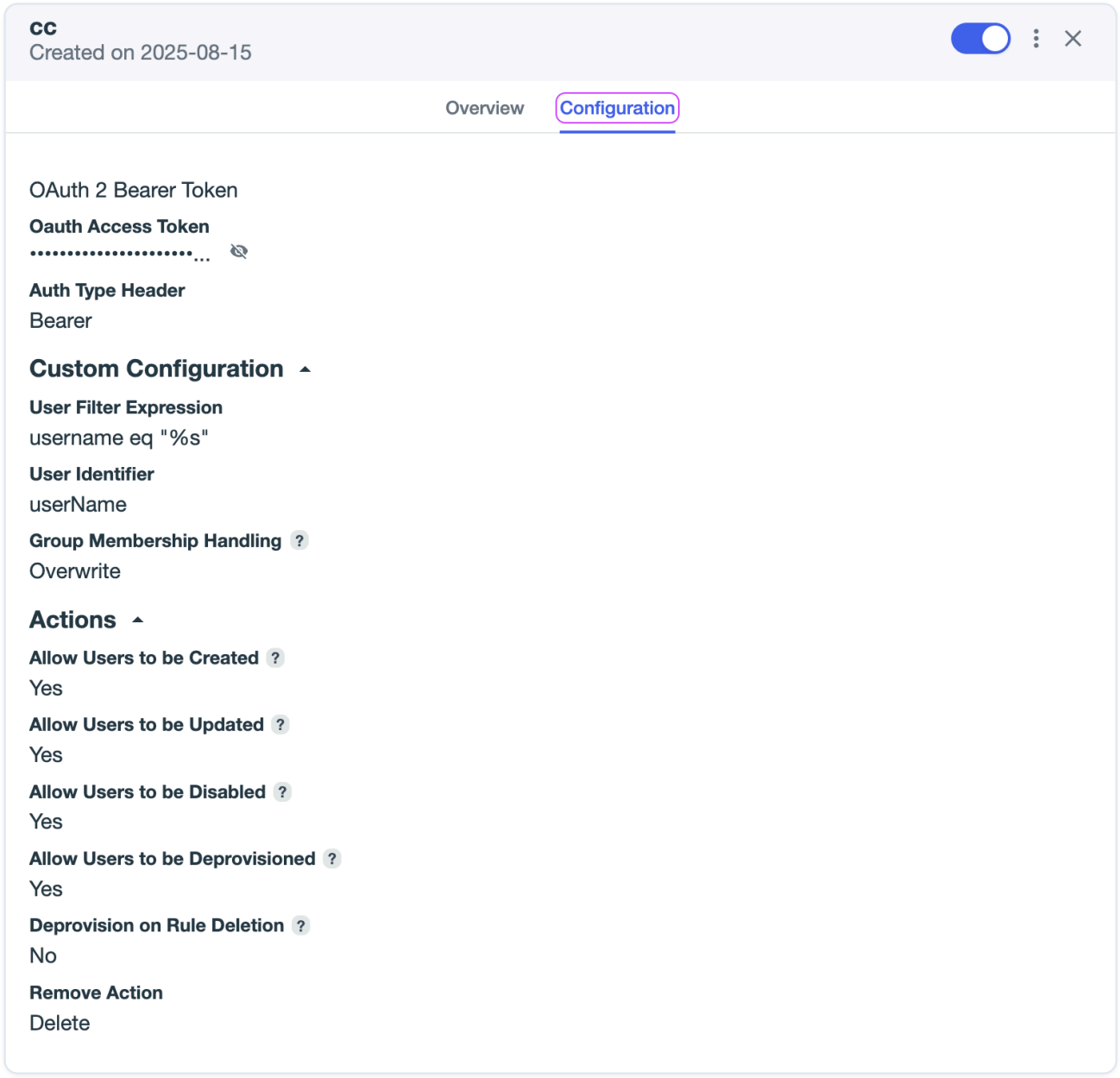
- **URL base de SCIM:** `https://<your-sds-hostname>/scim`
- **Expresión de filtro de usuario:** Cambie `username` a `userName`, y cambie `Eq` a `eq`.

La configuración es similar a este ejemplo:



Después de la configuración, el resultado es similar a estos ejemplos:


cc
Created on 2025-08-15
Overview
Configuration
Source
User Filter
Attribute Mapping
Group Provisioning
Target
Selected Target
Name
test
Description
See Details
Authorization
SCIM BASE URL
https://ketchup.conceptcloud.network/scim/
Users Resource
/Users
SCIM Version
2.0
Groups Resource
/Groups
Authentication Method
OAuth 2 Bearer Token
Oauth Access Token

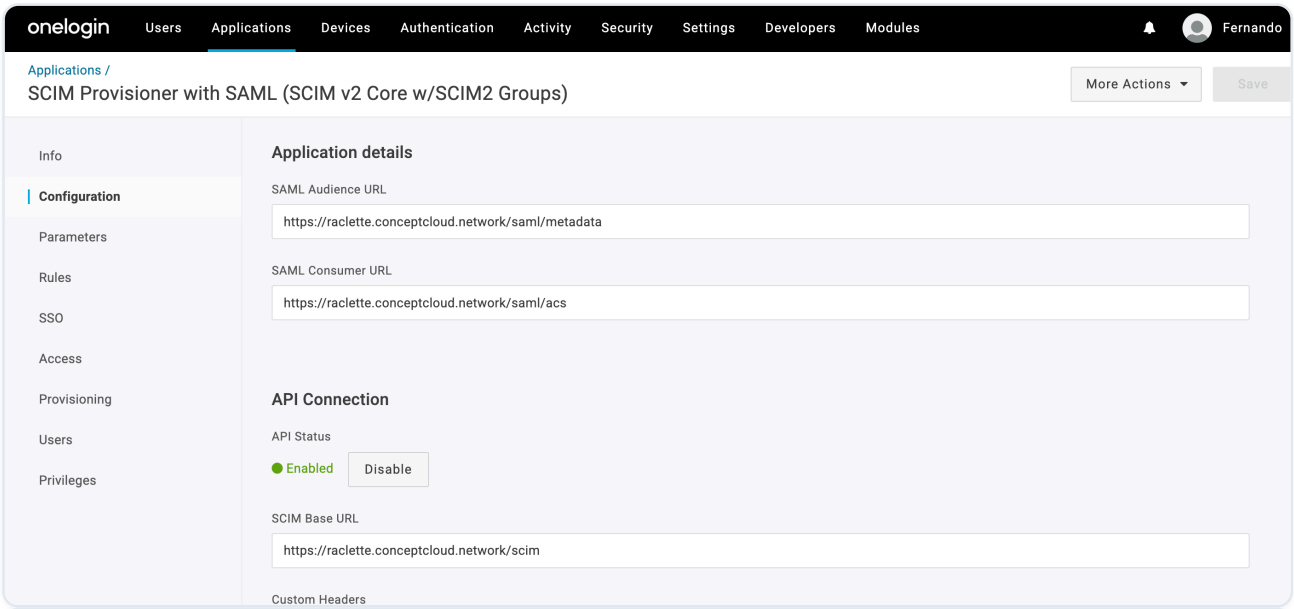


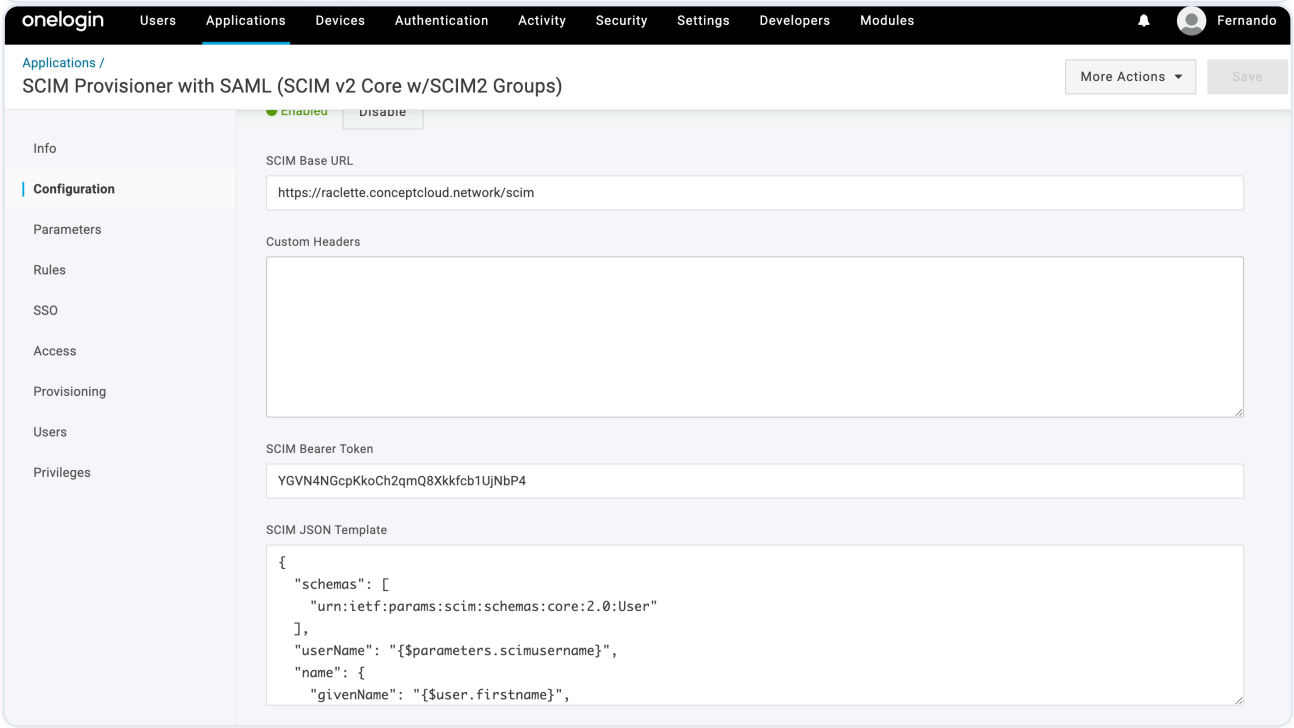
OneLogin

Para usar OneLogin, configure estos campos:

- **URL base de SCIM:** `https://<your-sds-hostname>/scim`
- **scimusername:** Establezca el valor en **Email**.

La configuración es similar a estos ejemplos:





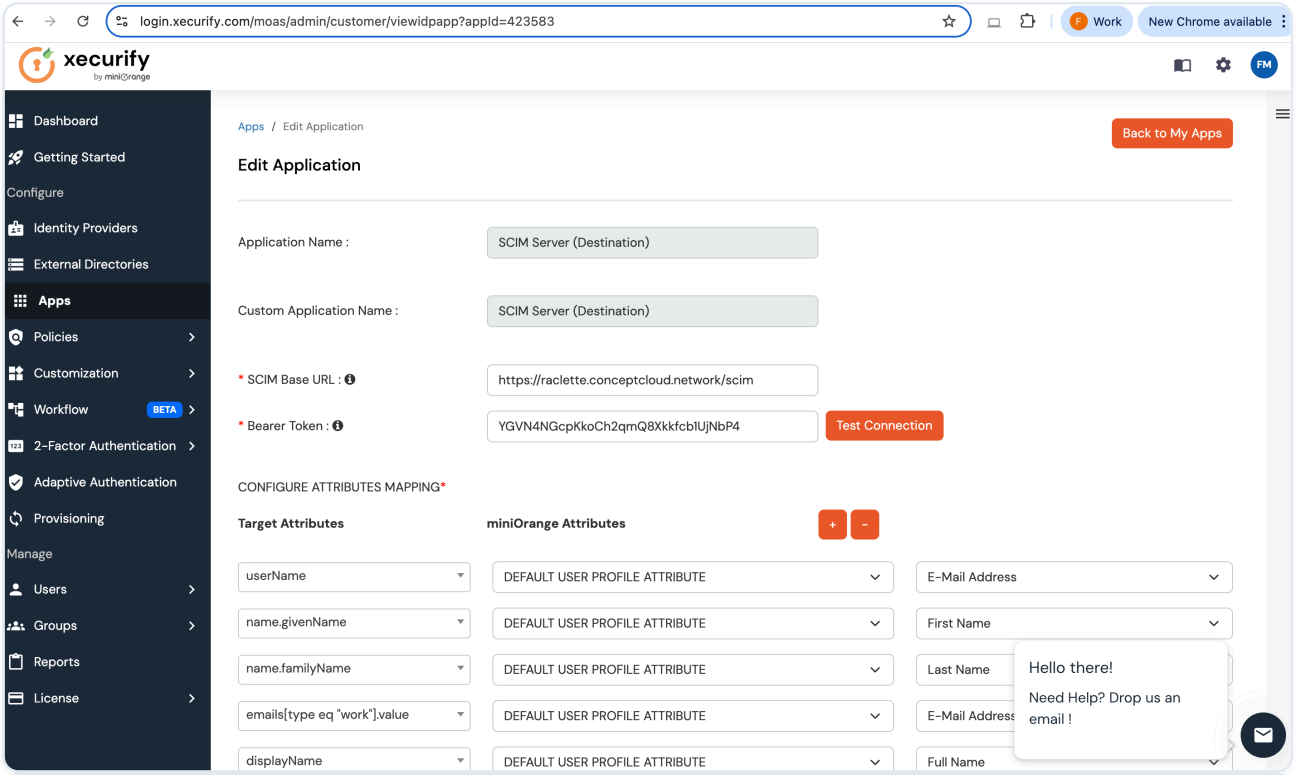
La sección de parámetros es similar a este ejemplo:

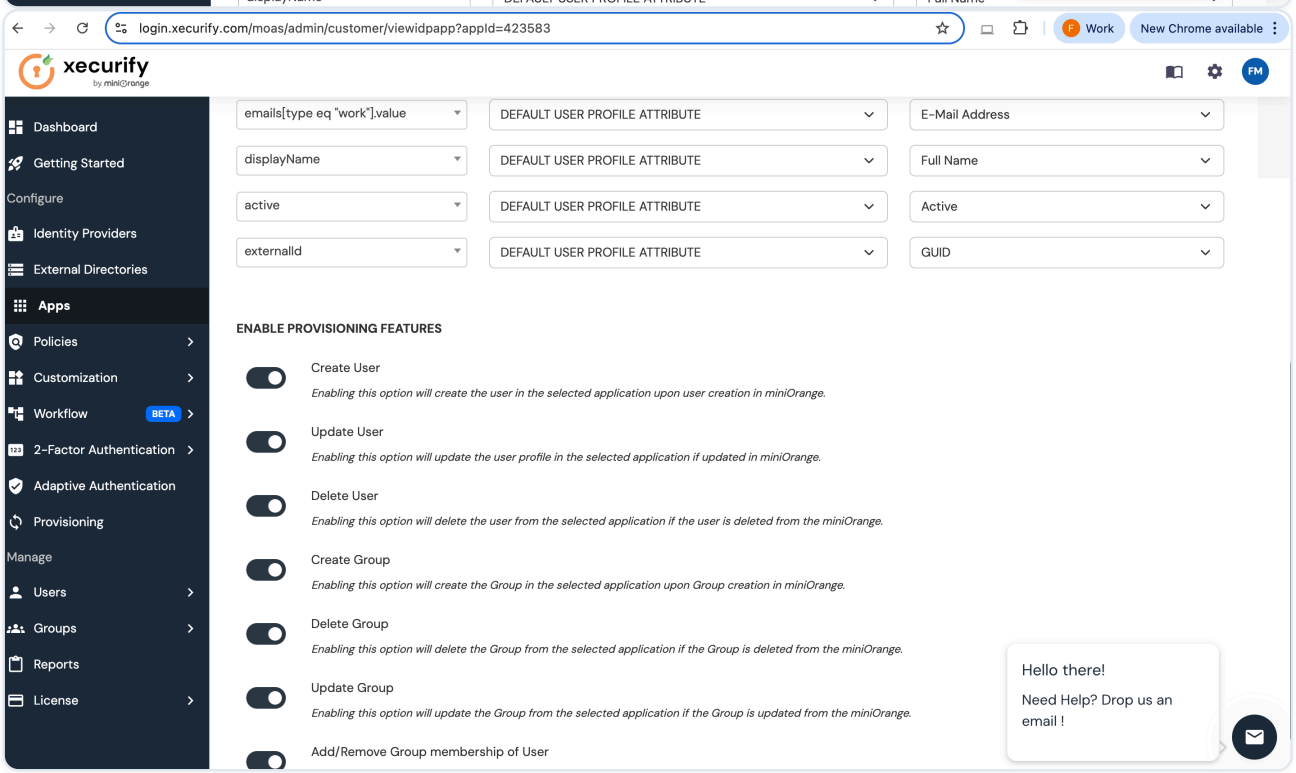
Xecurify

Para usar Xecurify, también conocido como miniOrange, configure estos campos:

- **URL base de SCIM:** `https://<your-sds-hostname>/scim`
- **userName:** Establezca el valor en **Dirección de correo electrónico**.

La configuración es similar a estos ejemplos:

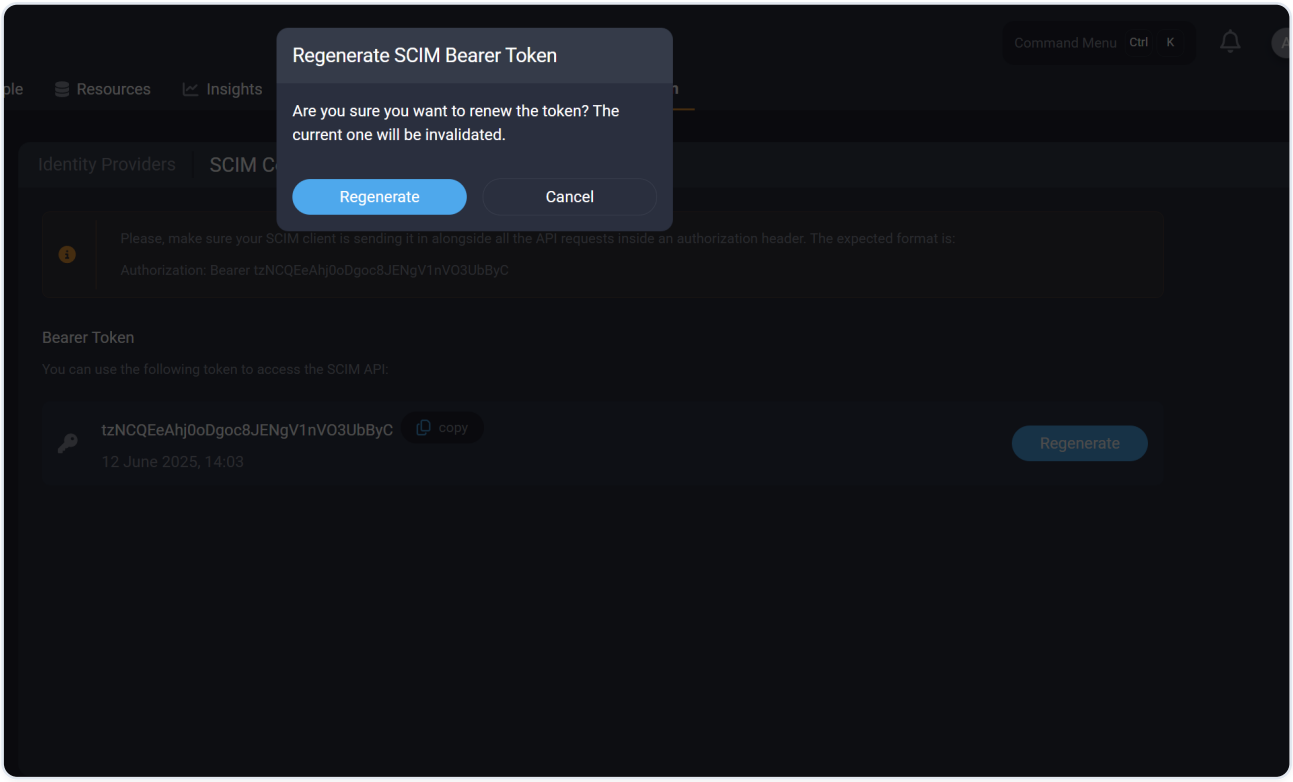




Configurar la plataforma SecurSpaces

No se necesita ninguna configuración adicional en la plataforma SecurSpaces. SCIM está habilitado por defecto.

Puede renovar el token en cualquier momento. La renovación del token invalida cualquier token emitido anteriormente.



Información relacionada

- Google OAuth
- Microsoft Entra
- OpenID Connect
- Roles de la plataforma
- Proveedores de identidad
- Identidad y acceso

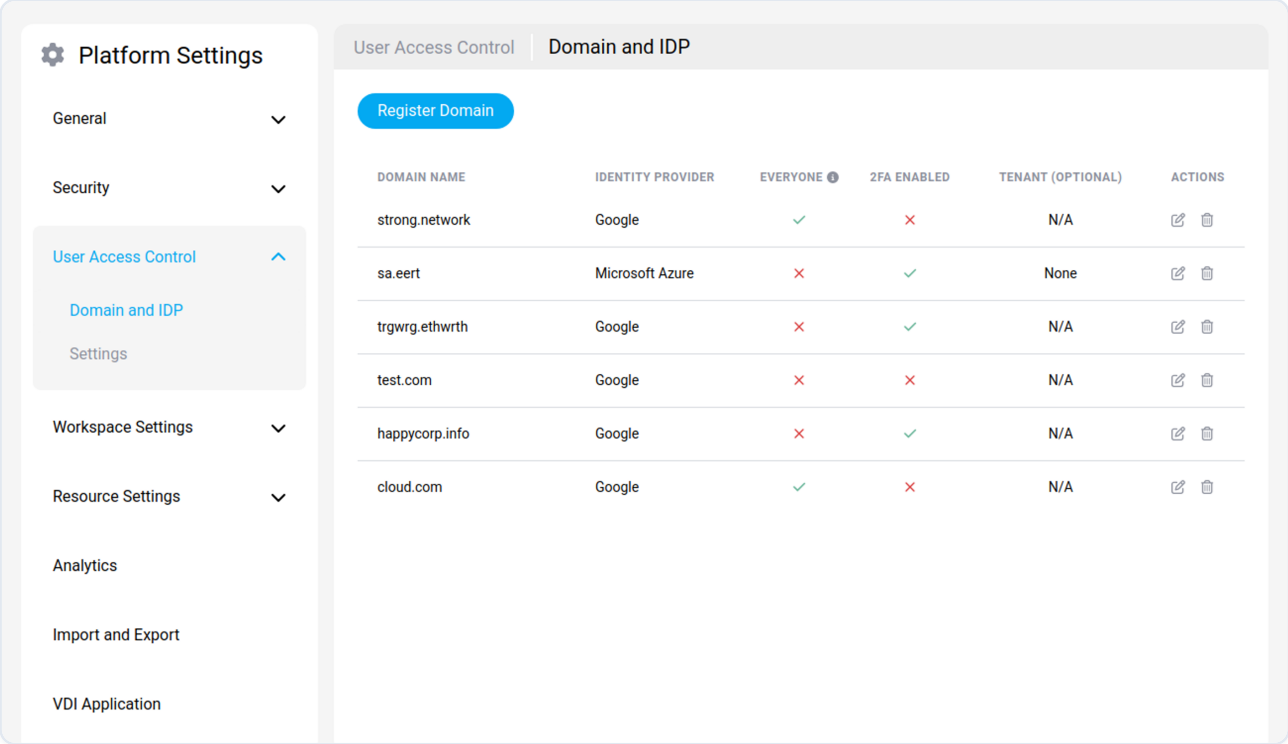
User access control

El control de acceso de usuario decide dos cosas a nivel de plataforma: qué proveedor de identidades autentica a un usuario determinado, y qué se le permite hacer a cualquier usuario, independientemente de su rol.

Encuéntrelo en **Configuración del sistema**. Los cambios aquí se aplican a todos en la plataforma.

Dominios registrados y proveedores de identidades

Los usuarios son dirigidos a un proveedor de identidades por el dominio de su dirección de correo electrónico. Registre un dominio, asócielo con un proveedor configurado, y cualquiera que inicie sesión desde ese dominio será autenticado por él.



Así es como una implementación soporta más de una organización a la vez. Los empleados de su propio dominio pueden ir a su proveedor de identidades corporativo, mientras que los contratistas de otro dominio usan uno diferente.

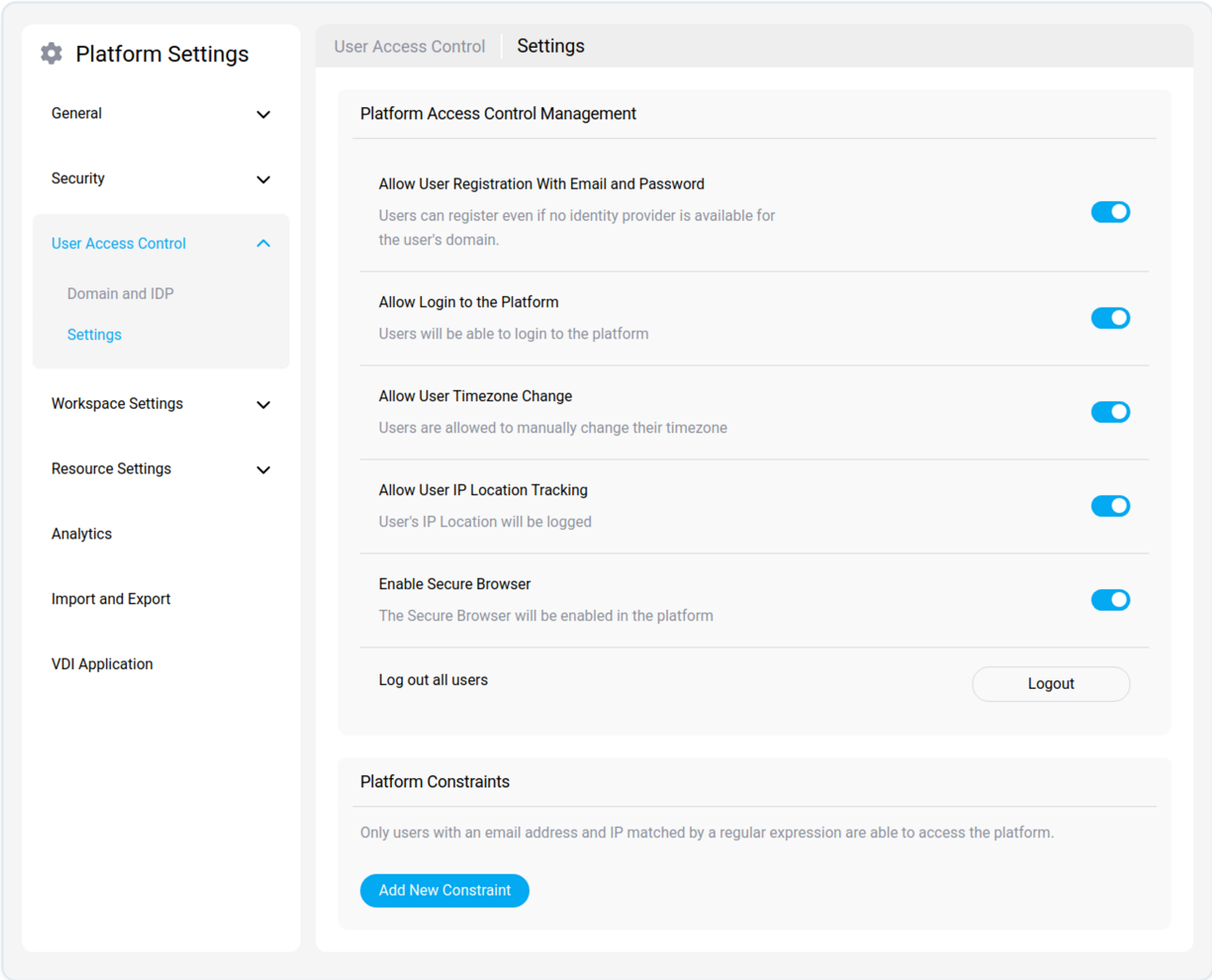
La autenticación de dos factores se habilita aquí, por dominio registrado.

Un dominio sin proveedor de identidades es el caso a observar. Si esos usuarios pueden iniciar sesión en absoluto depende de la restricción de plataforma a continuación que rige el registro con una dirección de correo electrónico y contraseña.

Consulte Proveedores de identidades para conectar un proveedor, y SAML o OpenID Connect para los protocolos.

Control de acceso y restricciones de la plataforma

Estas configuraciones se aplican a todos los usuarios de la plataforma, independientemente del rol que desempeñen.



CONFIGURACIÓN	CUANDO ESTÁ HABILITADO
Permitir inicio de sesión en la plataforma	Los usuarios pueden iniciar sesión. Desactivarlo cierra la plataforma para todos, lo cual es un control de mantenimiento y de incidentes, más que una configuración diaria.
Permitir el registro de usuarios con correo electrónico y contraseña	Los usuarios pueden registrarse incluso cuando ningún proveedor de identidad cubre su dominio. Desactívalo cuando todos los usuarios deban acceder a través de un proveedor de identidad.
Permitir el cambio de zona horaria del usuario	Los usuarios pueden establecer su propia zona horaria, lo que determina su horario de trabajo y, por lo tanto, cuándo se inician y pausan los espacios de trabajo.

CONFIGURACIÓN	CUANDO ESTÁ HABILITADO
Permitir el seguimiento de la ubicación IP del usuario	La ubicación IP del usuario se registra en los logs.
Soporte accesible para todos los usuarios	Todos los usuarios pueden acceder al menú de Soporte de la plataforma.

La configuración de registro es la que tiene el efecto más amplio. Si está activada, alguien cuyo dominio no esté registrado puede crear una cuenta con una contraseña, omitiendo el enrutamiento del proveedor de identidad anterior. La mayoría de las implementaciones que han conectado un proveedor de identidad deberían desactivarla.

Las restricciones de URL de imagen también forman parte de esta área. Consulta Acceso al registro.

Información relacionada

- Identidad y acceso
- Roles de la plataforma
- Roles y permisos
- Catálogo de controles

Code repositories

Antes de que el propietario de un proyecto pueda importar un repositorio, el proveedor de Git debe estar conectado a nivel de plataforma. Esa conexión es lo que permite a Citrix SecurSpaces™ autenticarse en nombre de un desarrollador, para que nadie tenga que guardar las credenciales del repositorio en su propio dispositivo.

Conecte un proveedor una vez. Cada organización y proyecto en la plataforma podrá importar repositorios desde él.

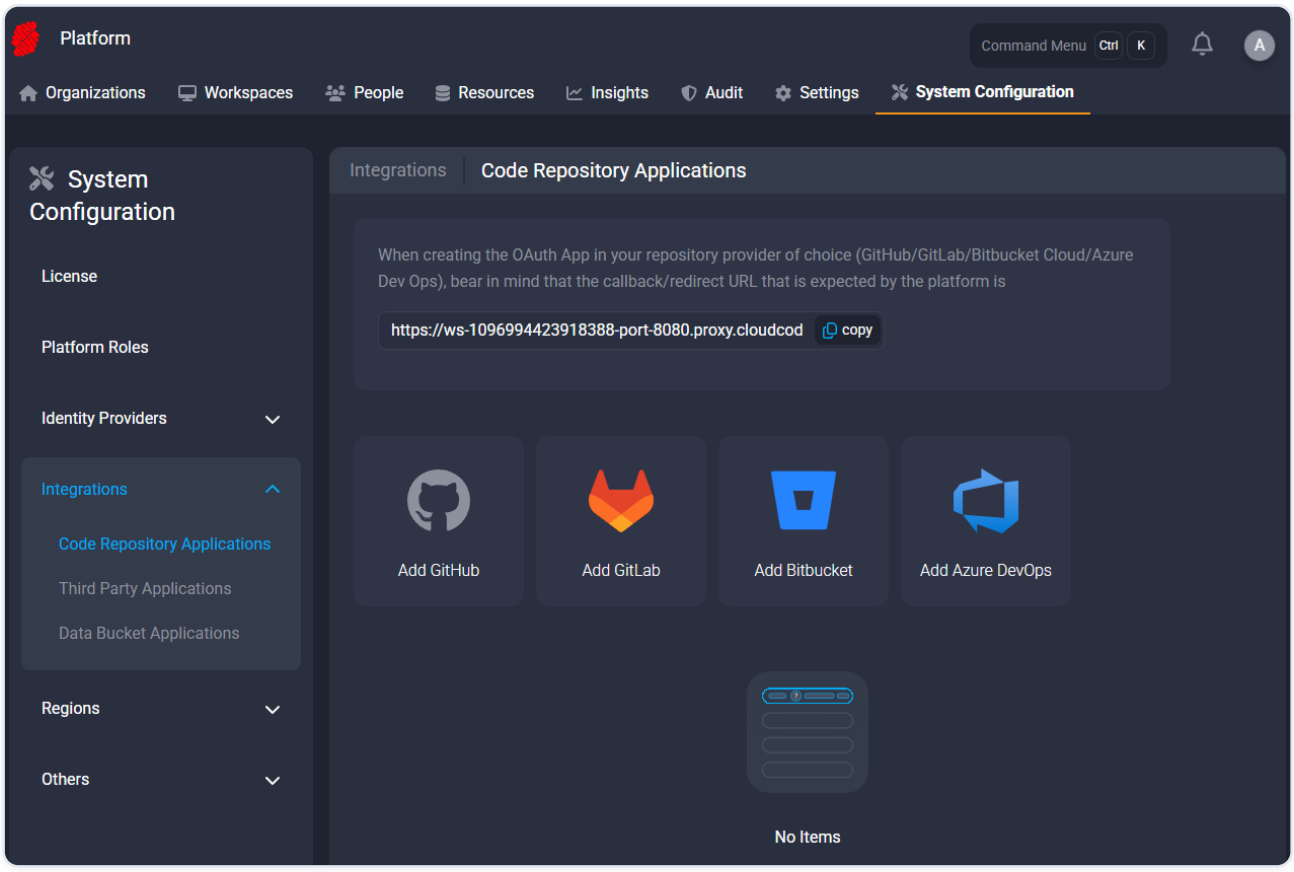
Elija un proveedor

PROVEEDOR	ALOJAMIENTO	LO QUE NECESITA
GitHub	Gestionado y autoalojado (GitHub Enterprise Server)	Una aplicación OAuth en su organización de GitHub

PROVEEDOR	ALOJAMIENTO	LO QUE NECESITA
GitLab	Gestionado y autoalojado	Una aplicación OAuth en su instancia de GitLab
Bitbucket	Nube y servidor	Credenciales que difieren entre la Nube y el Servidor — consulte la página
Azure DevOps	Gestionado	Un registro de aplicación en Microsoft Entra

Puede conectar más de uno, incluyendo dos instancias del mismo proveedor — por ejemplo, una organización de GitHub gestionada junto con un GitHub Enterprise Server autohospedado.

Se puede seguir utilizando un repositorio alojado en otro lugar. El propietario de un proyecto lo añade manualmente por URL, pero sin una aplicación conectada, la plataforma no puede enumerar repositorios ni inyectar credenciales para él.



¿Qué sucede después de conectarse?

El proveedor aparece como una opción cuando el propietario de un proyecto importa un repositorio. Consulte Repositorios de código para ver ese lado de la tarea.

A partir de entonces, las credenciales se inyectan en el espacio de trabajo en tiempo de ejecución y el tráfico al proveedor pasa a través del proxy de la plataforma, por lo que el acceso al repositorio es atribuible y puede ser auditado.

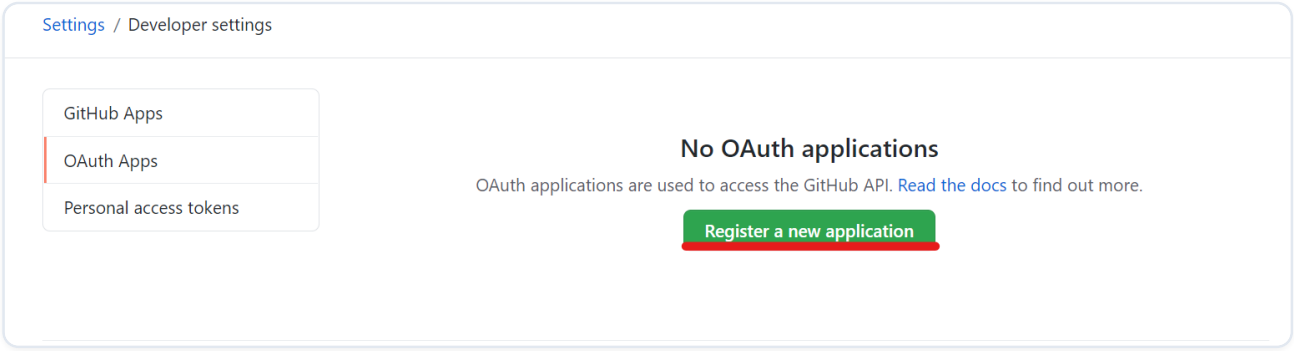
Información relacionada

- Integraciones
- Repositorios de código (nivel de proyecto)
- Límites de confianza

Connect GitHub

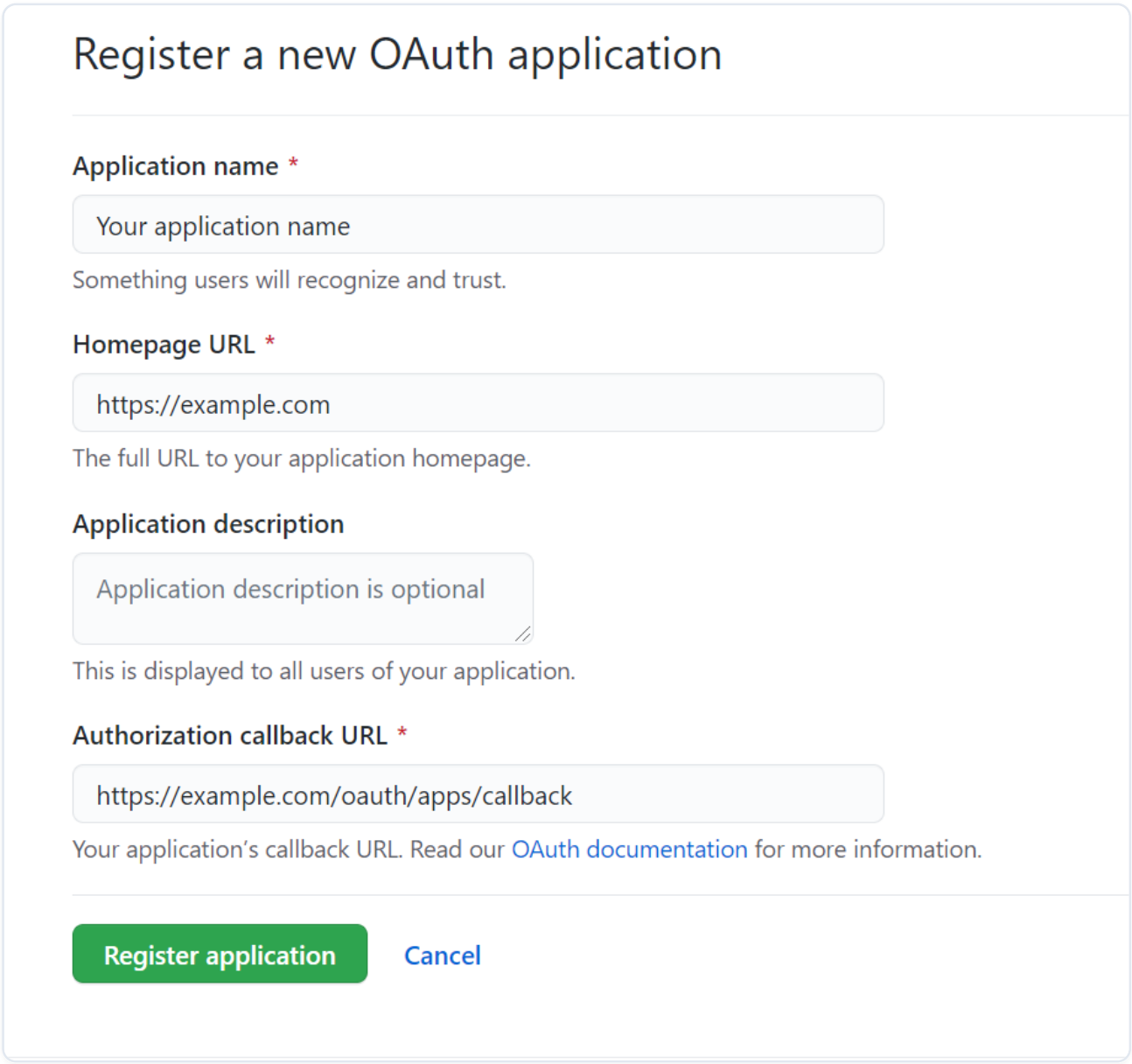
Siga estos pasos para crear una aplicación OAuth en GitHub y conectarla a la plataforma:

- **Navegar a la configuración de desarrollador:**
- Usando una cuenta de GitHub, vaya a su configuración y luego a "Configuración de desarrollador".
- Dentro de este menú, haga clic en "Aplicaciones OAuth".
- Puede seguir este https://github.com/settings/developers para acceder directamente a este menú.



- **Registrar nueva aplicación:**
- Haga clic en "Registrar nueva aplicación" y se le presentará una pantalla para configurar:
  - **Nombre de la aplicación:** A su discreción.
  - **URL de la página de inicio:** La ruta principal del dominio donde se ejecuta la plataforma.

- **URL de devolución de llamada de autorización:** La URL debe tener una estructura similar a `https://example.com/oauth/apps/callback`, donde "example.com" debe reemplazarse con el nombre de dominio adecuado (el mismo que la URL de la página de inicio).



- **Completar el registro:**
- Cuando este proceso esté terminado, haga clic en el botón verde "Registrar aplicación".
- Será redirigido a una nueva página de aplicación donde podrá ver el ID de cliente y generar el Secreto que debe configurarse en la plataforma.
- **Conceder acceso a la organización:**
- Deberá conceder acceso a la organización a esta aplicación OAuth recién creada en la organización que desea conectar a la plataforma.

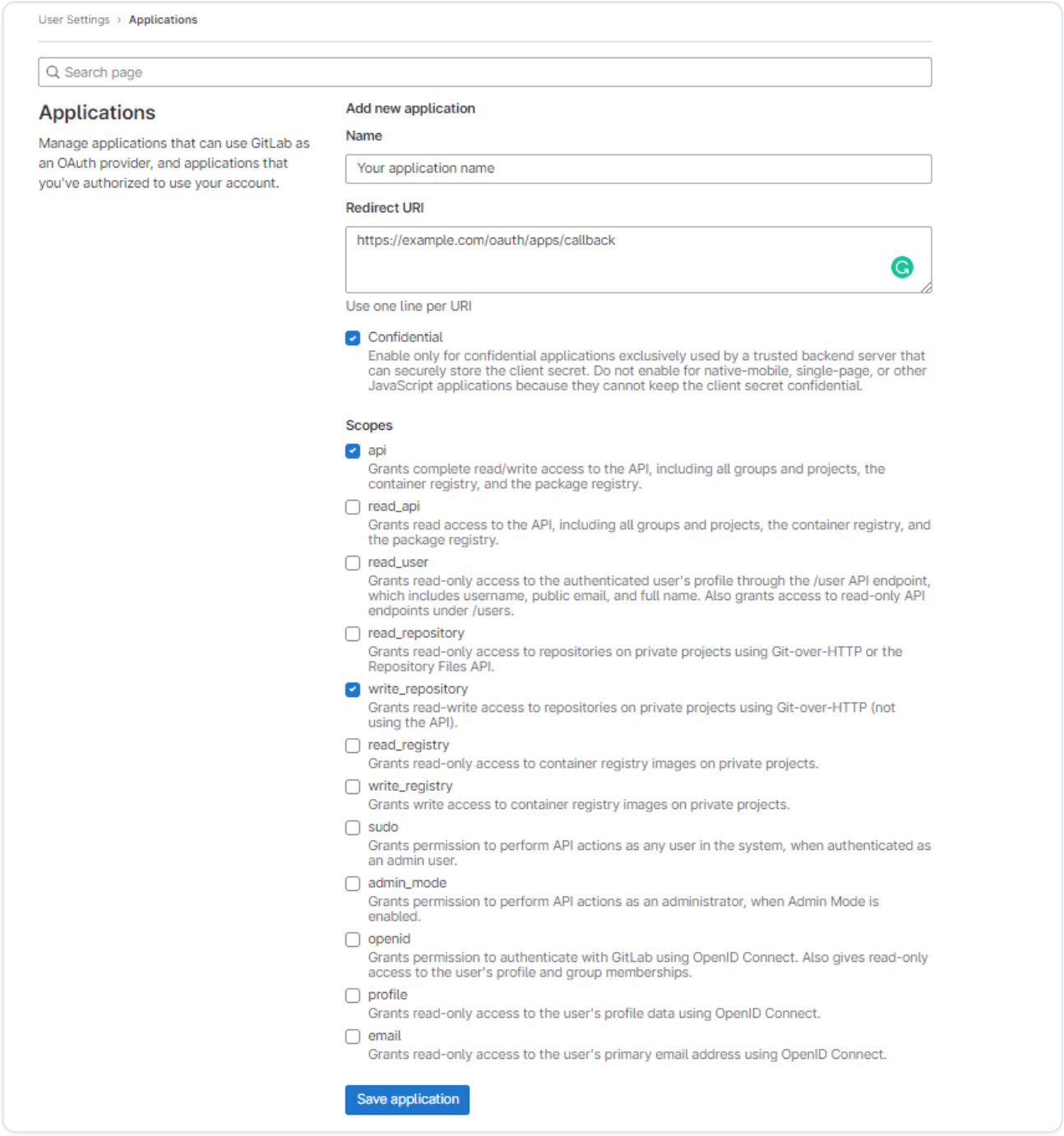
Información relacionada

- Azure DevOps
- Bitbucket
- GitLab
- Repositorios de código

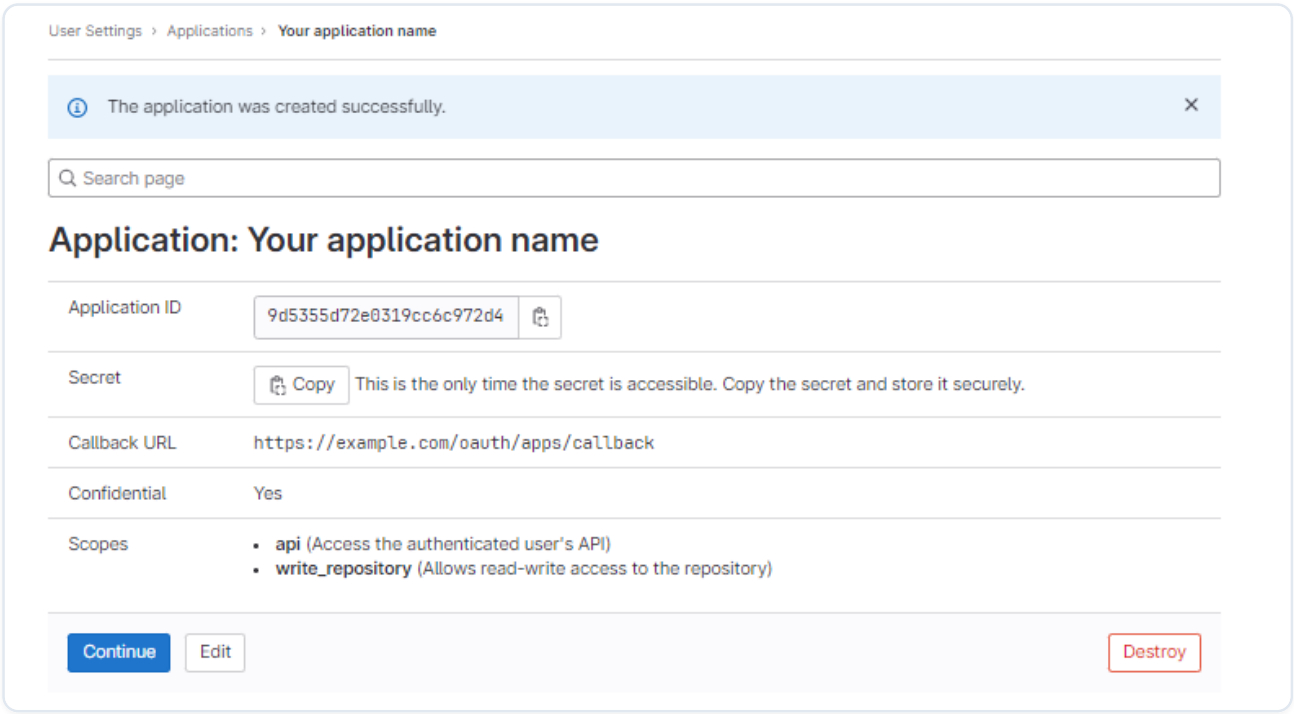
Connect GitLab

Siga estos pasos para crear una aplicación OAuth en GitLab y conectarla a la plataforma:

- **Navegar a Aplicaciones:**
- Con una cuenta de GitLab, vaya a la configuración de usuario y luego a «Aplicaciones».
- Puede seguir este https://gitlab.com/-/user_settings/applications para acceder directamente a este menú.
- **Crear una nueva aplicación OAuth:**
- Haga clic en «Nueva aplicación» y configure los siguientes campos:
  - **Nombre:** El nombre que desea dar a la aplicación. Será público.
  - **URI de redirección:** La URL debe tener una estructura similar a `https://example.com/oauth/apps/callback`, donde «example.com» debe ser reemplazado por el nombre de dominio adecuado.
  - **Confidencial:** Esto ya debería estar seleccionado por defecto; déjelo como está.
  - **Ámbitos:** Añada los ámbitos `api` y `write_repository`. Estos son necesarios para desplegar automáticamente las claves de despliegue.



- **Completar el registro:**
- Después de hacer clic en el botón «Guardar aplicación», se le presentará el ID de cliente (llamado ID de aplicación) y el Secreto, que deberá introducir en la configuración de la plataforma.



Información relacionada

- Azure DevOps
- Bitbucket
- GitHub
- Repositorios de código

Connect Bitbucket Cloud

Siga estos pasos para crear una aplicación OAuth en Bitbucket Cloud y conectarla a la plataforma:

- **Navegue a Consumidores OAuth:**
- Usando una cuenta de Bitbucket, vaya a la configuración principal de la organización y luego a "OAuth consumers".
- Puede seguir este `https://bitbucket.org/[YOUR_DOMAIN_NAME]/workspace/settings/api` para acceder directamente a este menú.
- **Añadir un nuevo consumidor:**
- Haga clic en el botón "Add consumer" y configure los siguientes campos:
  - **Nombre:** El nombre que desea dar a la aplicación. Será público.
  - **URL de devolución de llamada:** La URL debe tener una estructura similar a `https://example.com/oauth/apps/callback`, donde "example.com" debe ser reemplazado por el

nombre de dominio correcto. Esta URL se puede ver desde el panel de administración de la plataforma SecurSpaces.

- **Este es un consumidor privado:** Esto ya debería estar seleccionado por defecto; déjelo como está.
- **Ámbitos:** Seleccione "Read" en la sección Cuenta y "Write" en la sección Repositorios, y "Read" en la sección Solicitudes de extracción. Esto también se puede verificar en la plataforma Citrix SecurSpaces™ al hacer clic en el botón "Add Bitbucket".

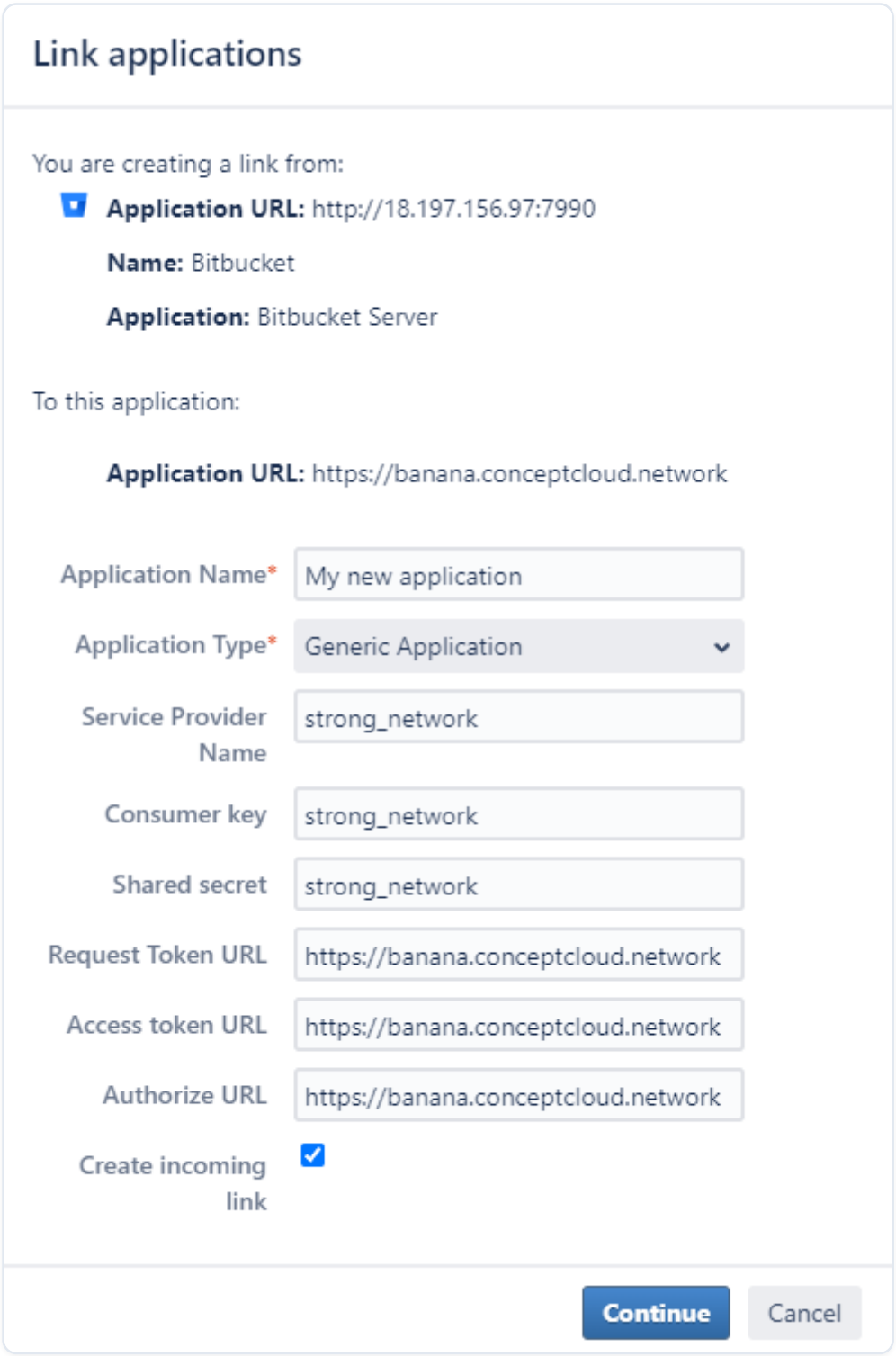
- **Complete el registro:**
- Después de hacer clic en el botón "Save", se le presentará el ID de cliente (llamado Key) y el Secreto, que deberá introducir en la configuración de la plataforma.

Integración de Bitbucket Server o Data Center como proveedor de repositorio de código

En esta sección, veremos cómo conectar la plataforma SecurSpaces a una instancia de Bitbucket autohospedada:

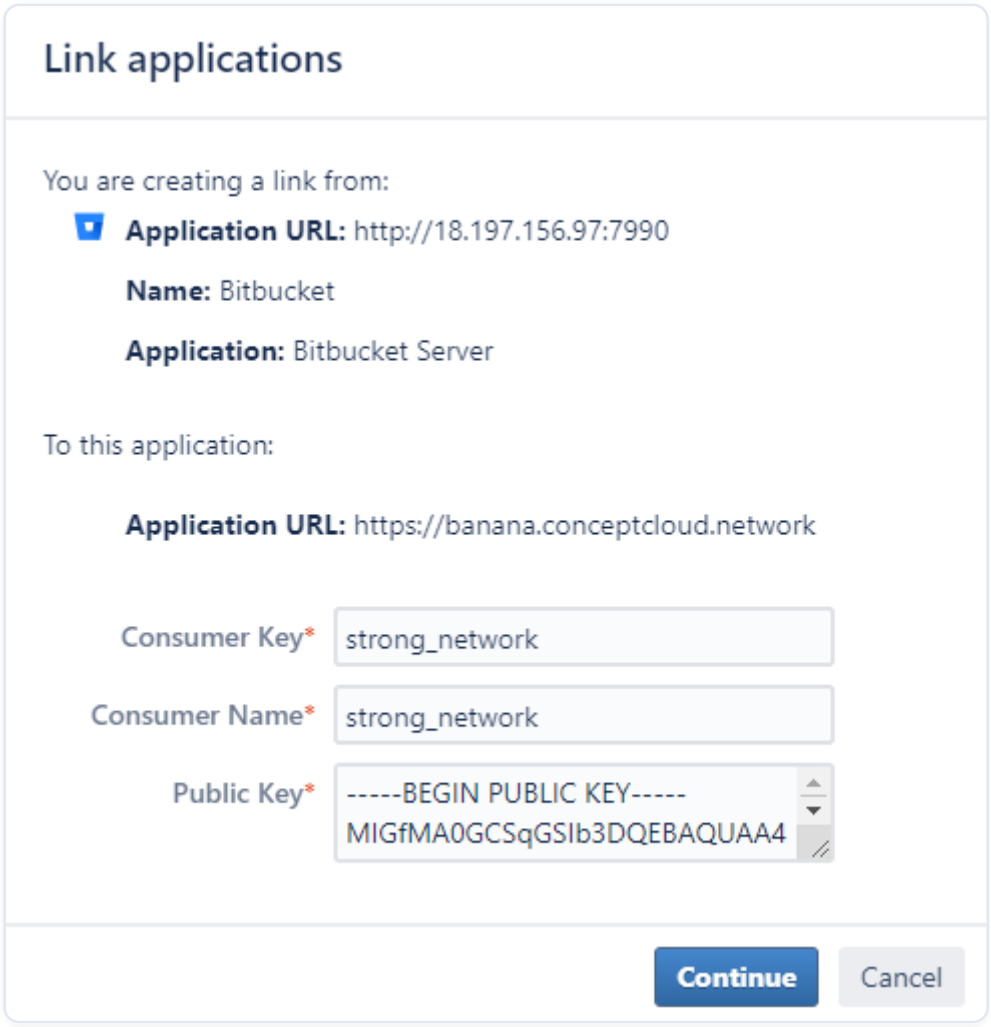
- **Configurar la plataforma SecurSpaces:**
- Ve a la configuración de la plataforma SecurSpaces y abre el menú "Aplicaciones de repositorio de código".
- Haz clic en el botón "Añadir Bitbucket".
- Selecciona la casilla de verificación para "Bitbucket Server o Data Center (autoalojado)".
- **Configura los siguientes campos:**
- **Nombre de la aplicación Bitbucket:** Puede ser cualquiera. Esto es lo que verán los usuarios al usar este proveedor de repositorio de código.
- **Dominio personalizado:** Introduce la URL donde está alojada la instancia de Bitbucket. Si no se especifica un esquema, se elegirá HTTPS por defecto.
- **Forzar a los usuarios a conectarse:** Si se selecciona, los usuarios deberán conectarse a Bitbucket antes de poder abrir sus espacios de trabajo. Esto puede evitar problemas de configuración/permisos por parte del usuario.
- **Completa el registro:**
- Haz clic en el botón "Crear" para completar la configuración en la plataforma SecurSpaces.
- Guarda la "Clave pública de Bitbucket Server" para usarla más tarde. También se puede encontrar en el menú de edición después de hacer clic en el botón "Crear".
- **Configurar instancia de Bitbucket (versión 7.20 o posterior):**

- Ve a Administración > Aplicaciones > Enlaces de aplicación y haz clic en "Crear enlace":
  - **Tipo de aplicación:** Aplicación externa
  - **Dirección:** Entrante
  - Haz clic en continuar
  - Establezca un nombre único
  - **URL de redirección:** Establezca `https://example.com/oauth/apps/callback`, donde "example.com" debe reemplazarse con el nombre de dominio adecuado.
  - **Permisos de la aplicación:** Cuenta: Escritura, Repositorios: Administrador
  - Después de hacer clic en el botón "Guardar", introduzca "strong_network" tanto para el ID de cliente como para el Secreto de cliente.
- **Configurar instancia de Bitbucket (versión 7.20 o anterior):**
- Vaya a Administración > Enlaces de aplicación.
- Introduzca la URL de la plataforma (p. ej., `https://example.com`, donde "example.com" debe reemplazarse con el nombre de dominio adecuado).
- Haga clic en "Crear nuevo enlace". Si ve un error de "No se ha recibido respuesta", ignórelo y haga clic en Continuar.
- En el siguiente menú, introduzca:
  - **Nombre de la aplicación:** Puede ser cualquiera.
  - **Tipo de aplicación:** Aplicación genérica
  - **Nombre del proveedor de servicios:** Puede ser cualquiera (recomendado: "strong_network").
  - **Clave de consumidor:** Establezca "strong_network".
  - **Secreto compartido:** Establezca "strong_network".
  - **URL de token de solicitud:** Establezca `http://example.com`, donde "example.com" debe reemplazarse con el nombre de dominio adecuado.
  - **URL de token de acceso:** Establecer en `http://example.com`, donde "example.com" debe reemplazarse con el nombre de dominio adecuado.
  - **URL de autorización:** Establecer en `http://example.com`, donde "example.com" debe reemplazarse con el nombre de dominio adecuado.
  - Marque "Crear enlace entrante" y haga clic en Continuar.



- En el siguiente menú, introduzca:
  - **Clave de consumidor:** Establecer en "strong_network".
  - **Nombre de consumidor:** Establecer en "strong_network".

- **Clave pública:** Introduzca el valor que se puede ver en la plataforma.



- **Completar la configuración:**
- Haga clic en Continuar. La configuración está completa.

Información relacionada

- Azure DevOps
- GitHub
- GitLab
- Repositorios de código

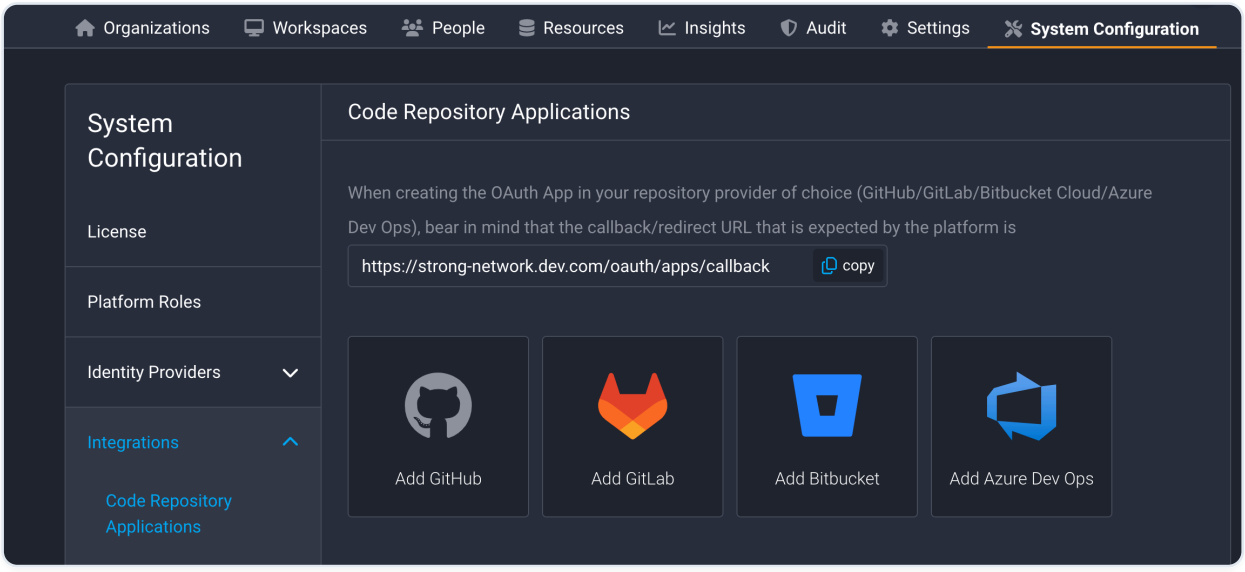
Azure DevOps

Siga estos pasos para crear una aplicación OAuth en Azure DevOps y conectarla a la plataforma.

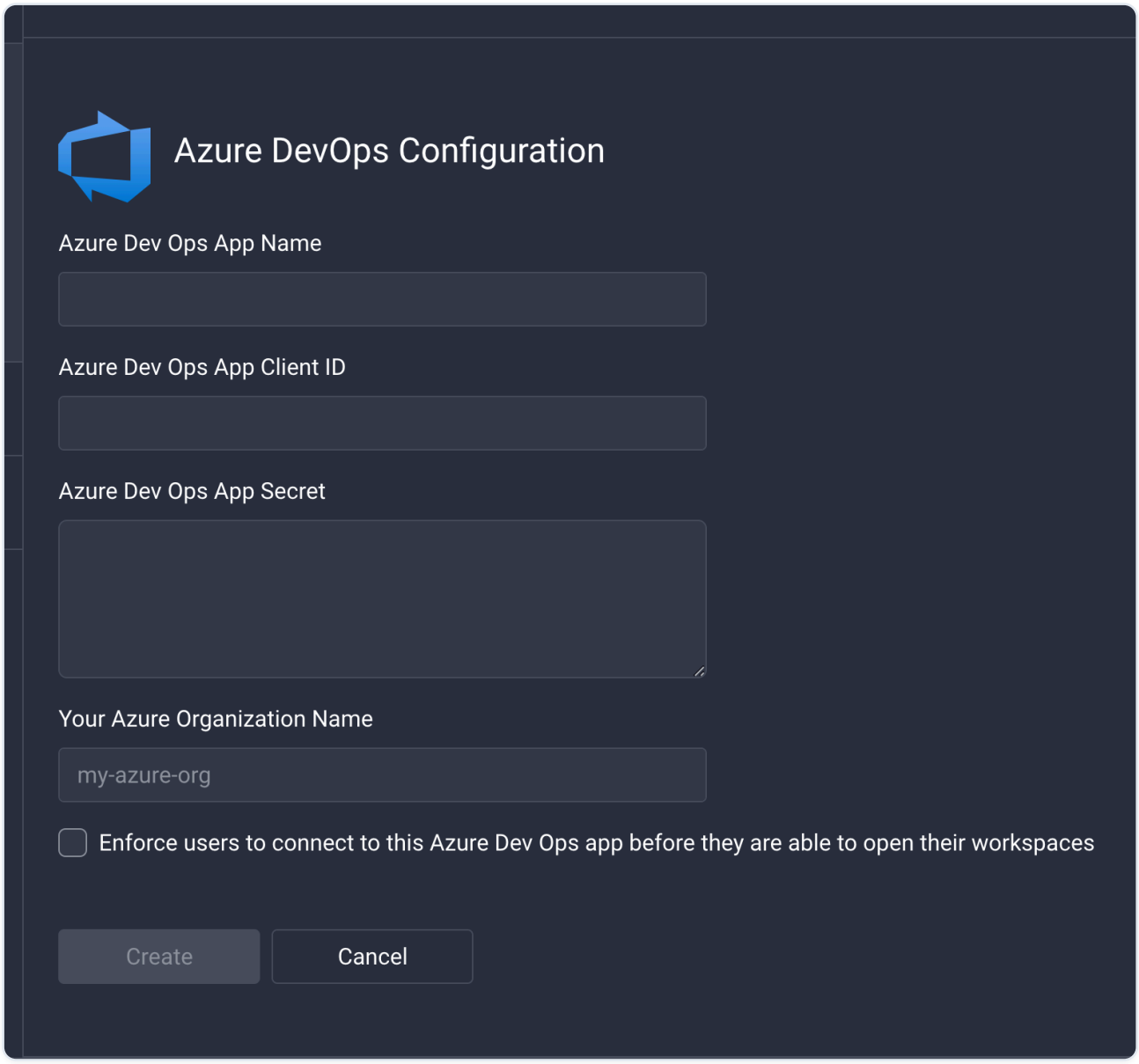
- Con una cuenta de Azure DevOps, vaya al siguiente enlace: Registrar una aplicación
- Haga clic en el botón «Add consumer» y configure los siguientes campos:

  - **Nombre de la empresa:** El nombre de su empresa.
  - **Nombre de la aplicación:** El nombre que desea dar a la aplicación. Será público.
  - **Sitio web de la aplicación:** Establezca en `https://example.com/oauth/apps/callback` (reemplace `example.com` con el nombre de dominio adecuado).
  - **URL de devolución de llamada de autorización:** Establezca en `https://example.com/oauth/apps/callback` (reemplace `example.com` con el nombre de dominio adecuado). Esta URL se puede encontrar en el panel de administración de la plataforma Citrix SecurSpaces™.
  - **Ámbitos autorizados:** `Code (read and write)` y `Project and team (read)`.

- Una vez hecho esto, haga clic en el botón «Create Application». Se le presentará el ID de cliente (llamado App ID) y el Secreto (llamado Client Secret) después de hacer clic en el botón «Show». Introduzca estos campos en la configuración de administrador de la plataforma SecurSpaces.
  - Registrar una aplicación
  - `https://example.com/oauth/apps/callback`
- Especifique el nombre de la organización de Azure. Esta aplicación solo puede acceder a los repositorios de esta organización específica. Para acceder a repositorios de diferentes organizaciones, cree varias aplicaciones de repositorio de código de Azure DevOps, cada una con su nombre de organización correspondiente. Puede usar el mismo ID de cliente y secreto en todas ellas.



Pegue el ID de cliente, el secreto de la aplicación y el nombre de la organización de los pasos anteriores:



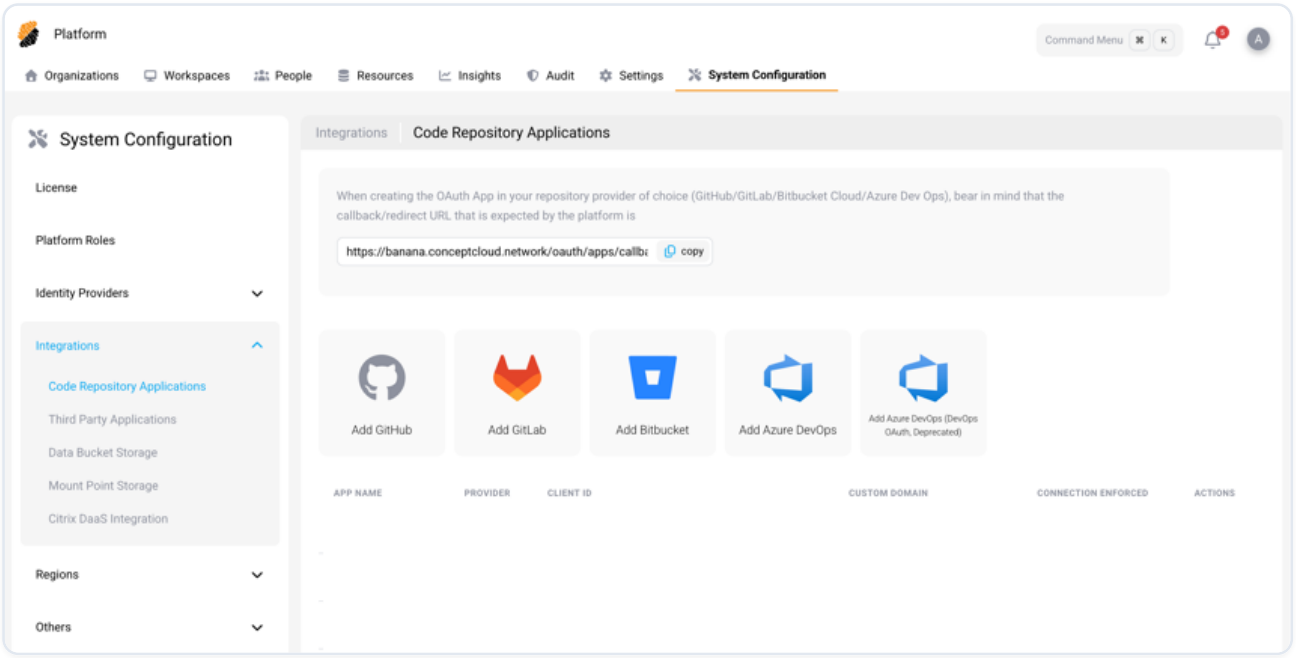
Información relacionada

- Bitbucket
- GitHub
- GitLab
- Repositorios de código

Integrations

Conecte Citrix SecurSpaces™ a las herramientas externas en las que confían sus equipos, desde repositorios de código y aplicaciones de terceros hasta almacenamiento y Citrix DaaS™. Active cada una y configúrela en **Integraciones**.

Encuentre estas configuraciones en **Configuración del sistema > Integraciones**.



Esto es lo que puede conectar:

- Aplicaciones de repositorio de código
- Aplicaciones de terceros
- Almacenamiento de cubos de datos
- Almacenamiento de puntos de montaje
- Integración de Citrix DaaS

Aplicaciones de repositorio de código

Agregue los proveedores de repositorio a los que sus desarrolladores se conectan desde sus espacios de trabajo, como GitHub, GitLab, Bitbucket y Azure DevOps. Cada uno se configura como una aplicación OAuth.

Para conocer los pasos de configuración, consulte Configurar aplicaciones de repositorio de código.

Aplicaciones de terceros

Agregue aplicaciones de terceros, como JFrog, a las que los desarrolladores acceden desde sus espacios de trabajo. Usted proporciona las credenciales y la URL de devolución de llamada que espera cada proveedor.

Para ver un ejemplo, consulte JFrog.

Almacenamiento de Data Buckets

Configure el almacenamiento detrás de **Data Buckets**, para que los equipos puedan compartir conjuntos de datos versionados, archivos y artefactos entre los espacios de trabajo de un proyecto.

Para obtener más información, consulte Data Buckets.

Almacenamiento de puntos de montaje

Active el **Almacenamiento de puntos de montaje** para dar a los equipos acceso directo al almacenamiento de archivos externo. Un punto de montaje conecta ese almacenamiento directamente al sistema de archivos del espacio de trabajo, de modo que los espacios de trabajo leen y escriben en tiempo real sin copiar datos en el clúster.

Active primero un tipo de almacenamiento aquí. Después de eso, los propietarios del proyecto pueden crear Puntos de Montaje. Los proveedores de almacenamiento compatibles incluyen Azure file storage, Amazon Elastic File System (EFS) y Amazon S3 Files.

Los interruptores que aparecen dependen de la nube que respalda los Puntos de Montaje, y la plataforma detecta esa nube a partir de las clases de almacenamiento de Puntos de Montaje presentes en el clúster en lugar de ofrecerla como una opción. En un clúster de AWS, un único interruptor, **Habilitar almacenamiento de archivos de AWS**, cubre tanto Amazon EFS como Amazon S3 Files.

> **Importante:**
>
> Los Puntos de Montaje de AWS dependen de recursos de AWS que SecurSpaces no crea, incluyendo el sistema de archivos, los destinos de montaje en cada Zona de Disponibilidad, los roles de IAM y las propias clases de almacenamiento de Kubernetes. Un administrador debe crear una clase de almacenamiento de AWS elegible en el clúster antes de que el tipo de almacenamiento de AWS aparezca aquí. Hasta entonces, no hay nada que activar.

> Los puntos de montaje no son compatibles con configuraciones multirregión.

Para obtener más información, consulte:

- Almacenamiento de puntos de montaje, para saber qué hace cada interruptor y qué permanece montado después de desactivar uno

- Preparar el almacenamiento de AWS para puntos de montaje, para los recursos de AWS que se crean antes de que aparezca la opción de AWS
- Compartir datos entre usuarios y Puntos de montaje, para lo que los propietarios del proyecto hacen a continuación

Integración de Citrix DaaS

Vincule SecurSpaces a Citrix DaaS y Citrix Workspace para que los usuarios accedan tanto a sus espacios de trabajo como a sus aplicaciones y escritorios virtuales de Citrix con un único inicio de sesión.

Para conocer los pasos de configuración, consulte Integración de Citrix DaaS.

Información relacionada

- Configuración del sistema

Use HashiCorp Vault as a secret manager

Puede usar **HashiCorp Vault** para almacenar todos los secretos de la plataforma en lugar de cifrarlos en MongoDB.

La plataforma Citrix SecurSpaces™ se conecta a HashiCorp Vault utilizando el **mecanismo de autenticación JWT** proporcionado por **Kubernetes**.

Para obtener más información, consulte Usar Kubernetes para la autenticación OIDC

Requisitos previos

La configuración depende de si su instancia de Vault está implementada en el mismo clúster de Kubernetes que la plataforma SecurSpaces:

- **Si Vault está implementado en el mismo clúster:**

  El punto de conexión del emisor de OpenID Connect (OIDC) es accesible automáticamente.

- **Si Vault está implementado en un clúster diferente:**

  Asegúrese de que el punto de conexión del emisor de OIDC del clúster de SecurSpaces sea accesible para Vault. Si no lo es, debe agregar manualmente la(s) **clave(s) pública(s) de firma** del clúster de SecurSpaces.

  Para obtener más detalles, consulte Usar Kubernetes para la autenticación OIDC

Configuración

Puede configurar Vault en la plataforma SecurSpaces utilizando los siguientes cuatro valores del gráfico de Helm:

```
# hashicorpVault:

#   If set, secrets are stored in Vault instead of the database.

#   vaultAddress: "https://example.com:8200"

#   vaultRoleName: "sds-role"

#   customMountPath: "" # Default is "secret"

#   vaultCertB64: ""    # Base64-encoded PEM CA certificate (optional)
```

Descripciones de los parámetros

PARÁMETRO	DESCRIPCIÓN
vaultAddress	Especifica la dirección de Vault. La instancia de Vault debe ser accesible desde el clúster de SecurSpaces. Todos los servicios de la plataforma utilizan esta dirección para almacenar y recuperar secretos.
vaultRoleName	Especifica el nombre del rol de Vault configurado para SecurSpaces. Si diferentes servicios de Kubernetes usan diferentes cuentas de servicio, el campo `bound_subject` puede variar. Puede omitir este campo al crear el rol.
customMountPath	Especifica la ruta de Vault donde se almacenan los secretos. Opcional. El valor predeterminado es `secret`.
vaultCertB64	Especifica el certificado TLS codificado en Base64 para Vault. Use esta configuración si Vault utiliza un certificado autofirmado. Opcional.

Información relacionada

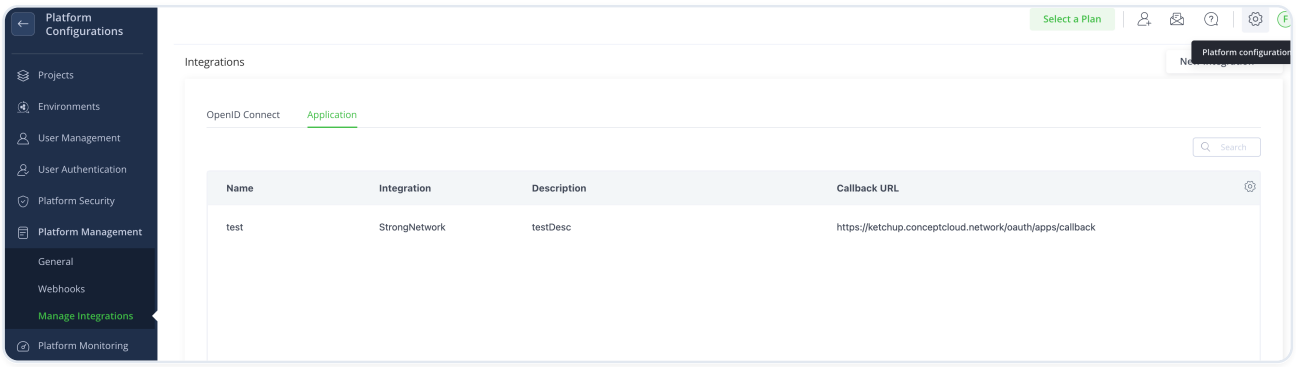
- AI Gateway
- Plugin de Backstage
- Citrix DaaS
- JFrog
- Publicar JetBrains Gateway
- Integraciones

Register JFrog as a third-party app

Puede seguir estos pasos para conectar su instancia de JFrog y la plataforma Citrix SecurSpaces™.

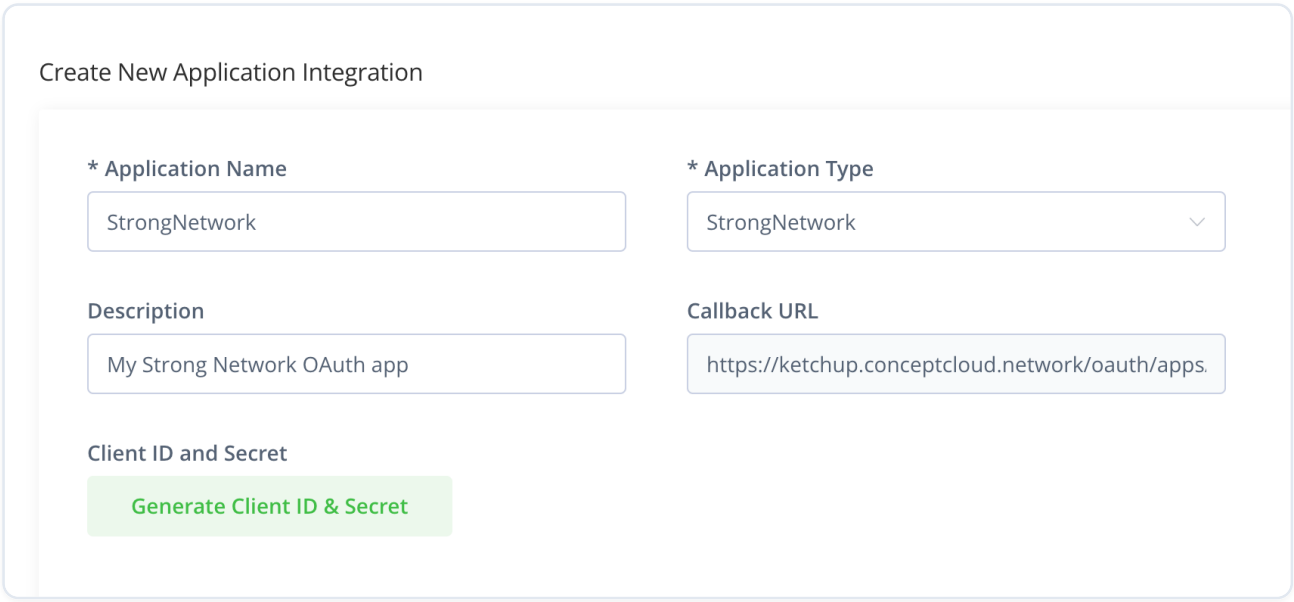
Actualmente, esta configuración solo se puede realizar en instancias de JFrog autohospedadas o solicitándolo al equipo de soporte de JFrog en la versión SaaS.

Inicie sesión en su implementación de JFrog como administrador, vaya a Gestión de plataforma y luego a Gestionar integraciones. Vaya a la pestaña llamada “Aplicación”. También puede seguir el enlace: `https://[your_domain_name].jfrog.io/ui/admin/configuration/integrations`



Haga clic en “Nueva integración” de tipo “Aplicación” y rellene los siguientes campos:

- **Nombre de la aplicación:** A su elección.
- **Tipo de aplicación:** Seleccione la plantilla que añadió en el archivo values.yaml.
- **Descripción:** A su elección.
- **URL de devolución de llamada:** Puede encontrarla en el menú de administrador de Aplicaciones de terceros en la plataforma SecurSpaces y tiene el formato de `https://[your_strong_network_domain]/oauth/apps/callback`

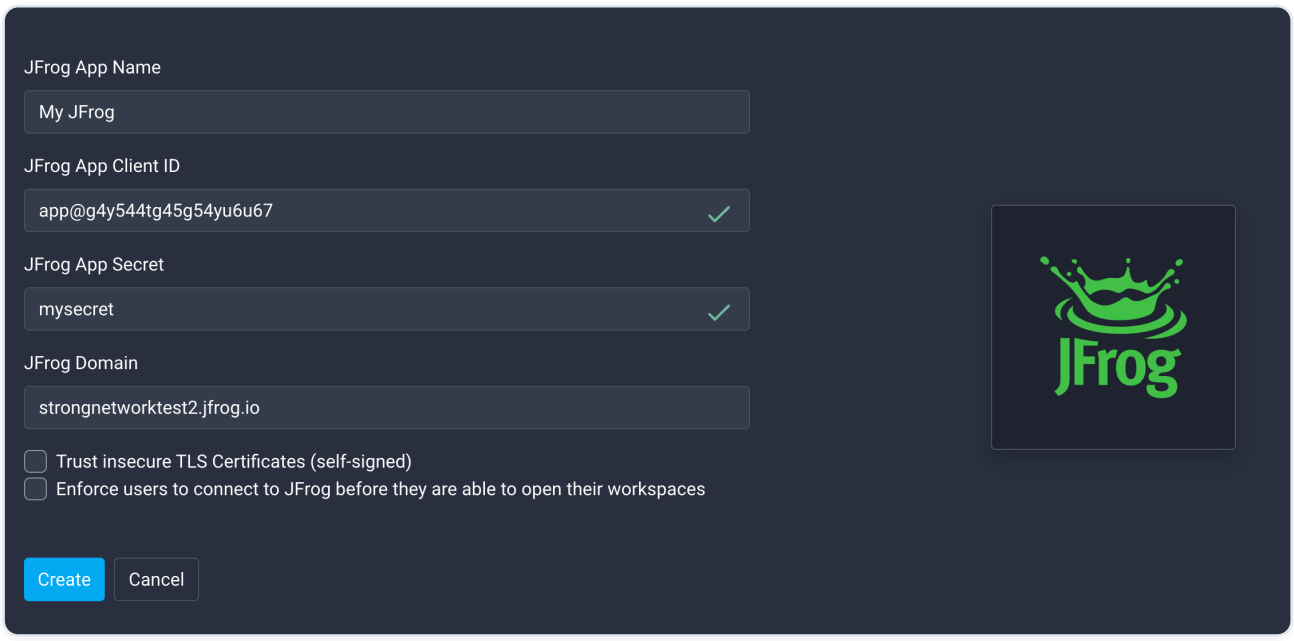


Haga clic en `Generate Client ID & Secret` y copie los valores.

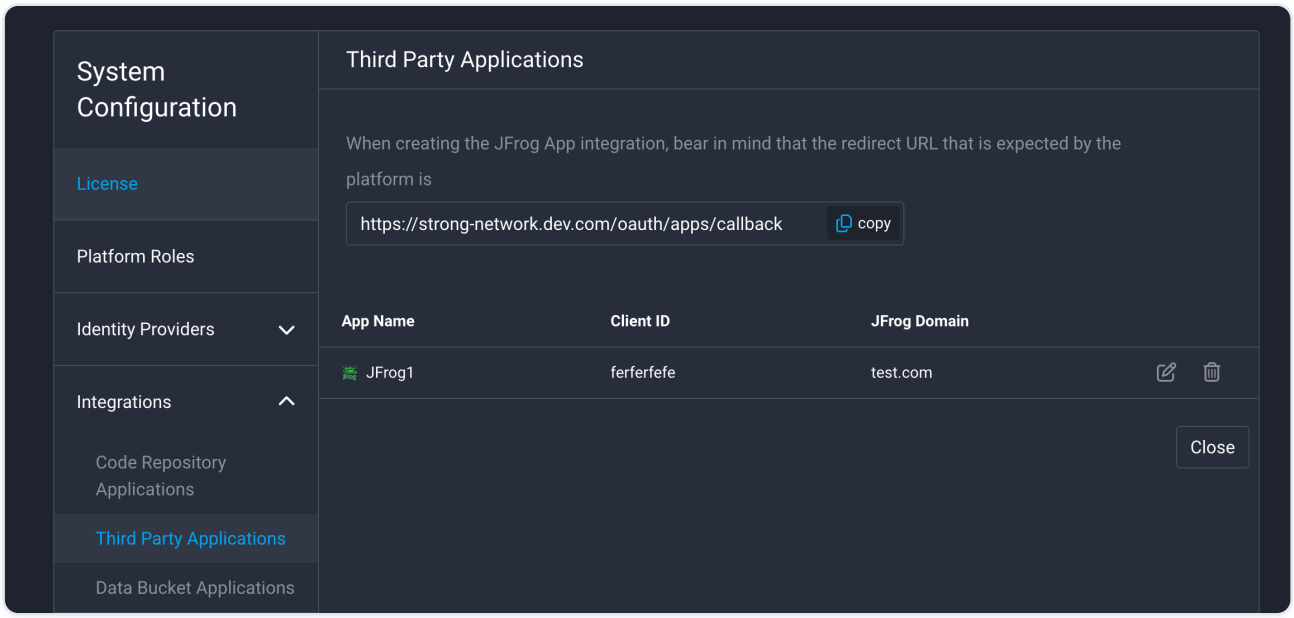
Por último, inicie sesión como administrador en la plataforma SecurSpaces, vaya a Configuración del sistema → Aplicaciones de terceros y seleccione JFrog. Deberá introducir:

- **Nombre:** A su elección, se mostrará a los usuarios de la plataforma
- **ID de cliente y secreto:** Valores copiados de JFrog
- **Dominio:** Su dominio de JFrog

Puede elegir si desea que la plataforma confíe en certificados TLS inseguros en caso de que su implementación de JFrog no tenga un certificado válido. También es posible que desee que los usuarios se conecten siempre a JFrog antes de acceder a sus espacios de trabajo; en este caso, recibirán una ventana emergente donde deberán conectarse antes de abrirlos. Si no selecciona esta opción, recibirán la ventana emergente pero podrán descartarla.

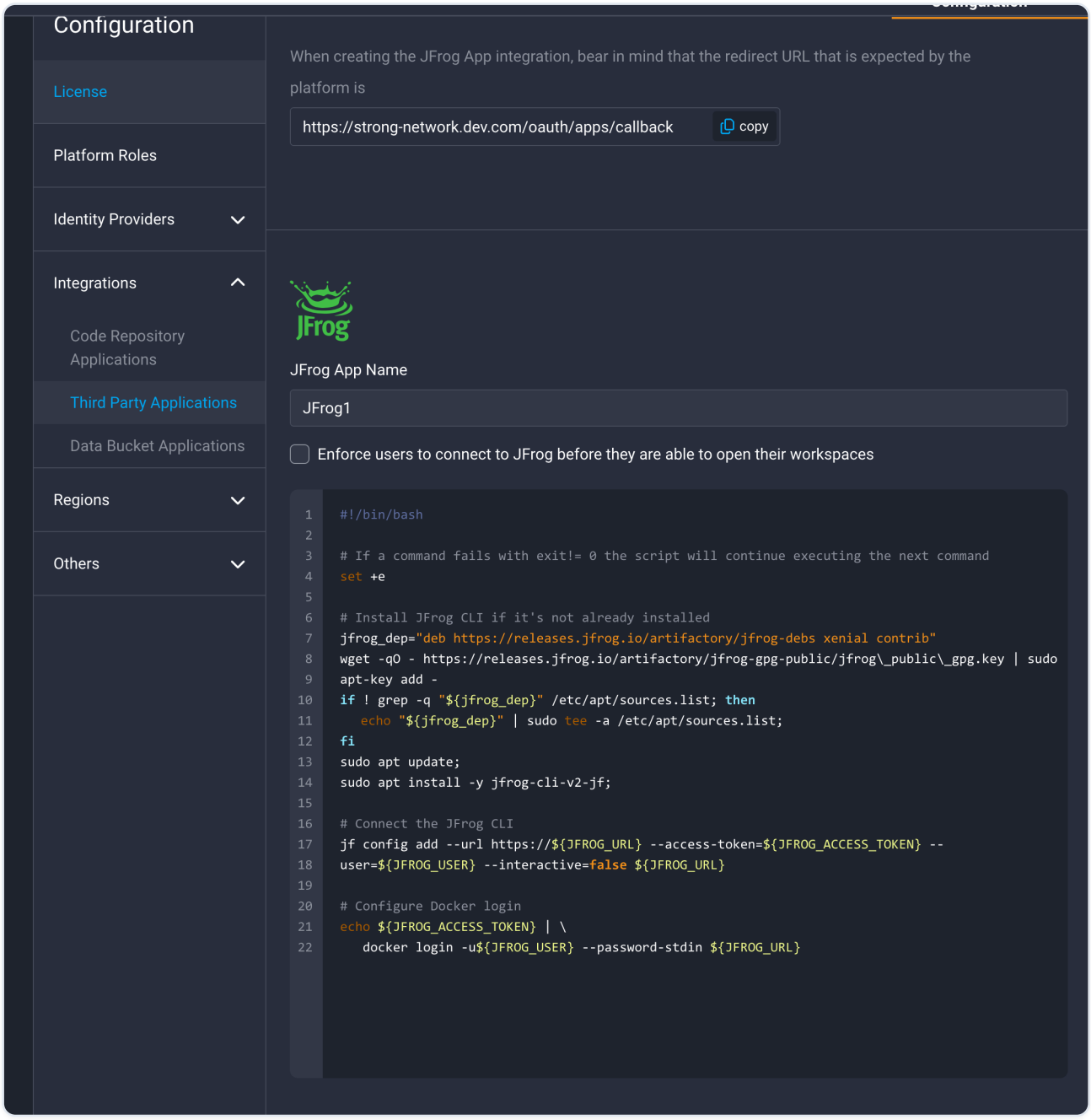


Cuando la aplicación está configurada, puede editarla haciendo clic en el icono de edición en el lado derecho.



Verá un menú en el que puede cambiar algunas configuraciones. En dicho menú, puede cambiar el script de inicio predeterminado de JFrog. Este es un script que se ejecutará en cada espacio de trabajo propiedad de un usuario que haya conectado su cuenta de JFrog. Puede ser útil para configurar ajustes específicos en todos los espacios de trabajo, por ejemplo, para configurar los diferentes lenguajes de programación para obtener las dependencias de su plataforma JFrog. Cada usuario puede basarse en este script para personalizarlo según sus propias necesidades.

Si este script predeterminado se actualiza, se cambiará automáticamente para los usuarios que no hayan definido su script personalizado.



Finalmente, si desea guardar los cambios, haga clic en “Guardar”. Ahora JFrog está configurado en toda la plataforma SecurSpaces, listo para ser utilizado sin problemas por los usuarios.

Información relacionada

- Pasarela de IA
- Plugin de Backstage
- Citrix DaaS
- Publicar JetBrains Gateway
- HashiCorp Vault como gestor de secretos
- Integraciones

Configure AI Gateway routing in SecurSpaces

Puede enrutar el tráfico seleccionado del servicio de IA desde los espacios de trabajo de Citrix SecurSpaces™ a través de una puerta de enlace de IA interna configurando los valores de Helm. Utilice esta opción cuando su organización desee un enrutamiento centralizado o control de políticas para los puntos finales del proveedor de IA.

Enrutar el tráfico de IA a través de una puerta de enlace también le proporciona un único lugar para medir el uso de la IA. SecurSpaces etiqueta cada solicitud reenviada con el usuario, el proyecto y el espacio de trabajo de origen, de modo que la puerta de enlace puede informar qué equipos y desarrolladores están consumiendo tokens. Consulte Informar sobre el uso de la IA.

Qué hace SecurSpaces y qué hace la puerta de enlace

Vale la pena separar las dos mitades, porque la división decide qué preguntas responde esta página.

SecurSpaces proporciona la interceptación y la atribución. El servicio de proxy de SecurSpaces ya termina e inspecciona el tráfico del espacio de trabajo. Reconoce las solicitudes destinadas a un punto final de IA configurado y etiqueta cada una de ellas con el usuario, el proyecto y el espacio de trabajo que la produjo. Esa es una capacidad de la plataforma y no depende de la puerta de enlace que ejecute.

La puerta de enlace proporciona enrutamiento y políticas. A dónde va una solicitud, qué credencial se utiliza, los límites de velocidad, y la superficie de informes son trabajo de la puerta de enlace.

Qué puerta de enlace

SecurSpaces reenvía a la dirección de servicio que configure en `platform.aiGateway.address`, por lo que la puerta de enlace es su elección:

PUERTA DE ENLACE	NOTAS
Puerta de enlace de IA de Envoy	Lo que cubre esta página, incluida la instalación
Puerta de enlace de IA de NetScaler	Una alternativa si ya ejecuta NetScaler. Consulte Puerta de enlace de IA en la documentación de NetScaler

Una nota sobre la terminología

La industria no se ha puesto de acuerdo en un único nombre para este componente. Algunos proveedores utilizan **AI Bridge** para el mismo concepto. En todos los productos de Citrix se denomina **AI Gateway**, y ese es el término que se utiliza en toda esta documentación.

Gobernanza del Protocolo de Contexto del Modelo

La gobernanza del tráfico MCP —a qué herramientas puede acceder un agente y qué puede hacer a través de ellas— está fuera del alcance de lo que SecurSpaces proporciona. SecurSpaces gobierna el espacio de trabajo en el que se ejecuta un agente y atribuye lo que consume; no inspecciona ni controla las llamadas MCP.

Cuando se requiere la gobernanza de MCP, NetScaler la proporciona. Consulte puerta de enlace MCP en la documentación de NetScaler.

Cómo se enruta el tráfico de IA

El tráfico de IA fluye desde el espacio de trabajo al servicio de proxy de SecurSpaces, luego a la AI Gateway y, finalmente, al punto de conexión LLM.

El servicio de proxy de SecurSpaces ya termina, inspecciona y vuelve a cifrar el tráfico HTTPS. El enrutamiento de la AI Gateway reutiliza esa capacidad para identificar las solicitudes que están destinadas a un punto de conexión LLM configurado, añadirles metadatos de SecurSpaces y reenviarlas a la puerta de enlace. El tráfico que no coincide con un punto de conexión configurado no se ve afectado.

Para ejecutar agentes dentro de los espacios de trabajo —aislamiento, ámbito de credenciales y coste—, consulte Ejecutar agentes de codificación de IA en espacios de trabajo.

Requisitos previos

- Un servicio interno de AI Gateway al que se pueda acceder desde los pods del servicio de proxy de SecurSpaces. Si no tiene uno, consulte Instalar Envoy AI Gateway.
- Los nombres de los puntos de conexión DNS que deben enrutarse a través de la AI Gateway
- Acceso para actualizar los valores de Helm de SecurSpaces y ejecutar `helm upgrade`

Instalar Envoy AI Gateway

SecurSpaces funciona con cualquier puerta de enlace que acepte el tráfico reenviado. Envoy AI Gateway es la implementación de referencia, y esta sección cubre lo que es específico para usarlo

con SecurSpaces. Para la instalación en sí, siga la documentación de Envoy AI Gateway, que se mantiene actualizada con el proyecto.

La instalación consta de dos partes, ambas mediante un gráfico de Helm:

COMPONENTE	ESPACIO DE NOMBRES
Envoy Gateway, el plano de control y de datos sobre el que se basa	`envoy-gateway-system`
Envoy AI Gateway, sus CRD y controlador	`envoy-ai-gateway-system`

Nota:

La instalación de Envoy Gateway **no** interfiere con su controlador de entrada existente. Crea sus propios pods y servicios de proxy en su propio espacio de nombres, y deja NGINX, NetScaler, HAProxy o cualquier otra cosa que sirva a la plataforma intactos. Consulte Ingress.

Envoy AI Gateway requiere Kubernetes 1.32 o posterior, requisito que cualquier clúster que ejecute SecurSpaces ya supera. Consulte Requisitos del sistema.

Fije las versiones del gráfico en lugar de seguir la última etiqueta. Las etiquetas de contenedor para las versiones en desarrollo se sobrescriben, por lo que una instalación no fijada puede cambiar entre implementaciones.

Cuando el gateway esté en funcionamiento, establezca `platform.aiGateway.address` en su dirección de servicio interno, como se describe en Configurar el enrutamiento del AI Gateway en toda la plataforma.

Aumentar el límite del búfer del cliente

Las solicitudes y respuestas de IA son considerablemente más grandes que el tráfico web típico, y el búfer predeterminado de Envoy no está dimensionado para ellas. Sin esto, las indicaciones grandes y las finalizaciones largas se truncan:

```
apiVersion: gateway.envoyproxy.io/v1alpha1

kind: ClientTrafficPolicy
```

```
metadata:

  name: client-buffer-limit

spec:

  targetRefs:

    - group: gateway.networking.k8s.io

      kind: Gateway

      name: <your-gateway-name>

  connection:

    bufferLimit: 50Mi
```

Establezca CPU y memoria explícitas también en la implementación del proxy de Envoy. La configuración de referencia los deja vacíos, lo cual es viable en un laboratorio pero no en producción.

Limitación de velocidad

Envoy AI Gateway puede aplicar límites de tasa basados en tokens por modelo, respaldados por Redis. Esto se configura completamente en la pasarela y no necesita nada de SecurSpaces. Consulte la documentación de Envoy AI Gateway para la configuración de `BackendTrafficPolicy` y el seguimiento de tokens.

Configurar el enrutamiento de la pasarela de IA en toda la plataforma

Añada el bloque `platform.aiGateway` a sus valores de Helm:

```
platform:

  aiGateway:

    address: "http://envoy-default-envoy-ai-gateway-07856df5.envoy-
gateway-system.svc.cluster.local"

    headers:
```

```
    userIdHeader: "x-user-id"
    projectIdHeader: "x-project-id"
    workspaceIdHeader: "x-workspace-id"
    hideProjectName: false
  healthCheck:
    enabled: false
    port: "80"
    failOpen: false
  dnsEndpoints:
    - "api.business.githubcopilot.com."
    - "copilot-proxy.githubusercontent.com."
    - "api.openai.com."
    - "chat.openai.com."
    - "chatgpt.com."
    - "api.anthropic.com."
    - "claude.ai."
    - "generativelanguage.googleapis.com."
    - "gemini.google.com."
    - "bard.google.com."
```

El valor `address` es la dirección de servicio interno para la pasarela de IA y puede incluir un esquema. La lista `dnsEndpoints` define los dominios del proveedor de IA que SecurSpaces intercepta y enruta a través de esa pasarela. Cada entrada es un nombre de dominio

completamente cualificado con un punto final, y se admiten entradas comodín como `"*.openai.azure.com."`.

SecurSpaces incluye una lista de puntos finales predeterminada que cubre los proveedores de LLM públicos más comunes, incluidos GitHub Copilot, OpenAI, Anthropic, Google, Azure OpenAI, Amazon Bedrock, Mistral y Hugging Face. La lista se actualiza como parte del ciclo de lanzamiento normal. Entre lanzamientos, mantenga la lista actualizada usted mismo y añada cualquier punto final de LLM privado o autoalojado que utilice su organización.

Identificar el uso de IA por usuario, proyecto y espacio de trabajo

SecurSpaces añade metadatos a cada solicitud que reenvía a la pasarela de IA, de modo que el uso de IA se pueda atribuir al espacio de trabajo que lo produjo. La pasarela y su pila de monitorización utilizan estas cabeceras para desglosar el uso por usuario, proyecto y espacio de trabajo.

Configure los nombres de las cabeceras en `platform.aiGateway.headers`:

VALOR	PREDETERMINADO	DESCRIPCIÓN
`userIdHeader`	`x-user-id`	Cabecera que contiene el ID del usuario que realizó la solicitud.
`projectIdHeader`	`x-project-id`	Encabezado que contiene el proyecto al que pertenece el espacio de trabajo.
`workspaceIdHeader`	`x-workspace-id`	Encabezado que contiene el ID del espacio de trabajo de origen.
`hideProjectName`	`false`	Cuando `false`, el encabezado del proyecto lleva el nombre del proyecto. Establezca en `true` para enviar el ID numérico del proyecto en su lugar.

Deje un nombre de encabezado vacío para evitar que SecurSpaces envíe ese valor.

> **Nota**

> Mantenga `hideProjectName` establecido en `false` si desea que los informes muestren nombres de proyecto legibles. Establézcalo en `true` cuando los nombres de proyecto sean sensibles y no deban salir del clúster.

Enrutar el tráfico de GitHub Copilot

GitHub Copilot necesita un manejo adicional, porque Envoy AI Gateway no lo reconoce como un proveedor por sí mismo. SecurSpaces cierra esa brecha para `api.githubcopilot.com` y `api.business.githubcopilot.com`: presenta cada solicitud en un formato que los procesadores de la pasarela reconocen y añade encabezados que sus reglas de enrutamiento pueden seleccionar.

Esto cubre las finalizaciones de chat compatibles con OpenAI, la API de respuestas de OpenAI y modelos de Anthropic como Claude. Usted configura las rutas; el resto es automático.

Encabezados a coincidir en sus rutas

Las reglas de enrutamiento en el gateway seleccionan un backend utilizando los encabezados que añade SecurSpaces:

ENCABEZADO	VALOR	COINCIDIR CON
`x-ai-process`	`true`	Seleccionar el tráfico de IA que el gateway debe procesar
`x-original-host`	El host solicitado por el espacio de trabajo	Elegir el backend de Copilot correcto
`x-ai-provider`	`anthropic`	Enrutar solicitudes de Anthropic, cuando sus equipos usan Claude a través de Copilot

Configurar el gateway

Defina un `Backend` para cada host de Copilot, un `BackendTLSPolicy` para que el gateway origine TLS hacia él, y reglas de enrutamiento que coincidan con los encabezados anteriores. Por ejemplo:

```
apiVersion: gateway.envoyproxy.io/v1alpha1

kind: Backend

metadata:

  name: github-copilot-chat

spec:

  endpoints:

    - fqdn:

        hostname: api.business.githubcopilot.com

        port: 443

---

apiVersion: gateway.networking.k8s.io/v1

kind: BackendTLSPolicy

metadata:

  name: github-copilot-chat-tls

spec:

  targetRefs:

    - group: gateway.envoyproxy.io

      kind: Backend

      name: github-copilot-chat

  validation:

    hostname: api.business.githubcopilot.com
```

```
    wellKnownCACertificates: System
```

Luego, haga coincidir los encabezados en su ruta y permita un tiempo de espera de solicitud generoso porque las respuestas del modelo son lentas:

```
rules:
  - timeouts:
      request: 300s
    matches:
      - headers:
          - type: Exact
            name: x-ai-process
            value: "true"
          - type: Exact
            name: x-original-host
            value: api.business.githubcopilot.com
    backendRefs:
      - name: github-copilot-chat
```

Repita para los otros hosts de Copilot a los que acceden sus desarrolladores.

Claude a través de Copilot

Si sus equipos usan Claude, añada un `AIServiceBackend` con el esquema de Anthropic y dirija `x-ai-provider: anthropic` a él.

Establezca `prefix: "/v1"` en el esquema. SecurSpaces presenta las solicitudes de Anthropic como `/anthropic/v1/messages` para que la pasarela seleccione su procesador de Anthropic. El

prefijo es lo que restaura la ruta ascendente real después. Sin él, la solicitud llega a Anthropic con el prefijo de enrutamiento aún adjunto, y falla.

```
apiVersion: aigateway.envoyproxy.io/v1beta1

kind: AIServiceBackend

metadata:

  name: github-copilot-chat-anthropic

spec:

  schema:

    name: Anthropic

    prefix: "/v1"

  backendRef:

    name: github-copilot-chat

    kind: Backend

    group: gateway.envoyproxy.io
```

Nota:

El punto final MCP de Copilot también se puede publicar a través de la pasarela con un `MCPRoute`, reenviando el encabezado `Authorization` del llamante para que cada desarrollador se autentique como sí mismo.

Tipos de herramientas en la API de respuestas

El procesador externo de la pasarela rechaza una solicitud `/v1/responses` que contiene un tipo de herramienta que no puede analizar, con `400 unknown tool type`. Para mantener esas solicitudes funcionando, SecurSpaces elimina los tipos de herramientas no reconocidos antes de reenviar.

La lista la mantiene SecurSpaces, no su pasarela, por lo que cambia con una versión de SecurSpaces en lugar de cuando actualiza Envoy AI Gateway. Actualmente permite `function`, `file_search`, `computer_use_preview`, `web_search`, `web_search_2025_08_26`, `mcp`, `code_interpreter`, `image_generation`, `custom`, `local_shell`, `shell`, `web_search_preview`, `web_search_preview_2025_03_11` y `apply_patch`.

Importante:

Una herramienta fuera de este conjunto se descarta silenciosamente. La solicitud se realiza correctamente y su uso de tokens sigue siendo informado, pero esa herramienta nunca llega al proveedor. Generalmente, estas son herramientas del lado del cliente en las que la API ascendente no actúa, por lo que el efecto suele ser invisible; pero si un desarrollador informa que una herramienta funciona fuera de SecurSpaces y no dentro, esto es lo primero que hay que verificar.

Configurar la comprobación de estado de AI Gateway

Por defecto, SecurSpaces no comprueba el estado de AI Gateway. Active la comprobación de estado para controlar qué sucede con el tráfico de IA cuando la pasarela no está disponible.

Configure la comprobación de estado en `platform.aiGateway.healthCheck`:

VALOR	PREDETERMINADO	DESCRIPCIÓN
`enabled`	`false`	Cuando `true`, SecurSpaces ejecuta comprobaciones de estado TCP periódicas contra el AI Gateway.
`port`	`80`	El puerto al que SecurSpaces se conecta para la comprobación de estado.
`failOpen`	`false`	Controla el comportamiento cuando el gateway no está en buen estado.

Cuando el gateway no está en buen estado:

- Con `failOpen: true`, el tráfico de IA omite el gateway y va directamente al proveedor de IA. Los desarrolladores no se ven interrumpidos, pero no se registran datos de uso mientras el gateway está inactivo.
- Con `failOpen: false`, la solicitud devuelve un error al usuario. Utilice esta configuración cuando el tráfico de IA nunca deba omitir el gateway.

Advertencia

`failOpen` por defecto es `false`. Si habilitas la comprobación de estado sin configurar `failOpen`, una interrupción de AI Gateway impide que los desarrolladores lleguen a los proveedores de IA. Configura `failOpen: true` si prefieres perder datos de uso a bloquear las solicitudes de IA.

Anular el enrutamiento de AI Gateway para una región

Para una región externa, añade `region.aiGateway` para anular la configuración de toda la plataforma:

```
region:
  isExternalRegion: true
  aiGateway:
    address: "ai-gateway.region.example.svc.cluster.local"
    headers:
      userIdHeader: "x-user-id"
      projectIdHeader: "x-project-id"
      workspaceIdHeader: "x-workspace-id"
    healthCheck:
      enabled: false
      port: "80"
```

```
      failOpen: false
    dnsEndpoints:
      - "api.openai.com."
      - "api.anthropic.com."
```

Los valores regionales se aplican solo a esa región. Si omites `region.aiGateway`, la región utiliza la `platform.aiGateway` de toda la plataforma configuración.

Aplicar la configuración

1. Actualiza tu archivo de valores de Helm de SecurSpaces.
2. Ejecuta tu comando estándar `helm upgrade`.
3. Reinicia cualquier sesión de espacio de trabajo afectada si necesitas que las conexiones existentes utilicen el nuevo enrutamiento.

Después de la actualización, SecurSpaces enruta las solicitudes para los puntos finales DNS configurados a través de la dirección de AI Gateway configurada.

Informar sobre el uso de IA

Enrutar el tráfico de IA a través de una puerta de enlace te permite responder preguntas como qué modelos se están utilizando, cuántos tokens consume cada proyecto y qué usuarios generan la mayoría de las solicitudes. Esta información respalda las discusiones sobre atribución de costos y contracargos.

SecurSpaces no analiza el tráfico de IA ni almacena métricas de uso por sí mismo. El AI Gateway extrae el número de solicitudes, los nombres de los modelos y el número de tokens, y los exporta a tu sistema de monitorización. La precisión y la cobertura del proveedor de los informes resultantes dependen del soporte de análisis de la puerta de enlace que implementes.

Implementación de referencia

La siguiente pila está validada para su uso con SecurSpaces:

- **Envoy AI Gateway** — recibe el tráfico de IA del servicio proxy de SecurSpaces, lo reenvía al proveedor de LLM y expone métricas como recuentos de solicitudes, nombres de modelos y recuentos de tokens de entrada y salida.
- **Prometheus** — recopila y almacena las métricas que expone Envoy AI Gateway.

- **Grafana** — consulta a Prometheus y presenta los paneles.

Implemente los tres en el mismo clúster de Kubernetes que SecurSpaces, luego configure `platform.aiGateway.address` a la dirección de servicio interna de Envoy AI Gateway.

Esta es una ruta de referencia, no un requisito. Envoy AI Gateway admite OpenTelemetry y una amplia gama de integraciones de monitoreo, por lo que puede enviar los mismos datos a su infraestructura de monitoreo existente en su lugar.

Ejemplo de panel de Grafana

SecurSpaces proporciona un panel de Grafana de ejemplo que puede importar y adaptar. El panel lee los encabezados de metadatos de SecurSpaces, por lo que el uso se puede filtrar y agrupar por modelo, proyecto y usuario.

El panel incluye:

- **Totales resumidos** — total de tokens de entrada, total de tokens de salida, recuento combinado de tokens y recuento total de solicitudes de LLM.
- **Tasa de uso de tokens** — tokens por minuto, desglosados en tokens de entrada, salida, entrada en caché, creación de caché y razonamiento.
- **Tasa de solicitudes y tiempo de respuesta** — solicitudes por segundo y tiempo de respuesta de LLM en los percentiles 50, 95 y 99.
- **Promedio de tokens por solicitud** — promedio de tokens de entrada y salida por solicitud.
- **Limitación de velocidad** — solicitudes con limitación de velocidad, solicitudes que superan el límite de velocidad global y usuarios que superan su límite de velocidad.
- **Tiempo de respuesta ascendente** — tiempo de respuesta del proveedor de LLM en los percentiles 50 y 95.
- **Por ID de proyecto** — uso de tokens, tasa de solicitudes y total de tokens por proyecto.
- **Por ID de usuario** — uso de tokens por usuario a lo largo del tiempo.
- **Por modelo** — uso de tokens, tasa de solicitudes y tokens totales por modelo.

Utilice los selectores de **Modelo**, **ID de proyecto** e **ID de usuario** en la parte superior del panel de control para filtrar todos los paneles.

> **Nota**

> Los paneles que desglosan el uso por proyecto y usuario dependen de los encabezados de metadatos descritos en Identificar el uso de IA por usuario, proyecto y espacio de trabajo. Si esos encabezados no están configurados, los paneles correspondientes estarán vacíos.

Información relacionada

- Complemento de Backstage
- Citrix DaaS
- JFrog
- Publicar JetBrains Gateway
- HashiCorp Vault como gestor de secretos
- Integraciones

Publish JetBrains Gateway

Esta guía describe cómo publicar JetBrains IntelliJ Gateway como una aplicación virtual en Citrix DaaS. Al preconfigurar el complemento Citrix SecurSpaces™ - Remote SSH, puede proporcionar una experiencia de desarrollo remoto sin interrupciones.

Información general

La publicación de JetBrains IntelliJ Gateway a través de Citrix DaaS proporciona un punto de entrada estandarizado y seguro para los desarrolladores. Esta configuración permite a los desarrolladores utilizar el rendimiento nativo de los IDE de JetBrains mientras mantienen el código fuente y los recursos informáticos dentro del perímetro seguro del espacio de trabajo de SecurSpaces.

Requisitos previos

Antes de empezar, asegúrese de tener lo siguiente:

- Entorno de SecurSpaces: el acceso SSH debe estar habilitado a nivel de plataforma, organización y proyecto.
- Imagen VDA: Un VDA de Windows con el instalador de JetBrains IntelliJ Gateway.
- Complemento de SecurSpaces: El complemento network.strong.remotessh.

Guía del administrador: Preparar y publicar la aplicación

Para proporcionar una experiencia de "instalación cero", los administradores deben incluir el complemento de SecurSpaces en la instalación de Gateway en la imagen maestra de VDA.

Instalar el complemento de SecurSpaces (método CLI)

Utilice la interfaz de línea de comandos para instalar el complemento para la automatización de VDA y la coherencia de la imagen.

1. Abra un símbolo del sistema.
2. Navegue al directorio bin de su instalación de JetBrains IntelliJ Gateway.
3. Ejecute el siguiente comando:

```
.\gateway64.exe installPlugins network.strong.remotessh --give-consent-to-use-third-party-plugins
```

Nota:

Automatización: Incluya este comando en su script de sellado de VDA o receta de App Layering para asegurar que cada sesión contenga el plugin requerido.

Publicar JetBrains IntelliJ Gateway en Citrix DaaS

1. Abra **Citrix Web Studio** y navegue hasta **Applications**.
2. Seleccione **Add Applications** y elija el **Delivery Group** que contiene sus VDA preparados.
3. En **Application Settings**, introduzca lo siguiente:
   - **Ruta al ejecutable**: C:\Program Files\JetBrains\JetBrains Gateway\bin\gateway64.exe (o su ruta personalizada)
   - **Nombre de la aplicación**: JetBrains IntelliJ Gateway
4. En **Assignment**, asigne la aplicación a los grupos de usuarios desarrolladores apropiados.
5. Seleccione **Finish** para que la aplicación esté disponible en Citrix Workspace.

Publicar URL de la plataforma SecurSpaces con Google Chrome en Citrix DaaS

1. Abra **Citrix Web Studio** y navegue hasta **Applications**.
2. Seleccione **Add Applications** y elija el **Delivery Group** que contiene sus VDA preparados.
3. En **Application Settings**, introduzca lo siguiente:
   - **Ruta al ejecutable**: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe (o su ruta personalizada)

- **Argumentos de línea de comandos**: {SDS_PLATFORM_URL}
- **Nombre de la aplicación**: SecurSpaces

4. En **Asignación**, asigne la aplicación a los grupos de usuarios desarrolladores apropiados.
5. Seleccione **Finalizar** para que la aplicación esté disponible en Citrix Workspace.

Guía del usuario final: Conectarse a los espacios de trabajo de SecurSpaces

Una vez publicadas las aplicaciones, los desarrolladores pueden conectarse a entornos remotos mediante JetBrains IntelliJ Gateway.

Configuración por primera vez

Siga estos pasos para autorizar y configurar su primera conexión entre SecurSpaces y JetBrains IntelliJ Gateway.

1. Abra la **aplicación Citrix Workspace** o vaya a la **URL de Citrix Workspace** de su organización.
2. Seleccione el icono de **SecurSpaces**.
3. En el panel de control de su plataforma SecurSpaces, localice su espacio de trabajo y seleccione **SSH** para iniciar la conexión.
4. En el cuadro de diálogo **Conectar mediante SSH**, seleccione **JetBrains Gateway**.
5. Seleccione **Autorizar** para otorgar a JetBrains Gateway permiso para conectarse a SecurSpaces.
6. Seleccione su **espacio de trabajo de SecurSpaces** de la lista.
7. Seleccione su versión de **IDE** preferida (como IntelliJ IDEA, PyCharm o GoLand).
8. Seleccione **Conectar**. El Gateway configura el túnel SSH y abre su proyecto remoto en JetBrains IntelliJ Gateway.

Iniciar la aplicación

Una vez completada la configuración inicial, puede iniciar su entorno de desarrollo directamente desde JetBrains IntelliJ Gateway.

1. Abra la **aplicación Citrix Workspace** o vaya a la **URL de Citrix Workspace** de su organización.
2. Seleccione el icono de **JetBrains IntelliJ Gateway**.
3. Seleccione su versión de **IDE**.

4. Seleccione **Conectar**. El Gateway configura el túnel SSH y abre su proyecto remoto en JetBrains IntelliJ Gateway.

Información relacionada

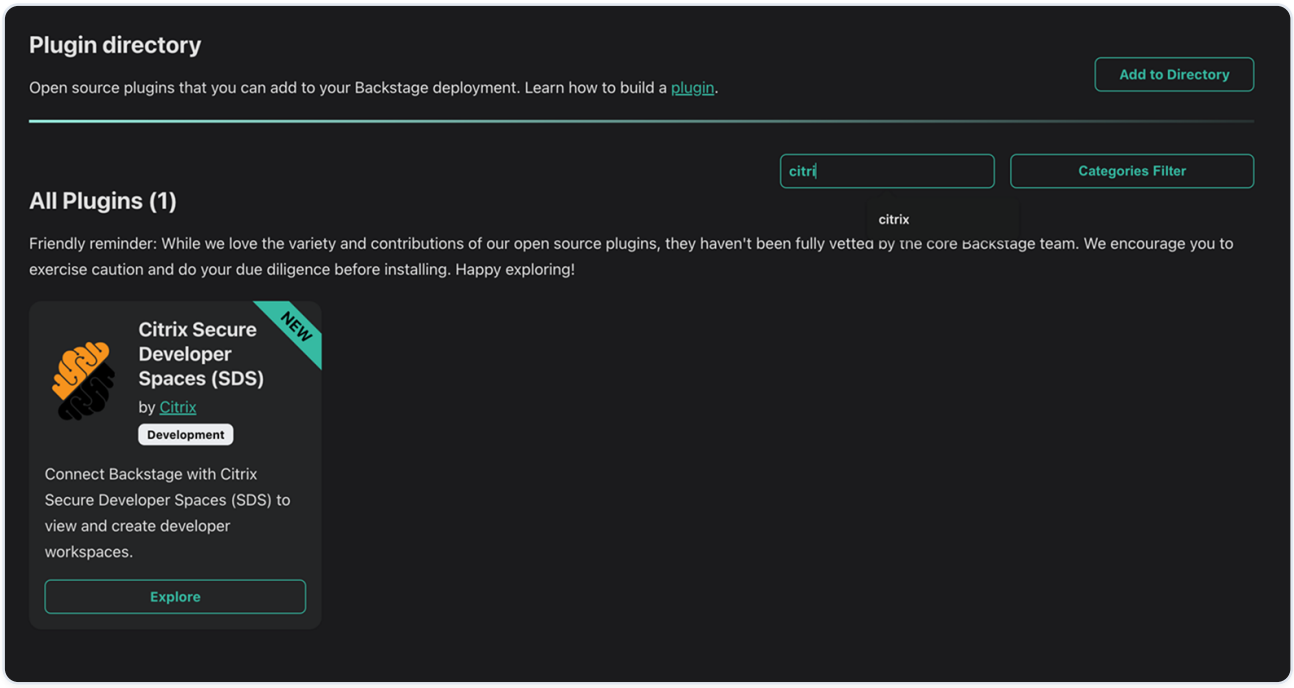
- AI Gateway
- Plugin de Backstage
- Citrix DaaS
- JFrog
- HashiCorp Vault como gestor de secretos
- Integraciones

SecurSpaces workspaces plugin for Backstage

Integre los espacios de trabajo de Citrix SecurSpaces™ en su portal de desarrolladores Backstage para gestionar directamente los espacios de trabajo seguros.

Descripción general

Backstage es un marco de portal de desarrolladores de código abierto que centraliza los componentes de software, las herramientas de infraestructura y la documentación en una interfaz unificada. Admite una arquitectura basada en complementos, lo que permite la extensibilidad tanto en las capas de frontend como de backend. El complemento de SecurSpaces Workspaces permite a los desarrolladores ver y gestionar los espacios de trabajo de SecurSpaces directamente desde las páginas de entidades de Backstage. Esta integración mejora la productividad del desarrollador al integrar las operaciones del espacio de trabajo en las herramientas que ya utilizan.

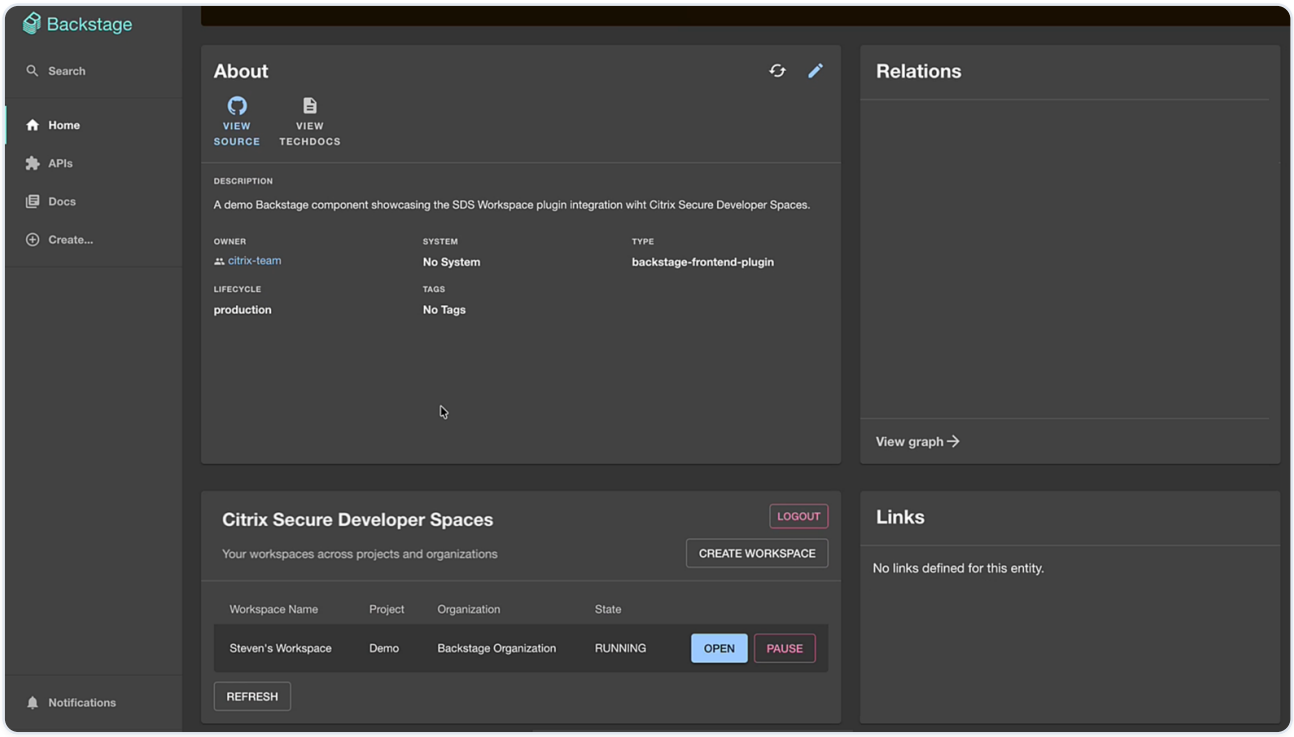


> Nota:

> La integración de SecurSpaces Workspaces requiere complementos tanto de frontend como de backend para funcionar correctamente.

Características principales

- Ver y gestionar los espacios de trabajo de SecurSpaces desde Backstage
- Tarjetas y pestañas personalizadas de SecurSpaces Workspace en las páginas de entidades
- Integración segura de backend con las API de la plataforma SecurSpaces
- Sin exposición de credenciales en el lado del cliente



Requisitos previos

- Una instancia de Backstage en ejecución
- Acceso a SecurSpaces
- URL base de la plataforma SecurSpaces

Arquitectura del complemento de Backstage

NOMBRE DEL COMPLEMENTO DE BACKSTAGE	DESCRIPCIÓN
@citrixcloud/backstage-sds-workspaces	Complemento de frontend para mostrar tarjetas y pestañas de espacios de trabajo de SecurSpaces
@citrixcloud/backstage-sds-workspaces-backend	Complemento de backend para la comunicación segura con la plataforma de espacios de trabajo de SecurSpaces

> Importante:

> Para usar el complemento de frontend de espacios de trabajo de SecurSpaces, también debe instalar y configurar el complemento backstage-sds-workspaces-backend en su proyecto de backend de Backstage. El complemento de backend actúa como puente entre

> su instancia de Backstage y la plataforma de espacios de trabajo de SecurSpaces, proporcionando todas las API necesarias para el complemento de frontend.

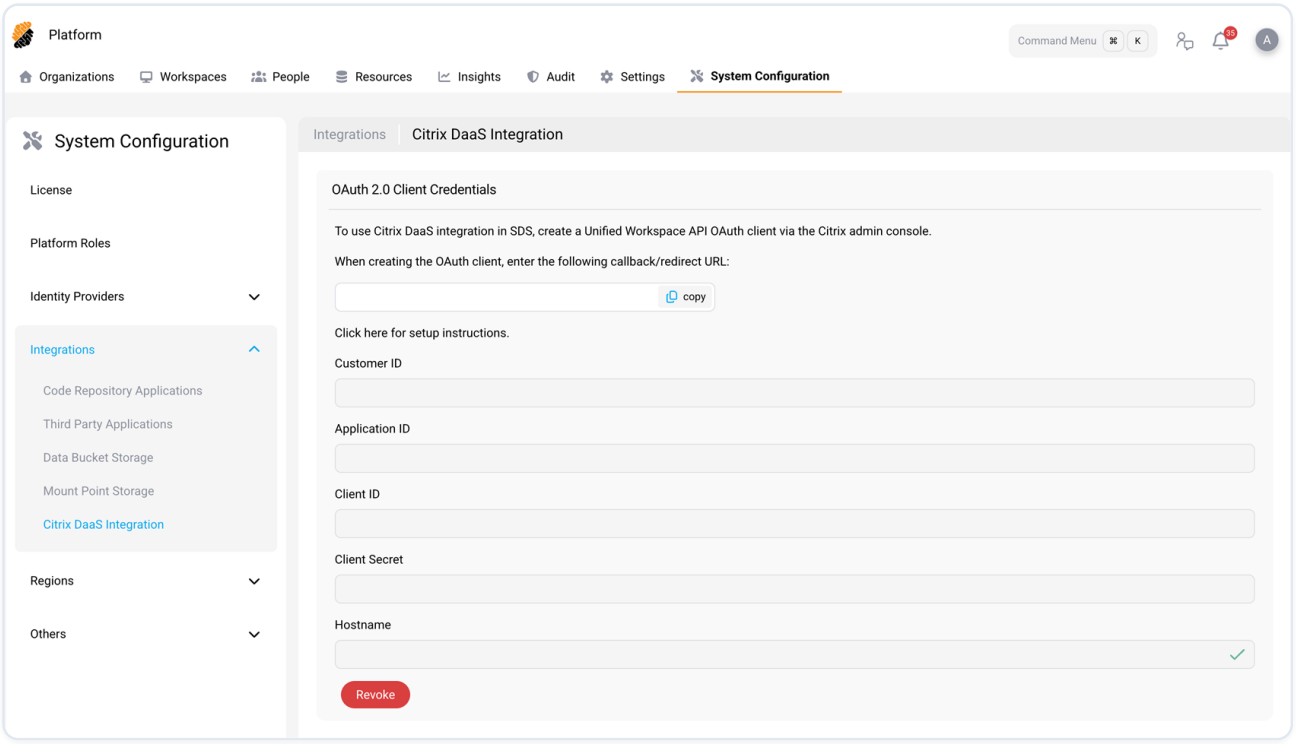
Información relacionada

- AI Gateway
- Citrix DaaS
- JFrog
- Publicar JetBrains Gateway
- HashiCorp Vault como gestor de secretos
- Integraciones

Citrix DaaS integration

La integración de Citrix DaaS conecta Citrix SecurSpaces™ con Citrix DaaS y Citrix Workspace. Después de configurar la integración, los usuarios pueden iniciar sesión una vez en la consola de SecurSpaces y acceder tanto a los espacios de trabajo de SecurSpaces basados en Kubernetes como a las aplicaciones y escritorios virtuales basados en Citrix sin autenticación adicional.

Esta página está disponible en **Configuración del sistema > Integraciones > Integración de Citrix DaaS**.



Requisitos previos

Antes de configurar la integración, necesita:

- Una cuenta de Citrix Cloud con una suscripción activa a DaaS.
- Un cliente OAuth de la API de Unified Workspace creado en la consola de administración de Citrix. Para obtener instrucciones, consulte Creación de un cliente en la documentación para desarrolladores de Citrix.

Cuando cree el cliente OAuth, utilice la siguiente URL de devolución de llamada/redirección que se muestra en la página de configuración:

```
https://<your-sds-hostname>/oauth/apps/callback
```

Configurar credenciales de cliente de OAuth 2.0

Utilice la sección **Credenciales de cliente de OAuth 2.0** para conectar SecurSpaces a su entorno de Citrix Cloud.

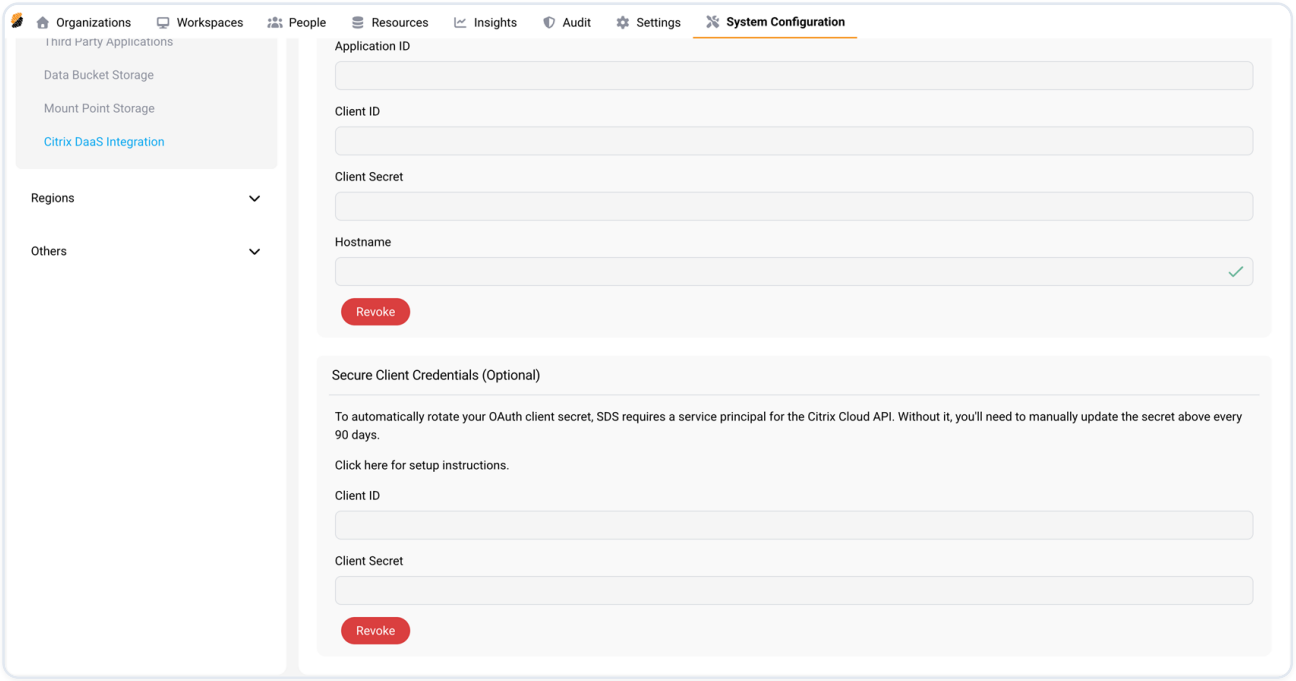
1. Vaya a **Configuración del sistema > Integraciones > Integración de Citrix DaaS**.
2. Introduzca los siguientes valores de su cliente OAuth de Citrix Cloud:

CAMPO	DESCRIPCIÓN
ID de cliente	Su ID de cliente de Citrix Cloud.
ID de aplicación	El ID de aplicación del cliente OAuth de la API de Unified Workspace.
ID de cliente	El ID de cliente generado al crear el cliente OAuth.
Secreto de cliente	El secreto de cliente generado al crear el cliente OAuth.
Nombre de host	El nombre de host de su entorno de Citrix Workspace (por ejemplo, `yourcompany.cloud.com`).

Para eliminar las credenciales almacenadas y desconectar la integración, seleccione **Revocar**.

Configurar credenciales de cliente seguras (opcional)

Los secretos de cliente OAuth caducan después de 90 días. Para evitar la rotación manual de secretos, puede configurar un principal de servicio que permita a SecurSpaces rotar el secreto automáticamente.



1. En la sección **Credenciales de cliente seguras**, introduzca el **ID de cliente** y el **Secreto de cliente** para un principal de servicio de la API de Citrix Cloud.
2. Para obtener instrucciones de configuración, consulte Rotación programática en la documentación para desarrolladores de Citrix.

Sin credenciales de cliente seguras, debe actualizar manualmente el secreto de cliente en esta página cada 90 días.

Qué sucede a continuación

Una vez configurada la integración de la plataforma:

1. Los **usuarios** inician sesión en su cuenta de Citrix desde **Perfil > Integraciones > Integración de Citrix**. Consulte Integración de Citrix (perfil de usuario).
2. Las **aplicaciones y escritorios virtuales** asignados al usuario en Citrix DaaS aparecen en la sección **Recursos de Citrix DaaS** de la página de Resumen del proyecto.

Información relacionada

- AI Gateway
- Plugin de Backstage

- JFrog
- Publicar JetBrains Gateway
- HashiCorp Vault como gestor de secretos
- Integraciones

Platform resources

Estas páginas cubren los recursos que la plataforma extrae y almacena en caché para los espacios de trabajo.

PÁGINA	QUÉ CUBRE
Acceso al registro	Restringe de qué registros de contenedores pueden extraer los espacios de trabajo y establece el registro de destino para las imágenes creadas en la plataforma.
Versiones de IDE	Aprende a gestionar las versiones de VSCode para los espacios de trabajo de SecurSpaces.
Almacenamiento en caché de imágenes	Almacena en caché las imágenes de contenedor de la plataforma en los nodos de los espacios de trabajo para que estos se inicien sin esperar a la extracción de una imagen.

Registry access

Dos configuraciones separadas controlan cómo Citrix SecurSpaces™ gestiona los registros de contenedores: una restringe el **origen** de las imágenes de espacio de trabajo, la otra establece dónde se almacenan las imágenes creadas en la plataforma.

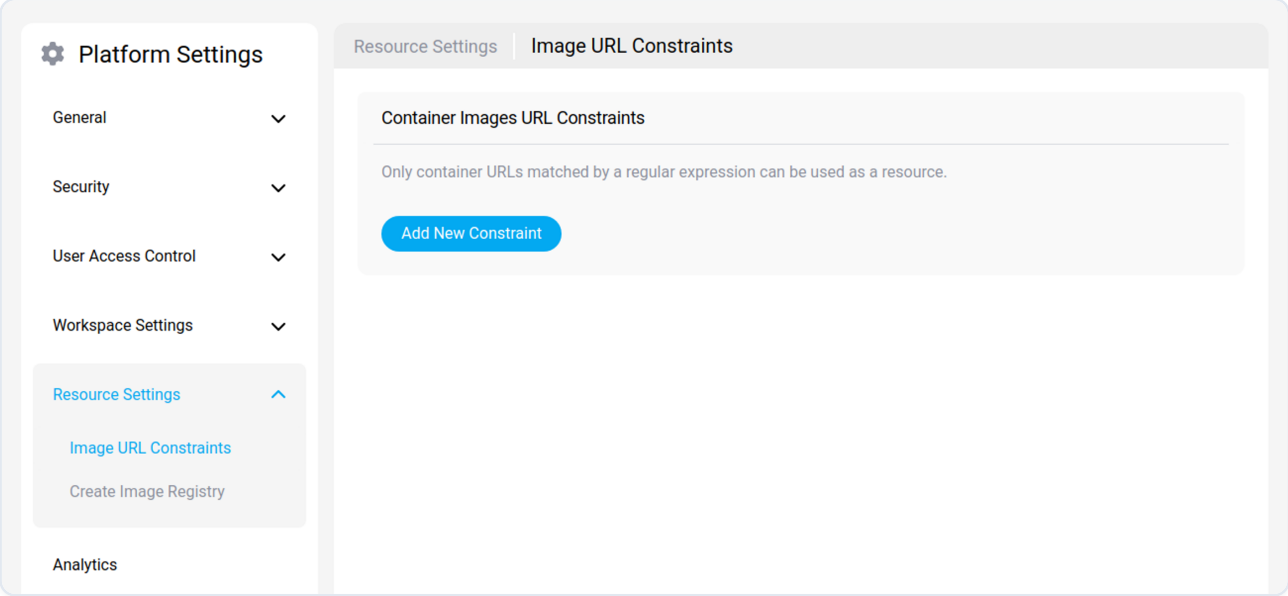
Ambas son a nivel de plataforma y requieren que el permiso de **Seguridad** esté configurado en **Gestionar**. Consulte Roles y permisos.

Restricciones de URL de imágenes

Por defecto, el propietario de un proyecto puede importar una imagen de espacio de trabajo desde cualquier registro al que pueda acceder. La **Gestión de acceso al registro** lo reemplaza con una

lista de permitidos: cuando la función está habilitada, SecurSpaces bloquea todos los registros excepto los que usted enumere.

Esto es importante porque una imagen de espacio de trabajo es código arbitrario que se ejecuta con acceso a su origen. Restringir los registros es la forma de evitar que una imagen provenga de un lugar que nadie ha revisado.



Para restringir registros:

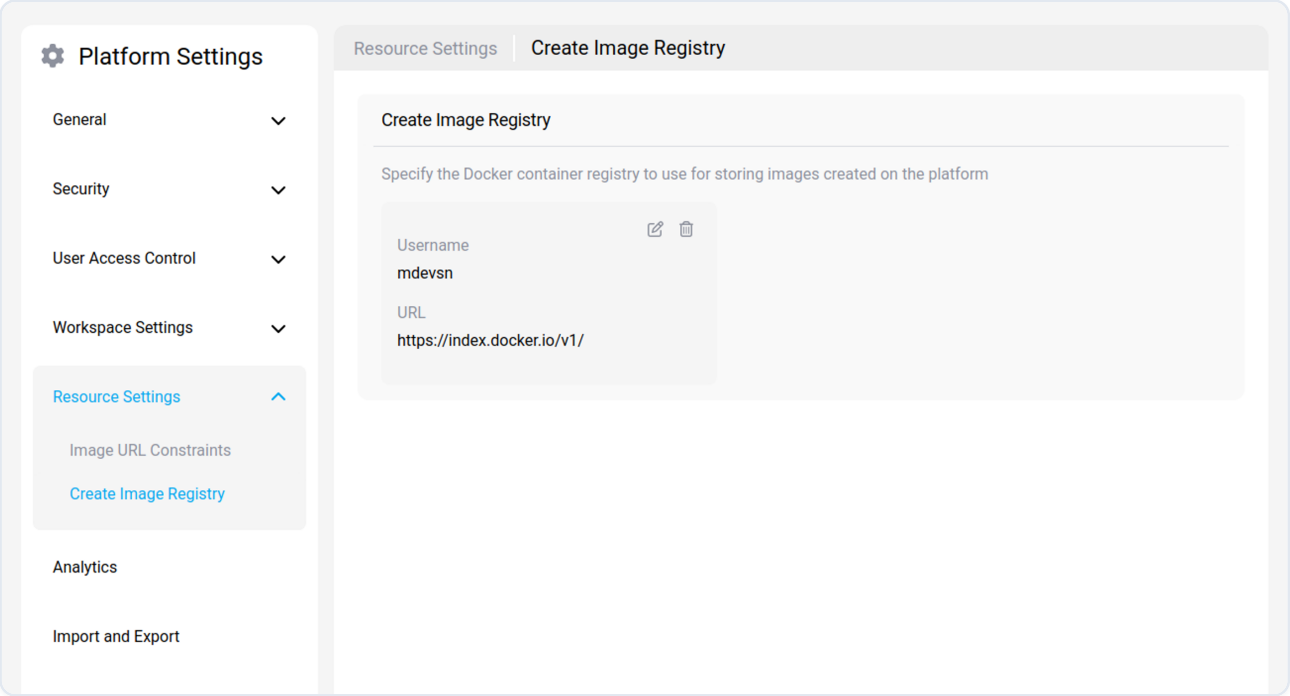
1. Abra **Configuración del sistema** y seleccione **Acceso al registro**.
2. Habilite la función.
3. Seleccione **Añadir registro** e introduzca el registro.
4. Establezca cada entrada en **Permitido** o **Denegado**.

Una entrada se puede cambiar entre permitido y denegado sin eliminarla, de modo que puede retirar un registro temporalmente sin perder la lista.

> **Nota:**
>
> Activar la función afecta a las importaciones realizadas a partir de ese momento. Revise también las imágenes ya registradas en la plataforma, ya que una imagen importada antes de que se aplicara la restricción sigue estando disponible. Consulte Imágenes de contenedor.

Crear registro de imágenes

Crear registro de imágenes especifica el registro de contenedores Docker utilizado para almacenar imágenes **creadas en la plataforma**. Es el destino de las imágenes que SecurSpaces construye, no una fuente de imágenes para importar.



Proporcione el punto final del registro y las credenciales que SecurSpaces debe usar para enviar a él. Cualquier registro compatible con OCI funciona — por ejemplo, Amazon ECR, Azure Container Registry, Google Artifact Registry o JFrog Artifactory.

La configuración de este registro también activa **Crear imagen a partir de una existente**, lo que permite a los miembros del proyecto construir una imagen derivada a partir de una existente proporcionando un script bash. Hasta que se establezca un registro de destino, esa opción no aparece. Consulte Crear una imagen a partir de una existente.

Si también utiliza restricciones de acceso al registro, asegúrese de que este registro de destino aparezca en la lista de permitidos. De lo contrario, la plataforma podría enviar una imagen que los espacios de trabajo tendrían bloqueado el acceso para extraer.

Información relacionada

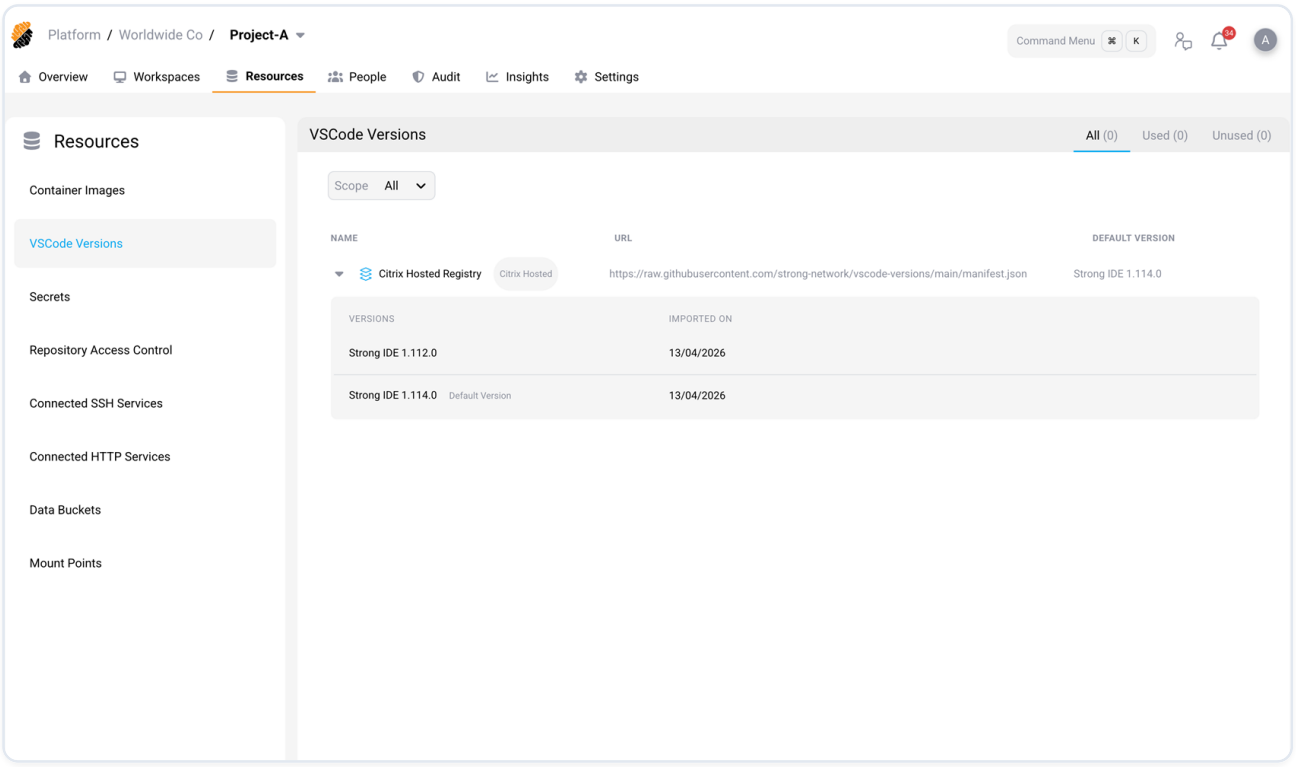
- Imágenes de contenedor
- Requisitos de la imagen de contenedor
- Imágenes de espacio de trabajo
- Configuración del sistema

IDE versions

La página de recursos de **Versiones de VSCode** gestiona las versiones de IDE disponibles para los espacios de trabajo. Las versiones de IDE se distribuyen independientemente de las actualizaciones de la plataforma Citrix SecurSpaces™, por lo que puede adoptar nuevas versiones del IDE basado en navegador (Strong IDE) sin esperar un lanzamiento de la plataforma.

Esta página está disponible en:

- **Nivel de plataforma:** Plataforma > Recursos > Versiones de VSCode
- **Nivel de organización:** Organización > Recursos > Versiones de VSCode
- **Nivel de proyecto:** Proyecto > Recursos > Versiones de VSCode



Cómo se distribuyen las versiones de IDE

Por defecto, SecurSpaces utiliza el **Registro alojado de Citrix** para importar versiones de IDE automáticamente. SecurSpaces comprueba si hay nuevas versiones una vez por hora. Cuando se publica una nueva versión, se importa y se envía una notificación a los oficiales de seguridad.

La página Versiones de VSCode muestra:

COLUMNA	DESCRIPCIÓN
Nombre	El nombre del registro. El valor predeterminado es "Registro alojado de Citrix",

COLUMNA	DESCRIPCIÓN
	marcado con una etiqueta de **Alojado por Citrix**.
URL	El origen que utiliza el registro. Para el Registro alojado de Citrix, este es el manifiesto de versión publicado por Citrix. Para un registro privado, esta es la URL de su registro de contenedores.
Versión predeterminada	La versión de IDE utilizada por los espacios de trabajo que siguen la configuración predeterminada.

Expanda una fila del registro para ver las versiones importadas, la fecha en que se importó cada versión y las acciones de versión disponibles para ese registro.

Requisitos de red

Para usar el Registro alojado de Citrix, su implementación debe poder acceder a los siguientes destinos a través de HTTPS:

DESTINO	UTILIZADO POR	PROPÓSITO
`raw.githubusercontent.com`	Servicios de plataforma de SecurSpaces	Recuperar el manifiesto de la versión durante la comprobación horaria
`registry-1.docker.io`, `auth.docker.io`, `production.cloudflare.docker.com`	Nodos de Kubernetes	Extraer las imágenes de contenedor de IDE a las que hace referencia el manifiesto

Si el tráfico saliente pasa a través de un proxy corporativo, consulte Configuración de proxy externo.

Si no puede permitir estos destinos, utilice un registro privado en su lugar. Consulte Cambiar a un registro privado.

Cómo se resuelve la versión del IDE

Cada espacio de trabajo almacena dos configuraciones que determinan su versión de IDE. SecurSpaces las evalúa en el siguiente orden cuando se inicia el espacio de trabajo:

1. **Versión fijada.** El espacio de trabajo está configurado para una versión específica del IDE. Esa versión es la que se utiliza.
2. **Versión predeterminada.** El espacio de trabajo utiliza **Usar la última versión predeterminada de la plataforma**. SecurSpaces resuelve la versión predeterminada para el ámbito del espacio de trabajo, buscando primero en el ámbito del proyecto, luego en el ámbito de la organización y finalmente en el ámbito de la plataforma.
3. **Predeterminado del sistema.** Ninguna de las configuraciones se aplica. El espacio de trabajo utiliza la imagen de IDE integrada que se incluye con la versión de la plataforma instalada.

Si una versión fijada o predeterminada no se puede resolver —por ejemplo, porque fue eliminada —, el espacio de trabajo recurre a la imagen predeterminada del sistema.

Para saber cómo configurar estos ajustes en un espacio de trabajo, consulte Crear un espacio de trabajo.

Establecer la versión predeterminada

La versión predeterminada se aplica a cada espacio de trabajo dentro del ámbito que utiliza **Usar la última versión predeterminada de la plataforma**.

1. Vaya a **Recursos > Versiones de VSCode**.
2. Expanda la fila del registro.
3. Apunte a la versión que desea usar y, a continuación, seleccione **Establecer como predeterminada**.

La columna **Versión predeterminada** se actualiza a la versión que seleccionó.

Necesita permiso para gestionar imágenes de contenedor para cambiar la versión predeterminada.

Si no se ha establecido una versión predeterminada para un ámbito, SecurSpaces selecciona una automáticamente después de una importación:

- Para el Registro alojado de Citrix, SecurSpaces selecciona la versión con la versión de VSCode ascendente más alta.
- Para un registro privado, SecurSpaces selecciona la versión importada más recientemente.

SecurSpaces nunca reemplaza una versión predeterminada que haya establecido un administrador.

Ciclo de vida de la versión

Cada importación horaria concilia las versiones importadas con el contenido del registro:

- Se importan nuevas versiones y se añaden a la lista.
- Los metadatos de las versiones ya importadas se actualizan.
- Las versiones que ya no están publicadas se eliminan.

Antes de eliminar una versión, SecurSpaces mueve cualquier espacio de trabajo o plantilla de espacio de trabajo que la utilice a la versión predeterminada actual. Los espacios de trabajo afectados adoptarán la nueva versión en su próximo inicio.

> **Nota:**

> Un espacio de trabajo migrado de esta manera queda anclado a la versión a la que se movió. Ya no sigue la versión predeterminada. Para restaurar las actualizaciones automáticas, seleccione de nuevo **Usar la última versión predeterminada de la plataforma** en el espacio de trabajo.

> La versión predeterminada actual nunca se elimina automáticamente. Para eliminarla, primero establezca otra versión como predeterminada.

Tipos de registro

SecurSpaces admite dos tipos de registro, y las acciones disponibles en la página Versiones de VSCode dependen del que utilice.

ACCIÓN	REGISTRO ALOJADO DE CITRIX	REGISTRO PRIVADO
Establecer una versión como predeterminada	Sí	Sí
Añadir una versión	No	Sí
Cambiar el nombre de una versión	No	Sí

ACCIÓN	REGISTRO ALOJADO DE CITRIX	REGISTRO PRIVADO
Eliminar una versión	No	Sí

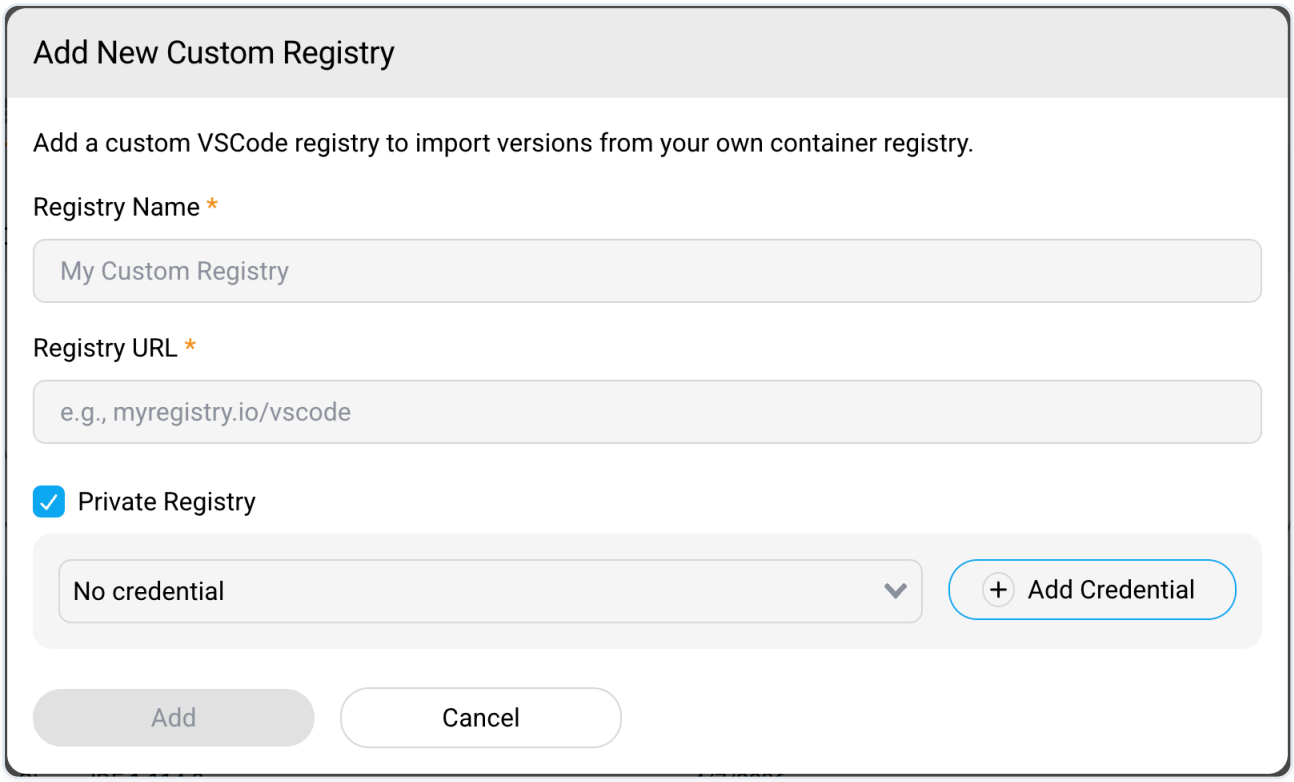
Las versiones en el Registro alojado de Citrix son gestionadas por Citrix y no se pueden editar.

Cambiar a un registro privado

Si su implementación está detrás de un proxy o firewall corporativo y no puede acceder al registro alojado por Citrix, un administrador de la plataforma puede cambiar a un registro privado que aloje sus propias imágenes de IDE.

1. Vaya a **Plataforma > Recursos > Versiones de VSCode**.
2. Seleccione **Cambiar a registro privado**.
3. Introduzca un **Nombre de registro** y la **URL del registro** de su registro de contenedores, por ejemplo `myregistry.io/vscode`. Ambos campos son obligatorios y el nombre debe ser único dentro del ámbito.
4. Si el registro requiere autenticación, seleccione **Registro privado** y, a continuación, seleccione una credencial de la lista. Para crear una credencial sin salir del cuadro de diálogo, seleccione **Añadir credencial**.
5. Seleccione **Añadir**.

Añadir permanece no disponible hasta que se rellenen el nombre y la URL del registro y, si se selecciona **Registro privado**, hasta que se elija una credencial.

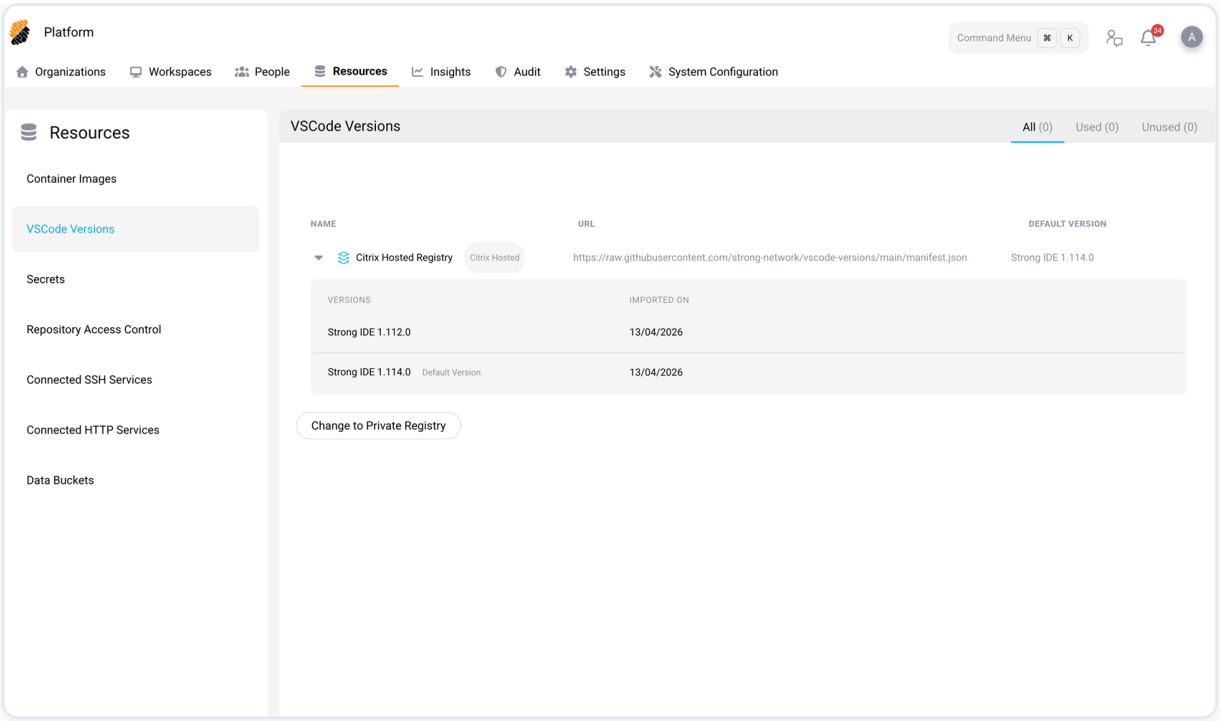


Después de añadir un registro privado, añada las versiones de IDE que desee poner a disposición:

1. Expanda la fila del registro privado.
2. Seleccione **Añadir nueva versión**.
3. Introduzca un **Nombre de versión** y la **Etiqueta de imagen**, por ejemplo `1.95.2`. SecurSpaces combina la etiqueta con la URL del registro para formar la URL completa de la imagen.
4. Opcionalmente, seleccione **Establecer como versión predeterminada**.

Nota:

Un registro privado reemplaza al Registro alojado de Citrix, no lo complementa. Aunque un registro privado se configure a nivel de plataforma, el Registro alojado de Citrix se oculta de la página de Versiones de VSCode y SecurSpaces deja de importar versiones de él.



El botón **Cambiar a registro privado** solo está disponible en la página de Versiones de VSCode a nivel de plataforma.

Volver al registro alojado de Citrix

1. Vaya a **Plataforma > Recursos > Versiones de VSCode**.
2. Seleccione **Cambiar a registro alojado de Citrix**.
3. Revise la lista de espacios de trabajo afectados.
4. Seleccione **Migrar espacios de trabajo y cambiar**.

Todas las versiones del registro privado se eliminan y los espacios de trabajo afectados se mueven a la versión predeterminada del Registro alojado de Citrix. SecurSpaces reanuda la importación de versiones del Registro alojado de Citrix.

Notificaciones

Cuando se importa una nueva versión de IDE, SecurSpaces envía una notificación a los oficiales de seguridad:

> Una nueva versión de VSCode "Strong IDE X.X.X" ya está disponible.

> La notificación aparece en la campana de notificaciones en la barra de navegación superior.

Administrar versiones de VSCode a través de la API

La API REST puede gestionar versiones de VSCode a nivel de plataforma, organización y proyecto. Úsela cuando desee importar imágenes IDE probadas, establecer valores predeterminados o mantener muchos proyectos alineados sin usar la consola.

Las operaciones de versión están disponibles en estas raíces de ámbito:

- Plataforma: `/v1/vscode-versions`
- Organización: `/v1/organizations/{organizationId}/vscode-versions`
- Proyecto: `/v1/projects/{projectId}/vscode-versions`

Cada ámbito admite listar versiones, importar una versión desde un registro por etiqueta de imagen, renombrar una versión, eliminar una versión y establecer una versión como predeterminada del ámbito.

La gestión de registros personalizados a nivel de plataforma está disponible en `/v1/vscode-registries`. Puede listar registros personalizados, añadir uno, renombrarlo o eliminarlo. El nombre de un registro personalizado debe ser único dentro de su ámbito, y cada ámbito puede tener un registro personalizado.

Para obtener detalles sobre los puntos finales, los campos de solicitud y respuesta, y la autenticación, consulte API REST.

Ver versiones de VSCode del espacio de trabajo a través de la API

Las respuestas de la API del espacio de trabajo incluyen dos campos que describen la versión del IDE asignada a un espacio de trabajo:

CAMPO	DESCRIPCIÓN
`vscode_version_id`	El ID de la versión a la que está anclado el espacio de trabajo. `0` cuando el espacio de trabajo no está anclado.
`vscode_version_auto_update`	`true` cuando el espacio de trabajo sigue la versión predeterminada para su ámbito.

Los dos campos se combinan de la siguiente manera:

- `vscode_version_auto_update` es `true` y `vscode_version_id` es `0` — el espacio de trabajo sigue la versión predeterminada.

- `vscode_version_auto_update` es `false` y `vscode_version_id` está configurado — el espacio de trabajo está anclado a esa versión.
- `vscode_version_auto_update` es `false` y `vscode_version_id` es `0` — el espacio de trabajo utiliza la imagen predeterminada del sistema.

Utilice estos campos cuando necesite auditar versiones de IDE, crear integraciones o solucionar problemas de comportamiento específicos de la versión.

Para obtener más información sobre los puntos finales de la API disponibles, consulte API REST.

Auditar cambios de versión de VSCode

Los cambios en las versiones y registros de VSCode se registran como eventos en el tipo de recurso `vscodeVersions`. Para obtener más información, consulte Integración SIEM.

Información relacionada

- Almacenamiento en caché de imágenes
- Acceso al registro

Image caching

Extraer una imagen de espacio de trabajo suele ser el mayor coste individual cuando se inicia un espacio de trabajo. Una imagen de espacio de trabajo suele tener más de un gigabyte, y un nodo que nunca ha ejecutado esa imagen tiene que descargarla y descomprimirla antes de que el espacio de trabajo pueda comenzar.

El almacenamiento en caché de imágenes elimina esa espera. Citrix SecurSpaces™ mantiene las imágenes que marca como almacenadas en caché presentes en los nodos del espacio de trabajo, de modo que un espacio de trabajo programado en uno de esos nodos se inicia sin extraer nada.

Lo que necesita

REQUISITO	DETALLE
Permiso	El permiso de **Seguridad** establecido en **Administrar** — el rol de oficial de seguridad
Ámbito	Solo imágenes de contenedor a nivel de plataforma. Las imágenes definidas a nivel de organización o proyecto no se pueden almacenar en caché.

El almacenamiento en caché no está disponible si un administrador de la plataforma ha deshabilitado la gestión de imágenes.

Almacenar en caché una versión de imagen

El almacenamiento en caché se configura por **versión**, no por imagen, por lo que puede almacenar en caché las etiquetas que los desarrolladores realmente usan y dejar las más antiguas sin tocar.

1. En la consola, vaya a **Recursos > Imágenes de contenedor**.
2. Seleccione la flecha junto a una imagen para expandir sus versiones.
3. En la columna **Imagen en caché**, active el interruptor para cada versión que desee almacenar en caché.

El cambio surte efecto inmediatamente y se aplica en todas las regiones.

Para dejar de almacenar una versión en caché, desactive el interruptor. La imagen ya no se mantiene en los nodos, y el siguiente espacio de trabajo que la necesite la extraerá normalmente.

> **Nota:**
>
> La imagen IDE predeterminada de la plataforma se almacena en caché automáticamente cuando está lista y no ha superado su fecha de obsolescencia. No es necesario marcarla. Consulte Versiones de IDE.

Cómo permanecen las imágenes en los nodos

Comprender el mecanismo explica tanto el beneficio como el coste.

SecurSpaces ejecuta un despliegue cuya única función es mantener las imágenes en caché. Cada uno de sus pods hace referencia a cada imagen en caché, lo que hace que Kubernetes extraiga esas imágenes al nodo en el que aterrice el pod. Los pods se distribuyen uno por nodo de espacio de trabajo, y no realizan ningún trabajo más allá de existir; su presencia es lo que mantiene las imágenes en el nodo.

Se derivan dos consecuencias:

- **El disco del nodo contiene todas las imágenes en caché.** Almacene en caché las versiones en uso activo en lugar de todo el historial de una imagen. Un patrón viable es la etiqueta

predeterminada actual y la anterior, de modo que una reversión también sea rápida, dejando las versiones anteriores sin caché.

- **La caché sigue a los nodos del espacio de trabajo.** A medida que el clúster escala, el despliegue se redimensiona para que los nuevos nodos también reciban las imágenes.

Imágenes en caché y nodos cálidos

El mismo despliegue proporciona nodos cálidos. Su tamaño es el número de nodos que ejecutan espacios de trabajo actualmente, más un búfer derivado de la configuración de nodos cálidos para la región.

Ese búfer es lo que hace que las dos características funcionen juntas: sin él, las imágenes solo se almacenarían en caché en nodos que ya están ocupados, y un espacio de trabajo que active un escalado aún esperaría la extracción. Los nodos cálidos mantienen una capacidad de reserva que ya contiene las imágenes, por lo que el primer espacio de trabajo del día evita ambos costes a la vez.

Configure el búfer en **Configuración del sistema > Regiones**. Consulte Configuración de nodos cálidos.

> **Nota:**
>
> El búfer se mantiene a cero hasta que al menos un espacio de trabajo se está ejecutando en una región, por lo que un clúster inactivo no se mantiene activo para nadie.

Confirmar que el almacenamiento en caché funciona

Dos comprobaciones, desde ambos lados:

- **En la consola**, el interruptor **Cached Image** está activado para la versión.
- **Para un desarrollador**, el registro de inicio del espacio de trabajo ya no muestra una descarga larga para esa imagen. Ábralo desde **Más acciones** (**...**) en el espacio de trabajo, luego **Registros**, y observe la fase de **Configuración del contenedor** . Consulte Solución de problemas.

Si la descarga sigue apareciendo, el espacio de trabajo se programó en un nodo al que el caché aún no ha llegado, lo que normalmente significa que el clúster acaba de escalar horizontalmente.

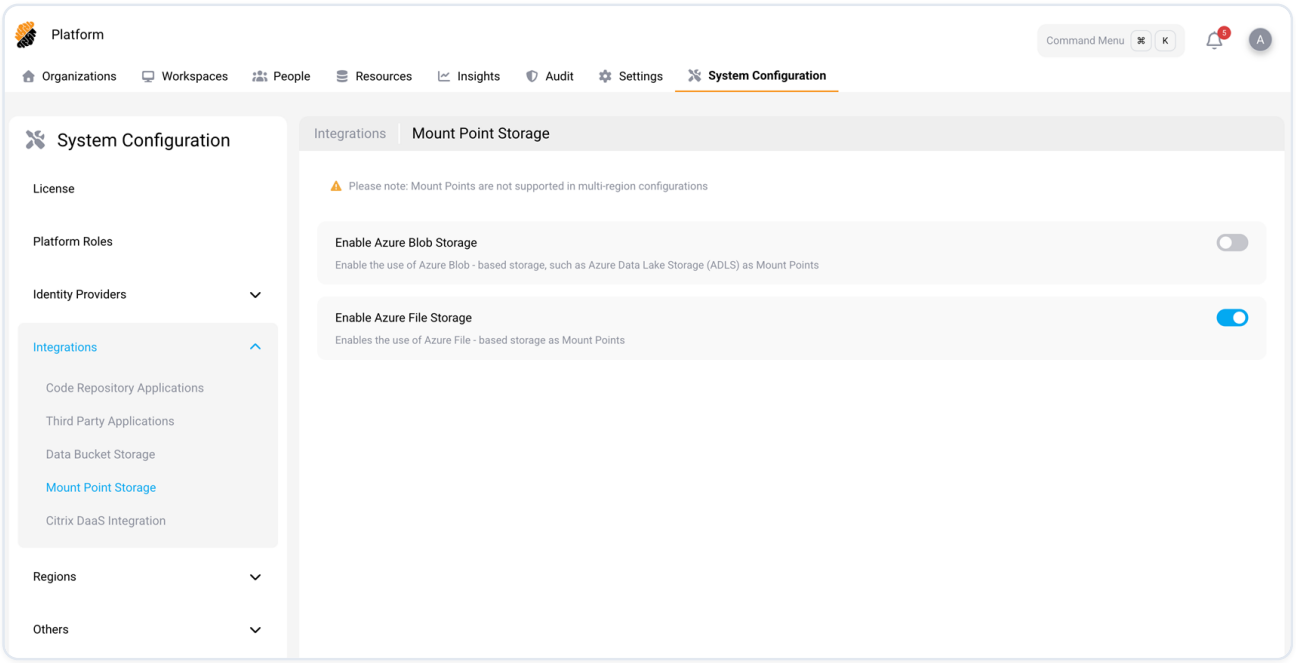
Información relacionada

- Imágenes de espacio de trabajo personalizadas
- Versiones de IDE
- Acceso al registro
- Regiones
- Dimensionamiento

Mount point storage

La sección **Almacenamiento de puntos de montaje** permite a los administradores de la plataforma habilitar o deshabilitar los tipos de almacenamiento de puntos de montaje para la plataforma.

Vaya a **Configuración del sistema > Integraciones > Almacenamiento de puntos de montaje**.



La captura de pantalla anterior se tomó de un clúster de Azure. Un clúster de AWS muestra un conmutador, **Habilitar almacenamiento de archivos de AWS Almacenamiento**, en lugar de los dos conmutadores de Azure.

> **Advertencia**
>
> Los puntos de montaje no son compatibles con las configuraciones multirregión.

Qué tipos de almacenamiento aparecen

Los conmutadores de esta página dependen de la nube que respalda los puntos de montaje, y esa nube se detecta en lugar de elegirse. La plataforma lee los aprovisionadores CSI de las clases de almacenamiento de puntos de montaje presentes en el clúster: `efs.csi.aws.com` significa AWS, y `file.csi.azure.com` significa Azure. Nada en esta página establece el proveedor, y un clúster se trata como respaldado por una sola nube.

- **Un clúster de Azure** muestra **Habilitar almacenamiento de archivos de Azure**, lo que habilita el almacenamiento basado en archivos de Azure como puntos de montaje. También muestra **Habilitar almacenamiento de blobs de Azure**, para el almacenamiento basado en blobs de Azure, como Azure Data Lake Storage (ADLS). Ese conmutador aún no está disponible. No se puede activar, y la plataforma rechaza una solicitud para crear un punto de montaje de blob de Azure.
- **Un clúster de AWS** muestra un conmutador, **Habilitar almacenamiento de archivos de AWS**, que habilita tanto Amazon Elastic File System (EFS) como Amazon S3 Files. No hay un conmutador separado para cada backend, por lo que no puede permitir uno y bloquear el otro desde esta página. El backend que utiliza un punto de montaje se decide por el parámetro `provisioningMode` en la clase de almacenamiento que usted crea — `efs-ap` para Amazon EFS, `s3files-ap` para Amazon S3 Files — por lo que el propietario de un proyecto elige el backend seleccionando la clase de almacenamiento. Asigne a cada clase de almacenamiento un nombre que haga el backend obvio. Consulte Configurar SecurSpaces para puntos de montaje de AWS.
- **Un clúster que contiene clases de almacenamiento de puntos de montaje tanto de AWS como de Azure** no muestra conmutadores. El proveedor no puede ser resuelto, la función se retira de los usuarios, y la página informa del conflicto y enumera los proveedores que detectó. Elimine las clases de almacenamiento de puntos de montaje de una nube y vuelva a visitar la página.
- **Un clúster sin una clase de almacenamiento de puntos de montaje elegible** tampoco muestra conmutadores. La página informa que no se detectó ninguna clase de almacenamiento elegible, y la lista de proveedores detectados está vacía. Una lista vacía significa que no se reconoció nada. Dos entradas significan el conflicto de nube mixta descrito anteriormente.

Habilitar un tipo de almacenamiento

1. Vaya a **Configuración del sistema > Integraciones > Almacenamiento de puntos de montaje**.

2. Active el conmutador para el tipo de almacenamiento que desee.

Cuando un tipo de almacenamiento está habilitado, los propietarios de proyectos pueden crear puntos de montaje de ese tipo, y los desarrolladores pueden adjuntarlos a los espacios de trabajo. Cuando está deshabilitado, el botón **Añadir punto de montaje** y el resto del flujo de creación se ocultan, y no se pueden crear nuevos puntos de montaje de ese tipo.

> **Advertencia**

> Desactivar un tipo de almacenamiento no desconectar el almacenamiento que ya está en uso. La plataforma comprueba el interruptor solo cuando se crea un punto de montaje, por lo que un espacio de trabajo que ya tiene uno adjunto sigue montándolo, con el mismo acceso de lectura y escritura, después de que el interruptor esté desactivado. Las configuraciones de puntos de montaje existentes tampoco se eliminan, y vuelven a estar disponibles si se vuelve a activar el interruptor. Para cortar el acceso, elimine el punto de montaje, o quítelo de cada espacio de trabajo y plantilla de espacio de trabajo que lo utilice.

> Las vistas de proyecto y espacio de trabajo no dan ninguna razón cuando los puntos de montaje no están disponibles. Simplemente ocultan la opción. Abra esta página primero cuando un usuario informe que los puntos de montaje han desaparecido.

Clases de almacenamiento de AWS

Para el almacenamiento de AWS, un administrador también debe proporcionar clases de almacenamiento de Kubernetes elegibles para el almacenamiento de respaldo. Los propietarios de proyectos solo ven las clases de almacenamiento compatibles cuando crean o adjuntan puntos de montaje de AWS.

Los puntos de montaje de AWS requieren recursos de AWS que Citrix SecurSpaces™ no crea, incluyendo el sistema de archivos, los destinos de montaje por zona de disponibilidad, los roles de IAM y las propias clases de almacenamiento. El tipo de almacenamiento de AWS no aparece aquí hasta que exista una clase de almacenamiento de AWS elegible en el clúster. Consulte Prepare AWS storage for Mount Points.

> **Nota**

> Después de añadir o eliminar una clase de almacenamiento de punto de montaje, espere unos 30 segundos antes de que esta página refleje el cambio. La plataforma almacena en caché el proveedor detectado y la lista de clases de almacenamiento elegibles durante ese tiempo. No es necesario reiniciar, así que no reinicie los pods ni fuerce una implementación mientras espera.

Información relacionada

- Puntos de montaje, para crear y usar puntos de montaje dentro de un proyecto
- Preparar el almacenamiento de AWS para puntos de montaje
- Configurar SecurSpaces para puntos de montaje de AWS
- Elegir entre depósitos de datos y puntos de montaje

Prepare AWS storage for Mount Points

Los puntos de montaje de AWS proporcionan a un proyecto almacenamiento de archivos POSIX compartido y persistente que se monta en sus pods de espacio de trabajo en `/mnt/<mount-point-name>`. Cada espacio de trabajo que lo monta lee y escribe los mismos archivos, en tiempo real. Es almacenamiento compartido colaborativo, no almacenamiento por usuario.

Se admiten dos backends de AWS, ambos a través del controlador `efs.csi.aws.com`:

- **Amazon EFS** — almacenamiento de archivos NFS elástico.
- **Archivos de Amazon S3** — un sistema de archivos construido sobre EFS a través de un bucket de S3. Los mismos bytes son accesibles como objetos y como archivos.

> **Importante**
>
> Los puntos de montaje de AWS dependen de recursos de AWS que Citrix SecurSpaces™ no crea ni valida. A diferencia del almacenamiento de archivos de Azure, el controlador CSI de EFS no puede crear un sistema de archivos; solo puede crear puntos de acceso dentro de un sistema de archivos ya existente. Debe aprovisionar el sistema de archivos, los destinos de montaje, los grupos de seguridad, los roles de IAM y las StorageClasses usted mismo antes de que alguien pueda usar la función.

> Si faltan estos requisitos previos, la función suele fallar silenciosamente en lugar de informar un error. Un cuadro de diálogo de creación vacío, un espacio de trabajo que se bloquea al iniciarse o un montaje que se ejecuta sin cifrar son todos síntomas de una preparación incompleta de AWS.

Lista de verificación de prioridades

Revise estos puntos antes de su primera implementación. Cada uno de ellos o bien rompe la función o debilita la seguridad de los datos.

REQUISITO	QUÉ SUCEDE SI LO OMITE
Establezca `tls` como una opción de montaje en cada StorageClass y cada PersistentVolume que cree.	El tráfico NFS viaja sin cifrar a través de la VPC en el puerto 2049.
Conceda al servicio de espacio de trabajo acceso de lectura a las StorageClasses.	La comprobación de cifrado no se puede ejecutar y se omite, por lo que un montaje sin cifrar puede tener éxito.
Asigne un nombre a un punto de acceso en `volumeHandle`. Nunca publique un ID de sistema de archivos sin formato.	El montaje expone los datos de todos los demás proyectos en ese sistema de archivos.
Etiquete cada PersistentVolume que cree con `strong.network/mount-point-scope`.	Un volumen sin etiquetar no se ofrece a nadie. Uno con un ámbito incorrecto se ofrece a los proyectos equivocados.
Establezca `persistentVolumeReclaimPolicy: Retain` en los volúmenes que cree.	Eliminar un punto de montaje puede destruir los datos subyacentes.
Establezca `storageClassName: ""` en los volúmenes que cree.	Un valor distinto de la cadena vacía nunca se vincula a la reclamación que crea SecurSpaces, por lo que el punto de montaje agota el tiempo de espera y entra en un estado de error.
Cree un destino de montaje por cada zona de disponibilidad que utilice su grupo de nodos, y permita NFS en el puerto 2049.	Los espacios de trabajo programados en una zona de disponibilidad sin destino de montaje se bloquean al iniciarse.

REQUISITO	QUÉ SUCEDE SI LO OMITE
Cree el sistema de archivos con cifrado en reposo, y habilite las copias de seguridad automáticas.	Los datos se almacenan sin cifrar, y las eliminaciones son permanentes e irrecuperables.
Utilice un proveedor de nube por clúster.	Las StorageClasses mixtas de AWS y Azure retiran la función a todos los usuarios.

Advertencia

No cambie el nombre de los identificadores técnicos de este artículo para que coincidan con el nombre del producto. La clave de etiqueta de volumen `strong.network/mount-point-scope`, los nombres de las métricas y las rutas de valores de Helm mantuvieron su ortografía original deliberadamente. Una etiqueta renombrada hace que el volumen no sea visible para nadie, sin mensaje de error.

Cómo usar esta sección

PÁGINA	QUÉ CUBRE
Preparar los recursos de AWS	Destinos de montaje, grupos de seguridad, requisitos previos de Amazon EFS y Amazon S3 Files, alcance de IAM, refuerzo de metadatos de instancia
Configurar SecurSpaces	La StorageClass, el cifrado en tránsito y la habilitación de la característica
Crear un PersistentVolume	Publicar su propio volumen para Attach Existing
Resolución de problemas	Síntomas, causas y soluciones
Límites y comportamiento de los puntos de montaje	Cuotas, semántica de eliminación, comportamiento de Amazon S3 Files, multirregión y métricas

Prepare the AWS resources

Citrix SecurSpaces™ no crea ni valida ninguno de los recursos de AWS de esta página. Aprovisione estos recursos antes de que nadie utilice la función.

Requisitos previos comunes para Amazon EFS y archivos de Amazon S3

Crear un destino de montaje en cada zona de disponibilidad

Cree un destino de montaje en cada Zona de disponibilidad en la que el grupo de nodos pueda colocar nodos de espacio de trabajo. Tome la lista de Zonas de disponibilidad del grupo de autoescalado del grupo de nodos, no de donde los nodos se ejecutan actualmente. EFS permite un destino de montaje por Zona de disponibilidad, compartido por todos los Puntos de montaje de ese sistema de archivos.

Un espacio de trabajo programado en una Zona de disponibilidad sin un destino de montaje accesible se bloquea en `ContainerCreating`, y Kubernetes no puede compensar. El destino de montaje no está representado en Kubernetes, por lo que este es el único síntoma.

La creación del destino de montaje es lenta. Espere hasta que cada destino de montaje informe `available` antes de crear los puntos de montaje.

Limitar el ámbito de la regla NFS a un grupo de seguridad

El origen de la regla NFS de entrada del destino de montaje decide quién puede montar el sistema de archivos. Si permite todo el CIDR de la VPC, todas las cargas de trabajo de la VPC pueden montarlo, no solo los nodos de su espacio de trabajo.

Establezca el origen de la regla de entrada en el grupo de seguridad del nodo de trabajo de EKS en lugar de un rango de IP:

```
aws ec2 authorize-security-group-ingress \

  --group-id <mount-target-sg> --protocol tcp --port 2049 \

  --source-group <eks-node-security-group-id>
```

Ambas partes de la regla son obligatorias:

- **Grupo de seguridad del destino de montaje, entrada** — TCP 2049, el origen es el grupo de seguridad del nodo.
- **Grupo de seguridad del nodo, salida** — TCP 2049, el destino es el grupo de seguridad del destino de montaje.

La mayoría de los grupos de nodos de EKS mantienen la salida predeterminada de permitir todo, por lo que la parte de salida suele estar ya satisfecha. Si su cuenta restringe la salida de nodos, añádala explícitamente. Una regla de salida que falta produce el mismo síntoma que un destino de montaje que falta: los espacios de trabajo se bloquean al iniciarse, sin ninguna indicación en Kubernetes.

No se necesitan reglas de salida en el grupo de seguridad del destino de montaje, porque los grupos de seguridad tienen estado.

> **Nota**
>
> El origen es siempre el grupo de seguridad del nodo, incluso en clústeres que utilizan grupos de seguridad de EKS para pods. El montaje lo realiza el DaemonSet del nodo CSI de EFS, que se ejecuta con `hostNetwork`, y los grupos de seguridad para pods no se aplican a los pods `hostNetwork`. Un `SecurityGroupPolicy` nunca coincide con el DaemonSet, por lo que limitar la regla de entrada a un grupo de seguridad de pods deja todos los espacios de trabajo colgados al iniciarse. Si debe usar un CIDR, limítelo a los CIDR de la subred del nodo de trabajo, nunca a toda la VPC. Un grupo de seguridad limita la accesibilidad, no el cifrado. Mantenga `tls` en el montaje de todos modos.

Adjuntar la política del controlador CSI

Un controlador CSI, `efs.csi.aws.com`, sirve tanto a Amazon EFS como a Amazon S3 Files, por lo que este paso se aplica a cualquier backend que utilice. Adjunte `AmazonEFSCSIDriverPolicy` al rol del controlador CSI. Debe incluir `DescribeMountTargets`, que el asistente de montaje utiliza para resolver el destino de montaje local de la Zona de disponibilidad.

Requisitos previos de Amazon EFS

- **Cree el sistema de archivos primero.** El controlador no puede crearlo. **Crear nuevo** crea un nuevo punto de acceso aislado en el sistema de archivos que ha aprovisionado. Nunca crea un sistema de archivos.
- **Créelo como un sistema de archivos regional, no como un sistema de archivos de una sola zona.** Un sistema de archivos regional permite un destino de montaje en cada Zona de disponibilidad, que es lo que requiere el requisito por Zona de disponibilidad anterior. Un sistema de archivos de una sola zona permite un único destino de montaje, por lo que no puede respaldar un punto de montaje. Los espacios de trabajo programados en las Zonas de

disponibilidad que no atiende se quedan colgados al iniciarse, y no hay ningún destino de montaje que pueda añadir para solucionarlo.

- **Habilite el cifrado en reposo al crear el sistema de archivos.** Los puntos de montaje funcionan de cualquier manera, por lo que nada le advertirá más tarde, y el cifrado no se puede habilitar después de la creación.

Habilitar copias de seguridad automáticas

EFS no tiene control de versiones, ni instantáneas, ni papelera de reciclaje. Sin un punto de recuperación que ya existiera cuando se perdieron los datos, una eliminación es permanente.

Un sistema de archivos regional, que es el único tipo que puede respaldar un punto de montaje, se crea con las copias de seguridad automáticas **deshabilitadas** cuando se utiliza la CLI, la API o Terraform. Solo la consola de EFS las habilita por usted. Pase `--backup` en la creación, o habilítelo después:

```
aws efs put-backup-policy --file-system-id <fs-id> --backup-policy
Status="ENABLED"

aws efs describe-backup-policy --file-system-id <fs-id>
```

Esto adjunta el plan de AWS Backup predeterminado para EFS: copias de seguridad diarias con una retención de 35 días. Confirme que AWS Backup se ofrece en su Región y presupueste para ello por separado de EFS.

Elegir rendimiento elástico

La CLI y la API utilizan por defecto el rendimiento de ráfaga (Bursting throughput), cuya línea base escala con los bytes almacenados. Un sistema de archivos de punto de montaje comienza vacío, por lo que converge en el mínimo y se limita a 35.000 IOPS de lectura y 7.000 de escritura. El rendimiento elástico (Elastic throughput) eleva esto a aproximadamente 250.000 y 50.000, que es lo que las muchas operaciones de archivos pequeños en un espacio de trabajo realmente necesitan.

```
aws efs update-file-system --file-system-id <fs-id> --throughput-mode
elastic
```

El modo de rendimiento es un atributo del sistema de archivos. No se puede configurar en la StorageClass, y SecurSpaces no puede verlo ni advertir sobre ello.

> **Nota**

> El rendimiento elástico mide cada gigabyte leído y escrito, con las escrituras cobradas a aproximadamente el doble de la tarifa de las lecturas. Calcule el cambio a partir de sus métricas de lectura y escritura de CloudWatch primero, y no cambie durante las horas de trabajo. El rendimiento elástico no reduce la latencia por operación, por lo que no es una solución para el trabajo lento con archivos pequeños.

Requisitos previos de Amazon S3 Files

Amazon S3 Files requiere los requisitos previos comunes descritos anteriormente —los destinos de montaje por zona de disponibilidad, la regla NFS con ámbito y la política del controlador CSI— además de lo siguiente.

> **Nota**

> No confunda Amazon S3 Files con Mountpoint para Amazon S3 (`s3.csi.aws.com`), que no es compatible con POSIX y no es un backend de punto de montaje compatible.

Preparar el bucket

El bucket de S3 debe tener el **control de versiones habilitado** y la **encriptación del lado del servidor** configurada antes de crear el sistema de archivos. El control de versiones del bucket es también la única forma de recuperar un archivo eliminado en S3 Files.

El indicador `--accept-bucket-warning` no es un interruptor de "datos existentes". S3 Files se niega a crear un sistema de archivos con ámbito a un prefijo que contenga un gran número de objetos, advirtiendo que los renombres o movimientos recursivos en dicho sistema de archivos son lentos y costosos, porque cada archivo necesita su propia copia y eliminación contra el bucket. Pase el indicador para reconocer la advertencia y permitir que la creación continúe. No hace nada con respecto al control de versiones o la encriptación, que aún deben configurarse de antemano.

Crear el rol de servicio

Cuando crea el sistema de archivos, pasa un rol de IAM que S3 Files asume para leer y escribir en su bucket y para administrar las reglas de EventBridge que impulsan la sincronización. La

consola de S3 crea este rol por usted. Desde la CLI o Terraform, debe crear tanto la política de confianza como la política de permisos.

Un rol con solo una política de confianza es aceptado en el momento de la creación, pero deja la sincronización inoperable.

La política de confianza permite que S3 Files asuma el rol, a través del principal de servicio `elasticfilesystem.amazonaws.com`. Mantenga las condiciones de cuenta y ARN. Impiden que otra cuenta de AWS use su rol contra su bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": { "Service": "elasticfilesystem.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": { "aws:SourceAccount": "<account-id>" },
      "ArnLike": { "aws:SourceArn": "arn:aws:s3files:<region>:<account-
id>:file-system/*" }
    }
  }]
}
```

La política de permisos debe otorgar lo siguiente. Limite cada declaración a los recursos que nombra y mantenga las condiciones: sin ellas, el rol tendría muchos más permisos de los que necesita este sistema de archivos.

- `s3:ListBucket` y `s3:ListBucketVersions` en el bucket, condicionado a que `aws:ResourceAccount` coincida con su ID de cuenta.

- `s3:AbortMultipartUpload`, `s3:DeleteObject*`, `s3:GetObject*`, `s3:List*` y `s3:PutObject*` en el contenido del bucket, con la misma condición `aws:ResourceAccount`. Las acciones con comodín son intencionadas: S3 Files utiliza las operaciones de S3 conscientes de la versión que habilita el control de versiones del bucket.
- `kms:GenerateDataKey`, `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncryptFrom` y `kms:ReEncryptTo` en el ARN de la clave que cifra el bucket, condicionado a que `kms:ViaService` coincida con `s3.<region>.amazonaws.com` y a que `kms:EncryptionContext:aws:s3:arn` coincida con el bucket y su contenido. Si se deja sin un recurso y estas condiciones, la declaración permite que el rol use cada clave en la cuenta cuya política de clave delega en IAM.
- Gestión de reglas de EventBridge — `events:PutRule`, `events:PutTargets`, `events:EnableRule`, `events:DisableRule`, `events:RemoveTargets` y `events:DeleteRule` — con ámbito en `rule/DO-NOT-DELETE-S3-Files*` y condicionado a que `events:ManagedBy` coincida con `elasticfilesystem.amazonaws.com`, además de las acciones de lectura de EventBridge.

Para ver los documentos de política completos, consulte la documentación de AWS sobre cómo trabajar con Amazon S3 Files.

Advertencia

Si el bucket utiliza SSE-KMS, el rol no puede leer ni escribir un solo objeto sin las acciones `kms:`. Las lecturas fallan y las escrituras nunca llegan al bucket, ambas de forma silenciosa. Mantenga la declaración de KMS incluso en un bucket SSE-S3, para que el rol siga funcionando si el bucket se cambia a SSE-KMS más tarde. Si la clave es una clave administrada por el cliente, su política de clave debe también permitir este rol. Una política de IAM por sí sola no es suficiente.

Las reglas de EventBridge llamadas `DO-NOT-DELETE-S3-Files...` son la forma en que los cambios realizados directamente en el bucket llegan a los espacios de trabajo montados. No las elimine ni las desactive. Sin ellas, los archivos en caché seguirán sirviendo contenido obsoleto.

Crear el sistema de archivos

```
aws s3files create-file-system --bucket <bucket-arn> [--prefix p/] --role-arn <service-role-arn>
```

El sistema de archivos cifra su propia capa de alto rendimiento en reposo por defecto. Puede proporcionar una clave administrada por el cliente para ese almacenamiento en su lugar. Esta es una clave diferente de la que cifra el bucket. Si proporciona una, debe estar en la misma Región que el sistema de archivos, y su política de clave debe permitir S3 Files `kms:Decrypt`, `kms:GenerateDataKeyWithoutPlaintext`, `kms:CreateGrant` y `kms:DescribeKey`. La política de clave predeterminada ya lo hace.

> **Advertencia**
>
> Deshabilitar o eliminar esa clave hace que el sistema de archivos, y cada punto de montaje en él, sea inaccesible. La deshabilitación surtirá efecto después de un breve retraso y se deshará al volver a habilitar la clave; eliminarla es permanente. Trate la clave como parte del sistema de archivos en lugar de como una clave que puede retirar durante la higiene rutinaria de claves.

Comprobar versiones y compatibilidad de plataforma

- **En el clúster** — el controlador CSI de Amazon EFS debe ser la versión 3.0.0 o posterior.
- **En cualquier host EC2 desde el que monte directamente** — el cliente `amazon-efs-utils` debe ser la versión 3.0.0 o posterior.
- **AWS CLI** — lo suficientemente reciente como para incluir los comandos `s3files`. verificar con `aws s3files help`.
- **En su Región** — confirme que Amazon S3 Files se ofrece en la Región en la que se ejecuta su clúster. Estuvo disponible de forma general en abril de 2026 en 34 Regiones, y la cobertura crece, así que consulte la tabla de servicios regionales de AWS para ver la lista actual.

Adjunte `AmazonS3FilesCSIDriverPolicy` y `AmazonS3FilesClientFullAccess` a la identidad del controlador, y `AmazonS3FilesClientFullAccess`, `AmazonElasticFileSystemsUtils` y lectura de S3 en el bucket a la identidad del nodo. Consulte Ámbito de los permisos de IAM antes de adjuntar las políticas administradas a nivel de cuenta.

Amazon S3 Files no admite la conexión estática entre cuentas: el sistema de archivos y el bucket deben estar en la misma cuenta de AWS que el clúster. No es compatible con EKS Fargate, EKS Hybrid Nodes o contenedores de Windows.

Ámbito de los permisos de IAM

El controlador CSI de EFS se autentica a través de roles de IAM para cuentas de servicio (IRSA).

> **Advertencia**

> La mayoría de los tutoriales de AWS adjuntan las políticas de nodo al rol de instancia de EC2 del grupo de nodos administrado. Una concesión de rol de instancia no es privada para el controlador CSI: cualquier carga de trabajo en ese nodo que pueda acceder al servicio de metadatos de la instancia puede usarla. Dado que los espacios de trabajo ejecutan código proporcionado por el cliente, trate cada política en el rol de nodo como una que ha concedido a sus desarrolladores.

> Asigne al controlador de nodo su propio rol vinculado a su cuenta de servicio en lugar de usar el rol de instancia:

1. Habilite el proveedor OIDC del clúster.
2. Cree un rol cuya política de confianza vincule tanto la cuenta de servicio como la audiencia de STS.
3. Anote `efs-csi-node-sa` con `eks.amazonaws.com/role-arn`. Haga lo mismo para `efs-csi-controller-sa`.

Utilice el valor exacto de `system:serviceaccount:<namespace>:<name>`. Un sujeto comodín, o una condición de audiencia faltante, permite que cualquier pod en el clúster asuma el rol.

Ámbito del acceso del cliente a sus sistemas de archivos

Todas las políticas de cliente de S3 Files administradas por AWS utilizan `"Resource": "*"` y no pueden limitarse a un sistema de archivos. `AmazonS3FilesClientFullAccess` se aplica tanto a la identidad del controlador como a la identidad del nodo, por lo que cualquier elemento que posea cualquiera de ellas está autorizado a montar todos los sistemas de archivos de S3 Files en la cuenta y a escribir en ellos como root.

Reemplace esa política administrada en ambas identidades con una política administrada por el cliente que nombre sus sistemas de archivos y les otorgue `s3files:ClientMount` y

`s3files:ClientWrite`. Agregue `s3files:ClientRootAccess` solo donde un montaje lo necesite genuinamente.

De manera similar, otorgue a la identidad del nodo lectura de S3 con ámbito en los buckets que respaldan los puntos de montaje en lugar de una política de solo lectura a nivel de cuenta como `AmazonS3ReadOnlyAccess`. Una política en línea que otorgue `s3:GetObject`, `s3:GetObjectVersion`, y `s3:ListBucket` en esos buckets es suficiente.

> **Nota**
>
> Una política de sistema de archivos que omite un rol no revoca una concesión de identidad a nivel de cuenta. Una autorización en la política de identidad o en la política de sistema de archivos es suficiente. O bien delimite la política de identidad, o añada una denegación explícita.

Reforzar los metadatos de la instancia

Requiera IMDSv2 y establezca el límite de saltos de metadatos en 1 en el grupo de nodos. Aplique los pasos en este orden. Si se aplican fuera de orden, esto interrumpe silenciosamente el aprovisionamiento de Mount Point.

1. **Confirme que el controlador utiliza su propio rol.** Las credenciales de rol se inyectan cuando se crea un pod, por lo que anotar las cuentas de servicio no es suficiente. Hasta que los pods se reinicien, el controlador recurre al rol del nodo y parece funcionar. Reinicie el controlador, confirme que cada pod informa de un ARN de rol y cree un Mount Point con éxito.
2. **Cambie la plantilla de lanzamiento**, para que los nodos de reemplazo se creen reforzados. Establezca `HttpTokens: required`, `HttpPutResponseHopLimit: 1` y `HttpEndpoint: enabled`. Editar la plantilla no es suficiente por sí solo: un grupo de nodos gestionado permanece anclado a la versión de la plantilla de lanzamiento con la que fue creado, así que actualice el grupo de nodos a la nueva versión también. De lo contrario, cada escalado horizontal y cada nodo reemplazado volverá a la versión anclada, y el endurecimiento se degradará silenciosamente en un clúster cuyos nodos de espacio de trabajo van y vienen.
3. **Implemente el cambio en los nodos en ejecución** uno a la vez, observando el espacio de nombres `kube-system` durante unos 15 minutos después del primero antes de continuar:

   ```
   aws ec2 modify-instance-metadata-options --instance-id <id> \
   ```

```
  --http-tokens required --http-put-response-hop-limit 1 --http-
endpoint enabled
```

Para revertir un nodo, establezca `--http-put-response-hop-limit 2` en esa instancia.

4. **Compruebe lo que el grupo de nodos entregará.** Lea las opciones de metadatos de la plantilla de lanzamiento y confirme que el grupo de nodos apunta a la versión que comprobó:

```
aws ec2 describe-launch-template-versions --launch-template-id <id> --
versions '$Latest' \

  --query
'LaunchTemplateVersions[0].LaunchTemplateData.MetadataOptions'
```

`"HttpPutResponseHopLimit": 2` significa que IMDSv2 está forzado, pero el acceso del pod al servicio de metadatos no está bloqueado.

5. **verificar desde un pod ordinario, no desde un terminal de espacio de trabajo.** Cada pod de espacio de trabajo ya descarta el tráfico a `169.254.169.254` dentro de su propio espacio de nombres de red, por lo que una sonda ejecutada en un terminal de espacio de trabajo no devuelve nada independientemente de si el nodo fue endurecido o no. Ejecútelo desde un pod que no tenga ese bloqueo y espere un tiempo de espera sin que se devuelva ningún token:

```
kubectl run imds-probe --rm -it --restart=Never --image=curlimages/curl
-- \

  sh -c 'curl -s -m2 -X PUT http://169.254.169.254/latest/api/token \

    -H "X-aws-ec2-metadata-token-ttl-seconds: 60"'
```

Luego, ejecute la misma solicitud en el host como un control positivo. Todavía debe tener éxito. Si no lo hace, ha roto los agentes del host en lugar de proteger los pods.

Las opciones de metadatos se fijan cuando se lanza una instancia. Cambiar la plantilla de lanzamiento no afecta a los nodos en ejecución, y cambiar un nodo en ejecución no sobrevive a su reemplazo.

> **Nota**

> Con `eksctl`, use `disablePodIMDS: true` en el grupo de nodos. La clave `disableIMDSv1` relacionada ya tiene un valor predeterminado de `true`, por lo que establecerla sola no cambia nada, y `eksctl` escribe un límite de saltos de 2 sin `disablePodIMDS`. Esto deja a cada pod capaz de tomar prestado el rol del nodo. `disablePodIMDS` no se puede combinar con `iam.withAddonPolicies`, y se rechaza cuando un grupo de nodos gestionado proporciona su propia plantilla de lanzamiento.

> Un límite de salto de 1 impide que los pods ordinarios lleguen al servicio de metadatos. Los procesos en el host y los pods que usan `hostNetwork` no se ven afectados, incluido el DaemonSet del nodo CSI. El controlador CSI se ejecuta en la red de pods y se ve afectado: si pierde el acceso a los metadatos, los nuevos puntos de montaje fallarán mientras que los montajes existentes seguirán funcionando.

Siguiente

- Configurar SecurSpaces

Información relacionada

- Crear un PersistentVolume
- Configurar SecurSpaces
- Solucionar problemas de puntos de montaje de AWS
- Puntos de montaje de AWS

Configure SecurSpaces for AWS Mount Points

Complete primero la preparación de AWS. Los pasos aquí dependen de un sistema de archivos, sus destinos de montaje y los roles de IAM ya existentes.

Crear la StorageClass

Usted crea la StorageClass manualmente, una por cada sistema de archivos de respaldo. SecurSpaces no incluye ninguna ni crea ninguna. Una missing StorageClass es la causa más común de un diálogo de creación vacío.

```
apiVersion: storage.k8s.io/v1

kind: StorageClass

metadata:
```

```
  name: sn-efs-mountpoint
provisioner: efs.csi.aws.com
mountOptions:
  - tls
parameters:
  provisioningMode: efs-ap
  fileSystemId: fs-0abc123
  basePath: "/dyn"
  directoryPerms: "700"
  gidRangeStart: "50000"
  gidRangeEnd: "51000"
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Valores requeridos:

- `provisioner: efs.csi.aws.com` para ambos backends.
- `parameters.provisioningMode` — `efs-ap` para Amazon EFS, `s3files-ap` para Amazon S3 Files. Este parámetro, no ninguna opción en la interfaz, selecciona el backend. Los usuarios eligen el backend seleccionando la StorageClass, así que dé a cada clase un nombre claro.
- `parameters.fileSystemId` — el ID del sistema de archivos que creó. Debe estar presente y debe coincidir exactamente. SecurSpaces también utiliza estos ID para distinguir los sistemas de archivos que comparte de los externos, por lo que un valor en blanco o mal escrito cuesta más que una sola clase. Compruébelo antes de que alguien use la clase.
- `mountOptions: [tls]` — una lista de nivel superior, un elemento hermano de `parameters`, no una clave dentro de él.

- `volumeBindingMode: Immediate` — EFS y S3 Files no tienen zonas. Una clase configurada en `WaitForFirstConsumer` nunca podrá vincularse y la creación será rechazada.

Los valores opcionales incluyen `basePath`, `subPathPattern`, `directoryPerms`, y el par `gidRangeStart` y `gidRangeEnd`, que limitan el ID de grupo POSIX que impone el punto de acceso. Configure ambos o ninguno. Mantenga un rango personalizado lo suficientemente amplio para cada Mount Point planificado en ese sistema de archivos, porque cada punto de acceso consume un ID de grupo.

Un sistema de archivos y una StorageClass sirven a muchos Mount Points. Añada más solo cuando exceda el límite de puntos de acceso, necesite aislamiento de rendimiento o necesite aislamiento estricto de inquilinos.

Comprobar el ID del sistema de archivos

Nada valida `fileSystemId` contra AWS cuando usted crea la clase. SecurSpaces acepta lo que usted escribe y actúa sobre ello solo cuando un usuario crea o adjunta un Mount Point. Un valor en blanco y un valor incorrecto fallan entonces de diferentes maneras.

Un valor en blanco falla de forma segura (closed), y el efecto no se limita a la clase que lo contiene. Una Mount Point StorageClass sin `fileSystemId` hace que SecurSpaces considere poco fiable toda su visión de los sistemas de archivos que comparte, por lo que se niega en lugar de adivinar: el modo de adjuntar en el que un usuario escribe coordenadas sin procesar se deniega para cada clase en el clúster, incluidos los adjuntos a sistemas de archivos no relacionados con el incompleto.

Un valor incorrecto no desactiva inmediatamente la protección. SecurSpaces reconoce los sistemas de archivos que comparte a partir de dos señales independientes: los ID declarados en sus Mount Point StorageClasses, y los sistemas de archivos en los que ya ha aprovisionado Mount Points en esa región. Un error tipográfico por sí solo no descomparte el sistema de archivos real. El riesgo es la ventana en la que la segunda señal está vacía — un sistema de archivos en el que SecurSpaces nunca ha aprovisionado, o uno donde cada Mount Point que creó allí falló su verificación de identidad posterior a la vinculación. En esa ventana, un ID incorrecto hace que el sistema de archivos compartido real parezca externo, y un volumen preconstruido que lo cubre por completo se vuelve adjuntable por un usuario común.

Lea el ID de AWS antes de que alguien use la clase:

```
aws efs describe-file-systems --file-system-id <fs-id> --query
'FileSystems[0].FileSystemId'
```

Cifrado en tránsito

Los archivos EFS y S3 se montan sobre NFS en el puerto 2049, y el controlador CSI solo cifra ese tráfico cuando el montaje lleva la opción `tls`. Establézcala en la StorageClass y en cada PersistentVolume que cree. Sin ella, cada byte leído o escrito viaja sin cifrar.

SecurSpaces se basa estrictamente en la opción de montaje literal `tls`. No acepta `parameters.encryptInTransit`, un punto de acceso habilitado para TLS, o una política de sistema de archivos EFS que imponga `SecureTransport` como sustitutos.

La rigurosidad con la que se aplica esto difiere según el modo:

- **Adjuntar existente falla cerrado.** En el momento de la vinculación, SecurSpaces lee el volumen que nombró y rechaza la conexión a menos que sea un volumen `efs.csi.aws.com` cuyas opciones de montaje contengan `tls`.
- **Crear nuevo es un esfuerzo óptimo.** Una StorageClass sin `tls` normalmente está oculta de la lista **Crear nuevo**, y nombrarla de todos modos es rechazado. Todas estas comprobaciones dependen de la lectura de la StorageClass desde la API de Kubernetes.

> **Advertencia**
>
> La lectura de StorageClass la realiza el servicio del espacio de trabajo. Si no puede leer StorageClasses, se omite cada comprobación de cifrado de Crear nuevo, una StorageClass sin `tls` se vuelve utilizable, y el montaje se ejecuta sin cifrar y sin errores. Este es el único fallo en este artículo que falla en la dirección permisiva.

Permisos del clúster

StorageClasses y PersistentVolumes tienen ambos ámbito de clúster, por lo que la concesión que permite al servicio del espacio de trabajo leerlos tiene que ser un ClusterRole. El gráfico lo instala como un ClusterRole y un ClusterRoleBinding, ambos llamados `<release>-workspace-api-clusterwide`, vinculados a la cuenta de servicio del espacio de trabajo `<release>-workspace-api`. Para todo lo demás a lo que la plataforma accede en el clúster, consulte Límites de confianza.

Los puntos de montaje dependen de estos permisos de lectura:

RECURSO	VERBOS	DE QUÉ DEPENDE
`storageclasses`	`get`, `list`	Listar las clases ofrecidas en **Crear nuevo**, y la comprobación de cifrado en tránsito
`persistentvolumes`	`get`, `list`	Leer el volumen asignado a un nuevo punto de montaje, y listar los volúmenes ofrecidos por **Adjuntar existente**

Dos configuraciones de Helm eliminan la concesión. Establecer `platform.serviceKubernetesConfig.serviceAccounts.wsAPIServiceAccount` en su propia cuenta de servicio significa que el gráfico no instala ninguno de los objetos RBAC del servicio del espacio de trabajo, por lo que debe crear y vincular los permisos equivalentes usted mismo. Establecer `platform.serviceKubernetesConfig.rbac.createWorkspaceClusterRoles` en `false` elimina todo el ClusterRole y su vinculación: no solo la lectura de StorageClass, sino también la lectura de PersistentVolume, los verbos de escritura de PersistentVolume que `allowPersistentVolumeAccess` añadiría de otro modo, y el acceso de lectura a nodos y métricas de nodos. El Role con ámbito de espacio de nombres que el gráfico instala junto a él no se ve afectado por esa configuración.

verificar cada verbo por separado. Kubernetes `list` no implica `get`:

```
kubectl auth can-i get storageclasses --
as=system:serviceaccount:<namespace>:<release>-workspace-api

kubectl auth can-i list storageclasses --
as=system:serviceaccount:<namespace>:<release>-workspace-api

kubectl auth can-i get persistentvolumes --
as=system:serviceaccount:<namespace>:<release>-workspace-api

kubectl auth can-i list persistentvolumes --
as=system:serviceaccount:<namespace>:<release>-workspace-api
```

`--as` suplanta otra identidad, lo que requiere cluster-admin o una concesión `impersonate` propia. En una instalación predeterminada, también puede confirmar que los objetos que llevan la concesión están presentes:

```
kubectl get clusterrole,clusterrolebinding <release>-workspace-api-
clusterwide
```

Si proporcionó `wsAPIServiceAccount`, ninguno de esos objetos existe y el gráfico nunca crea `<release>-workspace-api`, por lo que los comandos anteriores informan `no` para una cuenta bajo la cual no se ejecuta nada. Sustituya la cuenta que proporcionó, que puede leer desde el pod en ejecución:

```
kubectl -n <namespace> get pod -l app=<release>-workspace-api -o
jsonpath='{.items[0].spec.serviceAccountName}'
```

Lo que cuesta cada permiso faltante:

- La falta de `get` en `storageclasses` omite las comprobaciones de cifrado y permite un montaje sin cifrar.
- La falta de `list` en `storageclasses` interrumpe completamente el descubrimiento: la lista de creación está vacía y la característica desaparece.
- La falta de `get` en `persistentvolumes` permite que cada punto de montaje de **Crear nuevo** alcance el estado listo sin que su volumen sea leído de vuelta, por lo que el punto de montaje no guarda registro del volumen en el que se aprovisionó.
- La falta de `list` en `persistentvolumes` rompe el selector de volumen de **Adjuntar existente**, que muestra **Error al cargar volúmenes disponibles** y un enlace de **Reintentar**. Ese es un estado diferente de **No hay volúmenes disponibles para adjuntar**, lo que significa que la lectura fue exitosa y ningún volumen coincidió con la etiqueta de ámbito.

Habilitar la función

El almacenamiento de puntos de montaje se habilita en **Configuración del sistema > Integraciones > Almacenamiento de puntos de montaje**. La configuración del sistema es un área solo para administradores. Un oficial de seguridad que no sea también administrador no puede habilitarla.

- **El proveedor de la nube se detecta, no se elige.** SecurSpaces determina si los puntos de montaje están respaldados por AWS o Azure a partir de los aprovisionadores CSI de las StorageClasses en el clúster. Para exponer las opciones de AWS, cree primero las StorageClasses de puntos de montaje de AWS.
- **Active el interruptor de almacenamiento de archivos.** Mientras esté desactivado, el flujo de creación estará oculto para los usuarios.

- **Use una nube por clúster.** Si hay una StorageClass de puntos de montaje de AWS y otra de Azure, el proveedor no se puede resolver, los interruptores se desactivan y la función se retira. La página explica esto y enumera los proveedores que detectó. Elimine las clases de una nube y vuelva a visitar la página. No es necesario reiniciar, pero espere unos 30 segundos para la caché de configuración.
- **`allowPersistentVolumeAccess` rige un modo de conexión.** El modo en el que un usuario introduce coordenadas sin procesar y SecurSpaces construye el volumen requiere `platform.serviceKubernetesConfig.rbac.allowPersistentVolumeAccess`, que por defecto es `false`. Mientras esté desactivado, ese modo estará oculto, pero la conexión de un volumen que haya creado y la creación de nuevos Puntos de montaje seguirán funcionando. El cambio surte efecto cuando `helm upgrade` se completa, sin reiniciar el pod.

> **Nota**
>
> Solo esta página explica por qué los puntos de montaje no están disponibles. En las vistas de proyecto y espacio de trabajo, la opción simplemente está oculta. Clasifique cualquier informe de puntos de montaje faltantes abriendo esta página primero.

Siguiente

- Crear un PersistentVolume, si publica sus propios volúmenes
- Solución de problemas

Información relacionada

- Crear un PersistentVolume
- Preparar los recursos de AWS
- Solucionar problemas de puntos de montaje de AWS
- Puntos de montaje de AWS(/es-es/securspaces/administer/aws-mount-points.html)
- Límites de confianza(/es-es/securspaces/security/trust-boundaries.html)

Author a PersistentVolume for Attach Existing

SecurSpaces nunca crea, cambia ni limpia estos volúmenes. Solo crea una reclamación que se vincula a su volumen por nombre.

Establecer la etiqueta de ámbito

SecurSpaces registra el propietario del almacenamiento que crea. Para un volumen que usted crea, no tiene dicho registro, por lo que debe declarar el ámbito de consumidor previsto con la etiqueta `strong.network/mount-point-scope`.

VALOR DE LA ETIQUETA	QUIÉN PUEDE ADJUNTARLO
`project.<projectId>`	Solo ese proyecto.
`org.<organizationId>`	Cualquier proyecto de esa organización.
`shared`	Cualquier proyecto de toda la implementación.

Use un punto, no dos puntos. Kubernetes prohíbe `:` en un valor de etiqueta.

Un volumen sin etiqueta de ámbito, o con un valor no reconocido, no se ofrece a nadie y no se puede adjuntar. Una etiqueta olvidada nunca puede exponer accidentalmente un volumen, pero es la causa más común de "mi volumen no está en la lista".

Los ámbitos `project.` y `org.` se aplican mediante comprobaciones del lado del servidor, tanto en el selector como en la vinculación. El valor `shared` no tiene límites. Úselo solo para datos que desee que cualquier persona de la implementación pueda alcanzar.

Encuentre el ID numérico del proyecto o de la organización en la barra de direcciones del navegador. El ID es el segmento de ruta después de `/project/` o `/organization/`.

Cumpla los requisitos del volumen

```
apiVersion: v1

kind: PersistentVolume

metadata:

  name: shared-dataset-alpha

  labels:

    strong.network/mount-point-scope: "project.1090137447483732"

spec:
```

```
  capacity:
    storage: 1Gi
  accessModes: ["ReadWriteMany"]
  persistentVolumeReclaimPolicy: Retain
  storageClassName: ""
  mountOptions: ["tls"]
  csi:
    driver: efs.csi.aws.com
    volumeHandle: fs-0abc123::fsap-07c9def
    # volumeHandle: s3files:fs-0def456::fsap-001d    # Amazon S3 Files
keeps the prefix
```

SecurSpaces comprueba lo siguiente antes de permitir que se adjunte un volumen:

- `spec.csi.driver` es `efs.csi.aws.com`, para ambos backends.
- `spec.mountOptions` contiene `tls`.
- `spec.accessModes` permite el permiso que el propietario eligió, y su primera entrada es una que el controlador de almacenamiento acepta. Consulte Establecer los modos de acceso.
- `spec.capacity.storage` tiene un valor y no es menor que el tamaño solicitado por el propietario. Más allá de esa comprobación, el valor es nominal: EFS y S3 Files ignoran el tamaño y nunca lo aplican.
- El volumen está en la fase `Available`.

Escriba `spec.csi.volumeHandle` en el formato estático para su backend. Para Amazon EFS no tiene prefijo, `<fs-id>::<access-point-id>`; el prefijo `efs:` pertenece solo al aprovisionamiento dinámico. Para Amazon S3 Files mantiene el prefijo, `s3files:<fs-id>::<access-point-id>`. SecurSpaces no requiere que el identificador nombre un punto de acceso, por lo que el identificador que publique es lo que obtendrá el proyecto. Consulte Publicar solo identificadores de puntos de acceso.

Liste `tls` en `spec.mountOptions` y nada más. En particular, no añada `ro` allí para que los datos sean de solo lectura. Las opciones de montaje de un volumen se aplican a cada montaje del mismo, por lo que `ro` fija cada punto de montaje creado en ese volumen como de solo lectura, incluidos los que un propietario creó como de lectura/escritura, lo que para ellos se interpreta como pérdida de datos. La opción de solo lectura es una elección por punto de montaje, aplicada en el pod del espacio de trabajo.

SecurSpaces no lee ninguno de los dos campos siguientes, pero Kubernetes sí. Configúrelos usted mismo. Cada uno falla de una manera diferente, y ninguna de las fallas se explica en ninguna parte de la interfaz:

- `spec.persistentVolumeReclaimPolicy: Retain`. Un volumen configurado en `Delete` se ofrece y se vincula normalmente. Cuando se elimina el punto de montaje y la reclamación desaparece, el volumen queda **Liberado**: no se elimina y sus datos están intactos, pero no puede respaldar otro punto de montaje hasta que lo restablezca. Establezca `Retain` de todos modos. Si el volumen alguna vez lleva la anotación `pv.kubernetes.io/provisioned-by` del controlador CSI de EFS, `Delete` se lo entrega al controlador, que elimina el punto de acceso que nombra el volumen.
- `spec.storageClassName: ""`, una cadena vacía explícita. Kubernetes vincula una reclamación a un volumen solo cuando los dos valores `storageClassName` coinciden, y la reclamación que construye SecurSpaces siempre lleva `""`. Un volumen que nombra una StorageClass se ofrece y se acepta, y luego nunca se vincula: la conexión agota el tiempo de espera después de tres minutos y el Punto de montaje entra en un estado de error. Tampoco omita el campo. Un valor ausente permite que el controlador de admisión de StorageClass predeterminado convierta la vinculación estática en aprovisionamiento dinámico.

No se necesita ningún secreto de Kubernetes. El acceso a AWS está respaldado por IAM y el punto de acceso.

Establecer los modos de acceso

Utilice `accessModes: ["ReadWriteMany"]`. Ese único valor es la respuesta correcta para cada volumen de punto de montaje de AWS, ya sea que los propietarios lo adjunten en modo lectura/escritura o solo lectura.

No significa que el volumen deba ser escribible. La elección de lectura/escritura pertenece al punto de montaje, no al volumen. Un propietario que elige **Solo lectura** obtiene un montaje genuinamente de solo lectura, porque el espacio de trabajo monta el volumen en modo de solo

lectura y el controlador de almacenamiento aplica `ro` en el momento del montaje. El modo de acceso no influye en ello.

> **Nota**
>
> Un punto de montaje de lectura/escritura necesita `ReadWriteMany`. Uno de solo lectura acepta `ReadWriteMany` o `ReadOnlyMany`. Un volumen que lista `ReadWriteMany` deja, por lo tanto, ambas opciones abiertas al propietario. Cuando los modos del volumen permiten solo una de las dos, el diálogo fija la selección en **Solo lectura** y explica por qué. Nunca fuerza la selección a **Lectura/Escritura**.

> Ponga `ReadWriteMany` primero. Kubernetes pasa solo la primera entrada de `accessModes` al controlador de almacenamiento, y el controlador de AWS no acepta `ReadOnlyMany`. Un volumen cuyo primer modo es `ReadOnlyMany` no puede ser montado por ningún espacio de trabajo: el selector lo lista como no seleccionable y lo etiqueta como **no se puede montar**, y un intento de adjuntarlo es rechazado con **El volumen seleccionado no se puede montar**. Listar `ReadOnlyMany` después de `ReadWriteMany` es inofensivo pero inútil, porque nada lo lee. Un volumen que lista solo `ReadWriteOnce` no se ofrece en absoluto, porque un punto de montaje se comparte entre muchos pods de espacio de trabajo y necesita acceso de varios nodos.

`spec.accessModes` no es inmutable en un PersistentVolume, por lo que un volumen creado de forma incorrecta se corrige in situ:

```
kubectl patch pv <name> --type=merge -p '{"spec":{"accessModes":
["ReadWriteMany"]}}'
```

El parche se acepta en un volumen `Bound`, no altera la vinculación y deja los datos intactos. Reinicie cualquier espacio de trabajo que ya estuviera atascado en el volumen, para que obtenga un nuevo pod y se le pregunte al controlador de nuevo. La reclamación vinculada mantiene sus modos de acceso originales, lo cual es esperado e inofensivo: la especificación de una reclamación es realmente inmutable, solo el primer modo del volumen llega al controlador, y el estado de la reclamación sigue al parche. Si el volumen se reconcilia a partir de un manifiesto por GitOps, o está protegido por un webhook de admisión, cámbielo en el origen en su lugar, o la siguiente sincronización revertirá el parche.

Para encontrar volúmenes ya creados de forma incorrecta:

```
kubectl get pv -o json | jq -r '
  .items[] | select(.spec.csi.driver=="efs.csi.aws.com")
  | select(.spec.accessModes[0]=="ReadOnlyMany")
  | .metadata.name'
```

Advertencia

No elimine ni vuelva a crear un volumen para cambiar sus modos de acceso. Mientras una reclamación esté todavía vinculada a él, `kubectl delete pv` solo marca el volumen `Terminating`, porque Kubernetes mantiene el finalizador `kubernetes.io/pv-protection` hasta que el volumen sale de la fase `Bound`, por lo que el volumen corregido no puede aplicarse con el mismo nombre. Nunca elimine forzosamente ese finalizador en un volumen vinculado: hacerlo elimina la vinculación de un punto de montaje activo.

De ninguna manera `accessModes` publica un conjunto de datos de solo lectura. Los modos de acceso son una sugerencia utilizada para hacer coincidir una reclamación con un volumen, y no imponen nada en el momento del montaje. Para publicar datos que un consumidor genuinamente no puede escribir, impóngalo en la capa de almacenamiento: dé al punto de acceso una identidad POSIX de solo lectura, o deniegue las escrituras con una política de sistema de archivos. Eso se mantiene independientemente del permiso que elija el propietario del punto de montaje.

Publicar solo identificadores de puntos de acceso

El identificador de volumen tiene tres campos separados por dos puntos, `FileSystemId:Subpath:AccessPointId`. Deje un campo vacío para omitirlo, por lo que un identificador sin subruta lleva dos puntos. Solo el campo del punto de acceso impone el aislamiento.

IDENTIFICADOR	QUÉ MONTA	AISLAMIENTO
`fs-id`	La raíz del sistema de archivos.	Ninguna. El espacio de trabajo ve los datos de cada proyecto.

IDENTIFICADOR	QUÉ MONTA	AISLAMIENTO
`fs-id:/subdir`	Un subdirectorio.	Ninguna. Solo confinado a la ruta, tratado exactamente como un ID de sistema de archivos simple.
`fs-id::fsap-id`	Un punto de acceso.	Completa, pero solo si ese punto de acceso está restringido.
`fs-id:/subdir:fsap-id`	Un subdirectorio bajo la raíz del punto de acceso.	La misma condición. El aislamiento proviene del punto de acceso, nunca de la subruta.

Para combinar una subruta con un punto de acceso, coloque un solo dos puntos entre ellos. `fs-id:/subdir::fsap-id` no es ese identificador. Los dos puntos adicionales sacan el ID del punto de acceso del tercer campo, por lo que SecurSpaces no lee ningún ID de punto de acceso y trata el volumen como una conexión de sistema de archivos completa.

Nombrar un punto de acceso no es una condición para que se ofrezca. Se ofrece un identificador de sistema de archivos simple y se vincula como cualquier otro volumen. SecurSpaces lo retiene solo de un usuario que no es ni administrador ni oficial de seguridad, y solo cuando el sistema de archivos es uno desde el que aprovisiona puntos de montaje, o cuando no puede leer ese conjunto de sistemas de archivos. En cualquier otro sistema de archivos, publicar un identificador simple es su decisión exclusiva.

Advertencia

En la ruta donde publica un volumen, el identificador que publica es el límite de seguridad. Un identificador de sistema de archivos sin restricciones se monta y funciona, no hay una segunda verificación del lado del clúster cuando se vincula un volumen que usted preconstruyó, y nada advierte al usuario. Cualquier usuario que pueda crear un punto de montaje en un proyecto al que su volumen esté asignado puede vincularlo. Publique solo identificadores de puntos de acceso, a menos que desee que todos en ese ámbito vean todo el sistema de archivos.

> Un ID de punto de acceso no es por sí mismo aislamiento. SecurSpaces decide el aislamiento puramente en función de si un ID de punto de acceso está presente. Nunca lee la configuración del punto de acceso de AWS. En AWS, tanto el directorio raíz como el usuario POSIX son opcionales en un punto de acceso, y uno creado sin ellos expone la raíz del sistema de archivos mientras sigue satisfaciendo todas las comprobaciones. verificar antes de publicar:

```
aws efs describe-access-points --access-point-id <fsap-id> \

  --query 'AccessPoints[].
{Root:RootDirectory.Path,Uid:PosixUser.Uid,Gid:PosixUser.Gid}'
```

Publique solo si `Root` es una ruta real por conjunto de datos, no `/` ni `null`, y `Uid` y `Gid` están configurados. Los puntos de acceso no se pueden editar después de la creación, por lo que uno sin restricciones debe ser reemplazado.

Para buscar puntos de acceso sin restricciones en un sistema de archivos:

```
aws efs describe-access-points --file-system-id <fs-id> \

  --query 'AccessPoints[?RootDirectory.Path==`/` ||
PosixUser==`null`].AccessPointId'
```

Nunca publique un identificador de subruta que apunte a su StorageClass `basePath`. Ese directorio es el padre de cada directorio creado por **Crear nuevo**, incluidos los datos huérfanos de los puntos de montaje eliminados.

Restablecer un volumen liberado

Un volumen que usted crea es de un solo uso por ciclo de vinculación. Eliminar un punto de montaje solo elimina la reclamación. Debido a `Retain`, Kubernetes mueve el volumen a la fase `Released` y mantiene un `claimRef` obsoleto que impide la revinculación. El selector aún lo muestra, en un grupo separado no seleccionable marcado como que necesita un restablecimiento.

Confirme la fase primero, luego realice una ejecución de prueba del parche contra el servidor API y luego aplíquelo:

```
kubectl get pv <pv-name> -o jsonpath='{.status.phase}'     # must read:
Released
```

```
kubectl patch pv <pv-name> --type=json \

  -p='[{"op":"remove","path":"/spec/claimRef"}]' --dry-run=server

kubectl patch pv <pv-name> --type=json -p='[{"op":"remove","path":"/spec/
claimRef"}]'
```

Advertencia

Borrar `claimRef` devuelve el volumen al grupo con sus datos existentes intactos, y el siguiente proyecto que lo adjunte hereda esos datos. Restablezca solo los volúmenes que tenga la intención de devolver. El comando no tiene su propia comprobación de seguridad: si se ejecuta contra un volumen vinculado, elimina la vinculación de un punto de montaje activo. Confirme que la fase indique `Released` primero, y use la ejecución de prueba del lado del servidor para detectar un nombre de volumen mal escrito antes de que el parche en vivo cambie algo.

SecurSpaces no restablece el volumen por usted. Este flujo existe para operadores que no otorgan a SecurSpaces acceso de escritura a PersistentVolumes, por lo que SecurSpaces tiene acceso de solo lectura y nunca cambia un volumen de su propiedad.

Información relacionada

- Configurar SecurSpaces
- Límites y comportamiento de los puntos de montaje

Troubleshoot AWS Mount Points

Solución de problemas

SÍNTOMA	CAUSA PROBABLE	SOLUCIÓN
Existe una StorageClass, pero nunca aparece en la lista **Crear nuevo**.	Es una clase de AWS sin `mountOptions: [tls]` de nivel superior, o tiene el `provisioningMode` incorrecto.	Añada `tls` a la clase. Compruebe también `parameters.provisioningMode`: debe ser `efs-ap` para Amazon EFS o `s3files-ap` para Amazon

SÍNTOMA	CAUSA PROBABLE	SOLUCIÓN
		S3 Files. Una clase con cualquier otro valor no se reconoce en absoluto como clase de punto de montaje, por lo que añadir `tls` por sí solo no la recupera.
Error que cita la falta de TLS.	La StorageClass carece de `mountOptions: [tls]`.	Añada `tls` a la clase.
Un espacio de trabajo se bloquea al iniciarse, aunque el punto de montaje esté listo.	No hay destino de montaje en la zona de disponibilidad del espacio de trabajo, o el puerto 2049 está bloqueado.	Añada el destino de montaje o abra el puerto 2049. Si el sistema de archivos es de una sola zona, no se puede añadir ningún destino de montaje para una segunda zona de disponibilidad: recréelo como regional.
Un punto de montaje creado a partir de coordenadas escritas se prepara, y luego los espacios de trabajo se bloquean.	Un ID de sistema de archivos o punto de acceso incorrecto o inexistente. Las coordenadas no se validan con AWS.	verificar los IDs en AWS y vuelva a crear el punto de montaje.
"PV enlazable no encontrado".	El volumen está fuera del alcance del llamante, no es `Available`, o el nombre es incorrecto.	Corrija la etiqueta de alcance, o borre `claimRef`.
Adjuntar existente es rechazado con "El volumen seleccionado no se puede montar".	El volumen lista `ReadOnlyMany` primero en `spec.accessModes`. Solo la primera entrada llega al controlador de almacenamiento de AWS, que no la acepta, por lo que ningún espacio de trabajo pudo montar el volumen.	Solo un administrador puede solucionar esto. Ponga `ReadWriteMany` primero: `kubectl patch pv <pv-name> --type=merge -p '{"spec":{"accessModes":["ReadWriteMany"]}}'`. El volumen se cambia in situ y sus datos no se ven afectados. Si el volumen es reconciliado por GitOps o

SÍNTOMA	CAUSA PROBABLE	SOLUCIÓN
		protegido por un webhook de admisión, cámbielo en el origen en su lugar, o la próxima sincronización revertirá el parche.
Adjuntar existente es rechazado con "El volumen seleccionado no permite este acceso".	Los `spec.accessModes` del volumen no incluyen el modo solicitado. Un punto de montaje de lectura/escritura necesita `ReadWriteMany`; uno de solo lectura necesita `ReadWriteMany` o `ReadOnlyMany`.	Solo un administrador puede solucionar esto. Añada el modo que falta con el mismo parche in situ, listando cada modo que el volumen debería soportar. Los datos no se ven afectados.
Cada **Adjuntar existente** desde coordenadas escritas es rechazado con "Clase de almacenamiento no válida para el punto de montaje", aunque ese flujo no tiene una clase de almacenamiento para elegir. Los volúmenes que creó con un identificador de sistema de archivos básico también desaparecen del selector.	Una StorageClass de punto de montaje en el clúster tiene un `fileSystemId` vacío. SecurSpaces ya no puede saber qué sistemas de archivos comparte, por lo que se niega en lugar de adivinar.	Establezca `parameters.fileSystemId` en cada StorageClass de punto de montaje.
El diálogo de creación falta por completo.	El proveedor no es AWS, las StorageClasses están mezcladas, el interruptor de almacenamiento está apagado, o el rol del usuario no puede gestionar los puntos de montaje.	Compruebe la página de configuración.
La página de configuración no informa de ninguna clase de almacenamiento elegible.	No existe ninguna Mount Point StorageClass en el clúster, o las clases de AWS existentes tienen un `parameters.provisioning`	Cree una. Si ya existe una clase, establezca `parameters.provisioningMode` en `efs-ap` o

SÍNTOMA	CAUSA PROBABLE	SOLUCIÓN
	`Mode` que falta o es incorrecto, lo que impide que se consideren elegibles.	`s3files-ap` en lugar de crear una segunda clase.

Nota

Listo significa que el volumen está enlazado. No significa que el volumen ha sido montado. Las coordenadas introducidas nunca se comprueban con AWS, por lo que un ID de sistema de archivos incorrecto produce un punto de montaje que informa de estar listo y falla solo cuando se inicia un espacio de trabajo.

El aprovisionamiento está sujeto a dos tiempos de espera fijos que no se pueden cambiar: tres minutos para que el volumen se enlace, y cinco minutos para la llamada de aprovisionamiento general. Exceder cualquiera de ellos mueve el punto de montaje a un estado de error, desde el cual puede ser eliminado y recreado.

Un punto de montaje que queda a mitad de operación por un reinicio del plano de control se recupera sin necesidad de trabajo fuera de banda. Espere hasta que hayan transcurrido más de cinco minutos, luego elimínelo normalmente.

Advertencia

No elimine la reclamación, el volumen o el punto de acceso de AWS manualmente primero. Para un punto de montaje de **Crear nuevo** que destruye datos que la eliminación normal habría recuperado en el orden correcto.

Los errores mostrados a los usuarios están saneados, pero la fila no está en blanco. Un punto de montaje en error lleva una breve razón, mostrada contra su estado en la columna **Estado** de la página **Recursos > Puntos de montaje**: pase el ratón o enfoque el icono de información para leerla. Empiece por ahí. El texto sin procesar de AWS y Kubernetes detrás de esto solo se encuentra en los registros del servicio central y del servicio del espacio de trabajo. Habilite `platform.isDeploymentDebugMode` solo en entornos de prueba.

La rotación de claves es rechazada en AWS con el mensaje de que la rotación de claves no es compatible con los puntos de montaje de AWS. Los puntos de montaje de AWS no tienen clave: el acceso se realiza a través de IAM y el punto de acceso. Los administradores que migran desde Azure no deben buscar un campo de clave.

Información relacionada

- Preparar los recursos de AWS
- Configurar SecurSpaces
- Límites y comportamiento de los puntos de montaje

Platform settings

Estas páginas cubren la configuración que se aplica a toda la plataforma.

PÁGINA	QUÉ CUBRE
General	Configure los ajustes generales de la plataforma.
Política del espacio de trabajo	Configuración de seguridad, red, programación, especificación y registro del espacio de trabajo, y cómo se heredan entre la plataforma, la organización y el proyecto.
Ciclo de vida del espacio de trabajo y detección de inactividad	Cómo la plataforma decide que un espacio de trabajo está inactivo antes de pausarlo, y cómo omitir la programación.
Regiones	Configure regiones y nodos cálidos para que los espacios de trabajo se ejecuten más cerca de sus usuarios.
Acciones personalizadas	Automatice el mantenimiento rutinario definiendo reglas que actúen sobre espacios de trabajo o usuarios según un horario.
Etiquetas de proyecto	Defina una taxonomía compartida a partir de un archivo CSV que todos apliquen al crear o editar un proyecto.

PÁGINA	QUÉ CUBRE
Correos electrónicos de incorporación	Los correos electrónicos automáticos que incorporan a nuevos usuarios a la plataforma, y cómo solucionar problemas con ellos.
Pasarela de correo electrónico	Configure la pasarela de correo electrónico, el contacto de violación de datos, la clave del servidor SSH y la configuración de plataforma relacionada.
Política de seguridad de la información	Publique la política de seguridad de su organización a los usuarios y establezca cuánto tiempo dura su aceptación.
Acuerdos de términos de servicio	Publique documentos que los usuarios deben aceptar antes de poder usar la plataforma, y restablezca las aceptaciones.

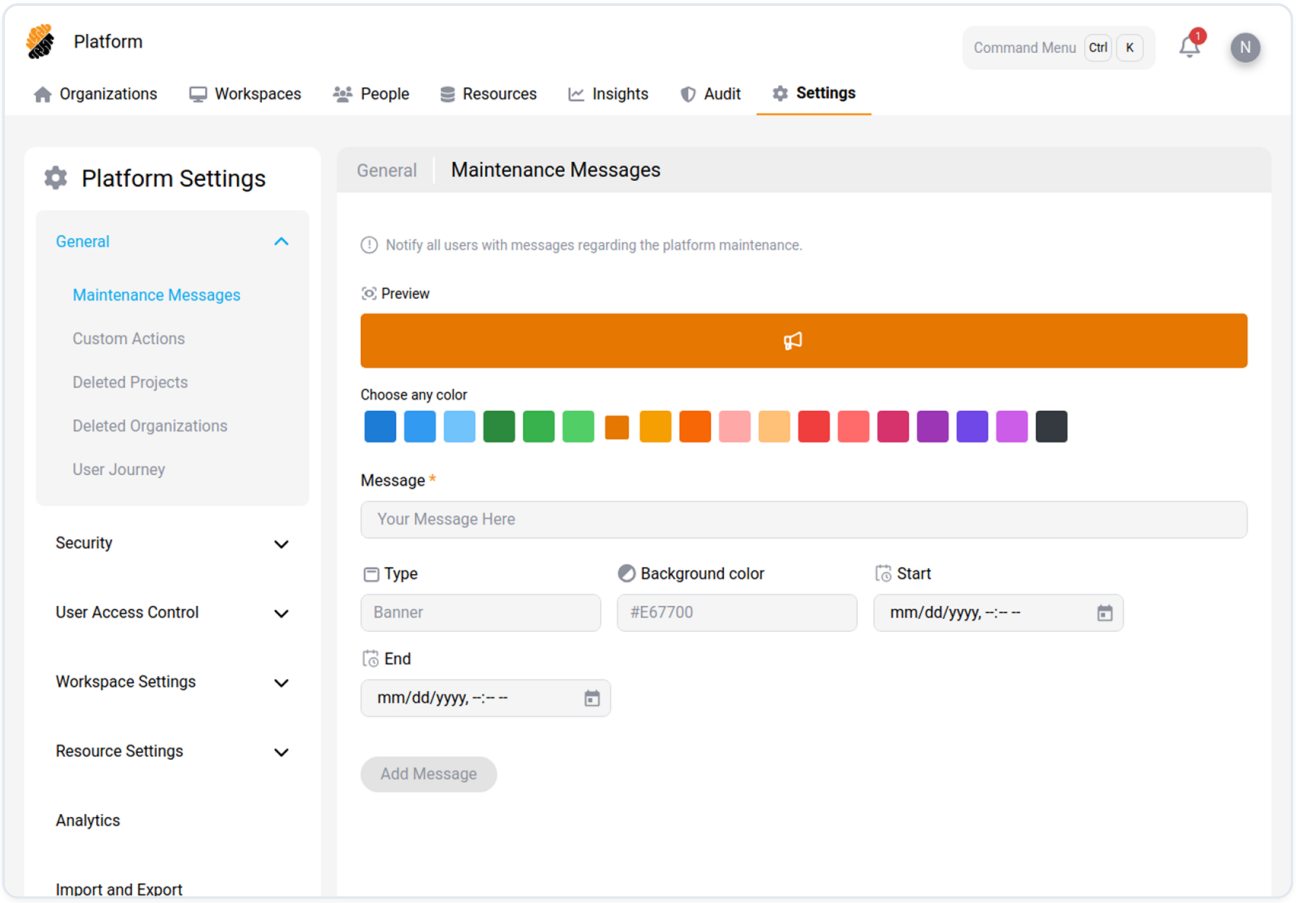
General settings

Esta sección cubre configuraciones fundamentales de toda la plataforma. Los administradores pueden gestionar **Mensajes de mantenimiento**, configurar **Acciones personalizadas**, recuperar **Proyectos eliminados** y **Organizaciones eliminadas**, establecer una **URL de documentación personalizada** y controlar las experiencias de **Incorporación y orientación**.

- Mensajes de mantenimiento
- Acciones personalizadas
- Proyectos eliminados
- Organizaciones eliminadas
- Documentación
- Mercado OpenVSX
- Incorporación y orientación

Mensajes de mantenimiento

Puede configurar y mostrar mensajes de mantenimiento a los usuarios. Estos mensajes pueden informar a los usuarios sobre tiempos de inactividad programados, mantenimiento en curso u otras notificaciones importantes de toda la plataforma.



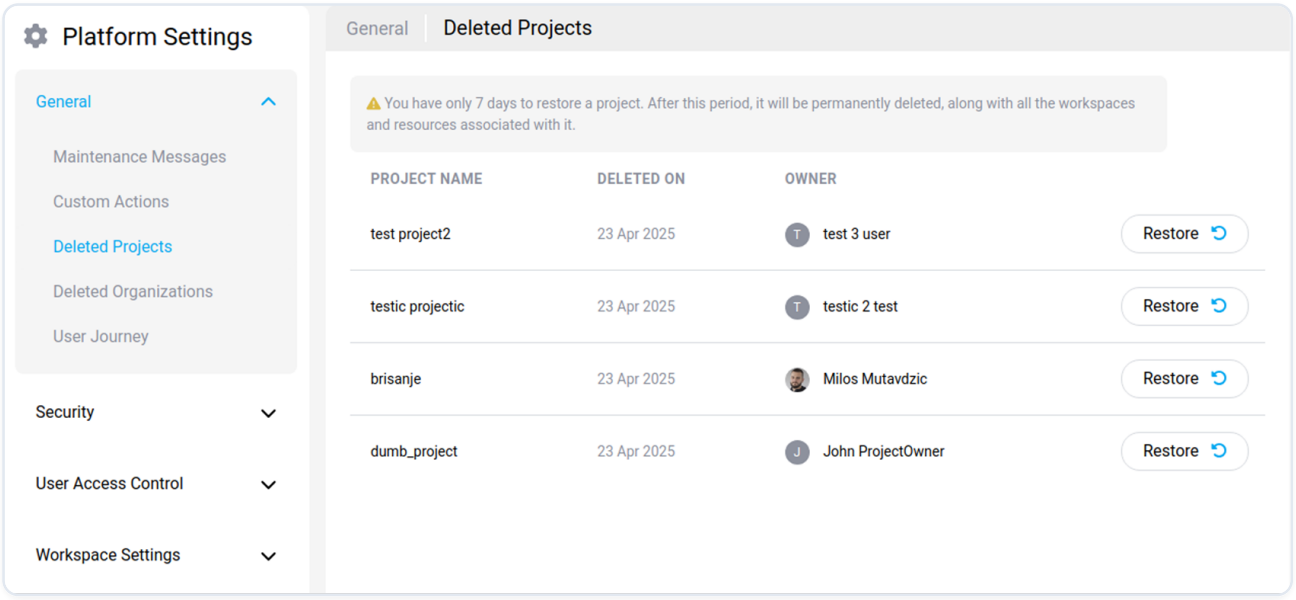
Acciones personalizadas

Configure acciones personalizadas que automaticen el mantenimiento rutinario, como la eliminación de espacios de trabajo que han estado inactivos durante mucho tiempo. Cada acción combina lo que se ejecuta, las condiciones que deciden a qué espacios de trabajo o usuarios se aplica y cuándo se ejecuta.

Para conocer las acciones, condiciones y opciones de programación disponibles —incluido cuándo usar **Cuando se cumpla la condición**—, consulte Acciones personalizadas.

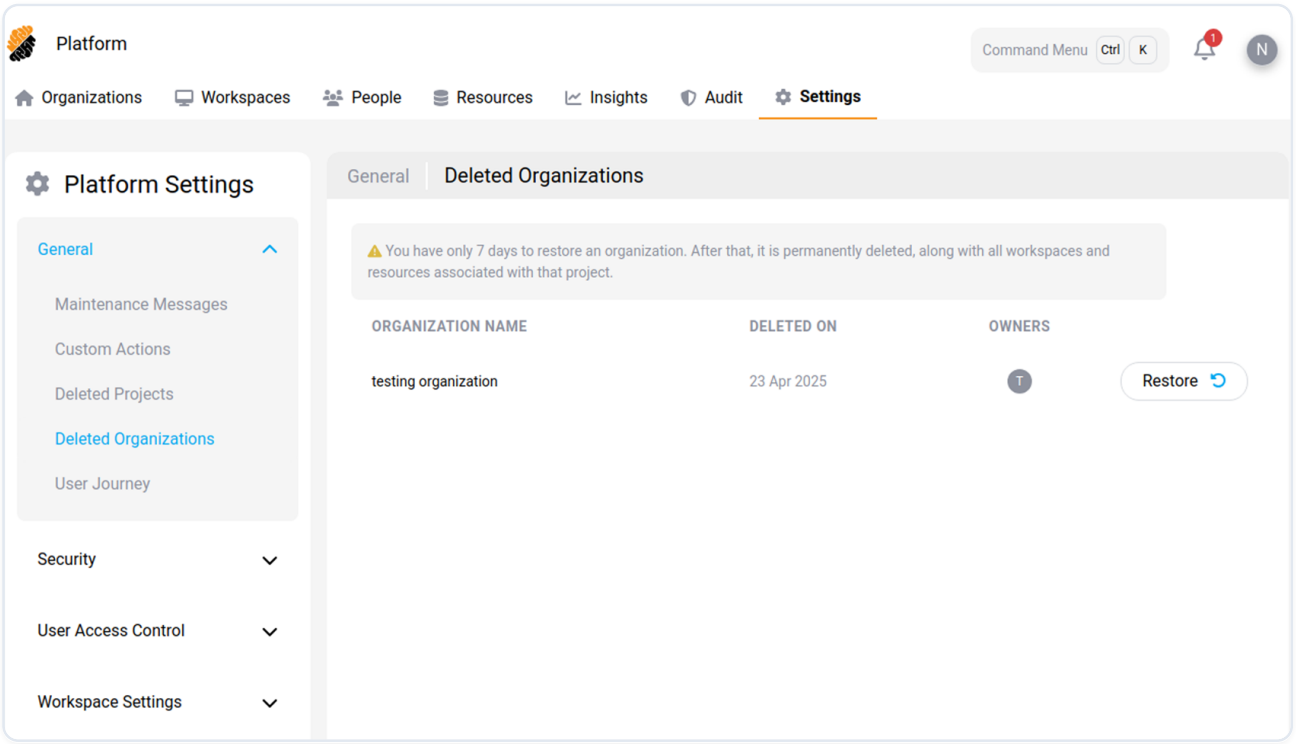
Proyectos eliminados

Puede recuperar un proyecto eliminado durante un período de 7 días en la pestaña **Proyectos eliminados**. Pulse el botón **Recuperar** a la derecha del proyecto que desea restaurar.



Organizaciones eliminadas

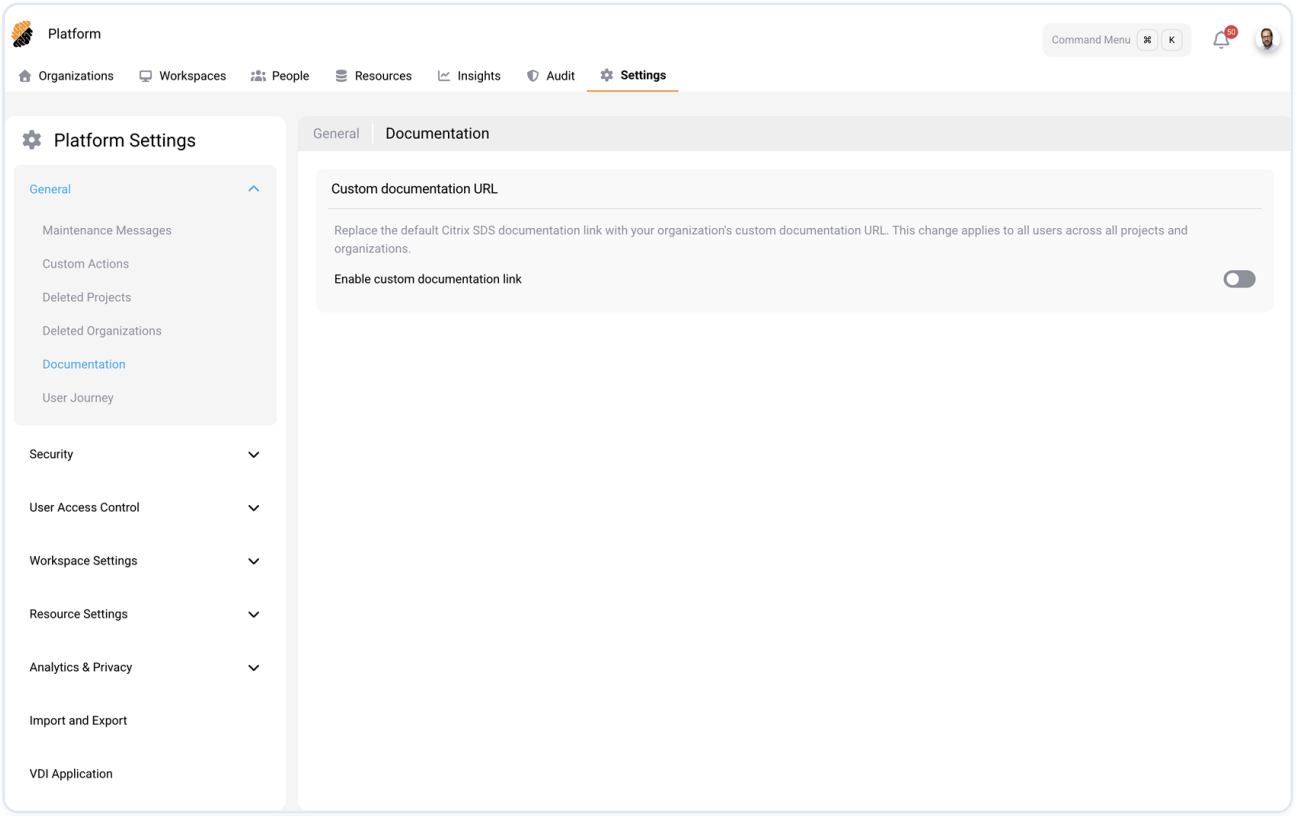
Puede recuperar una organización eliminada durante un período de 7 días en la pestaña **Organizaciones eliminadas**. Pulse el botón **Recuperar** a la derecha de la organización que desea restaurar.



Documentación

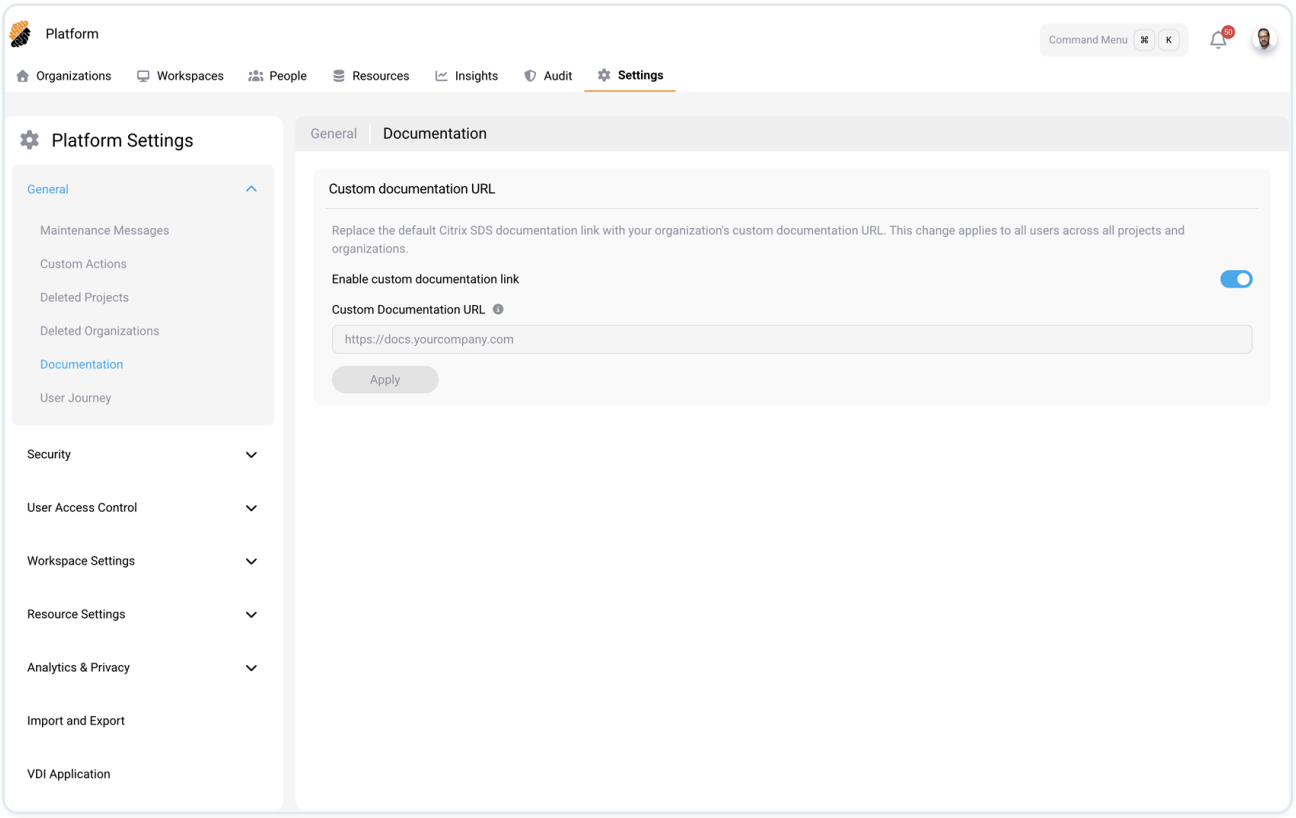
De forma predeterminada, la plataforma enlaza con la documentación estándar de Citrix SecurSpaces™. Puede reemplazar este enlace con una URL de documentación personalizada que apunte al sitio de documentación de su propia organización.

Cuando está habilitado, este cambio se aplica a todos los usuarios en todos los proyectos y organizaciones. Cuando desactiva la configuración, el enlace vuelve a la documentación predeterminada de Citrix SecurSpaces.



Para establecer una URL de documentación personalizada:

1. Vaya a **Configuración > General > Documentación**.
2. Active **Habilitar enlace de documentación personalizado**.
3. En el campo **URL de documentación personalizada**, introduzca la dirección web completa de su sitio de documentación, incluido `https://`.
4. Haga clic en **Aplicar**.

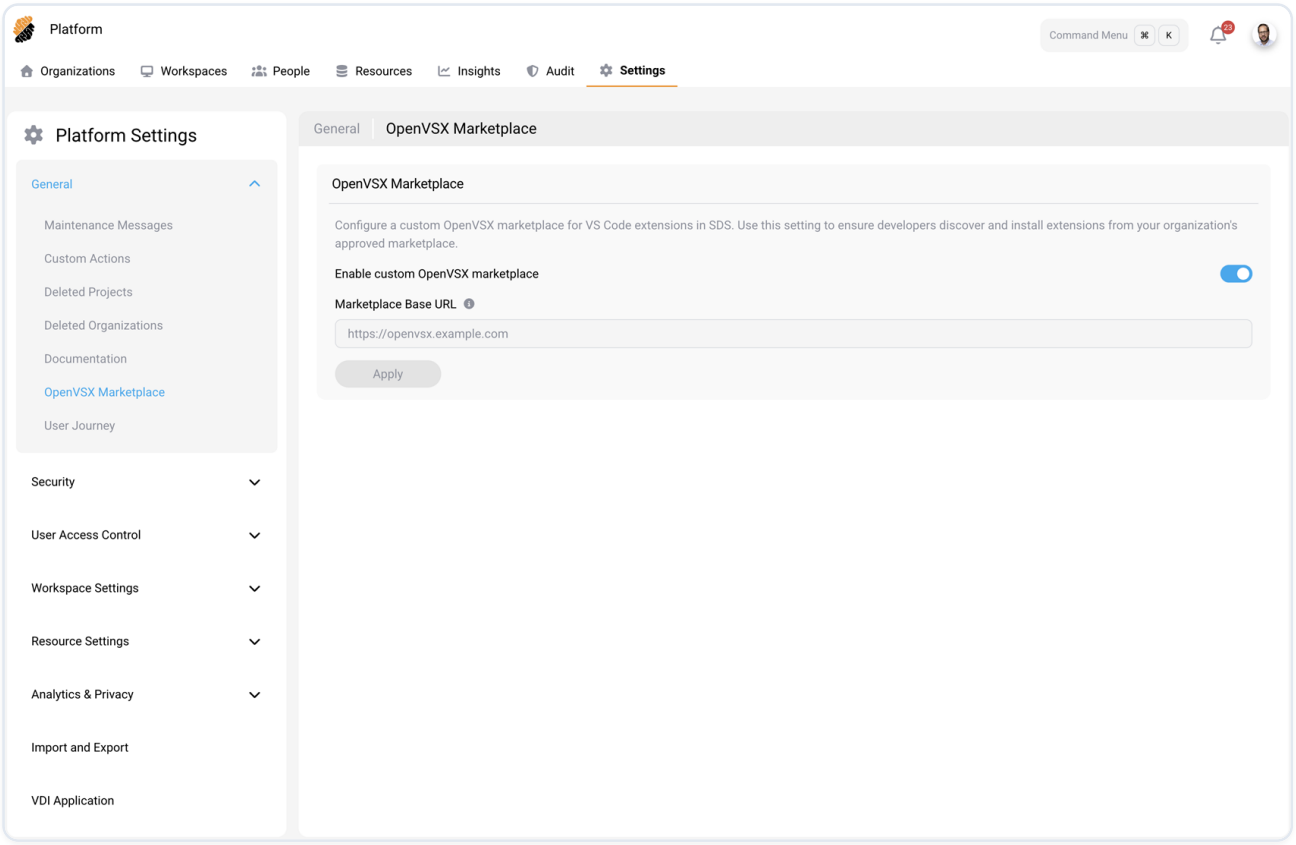


Para volver a la documentación predeterminada de SecurSpaces, desactive **Habilitar enlace de documentación personalizado**.

Mercado de OpenVSX

De forma predeterminada, los espacios de trabajo de VS Code en SecurSpaces utilizan el mercado público de Open VSX para el descubrimiento e instalación de extensiones. Puede anular esto con una URL de mercado de OpenVSX personalizada para que los desarrolladores solo descubran e instalen extensiones del mercado aprobado de su organización.

Esta configuración se establece a nivel de plataforma y es heredada por todas las organizaciones, proyectos y espacios de trabajo. Cuando está habilitada, los nuevos espacios de trabajo utilizan el mercado configurado inmediatamente. Los espacios de trabajo existentes utilizan el nuevo mercado después de su próximo reinicio.



Para configurar un mercado de OpenVSX personalizado:

1. Vaya a **Configuración > General > Mercado de OpenVSX**.
2. Active **Habilitar mercado de OpenVSX personalizado**.
3. En el campo **URL base del mercado**, introduzca la URL base de su servicio interno de OpenVSX, incluyendo `https://`.
4. Haga clic en **Aplicar**.

Para volver al mercado público predeterminado, desactive **Habilitar mercado de OpenVSX personalizado**.

> **Nota:**
>
> Los cambios surten efecto inmediatamente para los nuevos espacios de trabajo. Los espacios de trabajo existentes continúan utilizando su configuración de mercado actual hasta que se reinician.

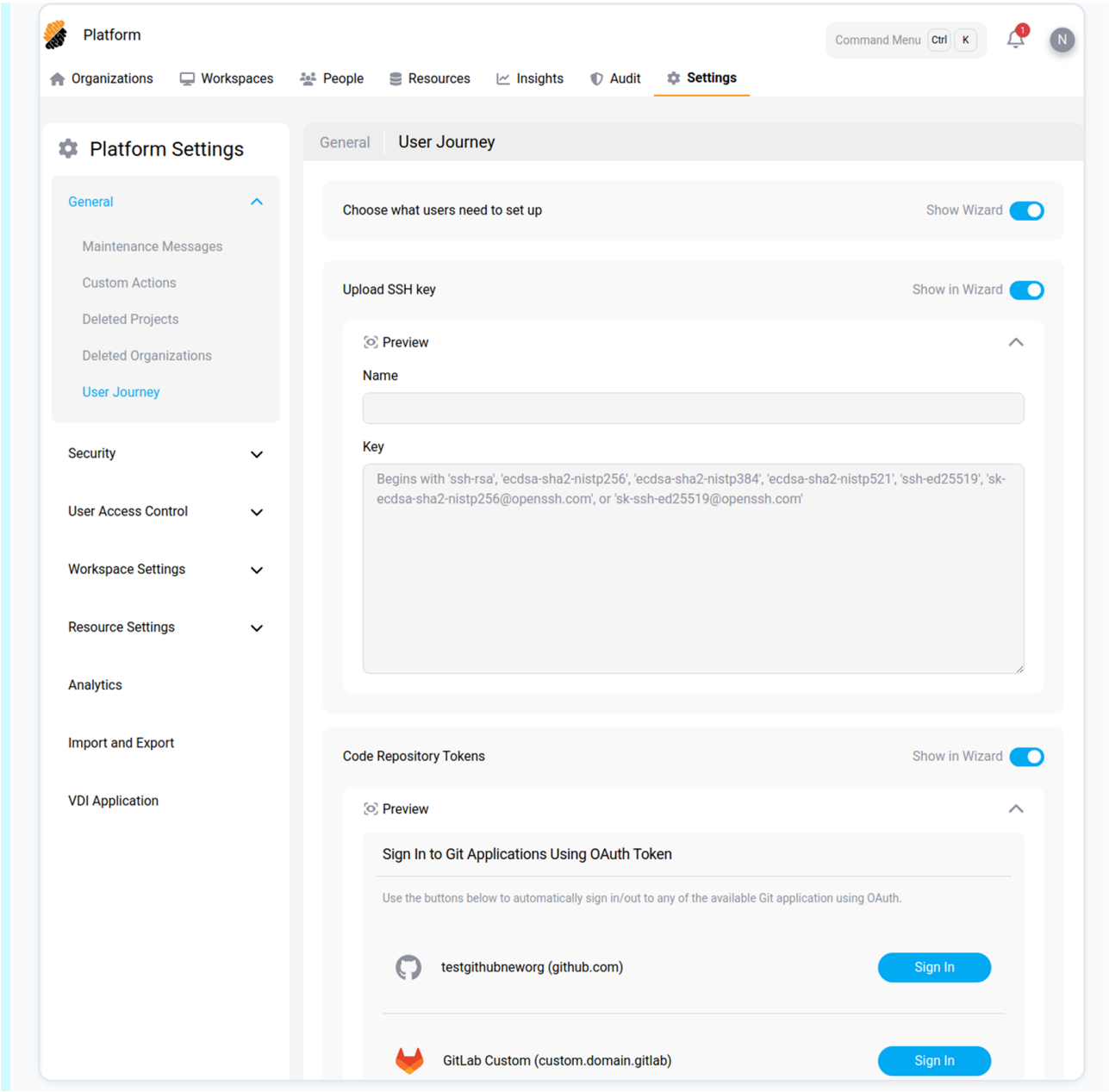
Incorporación y orientación

Esta sección controla las experiencias de incorporación que se muestran a los nuevos usuarios y propietarios de proyectos. Se pueden activar de forma independiente tres:

CONFIGURACIÓN	LO QUE MUESTRA
Lista de verificación de incorporación de usuarios	Una lista de verificación en la página de resumen del desarrollador
Lista de verificación de andamiaje de proyectos	Una lista de verificación en la página de resumen del propietario del proyecto
Recorrido clásico del usuario	El asistente de bienvenida heredado que se muestra al iniciar sesión, centrado en la configuración de seguridad del perfil

Nota:

Active solo las experiencias que sus usuarios necesitan. Varios flujos superpuestos a la vez pueden abrumar a un nuevo usuario y diluir el valor de cada uno.



Listas de verificación de incorporación

Las dos listas de verificación ofrecen a los propietarios de proyectos y a los desarrolladores los siguientes pasos guiados desde las páginas del proyecto. Cada una aparece como un panel lateral plegable y mantiene el progreso a medida que los usuarios avanzan por el producto.

La **Lista de verificación de andamiaje de proyectos** guía al propietario de un proyecto para que:

- Revise las imágenes de contenedor.
- Añadir repositorios de código.
- Configurar secretos.
- Crear plantillas de espacio de trabajo.
- Añadir usuarios.

La **lista de verificación de incorporación de usuarios** guía a un desarrollador para:

- Revisar su perfil.
- Configurar integraciones.
- Personalizar su configuración.
- Configurar credenciales de seguridad.
- Crear un espacio de trabajo.

Para configurar la disponibilidad de la lista de verificación:

1. Vaya a **Configuración > General > Incorporación y orientación**.
2. Active o desactive la **lista de verificación de andamiaje de proyectos**.
3. Active o desactive la **lista de verificación de incorporación de usuarios**.
4. Seleccione **Aplicar**.

Resultado esperado: La configuración de la lista de verificación seleccionada se aplica a las páginas del proyecto. Los usuarios conservan el progreso guardado de su lista de verificación a menos que la función esté deshabilitada.

Workspace policy

La política de espacios de trabajo rige los espacios de trabajo creados en la plataforma: qué pueden copiar, cuántos puede tener un usuario, si se puede acceder a ellos a través de SSH y qué tráfico de red pueden generar.

Las mismas configuraciones aparecen en tres ámbitos — **plataforma**, **organización** y **proyecto** — y se resuelven del más amplio al más específico. Esta página cubre los tres.

Dónde se puede configurar cada ajuste

AJUSTE	PLATAFORMA	ORGANIZACIÓN	PROYECTO
Seguridad del portapapeles	sí	sí	sí
Límites de proyecto predeterminados	sí	sí	sí
Desarrollo remoto a través de SSH	—	sí	sí

AJUSTE	PLATAFORMA	ORGANIZACIÓN	PROYECTO
Política de red	sí	sí	sí
Acceso SSH a espacios de trabajo	sí	—	—
Configuración de programación	sí	—	—
Configuración de aplicaciones del espacio de trabajo	sí	—	—
Especificación del espacio de trabajo	sí	—	—
Acceso al registro	sí	—	—
Espacios de trabajo eliminados	sí	—	—

La configuración de la plataforma se encuentra en **Configuración del sistema**. La configuración de la organización y del proyecto se encuentra en la página de configuración de esa organización o proyecto.

Cómo se resuelven las configuraciones

Las configuraciones se leen en orden —valores predeterminados, luego plataforma, luego organización, luego proyecto—, pero se aplican dos reglas diferentes, y la diferencia importa.

La mayoría de las configuraciones: el ámbito más restrictivo prevalece, a menos que se aplique

La seguridad del portapapeles, los límites predeterminados del proyecto y la política de red siguen esta regla. Si un proyecto establece un valor, este anula a la organización, que a su vez anula a la plataforma.

Un ámbito también puede **aplicar** su valor. La aplicación detiene la cadena: la configuración se bloquea en ese ámbito y ningún ámbito más restrictivo puede cambiarla. El control de aplicación aparece en el ámbito de la plataforma y la organización, ya que el proyecto es el nivel más restrictivo.

Desarrollo remoto a través de SSH: cada ámbito debe permitirlo

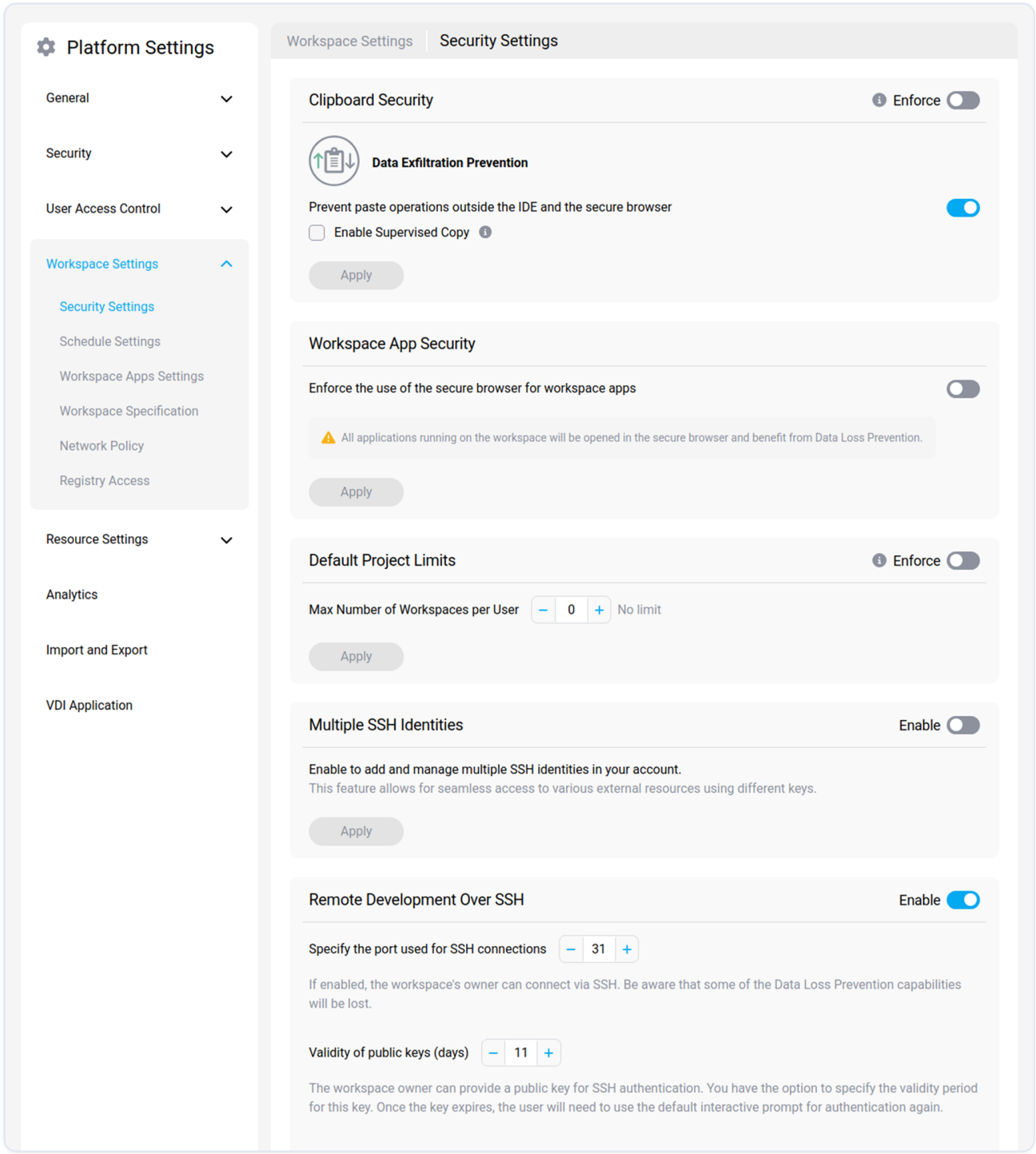
SSH no funciona de esa manera. Solo se permite cuando **todos** los ámbitos superiores lo permiten, y cualquier ámbito que lo deniegue lo desactiva para todo lo que esté por debajo. Este es el comportamiento predeterminado, no una configuración de aplicación.

Por lo tanto, el propietario de un proyecto no puede habilitar SSH si la plataforma lo tiene desactivado. El control está oculto en lugar de mostrarse como deshabilitado, así que si no lo encuentra, compruebe el ámbito superior.

Configuración de seguridad

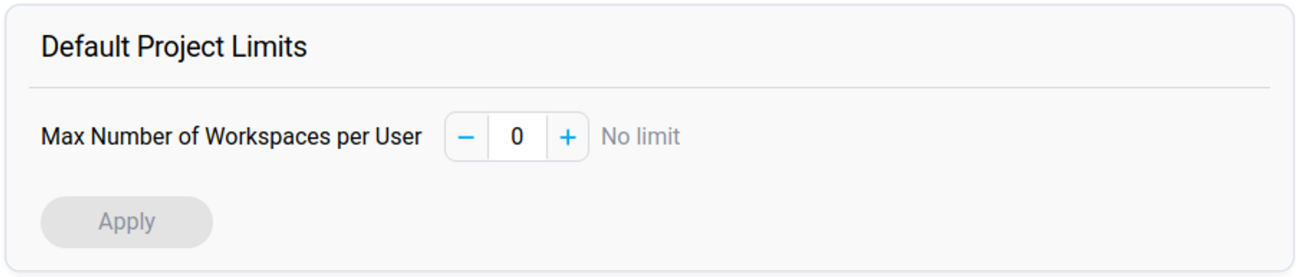
Seguridad del portapapeles

Evita que los usuarios peguen contenido del IDE y del navegador seguro en otras aplicaciones, como medida de prevención de pérdida de datos. Puede restringir la copia, restringir el pegado, limitar el número de caracteres y habilitar la copia supervisada.



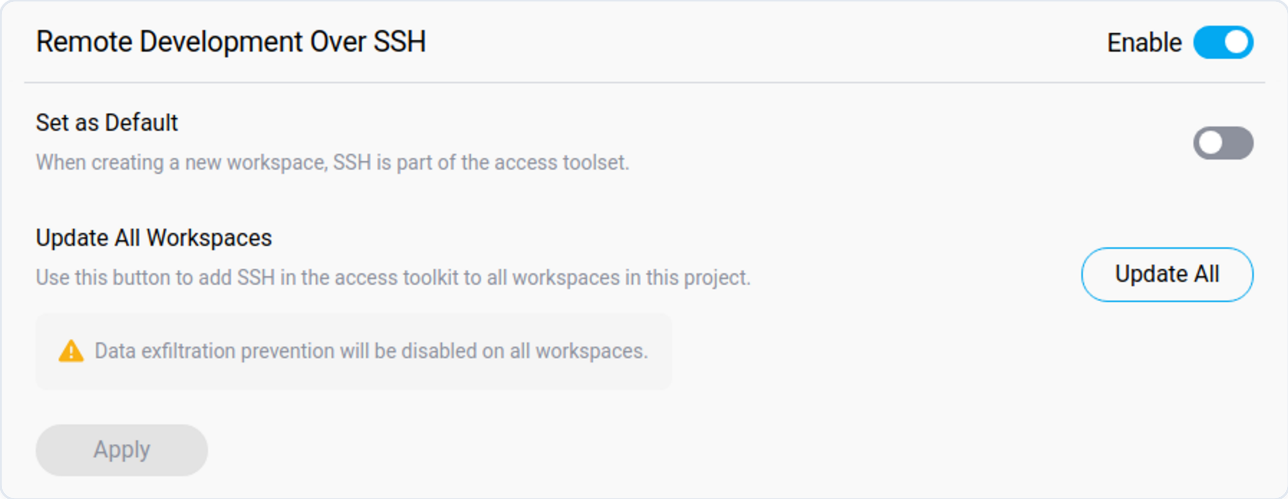
Límites predeterminados del proyecto

Limita el número de espacios de trabajo que un usuario puede crear, lo que restringe la proliferación de recursos y los costes. Un límite de cero significa que no hay límite.



Desarrollo remoto a través de SSH

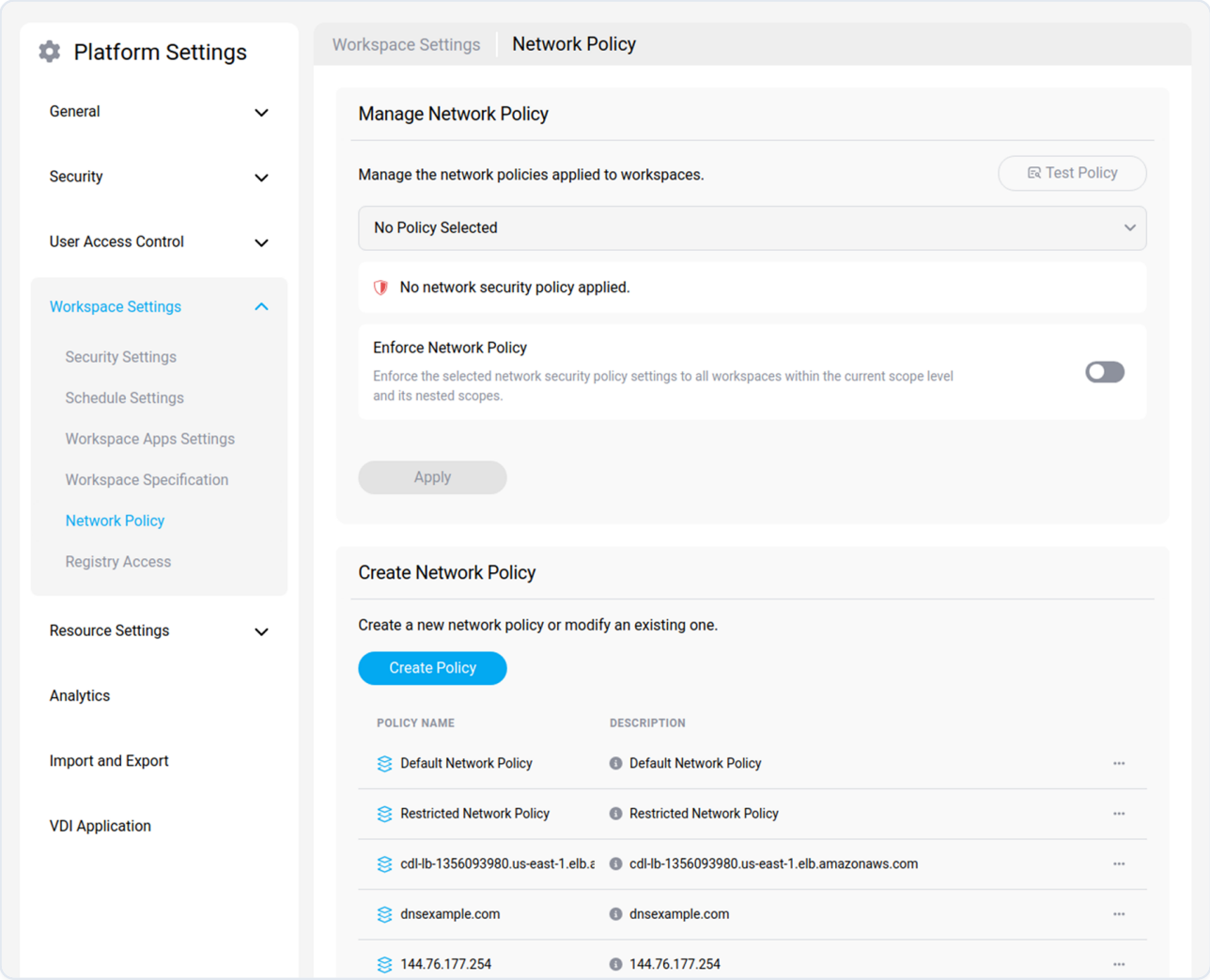
Permite a los desarrolladores conectarse a sus espacios de trabajo desde un IDE local a través de SSH. Es conveniente, pero reduce la eficacia de la prevención local de pérdida de datos, por lo que debe habilitarse deliberadamente.



Para saber qué hacen los desarrolladores una vez habilitado, consulte Conectarse a través de SSH.

Política de red

Las políticas de red controlan el tráfico saliente que un espacio de trabajo puede generar, coincidiendo con el dominio y la dirección IP. Una vez que se adjunta una política, el usuario del espacio de trabajo no puede eludirla.



Se crean tres políticas predeterminadas con cada proyecto:

POLÍTICA	COMPORTAMIENTO
Monitorizar tráfico (predeterminado)	Registra el tráfico TCP saliente y genera eventos de auditoría, sin restringirlo
Restringir tráfico (predeterminado, experto)	Bloquea el tráfico saliente excepto los recursos adjuntos y una lista de permitidos
Inspeccionar tráfico (predeterminado, experto)	Inspecciona el contenido TCP y lo informa al registro de auditoría

Las políticas de red tienen su propia sección, que cubre el modelo de políticas, la creación y asignación de políticas, los campos de modo experto y la resolución de problemas:

- Políticas de red
- Crear una política de red

- Asignar y aplicar una política

Configuración solo de plataforma

Estos existen solo en el ámbito de la plataforma.

Acceso SSH a espacios de trabajo

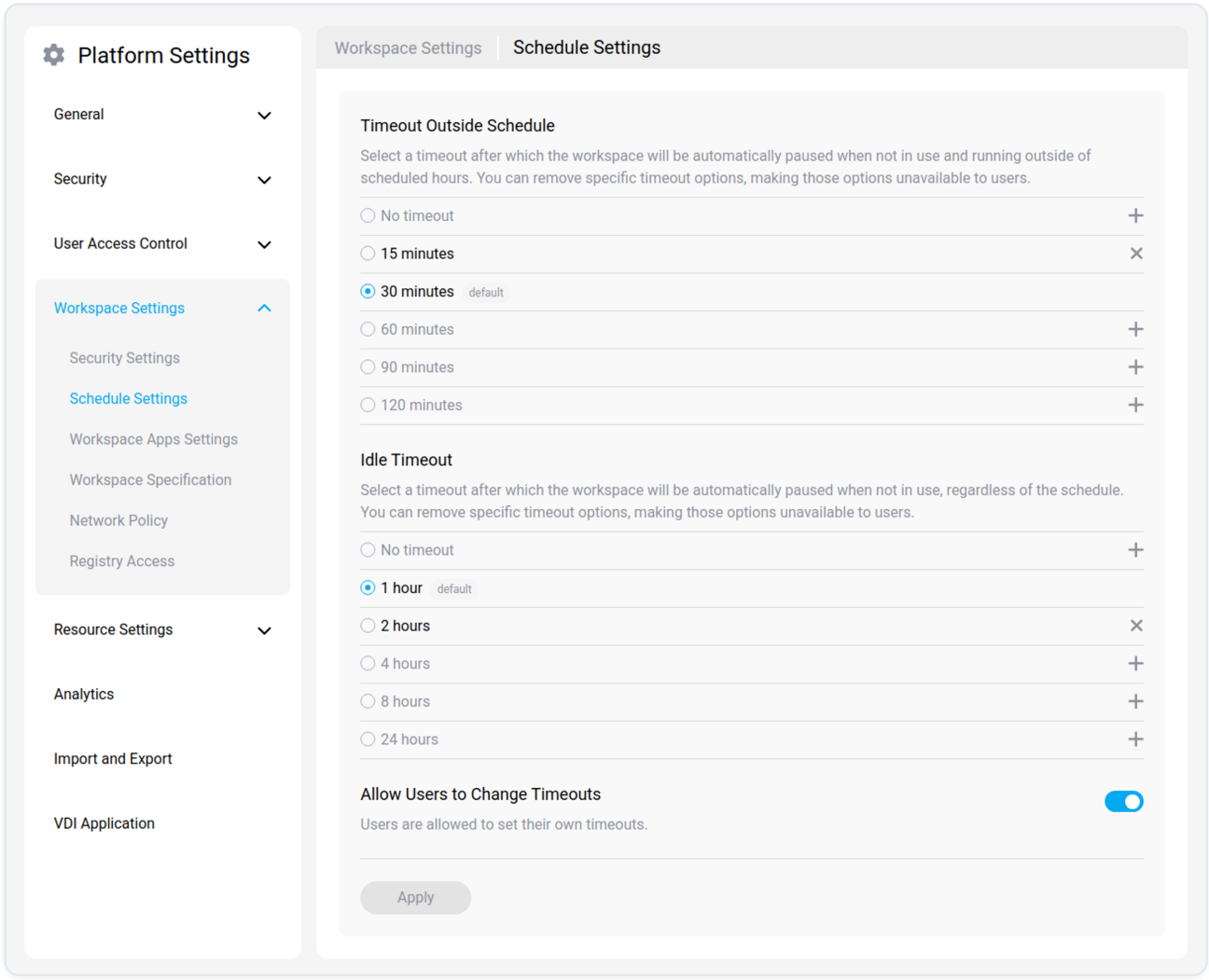
Habilita el acceso SSH para la implementación y establece la caducidad de la clave pública y el puerto. Dado que SSH sigue la regla restrictiva anterior, este interruptor controla cada organización y proyecto debajo de él.

La **validez de las claves públicas (días)** es **7** por defecto. Cuando una clave registrada alcanza esa edad, la plataforma deja de aceptarla. Las integraciones de IDE de SecurSpaces renuevan las claves automáticamente, por lo que los desarrolladores que las utilizan no se ven afectados; los desarrolladores que se conectan con cualquier otro cliente SSH deben volver a registrar su clave cada vez que caduca. Por lo tanto, establecer un período corto recae completamente en el segundo grupo. Consulte Caducidad y renovación de claves.

La configuración de la infraestructura es independiente; consulte Habilitar acceso SSH a espacios de trabajo.

Configuración de programación

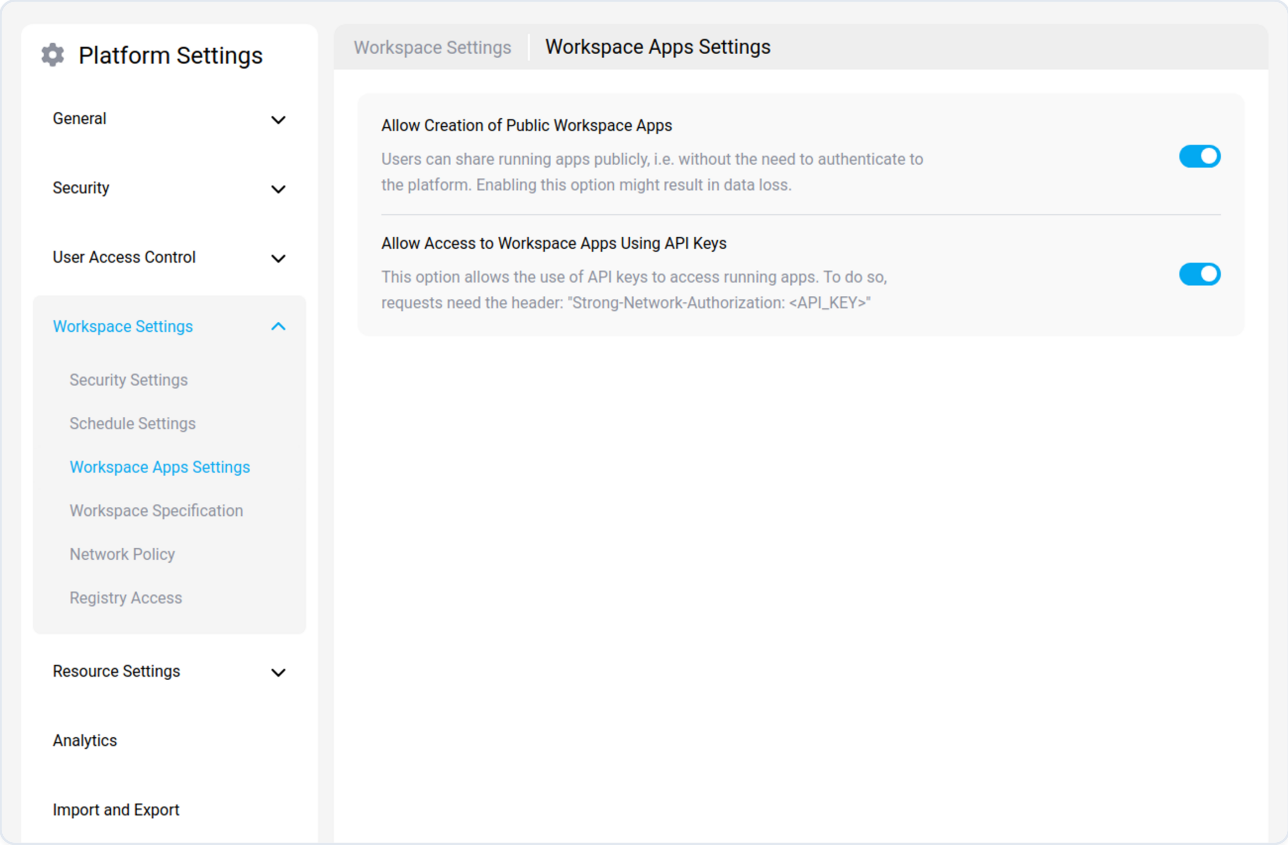
Establece las horas de funcionamiento y el apagado automático, para que los espacios de trabajo se ejecuten solo cuando sea necesario.



Configuración de aplicaciones de espacio de trabajo

Gobierna cómo se pueden compartir las aplicaciones del espacio de trabajo.

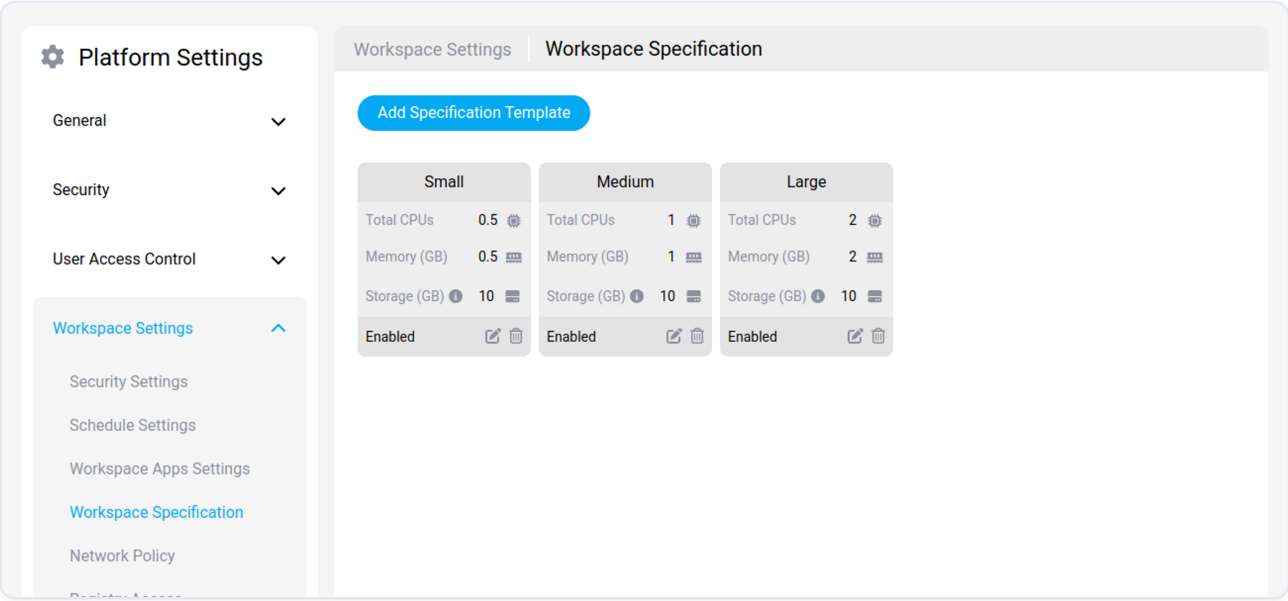
- **Permitir la creación de aplicaciones de espacio de trabajo públicas** — permite a los usuarios compartir una aplicación en ejecución sin autenticación de la plataforma. Esto puede provocar la pérdida de datos.
- **Permitir el acceso a aplicaciones de espacio de trabajo usando claves API** — permite a los usuarios acceder a una aplicación en ejecución con una clave API, enviada como el encabezado `Strong-Network-Authorization: <API_KEY>`.



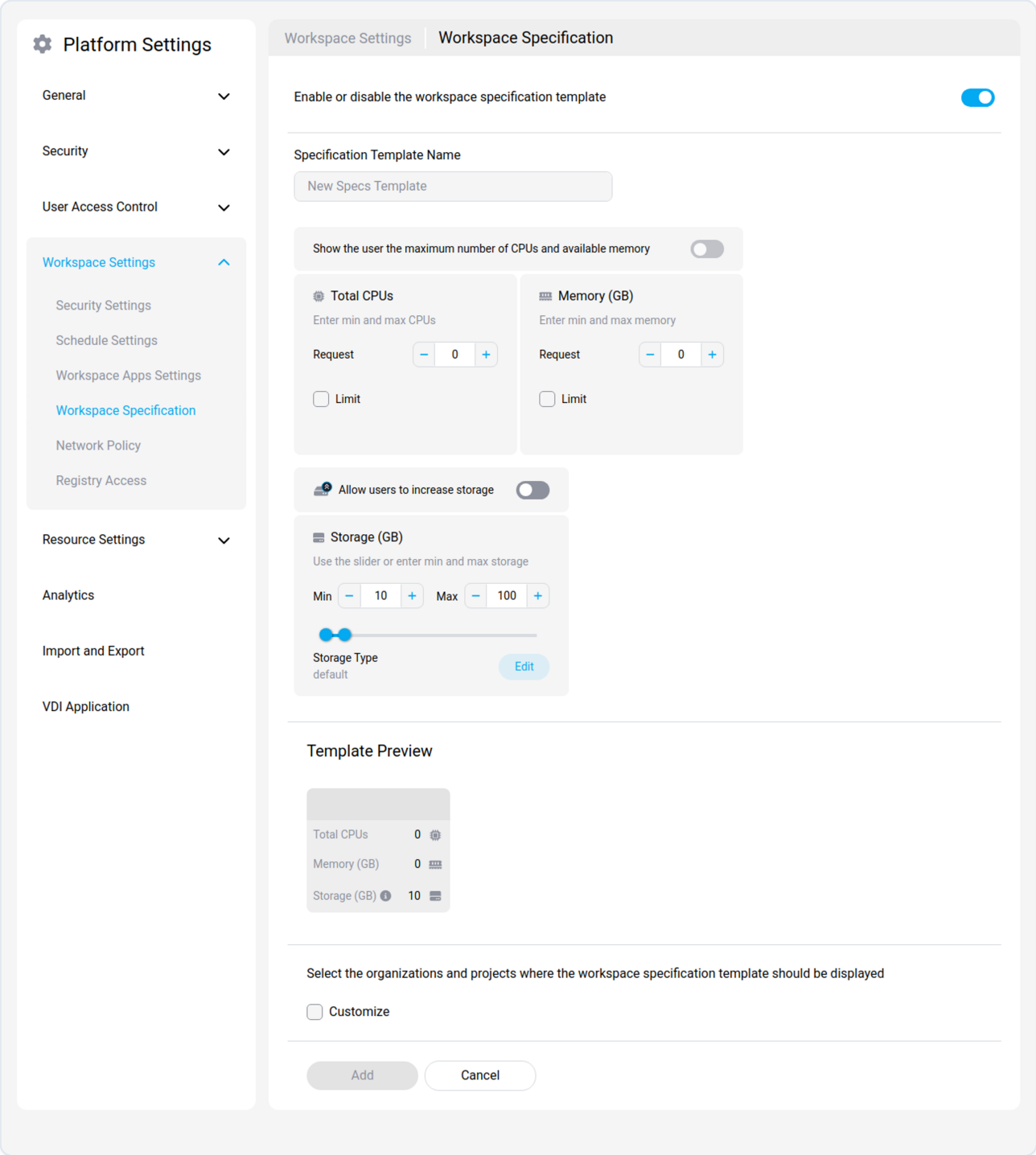
Para saber qué hacen los desarrolladores con esto, consulte Aplicaciones de espacio de trabajo.

Especificación del espacio de trabajo

Define las plantillas de recursos a partir de las cuales se puede crear un espacio de trabajo, con valores de solicitud y límite para CPU, RAM, y almacenamiento. Una plantilla puede restringirse a organizaciones o proyectos específicos, y los usuarios solo ven las plantillas que les corresponden.

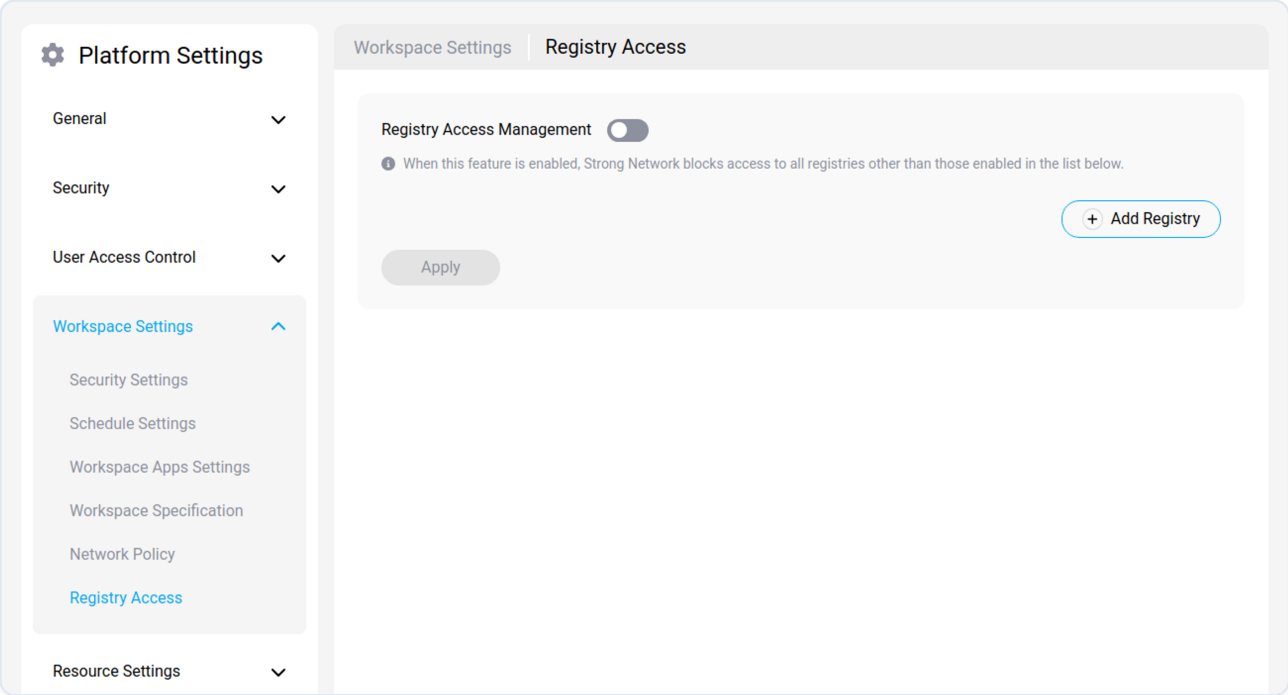


Al crear una plantilla, establezca los valores de solicitud iniciales y los valores límite máximos para CPU, RAM y almacenamiento.



Acceso al registro

Controla de qué registros de imágenes de contenedor pueden extraer los espacios de trabajo, de modo que solo se utilicen fuentes aprobadas.



Espacios de trabajo pendientes de eliminación

Eliminar un espacio de trabajo no lo destruye inmediatamente. Se mueve a una papelera de reciclaje, donde permanece recuperable hasta que transcurre un período de caducidad. **Espacios de trabajo pendientes de eliminación** enumera cada espacio de trabajo en toda la plataforma que se encuentra actualmente en ese estado, con su propietario, su organización y proyecto, y la fecha en que fue eliminado.

Desde la lista puede **Restaurar** un espacio de trabajo, **Eliminar** uno permanentemente o usar **Eliminar todos los espacios de trabajo** para vaciar la papelera.

Para configurar cuánto tiempo permanecen recuperables los espacios de trabajo eliminados:

1. Vaya a **Plataforma > Espacios de trabajo > Espacios de trabajo pendientes de eliminación**.
2. Establezca **Caducidad en días**, de **1 a 99**. El valor predeterminado es **7**.
3. Seleccione **Guardar**.

> **Importante:**

> El período de caducidad se aplica a los espacios de trabajo **que ya están en la papelera**, no solo a los eliminados posteriormente. La fecha límite para cada espacio de trabajo se recalcula a partir de la fecha en que fue eliminado cada vez que cambia la configuración. Acortar el período puede, por lo tanto, adelantar la eliminación de espacios de trabajo que ya

> están esperando, y puede purgar algunos de ellos en la próxima limpieza. Alargarlo les da más tiempo a todos.

> Los propietarios de espacios de trabajo ven sus propias eliminaciones pendientes y los correos electrónicos enviados al respecto en su página de perfil. Consulte Espacios de trabajo pendientes de eliminación.

PROYECTOS Y ORGANIZACIONES ELIMINADOS

Los proyectos y las organizaciones tienen sus propias papeleras de reciclaje, y **su retención está fijada en 7 días y no se puede configurar**. Cambiar **Caducidad en días** no les afecta.

ELEMENTO	RETENCIÓN	DÓNDE RESTAURARLO
Espacio de trabajo	1–99 días, 7 por defecto	Plataforma > Espacios de trabajo > Espacios de trabajo pendientes de eliminación
Proyecto	7 días, fijo	Plataforma u organización **Configuración > Proyectos eliminados**
Organización	7 días, fijo	Plataforma **Configuración > Organizaciones eliminadas**

Al eliminar un proyecto o una organización, también se eliminan los espacios de trabajo y los recursos que contiene, así que restaure el elemento principal primero si necesita algo de su interior. Consulte Configuración de proyectos y organizaciones.

Información relacionada

- Políticas de red
- Configuración de proyectos y organizaciones
- Roles y permisos
- Conectarse a través de SSH

Workspace lifecycle and idle detection

Citrix SecurSpaces™ 2026.4 introduce un motor híbrido de detección de inactividad que utiliza múltiples señales para determinar si un espacio de trabajo está realmente inactivo antes de

pausarlo. Esto reemplaza el enfoque anterior, en el que una conexión SSH abierta por sí sola era suficiente para mantener un espacio de trabajo en ejecución indefinidamente.

Cómo funciona

El motor de detección de inactividad utiliza un enfoque basado en prioridades con tres capas:

Señales de actividad del IDE (primarias)

Cuando la extensión del IDE de SecurSpaces está activa en el IDE del desarrollador, el sistema utiliza señales de entrada granulares, como la actividad del teclado y el ratón, para determinar si un usuario está presente. Una conexión SSH abierta pero sin usar ya no impide que un espacio de trabajo se pause.

Esto se aplica a los IDE que admiten la extensión de SecurSpaces, incluidos VS Code Desktop, Cursor, Windsurf y Kiro.

Respaldo SSH (secundario)

Para los desarrolladores que utilizan IDE que no admiten la extensión de SecurSpaces, el sistema recurre a la lógica anterior basada en SSH. Una conexión SSH activa sigue indicando que el espacio de trabajo está en uso, por lo que el trabajo activo no se interrumpe.

> **Nota**
>
> Iniciar un espacio de trabajo no es una señal de actividad. Un espacio de trabajo que se inicia y luego se deja solo se pausa normalmente una vez que se alcanza el tiempo de espera de inactividad. Sin embargo, iniciar un espacio de trabajo cuenta como uso para la condición de **Espacio de trabajo inactivo** que elimina automáticamente los espacios de trabajo no utilizados. Consulte Acciones personalizadas.

Omitir programación (anulación manual)

Los oficiales de seguridad y los administradores de la plataforma pueden desactivar la detección de inactividad para espacios de trabajo individuales. Cuando la opción Omitir programación está habilitada para un espacio de trabajo, el programador se omite y el espacio de trabajo sigue ejecutándose independientemente de la actividad del usuario detectada.

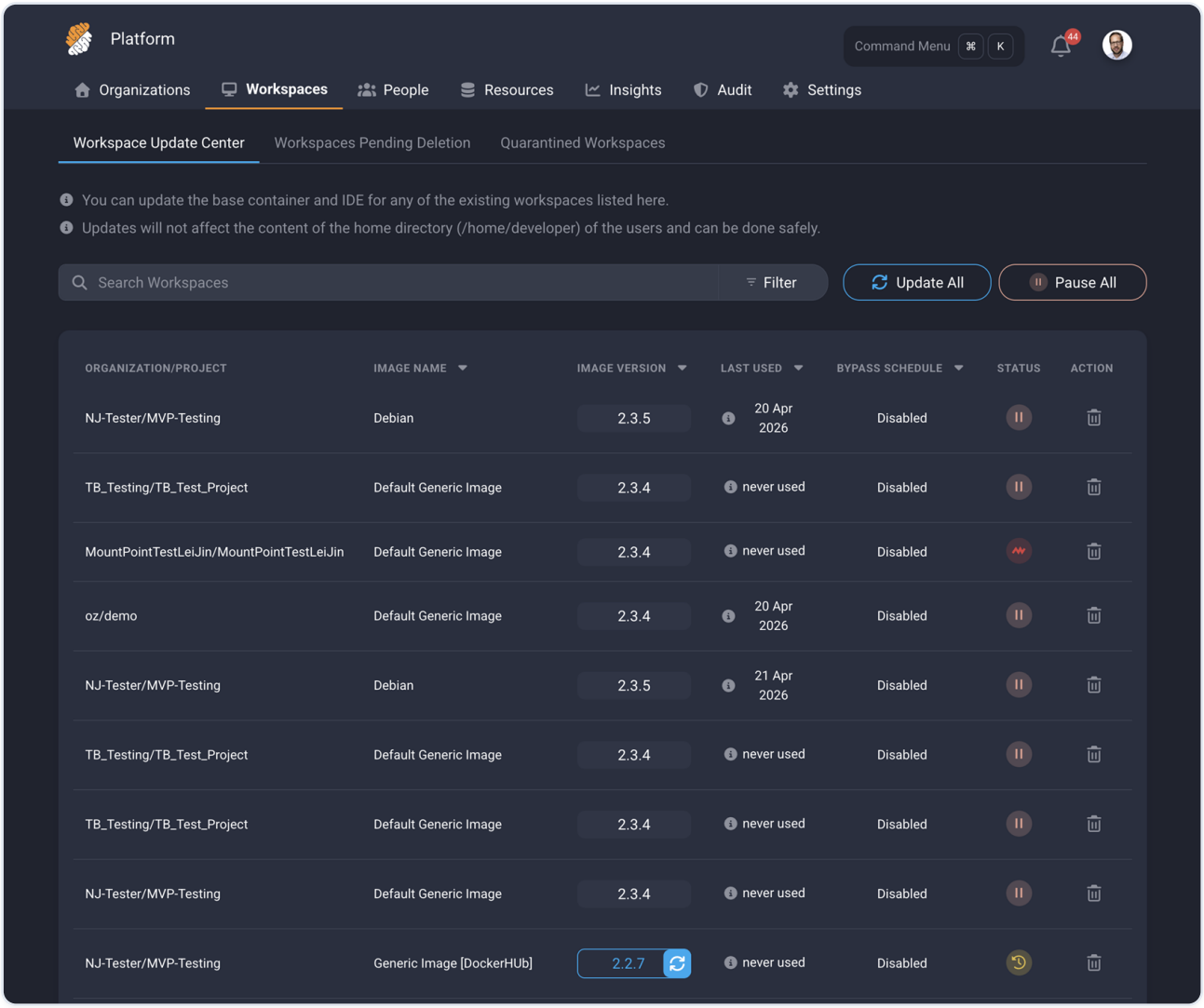
Esto está destinado a servicios de larga duración, como herramientas de desarrollo compartidas o componentes de infraestructura que deben permanecer disponibles de forma continua.

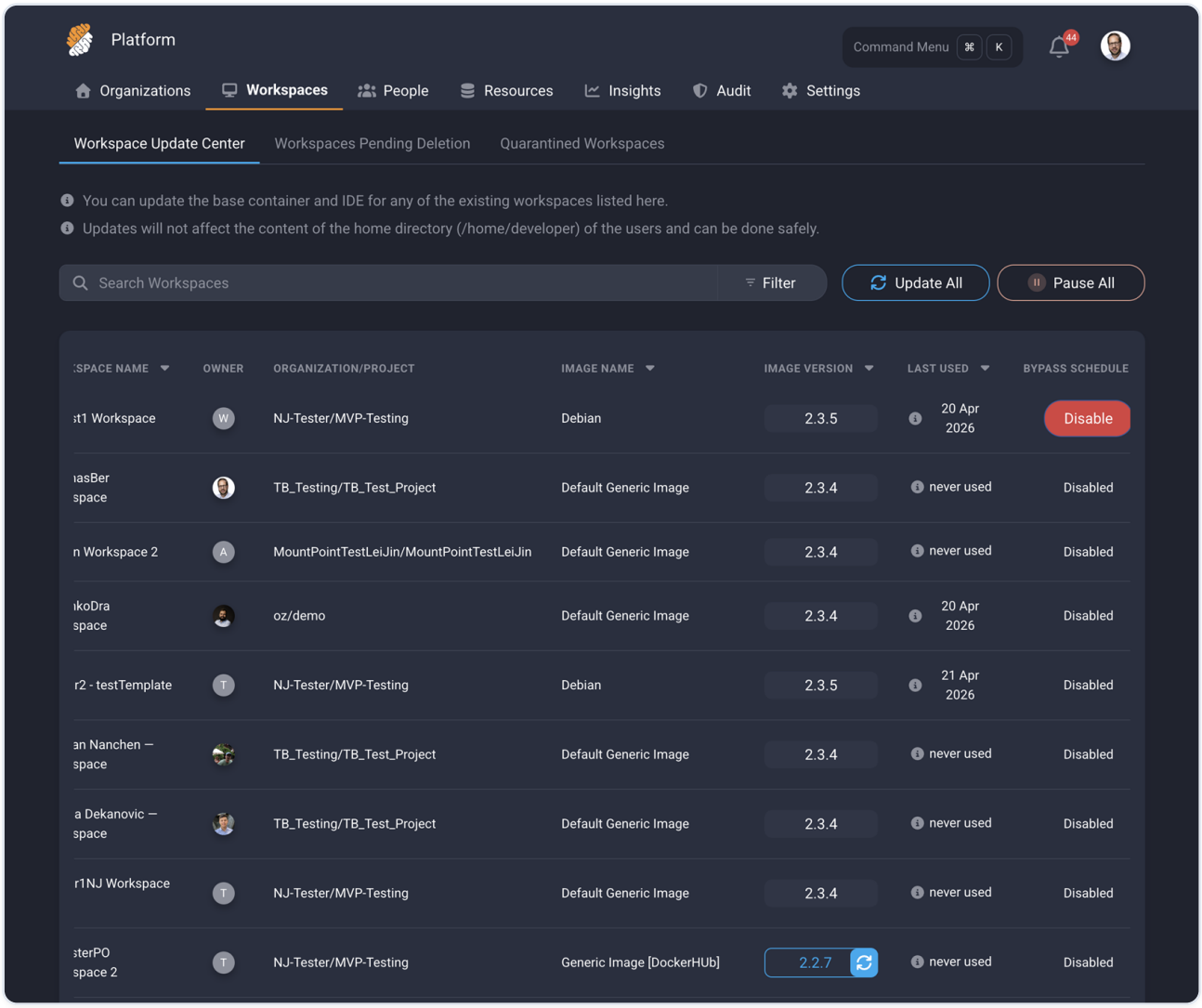
Omitir programación en el Centro de actualización de espacios de trabajo

La columna **Omitir programación** es visible en el **Centro de actualización de espacios de trabajo** a nivel de plataforma (Plataforma > Espacios de trabajo > Centro de actualización de espacios de trabajo). Cada fila de espacio de trabajo muestra uno de dos estados:

- **Deshabilitado** (predeterminado) — El espacio de trabajo sigue el programa normal de detección de inactividad. El espacio de trabajo se pausa automáticamente después del tiempo de espera configurado si no se detecta actividad.
- **Habilitado** — El espacio de trabajo omite el programa y sigue ejecutándose. Aparece un botón rojo de **Deshabilitar**, lo que permite a los administradores revertir.

Para habilitar Omitir programa para un espacio de trabajo, seleccione **Habilitar** en la columna Omitir programa para ese espacio de trabajo.





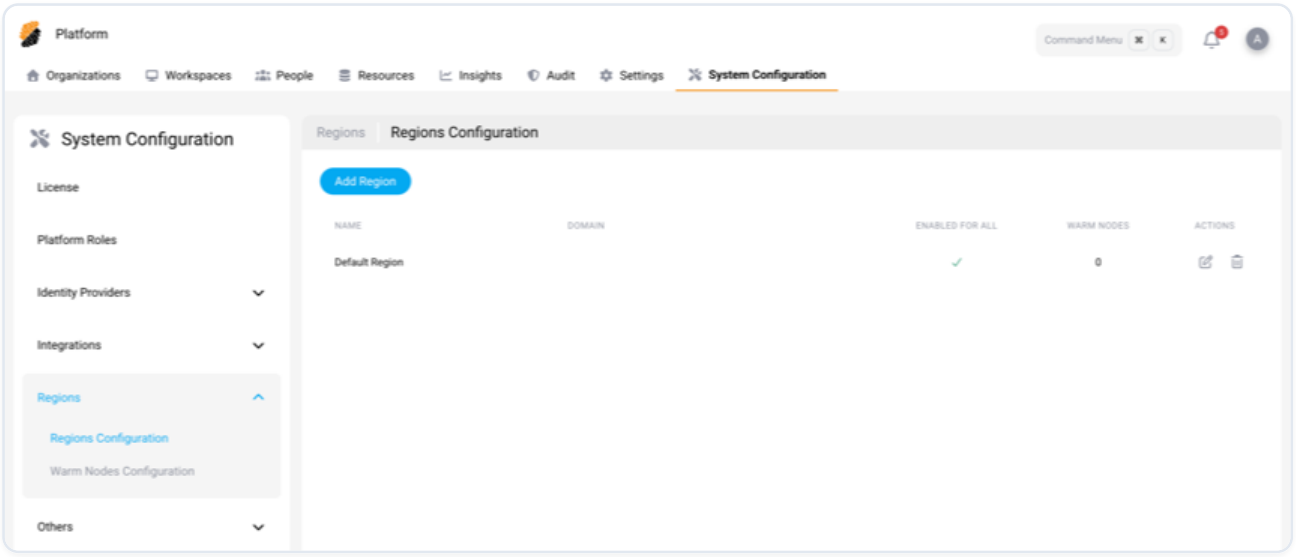
Permisos

Solo los **oficiales de seguridad** y los **administradores de plataforma** pueden activar o desactivar Omitir programa. Esta restricción existe porque omitir el programa afecta directamente los costos de infraestructura.

Regions

Ejecute espacios de trabajo más cerca de sus usuarios. En **Regiones**, configure las regiones y los nodos cálidos para una implementación multirregión de Citrix SecurSpaces™.

Encuentre esta configuración en **Configuración del sistema > Regiones**.



> **Nota:**
>
> Regiones aparece solo cuando la **Multirregión** está activada para su licencia.

> Hay dos páginas:

- Configuración de regiones
- Configuración de nodos cálidos

Configuración de regiones

Agregue las regiones donde se pueden ejecutar los espacios de trabajo. Para cada región, asígnele un nombre y un dominio únicos, y luego decida quién puede usarla:

- **Habilitar para todos** — Todos los usuarios de la plataforma pueden usar la región.
- Limítelo a organizaciones, proyectos o usuarios específicos.

> **Nota:**
>
> Si una región no está habilitada para todos y no se seleccionan organizaciones, proyectos o usuarios, nadie podrá usarla.

> Para conocer los requisitos previos y la configuración de la implementación, consulte Implementar SecurSpaces en varias regiones.

> **Nota:**
>
> Los puntos de montaje solo se admiten en la región principal. Un espacio de trabajo que utiliza un punto de montaje no se puede mover a otra región, y la región no se puede cambiar mientras uno esté adjunto. Consulte Elegir entre depósitos de datos y puntos de montaje.

Configuración de Nodos Cálidos

Mantenga un grupo de nodos listos para usar en una región con **nodos cálidos**. Dado que los nodos ya están aprovisionados, los espacios de trabajo se inician más rápido en lugar de esperar a que se inicien nuevos nodos.

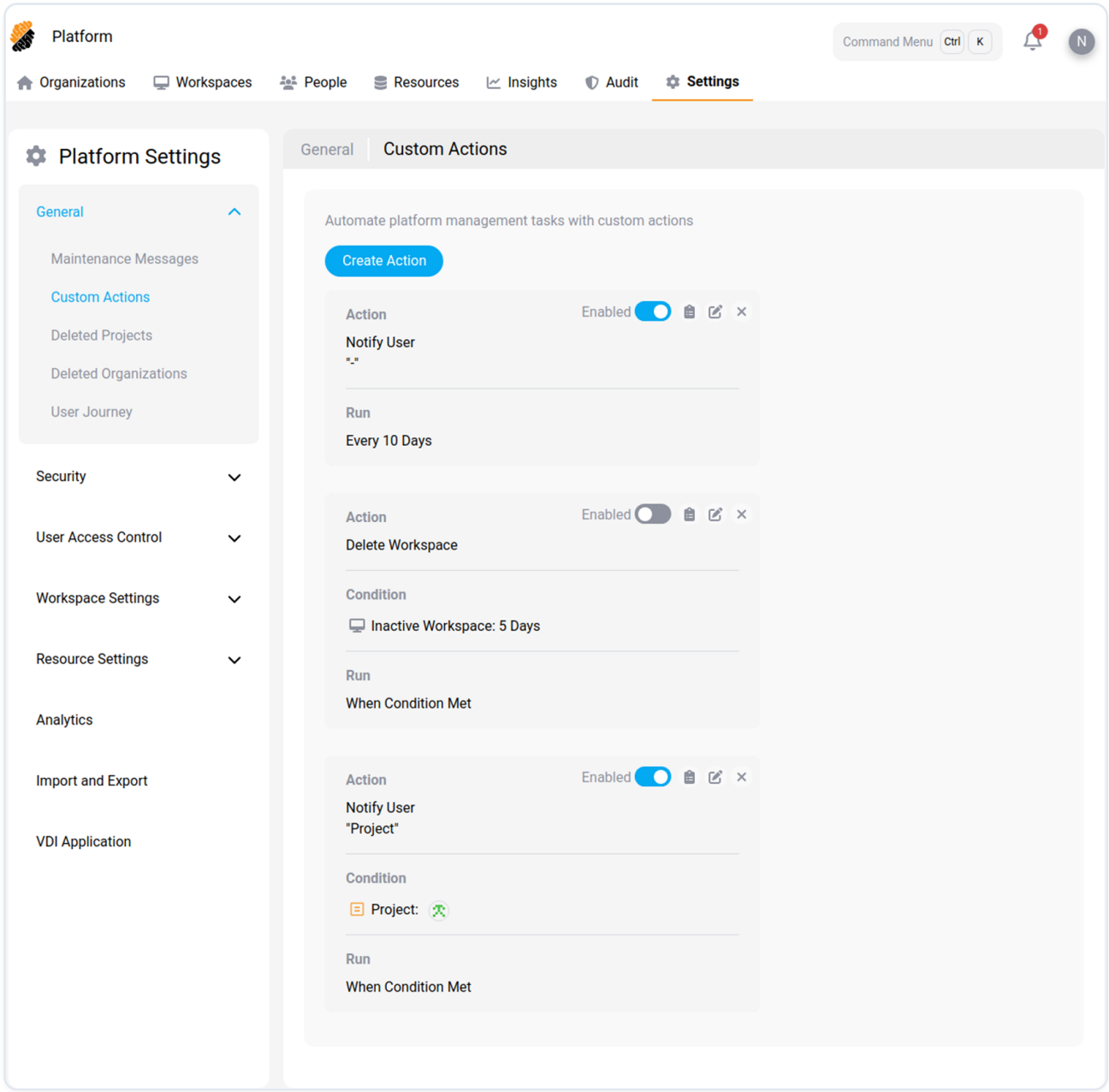
Información relacionada

- Licencia
- Configuración del sistema

Custom actions

Las Acciones personalizadas le permiten automatizar el mantenimiento rutinario de la plataforma. Se define una regla compuesta de tres partes: una acción a ejecutar, las condiciones que deciden a qué espacios de trabajo o usuarios se aplica y cuándo se ejecuta. Un ejemplo común es la eliminación de espacios de trabajo que han estado inactivos durante mucho tiempo.

Encuentre esta configuración en **Ajustes > General > Acciones personalizadas**.



Cómo se construye una acción personalizada

Cada acción personalizada combina tres partes.

Acción — qué se ejecuta

ACCIÓN	QUÉ HACE
Actualizar espacio de trabajo	Aplica una actualización a cada espacio de trabajo coincidente, como una actualización de imagen.
Eliminar espacio de trabajo	Elimina cada espacio de trabajo coincidente.

ACCIÓN	QUÉ HACE
Notificar usuario	Envía una notificación en la plataforma con un mensaje que usted escribe a cada usuario coincidente.

Condición — a qué espacios de trabajo o usuarios se aplica

Añada una o más condiciones para dirigir la acción. Las condiciones disponibles incluyen:

- **Organización:** Limitar a espacios de trabajo en organizaciones específicas.
- **Proyecto:** Limitar a espacios de trabajo en proyectos específicos.
- **Usuario:** Limitar a espacios de trabajo propiedad de usuarios específicos.
- **Espacio de trabajo inactivo:** Coincidir con espacios de trabajo que no se han utilizado durante un número determinado de días.
- **Después** y **Antes:** Limitar la acción a un período de tiempo estableciendo una fecha de inicio, una fecha de finalización o ambas.

Cuándo — cómo se programa la acción

El campo **Cuándo** controla la programación. Ofrece tres opciones:

OPCIÓN	COMPORTAMIENTO
Una vez	Se ejecuta una vez, en la fecha y hora que usted establezca.
Período de tiempo	Se ejecuta en un horario repetitivo, como cada 30 días.
Cuando se cumpla la condición	Se ejecuta continuamente en segundo plano y aplica la acción siempre que se cumplan las condiciones. Esta opción aparece solo después de añadir al menos una condición.

"Cuando se cumple la condición" frente a "Período de tiempo"

Esta es la elección clave para una regla de mantenimiento como la eliminación de espacios de trabajo inactivos, por lo que vale la pena entender cómo se comporta cada opción.

Cuando se cumple la condición evalúa sus condiciones en un ciclo de fondo recurrente, aproximadamente cada 15 minutos. En cada ciclo, encuentra todo lo que coincide actualmente y aplica la acción. No espera una fecha programada. Tan pronto como un espacio de trabajo cruza su umbral de inactividad, se detecta en el siguiente ciclo.

Período de tiempo se ejecuta en el intervalo fijo que usted establece — por ejemplo, cada 30 días. Las condiciones solo deciden qué espacios de trabajo se ven afectados cuando se produce esa ejecución programada. Cualquier cosa que coincida entre dos ejecuciones programadas espera hasta la siguiente ejecución.

Para una regla como "eliminar un espacio de trabajo cuando ha estado inactivo durante 365 días," **Cuando se cumple la condición** es la elección correcta. La acción comprueba continuamente y elimina cada espacio de trabajo poco después de que pasen 365 días de inactividad — no en un programa separado que tendría que mantener sincronizado.

> **Nota:**

> Con **Cuando se cumple la condición**, la acción no se ejecuta "una vez al día hasta que se cumpla la condición". Se reevalúa en un ciclo de fondo corto (aproximadamente cada 15 minutos) y actúa tan pronto como algo coincide. Dado que un espacio de trabajo eliminado ya no existe, no se vuelve a coincidir — cada espacio de trabajo se elimina una vez.

Ejemplo: eliminar espacios de trabajo inactivos durante 365 días

1. Vaya a **Configuración > General > Acciones personalizadas** y comience una nueva acción.
2. Para la acción, seleccione **Eliminar espacio de trabajo**.
3. Añada una condición, seleccione **Espacio de trabajo inactivo**, y establezca el período en **365** días.
4. Para **Cuándo**, seleccione **Cuando se cumple la condición**.
5. Guarde la acción.

La plataforma ahora comprueba continuamente. Cualquier espacio de trabajo que alcance los 365 días sin uso se elimina automáticamente dentro del siguiente ciclo de evaluación.

> **Nota:**

> La inactividad se mide desde el último uso registrado de un espacio de trabajo. Un espacio de trabajo que nunca se ha abierto no coincide con la condición de **Espacio de trabajo inactivo**.

Qué se considera uso

Un espacio de trabajo se considera usado cuando alguien trabaja en él a través de un IDE, un terminal o SSH. Iniciar un espacio de trabajo manualmente también cuenta, ya sea que se inicie desde la consola, la API REST o la extensión del IDE. Esto significa que un espacio de trabajo que un desarrollador inicia regularmente no coincide con la condición de **Espacio de trabajo inactivo**, incluso si nunca abre una sesión dentro de él.

Un espacio de trabajo que el programador reanuda automáticamente no se considera usado. Las reanudaciones automáticas no son actividad del usuario, por lo que no mantienen un espacio de trabajo que de otro modo no se usaría fuera del alcance.

Cuando un administrador inicia un espacio de trabajo en nombre de otra persona, el uso se registra contra el propietario del espacio de trabajo.

> **Nota:**
>
> Iniciar un espacio de trabajo no pospone el tiempo de espera de inactividad que pausa los espacios de trabajo inactivos. Los dos se miden por separado: iniciar un espacio de trabajo lo mantiene fuera del alcance de la eliminación, pero solo la actividad real dentro del espacio de trabajo evita que se pause. Consulta Detección de inactividad del espacio de trabajo.

Información relacionada

- Configuración general
- Gestión de espacios de trabajo

Project labels

Las etiquetas de proyecto le permiten construir una taxonomía compartida que organiza cada proyecto en la plataforma. Como administrador, usted define la taxonomía una vez cargando un archivo CSV. A partir de entonces, quienquiera que cree o edite un proyecto elige un valor en cada nivel de esa taxonomía, para que los proyectos permanezcan categorizados de forma consistente en todas las organizaciones.

Encuentre esta configuración en **System Configuration > Others > Project Labels**.

Para qué se utilizan las etiquetas de proyecto

Las etiquetas de proyecto le proporcionan un vocabulario único y controlado para clasificar proyectos. En lugar de dejar que cada equipo invente su propia nomenclatura, usted publica una jerarquía de la que todos seleccionan.

Una vez configuradas las etiquetas, aparecen en tres lugares:

- **Crear y editar proyecto:** Los usuarios eligen un valor en cada nivel de la jerarquía. Si las etiquetas están configuradas, se requiere una selección en cada nivel.
- **Lista de proyectos:** Una columna de **Etiquetas de proyecto** muestra la ruta de la etiqueta para cada proyecto, para que pueda ver cómo se categorizan los proyectos.
- **Informes de uso:** Las etiquetas seleccionadas se adjuntan a las métricas de espacio de trabajo y de usuarios activos, para que pueda agrupar los datos de uso por su taxonomía de negocio.

La jerarquía puede tener hasta cinco niveles de profundidad. Cada nivel se convierte en un menú desplegable separado cuando un usuario crea o edita un proyecto.

Cómo se estructura el archivo CSV

Usted define la taxonomía cargando un archivo CSV. La plataforma lee el archivo como un árbol: cada fila describe una ruta completa desde el nivel superior hacia abajo, y los valores repetidos se fusionan automáticamente.

PARTE DEL ARCHIVO	REQUISITO	PROPÓSITO
Primera fila (encabezado)	Obligatorio	Cada celda nombra un nivel de la jerarquía. Estos nombres se convierten en las etiquetas desplegables que los usuarios ven cuando crean un proyecto.
Filas restantes	Al menos uno obligatorio	Cada fila enumera un valor por nivel, de izquierda (nivel superior) a derecha.
Columnas	De 1 a 5 usadas	Cada columna es un nivel de la jerarquía. La plataforma lee más de cinco columnas,

PARTE DEL ARCHIVO	REQUISITO	PROPÓSITO
		pero solo las cinco primeras aparecen en el formulario del proyecto.
Celdas vacías	Opcional	Una fila puede detenerse en cualquier columna. Las celdas vacías se omiten.

Ten en cuenta estas reglas:

- Utiliza un archivo CSV estándar UTF-8, separado por comas.
- Enumera cada combinación que quieras permitir. La plataforma elimina automáticamente los valores duplicados en el mismo nivel, por lo que no tienes que preocuparte por repetir un valor padre en varias filas.
- La carga de un nuevo archivo reemplaza toda la taxonomía. No se fusiona con una carga anterior.

Referencia de columna

COLUMNA	NIVEL	ENCABEZADO DE EJEMPLO	TIPO DE DATOS
1	Nivel superior	Unidad de negocio	Texto
2	Segundo nivel	Línea de producto	Texto
3	Tercer nivel	Equipo	Texto
4	Cuarto nivel	Subequipo	Texto
5	Quinto nivel	Componente	Texto

Ejemplo de CSV

Supongamos que desea clasificar cada proyecto por unidad de negocio, luego por línea de producto y luego por equipo. Crearía un archivo como este:

```
Business Unit,Product Line,Team

Finance,Payments,Checkout
```

```
Finance,Payments,Fraud

Finance,Billing,Invoicing

Healthcare,Patient Portal,Web

Healthcare,Patient Portal,Mobile

Healthcare,Claims,Processing
```

Este archivo produce la siguiente jerarquía:

- **Finanzas**
  - Pagos > Pago, Fraude
  - Facturación > Facturación
- **Sanidad**
  - Portal del paciente > Web, Móvil
  - Reclamaciones > Procesamiento

Tenga en cuenta que **Finanzas** y **Pagos** aparecen en varias filas. La plataforma fusiona estos valores repetidos automáticamente, para que no cree duplicados; simplemente enumere cada ruta completa que desee permitir.

Lo que ve el usuario

Después de cargar el archivo, los tres nombres de encabezado se convierten en tres menús desplegables en el formulario Crear proyecto: **Unidad de negocio**, **Línea de producto** y **Equipo**. Los menús desplegables son en cascada, por lo que cada elección restringe la siguiente.

Por ejemplo, un usuario que crea un proyecto podría:

1. Elija **Unidad de negocio** > **Finanzas**. El menú desplegable **Línea de producto** ahora solo ofrece **Pagos** y **Facturación**.
2. Elija **Línea de producto** > **Pagos**. El menú desplegable **Equipo** ahora solo ofrece **Caja** y **Fraude**.
3. Elija **Equipo** > **Fraude**.

El proyecto ahora está etiquetado como **Finanzas > Pagos > Fraude**. Esa ruta aparece en la columna **Etiquetas de proyecto** de la lista de proyectos y viaja con los datos de uso del proyecto, para que pueda informar sobre todos los proyectos de Finanzas —o solo los del equipo de Fraude — en cualquier momento.

Cargar sus etiquetas de proyecto

1. Vaya a **Configuración del sistema > Otros > Etiquetas de proyecto**.
2. Seleccione el campo de archivo y elija su archivo CSV.
3. Seleccione **Cargar**.

La nueva taxonomía entra en vigor inmediatamente y reemplaza cualquier etiqueta cargada anteriormente. Los proyectos existentes conservan sus etiquetas actuales hasta que alguien edite el proyecto y elija nuevos valores.

Información relacionada

- Otros
- Configuración del sistema
- Proyectos

Onboarding emails

Citrix SecurSpaces™ envía notificaciones automáticas por correo electrónico que ayudan a los nuevos usuarios a familiarizarse con la plataforma y sus proyectos. Estos correos electrónicos proporcionan a los destinatarios un enlace de inicio de sesión directo, para que puedan empezar sin esperar instrucciones manuales.

Esta página explica qué correos electrónicos envía SecurSpaces, cuándo se activa cada uno y qué ven los destinatarios. Está escrita para administradores de plataforma y propietarios de proyectos que incorporan usuarios.

> **Nota:**

> Las notificaciones por correo electrónico solo se entregan cuando se configura una puerta de enlace de correo electrónico. Consulte Requisito previo: configurar una puerta de enlace de correo electrónico.

Cómo funcionan los correos electrónicos de incorporación

SecurSpaces genera un correo electrónico de incorporación cada vez que un evento añade un usuario a la plataforma o a un proyecto. La plataforma construye el mensaje a partir de una plantilla, lo personaliza con detalles como el nombre del invitador y un enlace de inicio de sesión, y lo envía a través de la puerta de enlace de correo electrónico configurada.

Los destinatarios no necesitan una cuenta existente para recibir estos correos electrónicos. Cada correo electrónico incluye un botón que lleva al usuario directamente a la página de inicio de sesión o al proyecto relevante.

Requisito previo: configurar una puerta de enlace de correo electrónico

Los correos electrónicos de incorporación se envían a través de la puerta de enlace de correo electrónico definida en **Configuración del sistema**. Hasta que se configure una puerta de enlace, SecurSpaces no genera correos electrónicos de incorporación.

Para configurar la puerta de enlace:

1. Inicie sesión como administrador de plataforma y seleccione **Configuración del sistema**.
2. Seleccione **Otros** > **Configuración de la puerta de enlace de correo electrónico**.
3. Elija un proveedor: **Amazon SES**, **SendGrid** o **SMTP**.
4. Introduzca los detalles requeridos para su proveedor, incluida la dirección de **Correo electrónico del remitente** que los destinatarios ven en el campo *De*.
5. Seleccione **Guardar**.

Para ver la lista completa de campos del proveedor, consulte Otros.

> **Nota:**
>
> La dirección de **correo electrónico del remitente** aparece como el remitente de cada correo electrónico de incorporación. Utilice una dirección que los destinatarios reconozcan y en la que confíen, y desde la que su proveedor esté autorizado a enviar.

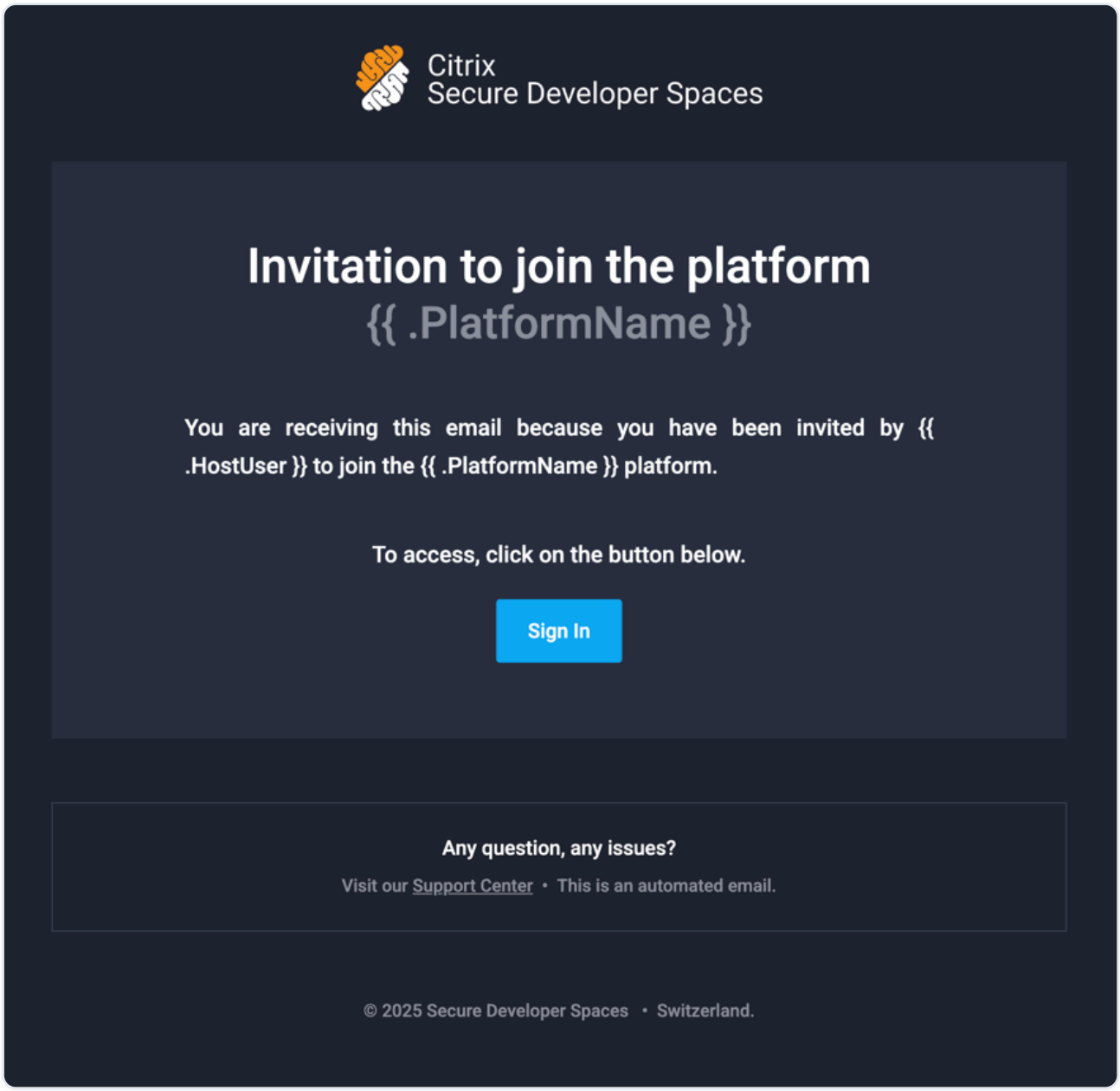
Tipos de correo electrónico

SecurSpaces envía tres correos electrónicos de incorporación.

CORREO ELECTRÓNICO	ACTIVADOR	ACCIÓN PRINCIPAL
Invitación para unirse a la plataforma	Se invita a un usuario a la plataforma.	**Iniciar sesión** — abre la página de inicio de sesión de la plataforma.
Te has unido a un nuevo proyecto	Se añade un usuario a un proyecto.	**Acceder al proyecto** — abre el proyecto.
Correo electrónico de prueba	Un administrador envía una prueba desde la configuración de la pasarela de correo electrónico.	Ninguno. Confirma que la pasarela funciona.

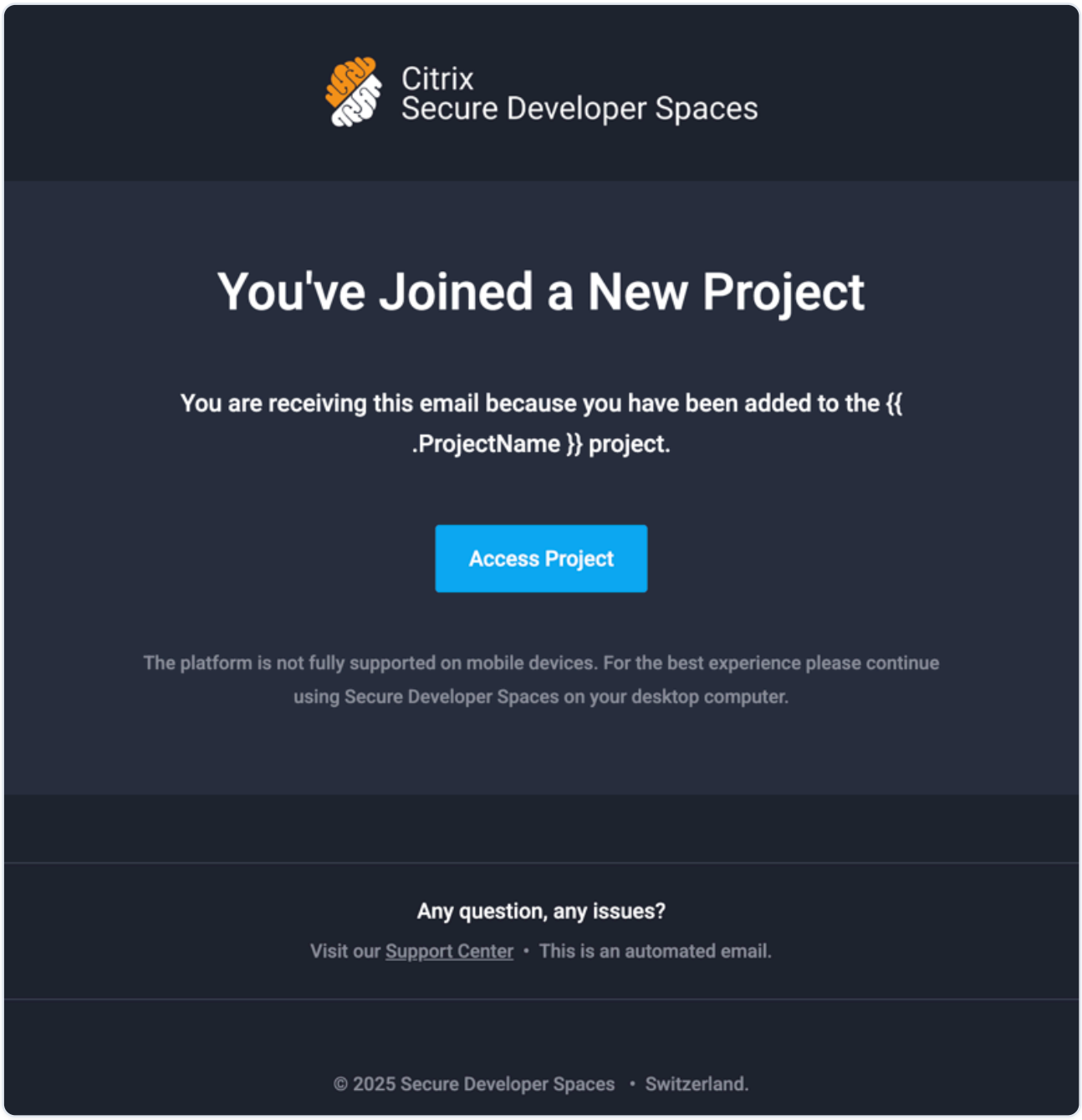
Invitación para unirse a la plataforma

Se envía cuando se invita a un usuario a la plataforma por primera vez. El correo electrónico nombra al invitador e incluye un botón de **Iniciar sesión** que abre la página de inicio de sesión con la dirección de correo electrónico del destinatario precargada.



Te has unido a un nuevo proyecto

Se envía cuando se añade un usuario a un proyecto. El correo electrónico nombra el proyecto e incluye un botón de **Acceder al proyecto** que lo abre.



Correo de prueba

Se envía cuando un administrador utiliza la opción de prueba en **Configuración de la pasarela de correo electrónico**. Úselo para confirmar que la pasarela está configurada correctamente antes de invitar a los usuarios. El correo electrónico de prueba no incluye un botón de acción.

Solucionar problemas de los correos electrónicos de incorporación

Si un usuario informa de que no ha recibido un correo electrónico de incorporación:

COMPROBAR	QUÉ HACER
Pasarela de correo electrónico	Confirme que hay una pasarela configurada en **Configuración del sistema** > **Otros** > **Configuración de la pasarela de correo electrónico**. Sin ella, SecurSpaces no envía correos electrónicos.
Estado de la pasarela	Envíe un correo electrónico de prueba desde la configuración de la pasarela para confirmar que el proveedor funciona.
Dirección del remitente	verificar que la dirección de **Correo electrónico del remitente** es válida y está autorizada para enviar a través de su proveedor.
Spam o cuarentena	Pida al destinatario que revise su carpeta de spam o cuarentena. Los correos electrónicos automatizados a veces se filtran.
Dirección de correo electrónico	Confirme que la dirección utilizada para invitar al usuario es correcta.

Si el correo electrónico de prueba llega pero los correos electrónicos de incorporación no, vuelva a comprobar el evento que debería haber activado el correo electrónico; por ejemplo, que el usuario se haya añadido realmente a la plataforma o al proyecto.

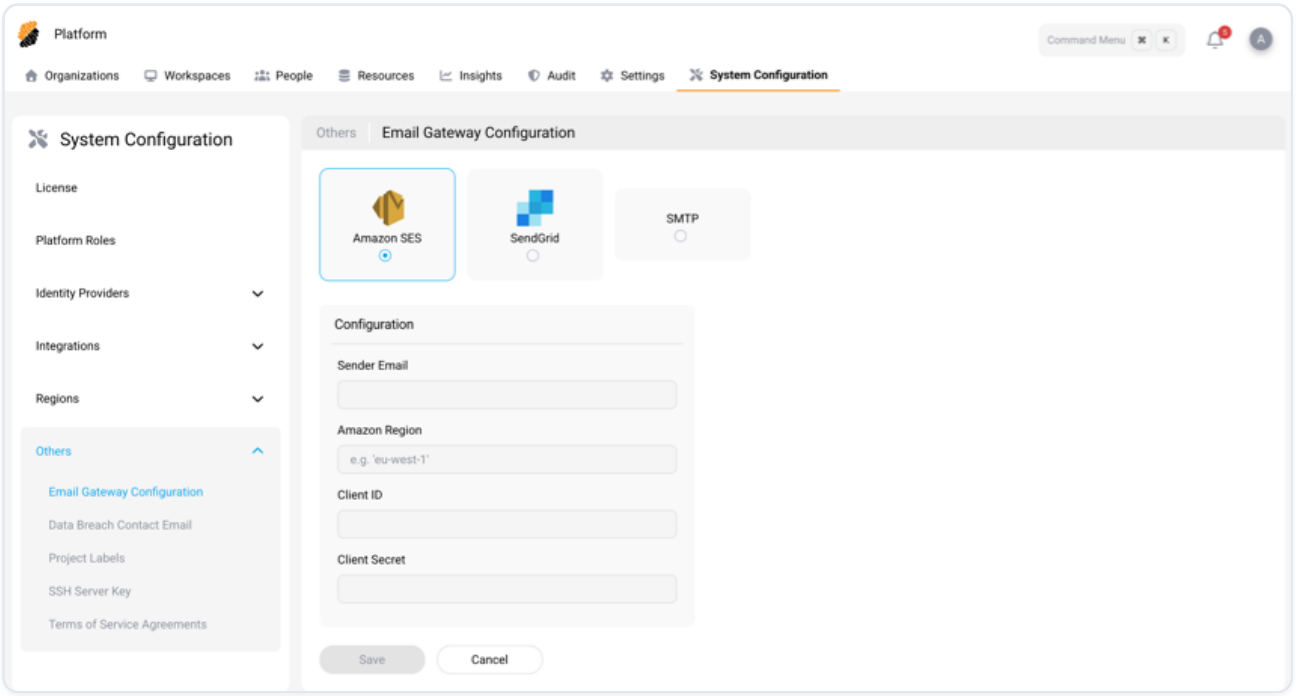
Información relacionada

- Otros
- Añadir y eliminar usuarios y grupos
- Configuración del sistema

Email gateway

Otros reúne un puñado de configuraciones de toda la plataforma que no encajan en las otras áreas.

Encuentre estas configuraciones en **Configuración del sistema > Otros**.



Esto es lo que encontrará:

- Configuración de la puerta de enlace de correo electrónico
- Correo electrónico de contacto para fugas de datos
- Clave del servidor SSH
- Acuerdos de términos de servicio
- Etiquetas de proyecto

Configuración de la puerta de enlace de correo electrónico

Configure la puerta de enlace que la plataforma utiliza para enviar notificaciones por correo electrónico, como invitaciones de incorporación. Elija un proveedor, introduzca sus detalles, añada la dirección de **Correo electrónico del remitente** que ven los destinatarios y envíe un correo electrónico de prueba para verificar que funciona.

Elija uno de los siguientes proveedores:

- **Amazon SES**
- **SendGrid**
- **SMTP**

El campo **Correo electrónico del remitente** se aplica a todos los proveedores. Los campos restantes dependen del proveedor que seleccione.

Amazon SES

CAMPO	DESCRIPCIÓN
Correo electrónico del remitente	La dirección que aparece como remitente de cada correo electrónico.
Región de Amazon	La región de AWS para su configuración de Amazon SES (por ejemplo, `eu-west-1`).
ID de cliente	Su ID de clave de acceso de Amazon SES.
Secreto de cliente	Su clave de acceso secreta de Amazon SES.

SendGrid

CAMPO	DESCRIPCIÓN
Correo electrónico del remitente	La dirección que aparece como remitente de cada correo electrónico.
Clave de API	Su clave de API de SendGrid.

SMTP

CAMPO	DESCRIPCIÓN
Correo electrónico del remitente	La dirección que aparece como remitente de cada correo electrónico.
Host	El nombre de host de su servidor SMTP (por ejemplo, `smtp.example.com`).
Puerto	El puerto de su servidor SMTP.
Nombre de usuario	El nombre de usuario SMTP. Opcional.
Contraseña	La contraseña SMTP. Opcional.

Para confirmar que la pasarela funciona, envíe un correo electrónico de prueba. Hasta que no se configure una pasarela, la plataforma no enviará notificaciones por correo electrónico. Para obtener detalles sobre los correos electrónicos que envía la plataforma, consulte Notificaciones por correo electrónico de incorporación.

Correo electrónico de contacto para filtraciones de datos

Ofrezca a los usuarios una forma sencilla de informar sobre una posible filtración de datos. Añada un correo electrónico de contacto y, a continuación, seleccione **Habilitar visualización de la información de informes** para mostrarlo en toda la plataforma.

Clave de servidor SSH

Administre la clave SSH del servidor utilizada para el tráfico fuera del ecosistema de Citrix SecurSpaces™. Cargue una nueva clave privada de servidor SSH siempre que necesite rotarla.

Acuerdos de términos de servicio

Añada los términos de servicio que los usuarios aceptan antes de usar la plataforma. Puede cargar más de un documento, eliminar un documento o restablecer todas las aceptaciones para que los usuarios lo acepten de nuevo.

Para obtener detalles sobre lo que ven los usuarios, si se requiere la aceptación y cómo restablecer las aceptaciones, consulte Acuerdos de términos de servicio.

Etiquetas de proyecto

Administre las etiquetas que le ayudan a clasificar y organizar proyectos en toda la plataforma. Usted define las etiquetas cargando un archivo CSV que describe una jerarquía, y los usuarios eligen de esa jerarquía cuando crean o editan un proyecto.

Para conocer el formato CSV, un ejemplo y los pasos de carga, consulte Etiquetas de proyecto.

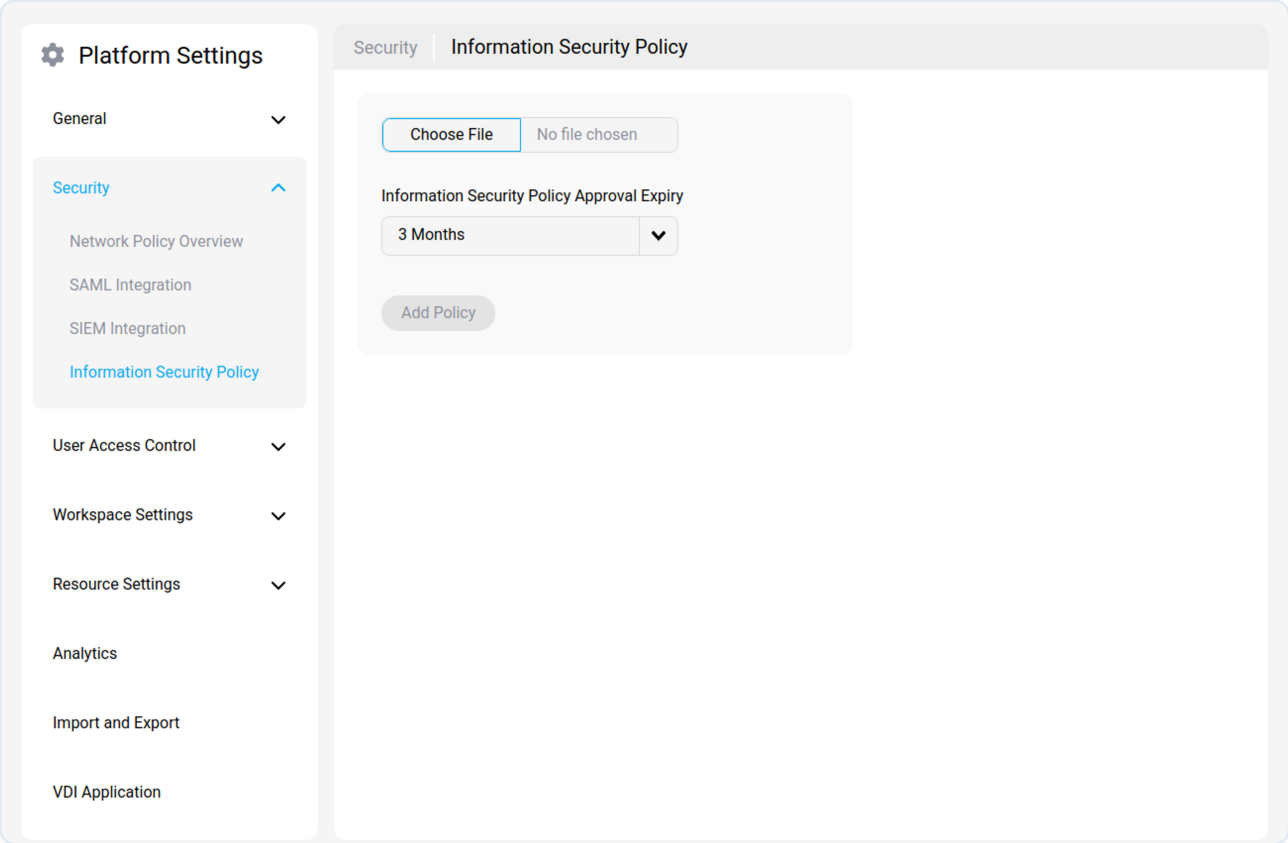
Información relacionada

- Notificaciones por correo electrónico de incorporación
- Configuración del sistema
- Acceso SSH a los espacios de trabajo

Information security policy

La Política de Seguridad de la Información le permite publicar el documento de política de seguridad de su organización para todos en la plataforma. Como administrador, usted carga un PDF y establece cuánto tiempo permanece válido antes de renovarlo. Los usuarios pueden abrir y leer la política en cualquier momento.

Encuentre esta configuración en **Settings > Security > Information Security Policy**.



Para qué se utiliza la Política de Seguridad de la Información

Utilice esta función para que una política de seguridad única y autorizada esté disponible en toda la plataforma. Usted carga el documento, y la plataforma almacena su fecha de envío, su fecha de renovación más reciente y su fecha de caducidad para que su política se mantenga actualizada.

El documento debe ser un PDF.

Dónde ven los usuarios la política

Cualquier persona que haya iniciado sesión en la plataforma puede abrir la política desde el enlace **Política** en el pie de página. Al seleccionarlo, se abre una ventana que muestra:

- La fecha de envío.
- La fecha de renovación.
- La fecha de caducidad.
- El propio documento de la política.

Los administradores también ven un botón de **Renovar** en esta ventana.

¿Se requiere aceptación?

No. La Política de Seguridad de la Información es un documento de referencia. Los usuarios pueden leerla cuando quieran, pero no se les pide que la acepten, y no se les impide usar la plataforma si no la han abierto.

> **Nota:**
>
> Si necesita que los usuarios acepten activamente un documento antes de poder usar la plataforma, utilice Acuerdos de Términos de Servicio en su lugar. Las dos características son independientes: los Acuerdos de Términos de Servicio requieren aceptación y bloquean el acceso hasta que el usuario los acepta, mientras que la Política de Seguridad de la Información es de solo lectura para los usuarios y nunca los bloquea.

Cómo funciona la caducidad de la aprobación

Cuando carga la política, establece un período de **Caducidad de la Aprobación de la Política de Seguridad de la Información**: 3, 6, 9, 12, 18 o 24 meses. La plataforma utiliza esto para calcular una fecha de caducidad, medida a partir de la fecha de carga.

Esto es un recordatorio para el administrador, no un programa de nueva aceptación por parte del usuario. Esto es lo que hace y no hace la caducidad:

- **No afecta a los usuarios.** Los usuarios nunca reciben una nueva solicitud, notificación o bloqueo cuando la política caduca.
- **Recuerda a los administradores.** Dentro de los 14 días anteriores a la fecha de caducidad, y después de que esta pase, los administradores ven una advertencia de que la política necesita atención. Esto mantiene su política publicada actualizada.

Así, el período de **Caducidad de la Aprobación** establece cuánto tiempo se considera vigente su documento antes de que usted, como administrador, necesite renovarlo o reemplazarlo. No se pide a los usuarios que aprueben la política basándose en este período.

Mantener la política actualizada

Borre una advertencia de caducidad de una de estas dos maneras:

- **Cargar una nueva política.** Vaya a **Configuración > Seguridad > Política de Seguridad de la Información**, cargue un nuevo PDF y establezca un nuevo período de Caducidad de la Aprobación. Esto reemplaza el documento actual.

- **Renovar la política actual.** Abra la política desde el pie de página y seleccione **Renovar**. Esto extiende la fecha de caducidad sin reemplazar el documento.

Información relacionada

- Configuración de seguridad
- Acuerdos de Términos de Servicio

Terms of service agreements

Los Acuerdos de Términos de Servicio le permiten presentar uno o más documentos que los usuarios deben aceptar antes de usar la plataforma. Como administrador, usted carga los documentos y la plataforma bloquea el acceso a cualquier usuario que no sea administrador hasta que haya aceptado todos los documentos actuales.

Encuentre esta configuración en **Configuración del sistema > Otros > Acuerdos de Términos de Servicio**.

Para qué se utilizan los Acuerdos de Términos de Servicio

Utilice esta función para exigir la aceptación de documentos legales o de políticas, como una política de uso aceptable o un acuerdo de servicio. Puede:

- Cargar uno o más documentos.
- Previsualizar o eliminar un documento.
- Restablecer las aceptaciones de un documento para que todos lo acepten de nuevo.

PDF es el formato de archivo recomendado. La página de aceptación también renderiza documentos HTML (`.html` o `.htm`) y de texto sin formato (`.txt`).

Cuando carga más de un documento, los usuarios los aceptan todos juntos en un solo paso.

Dónde ven los usuarios los Términos de Servicio

Después de que un usuario que no es administrador inicia sesión, la plataforma comprueba si ha aceptado todos los documentos actuales. Si alguno está pendiente, la plataforma los envía a una página dedicada de **Acuerdos de Términos de Servicio** antes de que puedan acceder a cualquier otra parte de la plataforma.

En esa página, el usuario:

1. Revisa cada documento, mostrado íntegramente en la página.

2. Selecciona **Aceptar todo** para aceptar todos los documentos pendientes a la vez.

Después de que el usuario acepta, la plataforma registra su aceptación y los lleva a la experiencia normal. La página no vuelve a aparecer a menos que añada un nuevo documento o restablezca las aceptaciones.

¿Se requiere la aceptación?

Sí. La aceptación es obligatoria y bloquea a los usuarios que no son administradores. Hasta que un usuario acepte todos los documentos actuales, no podrá navegar a proyectos, espacios de trabajo o configuraciones. La página muestra este aviso:

> Debe leer y aceptar todos los acuerdos de Términos de servicio antes de poder utilizar la plataforma.

> Algunos detalles importantes:

- **La aceptación es por usuario y por documento.** La plataforma rastrea qué documentos ha aceptado cada usuario.
- **Los administradores no están bloqueados.** Para que pueda seguir gestionando la plataforma, los administradores no son redirigidos a la página de aceptación, incluso cuando hay documentos pendientes.
- **Los nuevos documentos se aplican a todos.** Cuando añade un documento, se solicita a cada usuario que no es administrador que lo acepte la próxima vez que inicie sesión o navegue.

> **Nota:**

> La plataforma registra que un usuario aceptó un documento, pero no almacena una marca de tiempo de aceptación. Si su organización necesita un registro de auditoría fechado de la aceptación, mantenga ese registro fuera de la plataforma.

Restablecer aceptaciones

Restablecer las aceptaciones obliga a los usuarios a aceptar un documento de nuevo, por ejemplo, después de publicar una nueva versión.

1. Vaya a **Configuración del sistema > Otros > Acuerdos de términos de servicio**.

2. Busque el documento en la lista.
3. Seleccione el icono de restablecimiento junto al documento.
4. Confirme el restablecimiento.

La plataforma borra la aceptación de ese documento por parte de todos los usuarios. La próxima vez que cada usuario no administrador inicie sesión o navegue, se le pedirá que lo acepte de nuevo.

Información relacionada

- Otros
- Política de seguridad de la información
- Configuración del sistema

Security settings

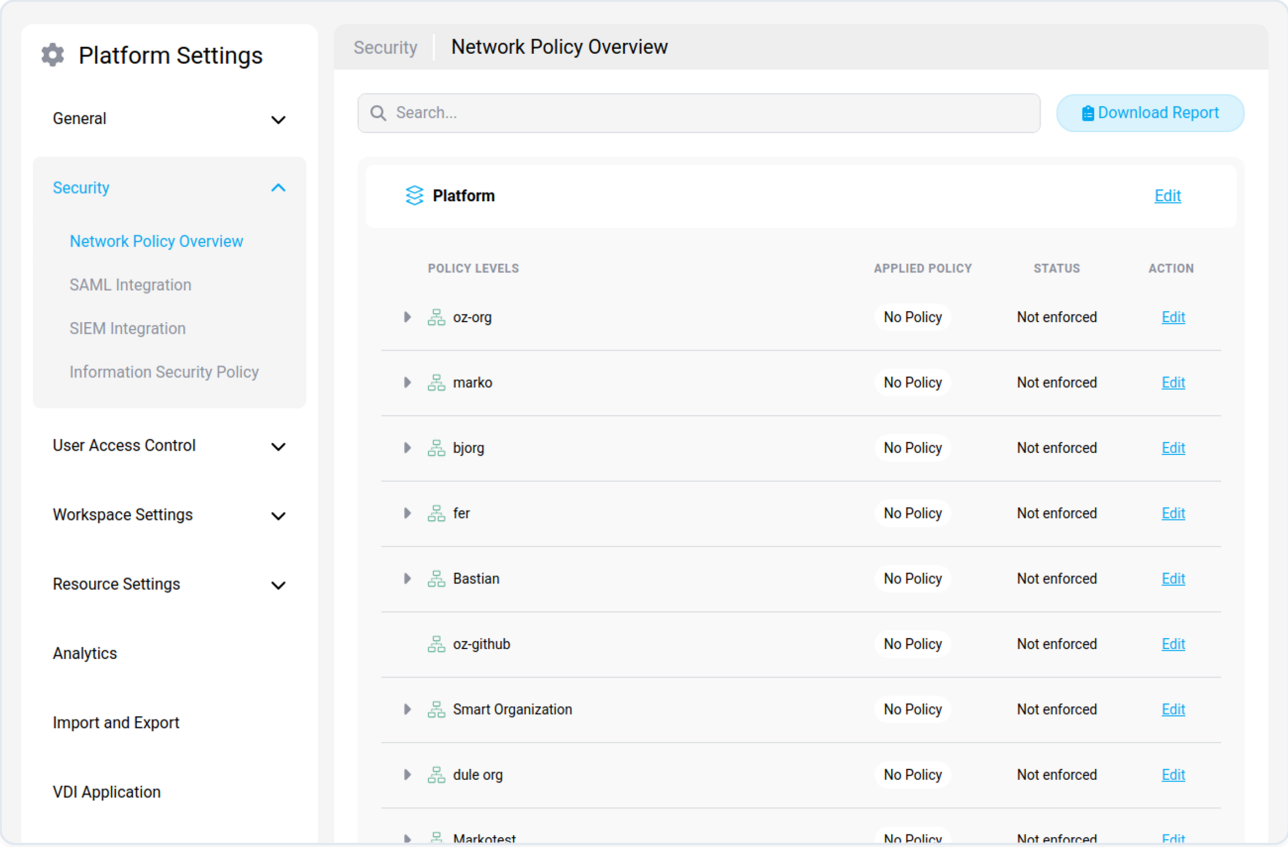
Configure parámetros de seguridad críticos para toda la plataforma. Esto incluye la gestión de la **integración SAML** para un acceso seguro a aplicaciones web a través de RBI, la configuración de la **integración SIEM** para el registro centralizado, la obtención de una **descripción general de la política de red** y el establecimiento de la **política de seguridad de la información** para toda la plataforma. Estos ajustes son esenciales para proteger los recursos de la plataforma y garantizar un acceso seguro a los usuarios.

- Descripción general de la política de red
- Integración SAML
- Integración SIEM
- Política de seguridad de la información

Descripción general de la política de red

Obtenga una vista resumida de las políticas de red actualmente aplicadas en toda la plataforma. Esta descripción general ayuda a los administradores a comprender rápidamente las configuraciones y reglas de seguridad de red existentes a un alto nivel.

Para el modelo de políticas y cómo se aplican, consulte Políticas de red.

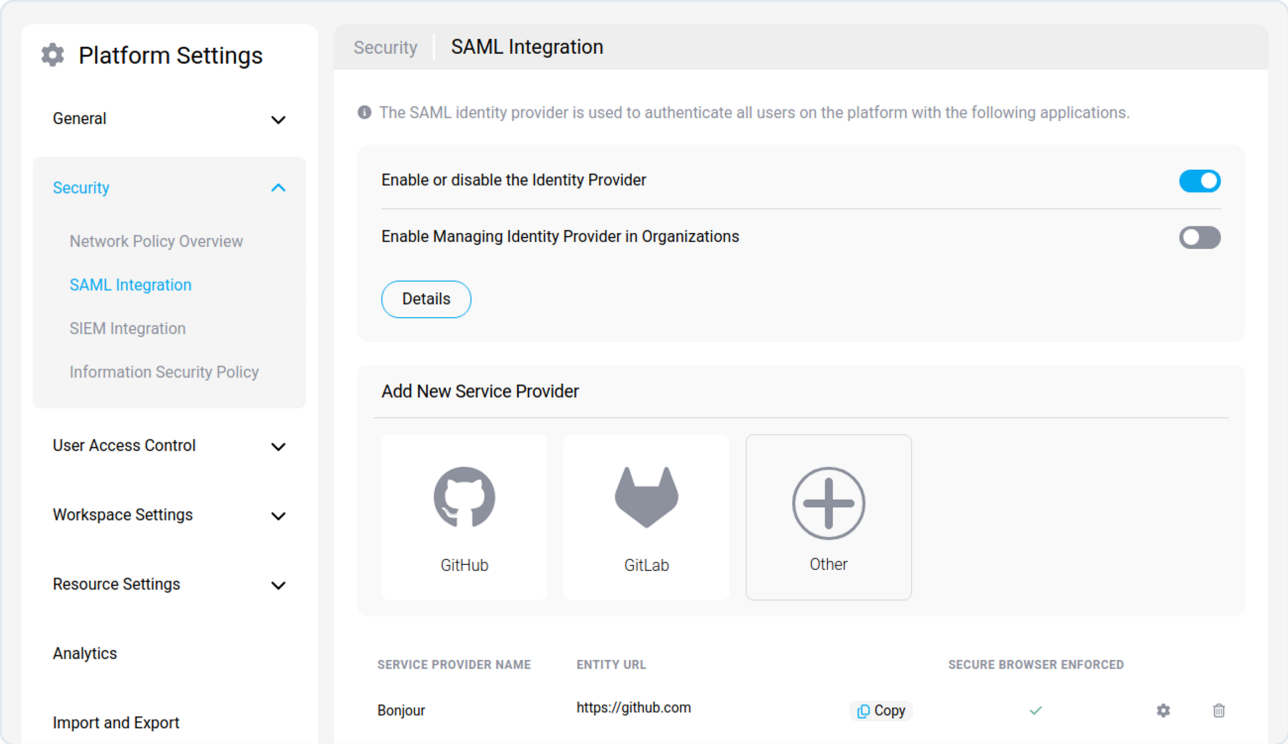


Integración SAML

La sección de **integración SAML** es responsable de autenticar a todos los usuarios en la plataforma al acceder a aplicaciones web. Los usuarios acceden a estas aplicaciones web a través del aislamiento remoto del navegador (RBI), conocido en la plataforma como el "Navegador Seguro". El Navegador Seguro ofrece acceso habilitado para DLP a cualquier dominio sensible, como GitHub, Jira y GitLab. Los usuarios están restringidos a acceder a estas aplicaciones web únicamente a través de la plataforma, prohibiendo el acceso a través de navegadores externos.

Los administradores tienen la opción de habilitar o deshabilitar un proveedor de identidad preconfigurado. También pueden permitir que las organizaciones supervisen sus propios proveedores de identidad.

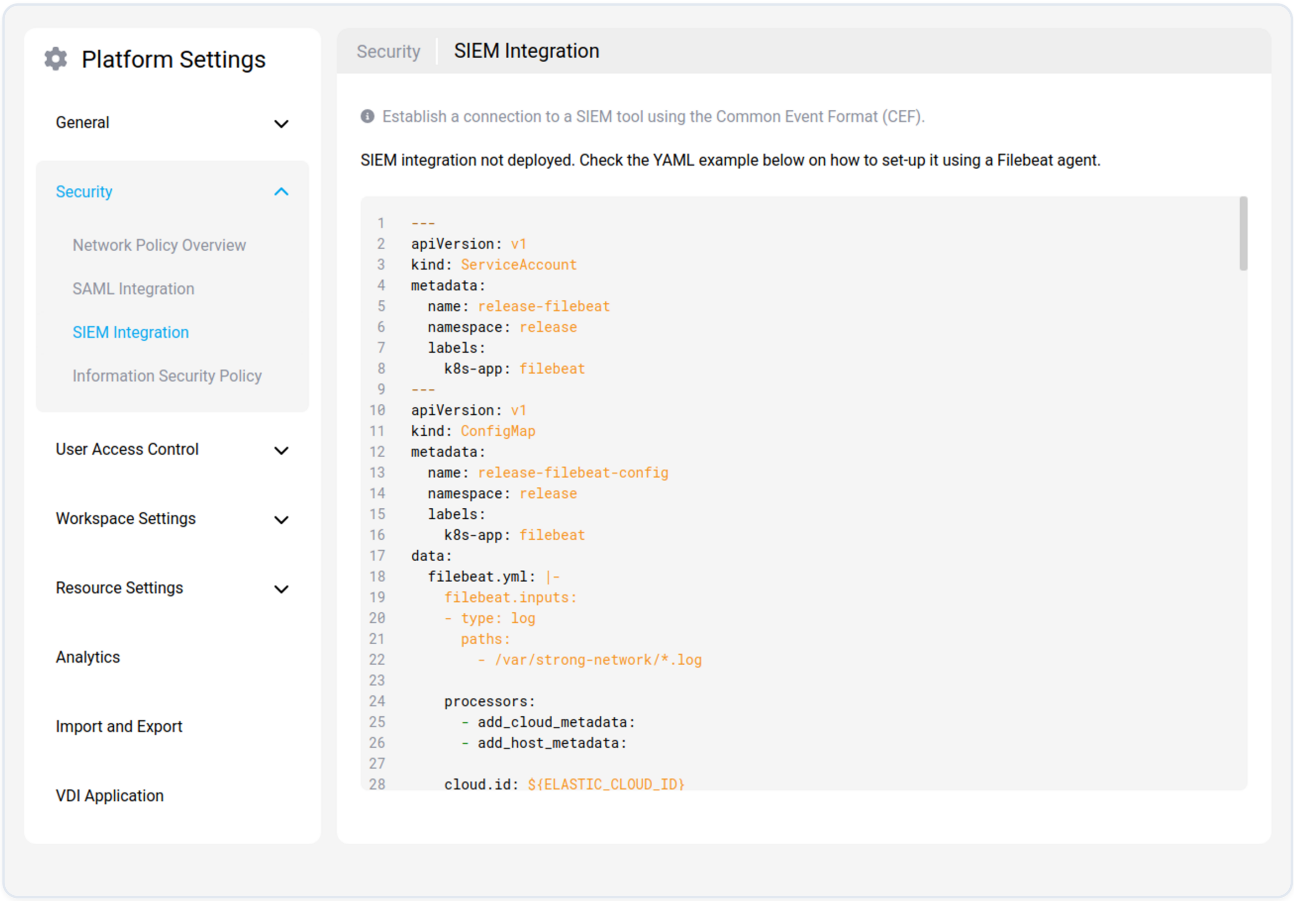
Para saber cómo configurar un proveedor de identidad SAML, consulte SAML.



Integración SIEM

Configure la integración de la plataforma con su sistema de Gestión de Información y Eventos de Seguridad (SIEM). Esto permite reenviar registros y eventos de seguridad desde la plataforma a su SIEM central para su monitorización, análisis y alerta.

Para el procedimiento de configuración y los eventos que se reenvían, consulte integración de SIEM.



Política de Seguridad de la Información

Publique la política de seguridad de la información de su organización para que todos en la plataforma puedan leerla. Usted carga un PDF y establece un período de caducidad de aprobación que le recuerda cuándo debe renovarla o reemplazarla.

Para saber dónde ven los usuarios la política, si se requiere su aceptación y cómo funciona el período de caducidad de la aprobación, consulte Política de Seguridad de la Información.

Operations

Estas páginas cubren el funcionamiento diario de la plataforma.

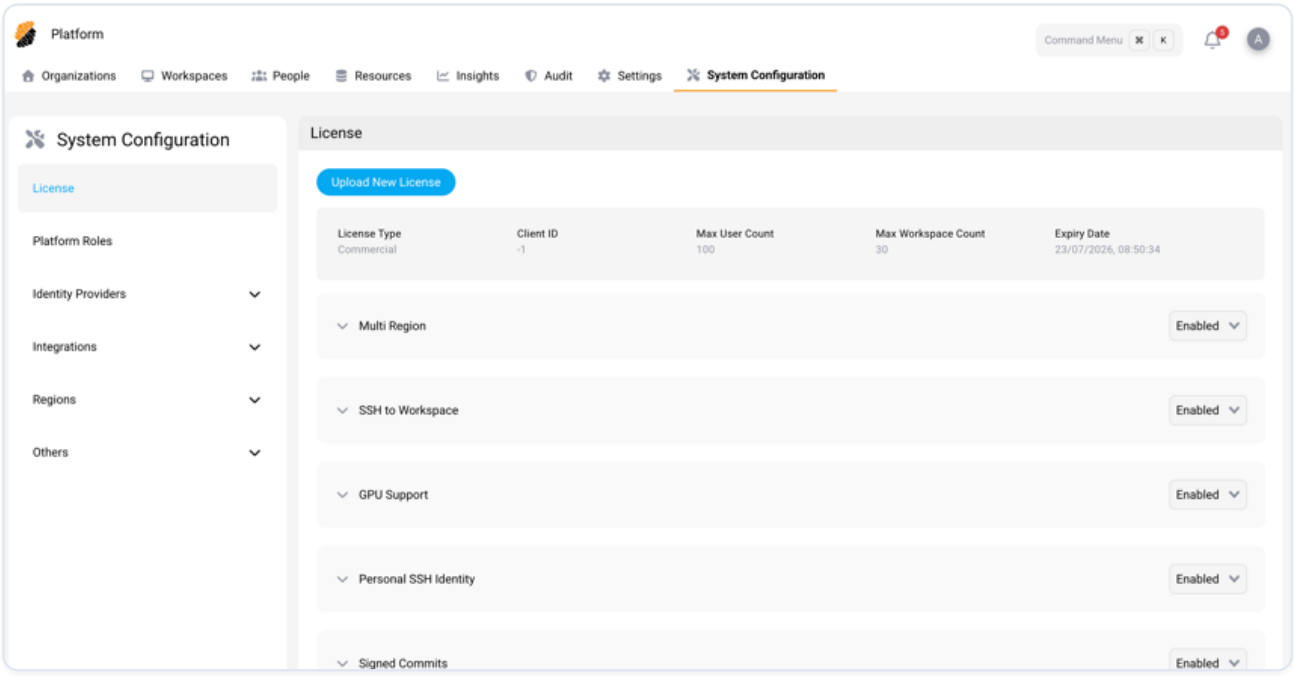
PÁGINA	QUÉ CUBRE
Licencias	Instale una licencia, revise lo que cubre y active o desactive las funciones con licencia.
La base de datos de SecurSpaces	Qué almacena la base de datos, por qué es crítica, cómo se implementa y cómo operarla de forma segura.

PÁGINA	QUÉ CUBRE
Dimensionamiento de la base de datos	Huella esperada por categoría de datos, una estimación de trabajo y orientación para el aprovisionamiento.
Hacer copia de seguridad de la base de datos	Configure las copias de seguridad de Percona con Helm, acceso a GCS sin clave, instantáneas de mongodump y copias de seguridad de servicios alojados.
Restaurar la base de datos	Ponga la plataforma en estado inactivo, restaure los datos, reoriente SecurSpaces y valide.
Análisis	Descargue informes del sistema y registros de uso de la plataforma.
Uso de recursos del espacio de trabajo(/es-es/securspaces/administer/operations/workspace-usage.html)	Datos históricos de CPU y memoria del espacio de trabajo para el dimensionamiento adecuado y el análisis de tendencias.

Licensing

Su licencia tiene dos funciones: permite que su instalación se ejecute y decide qué características y límites se aplican. En la página **Licencia**, instala su licencia y ve exactamente lo que cubre.

Encuentre esta página en **Configuración del sistema > Licencia**.



Revise su licencia

Cuando una licencia está activa, la fila de resumen muestra los detalles más importantes:

CAMPO	DESCRIPCIÓN
Tipo de licencia	El tipo de licencia, como Interna, Comercial, Edición Comunitaria o VM de 1 clic.
ID de cliente	El identificador de su organización.
Recuento máximo de usuarios	Cuántos usuarios puede registrar en la plataforma.
Recuento máximo de espacios de trabajo	Cuántos espacios de trabajo puede contener la plataforma.
Fecha de caducidad	Cuando la licencia caduca.

Cargar una nueva licencia

Puede instalar su licencia de dos maneras:

- **Licencia en línea** — La plataforma obtiene y actualiza su licencia automáticamente desde el servidor de licencias de Citrix. Utilice esta opción cuando la plataforma pueda acceder al servidor de licencias.

- **Licencia de archivo** — Usted carga un archivo de licencia manualmente. Utilice esta opción para instalaciones aisladas o sin conexión que no puedan acceder al servidor de licencias.

Para instalar o reemplazar una licencia:

1. Vaya a **Configuración del sistema > Licencia**.
2. Seleccione **Cargar nueva licencia**.
3. Lea y acepte los **Términos y condiciones**.
4. Elija cómo instalarla:
    - Para una licencia en línea, seleccione **Licencia en línea**. La plataforma la obtiene y la verifica desde el servidor de licencias.
    - Para una licencia de archivo, seleccione **Licencia de archivo** y elija su archivo de licencia.
5. Confirme la carga.

La fila de resumen se actualiza para mostrar su nueva licencia.

> **Nota:**
>
> Si tiene una licencia en línea y una de archivo, la en línea tiene prioridad.

Activar o desactivar funciones

La página de Licencia también enumera las funciones que cubre su licencia. Cada una muestra su estado actual, que puede cambiar:

- **Activado** — Todo el mundo puede usar la función.
- **Desactivado** — La función está desactivada.
- **Activado para usuarios seleccionados** — Solo los usuarios o grupos que elija pueden usarlo.
- **Activado para SO seleccionados** — Solo los sistemas operativos que elija pueden usarlo, donde sea aplicable.

> **Importante:**

Solo puede gestionar las funciones que cubre su licencia. Dentro de una función cubierta, puede cambiar su estado y ampliar el conjunto de usuarios o grupos a los que se aplica.

Estas son las funciones que puede gestionar desde esta página:

FUNCIÓN	QUÉ HACE
SSH a espacio de trabajo	Permite a los propietarios de espacios de trabajo conectarse a sus espacios de trabajo a través de SSH. Consulte Acceso SSH a espacios de trabajo.
Multirregión	Activa las implementaciones multirregión. Cuando está activado, aparece el área Regiones. Consulte Implementar SecurSpaces en varias regiones.
API REST	Permite el acceso a la API REST de Citrix SecurSpaces™. Consulte API.
Identidad SSH personal	Permite a los usuarios añadir y gestionar varias identidades SSH en su cuenta.
Confirmaciones firmadas	Activa las confirmaciones de Git firmadas desde los espacios de trabajo.
Compatibilidad con GPU	Activa los espacios de trabajo habilitados para GPU. Consulte Configurar un espacio de trabajo habilitado para GPU en AKS.
Usuario de desarrollo interno	Activa las cuentas de usuario de desarrollador interno.
Docker raíz en Docker	Permite Docker raíz en Docker dentro de los espacios de trabajo.
Imágenes de contenedor persistentes	Habilita las imágenes de contenedor persistentes.
Monitorización de información del usuario	Habilita la monitorización de información por usuario.

FUNCIÓN	QUÉ HACE
Tiempo de ejecución de contenedores Sysbox	Habilita el tiempo de ejecución de contenedores Sysbox.
Aplicación VDI	Habilita la aplicación VDI. Consulte Aplicación VDI.
Permitir descarga de archivos	Permite a los usuarios descargar archivos desde los espacios de trabajo.

Licencias y renovación en línea

Una licencia en línea se mantiene actualizada, por lo que normalmente no hay nada que hacer después de la primera instalación.

COMPORTAMIENTO	DETALLE
Período de validez	Cada licencia en línea es válida durante 21 días
Renovación automática	La plataforma contacta con el servidor de licencias varias veces al día para renovar
Reintento	Una renovación fallida, por ejemplo durante una interrupción de red, se reintenta automáticamente

La plataforma accede al servidor de licencias en `api.enterprise.strong.network` por el puerto 443. Consulte Destinos de red.

Advertencias de caducidad

Si la licencia no se puede renovar, la consola advierte antes de que algo deje de funcionar.

- Cuando la validez cae a 14 días sin una renovación exitosa, aparece un banner de advertencia en la parte superior de la consola.
- El banner indica el problema y hace una cuenta regresiva hasta la fecha de caducidad.

> **Nota:**

> Para entornos aislados (air-gapped), permita que el controlador de SecurSpaces acceda al servidor de licencias a través de su firewall, o solicite una licencia sin conexión para un funcionamiento completamente desconectado.

Información relacionada

- Configuración del sistema
- Regiones
- Destinos de red

The SecurSpaces database

Citrix SecurSpaces™ almacena la configuración y el estado de su plataforma en una base de datos MongoDB. Esta base de datos es el sistema de registro de su implementación. Si se pierde o se corrompe, la plataforma no puede funcionar, incluso cuando todos los demás componentes están sanos.

Esta sección está dirigida a los administradores de plataforma que implementan y operan SecurSpaces. Se asume que está familiarizado con Kubernetes, Helm y su modelo de alojamiento de MongoDB.

TAREA	PÁGINA
Estimar el tamaño de la base de datos	Dimensionamiento de la base de datos
Realizar copias de seguridad, programadas y antes de los cambios	Copia de seguridad de la base de datos
Recuperar desde una copia de seguridad	Restaurar la base de datos

Qué almacena la base de datos

La base de datos de SecurSpaces (nombre predeterminado `strong-network`) contiene los metadatos y el estado que definen su plataforma. **No** almacena el contenido de los espacios de trabajo de los desarrolladores. Los sistemas de archivos de los espacios de trabajo, los volúmenes de Docker y el código fuente residen en las reclamaciones de volumen persistente (PVC) de Kubernetes y en su sistema de control de versiones, no en MongoDB.

La base de datos almacena, entre otras cosas:

- **Organizaciones, proyectos y configuraciones** — configuración de la organización, el proyecto, la plataforma y la región, ordenación de secciones y listas de verificación de configuración.
- **Personas y acceso** — usuarios, grupos, roles, permisos y asignaciones de proveedores de identidad.
- **Definiciones y estado del espacio de trabajo** — especificaciones del espacio de trabajo, estado del ciclo de vida, programaciones, sesiones SSH y los metadatos que vinculan un espacio de trabajo a su proyecto, propietario y volúmenes persistentes.
- **Montajes de datos** — depósitos de datos y definiciones de puntos de montaje del espacio de trabajo.
- **Integraciones** — conexiones al control de código fuente y otros servicios externos, además de sus tokens de OAuth y de acceso.
- **Credenciales y secretos** — claves API y credenciales almacenadas. Por defecto, estos están **cifrados y almacenados en la base de datos**. Si configura HashiCorp Vault, los secretos se almacenan en Vault en lugar de en la base de datos (consulte la siguiente sección).
- **Datos de auditoría y eventos** — registros de seguimiento de auditoría y de eventos, además de uso, informes y agregados de cumplimiento utilizados por Insights y la integración SIEM.

> **Nota** La disposición exacta de la colección es un detalle de implementación interno y puede cambiar entre versiones. Trate la base de datos como una unidad opaca para la copia de seguridad y la restauración — siempre realice una copia de seguridad y restaure la base de datos completa, no colecciones individuales.

Dónde residen los secretos: base de datos vs. HashiCorp Vault

Por defecto, SecurSpaces cifra los secretos y las credenciales y los almacena en la base de datos, utilizando una clave de cifrado interna proporcionada en el momento de la instalación.

Si configura HashiCorp Vault (`platform.hashicorpVault` en los valores de Helm), SecurSpaces almacena los secretos en Vault en lugar de en la base de datos.

Esta distinción es importante para las copias de seguridad: cuando utiliza Vault, una copia de seguridad de la base de datos por sí sola **no** captura sus secretos — también debe hacer una copia de seguridad de Vault. Cuando no utiliza Vault, la copia de seguridad de la base de datos contiene los secretos (cifrados), y debe proteger tanto la copia de seguridad como la clave de cifrado.

Por qué la base de datos es crítica

La base de datos es la única fuente de verdad para la configuración y el estado de la plataforma. Los servicios de SecurSpaces son sin estado por diseño y leen su configuración de MongoDB al inicio y durante la operación. Como resultado:

- **Sin base de datos, no hay plataforma.** Si MongoDB no está disponible, los servicios de SecurSpaces no pueden iniciarse ni atender solicitudes, incluso cuando Kubernetes, la red y el almacenamiento estén en buen estado.
- **La pérdida de configuración es irrecuperable sin una copia de seguridad.** Las organizaciones, proyectos, usuarios, integraciones y metadatos del espacio de trabajo existen solo en la base de datos. Perderla significa reconstruir la configuración de su plataforma desde cero.
- **El acceso al espacio de trabajo depende de ella.** Aunque los sistemas de archivos del espacio de trabajo residen en PVC, los metadatos que asignan un desarrollador a su espacio de trabajo y sus volúmenes residen en la base de datos. Sin esos metadatos, los espacios de trabajo existentes no se pueden volver a adjuntar.

Por estas razones, trate la base de datos como un activo de nivel 1 y crítico para el negocio: ejecútela con redundancia, realice copias de seguridad programadas y pruebe su procedimiento de restauración.

Cómo se implementa la base de datos

SecurSpaces admite tres modelos de alojamiento de MongoDB. Su estrategia de copia de seguridad depende de cuál utilice.

MODELO DE ALOJAMIENTO	CUÁNDO SE UTILIZA	QUIÉN OPERA MONGODB
MongoDB interno (Percona)	Implementado por SecurSpaces en su clúster utilizando el operador de Percona. Se utiliza para pruebas de concepto y evaluación, y en producción donde no hay un servicio gestionado disponible.	Usted
MongoDB externo / alojado	**Recomendado para producción.** SecurSpaces se conecta a una implementación gestionada	El proveedor de servicios gestionados

MODELO DE ALOJAMIENTO	CUÁNDO SE UTILIZA	QUIÉN OPERA MONGODB
	externamente, como MongoDB Atlas.	
Bitnami MongoDB (heredado)	Implementaciones internas antiguas antes del cambio a Percona. Se está eliminando progresivamente.	Usted

El gráfico actualizado incluye **Percona Operator for MongoDB 1.23.0**, **Percona Server for MongoDB 7.0.37-20**, y **Percona Backup for MongoDB (PBM) 2.15.0**. El operador gestiona la base de datos como un `PerconaServerMongoDB` recurso personalizado con `crVersion: 1.23.0`.

Por defecto, la implementación interna utiliza:

- Un conjunto de réplicas de un solo miembro (`rs0`, tamaño `1`). Para producción, aumente el tamaño del conjunto de réplicas a al menos 3 para alta disponibilidad.
- Un volumen persistente de 10 GiB para datos.
- Solicitudes de recursos de 500m CPU / 1 GiB de memoria y límites de 2000m CPU / 4 GiB de memoria.

Nota:

Un servicio gestionado de MongoDB es la ruta más sencilla a producción, porque el proveedor se encarga de la redundancia, las copias de seguridad y el escalado por usted.

La base de datos interna es totalmente compatible en producción y es la elección correcta para implementaciones desconectadas y entornos donde un servicio gestionado no está disponible. La diferencia es de propiedad más que de capacidad: **usted configura y opera su resiliencia.** Los valores predeterminados están configurados para un inicio rápido —un conjunto de réplicas de un solo miembro, con copias de seguridad disponibles pero no activadas—, así que planifique lo siguiente antes de depender de ella:

- Un conjunto de réplicas con más de un miembro, para que la pérdida de un pod o nodo no detenga la plataforma. Consulte Principios operativos.

- Copias de seguridad configuradas, programadas y probadas de restauración. Consulte Realizar copia de seguridad de la base de datos.
- Recursos dimensionados para su propia carga en lugar de los predeterminados. Consulte Dimensionamiento.

Actualizaciones y copias de seguridad internas de Percona

Las actualizaciones desde SDS 2026.9 (operador 1.20.1) deben realizarse una versión menor a la vez. Después de `sds-cli upgrade`, ejecute el `percona-upgrade/upgrade-percona.sh` suministrado para hacer una copia de seguridad de la base de datos, actualice a través de 1.21.2 y 1.22.0, y aplique los CRD 1.23. Luego, ejecute el comando Helm impreso para completar la actualización a 1.23.0. Hem 3 no actualiza los CRD existentes; el script los aplica explícitamente. Consulte Actualización para el procedimiento completo y los comandos de recuperación.

Las copias de seguridad permanecen deshabilitadas por defecto. Configure `perconaServerMongoDB.backup` y `perconaServerMongoDB.serviceAccount` en los valores de Helm para habilitar las copias de seguridad y configurar la cuenta de servicio de la base de datos. El operador 1.23 admite copias de seguridad de GCS sin clave a través de GKE Workload Identity. Conceda acceso al bucket tanto a las cuentas de servicio de Kubernetes de la base de datos como del operador para que las copias de seguridad, las restauraciones y la limpieza de retención funcionen. Consulte Realizar copia de seguridad de la base de datos.

Credenciales internas de Percona MongoDB

El gráfico de Helm almacena las credenciales internas de Percona MongoDB en el `<release>-psmdb-secrets` Secreto de Kubernetes. Deje los valores de la contraseña en `perconaServerMongoDB.adminUsers` vacíos para un funcionamiento normal. En la primera instalación, el gráfico genera las contraseñas. En las actualizaciones posteriores de Helm del lado del servidor, el gráfico reutiliza los valores del Secreto activo en lugar de generar nuevos.

Este comportamiento evita que las actualizaciones rutinarias roten las contraseñas de la base de datos de forma inesperada. Si explícitamente establece una contraseña en el archivo de valores, ese valor configurado tendrá prioridad y rotará la credencial correspondiente. Cuando la credencial del administrador de la base de datos cambia, SecurSpaces reinicia los servicios de la plataforma que la leen para que tomen el Secreto actualizado.

Importante:

> `lookup` puede leer el Secreto existente solo durante una operación de Helm del lado del servidor contra el clúster. La renderización del lado del cliente, incluyendo `helm template`, la renderización GitOps del lado del cliente y `--dry-run=client`, no puede leer el Secreto activo. En esos modos, los valores de contraseña vacíos aún pueden renderizarse como nuevas contraseñas generadas. Utilice actualizaciones de Helm del lado del servidor para la implementación interna de Percona, o fije las contraseñas de la base de datos de Percona en su archivo de valores.

Principios operativos

- Ejecute MongoDB con redundancia en producción — un servicio gestionado, o un conjunto de réplicas de Percona con más de un miembro que usted opere — nunca un solo miembro.
- Habilite las copias de seguridad continuas / con recuperación a un momento dado, no solo las instantáneas periódicas.
- Almacene las copias de seguridad fuera del clúster y en un dominio de fallo separado.
- Cifre las copias de seguridad en reposo y en tránsito, y restrinja el acceso al almacenamiento de copias de seguridad.
- Realice una copia de seguridad de HashiCorp Vault junto con la base de datos cuando Vault almacene sus secretos.
- Siempre realice una copia de seguridad antes de las actualizaciones, migraciones y cambios importantes de configuración.
- Supervise el tamaño de la base de datos. Los datos de auditoría en la base de datos caducan automáticamente después de 360 días; reenvíe los eventos a su SIEM si necesita retención más allá de ese período.
- Pruebe las restauraciones según un cronograma y documente el manual de procedimientos.

Información relacionada

- Arquitectura
- Requisitos del sistema
- Configurar una base de datos externa
- Actualizar

Database sizing

Utilice estas cifras para dimensionar la base de datos de Citrix SecurSpaces™ para la implementación inicial, luego verificar contra el uso real durante su PoC y en producción.

Dado que la base de datos contiene metadatos y no el contenido del espacio de trabajo, permanece pequeña en relación con el almacenamiento de su espacio de trabajo. La categoría de mayor crecimiento son los **datos de auditoría y eventos**, que SecurSpaces persiste en la misma base de datos.

Qué límites establece realmente la retención

La base de datos no crece sin límite. SecurSpaces aplica índices TTL de MongoDB, y la ventana de retención difiere según el tipo de datos:

DATOS	RETENCIÓN	EFECTO EN EL TAMAÑO
Eventos de auditoría y seguridad	360 días	La categoría dominante de larga duración
Registros de actividad del sitio web	360 días	Crece con la actividad del usuario
Registros de errores	30 días	Insignificante en estado estable
Muestras en bruto de uso de Kubernetes	14 días	Acotado independientemente del número de espacios de trabajo
Actividad del proyecto, registros de depuración, registros cron	7 días	Insignificante

Esto es importante al dimensionar para una implementación más grande. El muestreo de uso por espacio de trabajo son los datos que más escalan con el número de espacios de trabajo, y se descartan después de 14 días, por lo que no se acumulan. Los eventos de red también se almacenan como resúmenes con un recuento de solicitudes en lugar de un documento por solicitud.

El resultado es que la base de datos tiende a un estado estable de aproximadamente un año de datos de auditoría y eventos, además de su configuración relativamente estática.

Huella estimada

La siguiente estimación es para un entorno de **500 desarrolladores que utilizan 500 espacios de trabajo**. Para implementaciones más pequeñas, incluida una prueba de concepto, consulte Implementaciones más pequeñas.

CATEGORÍA DE DATOS	HUELLA APROXIMADA	NOTAS
Organizaciones, proyectos, configuración	< 100 MB	Escala con el número de proyectos, no con el número de espacios de trabajo.
Usuarios, grupos, roles	< 250 MB	Escala con el número de usuarios.
Metadatos de espacios de trabajo y plantillas	< 500 MB	Escala con el número de espacios de trabajo y versiones de plantillas.
Credenciales y claves de API	< 250 MB	Menor si HashiCorp Vault almacena sus secretos.
Registros de auditoría, eventos, uso e informes	5–25 GB (estado estable)	Categoría más grande, limitada por la caducidad de 360 días. Varía más según la actividad de la plataforma.
Índices y sobrecarga	25–50% del tamaño de los datos	Índices de MongoDB más la sobrecarga del conjunto de trabajo.

Estimación de trabajo: la configuración y los metadatos para 500 desarrolladores y 500 espacios de trabajo son del orden de 1 GB. Con un año de datos de auditoría y eventos más índices, planifique **10–40 GB** de datos reales.

La horquilla es amplia porque el nivel de actividad, no el número de usuarios, es lo que impulsa la categoría más grande. Una plataforma donde cada espacio de trabajo funciona todo el día con la monitorización de red habilitada se sitúa en la parte superior de ese rango; una utilizada durante unas pocas horas al día se sitúa cerca de la parte inferior.

Guía de aprovisionamiento

- **Almacenamiento:** Aprovisione **al menos 100 GiB** para el volumen de datos a esta escala. El margen cubre el crecimiento, el oplog de replicación, los índices y el espacio temporal utilizado durante la compactación y la restauración. El valor predeterminado del gráfico de 10 GiB solo es adecuado para entornos PoC pequeños o de corta duración.
- **Memoria:** Dimensione MongoDB para que el conjunto de trabajo —documentos e índices a los que se accede con frecuencia— quepa en la caché de WiredTiger. Aprovisione hasta el **límite de 4 GiB** en lugar de la solicitud de 1 GiB, y supervise la presión de la caché. Las consultas de auditoría durante un período prolongado son lo que la impulsa.
- **CPU:** Aprovisione hasta el **límite de 2 núcleos** en lugar de la solicitud de 500m. La carga en estado estable es baja; los picos son consultas de informes, restauraciones y compactación.
- **Control de crecimiento:** La caducidad de 360 días es fija y no configurable. Para una retención más larga, reenvíe los eventos a su SIEM. La copia en la base de datos sigue caducando a los 360 días. Consulte Integración de SIEM.

> **Nota**
>
> Estas son cifras de planificación para una carga de trabajo típica de este tamaño. Cada entorno es diferente, y algunos tienen una huella mayor. Úselas para el dimensionamiento inicial, luego supervise el tamaño y el crecimiento reales de la base de datos durante su PoC y en producción, y ajuste según sea necesario.

Implementaciones más pequeñas

ENTORNO	DATOS ESTIMADOS	APROVISIONAMIENTO
50 desarrolladores, 50 espacios de trabajo (PoC)	1–3 GB	Al menos 20 GiB
100 desarrolladores, 100 espacios de trabajo	2–6 GB	Al menos 20 GiB
500 desarrolladores, 500 espacios de trabajo	10–40 GB	Al menos 100 GiB

El valor predeterminado del gráfico de 10 GiB es suficiente solo para una prueba de concepto de corta duración. Un piloto que se ejecuta durante meses acumula datos de auditoría todo el tiempo, y ninguno de ellos caduca hasta el día 360; por lo tanto, una prueba de concepto que comienza cómodamente dentro de los 10 GiB aún puede superarlo antes de que alguien decida si comprar. Aprovisionar 20 GiB desde el principio evita redimensionar un volumen a mitad de la evaluación.

Tenga en cuenta que el almacenamiento no se escala con los usuarios de la misma manera que los datos. La mayor parte de los 20 GiB es espacio libre para el oplog, los índices y el espacio temporal que necesita una restauración, y esos requisitos apenas cambian entre 50 y 100 desarrolladores.

Información relacionada

- La base de datos de SecurSpaces
- Dimensionamiento
- Requisitos del sistema

Back up the database

Realice una copia de seguridad de la base de datos de Citrix SecurSpaces™ antes de actualizaciones, migraciones y cambios de configuración importantes, y con una programación recurrente en producción. Si utiliza HashiCorp Vault para secretos, realice una copia de seguridad de Vault con la misma programación.

Local y autogestionado (Percona MongoDB interno)

> **Importante:**

> Las copias de seguridad están **deshabilitadas de forma predeterminada** en la base de datos interna. Si la ejecuta en producción, la habilitación, programación y prueba de restauración de las mismas es su responsabilidad. Consulte La base de datos de SecurSpaces.

> Utilice **Percona Backup for MongoDB (PBM)** como su mecanismo de copia de seguridad principal y programado. Utilice una `mongodump` manual solo como una instantánea secundaria de un momento dado antes de un cambio específico.

Principal: Percona Backup for MongoDB (PBM)

PBM es la herramienta de copia de seguridad integrada en Percona Operator. Admite copias de seguridad lógicas y físicas a petición y programadas y recuperación a un momento dado en un almacén de objetos externo (Amazon S3, Azure Blob Storage, Google Cloud Storage o cualquier almacén compatible con S3).

El gráfico con **Percona Operator 1.23.0** incluye **PBM 2.15.0**. Las copias de seguridad permanecen deshabilitadas de forma predeterminada. Configúrelas en sus valores de Helm con `perconaServerMongoDB.backup`, incluyendo `enabled`, almacenamiento, programaciones, retención y recuperación a un momento dado (PITR). Configure la cuenta de servicio de Kubernetes de la base de datos a través de `perconaServerMongoDB.serviceAccount`. El gráfico representa estas configuraciones en los recursos de Percona.

Mantenga la configuración de la copia de seguridad en los valores utilizados para las actualizaciones posteriores de Helm. Si editó `spec.backup` directamente, traslade esa configuración a `perconaServerMongoDB.backup` antes de aplicar el nuevo gráfico. No confíe en las ediciones de recursos personalizados como fuente de configuración para futuras actualizaciones.

Para una implementación existente en el operador 1.20.1, primero complete la actualización paso a paso a 1.23.

Consulte la documentación de copia de seguridad de Percona Operator para obtener la referencia autorizada:

- Descripción general de las copias de seguridad: https://docs.percona.com/percona-operator-for-mongodb/backups.html
- Configurar almacenamiento: https://docs.percona.com/percona-operator-for-mongodb/backups-storage.html
- Copias de seguridad a petición: https://docs.percona.com/percona-operator-for-mongodb/backups-ondemand.html
- Copias de seguridad programadas: https://docs.percona.com/percona-operator-for-mongodb/backups-scheduled.html

EJEMPLO: HABILITAR PBM Y HACER UNA COPIA DE SEGURIDAD EN AMAZON S3

Este ejemplo práctico sigue la guía de almacenamiento del operador de Percona. Reemplace `<release>` con el nombre de su versión de Helm de SecurSpaces y `<namespace>` con su

espacio de nombres de SecurSpaces. Ejecute `kubectl get psmdb -n <namespace>` para confirmar el nombre de su clúster; para SecurSpaces es `<release>-psmdb-db`.

1. Cree un secreto con sus credenciales de S3. Guárdelo como `backup-s3-secret.yaml` (los valores se codifican automáticamente en base64 cuando usa `stringData`):

```
apiVersion: v1

kind: Secret

metadata:

  name: sds-backup-s3

type: Opaque

stringData:

  AWS_ACCESS_KEY_ID: "<your-access-key-id>"

  AWS_SECRET_ACCESS_KEY: "<your-secret-access-key>"
```

```
kubectl apply -f backup-s3-secret.yaml -n <namespace>
```

2. Habilite las copias de seguridad y defina el almacenamiento en sus valores de Helm. Agregue lo siguiente al archivo de valores utilizado para su implementación. La entrada de almacenamiento hace referencia al secreto creado anteriormente:

```
perconaServerMongoDB:

  backup:

    enabled: true

    storages:

      s3-primary:

        type: s3

        s3:
```

```
        bucket: <your-backup-bucket>

        region: <your-region>        # for example, eu-central-1

        prefix: sds/strong-network   # optional sub-folder in the bucket

        credentialsSecret: sds-backup-s3
```

Aplique los valores usando su comando normal de actualización de Helm y la misma versión del gráfico. Por ejemplo:

```
helm upgrade <release> ./ninjahchart-<version>.tgz -n <namespace> -f
<your-values.yaml>
```

Nota En AWS EKS puede conceder acceso al bucket con un rol de IAM para la cuenta de servicio (IRSA) y omitir `credentialsSecret`. Para Azure Blob o Google Cloud Storage, use el tipo de almacenamiento `azure` o `gcs` en lugar de `s3`. Para el acceso a GCS sin clave, consulte Identidad de carga de trabajo de GCS.

3. Realice una copia de seguridad bajo demanda. Cree un recurso `PerconaServerMongoDBBackup` que haga referencia a su clúster y almacenamiento. Guárdelo como `sds-backup.yaml`:

```
apiVersion: psmdb.percona.com/v1

kind: PerconaServerMongoDBBackup

metadata:

  name: sds-backup-2026-07-02

  namespace: <namespace>

spec:

  clusterName: <release>-psmdb-db

  storageName: s3-primary
```

```
  type: logical                       # logical is the default; physical
is also supported
```

```
kubectl apply -f sds-backup.yaml
```

4. verificar que la copia de seguridad se completó. Rastree el recurso de copia de seguridad hasta que `STATUS` sea `ready`:

```
kubectl get psmdb-backup -n <namespace>
```

```
NAME                    CLUSTER               STORAGE      DESTINATION
                   TYPE      STATUS   AGE

sds-backup-2026-07-02  <release>-psmdb-db   s3-primary   s3://<bucket>/
sds/strong-network/… logical   ready    2m
```

5. (Recomendado) Agregue una programación y recuperación a un punto en el tiempo. Para una protección continua, agregue una tarea de copia de seguridad y habilite PITR en la misma sección `perconaServerMongoDB.backup` de su archivo de valores. Mantenga la definición de almacenamiento del paso anterior:

```
perconaServerMongoDB:

  backup:

    enabled: true

    pitr:

      enabled: true                   # continuous point-in-time recovery

    tasks:

      - name: daily-s3

        enabled: true

        schedule: "0 2 * * *"         # every day at 02:00 (cron)
```

```
        storageName: s3-primary

        retention:

          type: count

          count: 7                    # retain the 7 most recent
scheduled backups

          deleteFromStorage: true
```

Aplique los valores actualizados con su comando de actualización de Helm y confirme que las nuevas copias de seguridad aparecen según lo programado. Como buena práctica, almacene las copias de seguridad en un dominio de falla diferente al del clúster —una región o cuenta de nube separada— para que una falla del clúster o de la región no destruya también sus copias de seguridad.

> **Nota** Volver a aplicar los mismos valores de Helm conserva la configuración de la copia de seguridad. En la validación de GKE, una segunda actualización de Helm con valores sin cambios no causó reinicios y las copias de seguridad continuaron.

Identidad de carga de trabajo de GCS

Percona Operator **1.23.0** admite copias de seguridad sin clave en Google Cloud Storage (GCS) utilizando **Workload Identity Federation para GKE**. Use el tipo de almacenamiento nativo `gcs` y omita `gcs.credentialsSecret` para que PBM use las credenciales predeterminadas de la aplicación. No se requiere ninguna clave JSON de cuenta de servicio ni clave HMAC.

PREPARE GKE Y EL ACCESO AL BUCKET

Necesita un clúster de GKE con Workload Identity habilitado, el servidor de metadatos de GKE habilitado en los grupos de nodos que ejecutan la base de datos y los pods del operador, un bucket de copia de seguridad de GCS y permiso para administrar la política de IAM de ese bucket. Consulte la guía de configuración de Workload Identity de Google.

Utilice `perconaServerMongoDB.serviceAccount` en los valores del gráfico para configurar la cuenta de servicio de la base de datos. Inspeccione el gráfico de destino para ver sus opciones de cuenta de servicio antes de configurarlas:

```
helm show values ./ninjahchart-<version>.tgz
```

Conceda acceso al bucket a **ambas** cuentas de servicio de Kubernetes: la utilizada por los pods de la base de datos y la utilizada por el operador de Percona. PBM necesita acceso para la copia de seguridad y la restauración; el operador también necesita acceso para eliminar las copias de seguridad caducadas de GCS. Descubra las cuentas de los pods en ejecución en lugar de asumir nombres:

```
kubectl get pods -n <namespace> \

  -o custom-
columns='POD:.metadata.name,SERVICE_ACCOUNT:.spec.serviceAccountName'
```

El siguiente ejemplo concede acceso a objetos a nivel de bucket directamente a los dos principales de la cuenta de servicio de Kubernetes. Reemplace los marcadores de posición con el ID y el número del proyecto del clúster de GKE, su espacio de nombres, bucket, y los nombres de cuenta reales. `roles/storage.objectUser` permite la lectura, escritura, listado y eliminación de objetos.

```
PROJECT_ID="<gke-project-id>"

PROJECT_NUMBER="<gke-project-number>"

NAMESPACE="<namespace>"

GCS_BUCKET="<backup-bucket>"

DATABASE_KSA="<database-service-account>"

OPERATOR_KSA="<operator-service-account>"

POOL="projects/${PROJECT_NUMBER}/locations/global/workloadIdentityPools/$
{PROJECT_ID}.svc.id.goog"



for KSA in "$DATABASE_KSA" "$OPERATOR_KSA"; do

  gcloud storage buckets add-iam-policy-binding "gs://${GCS_BUCKET}" \
```

```
    --member="principal://iam.googleapis.com/${POOL}/subject/ns/$
{NAMESPACE}/sa/${KSA}" \

    --role="roles/storage.objectUser"

done
```

Esta configuración de principal directo no requiere una clave de cuenta de servicio de Google ni la suplantación de identidad de la cuenta de servicio. Si el operador se ejecuta en un espacio de nombres diferente, utilice ese espacio de nombres en su principal de IAM. Si cambia la cuenta de servicio de la base de datos en los valores de Helm, conceda acceso también a la nueva cuenta.

CONFIGURAR COPIAS DE SEGURIDAD EN LOS VALORES DE HELM

Combine este ejemplo con los valores de su implementación junto con `perconaServerMongoDB.serviceAccount`. Habilita copias de seguridad lógicas cada 10 minutos, captura continua de oplog PITR y retención de dos copias de seguridad programadas. Ajuste la programación y la retención a sus requisitos de recuperación:

```
perconaServerMongoDB:

  backup:

    enabled: true

    storages:

      gcs-wi:

        type: gcs

        gcs:

          bucket: <backup-bucket>

          prefix: sds/mongodb

    pitr:

      enabled: true

    tasks:
```

```
    - name: gcs-every-10-minutes
      enabled: true
      schedule: "*/10 * * * *"
      storageName: gcs-wi
      type: logical
      retention:
        type: count
        count: 2
        deleteFromStorage: true
```

Aplique los valores con su comando normal de actualización de Helm después de completar la actualización de Percona 1.23. Si migra desde el acceso a GCS basado en claves, elimine `credentialsSecret` de la configuración `gcs` del almacenamiento en sus valores y verificar que no esté presente en el recurso personalizado resultante. Un Secret de credenciales configurado tiene prioridad sobre Workload Identity.

VERIFICAR COPIAS DE SEGURIDAD, RETENCIÓN Y RESTAURACIÓN

1. Cree la `PerconaServerMongoDBBackup` bajo demanda que se muestra en el ejemplo de S3 anterior, utilizando un nombre único y `storageName: gcs-wi`. Espere a `ready` y confirme que la copia de seguridad está presente en el bucket.
2. Confirme que las copias de seguridad programadas se completan y que aparecen fragmentos de oplog continuos para PITR. PITR requiere una copia de seguridad base completada y cobertura de oplog para el tiempo de recuperación elegido.
3. Confirme que la retención elimina las copias de seguridad caducadas tanto de Kubernetes como de GCS. Si quedan objetos en GCS, compruebe los permisos del bucket para la cuenta de servicio del **operador**, así como para la cuenta de la base de datos.
4. Mantenga los mismos valores de copia de seguridad para las actualizaciones posteriores de Helm y verificar que las copias de seguridad continúan después.
5. Pruebe la restauración en una implementación de reemplazo, incluida una restauración a un segundo elegido al usar PITR. Consulte Restaurar la base de datos.

Este flujo se validó en GKE con concesiones directas de bucket a ambas cuentas de servicio de Kubernetes, copias de seguridad bajo demanda y programadas, PITR, recuento de retención `2`, y una actualización repetida de Helm. La recuperación también se validó después de eliminar la implementación y los volúmenes, reinstalar y restaurar a un segundo elegido; los datos recuperados coincidieron y la plataforma estaba operativa.

Para obtener detalles de autenticación y almacenamiento, consulte la guía de copia de seguridad de GCS de Percona.

Secundario: instantánea lógica con `mongodump`

El kit de actualización de Percona crea un archivo `mongodump` automáticamente antes de cambiar de versión e incluye scripts de restauración y eliminación coincidentes. Conserve este archivo previo a la actualización hasta que se complete la validación de la plataforma. Es independiente de sus copias de seguridad PBM programadas y del almacenamiento PITR.

`mongodump` / `mongorestore` son las herramientas oficiales de la base de datos MongoDB, y SecurSpaces las utiliza en su propio procedimiento de migración de conjunto de réplicas, por lo que este es un método compatible, no una solución alternativa.

Es seguro para **instantáneas ad hoc y en estado de inactividad** (por ejemplo, inmediatamente antes de una actualización) si sigue estas reglas:

- **Ponga en inactividad las escrituras antes de volcar, o vuelque desde un miembro secundario.** `mongodump` solo garantiza la coherencia entre colecciones cuando no se está escribiendo en la base de datos. La forma más sencilla de obtener una instantánea limpia es escalar primero los servicios de SecurSpaces a `0` (el mismo paso de inactividad utilizado en el procedimiento de restauración) y luego volcar. `mongodump` no puede producir una instantánea de punto en el tiempo entre colecciones de una única base de datos en un sistema en vivo; para copias de seguridad en línea y de punto en el tiempo, utilice PBM en su lugar.
- **Almacene el archivo fuera del clúster** y protéjalo (contiene secretos cifrados a menos que use Vault).
- **Restaure solo en una plataforma en estado de inactividad** (consulte la sección de restauración), y nunca utilice indicadores destructivos como `--drop` contra una base de datos en vivo y en uso.

No es un reemplazo para la recuperación ante desastres programada y de punto en el tiempo; PBM (interno) o las copias de seguridad de su servicio gestionado siguen siendo la estrategia

principal. Utilice `mongodump` para capturar una instantánea conocida como buena antes de un cambio arriesgado.

```
# Identify the Percona pods

kubectl get psmdb

kubectl get pods -l app.kubernetes.io/name=percona-server-mongodb



# Confirm which pod is primary (look for "[direct: primary]" in the
prompt)

kubectl exec -it <pod>-rs0-0 -- mongosh \

  --authenticationDatabase admin --username <admin-user> --password
<admin-password>



# Dump the strong-network database from the primary (quiesce writes first)

kubectl exec -it <primary-pod> -- mongodump \

  --db strong-network \

  --username <admin-user> --password <admin-password> \

  --authenticationDatabase admin \

  --gzip --archive=/tmp/strong-network-backup.gz



# Copy the archive off the pod

kubectl cp <primary-pod>:/tmp/strong-network-backup.gz strong-network-
backup.gz
```

Para referencia de la herramienta, consulte la documentación de MongoDB para `mongodump`: https://www.mongodb.com/docs/database-tools/mongodump/

Servicios de MongoDB alojados

Cuando utiliza un servicio de MongoDB gestionado, el proveedor suministra las herramientas de copia de seguridad. Habilítelo y configúrelo según sus objetivos de recuperación (RPO/RTO).

SecurSpaces es compatible con los servicios de MongoDB alojados en los tres principales hiperescaladores (AWS, Azure, y Google Cloud). MongoDB Atlas está disponible en los tres y es la opción a la que hacen referencia las guías de implementación de SecurSpaces. Utilice las copias de seguridad en la nube de Atlas con la copia de seguridad continua (punto en el tiempo) habilitada:

- Descripción general de las copias de seguridad en la nube de Atlas: https://www.mongodb.com/docs/atlas/backup/cloud-backup/overview/
- Descripción general de la restauración de Atlas: https://www.mongodb.com/docs/atlas/backup/cloud-backup/restore-overview/

Si utiliza un servicio nativo de la nube compatible con MongoDB en lugar de Atlas, habilite su función de copia de seguridad utilizando la documentación del proveedor que se indica a continuación.

PLATAFORMA	SERVICIO	DOCUMENTACIÓN OFICIAL DE COPIA DE SEGURIDAD
AWS	Amazon DocumentDB o MongoDB Atlas en AWS	Copia de seguridad y restauración en Amazon DocumentDB · Copias de seguridad en la nube de Atlas
Azure	Azure Cosmos DB para MongoDB o MongoDB Atlas en Azure	Copia de seguridad en línea y restauración a petición (Cosmos DB) · Fiabilidad en Azure Cosmos DB para MongoDB (vCore)
GCP	MongoDB Atlas en Google Cloud	Copias de seguridad en la nube de Atlas. Google Cloud no tiene un MongoDB administrado propio.

Orientación general para servicios alojados:

- Active la copia de seguridad **continua / con recuperación a un momento dado**, no solo las instantáneas diarias, para minimizar la pérdida de datos.
- Establezca un período de retención que cumpla con sus requisitos de cumplimiento y recuperación.
- Pruebe periódicamente a restaurar una instantánea en un clúster que no sea de producción.

Información relacionada

- Restaurar la base de datos
- La base de datos de SecurSpaces
- Actualizar

Restore the database

La restauración de la base de datos de Citrix SecurSpaces™ requiere una ventana de mantenimiento: la plataforma debe estar en estado de inactividad para que los servicios no escriban en la base de datos durante la restauración. El procedimiento para el paso 2 depende de su modelo de alojamiento.

Paso 1: Poner la plataforma en estado de inactividad

Reduzca los servicios de SecurSpaces para que nada escriba en la base de datos durante la restauración. La implementación de MongoDB en sí misma sigue en ejecución.

```
# Stop the SecurSpaces application services (leave MongoDB running)

kubectl scale deployment \

  <release>-central-service <release>-workspace-api <release>-coordinator
\

  <release>-frontend <release>-proxy \

  --replicas=0 -n <namespace>
```

> **Nota** Estos son los cinco despliegues de servicio en una plataforma principal de SecurSpaces. Un despliegue de región externa solo ejecuta `<release>-workspace-api` y `<release>-proxy`. Confirme lo que está presente con `kubectl get deploy -n <namespace>` antes de escalar.

Paso 2: Restaurar los datos

MongoDB interno de Percona — desde una copia de seguridad de PBM

Utilice el flujo de trabajo de restauración del Operador de Percona: cree un recurso `PerconaServerMongoDBRestore` que haga referencia a la copia de seguridad por nombre (o a un punto en el tiempo) y espere a que el operador complete la restauración. Guarde como `sds-restore.yaml`:

```
apiVersion: psmdb.percona.com/v1

kind: PerconaServerMongoDBRestore

metadata:

  name: sds-restore-2026-07-02

  namespace: <namespace>

spec:

  clusterName: <release>-psmdb-db

  backupName: sds-backup-2026-07-02        # the
PerconaServerMongoDBBackup to restore
```

```
kubectl apply -f sds-restore.yaml

kubectl get psmdb-restore -n <namespace>   # wait for STATUS: ready
```

Para restauraciones a un punto en el tiempo y opciones completas, consulte la documentación de restauración de Percona: https://docs.percona.com/percona-operator-for-mongodb/backups-restore.html

Para copias de seguridad de GCS con Workload Identity, configure el despliegue de reemplazo con acceso al mismo bucket y prefijo. Conceda acceso al bucket tanto a sus cuentas de servicio de Kubernetes de base de datos como de operador, y utilice los mismos valores `perconaServerMongoDB.backup` y `perconaServerMongoDB.serviceAccount` según corresponda para el entorno de reemplazo. Consulte GCS Workload Identity.

Después de perder el despliegue y sus volúmenes, el antiguo recurso de copia de seguridad de Kubernetes podría dejar de existir. Utilice el procedimiento de restauración desde almacenamiento de Percona en lugar de hacer referencia a un `backupName` que falta. Para PITR, elija un momento cubierto por una copia de seguridad base completada y los fragmentos de oplog almacenados. La validación de GKE incluyó la eliminación del despliegue y los volúmenes, la reinstalación y la recuperación a un segundo elegido con datos coincidentes.

Copia de seguridad del kit de actualización de Percona

Para un archivo tomado por `percona-upgrade/upgrade-percona.sh`, utilice el script de restauración correspondiente del kit de instalación después de poner la plataforma en estado de inactividad. Ejecútelo desde el directorio compartido donde el kit y el archivo están disponibles:

```
./percona-upgrade/restore-percona-backup.sh <namespace> <release>
<backup>.archive.gz
```

Por ejemplo, con el espacio de nombres `default` y la versión `release`:

```
./percona-upgrade/restore-percona-backup.sh default release
<backup>.archive.gz
```

El script restaura **solo los datos**. No degrada el operador, los CRD, MongoDB o PBM. Continúe con los pasos 3 y 4 a continuación para restaurar la plataforma y validarla. Una vez validada, elimine la copia de seguridad de actualización del directorio donde se creó:

```
./percona-upgrade/delete-percona-backup.sh
```

Para la secuencia de actualización completa, consulte Actualización.

MongoDB Percona interno — desde un archivo `mongodump`

Diríjase al miembro **principal** del conjunto de réplicas:

```
# Identify the current primary

kubectl get psmdb

kubectl exec -it <pod>-rs0-0 -- mongosh \

  --authenticationDatabase admin --username <admin-user> --password
<admin-password>
```

```
# Copy the archive to the primary pod

kubectl cp strong-network-backup.gz <primary-pod>:/tmp/strong-network-backup.gz



# Restore the strong-network database into the quiesced platform

kubectl exec -it <primary-pod> -- mongorestore \

  --nsInclude='strong-network.*' \

  --username <admin-user> --password <admin-password> \

  --authenticationDatabase admin \

  --gzip --archive=/tmp/strong-network-backup.gz
```

Si está restaurando en una base de datos recién aprovisionada (por ejemplo, después de pasar de un único pod de MongoDB a un conjunto de réplicas de Percona), es posible que también deba recrear el usuario de la base de datos de la aplicación para que SecurSpaces pueda conectarse:

```
kubectl exec -it <primary-pod> -- mongosh \

  --authenticationDatabase admin --username <admin-user> --password <admin-password> \

  --eval "db.createUser({user: '<app-user>', pwd: '<app-password>', roles: [{ db: 'strong-network', role: 'readWrite' }], mechanisms: ['SCRAM-SHA-1']});" \

  strong-network
```

MongoDB alojado — restaurar con las herramientas del proveedor

Restaure la instantánea o el punto en el tiempo utilizando la consola o CLI del proveedor, luego anote el punto final de conexión de la implementación restaurada (a menudo es un host **nuevo**):

- **MongoDB Atlas** — restaure una instantánea o un punto en el tiempo en el clúster existente o en un nuevo clúster: https://www.mongodb.com/docs/atlas/backup/cloud-backup/restore-overview/
- **Amazon DocumentDB** — restaure desde una instantánea o un punto en el tiempo en un nuevo clúster: https://docs.aws.amazon.com/documentdb/latest/developerguide/backup_restore.html
- **Azure Cosmos DB para MongoDB** — restaure en una nueva cuenta: https://learn.microsoft.com/es-es/azure/cosmos-db/restore-account-continuous-backup

Paso 3: Apuntar SecurSpaces a la base de datos restaurada

SecurSpaces lee su configuración de conexión de MongoDB de los valores de Helm, que el gráfico renderiza en las variables de entorno `MONGO_DB_HOST`, `MONGO_DB_PORT`, `MONGO_DB_NAME`, `MONGO_DB_USER` y `MONGO_DB_PASSWORD` en los pods de servicio. Puede cambiar la base de datos de destino actualizando esos valores y ejecutando `helm upgrade`.

Si restauró a un servicio alojado o a un nuevo punto final (MongoDB externo):

1. En su archivo de valores de Helm, asegúrese de que SecurSpaces esté en modo MongoDB externo y actualice los detalles de conexión:

```
mongodbAuth:
  source: "external"


platform:
  deployPerconaMongoDB: false
  deployBitnamiMongoDB: false
  externalMongodb:
    hostName: "<restored-cluster-host>"     # new endpoint from the
restore
    port: "27017"
    protocol: "mongodb+srv"                 # or "mongodb"
```

```
    additionalParameters: "retryWrites=true&w=majority"
    authMechanism: "SCRAM"                  # or "MONGODB-X509"
    auth:
      database: "strong-network"
      username: "<db-user>"
      password: "<db-password>"
```

Para la autenticación basada en certificados (X.509), configure los campos del certificado en lugar de `username` / `password`. Consulte Configurar MongoDB externo con autenticación X.509.

2. Aplique el cambio:

```
helm upgrade <release> <chart> -n <namespace> -f <your-values.yaml>
```

Si restauró la base de datos interna de Percona en su lugar:

El punto final del servicio no ha cambiado (`<release>-psmdb-db-rs0.<namespace>.svc.cluster.local`), por lo que normalmente no es necesario cambiar los valores de conexión. Si las credenciales cambiaron, actualice el Secret `<release>-psmdb-secrets` en consecuencia.

Paso 4: Vuelva a poner en marcha la plataforma y valide

```
# Scale the services back up (use your normal replica counts)
kubectl scale deployment \
  <release>-central-service <release>-workspace-api <release>-coordinator \
  <release>-frontend <release>-proxy \
  --replicas=1 -n <namespace>
```

```
# Or force a fresh rollout so pods pick up new connection settings

kubectl rollout restart deployment -n <namespace>
```

Luego valide la plataforma:

1. Confirme que los servicios se inician y se conectan a la base de datos (compruebe los registros del pod en busca de errores de conexión de MongoDB).
2. Inicie sesión y confirme que las organizaciones, proyectos, usuarios y espacios de trabajo están presentes.
3. Confirme que los espacios de trabajo existentes se pueden volver a adjuntar.
4. Si utiliza HashiCorp Vault, confirme que los secretos se resuelven correctamente.

Importante Una copia de seguridad que nunca ha restaurado no es una copia de seguridad. Pruebe su procedimiento completo de restauración regularmente en un entorno que no sea de producción para poder confiar en él durante un incidente.

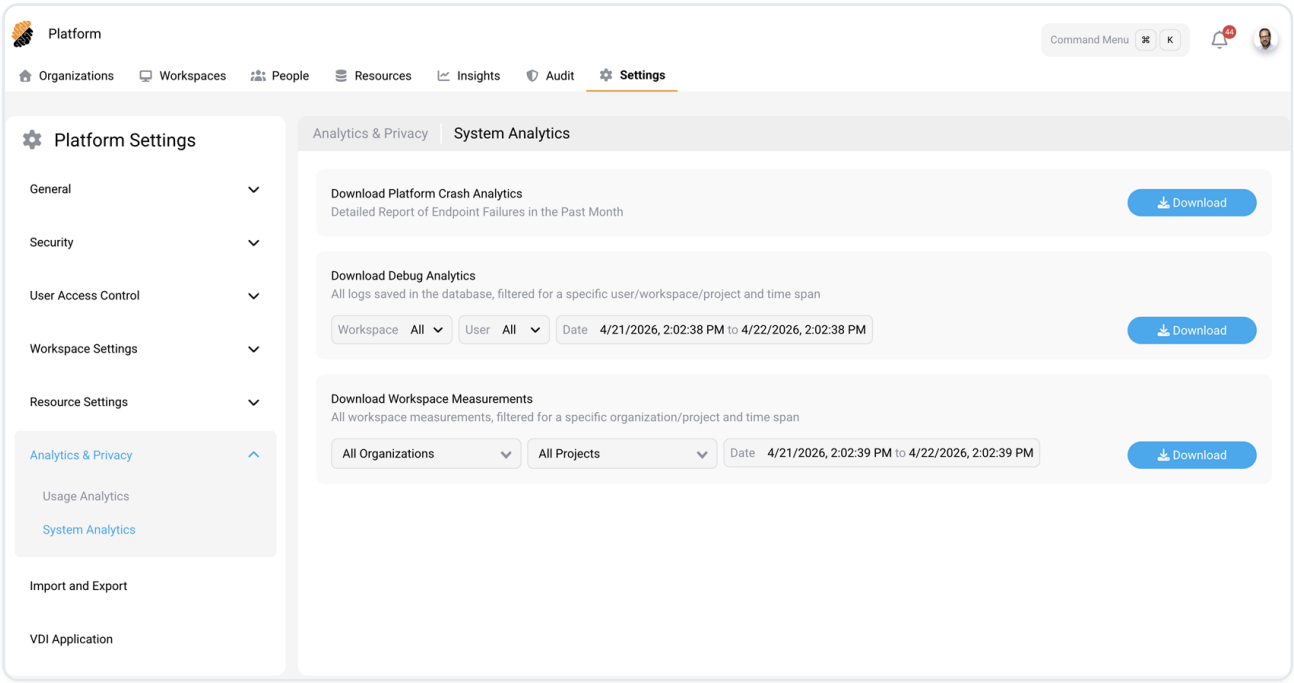
Información relacionada

- Realizar una copia de seguridad de la base de datos
- La base de datos de SecurSpaces

Analytics

Análisis del sistema

Utilice la sección Análisis del sistema para descargar informes y registros detallados de la plataforma Citrix SecurSpaces™. Los informes están disponibles en **Configuración de la plataforma > Análisis y privacidad > Análisis del sistema**.



Descargar análisis de fallos de la plataforma

Descargue un informe de fallos de API y puntos finales de los últimos 30 días. Este informe ayuda a identificar errores recurrentes y facilita la resolución de problemas a nivel de plataforma.

Descargar análisis de depuración

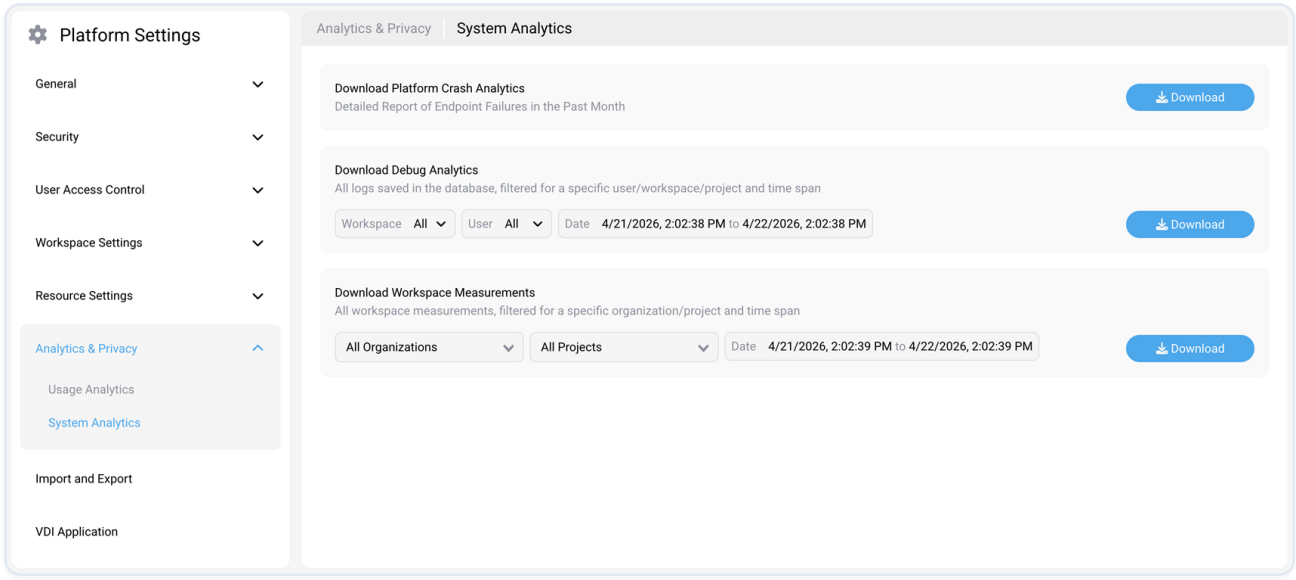
Descargue registros del sistema filtrados por espacio de trabajo, usuario o rango de tiempo. Utilice este informe para la resolución de problemas específicos y el análisis de la causa raíz.

Filtros disponibles:

- **Espacio de trabajo** — Seleccione un espacio de trabajo específico o elija **Todos** para incluir todos los espacios de trabajo.
- **Usuario** — Seleccione un usuario específico o elija **Todos** para incluir a todos los usuarios.
- **Fecha** — Especifique una fecha de inicio y fin para el informe. También está disponible la opción **Todas las fechas**.

Descargar mediciones del espacio de trabajo

Descargue las mediciones de uso de recursos del espacio de trabajo en toda la plataforma. Este informe contiene datos de medición del espacio de trabajo que se pueden filtrar por organización, proyecto y rango de tiempo. Dado que los archivos de medición pueden ser grandes, la plataforma utiliza una conexión WebSocket para facilitar la descarga.



Filtros disponibles:

- **Organización** — Seleccione una organización específica del menú desplegable o mantenga **Todas las organizaciones** para incluir datos de todas las organizaciones. El menú desplegable permite buscar una organización por nombre rápidamente.
- **Proyecto** — Seleccione un proyecto específico o mantenga **Todos los proyectos** para incluir datos de todos los proyectos.
- **Fecha** — Especifique una fecha de inicio y fin para el informe, o seleccione **Todas las fechas** para descargar el historial completo de mediciones.

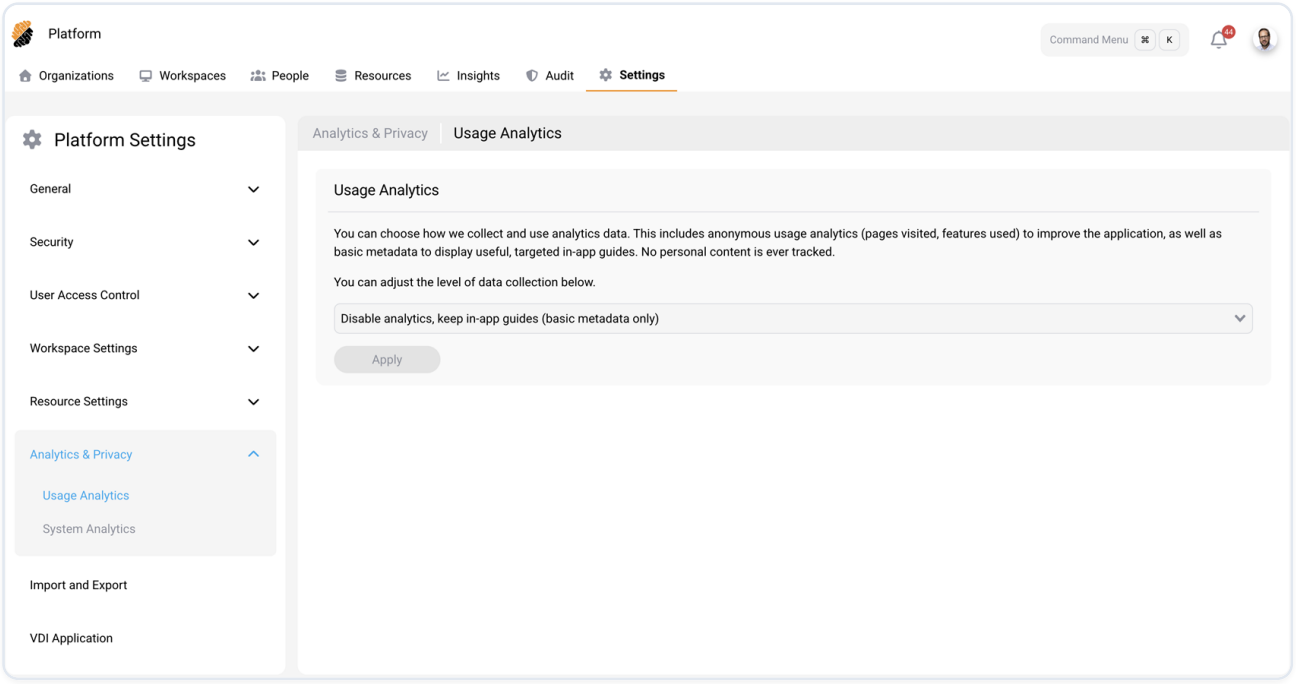
Para descargar las mediciones del espacio de trabajo:

1. Vaya a **Configuración de la plataforma > Análisis y privacidad > Análisis del sistema**.
2. En la sección **Descargar mediciones del espacio de trabajo**, seleccione una organización, un proyecto y un rango de fechas según sea necesario.
3. Seleccione **Descargar**.

> **Nota:**
>
> Solo los administradores de la plataforma y los oficiales de seguridad pueden acceder a la página de Análisis del sistema.

Análisis de uso

La consola de administración de SecurSpaces utiliza Pendo para ofrecer notificaciones en el producto, anuncios de funciones y orientación contextual. También recopila comentarios sobre el producto y telemetría de uso para ayudar a mejorar la experiencia de la plataforma.



Preferencias de recopilación de datos

Puede elegir cómo se recopilan y utilizan los datos analíticos. Esto incluye datos de uso anónimos (como páginas visitadas y funciones utilizadas) para mejorar la aplicación, y metadatos básicos para habilitar guías dirigidas dentro de la aplicación. Nunca se rastrea contenido personal.

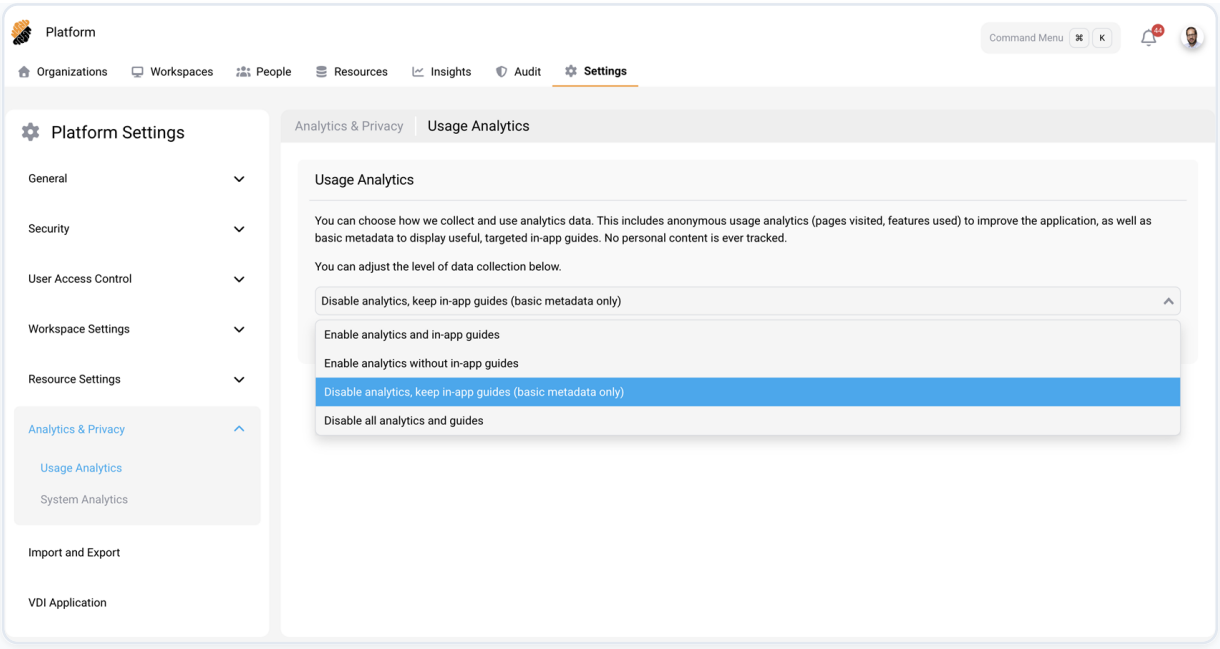
Para cambiar el nivel de recopilación de datos, vaya a **Configuración de la plataforma > Análisis y privacidad > Análisis de uso**, seleccione una opción del menú desplegable y seleccione **Aplicar**.

Opciones disponibles:

- **Habilitar análisis y guías en la aplicación** — Se recopila la telemetría de uso y se muestra la guía en la aplicación.
- **Habilitar análisis sin guías en la aplicación** — Esta es la opción predeterminada para las nuevas implementaciones. La telemetría de uso se recopila, pero se suprimen todas las superposiciones, avisos y sugerencias de las guías en la aplicación.
- **Deshabilitar análisis, mantener guías en la aplicación (solo metadatos básicos)** — No se comparte telemetría de uso con Citrix, pero la guía en la aplicación sigue estando disponible.

- **Deshabilitar todos los análisis y guías** — Todos los componentes de Pendo están deshabilitados y no se comparte ningún dato con Citrix. La guía en la aplicación, las notificaciones y la capacidad de enviar comentarios no están disponibles.

> **Nota**
>
> La opción predeterminada se aplica solo a las nuevas implementaciones. Una implementación que se instaló antes de que cambiara esta opción predeterminada mantiene el nivel que ya tenía configurado, incluido **Habilitar análisis y guías en la aplicación**.



Requisitos de conectividad

Para ver el contenido de Pendo en la consola de administración, asegúrese de que la dirección `http://citrix-sds-content.customer.pendo.io` sea accesible desde su red.

Pendo es un subprocesador externo que Citrix utiliza para proporcionar servicios de nube y soporte a los clientes de Citrix. Para obtener una lista completa de los subprocesadores, consulte Subprocesadores para los servicios de nube y soporte de Citrix y las filiales de Citrix.

Workspace resource usage insights

Citrix SecurSpaces™ proporciona información histórica sobre el uso de CPU y memoria del espacio de trabajo. Estos datos se recopilan y almacenan automáticamente en la base de datos de SecurSpaces para respaldar el análisis de dimensionamiento adecuado y la evaluación de tendencias a largo plazo.

Al aprovechar estos datos, los clientes pueden:

- Analizar el consumo de CPU y memoria de cada espacio de trabajo a lo largo del tiempo.
- Identificar la asignación óptima de recursos para los espacios de trabajo.
- Reducir los costes de infraestructura manteniendo una experiencia de desarrollador de alta calidad.

Requisitos

Para habilitar la recopilación de métricas del espacio de trabajo, debe instalarse el **Servidor de métricas de Kubernetes**. Este componente agrega datos de uso de recursos en los clústeres de Kubernetes y se implementa comúnmente en entornos alojados en la nube o en cualquier configuración que utilice el autoescalado.

Para obtener instrucciones de instalación y detalles adicionales, consulte la documentación del Servidor de métricas de Kubernetes

Recopilación y almacenamiento de datos

SecurSpaces consolida automáticamente los datos de medición brutos cada cinco minutos y proporciona los siguientes puntos de datos para el intervalo de 5 minutos anterior:

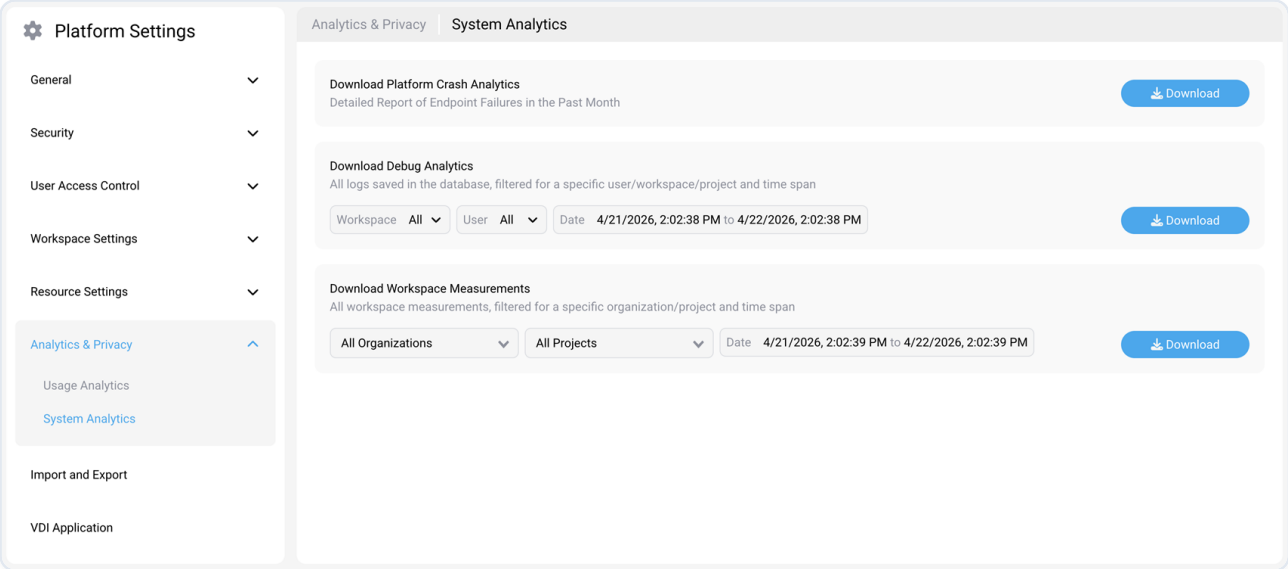
- Mínimo, Máximo, Promedio, P50, P75, P95 y P99

Acceder a las mediciones del espacio de trabajo

Los datos de medición del espacio de trabajo están disponibles a través de la consola de administración y mediante API.

Descargar desde la consola de administración

Los administradores de plataforma y los oficiales de seguridad pueden descargar las mediciones del espacio de trabajo como un archivo desde **Configuración de la plataforma > Análisis y privacidad > Análisis del sistema**.



Filtros disponibles:

- **Organización** — Seleccione una organización específica o mantenga **Todas las organizaciones** para incluir datos de cada organización.
- **Proyecto** — Seleccione un proyecto específico o mantenga **Todos los proyectos** para incluir datos de cada proyecto.
- **Fecha** — Especifique una fecha de inicio y fin, o seleccione **Todas las fechas** para descargar el historial completo de mediciones.

Para descargar las mediciones del espacio de trabajo:

1. Vaya a **Configuración de la plataforma > Análisis y privacidad > Análisis del sistema**.
2. En la sección **Descargar mediciones del espacio de trabajo**, seleccione una organización, un proyecto y un rango de fechas.
3. Seleccione **Descargar**.

Para obtener más información sobre la página Análisis del sistema, consulte Análisis del sistema.

Acceso mediante API

Los datos están disponibles en formatos brutos y agregados a través de la API. Los clientes pueden acceder a las métricas a nivel de plataforma, organización y proyecto.

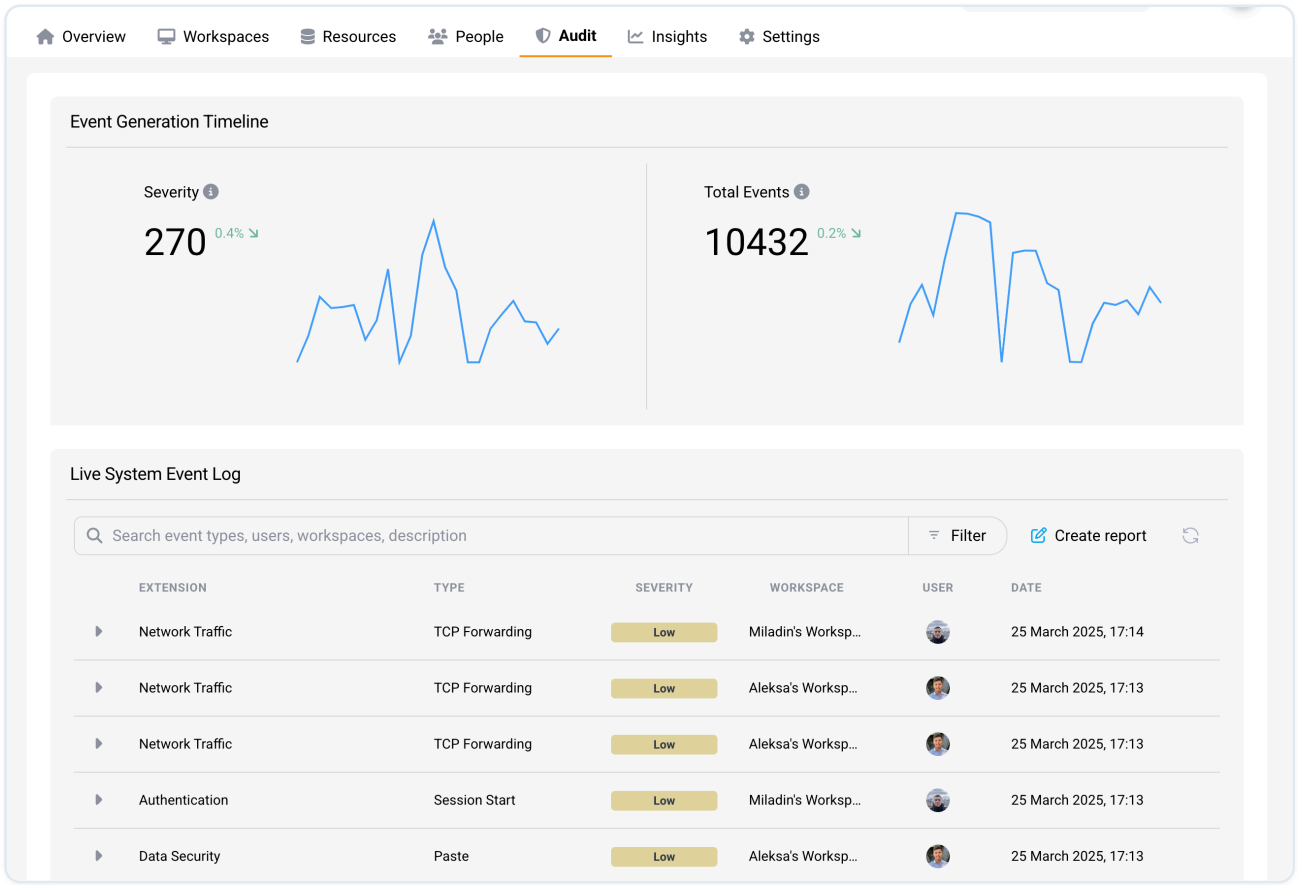
- Para datos brutos, utilice la API **workspace-measurements-samples** (por ejemplo, `/v1/metrics/workspace-measurements-samples`).
- Para datos agregados, utilice la API **workspace-measurements** (por ejemplo, `/v1/projects/{projectId}/metrics/workspace-measurements`).

Para obtener documentación de la API y ejemplos de uso, consulte la documentación de la API de SecurSpaces.

Audit page

Requiere que el conjunto de permisos de Seguridad esté en **Acceso**.

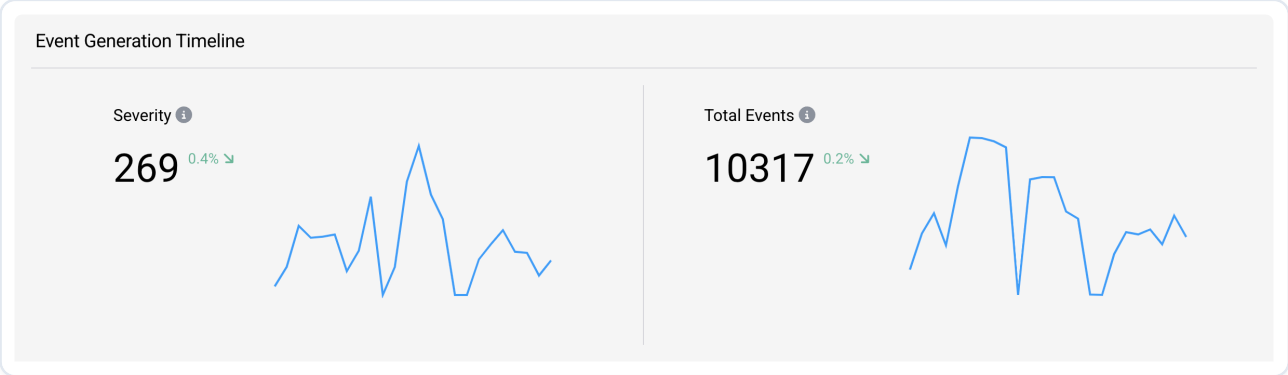
La **página de Auditoría** proporciona información sobre la seguridad de su **Proyecto**, incluyendo un gráfico de **Cronología de Generación de Eventos** que ilustra la cronología de los eventos activados por los espacios de trabajo dentro del proyecto actual. Además, el **Registro de Eventos del Sistema en Vivo** presenta una tabla que muestra registros detallados de cada evento.



- Cronología de Generación de Eventos
- Registros de Eventos
- Filtrado de Registros
- Visualización de Registros

Cronología de Generación de Eventos

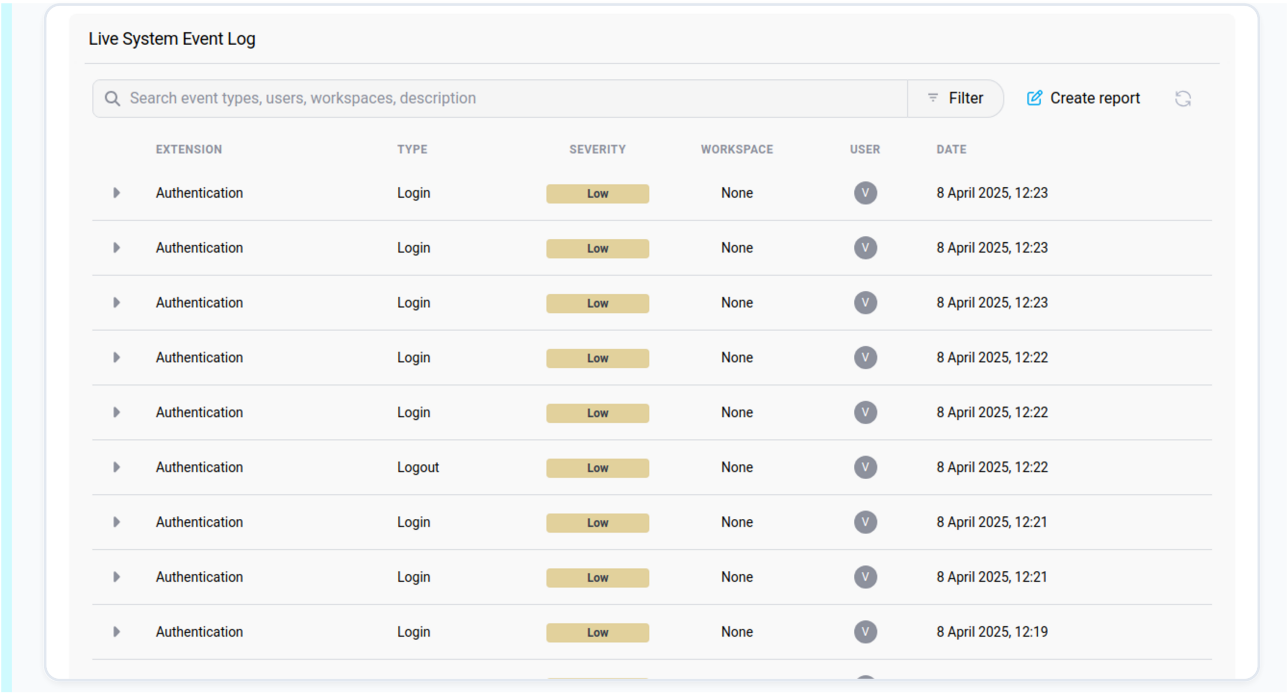
La cronología de generación de eventos consta de dos gráficos, donde el primero muestra el nivel de gravedad de los eventos activados a lo largo del tiempo, y el otro muestra la cantidad total de eventos activados a lo largo del tiempo.



Registros de Eventos

El **Registro de Eventos del Sistema en Vivo** muestra registros de eventos de seguridad activados por espacios de trabajo dentro de un proyecto específico. Estos eventos pueden adoptar muchas formas, como la monitorización del portapapeles o alertas de red, como una solicitud DNS. Estos registros son importantes ya que tienen la capacidad de descubrir posibles vulnerabilidades de seguridad.

> **Consejo**
>
> Los eventos se activan una vez que haya habilitado la opción "Registrar y grabar el tráfico de red saliente" para la Política de Red asociada.



Filtrado de registros

La vista de registros permite a los usuarios filtrar y buscar fácilmente en los registros de eventos del sistema. Esta función hace que sea muy conveniente identificar posibles problemas, solucionar errores y también supervisar el uso del sistema a un nivel más granular. Para mostrar las opciones de filtro, pulse el botón "**Filtrar**" situado en la parte superior derecha del panel **Registro de eventos del sistema en vivo**. Filtrar registros por:

- **Tipo** de evento,
- Nivel de **gravedad**,
- **Espacio de trabajo** desde donde se activó el evento,
- **Usuario** que activó el evento,
- **Fecha** y hora en que se activó el evento.

Además de filtrar los registros, puede buscarlos escribiendo palabras clave en la barra de búsqueda debajo del rango de fechas (por ejemplo, buscar un usuario específico).

Visualización de registros

La vista de registros proporciona información detallada sobre cada evento que ocurre dentro del sistema. Para cada registro, puede ver la siguiente información:

1. **Tipo**: Qué tipo de evento se activó,
2. **Gravedad**: Nivel de gravedad del evento,
3. **Espacio de trabajo**: Espacio de trabajo desde donde se activó el evento,

4. **Usuario**: Usuario que activó el evento,
5. **Fecha**: Fecha y hora en que se activó el evento,
6. **Descripción**: Describe la acción que desencadenó el evento.

Para ver más detalles sobre un evento, pulse el botón del menú desplegable a la izquierda del registro del evento.

SIEM integration

SecurSpaces puede reenviar eventos de auditoría de la plataforma a un sistema externo de Gestión de Información y Eventos de Seguridad (SIEM) utilizando el **Formato de Evento Común (CEF)**. Puede usar cualquier herramienta de envío de registros que admita CEF para recopilar y reenviar estos eventos. El tutorial a continuación utiliza Filebeat implementado como un DaemonSet de Kubernetes como ejemplo.

La configuración de la integración de SIEM requiere dos fases: una implementación de backend realizada por el operador de la plataforma, seguida de la activación en la consola de administración por un administrador de la plataforma.

Requisitos previos

- Acceso al gráfico de Helm de Citrix SecurSpaces™ y al archivo de configuración `values.yaml`
- Permiso para implementar actualizaciones en el clúster de Kubernetes que aloja SecurSpaces
- Rol de administrador de plataforma o de oficial de seguridad en la consola de administración de SecurSpaces
- Un sistema SIEM de destino que acepte eventos con formato CEF (por ejemplo, Elastic SIEM)

Fase 1: Configurar el backend

Complete estos pasos en su entorno de implementación antes de activar la integración en la consola de administración.

Paso 1: Habilitar syslog en los valores de Helm

Abra el archivo `values.yaml` para su implementación de SecurSpaces y descomente el bloque de configuración bajo `ninja.clusterConfig.syslog`. Actualice los valores para que coincidan con su entorno:

```
syslog:
  volumeName: "syslog-volume"
  volume:
    name: "syslog-volume"
    hostPath:
      path: "/strong-network/siem"
      type: DirectoryOrCreate
  mountPath: "/var/strong-network/"
  hostPath: "/strong-network/siem"
```

PARÁMETRO	DESCRIPCIÓN
`volumeName`	Identificador de nombre para el volumen de Kubernetes.
`volume`	Definición de volumen de Kubernetes. El tipo `hostPath` asigna un directorio del sistema de archivos del nodo al pod. `DirectoryOrCreate` le indica a Kubernetes que cree el directorio si aún no existe.
`mountPath`	Ruta dentro de los contenedores del servicio de plataforma donde se monta el volumen. La aplicación escribe los archivos `.log` aquí (por ejemplo, `/var/strong-network/<name>.log`).
`hostPath`	Ruta en el nodo host donde se conservan los archivos de registro. Su herramienta de envío de registros (por ejemplo, Filebeat) lee desde esta misma ruta.

El efecto neto: los pods de la plataforma montan el directorio del host `/strong-network/siem` en `/var/strong-network/` dentro del contenedor y escriben los archivos `.log` allí. Filebeat (o la herramienta elegida) lee esos mismos archivos a través de la ruta del host.

Paso 2 — Preparar el YAML de Filebeat

1. En la consola de administración de SecurSpaces, vaya a **Plataforma > Configuración > Seguridad > Integración SIEM**.
2. Copie el ejemplo de YAML que se muestra en la página. Este YAML define una implementación de Filebeat que comprende un `ServiceAccount`, un `ConfigMap` (que contiene la configuración de la canalización de Filebeat) y un `DaemonSet`.
3. En el YAML copiado, reemplace cada instancia de `release` con su espacio de nombres de implementación real.
4. Rellene las credenciales de conexión de Elasticsearch en la sección de variables de entorno de la especificación de DaemonSet. Para implementaciones de producción, almacene estas credenciales en un Secreto de Kubernetes y haga referencia al Secreto en las variables de entorno en lugar de colocar valores de texto sin formato en el YAML.

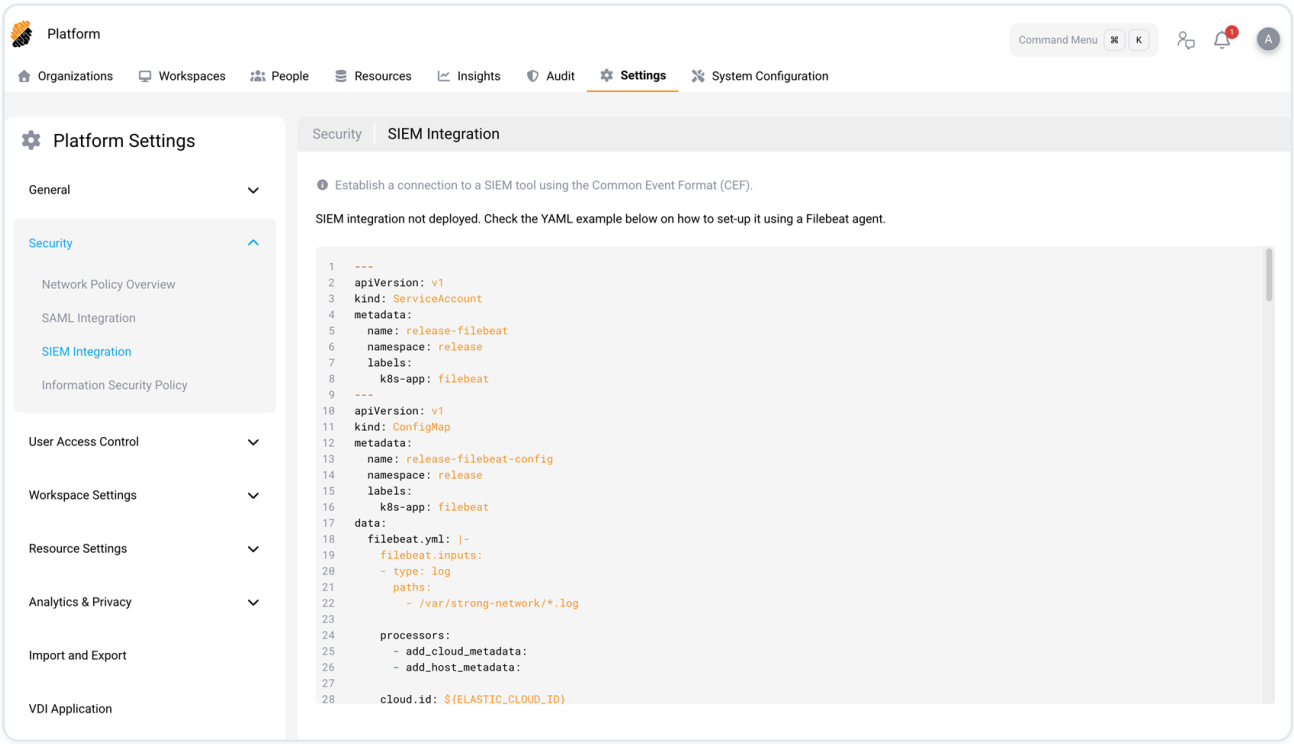
Paso 3 — Implementar

Coloque el YAML actualizado en sus gráficos de Helm y ejecute una nueva implementación para aplicar la configuración de Helm actualizada y el DaemonSet de Filebeat al clúster.

Fase 2: Activar en la consola de administración

1. Inicie sesión en la consola de administración de SecurSpaces como administrador de plataforma o oficial de seguridad.
2. Vaya a **Plataforma > Configuración > Seguridad > Integración SIEM**.
3. Si el DaemonSet está en buen estado y el volumen está montado correctamente, aparecerá un interruptor para activar la integración. Habilite el interruptor.

Una vez activada, la plataforma comienza a reenviar los eventos de auditoría al destino SIEM configurado.



Cómo funciona

1. Los servicios de la plataforma SecurSpaces escriben eventos de auditoría como archivos `.log` en formato CEF en la ruta de montaje del contenedor (`/var/strong-network/`), que se asigna a `/strong-network/siem` en el nodo host.
2. El DaemonSet de Filebeat que se ejecuta en cada nodo del clúster lee los archivos de registro de la ruta del host (`/strong-network/siem`).
3. Filebeat envía los eventos al destino SIEM configurado (por ejemplo, Elasticsearch).

Eventos de auditoría

La plataforma reenvía eventos en ocho categorías. A cada evento se le asigna un **ClassID** que identifica su categoría en la carga útil de CEF.

Para cada evento y sus atributos, consulte Catálogo de eventos de auditoría.

Extensiones comunes

Todos los eventos incluyen las siguientes extensiones CEF:

EXTENSIÓN	DESCRIPCIÓN
`timestamp`	Hora en que se generó el evento.
`suid`	ID de usuario del actor.

EXTENSIÓN	DESCRIPCIÓN
`suser`	Nombre de usuario del actor.
`wsid`	ID del espacio de trabajo (cuando corresponda).
`wsname`	Nombre del espacio de trabajo (cuando corresponda).
`projectId`	ID del proyecto.
`projectName`	Nombre del proyecto.
`eventId`	Identificador único para el evento.

Categorías de eventos

AUTENTICACIÓN (CLASSID 1)

Login, Logout, SessionStart, SessionEnd, SessionInterrupt

AUTORIZACIÓN (CLASSID 2)

- **Usuario:** UserBlocked, UserUnblocked, ProjectManagerSeat
- **Espacio de trabajo:** SharedWithUser, UnsharedWithUser

SEGURIDAD DE DATOS (CLASSID 3)

Copy, Paste, Cut, Upload, UploadLargeFile, Download, DownloadLargeFile, SupervisedCopy

Los eventos de seguridad de datos incluyen extensiones adicionales: `data`, `isSecret`, `isCode`.

SISTEMA (CLASSID 4)

WorkspaceSpecsUpdated

ACTIVIDAD DEL USUARIO (CLASSID 5)

VSCodeExtensionInstalled

Los eventos de instalación de extensiones incluyen extensiones adicionales: `extensionName`, `extensionId`, `extensionUUID`.

GESTIÓN DE CUENTAS (CLASSID 6)

UserAddedToProject, UserRemovedFromProject, RoleChanged, UserCreated, UserDeleted, UserAddedAsSecurityOfficer, UserRemovedAsSecurityOfficer, UserAddedAsOrganizationOwner, UserRemovedAsOrganizationOwner, UserPasswordUpdated

TRÁFICO DE RED (CLASSID 7)

SSH Commands, External SSH Commands, HTTP Requests, Git-over-HTTP, TCP Forwarding, DNS Resolution

ACCESO A RECURSOS (CLASSID 8)

Actions: Created, Imported, ManuallyImported, Updated, SharedWithUsers, SharedPublicly, WorkspaceAttached, WorkspaceDetached, Deleted

Recursos: repositorios, buckets, secretos, servicios conectados, política de seguridad, imágenes, credenciales, puntos de montaje, workspaceApp, script de inicio, espacios de trabajo, token de API, SSH personal, versiones de VS Code

Mapeo de gravedad

Cada evento lleva un valor de gravedad CEF (0–10). La plataforma asigna la gravedad a la prioridad de syslog de la siguiente manera:

GRAVEDAD CEF	PRIORIDAD DE SYSLOG
0–3	`LOG_INFO`
4–6	`LOG_ALERT`
7–10	`LOG_CRIT`

Filtrado de eventos

Puede controlar qué eventos reenvía la plataforma utilizando dos filtros en la página de configuración de Integración SIEM:

- **Filtro de gravedad** — Establece un umbral de gravedad mínimo. Los eventos por debajo del umbral no se reenvían.
- **Filtro de tipo de evento** — Selecciona categorías de eventos específicas o tipos de eventos individuales para reenviar.

verificar la integración

Después de la implementación, confirme que la canalización funciona de extremo a extremo:

1. verificar que los pods de Filebeat se están ejecutando:

```
kubectl get pods -n <namespace>
```

1. Confirme que los archivos `.log` existen en la ruta del host:

```
ls /strong-network/siem/
```

1. Compruebe la página de Integración SIEM en la consola de administración; el estado debería indicar que la integración está activa.
2. Realice una acción auditable en SecurSpaces (por ejemplo, inicie sesión o cree un espacio de trabajo) y verificar que el evento correspondiente aparece en su herramienta SIEM.

Insights page

La **página de Insights** muestra información sobre la actividad de los miembros del **Proyecto**, la asignación de recursos y las métricas de los procesos de los contenedores. La información mostrada en esta página depende de la implementación de la plataforma en su organización. Esta sección proporciona una vista general de la información que se encuentra comúnmente en las implementaciones.

> **Información**

> Dependiendo de sus permisos dentro del proyecto, parte de esta información podría no estar disponible.

Contenido

- **Asignación de recursos**
- **Métricas de procesos de contenedores**

Resource allocation

Requiere el conjunto de permisos Métricas para **Acceder al proyecto**.

La pestaña **Asignación de recursos** grafica cuánto están consumiendo realmente los espacios de trabajo de su clúster, a lo largo del tiempo. Dado que un espacio de trabajo mantiene su

asignación solo mientras se está ejecutando, la curva rastrea cuántos espacios de trabajo se están ejecutando en cualquier momento.

Los gráficos

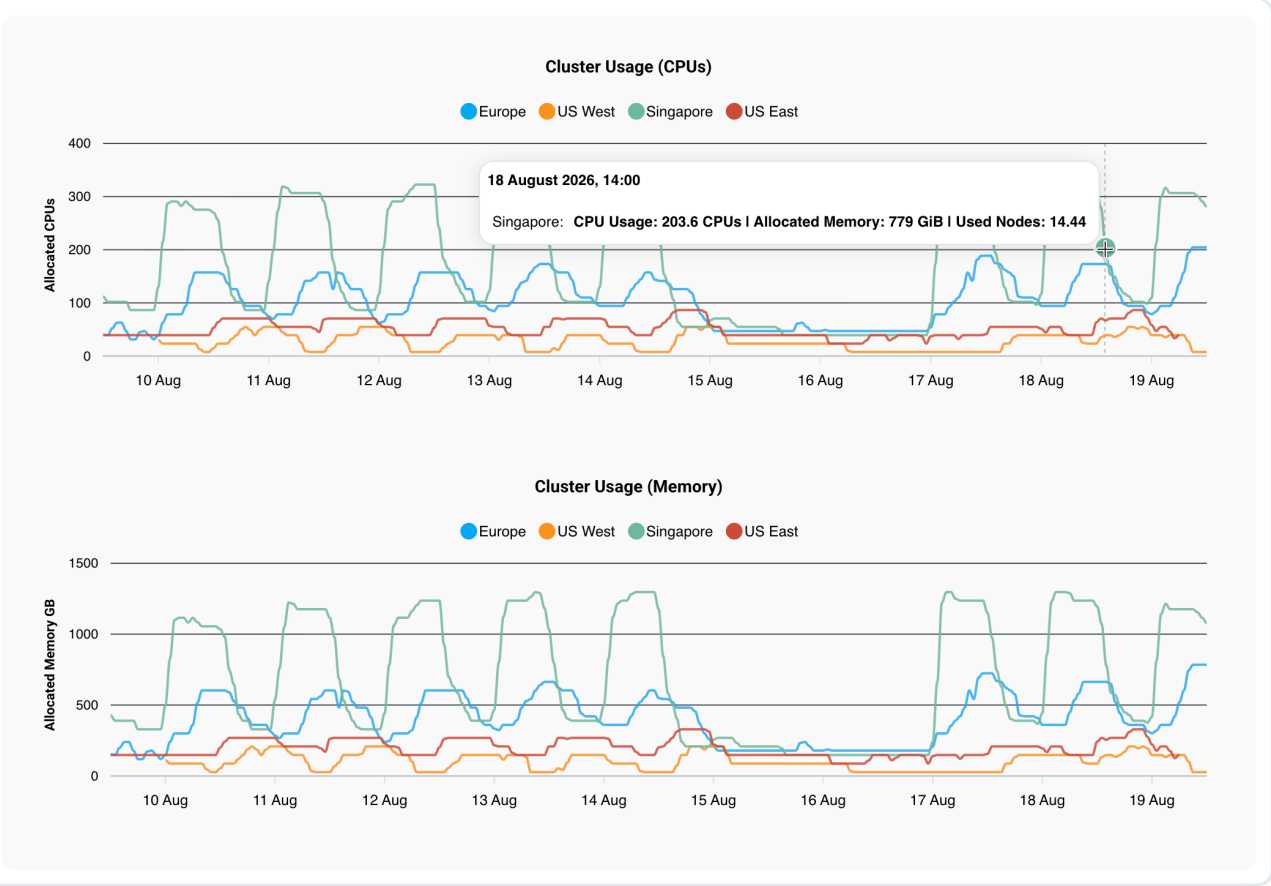
Se muestran dos gráficos, uno para CPU y otro para memoria, con el tiempo en el eje horizontal. En una implementación multirregión, cada región se grafica como su propia línea, para que pueda compararlas directamente.

Los títulos de los gráficos cambian según su ubicación. La tarjeta es la misma en los tres lugares, pero su alcance se ajusta a lo que está viendo:

DÓNDE LO ABRE	TÍTULOS DE LOS GRÁFICOS
Plataforma	Uso del clúster (CPU) y Uso del clúster (Memoria)
Organización	Asignación de recursos de la organización (CPU) y (Memoria)
Proyecto	Asignación de recursos del proyecto (CPU) y (Memoria)

Así, el propietario de un proyecto ve el consumo de su proyecto, no el del clúster. Solo la vista de la plataforma cubre toda la implementación, que es la que se debe usar para las preguntas de capacidad en Dimensionamiento.

Use la lista de rango de tiempo encima de los gráficos para cambiar la ventana. Por defecto es **Últimos 10 días**, y también ofrece Últimos 7 días, Últimas 7 semanas, Últimos 30 días, Últimos 90 días y Último año.



Al pasar el ratón sobre un punto, se muestran los valores de ese momento para esa región:

VALOR	SIGNIFICADO
Uso de CPU	Núcleos asignados a espacios de trabajo en ejecución
Memoria asignada	Memoria asignada a espacios de trabajo en ejecución
Nodos utilizados	Nodos del clúster en uso, como promedio durante el intervalo

Interpretación de la forma

La forma de la curva es más informativa que cualquier número individual.

Un aumento y una disminución diarios es el aspecto de una implementación saludable. Los espacios de trabajo se inician cuando los desarrolladores comienzan a trabajar, y se pausan cuando están inactivos, por lo que el uso aumenta durante el día laboral y disminuye durante la noche. Los períodos planos durante los fines de semana y días festivos son el mismo efecto durante un período más largo.

Una curva que no desciende es la que debe investigarse. Si el uso se mantiene alto durante la noche, los espacios de trabajo están en ejecución cuando nadie los está utilizando, y usted está pagando por los nodos que los alojan. Las causas habituales son:

- La detección de inactividad no está configurada, o el tiempo de espera es demasiado largo. Consulte Detección de inactividad del espacio de trabajo.
- **Bypass Schedule** está habilitado en más espacios de trabajo de lo previsto. Está diseñado para tareas desatendidas y exime a un espacio de trabajo de pausarse por completo.
- Los procesos de larga duración mantienen las sesiones activas.

Comparar la amplitud entre regiones es una forma rápida de ver esto: una región cuya línea apenas se mueve, mientras que las otras ciclan, suele ser una diferencia de configuración más que una diferencia en cómo trabaja la gente.

Una línea de base ascendente durante semanas significa que el nivel mínimo está subiendo — espacios de trabajo que nunca se detienen, o crecimiento en el número de espacios de trabajo. De cualquier manera, es la señal para planificar la capacidad antes de que se vuelva urgente.

Consumo del espacio de trabajo

Debajo de los gráficos, una lista ordenable muestra el consumo total por espacio de trabajo en el proyecto, para que puedas atribuir un pico a los espacios de trabajo que lo causaron.

Cada espacio de trabajo se crea según una especificación que fija su CPU, memoria y disco. Lo que muestra la lista es el consumo en relación con esa especificación, que es cómo se encuentran espacios de trabajo dimensionados muy por encima de lo que utilizan.

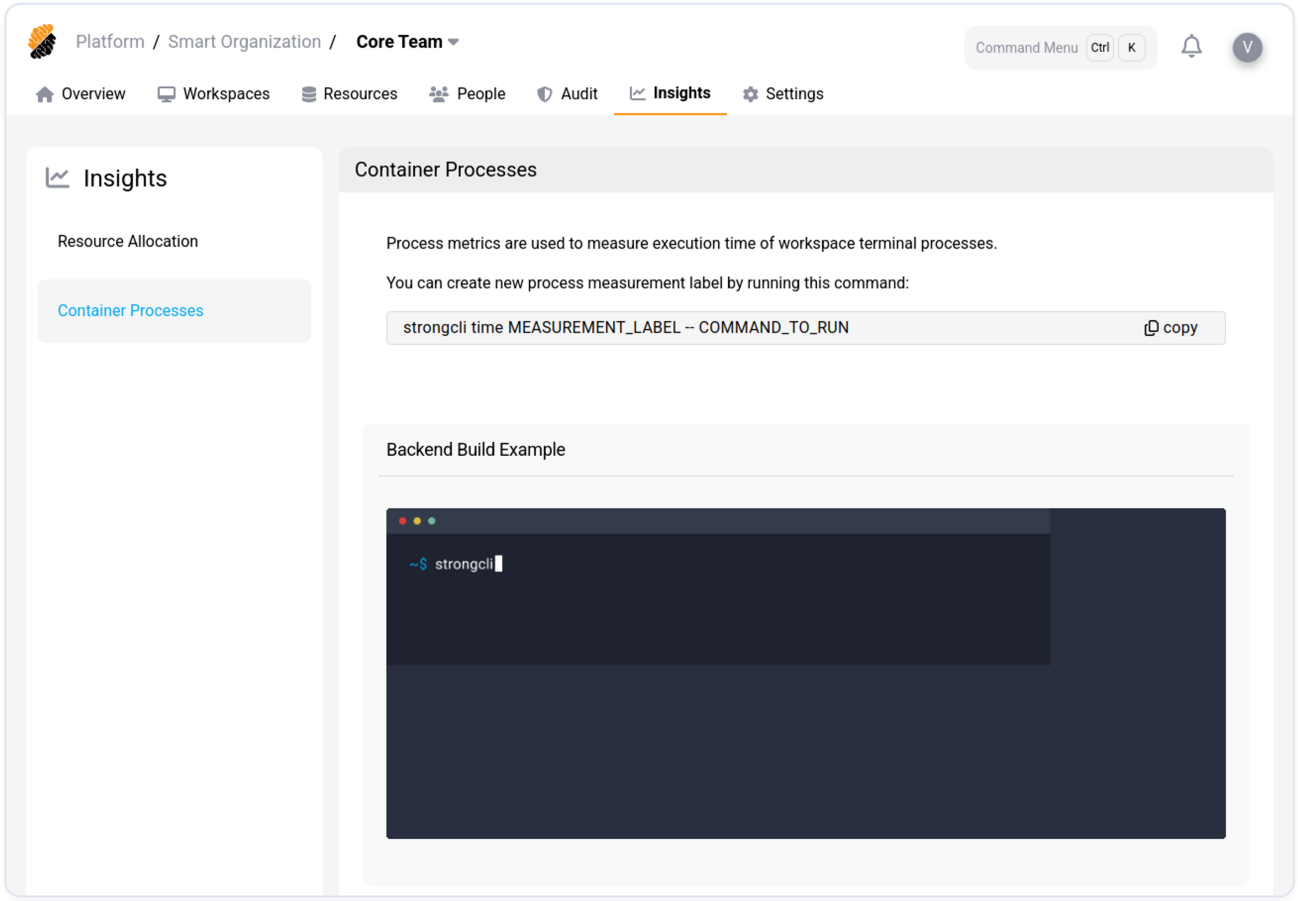
Información relacionada

- Uso de recursos del espacio de trabajo
- Detección de inactividad del espacio de trabajo
- Métricas de procesos de contenedores
- Requisitos del sistema

Container process metrics

La sección **Container Process** muestra métricas de tiempo registradas usando la Interfaz de Línea de Comandos (CLI) de la plataforma **strongcli** disponible en espacios de trabajo de desarrolladores. Las métricas se registran usando la opción 'time' y están disponibles en la sección **Container Process** del panel de Insights. Esta CLI se usa típicamente en scripts

incrustados en los contenedores del proyecto para que, al inicio, se pueda registrar una selección de procesos para la evaluación del rendimiento. Una vez registradas en una flota de espacios de trabajo, las métricas se agregan y finalmente se muestran en la página de Insights.



- Rastrear un proceso de contenedor
- Período de Insights
- Insights del proceso de contenedor
  - Promedio
  - Total

Rastrear un proceso de contenedor

Puede rastrear el tiempo de ejecución de los procesos de contenedor en los espacios de trabajo utilizando la Interfaz de Línea de Comandos (CLI) de la plataforma **strongcli**. Use el siguiente comando para hacerlo:

```
> strongcli time LABEL -- COMMAND_TO_RUN
```

Donde:

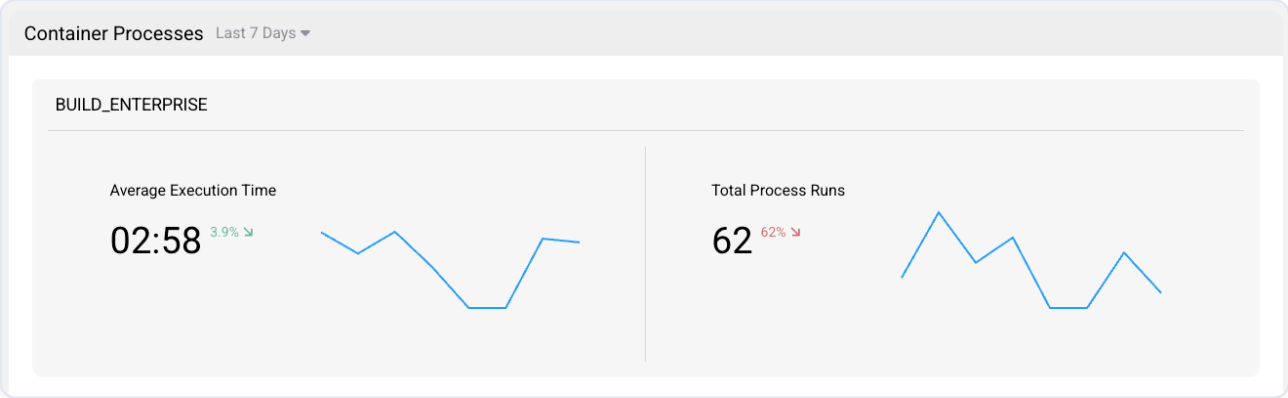
- **LABEL**: Esto permite establecer una etiqueta para identificar el proceso en el panel de Insights,
- **COMMAND_TO_RUN**: El comando de terminal para el cual desea medir el tiempo de ejecución.

Esto registra un nuevo proceso para su espacio de trabajo entre los **procesos de contenedor** y mide su tiempo de ejecución.

Período de Insights

Después de seleccionar un proceso de contenedor, puede variar el período de las estadísticas desde un promedio de ejecución de 7 días hasta un promedio anual.

- Haga clic en el menú desplegable a la derecha de "**Last 7 days**" para cambiar el período de evaluación.

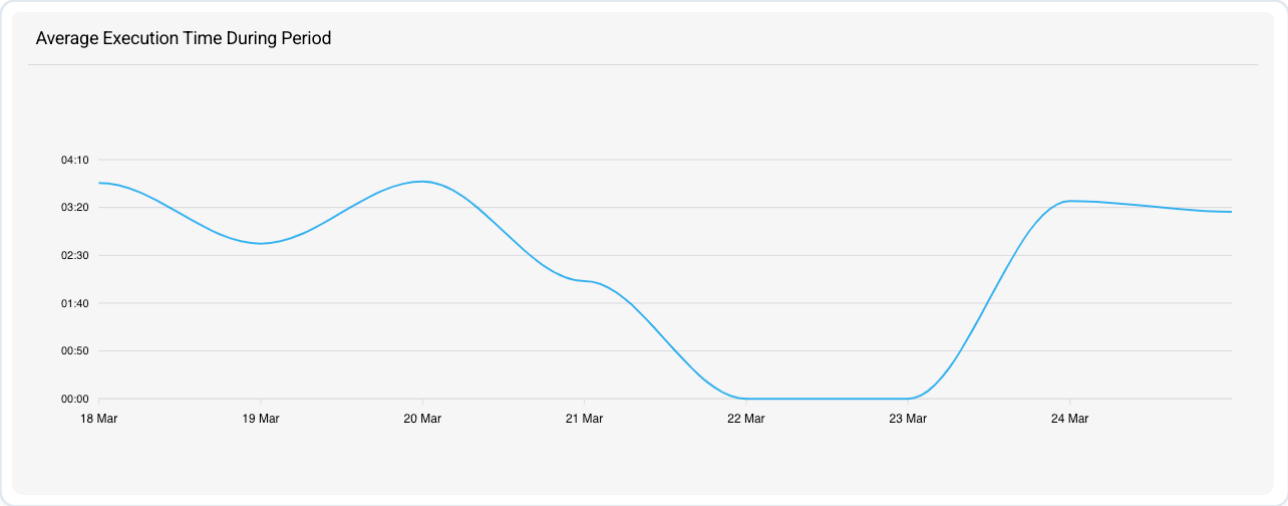


Según el período seleccionado, la escala del gráfico se adaptará en consecuencia.

Información sobre procesos de contenedores

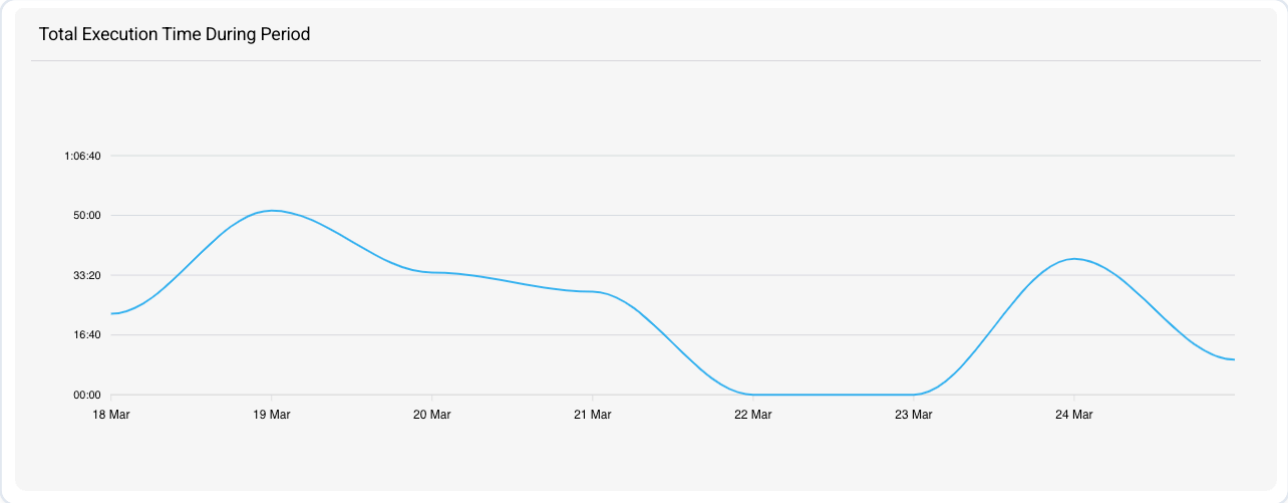
Promedio

El gráfico de "tiempo de ejecución promedio" en la sección de Procesos de contenedores del panel de Insight muestra el tiempo promedio que tardó en ejecutarse un comando dentro del espacio de trabajo de un desarrollador, según lo registrado por la Interfaz de Línea de Comandos (CLI) de la plataforma. El período de tiempo que se muestra en el gráfico de tiempo de ejecución promedio se puede ajustar, lo que le permite ver métricas para un rango de fechas específico.



Total

El gráfico de "tiempo total de ejecución" en la sección de **procesos de contenedores** del panel de Insight muestra el tiempo total que el comando se ha ejecutado en el espacio de trabajo de un desarrollador. El período de tiempo que se muestra en el gráfico de tiempo total de ejecución se puede ajustar, lo que le permite ver métricas para un rango de fechas específico.



Security and compliance

Esta sección está escrita para revisores de seguridad, ya sea que estén evaluando SecurSpaces antes de su adopción o respondiendo preguntas sobre una implementación que ya tienen en ejecución.

SecurSpaces está alojado por el cliente, por lo que la responsabilidad es compartida. La plataforma proporciona controles; su clúster, el ingreso y el cifrado de la infraestructura son suyos. Límites de confianza indica dónde se establece la línea.

Evaluación de la plataforma

PREGUNTA	PÁGINA
¿Qué controles existen y cómo cito uno?	Catálogo de controles
¿Dónde separa la implementación la confianza y quién es el propietario de cada lado?	Límites de confianza
¿Cómo se mueven los datos entre componentes?	Flujos de datos
¿Qué puertos deben estar abiertos y qué cifra qué?	Puertos y protocolos, Criptografía

Control del tráfico del espacio de trabajo

TAREA	PÁGINA
Comprender el modelo de políticas y los valores predeterminados	Políticas de red
Crear una política	Crear una política de red
Aplicar una en todos los proyectos	Asignar y aplicar una política
Averiguar por qué se bloqueó el tráfico	Supervisar y solucionar problemas

SecurSpaces Flex

Flex es la oferta gestionada, con una división de responsabilidades diferente. Consulte Seguridad de SecurSpaces Flex.

Información relacionada

- Panel de auditoría
- Catálogo de eventos de auditoría
- Problemas resueltos — incluye correcciones de seguridad por versión

Security control catalogue

Introducción

Este documento proporciona una visión general de los controles de seguridad disponibles en Citrix SecurSpaces™. Sirve de apoyo para las evaluaciones de seguridad, las evaluaciones de riesgos y las revisiones de diligencia debida de terceros.

Los controles descritos en este documento reflejan la arquitectura de seguridad de SecurSpaces, las prácticas operativas y el modelo de responsabilidad compartida como una solución alojada por el cliente. Están diseñados para alinearse con los requisitos de seguridad empresarial y las mejores prácticas del sector.

Se puede proporcionar documentación adicional y pruebas de respaldo previa solicitud para abordar requisitos específicos de seguridad, cumplimiento o auditoría.

Acerca de estos identificadores

Cada control a continuación tiene un identificador estable, como SDS-NET-01. Citrix asigna estos identificadores para que un control específico pueda citarse en una evaluación, una respuesta a un cuestionario o un caso de soporte.

No son una asignación a ISO 27001, SOC 2, NIST o cualquier otro marco, y no implican certificación contra ninguno de ellos. Para una asignación a un marco específico, o para obtener pruebas de respaldo, póngase en contacto con Citrix y especifique lo que requiere su revisión.

Los identificadores son estables. Un control que se retira conserva su identificador, que no se reutiliza.

Identidad y acceso

ID	CONTROL	IMPLEMENTACIÓN
SDS-IAM-01	Inicio de sesión único y autenticación multifactor	SecurSpaces admite el inicio de sesión único (SSO) empresarial a través de la federación de identidades basada en estándares utilizando SAML 2.0 u OpenID Connect (OIDC). El proveedor de identidades puede aplicar la autenticación multifactor (MFA) como parte del flujo de autenticación. SecurSpaces también incluye capacidades de MFA nativas.
SDS-IAM-02	Identidad y autenticación	SecurSpaces es compatible con SAML 2.0 y OIDC para la aplicación de SSO y MFA. SecurSpaces también es compatible con el Sistema de Gestión de Identidades entre Dominios (SCIM) para el aprovisionamiento, desaprovisionamiento y sincronización automatizados del ciclo de vida de las identidades de usuario desde un proveedor de identidades central.
SDS-IAM-03	Gestión de acceso	SecurSpaces incluye control de acceso basado en roles (RBAC) integrado. Los administradores pueden asignar permisos de aplicación a cuentas de usuario locales o a grupos de directorio sincronizados desde el proveedor de identidades. Para obtener

ID	CONTROL	IMPLEMENTACIÓN
		más información, consulte Control de acceso basado en roles.
SDS-IAM-04	Gestionar privilegios a nivel de TI	SecurSpaces separa la gestión a nivel de infraestructura de la administración a nivel de aplicación. Dado que SecurSpaces está contenerizado y alojado en Kubernetes, el equipo de infraestructura del cliente mantiene el control sobre el clúster subyacente, los nodos y la capa de orquestación de contenedores. Los privilegios de TI específicos de la aplicación, como la gestión de usuarios y los cambios de configuración, están restringidos a la capa de aplicación mediante un RBAC granular. Estos privilegios no requieren acceso directo a la infraestructura de alojamiento.

Criptografía y secretos

ID	CONTROL	IMPLEMENTACIÓN
SDS-CRY-01	Cifrar datos en tránsito	SecurSpaces cifra los datos en tránsito utilizando protocolos seguros. El tráfico web externo utiliza HTTPS. TLS se termina en el controlador de entrada, por lo que las versiones de TLS y los conjuntos de cifrado

ID	CONTROL	IMPLEMENTACIÓN
		permitidos son configurados por la configuración de entrada del cliente. Las sesiones de terminal seguras utilizan SSH. Dentro del clúster de Kubernetes, el tráfico de entrada a servicio y de servicio a servicio se cifra con TLS. Para la lista completa, consulte Criptografía.
SDS-CRY-02	Cifrar datos en reposo	SecurSpaces es una solución alojada por el cliente. El cliente es responsable de aprovisionar y gestionar la base de datos subyacente y los volúmenes de almacenamiento persistente. SecurSpaces es compatible con tecnologías de cifrado en reposo estándar de la industria, incluido el cifrado de almacenamiento gestionado en la nube, como AWS KMS o Azure Key Vault, y los volúmenes persistentes de Kubernetes (PVs) cifrados. SecurSpaces también aplica protección a nivel de aplicación. Cuando la función de Vault externo no está habilitada, los secretos de desarrollador se cifran en la base de datos utilizando AES-128-GCM.
SDS-CRY-03	Gestionar certificados y el ciclo de vida de los certificados	SecurSpaces se basa en certificados X.509 estándar para el cifrado TLS. Para el tráfico externo, SecurSpaces

ID	CONTROL	IMPLEMENTACIÓN
		admite herramientas automatizadas de gestión del ciclo de vida de los certificados, como cert-manager, Let's Encrypt o PKI interno, para admitir la renovación de certificados sin tiempo de inactividad de la aplicación. Para el tráfico interno del clúster, SecurSpaces gestiona automáticamente los certificados necesarios para mantener TLS entre el controlador de entrada y los servicios de backend.
SDS-CRY-04	Gestión de secretos	SecurSpaces separa el manejo de secretos de aplicación e infraestructura. Los secretos de aplicación y de desarrollador se gestionan en la capa de aplicación. Por defecto, estos secretos se cifran antes de escribirse en la base de datos utilizando AES-128-GCM. SecurSpaces también admite la integración con una instancia externa de HashiCorp Vault. Los secretos se inyectan de forma segura en los entornos de ejecución del espacio de trabajo a través de variables de entorno o archivos de configuración montados en volumen. Los secretos de infraestructura, como las credenciales de arranque de la plataforma y las conexiones a la base de

ID	CONTROL	IMPLEMENTACIÓN
		datos, utilizan Kubernetes Secrets estándar. Dado que SecurSpaces está alojado por el cliente, los clientes pueden añadir protecciones a nivel de infraestructura, como el cifrado de sobre KMS del proveedor de la nube para `etcd` o un controlador CSI de Secrets Store para inyectar claves de infraestructura desde una bóveda empresarial.

Seguridad de red

ID	CONTROL	IMPLEMENTACIÓN
SDS-NET-01	Restringir el uso de puertos de red a los servicios esenciales	SecurSpaces opera con una huella de red mínima y expone solo los puertos esenciales necesarios para los servicios principales: HTTPS en el puerto 443 y SSH en un puerto externo que usted elija al configurar el controlador de entrada, comúnmente el puerto 22. SecurSpaces también es compatible con las políticas de red de Kubernetes, lo que permite a los equipos de seguridad de red aislar la comunicación de pod a pod dentro del clúster y restringir el tráfico a rutas esenciales. Para obtener la lista completa, consulte Puertos y protocolos.

ID	CONTROL	IMPLEMENTACIÓN
SDS-NET-02	Políticas de red	SecurSpaces está en contenedores y requiere un entorno de Kubernetes. Se puede implementar en una nube privada virtual (VPC) o subred aislada. SecurSpaces incluye políticas de red de Kubernetes preconfiguradas para restringir la comunicación interna de pod a pod. Los clientes pueden añadir o personalizar estas políticas para que coincidan con los requisitos de seguridad de su clúster.
SDS-NET-03	Proteger las aplicaciones expuestas	SecurSpaces está diseñado para ejecutarse detrás de los firewalls de aplicaciones web (WAF), proxies inversos y pasarelas API preferidos por el cliente. Estos controles pueden ayudar a filtrar el tráfico web malicioso y proteger contra riesgos comunes de aplicaciones web, incluidas las 10 principales amenazas de OWASP.
SDS-NET-04	Protección de datos de confianza cero	SecurSpaces aplica principios de confianza cero en las capas de aplicación y de red. En la capa de aplicación, cada llamada a la API y solicitud de datos requiere autenticación y autorización explícitas. SecurSpaces verifica los tokens criptográficos antes de conceder acceso a los

ID	CONTROL	IMPLEMENTACIÓN
		datos. En la capa de red, el tráfico desde el controlador de entrada a los servicios de backend se cifra con TLS. Dentro del clúster, SecurSpaces es compatible con las políticas de red de Kubernetes para aislar y restringir la comunicación de pod a pod, de modo que solo los microservicios explícitamente autorizados puedan intercambiar tráfico de red.

Reforzamiento de la plataforma y los contenedores

ID	CONTROL	IMPLEMENTACIÓN
SDS-HRD-01	Línea base de endurecimiento	SecurSpaces utiliza una línea base de contenedores endurecida. Las imágenes de contenedores de servicio principales de SecurSpaces se construyen sobre la imagen Distroless basada en Debian `gcr.io/distroless/static-debian12`, que elimina paquetes, shells y utilidades del sistema innecesarios para minimizar la superficie de ataque explotable. Se utiliza una imagen dedicada basada en Ubuntu solo cuando las características específicas del espacio de trabajo de SecurSpaces requieren utilidades estándar del sistema operativo.

ID	CONTROL	IMPLEMENTACIÓN
SDS-HRD-02	Seguridad de contenedores	Los servicios de backend principales utilizan imágenes mínimas de Debian Distroless para reducir la superficie de ataque. Cuando las características específicas del espacio de trabajo requieren utilidades estándar del sistema operativo, SecurSpaces utiliza imágenes dedicadas de Ubuntu. Dado que SecurSpaces está alojado por el cliente, los clientes son responsables de implementar y operar el escaneo de contenedores en tiempo de ejecución para validar las imágenes contra las líneas base corporativas. SecurSpaces es compatible con estos controles de escaneo.
SDS-HRD-03	Aislamiento de la construcción de imágenes	Las imágenes construidas en la plataforma con Create Image From Existing se ejecutan en un trabajo de Kubernetes utilizando BuildKit sin privilegios de root dentro de un espacio de nombres de usuario. El contenedor de construcción no tiene privilegios y se ejecuta como un usuario no root, todas las capacidades de Linux se eliminan y el proceso de construcción proporcionado por el usuario no tiene ninguna. Los límites de CPU y memoria restringen

ID	CONTROL	IMPLEMENTACIÓN
		la construcción para que un script descontrolado no pueda agotar el nodo, un plazo de tiempo real detiene una construcción colgada y el trabajo nunca se reintenta. La función está inactiva hasta que un administrador de la plataforma configura un registro de destino.

Prevención de pérdida de datos

ID	CONTROL	IMPLEMENTACIÓN
SDS-DLP-01	Prevención de pérdida de datos	SecurSpaces proporciona controles nativos que respaldan una estrategia de prevención de pérdida de datos (DLP). Se puede aplicar seguridad del portapapeles para evitar que los usuarios peguen contenido del IDE o del navegador seguro en aplicaciones externas. La seguridad de las aplicaciones del espacio de trabajo puede requerir que las aplicaciones del espacio de trabajo se abran solo en un navegador seguro, lo que ayuda a reducir el riesgo de exfiltración de datos cuando los desarrolladores comparten aplicaciones internas. Las políticas de red salientes pueden restringir el tráfico del espacio de trabajo a repositorios y dominios aprobados. Los eventos de

ID	CONTROL	IMPLEMENTACIÓN
		auditoría proporcionan visibilidad de la actividad supervisada o bloqueada. Cuando el desarrollo remoto a través de SSH está habilitado, la eficacia de la DLP podría reducirse y debe regirse por la política del cliente. Consulte Controles por capas con la plataforma Citrix.

Registro y supervisión

ID	CONTROL	IMPLEMENTACIÓN
SDS-LOG-01	Aplicar política de registro	SecurSpaces proporciona registro de plataforma estructurado y eventos de auditoría en tiempo real. Los registros de la plataforma capturan el comportamiento de las aplicaciones y los servicios para respaldar la resolución de problemas operativos, la supervisión de la plataforma y las investigaciones de seguridad. La capacidad de auditoría registra eventos relevantes para la seguridad, incluida la autenticación y la actividad de la sesión, las acciones de autorización de usuarios y espacios de trabajo, y los eventos de seguridad de datos como el portapapeles, la carga, la descarga y la actividad de red saliente supervisada. Estos eventos están disponibles en la

ID	CONTROL	IMPLEMENTACIÓN
		página **Auditoría** de SecurSpaces, donde los equipos de seguridad pueden filtrarlos por tipo de evento, gravedad, espacio de trabajo, usuario y fecha y hora. Esto proporciona una pista de auditoría operativa para la investigación y revisión. Los eventos de auditoría de la plataforma también se pueden exportar en formatos estándar para la supervisión posterior y la integración con SIEM.
SDS-LOG-02	Enviar registros a un sistema de gestión de información y eventos de seguridad	SecurSpaces admite la integración con sistemas de gestión de información y eventos de seguridad (SIEM) escribiendo registros de seguridad en formato de evento común (CEF) en los nodos host subyacentes. Estos registros se pueden recopilar y transmitir al SIEM corporativo configurando un reenviador de registros estándar, como Filebeat o Fluent Bit, para supervisar el directorio configurado. Para obtener más información, consulte Integración de SIEM.
SDS-LOG-03	Establecer casos de uso de detección con el CSIRT	La integración de SIEM admite el filtrado de registros por umbral de gravedad y tipo de evento. Esto permite al Equipo de Respuesta a Incidentes de Ciberseguridad

ID	CONTROL	IMPLEMENTACIÓN
		(CSIRT) crear alertas para eventos críticos, como cambios de privilegios o intentos de acceso no autorizados. Para obtener más información, consulte Categorías y atributos de eventos.

Operaciones y resiliencia

ID	CONTROL	IMPLEMENTACIÓN
SDS-OPS-01	Gestión de vulnerabilidades	Citrix escanea continuamente el código fuente de SecurSpaces y las dependencias de software en busca de vulnerabilidades. Los parches de seguridad y las actualizaciones menores se publican periódicamente.
SDS-OPS-02	Gestión de parches	Las implementaciones de SecurSpaces utilizan etiquetas de contenedor estándar y mecanismos de gestión de paquetes. Las actualizaciones se pueden implementar con una interrupción mínima, utilizando enfoques como las actualizaciones continuas o las implementaciones azul-verde, según la configuración de la infraestructura del cliente.
SDS-OPS-03	Aplicar política de copia de seguridad	SecurSpaces separa la lógica de aplicación sin estado de los almacenes de datos con estado. Los clientes pueden

ID	CONTROL	IMPLEMENTACIÓN
		aplicar instantáneas estándar, scripts de copia de seguridad de bases de datos y políticas de retención de copias de seguridad a los volúmenes de almacenamiento subyacentes.
SDS-OPS-04	Segregar entornos de producción y no producción	El modelo de implementación de SecurSpaces admite instancias aisladas. Los clientes pueden implementar clústeres o servidores separados para entornos de desarrollo, preproducción y producción utilizando configuraciones de entorno separadas.

Gobernanza y aseguramiento

ID	CONTROL	IMPLEMENTACIÓN
SDS-GOV-01	Gobernanza y gestión de cambios	SecurSpaces es compatible con las canalizaciones de implementación estándar de DevOps y GitOps. Los cambios en la configuración de la aplicación se pueden rastrear mediante el control de versiones y la infraestructura como código (IaC). Las actualizaciones y los cambios de configuración se documentan en las notas de la versión. Para obtener más información, consulte Novedades de SecurSpaces.

ID	CONTROL	IMPLEMENTACIÓN
SDS-GOV-02	Proporcionar documentación de arquitectura	La documentación de la arquitectura de SecurSpaces está disponible en la documentación del producto. También se puede proporcionar un diagrama de flujo de datos como anexo cuando sea necesario. Para obtener más información, consulte Arquitectura.
SDS-GOV-03	Inventario de aplicaciones	Citrix puede proporcionar un inventario de aplicaciones y componentes para la plataforma SecurSpaces bajo petición. Los clientes deben especificar el nivel de detalle requerido para su evaluación.
SDS-GOV-04	Infraestructura y acceso	SecurSpaces está alojado por el cliente. El acceso físico, al sistema operativo y a nivel de infraestructura es controlado y gestionado por el cliente. SecurSpaces no requiere conectividad de proveedor entrante externa para funcionar.
SDS-GOV-05	Pila de seguridad en la plataforma SecurSpaces	Las configuraciones de implementación de SecurSpaces, como los gráficos de Helm o los manifiestos de Kubernetes, y las imágenes de contenedor entregadas son compatibles con la validación a través de la pila de seguridad del cliente. Aunque no se proporciona código fuente propietario, SecurSpaces

ID	CONTROL	IMPLEMENTACIÓN
		admite el linting automatizado de infraestructura como código, las comprobaciones de cumplimiento de la configuración y el escaneo de vulnerabilidades de imágenes de contenedor, incluido el análisis de composición de software (SCA), antes de la implementación.
SDS-GOV-06	Diligencia debida de terceros	Citrix puede proporcionar documentación estándar de garantía de terceros bajo petición. Los clientes deben especificar los artefactos necesarios para su revisión.
SDS-GOV-07	Anexo de seguridad	Se puede proporcionar un diagrama de flujo de datos como parte del anexo de seguridad cuando sea necesario para fines de evaluación o auditoría.
SDS-GOV-08	Acuerdo de confidencialidad	Los acuerdos de confidencialidad están cubiertos como parte del marco contractual global con Citrix.

Información relacionada

- Flujos de datos de seguridad
- Límites de confianza
- Puertos y protocolos
- Criptografía
- Políticas de red

Trust boundaries

Cuando una implementación de Citrix SecurSpaces™ separa un nivel de confianza de otro, qué refuerza cada separación, y qué lado le pertenece a usted. Esta página sirve de apoyo para la revisión de la seguridad de la red y la evaluación de la arquitectura.

Describe los límites que implementa la plataforma. No es un modelo de amenazas: no enumera adversarios, casos de abuso o clasificaciones de riesgo.

Resumen

LÍMITE	REFORZADO POR	PROPIETARIO
Su red al clúster	Controlador de entrada, terminación TLS	Usted
Entrada a los servicios de SecurSpaces	Kubernetes NetworkPolicy, TLS	SecurSpaces
Servicios de SecurSpaces a la base de datos	Kubernetes NetworkPolicy	SecurSpaces
Espacio de trabajo a espacio de trabajo	Kubernetes NetworkPolicy	SecurSpaces
Espacio de trabajo a internet	Una política de red de Kubernetes confina el espacio de trabajo al servicio de proxy, que luego aplica la política de red de SecurSpaces adjunta a él.	SecurSpaces, configurado por usted
Plataforma a la API de Kubernetes	Kubernetes RBAC	SecurSpaces
Clúster a los nodos y al host	Su configuración de clúster	Usted

Importante:

Cada límite dentro del clúster en esta página es una política de red de Kubernetes, por lo que solo es válida si su clúster ejecuta un complemento de red que implementa la API de

> NetworkPolicy `networking.k8s.io/v1`. Si no lo hace, estas políticas son aceptadas por el servidor de API y no hacen nada en silencio. Consulte Requisitos.

El perímetro

El tráfico llega al despliegue a través del controlador de entrada. TLS finaliza allí, por lo que las versiones de TLS y los conjuntos de cifrado permitidos forman parte de su configuración de entrada en lugar de algo que SecurSpaces establezca.

El equilibrador de carga delante del controlador de entrada opera en la Capa 4 y no finaliza TLS.

Para los puertos que deben ser accesibles, consulte Puertos y protocolos.

Dentro del clúster

SecurSpaces etiqueta sus pods por tipo y envía NetworkPolicies que actúan sobre esas etiquetas.

TIPO DE POD	ETIQUETA
Servicios de plataforma	`strong.network/type: service`
Base de datos	`strong.network/type: database`
Espacios de trabajo y navegadores seguros	`strong.network/type: workspace`, `strong.network/type: browser`
Espacios de trabajo con una política de red adjunta	`strong.network/hardened: no_egress`

> **Importante:**

> No cambie el nombre de estas etiquetas. Las NetworkPolicies las seleccionan, y una etiqueta renombrada produce una política que no coincide con nada, sin error.

Los pods de servicio aceptan tráfico de cualquier origen

La NetworkPolicy para los pods `service` acepta el tráfico de entrada desde cualquier origen. Esto es intencional —son el punto de entrada para la implementación—, pero significa que el perímetro alrededor de los servicios de la plataforma es su configuración de entrada, no una NetworkPolicy.

La política de base de datos

SecurSpaces incluye una NetworkPolicy que restringe el tráfico de entrada a los pods etiquetados `database`, aceptando conexiones solo de pods etiquetados `service`.

> **Importante:**

> Una NetworkPolicy solo cubre los pods que llevan la etiqueta que selecciona. Si sus pods de base de datos la llevan depende de cómo se implemente la base de datos, y una base de datos que se ejecuta fuera del clúster no está cubierta en absoluto. Confirme que la etiqueta esté presente en sus pods de base de datos antes de tratar esta política como el control que los aísla, y aplique sus propios controles de red donde no lo esté.

Los espacios de trabajo aceptan tráfico solo de la API del espacio de trabajo

Los pods etiquetados `workspace` o `browser` aceptan el tráfico de entrada solo del pod de la API del espacio de trabajo.

Esto es lo que aísla los espacios de trabajo entre sí. Un espacio de trabajo no puede abrir una conexión a otro, y esto se mantiene independientemente de si hay una política de red adjunta o no, porque se aplica en el lado receptor.

La salida del espacio de trabajo depende de la política adjunta

Dos mecanismos diferentes comparten el nombre *política de red*, y ambos están involucrados aquí.

Un espacio de trabajo lleva la etiqueta `strong.network/hardened: no_egress` solo mientras una **política de red de SecurSpaces** esté adjunta a él. Una **Kubernetes NetworkPolicy** selecciona los pods con esa etiqueta y les permite enviar tráfico solo a los pods `service`, lo que deja al servicio proxy de SecurSpaces como la única ruta de salida del espacio de trabajo. El servicio proxy luego permite o rechaza cada destino según la política de red de SecurSpaces.

Así, la Kubernetes NetworkPolicy decide que un espacio de trabajo solo puede comunicarse con el servicio proxy. La SecurSpaces política de red decide a dónde lo llevará el servicio proxy.

> **Importante:**

> Un espacio de trabajo sin una política de red adjunta no se etiqueta como reforzado, por lo que esta NetworkPolicy no se le aplica y su tráfico saliente no está restringido por la plataforma. La restricción de salida es algo que se activa adjuntando una política. Consulte Políticas de red.

Acceso de la plataforma a la API de Kubernetes

La API del espacio de trabajo gestiona el ciclo de vida del espacio de trabajo a través de la API de Kubernetes, utilizando una cuenta de servicio con ámbito en el espacio de nombres de la versión.

ÁMBITO	ACCESO
Espacio de nombres	Pods, servicios, secretos, reclamaciones de volumen persistente, mapas de configuración, cuentas de servicio, eventos, trabajos, despliegues y conjuntos con estado, registros de pods y un arrendamiento con nombre
A nivel de clúster	Clases de almacenamiento y volúmenes persistentes, solo lectura. Nodos y métricas de nodos, solo lectura.

El acceso de escritura a los volúmenes persistentes no se concede por defecto. Se habilita mediante la configuración de Helm `platform.serviceKubernetesConfig.rbac.allowPersistentVolumeAccess`, que por defecto es `false`.

Concéderlo solo para los modos de adjuntar en los que SecurSpaces construye el volumen por sí mismo: Azure Files Attach Existing, y el modo AWS Attach Existing en el que un usuario proporciona las coordenadas del sistema de archivos y SecurSpaces construye un volumen estático a partir de ellas. Adjuntar un PersistentVolume que usted haya creado no lo necesita — SecurSpaces solo crea la reclamación, por lo que el acceso de lectura anterior es suficiente, y nunca modifica un volumen de su propiedad. Crear un nuevo punto de montaje tampoco lo necesita. Mientras la configuración está desactivada, los modos que lo requieren se ocultan y rechazan, y los otros modos siguen funcionando. Consulte Configurar SecurSpaces para puntos de montaje de AWS.

Cambios a nivel de host en los nodos del espacio de trabajo

SecurSpaces ejecuta un DaemonSet en nodos que no están etiquetados como nodos de servicio. Su contenedor de inicio se ejecuta como root con `privileged: true`, en los espacios de nombres de red, PID e IPC del host, y monta `/sys` del host.

Establece estos parámetros del kernel en esos nodos:

PARÁMETRO	VALOR	PROPÓSITO
`kernel.unprivileged_userns_clone`	`1`	Permite espacios de nombres de usuario sin privilegios, que requieren los contenedores sin raíz en los espacios de trabajo
`user.max_user_namespaces`	`49152`	Aumenta el límite del espacio de nombres de usuario por la misma razón
`fs.inotify.max_user_watches`	`1524288`	Aumenta el límite de vigilancia de archivos que el IDE necesita en repositorios grandes
`kernel.yama.ptrace_scope`	`0`	Permite que un depurador se adjunte a un proceso en ejecución. Los desarrolladores necesitan esto para depurar binarios compilados, como C y C++, dentro de un espacio de trabajo. Esto relaja la restricción predeterminada en la mayoría de las distribuciones.
`fs.suid_dumpable`	`0`	Evita volcados de memoria de programas setuid
`kernel.core_pattern`	`/dev/null`	Descarta los volcados de memoria en lugar de escribirlos en el disco

Estos son ajustes a nivel de nodo y se aplican a todo lo programado en esos nodos. Si ejecuta otras cargas de trabajo en los mismos nodos, téngalo en cuenta al planificar los grupos de nodos.

Trabajar desde un IDE local

Un desarrollador puede trabajar en el IDE en la nube en un navegador, o conectar un IDE local a través de SSH. La segunda es un canal de acceso compatible en lugar de una solución alternativa, pero no es equivalente: un IDE local es un software que se ejecuta en el punto final, por lo que amplía ligeramente el límite. Esta sección es lo que un revisor de seguridad necesita para juzgar cuánto.

El entorno de desarrollo en sí no se mueve. El código, la ejecución y las credenciales permanecen en el espacio de trabajo independientemente del canal utilizado; lo que cambia es dónde se renderiza el editor.

Dónde reside cada artefacto

ARTEFACTO	RESIDE	¿EN EL PUNTO FINAL?
Código fuente	Sistema de archivos del espacio de trabajo	No. El IDE local lo edita de forma remota y no lo escribe en el disco local
Credenciales del repositorio	Gestionado por el servicio de proxy de SecurSpaces	No. Nunca expuesto al punto final, y tampoco legible desde dentro del espacio de trabajo
Clave SSH que abre el túnel	El punto final del desarrollador	**Sí, necesariamente.** Esta es la clave que autentica al desarrollador en el espacio de trabajo
Identidad SSH personal, utilizada para cualquier servicio SSH	Mantenida por la plataforma y presentada por el servicio de proxy de SecurSpaces cuando se establece la conexión	No. No se escribe en el espacio de trabajo, por lo que un proceso allí no puede copiarla
Servicios SSH adjuntos como recursos del proyecto	Mantenidos por la plataforma, inyectados de la misma manera	No

ARTEFACTO	RESIDE	¿EN EL PUNTO FINAL?
Artefactos de compilación	Sistema de archivos del espacio de trabajo	No, a menos que un desarrollador los copie deliberadamente, lo cual está regido por los controles de egreso y transferencia
Cachés de paquetes de lenguaje, como npm y pip	Sistema de archivos del espacio de trabajo	No
Contexto del modelo de IA	Dentro del espacio de trabajo y del límite de la política, atribuido por usuario, proyecto y espacio de trabajo	No
Datos de extensión del IDE	Dividido. Las extensiones que renderizan la interfaz de usuario se ejecutan en el punto final; las extensiones que ejecutan código se ejecutan en el espacio de trabajo	**Parcialmente.** El host de extensión de la interfaz de usuario es la única parte del IDE que es genuinamente local

Nota:

Los dos roles de clave SSH son fáciles de confundir y la distinción es importante. La clave que abre el túnel es propia del desarrollador y reside en su máquina, como cualquier clave de cliente SSH. La clave que el *espacio de trabajo* presenta cuando se conecta —su identidad SSH personal, o un servicio SSH adjunto como recurso de proyecto— es mantenida por la plataforma y no llega ni al punto final ni al tiempo de ejecución del espacio de trabajo. Véase Cómo se gestionan las conexiones SSH.

Lo que el punto final aún puede ver

Dado que el IDE se renderiza localmente, un punto final comprometido aún podría capturar pulsaciones de teclas, contenido de pantalla o datos del portapapeles, y el host de extensión ejecuta código local. Los controles del portapapeles siguen aplicándose, pero se aplican a la sesión en lugar de al sistema operativo.

Esto es inherente a cualquier modelo de desarrollo remoto basado en SSH, más que específico de SecurSpaces, y es una superficie de ataque menor que la de un portátil o una sesión VDI con un subsistema Linux local, donde el código fuente, las credenciales, y las cachés de paquetes son todos genuinamente locales. Sigue siendo mayor que el IDE en la nube, por lo que el desarrollo remoto a través de SSH es una configuración que un administrador activa deliberadamente. Consulte Política de espacio de trabajo.

Lo que usted posee

SecurSpaces está alojado por el cliente, por lo que lo siguiente está fuera del límite que controla la plataforma:

- El controlador de entrada y su configuración TLS.
- Un complemento de red que aplica NetworkPolicy. Sin uno, los límites dentro del clúster mencionados anteriormente no se mantienen.
- El endurecimiento del clúster y los nodos, y qué cargas de trabajo comparten un grupo de nodos con los espacios de trabajo.
- Cifrado en reposo para la base de datos, volúmenes persistentes y `etcd`.
- Escaneo de contenedores en tiempo de ejecución y control de admisión de imágenes.
- La accesibilidad de la red entre el clúster y cualquier dependencia externa, como la base de datos, los registros, los proveedores de repositorios y su SIEM.

Información relacionada

- Cómo funciona el servicio de proxy de SecurSpaces
- Flujos de datos de seguridad
- Catálogo de controles de seguridad
- Puertos y protocolos
- Criptografía
- Políticas de red
- Requisitos

How the SecurSpaces proxy service works

La mayoría de las afirmaciones de seguridad en esta documentación se resuelven en un solo componente. Las credenciales no llegan a la máquina del desarrollador porque el servicio proxy de SecurSpaces las retiene. La salida está restringida porque el servicio proxy la filtra. El gasto en

IA es atribuible porque el servicio proxy lo etiqueta. El acceso al repositorio es auditable porque el servicio proxy lo ve.

Esta página explica lo que hace ese componente. No hay nada que configurar en él: el servicio proxy no es opcional y no tiene configuraciones propias. Lo que se configura es la política de red, los recursos del proyecto y el enrutamiento de IA, cada uno documentado por separado.

Por qué todo pasa a través de él

Un espacio de trabajo de Citrix SecurSpaces™ no tiene una ruta directa a nada. No puede acceder a internet, a sus repositorios o a sus sistemas internos por sí mismo; cada conexión que abre termina primero en el servicio proxy. primero.

Esa única propiedad es lo que hace que los demás controles sean aplicables en lugar de meramente consultivos. Una política que un espacio de trabajo pudiera eludir sería una recomendación. Debido a que no hay un camino que evite el servicio proxy, un desarrollador con control total de su propio espacio de trabajo —incluyendo el acceso de root en un contenedor que haya construido— aún no puede alcanzar un destino que la política prohíbe, y aún no puede leer las credenciales que sus herramientas están utilizando.

Qué pasa a través de él

TRÁFICO	QUÉ HACE EL SERVICIO PROXY
HTTP y HTTPS	Aplica la política de red, gestiona las credenciales para repositorios y servicios, y registra la solicitud
Git sobre HTTP, incluyendo Git LFS	Enruta el tráfico del repositorio para que el acceso utilice credenciales mantenidas por la plataforma y siga la política
DNS	Resuelve nombres para el espacio de trabajo, incluyendo los nombres internos utilizados para acceder a las aplicaciones del espacio de trabajo
TCP y UDP	Transporta tráfico para servicios que no son HTTP

TRÁFICO	QUÉ HACE EL SERVICIO PROXY
SSH	Transporta SSH saliente, cuando un administrador lo ha habilitado y se ha configurado un método para el host de destino

Las credenciales se retienen, no se entregan

Cuando un espacio de trabajo accede a un repositorio o a un servicio externo, no presenta una credencial, porque no tiene ninguna. Se dirige al destino mediante un identificador que la plataforma asigna, y el servicio proxy resuelve eso al punto final real y adjunta la credencial en el camino.

Las consecuencias prácticas merecen ser expuestas claramente:

- No se escribe nada de larga duración en la máquina del desarrollador, independientemente del IDE o método de conexión que utilice.
- Tampoco se escribe nada legible dentro del espacio de trabajo, por lo que un espacio de trabajo comprometido no produce una credencial utilizable.
- Revocar el acceso en la plataforma surte efecto en la siguiente solicitud, sin afectar a ningún punto final o espacio de trabajo.

La política se aplica aquí

Las políticas de red adjuntas a nivel de plataforma, organización y proyecto se combinan, y el resultado se aplica a cada conexión. Se deniega un destino que ninguna política permite.

Las políticas se evalúan tanto contra la dirección como contra el dominio, por lo que una lista de permitidos funciona incluso cuando un destino se resuelve en un conjunto cambiante de direcciones. Para saber cómo se escriben y asignan las políticas, consulte Políticas de red.

Cómo se gestionan las conexiones HTTPS

Una conexión HTTPS desde un espacio de trabajo son dos conexiones. El servicio proxy termina la conexión desde el espacio de trabajo, lee la solicitud, decide qué hacer con ella, luego abre su propia conexión al destino y reenvía la solicitud allí.

Esto es lo que hace posible el resto de los controles de la plataforma sobre el tráfico cifrado:

EL SERVICIO DE PROXY PUEDE	PORQUE LEE LA SOLICITUD
Aplicar políticas a un dominio en lugar de solo a una dirección IP	El destino está en la solicitud, no solo en el handshake TLS
Adjuntar una credencial de repositorio o servicio	La credencial se añade a una solicitud que el espacio de trabajo nunca ve
Atribuir el uso de IA a un usuario, proyecto y espacio de trabajo	Se añaden encabezados de identificación antes de que se reenvíe la solicitud
Enrutar el tráfico del proveedor a una puerta de enlace de IA	El destino se compara con los puntos finales configurados

Nada de eso es posible mientras la conexión sea opaca para la plataforma.

En qué confía el espacio de trabajo

Dado que el servicio de proxy presenta su propio certificado al espacio de trabajo, este debe confiar en la autoridad de certificación que lo emitió. SecurSpaces añade su certificado de CA de servicio a los almacenes de confianza del espacio de trabajo al inicio, por lo que las herramientas HTTPS dentro de un espacio de trabajo funcionan sin configuración por herramienta.

Una consecuencia que vale la pena conocer: una herramienta que fija un certificado, o que utiliza su propio almacén de confianza en lugar del del sistema, puede rechazar la conexión. Algunos entornos de ejecución de lenguajes y gestores de paquetes hacen esto. Consulte Requisitos de la imagen del contenedor.

Dónde ocurre el descifrado

El descifrado ocurre dentro del despliegue que usted aloja, en los pods del servicio proxy, y la solicitud se vuelve a cifrar antes de que salga hacia el destino. El tráfico no se envía a Citrix y no se descifra en ningún lugar fuera de su clúster. En SecurSpaces Flex, lo mismo ocurre con el entorno gestionado por Citrix que se asigna a su organización asignado.

> **Nota:**

> **Inspeccionar** también nombra un comportamiento específico de la política de red, que informa sobre el contenido TCP y se aplica a través de la política integrada de **Inspeccionar Tráfico**. Esa es una configuración separada y opcional. El manejo descrito aquí se aplica a

> HTTPS siempre que se adjunte una política de red de SecurSpaces, independientemente del comportamiento que utilice la política. Consulte Políticas de red.

Cómo se gestionan las conexiones SSH

SSH se gestiona de la misma manera estructuralmente —una conexión SSH desde un espacio de trabajo también son dos conexiones en lugar de un túnel— con una diferencia importante. El servicio proxy no lee el contenido de una sesión SSH. Termina el transporte, decide si la conexión está permitida y presenta la credencial correcta, pero lo que pasa después no se examina.

Un espacio de trabajo abre una conexión SSH al servicio proxy en lugar de al destino. El servicio proxy autentica el espacio de trabajo, aplica la política de red de SecurSpaces al destino, luego abre una conexión separada y se autentica en el propio destino.

La credencial que presenta es la identidad SSH personal del desarrollador, que la plataforma guarda. Se lee del gestor de secretos en el momento en que se establece la conexión y se utiliza para firmar el handshake; no se escribe en el espacio de trabajo, por lo que un proceso dentro del espacio de trabajo no puede copiarla.

> **Nota:**

> El SSH entrante —un desarrollador que se conecta desde un IDE local a su espacio de trabajo— es terminado por el servicio de espacio de trabajo en lugar del servicio proxy. Esa conexión se autentica contra la clave pública registrada del desarrollador y la sesión se registra. El servicio proxy gobierna el tráfico que sale de un espacio de trabajo.

> Lo que esto significa para una evaluación:

- Un espacio de trabajo no puede abrir una conexión SSH a un destino que la política de red de SecurSpaces no permite.
- La clave privada utilizada para sistemas externos nunca está en el espacio de trabajo.
- El contenido de la sesión no se descifra ni se registra. Los comandos escritos en una sesión SSH no son registrados por el servicio proxy, por lo que SSH no proporciona la visibilidad a nivel de solicitud que sí ofrece HTTPS.

Lo que no hace

- **No es el proxy de salida propio de su organización.** Si su organización requiere que el tráfico saliente pase a través de un proxy existente propio, eso se configura por separado y se encuentra aguas abajo. Consulte Configuración de proxy externo.
- **No es un firewall de aplicaciones web.** Gobierna dónde puede conectarse un espacio de trabajo y qué identidad se utiliza, no el contenido de las cargas útiles de la aplicación.
- **No inspecciona el contenido de las sesiones SSH.** Consulte Cómo se gestionan las conexiones SSH.
- **No gobierna el tráfico del Protocolo de Contexto del Modelo.** Consulte AI Gateway.

Información relacionada

- Límites de confianza
- Flujos de datos de seguridad
- Políticas de red
- Configurar el enrutamiento de AI Gateway
- Puertos y protocolos
- Configuración del proxy externo

Layered controls with the Citrix platform

SecurSpaces aplica sus propios controles en el entorno de desarrollo. También se ejecuta dentro de la plataforma más amplia de Citrix , por lo que la capa de acceso delante de un espacio de trabajo puede tener sus propios controles.

Esta página separa ambos, para que pueda ver qué control proviene de dónde al evaluar la cobertura o cerrar una brecha específica.

Lo que SecurSpaces aplica

Estas son propiedades de la propia plataforma y se aplican independientemente de cómo un desarrollador acceda a un espacio de trabajo.

CONTROL	LO QUE APLICA
Aislamiento del código fuente	El código permanece en el espacio de trabajo y nunca se clona en el punto final

CONTROL	LO QUE APLICA
Intermediación de credenciales	Las credenciales del repositorio y del servicio son gestionadas por la plataforma y se inyectan en tiempo de ejecución, en lugar de almacenarse en la máquina del desarrollador
Control del portapapeles	Se puede bloquear la copia desde el IDE o el navegador seguro
Confinamiento de la aplicación del espacio de trabajo	Se puede exigir que una aplicación publicada desde un espacio de trabajo se abra solo en un navegador seguro
Política de salida de red	El tráfico saliente está restringido a repositorios y dominios aprobados, aplicado en el proxy
Auditoría	Cada acción se registra y se puede exportar a un SIEM

Consulte el catálogo de controles para ver el conjunto completo con identificadores.

Qué añade la capa de acceso

SecurSpaces se integra con los componentes de Citrix que ya pueda estar ejecutando, en lugar de introducir una segunda pila de acceso. Cada uno rige la ruta al espacio de trabajo, no el espacio de trabajo en sí.

COMPONENTE	QUÉ RIGE
Citrix DaaS	Entrega de escritorios y aplicaciones publicadas, incluyendo el acceso a un espacio de trabajo desde un VDA
Secure Private Access	Acceso de confianza cero a aplicaciones privadas, incluyendo la postura del dispositivo y el acceso condicional antes de que se inicie una sesión
Chrome Enterprise Premium	Controles a nivel de navegador en la propia sesión, como restricciones en la impresión,

COMPONENTE	QUÉ RIGE
	capturas de pantalla y transferencia de archivos
Citrix Workspace	Un único punto de entrada a todo lo anterior

Para saber qué aplica cada uno de ellos y cómo configurarlo, consulte la documentación propia de ese producto. Esta página describe únicamente cómo se relacionan con SecurSpaces.

Donde las capas importan más

Dos casos en los que un control de la capa de acceso cierra algo que SecurSpaces no puede cerrar por sí solo.

Desarrollo remoto a través de SSH. Cuando un desarrollador conecta un IDE local a través de SSH, los controles del espacio de trabajo siguen aplicándose al entorno, pero la sesión termina en una máquina que SecurSpaces no gobierna. Las restricciones de portapapeles y transferencia de archivos que dependen del navegador no se aplican. Cuando esto sea relevante, restrinja el acceso SSH por rol, o gobierne el punto final a través de la capa de acceso. Esta limitación se establece en el catálogo de controles como SDS-DLP-01.

Dispositivos no gestionados y de contratistas. SecurSpaces mantiene el código fuente fuera del dispositivo, lo que constituye la mayor parte del riesgo. Los controles sobre lo que el *usuario* puede hacer con la sesión renderizada —captura de pantalla, impresión, copia a una aplicación local— pertenecen al navegador o a la capa de acceso, en lugar de al espacio de trabajo.

Licencias

SecurSpaces se incluye en la licencia de plataforma de Citrix, sin nueva SKU y sin límite de usuarios. El derecho a los demás componentes mencionados anteriormente depende de su acuerdo; confirme lo que su organización tiene con su equipo de cuentas de Citrix antes de planificar un diseño en torno a ellos.

Información relacionada

- Catálogo de controles de seguridad
- Límites de confianza
- Flujos de datos de seguridad
- Políticas de red

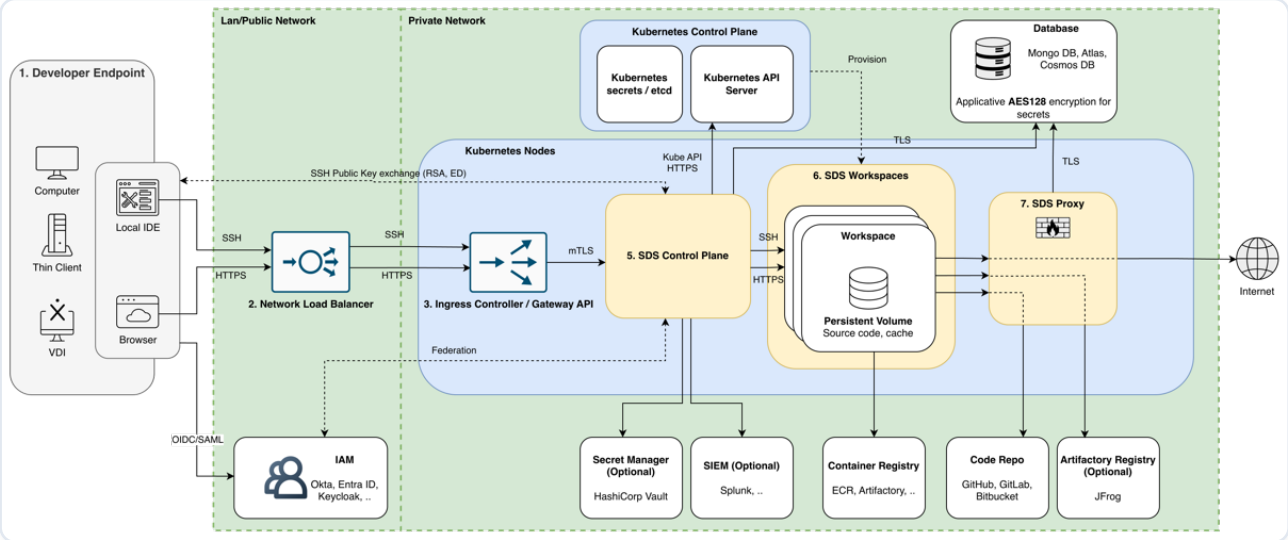
- Trabajar desde un VDA

Security data flows

Introducción

Este documento proporciona una visión general centrada en la seguridad de la arquitectura de Citrix SecurSpaces™ y los principales flujos de datos entre los componentes centrales y las dependencias externas. Explica cómo el acceso de los usuarios, el manejo del tráfico, la federación de identidades, el aislamiento del espacio de trabajo, la gestión de secretos y las integraciones externas ayudan a proteger la actividad de desarrollo sensible y a mantener un modelo operativo seguro.

Resumen del flujo de datos



FLUJO N.º	COMPONENTE	FLUJO DE DATOS DE SEGURIDAD
1.	Punto final del desarrollador	El punto final del desarrollador representa el dispositivo del usuario, como un ordenador físico, un cliente ligero o una sesión de infraestructura de escritorio virtual (VDI). Los usuarios acceden a SecurSpaces a través de un IDE local por SSH o a través de un navegador web por HTTPS. La actividad de desarrollo se

FLUJO N.º	COMPONENTE	FLUJO DE DATOS DE SEGURIDAD
		ejecuta de forma remota, lo que ayuda a evitar que el código fuente sensible se almacene en el punto final local.
2.	Balanceador de carga de red	El balanceador de carga de red proporciona conectividad de capa 4 entre la red pública o empresarial y el entorno privado de SecurSpaces. No termina TLS. En su lugar, reenvía sesiones TCP sin procesar y conserva el cifrado de extremo a extremo hasta que el tráfico llega al controlador de entrada.
3.	Controlador de entrada o API de Gateway	El controlador de entrada de Kubernetes o la API de Gateway proporciona enrutamiento de tráfico de capa 7 para los servicios de SecurSpaces y actúa como el punto de terminación TLS para el tráfico HTTPS. Al terminar TLS en esta capa, puede inspeccionar los metadatos de la solicitud y aplicar reglas de enrutamiento que dirigen el tráfico a los servicios internos de SecurSpaces apropiados. La comunicación descendente entre la capa de entrada y los servicios internos de SecurSpaces se cifra con TLS. Las versiones de TLS y los conjuntos de cifrado permitidos para el

FLUJO N.º	COMPONENTE	FLUJO DE DATOS DE SEGURIDAD
		tráfico externo se configuran mediante la configuración de entrada del cliente.
4.	Gestión de identidades y accesos	SecurSpaces puede integrarse con un proveedor de identidades (IdP) empresarial para admitir la autenticación federada a través del inicio de sesión único (SSO) corporativo utilizando estándares como OpenID Connect (OIDC) o SAML. Cuando se utiliza esta integración, las credenciales de usuario permanecen gestionadas por el sistema de identidades del cliente en lugar de almacenarse en SecurSpaces. SecurSpaces también puede operar como el proveedor de identidades y gestionar las credenciales de usuario directamente.
5.	Plano de control de SecurSpaces	El plano de control de SecurSpaces contiene la lógica de aplicación central y actúa como el centro principal de seguridad y gestión. Realiza la terminación SSH y TLS para el enrutamiento y el proxy de tráfico, lo que permite la inspección del tráfico y la auditoría detallada de las sesiones de usuario. También proporciona la interfaz de usuario de administración web y la API central de

FLUJO N.º	COMPONENTE	FLUJO DE DATOS DE SEGURIDAD
		SecurSpaces, que aloja la lógica de negocio principal de la plataforma. Para la gestión de espacios de trabajo, el plano de control envía solicitudes de orquestación al plano de control de Kubernetes para gestionar el ciclo de vida del espacio de trabajo, incluyendo el aprovisionamiento, el escalado y la desmantelación. Las operaciones de gestión de espacios de trabajo siguen un modelo de control de acceso basado en roles (RBAC) de Kubernetes basado en el principio de privilegio mínimo.
6.	Espacios de trabajo y almacenamiento de SecurSpaces	Los espacios de trabajo son entornos efímeros y en contenedores aislados dentro de la red privada. Los datos persistentes se almacenan en volúmenes cifrados para que el código fuente y las cachés de compilación permanezcan seguros y aislados si un espacio de trabajo se reinicia o se destruye.
7.	Servicio de proxy de SecurSpaces	El servicio de proxy de SecurSpaces funciona como un firewall de salida de espacio de trabajo dedicado para ayudar a prevenir la exfiltración de datos. Para

FLUJO N.º	COMPONENTE	FLUJO DE DATOS DE SEGURIDAD
		saber qué hace y por qué cada conexión pasa a través de él, consulte Cómo funciona el servicio de proxy de SecurSpaces. El tráfico saliente de los espacios de trabajo se enruta a través de este componente para el filtrado de URL. Esto ayuda a garantizar que los espacios de trabajo se comuniquen solo con dominios externos aprobados y ayuda a prevenir transferencias de datos no autorizadas a Internet.
8.	Dependencias externas	SecurSpaces se basa en componentes externos para gestionar los datos de la aplicación, las imágenes de contenedor, el acceso al código y la telemetría de seguridad. La conectividad entre SecurSpaces y estas dependencias es gestionada por el cliente utilizando mecanismos de integración de red privada como el enrutamiento privado, VPN, emparejamiento de red o puntos de conexión privados. Estos controles ayudan a mantener el tráfico dentro de un límite de red seguro y controlado.
9.	Secretos de Kubernetes	SecurSpaces utiliza Secretos de Kubernetes nativos para gestionar certificados, claves de acceso, claves de cifrado,

FLUJO N.º	COMPONENTE	FLUJO DE DATOS DE SEGURIDAD
		credenciales de base de datos y claves privadas de JSON Web Token (JWT). Por defecto, estos secretos se almacenan en `etcd`, que debe protegerse con cifrado en reposo. Para entornos con requisitos de seguridad más altos, SecurSpaces puede integrarse con mecanismos avanzados de Kubernetes como el controlador CSI de Secrets Store o los operadores de External Secrets.

Flujos de datos de dependencias externas

DEPENDENCIA	FLUJO DE DATOS DE SEGURIDAD
Base de datos MongoDB	Almacena el estado de la aplicación. SecurSpaces utiliza AES-128-GCM para proteger datos sensibles en la capa de aplicación, incluidos los secretos personales del desarrollador.
Repositorios de código	Las integraciones de repositorios Git se enrutan a través del servicio proxy de SecurSpaces, lo que permite el SSO y aplica las políticas de seguridad de SecurSpaces para el acceso y la gestión de repositorios Git.
Registro de contenedores	Aloja las imágenes de contenedor utilizadas por los espacios de trabajo de SecurSpaces. Las imágenes se pueden almacenar en uno o más registros, dependiendo del entorno del cliente. Un registro de contenedores también proporciona imágenes para los componentes centrales de SecurSpaces, como el plano de control de SecurSpaces y el servicio proxy de

DEPENDENCIA	FLUJO DE DATOS DE SEGURIDAD
	SecurSpaces. Estos flujos de imágenes de componentes centrales suelen omitirse de los diagramas de flujo de datos de alto nivel porque no son configurables en SecurSpaces.
SIEM	Recibe registros de auditoría y eventos de seguridad de SecurSpaces para la monitorización centralizada, el cumplimiento y las alertas. Algunos ejemplos incluyen plataformas SIEM como Splunk.

Flujos de datos de secretos de Kubernetes

TIPO DE SECRETO	USO
Certificados	Claves TLS para el plano de control de SecurSpaces y los componentes internos.
Claves de acceso	Claves privadas SSH para la autenticación del espacio de trabajo. Las identidades SSH personales utilizan Ed25519.
Claves de cifrado	Claves AES-128 utilizadas con AES-GCM para la protección de datos a nivel de aplicación.
Credenciales de base de datos	Contraseñas y credenciales de conexión para MongoDB.
Claves privadas JWT	Claves utilizadas para la firma segura de tokens.

Puertos y criptografía

Para los puertos expuestos externamente y los algoritmos utilizados para cada propósito, consulte Puertos y protocolos y Criptografía. Para saber dónde la implementación separa un nivel de confianza de otro, consulte Límites de confianza.

Consideraciones de seguridad

SecurSpaces utiliza un modelo de seguridad por capas en las capas de punto final, red, aplicación, espacio de trabajo e infraestructura. El cliente sigue siendo responsable de la seguridad del entorno de alojamiento, incluyendo los límites de la red, el cifrado en reposo para los servicios de infraestructura, el endurecimiento del clúster de Kubernetes y la protección de `etcd`.

Cuando la implementación requiere una protección de secretos más sólida, los clientes pueden utilizar integraciones nativas de Kubernetes, como Secrets Store CSI Driver o External Secrets Operators, para conectar SecurSpaces con una plataforma de gestión de secretos empresarial.

Network policies

Las políticas de red controlan el tráfico de red saliente que los espacios de trabajo pueden generar. Con una política de red, puedes supervisar dónde se conecta un espacio de trabajo, restringirlo a un conjunto aprobado de dominios y direcciones IP, o inspeccionar su tráfico, y ver cada uno de esos eventos en el panel de control de **Auditoría**.

Esta página explica el modelo. Para las tareas, consulta:

- Crear una política de red
- Asignar y aplicar una política
- Supervisar y solucionar problemas
- Campos de la política de red

Comportamientos de la política

Cada política aplica uno de tres comportamientos al tráfico saliente.

COMPORTAMIENTO	QUÉ HACE
Supervisar	El tráfico TCP está permitido y se registra sin restricciones. Utiliza esto para ver dónde se conecta un espacio de trabajo sin limitarlo a una lista de permitidos.
Restringir	El tráfico está bloqueado por defecto. Solo se puede acceder a los recursos adjuntos y a los dominios y direcciones IP de la lista de

COMPORTAMIENTO	QUÉ HACE
	permitidos. Las solicitudes bloqueadas se registran.
Inspeccionar	El contenido del tráfico TCP se inspecciona y se informa. Utilice esto cuando necesite la visibilidad más profunda de lo que envía un espacio de trabajo.

Nota:

Usted configura el comportamiento de **monitorización** y **restricción** cuando crea o edita una política. La **inspección** se proporciona solo a través de la política integrada **Inspeccionar tráfico (predeterminado, experto)**. Puede aplicarla a los espacios de trabajo, pero no puede crear una nueva política de inspección en el editor de políticas.

Qué sucede cuando se adjunta una política

Adjuntar cualquier política cambia la forma en que el espacio de trabajo accede a la red, independientemente del comportamiento que la política aplique.

Un espacio de trabajo con una política adjunta se etiqueta como reforzado, y una Kubernetes NetworkPolicy le permite entonces enviar tráfico solo a los pods de servicio de SecurSpaces. Por lo tanto, todo el tráfico saliente pasa a través del servicio de proxy de SecurSpaces. El DNS sigue funcionando porque es servido por un servicio de SecurSpaces.

Importante:

En el momento en que cualquier política de red se adjunta a un espacio de trabajo — incluso una política de **monitorización** — el tráfico saliente del espacio de trabajo se enruta a través del servicio de proxy de SecurSpaces, y el tráfico UDP que no es DNS se descarta. Un espacio de trabajo **sin** política adjunta no se ve afectado. Tenga esto en cuenta si sus cargas de trabajo dependen de UDP, por ejemplo, algunos VPN, QUIC o protocolos personalizados basados en UDP. Esas conexiones dejan de funcionar una vez que se adjunta una política, sea cual sea el comportamiento de la política.

Antes de usar la restricción o la inspección

> **Nota:**
>
> Las políticas de restricción e inspección pueden hacer que algunas aplicaciones dejen de funcionar, porque cambian lo que el espacio de trabajo puede alcanzar. Se recomiendan para administradores experimentados.

> Bajo una política de inspección, es probable que falle una aplicación que lee certificados desde una ubicación personalizada dentro del contenedor. Consulte con su administrador de plataforma antes de aplicar **Inspeccionar tráfico (predeterminado, experto)** a un espacio de trabajo que dependa de una.

Ámbitos

Las políticas de red se definen en tres niveles de ámbito. Una política definida en un ámbito superior puede aplicarse — y opcionalmente aplicarse — a cada ámbito anidado debajo de ella.

ÁMBITO	¿QUIÉN LO GESTIONA?	USO TÍPICO
Plataforma	Administradores de plataforma, oficiales de seguridad	Política de referencia para toda la implementación
Organización	Propietarios de la organización, oficiales de seguridad	Política para todos los proyectos de una organización
Proyecto	Propietarios del proyecto, oficiales de seguridad	Política para todos los espacios de trabajo de un proyecto

No se puede definir una política a nivel de espacio de trabajo. Un espacio de trabajo solo puede tener una política existente *aplicada* a él, seleccionada de las políticas definidas en el ámbito de la plataforma, la organización o el proyecto.

Aplicado y exigido

Dos conceptos rigen cómo una política llega a un espacio de trabajo.

TÉRMINO	SIGNIFICADO
Aplicada	La política se selecciona como la política activa para un ámbito o espacio de trabajo.
Impuesta	La política queda fijada para el ámbito actual y para cada ámbito anidado debajo de él. Los ámbitos inferiores y sus espacios de trabajo la heredan y no pueden reemplazarla.

¿Quién puede gestionar las políticas de red?

La creación, edición, selección y aplicación de políticas de red requiere que el permiso de **Seguridad** esté establecido en **Gestionar**. El permiso de **Seguridad** tiene tres niveles: **Sin acceso**, **Acceso** y **Gestionar**.

Gestionar pertenece a:

- Oficiales de seguridad
- Propietarios de la organización
- Propietarios de proyectos y cualquier rol personalizado al que se le haya concedido el nivel de **Gestionar**

Los desarrolladores y otros miembros del proyecto no pueden crear, cambiar o asignar políticas de red, ni siquiera para sus propios espacios de trabajo. Con el nivel de **Acceso** pueden ver qué políticas se aplican, por ejemplo, a través de **Ver resumen**, pero la selección es de solo lectura para ellos.

Cuando un desarrollador crea un espacio de trabajo personal, sus políticas de red se aplican automáticamente desde la configuración del proyecto y de la plataforma. Las políticas marcadas como obligatorias se aplican de forma obligatoria y se bloquean, y otras políticas configuradas se aplican como las políticas seleccionadas del espacio de trabajo. El desarrollador no las elige.

Las políticas predeterminadas

Cuando se crea un proyecto, Citrix SecurSpaces™ añade tres políticas listas para usar en el ámbito del proyecto.

POLÍTICA	COMPORTAMIENTO	USAR CUANDO
Monitorizar tráfico (predeterminado)	Monitorizar	Desea registrar el tráfico TCP saliente y generar eventos de auditoría sin restringirlo a una lista de permitidos.
Restringir tráfico (predeterminado, experto)	Restringir	Desea bloquear todo el tráfico saliente excepto los recursos adjuntos y una lista de permitidos aprobada.
Inspeccionar tráfico (predeterminado, experto)	Inspeccionar	Desea inspeccionar el contenido TCP e informarlo al registro de auditoría. Este comportamiento solo está disponible como esta política integrada.

Restringir tráfico (predeterminado, experto) se envía con una lista de permitidos inicial que cubre fuentes comunes de paquetes de desarrollador, para que las herramientas estándar sigan funcionando:

- `*.ubuntu.com`
- `*.nodesource.com`, `*.yarnpkg.com`
- `*.npmjs.org`, `*.npm.im`, `*.npm.me`, `*.npm.red`
- `python.org`, `*.pypi.org`, `*.pythonhosted.org`
- `open-vsx.org`
- `opensuse.org`, `sourceforge.net`, `virtualbox.org`
- `*.windows.net`

Utilice estos valores predeterminados tal cual, duplíquelos como punto de partida o cree sus propias políticas.

Dónde se configuran las políticas

UBICACIÓN	QUÉ SE HACE ALLÍ
Configuración de la plataforma > Configuración de seguridad > Resumen de políticas de red	Revise qué política se aplica en cada ámbito y si se aplica, y descargue un informe. Solo lectura.
Configuración del espacio de trabajo > Política de red, a nivel de plataforma, organización o proyecto	Cree, edite, seleccione, aplique y pruebe la política para ese ámbito.
La **Configuración de seguridad > Seguridad de red** de un espacio de trabajo	Seleccione la política para un espacio de trabajo individual. Solo lectura sin el nivel de **Administración**.

Información relacionada

- Crear una política de red
- Asignar y aplicar una política
- Supervisar y solucionar problemas
- Campos de la política de red
- Panel de auditoría

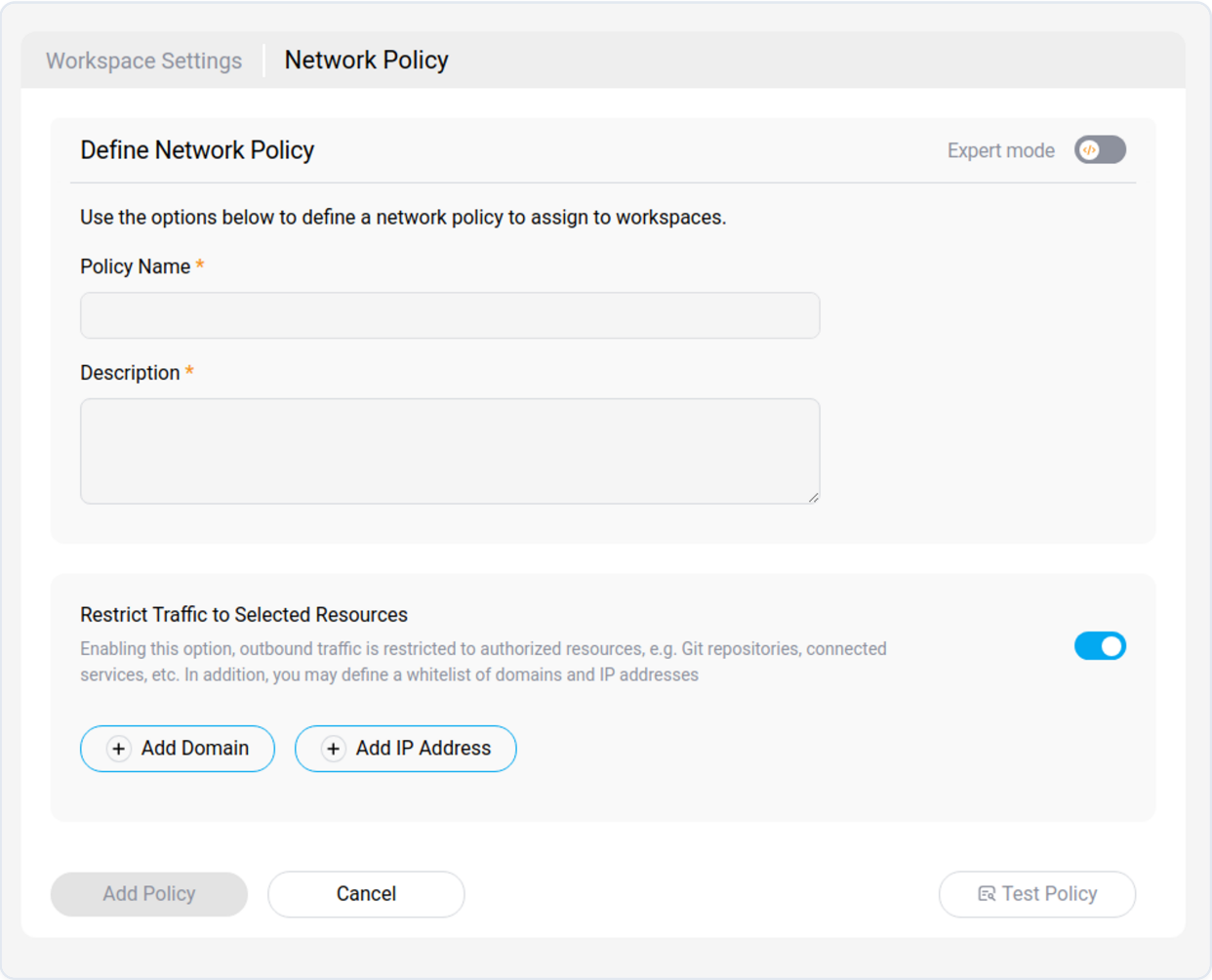
Create a network policy

Puede crear y editar políticas desde una página de **Configuración del espacio de trabajo > Política de red** en el ámbito que gestione: plataforma, organización o proyecto.

Necesita el conjunto de permisos de **Seguridad** establecido en **Gestionar**. Consulte Quién puede gestionar las políticas de red.

Crear la política

1. Vaya a **Configuración del espacio de trabajo > Política de red** para su ámbito.
2. Seleccione **Crear política**.



3. Introduzca un **Nombre de política** y una **Descripción**. Ambos son obligatorios. Utilice una descripción que explique lo que la política permite o bloquea, para que otros administradores entiendan su propósito.
4. Elija cómo configurar el resto de la política:
   - Deje el conmutador de **Modo experto** desactivado para usar el formulario guiado. Consulte Modo básico.
   - Active el conmutador de **Modo experto** para editar la política como YAML. Consulte Modo experto.
5. (Opcional) Seleccione **Probar política** para validar la política antes de guardarla. Consulte Probar una política.
6. Guarde la política.

El formulario básico y el editor YAML experto describen la misma política. Puede alternar entre ellos con el conmutador de **Modo experto** mientras trabaja.

Modo básico

El modo básico le ofrece un formulario guiado para la configuración más común.

1. Establezca **Restringir el tráfico a los recursos seleccionados**:
   - **Desactivado** — La política supervisa el tráfico. Todo está permitido y registrado.
   - **Activado** — La política bloquea todo el tráfico saliente excepto los recursos adjuntos y los recursos de su lista de permitidos.
2. Si activó la restricción, cree la lista de permitidos:
   - Seleccione **Añadir dominio** para permitir un dominio. Opcionalmente, active **Incluir subdominios** para permitir también todos los subdominios de ese dominio.
   - Seleccione **Añadir dirección IP** para permitir una única dirección IPv4 o un rango CIDR, por ejemplo `10.0.0.0/24`.
3. Si su plataforma utiliza un proxy externo, aparece una sección de **puntos finales personalizados a través de proxy**. Úsela para listar los dominios y direcciones IP a los que el espacio de trabajo puede acceder a través del proxy. Esta sección está oculta cuando no hay ningún proxy externo configurado.
4. Guarde la política.

Modo experto

El modo experto reemplaza el formulario con un editor YAML, dándole control sobre cada campo. Active el interruptor de **Modo experto** para usarlo.

Para cada campo, su tipo y sus reglas de validación, consulte Campos de política de red.

```
name: Backend services policy

description: Restrict workspaces to internal package mirrors and the
corporate API.

restrictedTraffic: true

whitelistedDomains:

  - domain: pypi.internal.example.com

    includeSubdomains: false
```

```
  - domain: example.com
    includeSubdomains: true
whitelistedIps:
  - 10.0.0.0/24
  - 192.168.1.50
```

Crear la lista de permitidos

Cuando una política restringe el tráfico, el espacio de trabajo solo puede acceder a:

- **Recursos adjuntos** — Cualquier recurso adjunto al espacio de trabajo, como repositorios, servicios SSH y servicios HTTP, siempre es accesible. Los recursos adjuntos siguen funcionando sin configuración adicional.
- **Dominios permitidos** — Cada dominio en la lista de permitidos.
- **Direcciones IP permitidas** — Cada dirección IPv4 o rango CIDR en la lista de permitidos.

Cómo se comparan los dominios

- Una entrada de dominio con **Incluir subdominios** desactivado solo coincide con ese dominio exacto.
- Una entrada de dominio con **Incluir subdominios** activado coincide con el propio dominio y cualquier subdominio. Por ejemplo, `example.com` con subdominios habilitados permite `example.com` y `*.example.com`, como `api.example.com`.

Cómo se comparan las direcciones IP

Introduzca una única dirección IPv4, por ejemplo `192.168.1.50`, o un rango CIDR, por ejemplo `10.0.0.0/24`. El editor de políticas valida el formato antes de que pueda guardar. Las direcciones IPv6 no son aceptadas.

Información relacionada

- Políticas de red
- Asignar y aplicar una política
- Campos de política de red

Assign and enforce a network policy

Crear una política no cambia ningún espacio de trabajo por sí solo. Se la asigna a un ámbito y, opcionalmente, la aplica en la jerarquía.

Necesita que el permiso de **Seguridad** esté establecido en **Administrar**. Consulte Quién puede administrar políticas de red.

Asignar una política a un ámbito

1. Vaya a **Configuración del espacio de trabajo > Política de red** para el ámbito que administra.
2. Seleccione la política que desea aplicar de la lista de políticas disponibles.
3. Para bloquear la política para este ámbito y todo lo anidado debajo, active **Aplicar política de red**. Cuando la aplicación está activada:
   - La política se aplica a todos los espacios de trabajo actuales y futuros en el ámbito.
   - Los ámbitos anidados y sus espacios de trabajo heredan la política y no pueden reemplazarla.
4. Guarde los cambios.

Si no aplica la política, los ámbitos inferiores y los espacios de trabajo individuales aún pueden elegir una política diferente. La aplicación es lo que garantiza un comportamiento coherente en toda una organización o proyecto.

Seleccionar una política para un espacio de trabajo

Un propietario de proyecto o un oficial de seguridad puede establecer la política de red para un espacio de trabajo individual al crear o editar el espacio de trabajo. Si un ámbito principal aplica una política, esa política se hereda y la selección se bloquea.

1. En el flujo de creación o edición del espacio de trabajo, abra **Configuración de seguridad**.
2. En **Seguridad de red**, elija una política. Por defecto, un espacio de trabajo comienza con **Ninguna política seleccionada**.
3. Seleccione **Ver resumen** para revisar exactamente lo que la política permite o bloquea antes de aplicarla.
4. Guarde el espacio de trabajo.

> **Nota:**

> Esto requiere que el permiso de **Seguridad** esté configurado en **Administrar**. Los desarrolladores no pueden cambiar la política de un espacio de trabajo. Cuando un desarrollador crea un espacio de trabajo personal, sus políticas se aplican automáticamente desde la configuración del proyecto y de la plataforma: las políticas requeridas se aplican y otras políticas configuradas se aplican.

Probar una política

Antes de confiar en una política, pruébela para confirmar que permite lo que espera y bloquea lo que no.

1. Abra la política en **Configuración del espacio de trabajo > Política de red**.
2. Seleccione **Probar política**.
3. En el cuadro de diálogo de prueba, proporcione los destinos que desea verificar.
4. Revise el resultado para confirmar si cada destino está permitido o bloqueado según la política.

Las pruebas son especialmente útiles para las políticas de restricción e inspección, donde una lista de permitidos incompleta puede romper las herramientas dentro del espacio de trabajo.

Revisar la descripción general de la política de red

Para auditar su configuración en toda la implementación, vaya a **Configuración de la plataforma > Configuración de seguridad > Descripción general de la política de red**.

La descripción general muestra, para la plataforma y cada organización:

- La **política aplicada** en ese ámbito.
- El **estado**, ya sea **Aplicada** o **No aplicada**.

Seleccione **Descargar informe** para exportar el resumen para su archivo o revisión.

Información relacionada

- Políticas de red
- Crear una política de red
- Supervisar y solucionar problemas

Monitor and troubleshoot network policies

Cada comportamiento de la política de red alimenta el panel de control de **Auditoría**, que es su herramienta principal para comprender y solucionar los efectos de la política.

- **Tráfico supervisado** genera eventos de registro para todas las conexiones salientes.
- **Tráfico restringido** registra cada solicitud bloqueada, para que pueda ver exactamente qué destino fue denegado.
- **Tráfico inspeccionado** informa sobre el contenido TCP inspeccionado y el tráfico UDP descartado.

Buscar los registros de tráfico

Los eventos de red aparecen en el panel de control de **Auditoría** del proyecto, en el **Registro de eventos del sistema en vivo**.

1. Abra **Auditoría** para el proyecto. Necesita que el permiso de **Seguridad** esté configurado en **Acceso** o **Administrar**.
2. Busque los eventos de red, por ejemplo, solicitudes DNS que muestran el dominio al que un espacio de trabajo intentó acceder.
3. Seleccione **Filtrar** para acotar el registro por tipo de evento, gravedad, espacio de trabajo, usuario o fecha, o utilice la barra de búsqueda para encontrar un destino específico.
4. Expanda una fila para ver los detalles completos del evento, incluida la descripción de lo que lo desencadenó.

Utilice una política de supervisión para crear una lista de permitidos

Una política de solo supervisión es la forma recomendada de descubrir lo que necesita un espacio de trabajo antes de restringirlo.

1. Aplique la política de **Supervisar tráfico (predeterminada)**, o cualquier política con la restricción desactivada, al espacio de trabajo.
2. Utilice el espacio de trabajo con normalidad para que sus herramientas generen sus llamadas de red habituales.
3. En el registro de auditoría, revise los eventos de red para ver qué dominios y direcciones IP el espacio de trabajo realmente alcanzó.
4. Cree una política de restricción y añada esos destinos a la lista de permitidos. Consulte Crear la lista de permitidos.

5. Cambie el espacio de trabajo a la política de restricción. Cualquier destino que haya omitido ahora aparece como una solicitud bloqueada en el mismo registro de auditoría, para que pueda refinar la lista de permitidos y repetir el proceso.

> **Consejo:**
>
> Los recursos adjuntos, como repositorios, servicios SSH y servicios HTTP, siempre son accesibles bajo una política de restricción. No es necesario añadirlos a la lista de permitidos.

Problemas comunes

Una aplicación no puede acceder a un servicio que necesita

Es probable que el destino falte en la lista de permitidos. Compruebe el panel de auditoría para ver la solicitud bloqueada, entonces añada el dominio o la dirección IP a la política. Si el servicio utiliza subdominios, active **Incluir subdominios**.

Una herramienta que utiliza UDP deja de funcionar después de aplicar una política

Cualquier política de red adjunta —de supervisión, restricción o inspección— descarta el tráfico UDP que no es DNS por diseño. DNS sigue funcionando, pero otros protocolos basados en UDP no. Si una carga de trabajo depende de UDP, no puede ejecutarse en un espacio de trabajo que tenga una política de red adjunta.

Consulte Qué sucede cuando se adjunta una política.

Un espacio de trabajo ignora la política que ha seleccionado

Es probable que un ámbito principal esté aplicando una política diferente, o que la política se haya aplicado automáticamente desde la configuración del proyecto. Compruebe el resumen de políticas de red para ver qué ámbito aplica la política heredada. Solo los oficiales de seguridad, los propietarios de la organización y los propietarios del proyecto pueden cambiar la política de un espacio de trabajo.

Información relacionada

- Políticas de red
- Asignar y aplicar una política
- Panel de auditoría

Technical security overview for SecurSpaces Flex

Este artículo describe la arquitectura de seguridad, el modelo de responsabilidad compartida, las prácticas de manejo de datos y la postura de cumplimiento de Citrix SecurSpaces™ Flex. Está dirigido a equipos de seguridad, revisores de adquisiciones y CISO que evalúan el servicio.

Descripción general de la arquitectura

Citrix SecurSpaces Flex se basa en tres capas:

CAPA	DESCRIPCIÓN	OPERADO POR
Plano de control	Gestiona el aprovisionamiento, el acceso, las políticas y el ciclo de vida del espacio de trabajo. Construido sobre Azure Kubernetes Service (AKS) y Azure Cosmos DB.	Citrix
Plano de ejecución	Ejecuta espacios de trabajo Linux aislados y en entornos de pruebas. Cada espacio de trabajo es un entorno en contenedores con vCPU, RAM y almacenamiento persistente definidos.	Citrix
Capa de integración	Conecta los espacios de trabajo a los sistemas propiedad del cliente: proveedores de identidad, repositorios Git, canalizaciones CI/CD, gestores de secretos y fuentes de datos.	Cliente + Citrix (infraestructura de conectividad)

Todos los componentes se ejecutan dentro de las suscripciones de Azure gestionadas por Citrix en las regiones de Azure acordadas para su implementación. Los datos de la aplicación del cliente, las imágenes de contenedor, los secretos y la configuración de identidad permanecen bajo la propiedad y el control del cliente.

Modelo de responsabilidad compartida

Citrix SecurSpaces Flex utiliza una clara división de responsabilidades entre Citrix y el cliente en cuanto a configuración y gestión, infraestructura y soporte continuo.

Configuración y gestión

CLIENTE	CITRIX
Alojamiento y gestión de imágenes de espacio de trabajo	Configuración y actualizaciones de la plataforma Citrix SecurSpaces
Gestión de espacios de trabajo y plantillas	Gestión de regiones de Citrix SecurSpaces (previa solicitud)
Cuentas de usuario, acceso y permisos	Configuraciones de Citrix SecurSpaces para toda la plataforma
Organizaciones, proyectos y secretos	Especificaciones del espacio de trabajo
Políticas de red y supervisión de seguridad	Copias de seguridad, planificación de DR y supervisión de disponibilidad

Infraestructura

CLIENTE	CITRIX
Autenticación (IdP)	Azure AKS, Cosmos DB e inquilino de Azure
Repositorios de código fuente	VM de zona de aterrizaje
Artifactorios	Escalado del plano de control de Citrix SecurSpaces (ascendente/descendente)
Emparejamiento de vNET de Azure / puerta de enlace VPN (compartido)	Emparejamiento de vNET de Azure / puerta de enlace VPN (compartido)

Soporte continuo

CLIENTE	CITRIX
Soporte al usuario final	Soporte de infraestructura de Citrix SecurSpaces y Azure

CLIENTE	CITRIX
	Soporte de producto de Citrix SecurSpaces

Los compromisos de disponibilidad del servicio, y la solución si Citrix no los cumple, se establecen en el SLA de Platform Flex.

> **Nota:** El emparejamiento de vNET de Azure y la puerta de enlace VPN son una responsabilidad compartida. Citrix aprovisiona y opera el lado de la conexión gestionado por Citrix; el cliente configura y mantiene su lado. Consulte Conexiones de red para obtener más detalles.

Aislamiento del espacio de trabajo

Cada espacio de trabajo es un contenedor Linux aislado y en un entorno limitado. El aislamiento se aplica a nivel de tiempo de ejecución de Kubernetes.

- **No hay sistemas de archivos compartidos entre espacios de trabajo.** Cada espacio de trabajo tiene su propia Persistent Volume Claim (PVC) para el estado persistente.
- **Sin movimiento lateral.** Un espacio de trabajo comprometido no puede acceder a otros espacios de trabajo ni al plano de control.
- **Entrada y salida controladas.** El tráfico de red del espacio de trabajo está sujeto a reglas definidas por políticas. La salida a Internet y a las redes de clientes está controlada; el acceso saliente sin restricciones no es el predeterminado.
- **Contención de agentes de IA.** Los agentes de codificación de IA se ejecutan dentro del mismo entorno limitado del espacio de trabajo que las sesiones humanas. Los procesos de los agentes están sujetos a los mismos controles de salida, reglas de DLP y registro de auditoría que cualquier otra actividad del espacio de trabajo.

Prevención de pérdida de datos (DLP)

Citrix SecurSpaces Flex incluye controles DLP integrados.

- **DLP del portapapeles** — Las operaciones del portapapeles entre el espacio de trabajo y el dispositivo local del usuario están controladas por políticas. Los administradores pueden restringir o supervisar el comportamiento de copiar/pegar.
- **Supervisión de sesiones** — La actividad del espacio de trabajo puede estar sujeta a grabación de sesiones y supervisión del comportamiento con fines de cumplimiento y forenses.

- **Registro de auditoría** — Todas las acciones administrativas y de desarrollador generan entradas de registro de auditoría. Los registros se conservan y son exportables para la integración con SIEM.

Residencia de datos y cifrado

Residencia de datos

La ejecución del espacio de trabajo se realiza en la región de Azure designada como su región principal y en cualquier región secundaria aprovisionada para su implementación. Citrix no transfiere datos del espacio de trabajo entre regiones fuera de las regiones acordadas para su implementación.

Los activos propiedad del cliente —imágenes de contenedor, secretos, código fuente, configuraciones de identidad— permanecen en la infraestructura propiedad del cliente y no se replican en sistemas gestionados por Citrix, excepto cuando sea necesario para la ejecución del espacio de trabajo (por ejemplo, al extraer una imagen de contenedor en el inicio del espacio de trabajo).

Cifrado

- **En tránsito** — Toda la comunicación entre los clientes del espacio de trabajo y la plataforma utiliza TLS 1.2 o superior. La comunicación entre los componentes internos de la plataforma está cifrada.
- **En reposo** — El almacenamiento persistente del espacio de trabajo (PVC) se cifra en reposo utilizando claves de cifrado gestionadas por Azure. Los datos de configuración del plano de control almacenados en Cosmos DB se cifran en reposo.

Control de acceso basado en roles (RBAC)

Citrix SecurSpaces Flex aplica el control de acceso basado en roles a nivel de plataforma.

- **Administradores** gestionan las implementaciones, las plantillas de espacio de trabajo, el acceso de usuarios y la configuración de políticas.
- **Desarrolladores** acceden a los espacios de trabajo que se les asignan. No pueden acceder a los espacios de trabajo de otros desarrolladores ni a las funciones administrativas.
- Los roles y permisos se gestionan en la consola de Citrix SecurSpaces y se integran con el IdP del cliente.

Más información

- Descripción general de SecurSpaces Flex — el punto de partida para toda la documentación de Flex
- Conexiones de red(/es-es/securspaces/security/flex/network-connections.html)
- Plantillas de espacio de trabajo(/es-es/securspaces/manage/flex-workspace-templates.html)
- SLA de Platform Flex(/es-es/citrix-daas-flex/service-level-agreement.html)
- Centro de confianza de Citrix(https://www.citrix.com/about/trust-center/)

Network connections for SecurSpaces Flex

Este artículo describe cómo los espacios de trabajo Citrix SecurSpaces™ Flex se conectan a los sistemas propiedad del cliente, las opciones de conectividad disponibles y lo que cada opción permite.

Información general

Los espacios de trabajo de Citrix SecurSpaces Flex se ejecutan en un inquilino de Azure administrado por Citrix. Para habilitar los flujos de trabajo de los desarrolladores, los espacios de trabajo suelen necesitar acceso a sistemas propiedad del cliente, como proveedores de identidades, repositorios de Git, canalizaciones de CI/CD, almacenes de artefactos y administradores de secretos.

La conectividad entre el plano de ejecución administrado por Citrix y los sistemas propiedad del cliente se establece a través de una capa de integración. Esta capa utiliza primitivas de red estándar de Azure. El cliente es responsable de configurar su lado de la conexión.

Opciones de conectividad

Citrix SecurSpaces Flex admite dos opciones de conectividad para conectar los espacios de trabajo a la infraestructura propiedad del cliente.

Emparejamiento de red virtual (vNET) de Azure

El emparejamiento de vNET de Azure crea una ruta de red privada y de baja latencia entre la red virtual de Azure administrada por Citrix y una red virtual en la suscripción de Azure del cliente.

Utilice esta opción cuando:

- Sus sistemas propiedad del cliente (IdP, Git, CI/CD, administrador de secretos) están alojados en Azure.

- Desea una conectividad privada y de alto rendimiento sin enrutamiento de tráfico a través de Internet público.

Lo que el cliente configura:

- Una red virtual en la suscripción de Azure del cliente.
- Una solicitud de emparejamiento desde la vNET del cliente a la vNET administrada por Citrix (Citrix proporciona el identificador de recurso durante la configuración).
- Reglas del grupo de seguridad de red (NSG) y enrutamiento para permitir que el tráfico del espacio de trabajo llegue a los sistemas de destino.

Puerta de enlace VPN

Una puerta de enlace VPN conecta la vNET de Azure administrada por Citrix con la red del cliente mediante un túnel VPN IPsec/IKE.

Utilice esta opción cuando:

- Sus sistemas propiedad del cliente estén en las instalaciones o en un entorno que no sea de Azure.
- El emparejamiento de vNET de Azure no esté disponible o no sea adecuado para su arquitectura de red.

Qué configura el cliente:

- Un dispositivo o puerta de enlace VPN en el límite de la red del cliente.
- Una configuración de túnel IPsec/IKE (Citrix proporciona el punto final de la puerta de enlace remota durante la configuración).
- Reglas de enrutamiento para dirigir el tráfico del espacio de trabajo a los sistemas locales adecuados.

Qué pueden alcanzar los espacios de trabajo

Una vez establecida la conectividad, los espacios de trabajo pueden acceder a cualquier sistema accesible dentro de la red conectada, sujeto a las reglas de enrutamiento y de grupo de seguridad que configure. Los objetivos de integración comunes incluyen:

TIPO DE SISTEMA	EJEMPLOS
Proveedores de identidades	Azure Active Directory, Okta, cualquier proveedor de SAML 2.0 u OpenID Connect

TIPO DE SISTEMA	EJEMPLOS
Repositorios de código fuente	GitHub Enterprise, GitLab autogestionado, Bitbucket Server, Azure Repos
Repositorios de artefactos	Artifactory, Nexus, Azure Artifacts
Sistemas de CI/CD	Jenkins, Azure DevOps, CircleCI
Administradores de secretos	HashiCorp Vault, Azure Key Vault
Fuentes de datos internas	Bases de datos, lagos de datos, API internas

Sin conectividad (estado predeterminado)

Por defecto, antes de configurar cualquier opción de conectividad, los espacios de trabajo tienen acceso a:

- Internet público (sujeto a las reglas de política de salida que defina en la consola de Citrix SecurSpaces).
- Servicios de plataforma gestionados por Citrix (necesarios para el funcionamiento del espacio de trabajo).

Los espacios de trabajo **no** tienen acceso predeterminado a las redes privadas propiedad del cliente. La conectividad debe configurarse explícitamente utilizando una de las opciones anteriores.

Resumen de responsabilidades

TAREA	PARTE RESPONSABLE
Proporcionar el identificador de recurso de vNET gestionado por Citrix o el punto final de VPN	Citrix
Configurar el emparejamiento o el túnel VPN del lado del cliente	Cliente
Configurar las reglas de NSG y el enrutamiento en la red del cliente	Cliente
Gestionar el acceso a los sistemas propiedad del cliente una vez conectados	Cliente

TAREA	PARTE RESPONSABLE
Aplicar la política de egreso dentro de los espacios de trabajo	Citrix (plataforma) + Cliente (configuración de políticas)

Más información

- Descripción general de SecurSpaces Flex — el punto de partida para toda la documentación de Flex
- Descripción general de seguridad técnica
- Plantillas de espacio de trabajo
- Documentación de emparejamiento de vNET de Azure — Microsoft Azure
- Documentación de Azure VPN Gateway — Microsoft Azure

Reference

Material de consulta: nombres exactos, valores y límites. Estas páginas indican qué es, sin explicar cómo usarlo — las secciones de tareas lo hacen y enlazan aquí.

Ordenado alfabéticamente, porque la referencia se busca en lugar de leerse.

PÁGINA	QUÉ CUBRE
Catálogo de eventos de auditoría	Cada evento de auditoría, por categoría, con sus atributos
Requisitos de imagen de contenedor	Lo que debe proporcionar una imagen de espacio de trabajo
Criptografía	Algoritmos en uso y dónde se aplica cada uno
Límites y comportamiento de los puntos de montaje	Cuotas, semántica de eliminación, métricas
Destinos de red	Direcciones externas necesarias para instalar y licenciar
Campos de política de red	Campos YAML en modo experto y su validación
Puertos y protocolos	Puertos expuestos y el modelo de reenvío SSH
API REST	La superficie de la API pública
CLI de SDS	Cada comando y opción del instalador
IDEs compatibles	Qué editores funcionan y cómo se conecta cada uno
Requisitos del sistema	Kubernetes, redes, almacenamiento, herramientas

Audit event catalog

Las tablas a continuación ofrecen una referencia rápida a los eventos monitorizados en tiempo real en la plataforma Citrix SecurSpaces™. Estos eventos se capturan sistemáticamente utilizando métodos estandarizados y están disponibles en la sección de auditoría. Se pueden exportar fácilmente en formatos comunes para su integración con sistemas de Gestión de Información y Eventos de Seguridad (SIEM), lo que permite una monitorización y análisis exhaustivos.

Todos los eventos

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
	Todos	Atributos compartidos por todos los eventos		id, marca de tiempo, id de usuario, nombre de usuario, id de sesión, id de proyecto, nombre de proyecto, id de espacio de trabajo, nombre de espacio de trabajo, gravedad

Autenticación

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
1	Autenticación	Inicio de sesión	El usuario inició sesión en la plataforma	
2	Autenticación	Cierre de sesión	El usuario cerró sesión en la plataforma	

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
3	Autenticación	Inicio de sesión	El usuario inició una sesión de espacio de trabajo	
4	Autenticación	Fin de sesión	El usuario finalizó una sesión de espacio de trabajo	
5	Autenticación	Interrupción de sesión	La sesión del espacio de trabajo del usuario ha sido interrumpida	

Autorización

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
6	Autorización de usuario	Usuario bloqueado	El usuario ha sido bloqueado	user_id, user_name, role_name
7	Autorización de usuario	UserUnblocked	El usuario ha sido desbloqueado	user_id, user_name, role_name
9	Autorización de espacio de trabajo	SharedWithUser	El usuario comparte el espacio de trabajo con otro usuario	user_id, user_name
10	Autorización de espacio de trabajo	UnsharedWithUser	El usuario revoca el acceso a un espacio de	user_id, user_name

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
			trabajo compartido previamente.	

Seguridad de los datos

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
11	Seguridad de los datos	Copiar	En el espacio de trabajo, el usuario copia datos al portapapeles.	datos, es_secreto, es_código
12	Seguridad de los datos	Pegar	En el espacio de trabajo, el usuario pega los datos copiados en una nueva ubicación	datos, es_secreto, es_código
13	Seguridad de los datos	Cortar	En el espacio de trabajo, el usuario corta los datos seleccionados para una posible reubicación	datos, es_secreto, es_código
14	Seguridad de los datos	Portapapeles	En el navegador seguro, los datos se copian, cortan o pegan	datos, es_secreto, es_código

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
15	Seguridad de los datos	ShareClipboardUrl	En el navegador seguro, el usuario comparte una URL o un enlace almacenado en el portapapeles	datos, es_secreto, es_código
16	Seguridad de los datos	Subir	Envía un archivo o datos desde un dispositivo local a un entorno remoto	datos, es_secreto, es_código
17	Seguridad de los datos	UploadLargeFile	Envía archivos de gran tamaño desde un dispositivo local a un entorno remoto	datos, es_secreto, es_código
18	Seguridad de los datos	Descargar	Recupera un archivo o datos de un entorno remoto a un dispositivo local	datos, es secreto, es código
19	Seguridad de los datos	DownloadLargeFile	Recupera archivos de gran tamaño de un entorno remoto a un dispositivo local	datos, es secreto, es código
20	Seguridad de los datos	SupervisedCopy	En el espacio de trabajo, la acción de copia	datos, es secreto, es código

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
			bajo supervisión o monitorización	

Sistema

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
21	Sistema	WorkspaceSpecsUpdated	Modificaciones o actualizaciones realizadas en las especificaciones de un espacio de trabajo	
60	Sistema	BulkWorkspaceUpdate	Una actualización masiva de espacios de trabajo iniciada desde el Centro de Actualizaciones	
61	Sistema	BulkWorkspacePause	Una pausa masiva de espacios de trabajo iniciada desde el Centro de Actualizaciones	

Eventos de nivel gestionado de SecurSpaces Flex

En Citrix SecurSpaces Flex, los niveles de tamaño de espacio de trabajo gestionados también generan eventos de ResourceAccess. SecurSpaces registra los cambios exitosos en la disponibilidad de los niveles y las actualizaciones masivas de la versión de los niveles, y registra

los intentos rechazados de modificar las definiciones de los niveles gestionados por Citrix. El evento incluye el usuario que actúa, la marca de tiempo, la versión del nivel gestionado, y el resultado.

Seguridad de los datos

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
22	SecureBrowser Navigation	SecureBrowser Navigation	Garantiza prácticas de navegación seguras durante la navegación	URL, título permitido
23	VSCodeExtensionInstalled	VSCodeExtensionInstalled	Instalación de una extensión dentro de Visual Studio Code	extension_name, extension_id extension_uuid
24	AccountManagement	UserAddedToProject	Adición de un usuario a un proyecto específico	user_id, user_name, role_name
25	AccountManagement	UserRemovedFromProject	Eliminación de un usuario de un proyecto específico	
26	AccountManagement	RolCambiado	Modificación o alteración de los roles y permisos de un usuario	
27	Gestión de Cuentas	UsuarioCreado	Creación de un nuevo perfil o cuenta de usuario	

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
28	Gestión de Cuentas	UsuarioEliminado	Eliminación o supresión de un perfil o cuenta de usuario	

Tráfico de Red

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
29	SSHCommand	SSHCommand	Ejecución de un comando a través de Secure Shell (SSH)	emisor, comando, tipo, destino, confirmación, solicitud, rama_git
30	ExternalSSHCommand	ExternalSSHCommand	Ejecución de un comando externo a través de Secure Shell (SSH)	id_servicio, comando, destino, tipo
31	HTTPRequest	HTTPRequest	Transmisión de una solicitud mediante el Protocolo de transferencia de hipertexto (HTTP)	emisor, destino, tipo_de_solicitud, bloqueado, código_de_estado, id_de_navegador
32	GitOverHTTP	GitOverHTTP	Operaciones de Git realizadas a través del protocolo HTTP	emisor, comando, destino, solicitud
33	TCPForwarding	TCPForwarding	Reenvío de tráfico del Protocolo de	dirección_de_destino

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
			Control de Transmisión (TCP)	
34	DNS	DNS	Operaciones o solicitudes del Sistema de Nombres de Dominio (DNS)	dominio, dirección, inspeccionado
59	AIRequest	AIRequest	Una solicitud de un espacio de trabajo a un servicio de IA, registrada por la puerta de enlace de IA	host, url, método, código_estado, bloqueado, modelo
35	ResourceAccess	Creado	Se ha creado un nuevo recurso dentro del sistema	nombre_recurso, id_recurso, tipo_acción, tipo_recurso, aplicación_o_auth
36	ResourceAccess	Importado	Se importan datos o información de una fuente externa	resource_name, resource_id, action_type, resource_type, o_auth_app
37	ResourceAccess	ManuallyImported	Datos específicos se transfieren o importan manualmente al sistema	resource_name, resource_id, action_type, resource_type, o_auth_app
38	ResourceAccess	Updated	Los datos o la información existentes	resource_name, resource_id, action_type,

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
			sufren modificaciones o actualizaciones dentro del sistema	resource_type, o_auth_app
39	ResourceAccess	SharedWithUsers	El recurso se comparte con varios usuarios dentro del sistema	resource_name, resource_id, action_type, resource_type, o_auth_app
40	ResourceAccess	SharedPublicly	El recurso se hace accesible a los usuarios públicos	resource_name, resource_id, action_type, resource_type, o_auth_app
41	ResourceAccess	WorkspaceAttached	El recurso está adjunto a un espacio de trabajo	resource_name, resource_id, action_type, resource_type, o_auth_app
42	ResourceAccess	WorkspaceDetached	Eliminación del recurso de un espacio de trabajo	resource_name, resource_id, action_type, resource_type, o_auth_app
43	ResourceAccess	Eliminado	Un recurso se elimina o borra del sistema	resource_name, resource_id, action_type, resource_type, o_auth_app
44	ResourceAccess	Repositorio	Gestión de una aplicación Git utilizada para el almacenamient	resource_name, resource_id, action_type,

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
			o de código o datos	resource_type, o_auth_app
45	ResourceAccess	Bucket	Contenedor utilizado para el almacenamiento de datos, comúnmente usado en la computación en la nube	resource_name, resource_id, action_type, resource_type, o_auth_app
46	ResourceAccess	Secret	Datos sensibles como contraseñas, claves o tokens	resource_name, resource_id, action_type, resource_type, o_auth_app
47	ResourceAccess	Connected_service	Establecimiento o utilización de un servicio externo o integración dentro del sistema	resource_name, resource_id, action_type, resource_type, o_auth_app
48	ResourceAccess	Network_policy	Establecimiento de reglas o configuraciones que rigen el comportamiento o el acceso a la red	resource_name, resource_id, action_type, resource_type, o_auth_app
49	ResourceAccess	Imagen	Gestión de representaciones o instantáneas de datos, a menudo utilizado en	resource_name, resource_id, action_type, resource_type, o_auth_app

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
			entornos informáticos	
50	ResourceAccess	Credencial	Gestión de información utilizada para autenticación o control de acceso	resource_name, resource_id, action_type, resource_type, o_auth_app
51	ResourceAccess	Workspace_app	Utilización o gestión de una aplicación de espacio de trabajo	resource_name, resource_id, action_type, resource_type, o_auth_app
52	ResourceAccess	Startup_script	Ejecución o gestión de scripts o instrucciones durante el inicio del sistema	resource_name, resource_id, action_type, resource_type, o_auth_app
53	ResourceAccess	Workspace	Gestión o utilización de un entorno de codificación para trabajo colaborativo	resource_name, resource_id, action_type, resource_type, o_auth_app
54	ResourceAccess	GitHub	Utilización o interacción con la aplicación OAuth de GitHub para diversos fines	resource_name, resource_id, action_type, resource_type, o_auth_app
55	ResourceAccess	GitLab	Utilización o interacción con la aplicación OAuth de	resource_name, resource_id, action_type,

ID	CATEGORÍA	TIPO DE EVENTO	DESCRIPCIÓN DEL EVENTO	ATRIBUTOS
			GitLab para diversos fines	resource_type, o_auth_app
56	ResourceAccess	Bitbucket	Utilización o interacción con la aplicación OAuth de Bitbucket para diversos fines	resource_name, resource_id, action_type, resource_type, o_auth_app
57	ResourceAccess	AzureDevOps	Utilización o interacción con la aplicación OAuth de AzureDevOps para diversos fines	resource_name, resource_id, action_type, resource_type, o_auth_app
58	ResourceAccess	JFrog	Utilización o interacción con la aplicación OAuth de JFrog para varios propósitos	resource_name, resource_id, action_type, resource_type, o_auth_app

Atributos

ATRIBUTOS	DESCRIPCIÓN DEL ATRIBUTO
action_type	Tipo de acción
dirección	Dirección DNS
permitido	Indicador que indica si se permite la navegación
bloqueado	Indicador que señala si la solicitud está bloqueada
browser_id	ID del navegador

ATRIBUTOS	DESCRIPCIÓN DEL ATRIBUTO
comando	El comando SSH ejecutado
confirmación	El hash de commit relacionado
datos	Datos del portapapeles, si se aplican
destino	El nombre del servicio git
destino	El nombre del servicio externo
destino	El nombre de destino
destination_address	Dirección de destino
dominio	Nombre de dominio
extension_id	ID de la extensión de Visual Studio Code
extension_name	Nombre de la extensión de Visual Studio Code
extension_uuid	UUID de la extensión de Visual Studio Code
git_branch	El nombre de la rama git, si se aplica
anfitrión	El host del servicio de IA contactado
id	ID de evento
inspeccionado	Indicador que señala si la solicitud ha sido inspeccionada
is_code	Indicador de detección de código
is_secret	Indicador de detección de secreto
emisor	Correo electrónico o ID de usuario del emisor
método	El método HTTP utilizado
modelo	El modelo de IA nombrado en la solicitud, si está presente

ATRIBUTOS	DESCRIPCIÓN DEL ATRIBUTO
o_auth_app	Nombre de la aplicación de terceros, si se aplica
project_id	ID del proyecto
project_name	Nombre del proyecto
solicitud	El tipo de solicitud
request_type	Tipo de solicitud
resource_id	ID del recurso
resource_name	Nombre del recurso
resource_type	Tipo de recurso
role_name	El rol de usuario en la plataforma
role_name	El nombre del rol en el proyecto, si aplica
service_id	El ID del servicio
session_id	ID de sesión del IDE
gravedad	Gravedad 0-3 = Baja - 4-6 = Media - 7-8 = Alta - 9-10 = Crítica
status_code	Código de estado HTTP
marca de tiempo	Fecha en la que se registró el evento
título	Título de la página web
tipo	Push o pull
URL	URL de la página web
user_id	El ID de usuario en la plataforma
user_name	El nombre de usuario en la plataforma

ATRIBUTOS	DESCRIPCIÓN DEL ATRIBUTO
workspace_id	ID del espacio de trabajo
workspace_name	Nombre del espacio de trabajo

Container image requirements

Cada imagen de contenedor utilizada para un espacio de trabajo de Citrix SecurSpaces™ debe cumplir los requisitos de esta página. Una imagen que no los cumpla puede que no se inicie, o que se inicie sin que el IDE en la nube funcione.

Como mínimo, una imagen debe proporcionar:

1. Un cliente SSH.
2. Git y Git LFS.
3. Un usuario llamado `developer` con UID 1000.

El resto de esta página establece los requisitos completos. Para añadir una imagen a un proyecto una vez que los cumpla, consulte Imágenes de contenedor. Para construir una, consulte Imágenes de espacio de trabajo.

Paquetes principales

Requerido en todas las distribuciones, para la compatibilidad con la plataforma y con el servidor IDE que se ejecuta dentro del espacio de trabajo.

PAQUETE	PROPÓSITO
`glibc >= 2.28`	Biblioteca estándar de C requerida por el servidor IDE. En Alpine, use `musl` con `gcompat` en su lugar.
`libstdc++ >= 3.4.25`	Biblioteca estándar de C++
`libgcc`	Tiempo de ejecución de GCC
`bash`	Shell predeterminado requerido por el servidor IDE

PAQUETE	PROPÓSITO
`curl` o `wget`	Descarga el servidor y las dependencias externas
`git`	Integración de control de código fuente e inicialización del espacio de trabajo
`git-lfs`	Manejo de archivos grandes y activos binarios
`openssh-client` / `openssh-clients`	Autenticación Git basada en SSH y acceso remoto

Cuenta de usuario

La imagen debe aprovisionarse con esta cuenta y directorio de inicio. Los valores no son configurables. El contenedor del espacio de trabajo se ejecuta como UID 1000, y el volumen persistente se monta en `/home/developer`, por lo que una imagen que utilice un usuario o directorio de inicio diferente no podrá escribir en él.

PROPIEDAD	VALOR
Nombre de usuario	`developer`
Directorio personal	`/home/developer`
UID	`1000`
GID	`1000`
Shell de inicio de sesión	`/bin/bash`

Termine el Dockerfile con `USER 1000` y `WORKDIR /home/developer` para que el espacio de trabajo se inicie como el usuario correcto en el directorio correcto.

Cómo la plataforma comprueba una imagen

Cuando un administrador añade una imagen, o añade una etiqueta a una imagen existente, SecurSpaces la prueba antes de que cualquiera pueda usarla. Inicia un **espacio de trabajo fantasma** temporal a partir de la imagen y ejecuta una comprobación dentro de él. La imagen se marca como lista solo si la comprobación es exitosa.

La comprobación evalúa cuatro aspectos, todos ejecutando el comando o buscando al usuario dentro del contenedor:

COMPROBADO	MENSAJE DE ERROR
`ssh` está en el `PATH`	`SSH is not present on the image`
`git` está en el `PATH`	`Git is not present on the image`
`git-lfs` está en el `PATH`	`Git-lfs is not present on the image`
Existe un usuario llamado `developer`	`User(ID 1000) could not be accessed: the user developer is not present on the image`

Si alguno falla, la imagen se marca como **La imagen no es compatible con nuestra infraestructura de espacio de trabajo**, seguido de **No se cumplen los siguientes requisitos:** y los fallos específicos. La imagen no se puede usar hasta que se reconstruya y se vuelva a añadir.

> **Importante:**

> La comprobación cubre solo esos cuatro elementos. Todo lo demás en esta página —el UID y GID, el directorio de inicio, el shell de inicio de sesión, el directorio de scripts de inicio, la arquitectura y la versión `glibc` — sigue siendo obligatorio, pero una imagen puede pasar la comprobación y fallar más tarde en tiempo de ejecución. Aprobar es un mínimo, no una certificación.

Leer el resultado

La comprobación de compatibilidad aparece en el registro de la imagen como **Comprobando la compatibilidad de la imagen con nuestra infraestructura de espacio de trabajo**, en la fase de **Configuración del espacio de trabajo**. Ábrela desde la entrada de la imagen en **Recursos > Imágenes de contenedor**.

El registro también muestra el espacio de trabajo fantasma extrayendo tu imagen, por lo que es un lugar útil para confirmar que la imagen fue encontrada y cuál es su tamaño.

Paquetes específicos de la distribución

Ubuntu y Debian

Se recomienda Ubuntu 20.04 o posterior, o Debian 11 o posterior, para la compatibilidad con `glibc`.

PAQUETE	PROPÓSITO
`tar`	Desempaqueta el paquete del servidor
`ca-certificates`	Conexiones HTTPS seguras al descargar extensiones

Red Hat Enterprise Linux

RHEL 8.x y 9.x cumplen los requisitos principales.

PAQUETE	PROPÓSITO
`tar`	Desempaqueta el paquete del servidor

CentOS Stream y distribuciones compatibles con RHEL

CentOS Stream 8 y 9, Rocky Linux 8 y 9, y AlmaLinux 8 y 9 cumplen los requisitos principales.

CentOS 7 no cumple los requisitos, porque se distribuye con `glibc 2.17`.

PAQUETE	PROPÓSITO
`tar`	Desempaqueta el paquete del servidor

Alpine Linux 3.16 o posterior

PAQUETE	PROPÓSITO
`musl >= 1.2.3`	Biblioteca estándar de C nativa para Alpine
`gcompat`	Proporciona la capa de compatibilidad de glibc

> **Nota:**

> Alpine usa `musl` en lugar de `glibc`. Las características principales funcionan a través de capas de compatibilidad, pero las imágenes basadas en Ubuntu y RHEL ofrecen la experiencia más estable con el servidor IDE.

Arquitectura

SecurSpaces se ejecuta en `linux/amd64` (x86_64). Las imágenes de espacio de trabajo deben compilarse para esa arquitectura. Otras arquitecturas, incluida ARM, no son compatibles.

Solución de problemas

`GLIBC_2.xx not found` cuando se inicia el terminal

El IDE en la nube se abre, pero el terminal falla inmediatamente, con un mensaje similar a:

```
The terminal process failed to launch: A native exception occurred during
launch

(/lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34' not found

(required by /strong/strong-ide/node_modules/node-pty/build/Release/
pty.node)).
```

La imagen se basa en una distribución cuyo `glibc` es más antiguo de lo que requiere el servidor IDE. CentOS 7 es la causa habitual, en `glibc 2.17`. Recompile en una base más reciente — Ubuntu 20.04 o posterior, Debian 11 o posterior, o RHEL 8 o posterior — o póngase en contacto con el soporte de Citrix para preguntar si su distribución puede ser compatible.

La imagen está marcada como no compatible

La imagen se añadió pero no es utilizable, y muestra **La imagen no es compatible con nuestra infraestructura de espacio de trabajo**.

Falta uno de los cuatro requisitos comprobados. El mensaje indica cuál. En la práctica, casi siempre se trata de una imagen base que nunca fue diseñada para el desarrollo interactivo — una imagen de aplicación como una base de datos o un panel de control no tiene motivos para incluir `git`, `git-lfs` o un cliente SSH, y a menudo no tiene un usuario `developer`.

Añada los paquetes y el usuario que faltan, recompile y añada la imagen de nuevo. Consulte Cómo la plataforma comprueba una imagen, y Cree su primera imagen base para un punto de partida funcional. punto.

El espacio de trabajo se inicia pero faltan los archivos escritos durante la compilación

Cualquier cosa escrita en `/home/developer` en el Dockerfile se oculta una vez que el volumen persistente se monta sobre ella. Instale en un directorio del sistema en su lugar, o escriba los archivos desde un script de inicio. Consulte Comprensión de la persistencia.

Información relacionada

- Imágenes de espacio de trabajo — creación de una imagen
- Imágenes de contenedor — añadir una a un proyecto
- Qué persiste en un espacio de trabajo de SecurSpaces
- strong-network/images en GitHub y strongnetwork en Docker Hub — imágenes de ejemplo y precompiladas

Cryptography

Los algoritmos criptográficos que utiliza Citrix SecurSpaces™ y dónde se aplica cada uno. Esta página es compatible con la revisión de seguridad de la red y la evaluación de terceros.

Datos en tránsito

TRÁFICO	PROTECCIÓN
Tráfico del navegador y de la API desde fuera del clúster	HTTPS. TLS se termina en el controlador de entrada.
Controlador de entrada a los servicios de SecurSpaces	TLS
Servicio de SecurSpaces a servicio de SecurSpaces	TLS
Sesiones de desarrollo remoto	SSH

> **Nota:**

> Dado que TLS se termina en el controlador de entrada, las versiones de TLS y los conjuntos de cifrado permitidos para el tráfico externo se determinan mediante la configuración de entrada, no por SecurSpaces. Configúrelos para que cumplan con su propia política.

Datos en reposo

SecurSpaces está alojado por el cliente, por lo que el cifrado en reposo para la base de datos, los volúmenes persistentes y `etcd` es su responsabilidad. SecurSpaces añade cifrado de capa de aplicación además de esto.

DATOS	PROTECCIÓN
Secretos de desarrollador y de aplicación almacenados en la base de datos	AES-128-GCM, cuando la integración externa de Vault no está en uso
Base de datos, volúmenes persistentes, `etcd`	Cifrado de su infraestructura, como KMS del proveedor de la nube o volúmenes persistentes cifrados de Kubernetes

Claves y certificados

PROPÓSITO	ALGORITMO
Cifrado de secretos de aplicación	AES-128-GCM
Tokens de API	AES-GCM
Identidades SSH personales	Ed25519
Certificado de firma SAML, cuando SecurSpaces actúa como proveedor de identidad	RSA 2048
Firma de tokens	Claves de firma de JSON Web Token, almacenadas como Kubernetes Secrets
TLS	Certificados X.509

SecurSpaces admite la gestión automatizada del ciclo de vida de los certificados para el tráfico externo, como cert-manager, Let's Encrypt, o una PKI interna. Gestiona los certificados para el tráfico interno del clúster por sí mismo.

Almacenamiento de secretos

SECRETO	DÓNDE SE GUARDA
Secretos de desarrollador y aplicación	Cifrado en la base de datos, o en una instancia externa de HashiCorp Vault cuando esa integración está habilitada
Certificados, claves de acceso, claves de cifrado, credenciales de base de datos, claves de firma de tokens	Kubernetes Secrets, almacenados en `etcd`

Los Secrets de Kubernetes se almacenan en `etcd`, que debe proteger con cifrado en reposo. Para una separación más robusta, SecurSpaces funciona con los operadores Secrets Store CSI Driver y External Secrets.

Información relacionada

- Puertos y protocolos
- Flujos de datos de seguridad
- Catálogo de controles de seguridad

Mount point limits and behavior

Capacidad, cuotas y escala

Los archivos EFS y S3 son elásticos. No hay un tamaño aprovisionado. El valor de almacenamiento en el volumen es requerido por Kubernetes, pero se ignora, así que no prometa a los usuarios una cuota de tamaño por punto de montaje.

LÍMITE	VALOR
Puntos de acceso por sistema de archivos EFS	Aproximadamente 10.000. Un valor predeterminado que el Soporte de AWS puede aumentar.
Puntos de acceso por sistema de archivos S3 Files	25.000. No se puede aumentar.
Destinos de montaje por Zona de Disponibilidad	1 por Zona de Disponibilidad. Límite estricto.

LÍMITE	VALOR
Puntos de montaje creados por sistema de archivos, por región	1.000. Impuesto por SecurSpaces y no configurable.

Cada punto de montaje de **Crear nuevo** consume un punto de acceso, y el límite se comparte entre todos los proyectos de ese sistema de archivos. Un punto de acceso que cree manualmente ocupa una ranura desde el momento en que lo crea, así que cuente los puntos de acceso precreados en el mismo presupuesto.

Cuando se alcanza el límite de 1.000, las nuevas solicitudes de **Crear nuevo** se rechazan con un mensaje que indica que el sistema de archivos ha alcanzado su límite de almacenamiento. La restricción solo se aplica a Crear nuevo. Un punto de montaje de **Adjuntar existente** no se cuenta contra los 1.000 ni es bloqueado por este, porque no consume una nueva ranura de punto de acceso.

El límite está compilado en el producto. No es un valor de configuración, Helm o entorno. También es aproximado, y hay tres formas en que un sistema de archivos lo supera:

- Una ráfaga de creaciones simultáneas puede superar ligeramente el límite de un sistema de archivos.
- Durante una interrupción del almacén de datos, el recuento no se puede leer y la creación se permite sin verificar.
- Cuando no se puede leer la lista de StorageClass, no se puede resolver el ID del sistema de archivos, por lo que se omite la puerta por completo y la creación procede sin protección. Este es el mismo permiso faltante que desactiva las comprobaciones de cifrado de Create New, descritas en Configurar SecurSpaces.

Considere el límite como un indicador principal y el techo de AWS como el verdadero tope. Ambos de los dos últimos casos se cuentan, por lo que puede configurar alertas sobre ellos. Consulte Métricas.

Prefiera un sistema de archivos dedicado a los puntos de montaje de SecurSpaces. En un sistema de archivos compartido, SecurSpaces solo cuenta sus propios puntos de acceso, por lo que el total real puede acercarse al techo de AWS mientras SecurSpaces todavía cree que hay espacio.

El aislamiento entre los puntos de montaje es la identidad de directorio y POSIX en un sistema de archivos compartido. Los puntos de acceso en un sistema de archivos comparten una clave de

cifrado y un grupo de rendimiento. Coloque un inquilino que necesite su propia clave, grupo de rendimiento y dominio de fallo en un sistema de archivos separado.

> **Nota**
>
> Un sistema de archivos separado no es por sí mismo un límite de acceso. Quién puede montar lo deciden IAM y la red. Para que la división sea real, limite los permisos de cliente del rol del nodo a sistemas de archivos con nombre y mantenga los destinos de montaje del sistema de archivos cerrados a los nodos de otros clústeres.

Eliminación y protección de datos

Lo que una eliminación elimina depende de cómo se creó el punto de montaje:

MODO	LO QUE SECURSPACES ELIMINA	DATOS DE RESPALDO
Crear nuevo	La reclamación. La política de recuperación de StorageClass elimina entonces el volumen.	Destruido. El punto de acceso se elimina.
Adjuntar existente, volumen creado por SecurSpaces	La reclamación y el volumen.	Retenido.
Adjuntar existente, volumen que usted creó	Solo la reclamación.	Retenido.

Al eliminar un punto de montaje de **Crear nuevo** se elimina el punto de acceso, pero deja su directorio y archivos en el sistema de archivos. Planifique una limpieza periódica de estos directorios huérfanos y nunca adjunte un volumen raíz del sistema de archivos sobre un sistema de archivos de este tipo.

Un punto de montaje no se puede eliminar mientras un espacio de trabajo activo o una plantilla de espacio de trabajo lo utilice. Tampoco se puede eliminar mientras un espacio de trabajo eliminado en la papelera de reciclaje lo siga utilizando, porque ese espacio de trabajo puede restaurarse. Desvincularlo no ayuda en ese caso. Elimine permanentemente los espacios de trabajo nombrados de **Espacios de trabajo eliminados**, espere a que expire el período de retención, o restaure el espacio de trabajo y elimine el punto de montaje de él.

Las actualizaciones son solo de metadatos. Solo se pueden cambiar el nombre y la ruta de montaje. El ID del sistema de archivos, el punto de acceso y la subruta se fijan cuando se crea el punto de montaje, los puntos de montaje de AWS no se pueden redimensionar, y la configuración de lectura-escritura o solo lectura no se puede cambiar después de la creación.

Advertencia

Un punto de montaje es un almacenamiento colaborativo de lectura-escritura sin opción de deshacer. Cada espacio de trabajo que lo monta puede eliminar cualquier archivo, y el punto de acceso consolida toda la actividad en una única identidad POSIX, por lo que la propiedad del archivo no ofrece protección por usuario. SecurSpaces no crea, programa, verificar ni supervisa copias de seguridad. La copia de seguridad y la recuperación de los datos del punto de montaje son enteramente responsabilidad del propietario de la cuenta de AWS.

Para Amazon EFS, la única ruta de recuperación es un punto de recuperación de AWS Backup que existía antes de la pérdida. Las copias de seguridad se toman por sistema de archivos, no por punto de montaje. Una restauración completa devuelve el directorio de cada proyecto en ese sistema de archivos junto, y quien pueda ejecutarla puede leerlo todo. Una restauración a nivel de elemento puede dirigirse a archivos y directorios, por lo que recuperar una carpeta eliminada no significa traer de vuelta todo. Prefiera una restauración a nivel de elemento cuando solo se esté recuperando una carpeta.

Para los archivos de Amazon S3, el control de versiones de los buckets es la ruta de recuperación: un archivo eliminado a través del sistema de archivos se convierte en una versión de objeto no actual. Combínelo con una regla de ciclo de vida que mantenga las versiones no actuales el tiempo suficiente para que sean útiles.

Advertencia

Nunca permita que los datos en vivo se muevan a un nivel de archivo. Los objetos en Glacier Flexible Retrieval o Deep Archive, y los objetos de Intelligent-Tiering que han caído en un nivel de Archive Access, no se pueden leer a través del sistema de archivos en absoluto. Deben restaurarse a través de la API de S3 antes de que el sistema de archivos pueda leerlos de nuevo, y nada en SecurSpaces o en el montaje le advierte: los archivos simplemente se vuelven ilegibles para cada espacio de trabajo. Aplique las reglas de transición solo a versiones no actuales, y mantenga cada objeto actual en una clase

directamente legible: Standard, Standard-IA, One Zone-IA, o Intelligent-Tiering con los niveles de archivo desactivados. Una regla de transición es solo una de las dos formas de entrada. Los niveles de archivo de Intelligent-Tiering son una configuración de bucket, no una regla de ciclo de vida.

Una restauración nunca devuelve los archivos a su ubicación original. AWS Backup escribe en un nuevo directorio fuera de la raíz del sistema de archivos, llamado `aws-backup-restore_<datetime>`, y cada intento crea uno nuevo. Dado que cada Mount Point está enraizado dentro de un directorio de punto de acceso, ese directorio se encuentra por encima de la raíz del montaje y es invisible desde cualquier espacio de trabajo. Prevea una copia manual como parte de cada restauración:

1. Ejecute la restauración. Restaure en el sistema de archivos **de origen** siempre que aún exista. Eso mantiene el ID del sistema de archivos y cada punto de acceso válidos, por lo que ningún Mount Point tiene que cambiar. Restaure en un nuevo sistema de archivos solo si el original ha desaparecido.
2. Desde un host administrativo en la misma VPC, no desde un espacio de trabajo de desarrollador, monte el sistema de archivos sin un punto de acceso: `sudo mount -t efs -o tls <file-system-id>:/ /mnt/recovery`.
3. Copie los archivos deseados de `/mnt/recovery/aws-backup-restore_<datetime>/` al directorio del punto de acceso que el Mount Point utiliza, conservando la propiedad y los permisos con `cp -a` o `rsync -a`.
4. Elimine el directorio de recuperación una vez que haya confirmado la copia de seguridad, ya que sigue facturando como almacenamiento del sistema de archivos. Luego desmonte `/mnt/recovery`.

Advertencia

Ese montaje no tiene punto de acceso, por lo que expone los datos de cada proyecto en el sistema de archivos. Ejecútelo bajo control de cambios y desmóntelo tan pronto como finalice la copia de seguridad. Mantenga la opción `tls`: el requisito de SecurSpaces de que cada montaje lleve `tls` se aplica a los volúmenes que crea el producto, no a un montaje que ejecute manualmente, por lo que sin ello la copia de seguridad cruza la VPC sin cifrar en el puerto 2049.

> Si el sistema de archivos original ha desaparecido, una restauración recupera bytes, no Mount Points. Un nuevo sistema de archivos tiene un nuevo ID de sistema de archivos y ningún punto de acceso, y el ID del sistema de archivos, el punto de acceso y la subruta de un Mount Point se fijan en el momento de la creación. Cada Mount Point afectado debe eliminarse y recrearse contra el sistema de archivos restaurado, con sus datos copiados en el directorio recién creado.

Ensaye todo el procedimiento, no solo el trabajo de restauración. Una restauración que informa éxito no prueba nada sobre si los desarrolladores recuperan sus archivos. Confirme desde dentro de un espacio de trabajo que los archivos y su propiedad aparecen en la ruta de montaje.

Nota

> Mantenga sus manifiestos de StorageClass y volumen en el control de código fuente. Si pierde el clúster, los volúmenes, las reclamaciones y las StorageClasses desaparecen, mientras que los registros de los Mount Points sobreviven y siguen informando como listos.

Comportamiento de los archivos de Amazon S3 a tener en cuenta

- **No hay hardlinks.** Un archivo es una clave de objeto de S3, y un intento devuelve `Too many links`. Las herramientas que desduplican usando hardlinks fallan o recurren a otras opciones. Los symlinks funcionan.
- **La exportación es asíncrona**, tardando aproximadamente entre 60 y 72 segundos. Un archivo escrito en un espacio de trabajo aparece como un objeto después de una sincronización, no instantáneamente. Dentro del sistema de archivos, las lecturas, escrituras y el bloqueo son inmediatamente consistentes.
- **Las escrituras en conflicto descartan la versión del espacio de trabajo.** Si el mismo archivo cambia tanto en un espacio de trabajo como directamente en S3, el bucket prevalece. No se devuelve ningún error a quien escribió el archivo, y SecurSpaces tampoco muestra el conflicto, por lo que el único canal de detección es AWS. Active una alarma en `LostAndFoundFiles`, el recuento por sistema de archivos que Amazon S3 Files publica en el espacio de nombres `AWS/S3/Files` bajo la dimensión `FileSystemId`. Cuenta los archivos que se encuentran actualmente en el directorio de objetos perdidos, así que active una alarma ante cualquier aumento. Divida el bucket por escritor, o mantenga los procesos externos en modo de solo lectura.

- **Los archivos desplazados terminan donde los espacios de trabajo no pueden verlos**, en un directorio llamado `.s3files-lost+found-<file-system-id>` en la raíz del sistema de archivos. El nombre tiene un prefijo de punto, por lo que un `ls` simple no lo muestra, y se encuentra por encima de cada raíz de montaje, por lo que solo un operador puede recuperar los archivos. Esas copias nunca se exportan, por lo que nunca existe una versión de objeto para ellas: el control de versiones del bucket no las cubre, y la recuperación desde ese directorio es la única vía. AWS los conserva y factura indefinidamente.
- **Una ruta más larga que el límite de clave de S3 de 1024 bytes nunca llega al bucket.** La exportación falla de forma terminal, por lo que no existe una versión de objeto para restaurar y el control de versiones del bucket no la cubre. Active una alarma en la métrica `ExportFailures` de CloudWatch en el espacio de nombres `AWS/S3/Files`.

Utilice Amazon EFS para trabajos sensibles a la latencia, como árboles de git y cachés de compilación. Utilice Amazon S3 Files para conjuntos de datos grandes y en su mayoría inmutables, donde es sustancialmente más barato.

Los archivos son propiedad de la identidad del punto de acceso en lugar del usuario del espacio de trabajo, por lo que las herramientas sensibles a la propiedad, como la comprobación `safe.directory` de git, pueden emitir una advertencia. Este es un comportamiento normal del punto de acceso.

Recuperar un archivo desplazado

Acceder al directorio de objetos perdidos significa montar el sistema de archivos sin un punto de acceso, lo que expone los datos de cada proyecto en ese sistema de archivos. Trate todo el procedimiento como una operación controlada por cambios en un host administrativo en la misma VPC, nunca como algo ejecutado desde un espacio de trabajo de desarrollador. Si prefiere no montar sin un punto de acceso, cree un punto de acceso temporal sin restricción de directorio raíz y un usuario POSIX fijo, permítalo solo desde el host de recuperación y elimínelo en la misma ventana de cambio. Un punto de acceso con raíz en el directorio de objetos perdidos no es una solución alternativa: los archivos no se pueden mover ni renombrar dentro de él, y la copia de seguridad escribe en la ruta original del archivo, que se encuentra fuera de él.

Monte el sistema de archivos y liste el directorio:

```
sudo mount -t s3files <file-system-id>:/ /mnt/recovery

ls -la /mnt/recovery/.s3files-lost+found-<file-system-id>
```

Los nombres allí no son los originales. Se antepone un ID hexadecimal para que los conflictos repetidos en un archivo permanezcan distintos, los nombres de más de 100 caracteres se truncan y la ruta del directorio original no se conserva. La ruta solo sobrevive en un atributo extendido. Léalo con `getfattr`. La marca de tiempo en el nombre del atributo es necesaria, porque fuerza una lectura de estado actualizada:

```
getfattr -n "user.s3files.status;$(date -u +%s)" \

  /mnt/recovery/.s3files-lost+found-<file-system-id>/<hex-id>_<name> --
only-values
```

`S3Key` es la clave del objeto y está vacía si el objeto se eliminó en el bucket. `FilePath` es la ruta que tenía el archivo antes del conflicto.

Para mantener la versión del espacio de trabajo, copie el archivo de nuevo a `FilePath` bajo el montaje. S3 Files lo exporta de nuevo como una nueva versión de objeto. Para mantener la versión del bucket, elimine la copia desplazada en su lugar. Puede copiar fuera de este directorio y eliminar dentro de él, pero no puede mover ni renombrar dentro de él, y no puede eliminar el directorio en sí.

Finalice en la misma ventana de cambio: desmonte y elimine cualquier punto de acceso temporal que haya creado. Cualquier cosa que quede en el directorio seguirá facturándose como almacenamiento del sistema de archivos.

Multirregión

Los puntos de montaje no son compatibles con configuraciones multirregión. El diálogo de creación no ofrece opción de región, por lo que un punto de montaje creado allí siempre pertenece a la región principal, y el paso **Recursos** del espacio de trabajo impide añadir un punto de montaje a un espacio de trabajo en cualquier otra región.

> **Advertencia**

> Esa restricción se aplica en el diálogo de creación, no en el endpoint REST de creación. En una implementación con una región secundaria configurada, un llamador de API que establece `region_id` a esa región crea un punto de montaje allí. El registro no se filtra después, por lo que permanece en la lista de **Puntos de Montaje** del proyecto y se puede

> adjuntar a un espacio de trabajo de región primaria, donde el volumen no existe. Deje `region_id` sin establecer cuando cree un punto de montaje a través de la API.

> Las plantillas de espacio de trabajo no están cubiertas por ese bloque. El editor de plantillas permite adjuntar un punto de montaje independientemente de la región, por lo que se puede guardar una plantilla que contenga almacenamiento que los espacios de trabajo fuera de la región primaria no pueden usar. No trate esto como una forma compatible de usar puntos de montaje en una región secundaria.

Tiempos de espera

El aprovisionamiento está sujeto a dos tiempos de espera fijos. Ninguno es configurable.

TIEMPO DE ESPERA	VALOR
Enlace de volumen	3 minutos
Llamada de aprovisionamiento general	5 minutos

Exceder cualquiera de ellos mueve el punto de montaje a un estado de error, desde el cual se puede eliminar y volver a crear.

Métricas

SecurSpaces publica métricas de Prometheus para los puntos de montaje en dos endpoints, y solo uno de ellos es accesible tal como se entrega:

- **El plano de control** sirve `/metrics` a través de **HTTPS**, en el puerto 8080, junto con el resto de su API.
- **El servicio de espacio de trabajo** sirve `/metrics` a través de **HTTP sin cifrar**, en el puerto 2112. El gráfico no coloca ese puerto en un servicio de Kubernetes y no lo declara como un puerto de contenedor, por lo que nada puede extraerlo hasta que lo exponga usted mismo.

El gráfico tampoco incluye ServiceMonitor, PodMonitor, PrometheusRule, anotaciones de scrape o paneles. La creación de sus propias alertas comienza con la configuración de scrape. Dado que el punto final del plano de control es HTTPS, un trabajo dirigido a `http://` falla en el handshake TLS, sin que el producto ofrezca ninguna explicación:

```
scrape_configs:

  - job_name: securspaces-central

    scheme: https

    metrics_path: /metrics

    tls_config:

      # The CA that signed the control plane's certificate.

      ca_file: /etc/prometheus/certs/ca.crt

    static_configs:

      - targets: ["<release>-central-service:8080"]
```

Para acceder a las métricas del servicio del espacio de trabajo, añada el puerto 2112 a los puertos del contenedor del servicio del espacio de trabajo y a un Servicio delante de él, luego añada un segundo trabajo para ese Servicio con `scheme: http`.

Métricas publicadas

MÉTRICA	ETIQUETAS	LO QUE REGISTRA
`sds_mountpoint_create_total`	`type`, `result`, `reason`	Resultado final de la creación de un punto de montaje
`sds_mountpoint_create_rejected_total`	`reason`	Creaciones rechazadas antes de que comience el aprovisionamiento, excluyendo el rechazo por cuota flexible contado por separado
`sds_mountpoint_quota_gate_total`	`outcome`: `allowed`, `rejected`, `failed_open`, `skipped_no_fsid`	Decisiones de la puerta de cuota flexible por sistema de archivos en Crear nuevo
`sds_mountpoint_attach_admit_total`	`sub_mode`, `decision`, `reason`	Adjuntar decisiones de admisión existentes

MÉTRICA	ETIQUETAS	LO QUE REGISTRA
`sds_mountpoint_readback_total`	`provider`, `mount_point_type`, `result`	Resultado de la lectura del identificador de volumen después del enlace
`sds_mountpoint_state_write_total`	`outcome`: `persisted`, `write_error`, `lost_race`. `state`: `MOUNT_POINT_PROVISIONING`, `MOUNT_POINT_READY`, `MOUNT_POINT_ERROR`	Cada transición de estado del punto de montaje, excepto las dos escrituras de reclamación que inician una eliminación y una actualización
`sds_mountpoint_stranded_recovered_total`	`state`: `MOUNT_POINT_CREATING`, `MOUNT_POINT_PROVISIONING`, `MOUNT_POINT_DELETING`	Filas readmitidas después de quedar varadas en un estado transitorio
`sds_mountpoint_enable_flag_failopen_total`	`cause`	Veces que la comprobación de la bandera de habilitación falló abierta, permitiendo una creación a pesar de una configuración ilegible o ausente
`sds_mountpoint_picker_classes_hidden`	`region`	StorageClasses actualmente ocultas del selector Crear nuevo por falta de la opción de montaje `tls`

Cada métrica de esta tabla es publicada por el plano de control, excepto `sds_mountpoint_readback_total`, que es publicada por el servicio del espacio de trabajo. Una alerta en el contador de lectura permanece permanentemente vacía hasta que el puerto 2112 se expone y se rastrea.

Consulte los valores de las etiquetas exactamente como están escritos arriba. La etiqueta `state` contiene los nombres de enumeración del búfer de protocolo, en mayúsculas, mientras que cualquier otro valor de etiqueta es un token en minúsculas, por lo que una consulta para `state="ready"` no coincide con nada y se lee como saludable. Tenga en cuenta también que la

serie de un contador no existe hasta que se incrementa por primera vez, por lo que no puede descubrir estos valores rastreando una implementación que aún no ha alcanzado la condición.

> **Advertencia**
>
> No cambie el nombre de estas métricas para que coincidan con el nombre del producto. Mantuvieron su ortografía original deliberadamente, y cambiar el nombre de una rompe silenciosamente cada panel y alerta construidos sobre ella.

Alertas que vale la pena construir

No se incluyen alertas con el producto. Estas son las que vale la pena construir primero.

- **`sds_mountpoint_quota_gate_total`** con un `outcome` de `failed_open` o `skipped_no_fsid`. Cualquiera de los valores significa que se permitió un Crear nuevo con el recuento por sistema de archivos sin verificar. Alerte sobre cualquier valor distinto de cero de cualquiera de ellos.
- **`sds_mountpoint_attach_admit_total{decision="deny"}`**. Un adjunto denegado, incluido un intento entre proyectos. Estas denegaciones existen como líneas de registro del plano de control y solo en este contador. No se escriben como eventos de auditoría, por lo que no aparecen en la página de **Auditoría** y no llegan a una exportación CEF o SIEM. Si su equipo de seguridad espera denegaciones de adjuntos en el SIEM, este contador es el único canal.
- **`sds_mountpoint_readback_total{mount_point_type="create_new",result="no_access_point"}`**. Limite la alerta a `create_new`. Un Crear nuevo cuyo identificador de volumen se resuelve sin un punto de acceso es rechazado: SecurSpaces no lo marca como listo y el registro pasa al estado de error, por lo que ningún punto de montaje de este tipo es utilizable. Un recuento distinto de cero significa que se aceptó un Crear nuevo aunque su StorageClass debería haber sido rechazada. No significa que se hayan expuesto datos. No alerte sobre cada `result` que no sea `resolved`: un Adjuntar existente que deliberadamente no nombra ningún punto de acceso devuelve `no_access_point`, y esa es una configuración compatible. Este contador es el publicado por el servicio del espacio de trabajo, por lo que la alerta necesita el rastreo del puerto 2112 descrito anteriormente.
- **`sds_mountpoint_state_write_total`** con un `outcome` de `write_error`, y `lost_race` con `state="MOUNT_POINT_READY"`. Una escritura READY perdida puede dejar un registro que parece correcto en el producto pero que nunca alcanzó realmente el estado de listo.

- `sds_mountpoint_enable_flag_failopen_total`. Cualquier valor distinto de cero significa que se permitió una creación mientras no se pudo leer la configuración.
- `sds_mountpoint_picker_classes_hidden` por encima de cero. Eso significa que al menos una StorageClass está oculta de la lista Crear nuevo. Cero no significa que no haya una configuración incorrecta: una clase que mantienes visible deliberadamente no se cuenta, y una sonda que falla también informa cero, incluso cuando falla porque falta el permiso de lectura de StorageClass. Limite la alerta a las regiones que aún están en servicio, porque la serie por región nunca se elimina y una región desmantelada sigue informando su último valor.

El único fallo sin contador

Si el servicio de espacio de trabajo no puede leer StorageClasses, las comprobaciones de cifrado de Crear nuevo se desactivan y las creaciones proceden sin ellas. Ese fallo no incrementa ningún contador. Aparece solo como una línea de registro, y solo en los registros del **servicio de espacio de trabajo**, no en los del plano de control.

Cree una alerta de registro sobre el texto literal `RBAC forbidden` en los registros del servicio de espacio de trabajo. Haga coincidir esa cadena en lugar de una frase más larga: el fallo de permiso se informa desde varias comprobaciones diferentes, y una coincidencia más específica solo detecta una de ellas.

Configurar SecurSpaces cubre el mismo permiso, la comprobación única `kubectl auth can-i`, y las dos configuraciones de Helm que eliminan la concesión.

Información relacionada

- Preparar el almacenamiento de AWS para puntos de montaje
- Solucionar problemas de puntos de montaje de AWS

Network destinations

Las direcciones externas a las que debe acceder una implementación de Citrix SecurSpaces™ para las reglas de firewall y la planificación de entornos aislados.

Los números de versión de esta página corresponden a la versión 2026.9.4. Sustituya la versión que esté instalando.

Resumen

DESTINO	PROPÓSITO	NECESARIO
`api.enterprise.strong.network:443`	Verificación y renovación de licencias	Continuamente, a menos que utilice una licencia sin conexión
Docker Hub	La imagen de Strong Installer	En el momento de la instalación y actualización
`europe-docker.pkg.dev` y espejos regionales	Gráfico de Helm e imágenes de contenedor	En el momento de la instalación y actualización

Servidor de licencias

ELEMENTO	VALOR
Dirección	`api.enterprise.strong.network`
Puerto	443
Propósito	Verificación y renovación de licencias en línea

Durante la instalación, la plataforma se conecta al servidor de licencias para validar la licencia y emitir un token temporal para el registro de imágenes de contenedor.

Puede proporcionar una licencia firmada en su lugar, configurando `platform.license` en los valores de Helm a una licencia codificada en base64. Se aplica automáticamente al implementar y actualizar.

> **Nota:**

> Para entornos aislados, permita que el controlador de SecurSpaces acceda al servidor de licencias a través de su firewall, o solicite una licencia sin conexión para un funcionamiento totalmente desconectado. Consulte Licencia.

Imagen del instalador

ELEMENTO	VALOR
Origen	Docker Hub
Imagen	`strongnetwork/strong_installer:2026.9.4`

Gráfico de Helm

ELEMENTO	VALOR
Origen	Google Artifact Registry
Principal	`europe-docker.pkg.dev/strong-network-release/charts/ninjahchart:2026.9.4`
Réplicas	`us-docker.pkg.dev`, `asia-docker.pkg.dev`

Imágenes de contenedor

ELEMENTO	VALOR
Origen	Google Artifact Registry
Principal	`europe-docker.pkg.dev/strong-network-release/images`
Réplicas	`us-docker.pkg.dev`, `asia-docker.pkg.dev`

Elija la réplica más cercana a su clúster con el indicador `--source-registry-region`. Consulte referencia de la CLI de SDS.

Imágenes de servicio

IMAGEN
`cloud_editor_sidecar_proxy:2026.9.4`

IMAGEN
`sn_enterprise_bundle:2026.9.4`

Imagen del espacio de trabajo

IMAGEN
`ws-images/cloud_editor_generic:2.3.9`

Esta es la única imagen de espacio de trabajo que el instalador envía. La etiqueta proviene del valor predeterminado integrado del instalador, que puede anular con el indicador `-w` o `--workspace-image-tag`.

Imágenes adicionales de espacio de trabajo

Citrix publica más imágenes de espacio de trabajo y definiciones de imágenes de ejemplo, que cubren IDEs y cadenas de herramientas de lenguaje más allá de la imagen predeterminada.

ORIGEN	DIRECCIÓN
Definiciones de imágenes de ejemplo	github.com/strong-network/images
Imágenes precompiladas	hub.docker.com/u/strongnetwork

Importante:

El instalador no envía estas imágenes. Solo envía las imágenes de servicio y la única imagen de espacio de trabajo mencionada anteriormente. Para usar una imagen adicional en una implementación aislada, extráigala y envíela a su propio registro, y luego agréguela como una imagen de contenedor.

Consulte Imágenes de contenedor para agregar una imagen a un proyecto, y Requisitos de imágenes de contenedor para saber qué debe proporcionar una imagen.

Información relacionada

- Requisitos del sistema
- Puertos y protocolos

- Referencia de la CLI de SDS
- Instalar con la CLI de Strong Installer

Network policy fields

Los campos disponibles en el editor YAML de modo experto para una política de red de Citrix SecurSpaces™. Para saber cómo acceder a el editor, consulte Crear una política de red.

Campos de la política

CAMPO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`name`	cadena	Sí	El nombre de la política. No debe estar vacío.
`description`	cadena	Sí	Lo que hace la política. No debe estar vacío.
`restrictedTraffic`	booleano	Sí	`true` restringe el tráfico saliente a los recursos adjuntos y a la lista de permitidos. `false` monitoriza el tráfico sin bloquearlo.
`customEndpointsEnabled`	booleano	No	Habilita las listas de permitidos de custom-endpoints-via-proxy. Relevante solo cuando la plataforma utiliza un proxy externo.
`whitelistedDomains`	lista de entradas de dominio	No	Dominios a los que el espacio de trabajo tiene permitido acceder.

CAMPO	TIPO	OBLIGATORIO	DESCRIPCIÓN
`whitelistedIps`	lista de cadenas	No	Direcciones IPv4 o rangos CIDR a los que el espacio de trabajo tiene permitido acceder.
`customEndpointsViaProxyDomains`	lista de entradas de dominio	No	Dominios accesibles a través del proxy externo. Se utiliza solo cuando `customEndpointsEnabled` es `true`.
`customEndpointsViaProxyIps`	lista de cadenas	No	Direcciones IPv4 o rangos CIDR accesibles a través del proxy externo. Se utiliza solo cuando `customEndpointsEnabled` es `true`.

Importante:

El editor rechaza cualquier campo que no esté en esta tabla. Una política que contenga un campo no reconocido no se valida.

Entradas de dominio

Cada entrada en `whitelistedDomains` y `customEndpointsViaProxyDomains` tiene esta forma.

CAMPO	TIPO	DESCRIPCIÓN
`domain`	cadena	El dominio a permitir, por ejemplo `example.com`.

CAMPO	TIPO	DESCRIPCIÓN
`includeSubdomains`	booleano	Cuando `true`, se permiten el dominio y todos sus subdominios.

Las dos listas validan `domain` de forma diferente:

- En `whitelistedDomains`, el valor debe ser un nombre de dominio simple, como `example.com` o `pypi.internal.example.com`. Utilice `includeSubdomains` para cubrir subdominios en lugar de escribir un comodín.
- En `customEndpointsViaProxyDomains`, se acepta un prefijo inicial, por lo que un valor como `*.example.com` es válido.

Entradas de direcciones IP

`whitelistedIps` y `customEndpointsViaProxyIps` aceptan:

- Una única dirección IPv4, por ejemplo `192.168.1.50`.
- Un rango CIDR IPv4 con una longitud de prefijo de `/0` a `/32`, por ejemplo `10.0.0.0/24`.

No se aceptan direcciones IPv6.

Ejemplo

```
name: Backend services policy

description: Restrict workspaces to internal package mirrors and the
corporate API.

restrictedTraffic: true

whitelistedDomains:

  - domain: pypi.internal.example.com

    includeSubdomains: false

  - domain: example.com

    includeSubdomains: true
```

```
whitelistedIps:

  - 10.0.0.0/24

  - 192.168.1.50
```

Nota:

Cuando `customEndpointsEnabled` es `false`, las listas de puntos finales personalizados se ignoran y se borran. Configure esos campos solo cuando se utilice un proxy externo.

Información relacionada

- Políticas de red
- Crear una política de red

Ports and protocols

Los puertos de red que expone una implementación de Citrix SecurSpaces™ para reglas de firewall y seguridad de red.

Esta página cubre las implementaciones en un clúster de Kubernetes. Para los puertos que necesita un entorno de evaluación de VM de 1 clic, consulte Implementar en la nube.

Puertos expuestos externamente

Estos son los únicos puertos que deben llegar al clúster desde su red.

PUERTO	PROTOCOLO	PROPÓSITO
443	HTTPS	La consola de SecurSpaces, la API y las aplicaciones de espacio de trabajo servidas a través del nombre de host del proxy
80	HTTP	Redirige a HTTPS

PUERTO	PROTOCOLO	PROPÓSITO
Su elección, comúnmente 22	TCP, que transporta SSH	Desarrollo remoto a través de SSH. Reenviado por el controlador de entrada a la API del espacio de trabajo.

TLS se termina en el controlador de entrada. Las versiones de TLS y los conjuntos de cifrado permitidos son, por lo tanto, establecidos por la configuración de su entrada, no por SecurSpaces.

Reenvío de puertos SSH

SecurSpaces no fija el puerto SSH externo. Usted lo elige al configurar el reenvío TCP en el controlador de entrada, y la entrada lo reenvía al puerto `2222` en la API del espacio de trabajo.

LADO	PUERTO
Externo	Lo que configure en el controlador de entrada. Comúnmente 22.
Interno, en la API del espacio de trabajo	`2222`

> **Importante:**

> El puerto `2222` está codificado en la API del espacio de trabajo. No lo cambie.

> Para los pasos de configuración, consulte Habilitar el acceso SSH a los espacios de trabajo.

Puertos de servicio internos

Los servicios de SecurSpaces se comunican a través de puertos adicionales dentro del clúster, incluidos los puertos gRPC y HTTP en los servicios central, coordinador, monitor, espacio de trabajo y proxy. Estos son internos al clúster. No necesitan ser accesibles desde fuera del clúster, y puede restringirlos con las políticas de red de Kubernetes.

Para saber cómo SecurSpaces utiliza las políticas de red para controlar el tráfico del espacio de trabajo, consulte Políticas de red.

Información relacionada

- Criptografía
- Flujos de datos de seguridad
- Habilitar el acceso SSH a los espacios de trabajo

Sizing

Cuánta infraestructura necesita una implementación de Citrix SecurSpaces™ y qué la impulsa.

Para saber qué requiere la plataforma en lugar de cuánto, consulte Requisitos del sistema.

Cómo abordarlo

Un clúster de SecurSpaces tiene dos tipos de nodos, y su tamaño se calcula de forma diferente:

GRUPO DE NODOS	EJECUTA	ESCALA CON
Servicio	El plano de control — servicio central, frontend, coordinador, proxy, servicio de espacio de trabajo y la base de datos si está en el clúster	El tamaño de la plataforma, no el número de desarrolladores. En gran medida fijo.
Espacio de trabajo	Espacios de trabajo de desarrollador, un pod cada uno	El número de espacios de trabajo **ejecutándose simultáneamente**, no el número que existen

El dimensionamiento del grupo de servicios es una planificación de capacidad que se realiza una vez. El dimensionamiento del grupo de espacios de trabajo es una operación aritmética sobre las especificaciones de espacio de trabajo que ofrece, y es la parte que cambia.

Esta página proporciona cifras para dos tamaños: una **prueba de concepto para 50 desarrolladores** y una **implementación de producción de 500 desarrolladores**. Trate ambos como puntos de partida y verificar con su propio uso — consulte Asignación de recursos para leer el consumo real.

> **Nota**

> Si desea evaluar SecurSpaces en lugar de ejecutar un piloto con usuarios reales, la VM de 1 clic es una ruta más rápida que construir un clúster. Ejecuta toda la plataforma en una única máquina virtual. Para sus tamaños, consulte VM de 1 clic. Para implementarla, consulte Implementar un entorno de evaluación. La guía a continuación es para una implementación de Kubernetes que un grupo de desarrolladores realmente utilizará.

Grupos de nodos de referencia

500 desarrolladores

NUBE	GRUPO DE NODOS DE SERVICIO	GRUPO DE NODOS DE ESPACIO DE TRABAJO
AWS	Dos `m7i.2xlarge` (8 vCPU, 32 GiB)	`m7i.4xlarge` (16 vCPU, 64 GiB), escalado automático
Azure	Dos `Standard_D8as_v6` (8 vCPU, 32 GiB)	`Standard_D16as_v6` (16 vCPU, 64 GiB), escalado automático
Google Cloud	Dos `n2-standard-8` (8 vCPU, 32 GiB)	`n2-standard-16` (16 vCPU, 64 GiB), autoescalado

50 desarrolladores (prueba de concepto)

NUBE	GRUPO DE NODOS DE SERVICIO	GRUPO DE NODOS DE ESPACIO DE TRABAJO
AWS	Un `m7i.2xlarge` (8 vCPU, 32 GiB)	`m7i.2xlarge` (8 vCPU, 32 GiB), autoescalado 1–6
Azure	Un `Standard_D8as_v6` (8 vCPU, 32 GiB)	`Standard_D8as_v6` (8 vCPU, 32 GiB), autoescalado 1–6
Google Cloud	Un `n2-standard-8` (8 vCPU, 32 GiB)	`n2-standard-8` (8 vCPU, 32 GiB), autoescalado 1–6

El nodo de servicio no se reduce cuando lo hace la implementación. El plano de control ejecuta los mismos servicios de cualquier manera, y una base de datos en clúster aún puede usar 2 núcleos y

4 GiB en su límite, por lo que 8 vCPU y 32 GiB sigue siendo el mínimo sensato. Lo que cambia es el **recuento**: un nodo de servicio en lugar de dos.

Ese nodo único es la compensación a entender. Una prueba de concepto con un solo nodo de servicio no tiene control de redundancia del plano — durante un fallo o una actualización del nodo, la plataforma no está disponible y los espacios de trabajo en ejecución pierden su conexión. Esto suele ser aceptable durante la evaluación y nunca aceptable en producción. **Pase a dos nodos de servicio antes de incorporar usuarios reales**, independientemente de si el número de desarrolladores ha crecido.

El grupo de espacios de trabajo es más pequeño tanto en forma como en número, porque un grupo que escala en pasos de 16 vCPU es un ajuste tosco cuando la demanda máxima es de 20 espacios de trabajo. Los nodos más pequeños desperdician menos mientras están inactivos.

Ambos tamaños

Lo que importa es la forma — 8 vCPU / 32 GiB para nodos de servicio y 16 vCPU / 64 GiB para nodos de espacio de trabajo — no la familia específica. Generaciones anteriores como `m6i` o `Standard_D8as_v5` son equivalentes, y cualquier instancia de propósito general del mismo tamaño funciona.

> **Importante:**

> SecurSpaces requiere nodos `amd64`. Las instancias AWS Graviton (`m7g`, `m8g`) y los tamaños basados en ARM de Azure son `arm64` y no son compatibles. Consulte Requisitos del sistema.

> Dos nodos de servicio son un mínimo para la disponibilidad más que para la capacidad. Ejecute el grupo de espacios de trabajo con autoescalado: los espacios de trabajo se pausan cuando están inactivos, por lo que el grupo debería poder reducirse durante la noche y crecer durante el día.

Recursos del plano de control

El gráfico solicita recursos modestos y permite considerablemente más. **Dimensione sus nodos según los límites, no las solicitudes** — las solicitudes son lo que un servicio necesita en reposo, y los límites son lo que puede usar bajo carga. Un clúster aprovisionado según las solicitudes se programará con éxito y luego se limitará.

COMPONENTE	SOLICITUD	LÍMITE
MongoDB (Percona, en clúster)	500m CPU, 1 GiB de memoria	2 CPU, 4 GiB de memoria
MongoDB (ruta heredada de Bitnami)	1 CPU, 2 GiB de memoria	4 CPU

Dos nodos de servicio `m7i.2xlarge` proporcionan un total de 16 vCPU y 64 GiB, lo que permite alojar los servicios de la plataforma junto con una base de datos en clúster en sus límites, con espacio para el controlador de entrada y los complementos del clúster. Un solo nodo del mismo tamaño se adapta a la misma carga de trabajo para una prueba de concepto, sin la redundancia.

El uso de una base de datos gestionada en lugar de una en clúster libera ese margen de capacidad, lo cual es una de las razones por las que es la recomendación para producción. Las cifras anteriores son los valores predeterminados para una implementación de un solo miembro. Si ejecuta la base de datos interna en producción, ajústela a su propia carga y redundancia en lugar de basarse en esta tabla. Consulte La base de datos de SecurSpaces.

Capacidad del espacio de trabajo

Un espacio de trabajo mantiene su asignación de CPU, memoria y disco solo mientras está en ejecución. Por lo tanto, la capacidad está determinada por cuántos se ejecutan simultáneamente, lo que la detección de inactividad determina en gran medida.

Para estimar el grupo de espacios de trabajo:

1. Tome las especificaciones del espacio de trabajo que ofrece, por ejemplo, 2 vCPU y 8 GiB.
2. Estime la concurrencia máxima. Es inferior a su número de desarrolladores; tenga en cuenta las zonas horarias, las reuniones y los espacios de trabajo que se pausan cuando están inactivos.
3. Multiplique, luego añada aproximadamente un 20 % para la sobrecarga propia del nodo y para la holgura de programación.

Dos ejemplos prácticos, ambos con 2 vCPU y 8 GiB por espacio de trabajo:

IMPLEMENTACIÓN	CONCURRENCIA MÁXIMA	TOTAL	NODOS DE ESPACIO DE TRABAJO
500 desarrolladores	200 espacios de trabajo	400 vCPU, 1.600 GiB	Aproximadamente 28 `m7i.4xlarge`
50 desarrolladores (PoC)	20 espacios de trabajo	40 vCPU, 160 GiB	Aproximadamente 6 `m7i.2xlarge`

Ambos están limitados por la memoria en lugar de por la CPU en esta proporción, lo cual es típico: un espacio de trabajo de 8 GiB en un nodo con 4 GiB de RAM por núcleo agota la memoria antes que la CPU. Si las especificaciones de su espacio de trabajo requieren mucha memoria, dimensione según la memoria y trate el número de núcleos como un subproducto.

Esta es también la razón por la que el grupo de espacios de trabajo se autoescala y el grupo de servicios no. En una prueba de concepto, la diferencia es marcada — fuera del horario laboral, un grupo que se escala a un solo nodo cuesta una sexta parte de uno que no lo hace.

La detección de inactividad es la mayor palanca individual en esta cifra. Una implementación donde los espacios de trabajo nunca se pausan necesita un grupo dimensionado para cada espacio de trabajo existente, en lugar de para los que están en uso. Consulte Detección de inactividad del espacio de trabajo.

Límites de especificación

La plataforma impone estos máximos en una única especificación de espacio de trabajo:

RECURSO	MÁXIMO
CPU	1000 núcleos
Memoria	10.000 GiB
Disco	10.000 GiB
GPU	1000

Estos son límites del producto, no recomendaciones. Lo que realmente puede solicitar está limitado por el hardware de su clúster.

Memoria compartida

Por defecto, un pod de espacio de trabajo obtiene su propia `/dev/shm` del tiempo de ejecución del contenedor, que es pequeña. Las herramientas que dependen de la memoria compartida —ejecutores de pruebas basados en navegador como Chrome o Playwright, y algunas bibliotecas de ciencia de datos y aprendizaje automático— fallan cuando esta se agota, generalmente con un error que no menciona `/dev/shm`.

Para asignar a cada espacio de trabajo un segmento de memoria compartida más grande, establezca el tamaño en sus valores de Helm:

```
workspaceShmVolumeSize: "2Gi"
```

Cada pod de espacio de trabajo monta entonces un `emptyDir` respaldado por memoria en `/dev/shm` con ese límite de tamaño. Deje el valor en blanco, o configúrelo como vacío, y no se montará ningún volumen adicional.

El volumen está respaldado por memoria, por lo que cuenta contra la RAM del nodo en lugar de su disco. Añádalo a la cifra de memoria por espacio de trabajo al dimensionar el grupo de espacios de trabajo.

Base de datos

Dimensionada por separado, porque crece con los datos de auditoría retenidos en lugar de con la concurrencia. Consulte Dimensionamiento de la base de datos.

En resumen: planifique 10–40 GB de datos para 500 desarrolladores y aprovisione al menos 100 GiB de almacenamiento. Para una prueba de concepto de 50 desarrolladores, planifique 1–3 GB y aprovisione al menos 20 GiB. Dimensione MongoDB a su límite de memoria de 4 GiB en ambos casos; el conjunto de trabajo se rige por los patrones de consulta en lugar de por el número de usuarios.

Registro y almacenamiento

COMPONENTE	ORIENTACIÓN
Registro de contenedores	El nivel estándar es suficiente para cualquier tamaño. Habilite la replicación entre regiones para implementaciones multirregionales.

COMPONENTE	ORIENTACIÓN
Almacenamiento del espacio de trabajo	Un volumen persistente por espacio de trabajo, con el tamaño de disco especificado. Este suele ser el mayor consumidor de almacenamiento en la implementación.

VM de 1 clic

La configuración de capacidad de la máquina del instalador establece el número máximo de espacios de trabajo ejecutándose simultáneamente y ajusta la despliegue para la VM. En una VM local, no cambia los recursos de la VM; la VM ya debe tenerlos.

CAPACIDAD	VCPU	MEMORIA	DISCO	ESPACIOS DE TRABAJO EJECUTÁNDOSE A LA VEZ
Pequeño	4	16 GB	200 GB	Hasta 3
Mediano (predeterminado)	8	32 GB	500 GB	Hasta 11
Grande	16	64 GB	1 TB	Hasta 25
Personalizado	Definido por el usuario	Definido por el usuario	1 TB o más	Depende de los recursos

Las imágenes del espacio de trabajo utilizan la mayor parte del disco. En un hipervisor, asigne la memoria como una cantidad fija en lugar de memoria dinámica.

Los perfiles de recursos del espacio de trabajo, como Mínimo, son solicitudes de recursos, no límites. El uso medido puede ser mayor.

Información relacionada

- Requisitos del sistema
- Dimensionamiento de la base de datos
- Asignación de recursos
- Implementación de Kubernetes

REST API

La API REST de Citrix SecurSpaces™ expone los recursos de la plataforma para la automatización: espacios de trabajo, proyectos, organizaciones, recursos, usuarios e informes. Todo lo que la consola hace con un recurso de la plataforma, la API puede hacerlo.

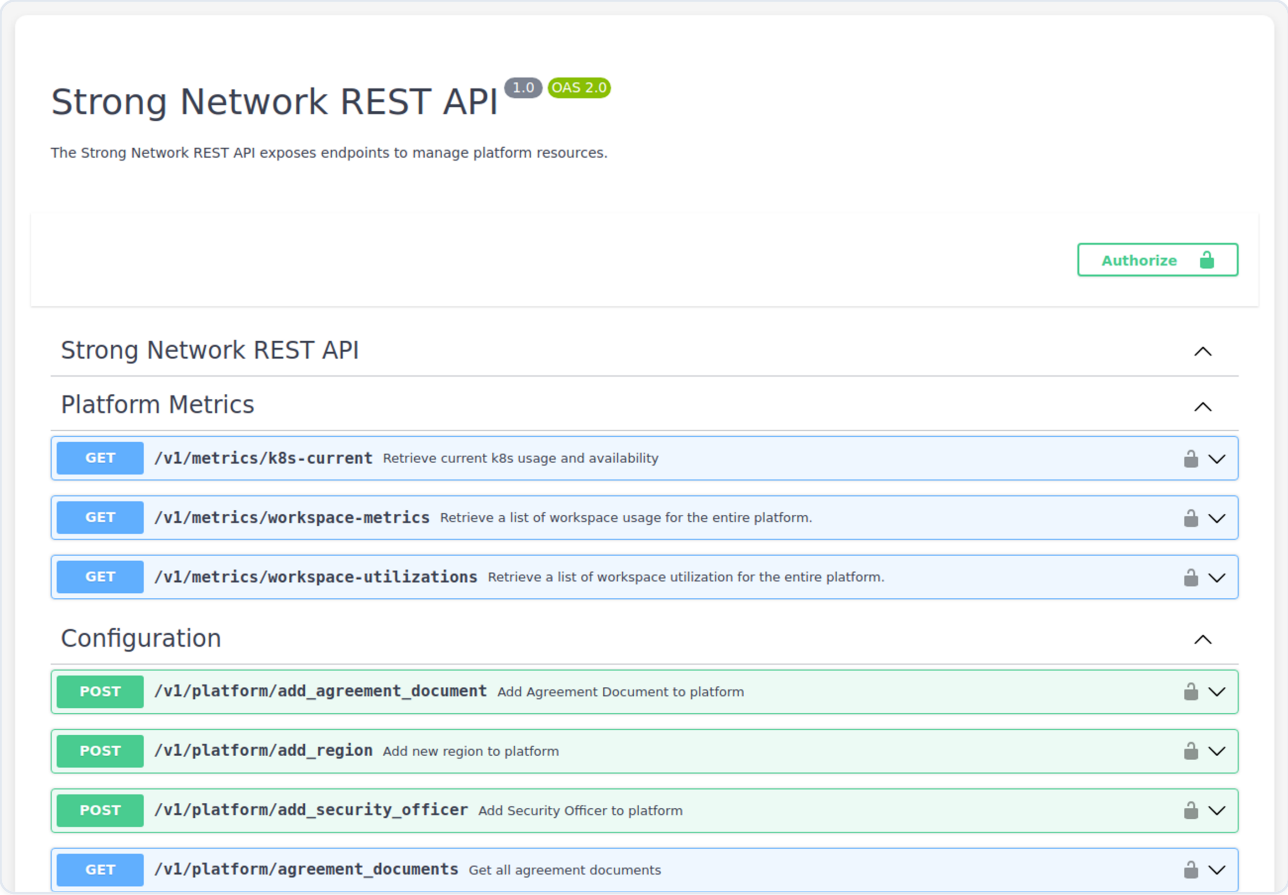
La especificación es proporcionada por su propia implementación, en `https://<your-sds-hostname>/api`. Esa copia es la autorizada, porque coincide con la versión que está ejecutando. Esta página cubre lo que la especificación no le dice: cómo acceder a ella, cómo autenticarse y cómo están organizados los puntos finales.

> **Nota:**
>
> La API REST está controlada por un indicador de función de la plataforma, que un administrador de la plataforma activa. Consulte Activar o desactivar funciones. Solo los usuarios que han iniciado sesión en la plataforma pueden abrir la documentación de la API.

Abrir la documentación de la API

1. Iniciar sesión en SecurSpaces.
2. Seleccione su imagen de perfil en la parte superior derecha de la pantalla para abrir el menú de la cuenta.
3. Seleccione **API REST**.

O navegue directamente a `https://<your-sds-hostname>/api`.



La página es un navegador de especificaciones interactivo. Puede expandir cualquier operación para ver sus parámetros, el cuerpo de la solicitud y el esquema de respuesta, y llamarla directamente desde la página una vez que se haya autorizado.

Autenticarse con una clave de API

La API se autentica con una **clave de API**, enviada en el encabezado `Authorization`:

Esquema	Clave de API
Nombre del parámetro	`Authorization`
Ubicación	Encabezado de solicitud

Cree una clave en **Perfil > Seguridad > Claves de API**. Consulte Seguridad.

Una clave lleva la identidad del usuario que la creó, por lo que una solicitud solo puede hacer lo que ese usuario podría hacer en la consola. Trátela como una contraseña y revóquela desde la misma página si se expone.

Para probar operaciones desde la propia página de documentación, seleccione **Autorizar** y proporcione su clave.

Cómo se organizan los puntos finales

La API refleja la jerarquía de la plataforma. La mayoría de los recursos existen en más de un ámbito, y la ruta le indica a cuál se está dirigiendo:

ÁMBITO	PREFIJO DE RUTA	QUÉ ABORDA
Plataforma	`/v1/platform/...`.	Configuración de todo el despliegue, regiones, acuerdos, usuarios y recursos de la plataforma
Organización	`/v1/organizations/{organizationId}/...`.	Todo lo que pertenece a una organización
Proyecto	`/v1/projects/{projectId}/...`.	Todo lo que pertenece a un proyecto

Así, un cubo de datos, por ejemplo, es accesible a nivel de proyecto, organización y plataforma, con la misma forma en cada uno. Elegir el ámbito suele ser la primera decisión al escribir contra esta API.

Junto a estos, varias familias de recursos se encuentran en el nivel superior:

RUTA	CUBRE
`/v1/workspaces`, `/v1/personal_workspaces`	Espacios de trabajo y los propios espacios de trabajo del llamador
`/v1/workspace-images`	Imágenes de contenedor disponibles para los espacios de trabajo
`/v1/network-policies`	Definiciones de políticas de red
`/v1/data-buckets`	Cubos de datos
`/v1/metrics`	Datos de uso e informes
`/v1/groups`	Grupos

Dentro de la página de documentación, las operaciones se agrupan por área — configuración, usuarios, espacios de trabajo, recursos, métricas y estado — en cada ámbito.

La especificación

Formato	OpenAPI 2.0 (Swagger)
Versión actual	1.1
Tipo de contenido	`application/json`

La versión 1.1 define 207 rutas y 258 operaciones. Estas cifras varían con el producto, así que considere la especificación de su propia implementación como autoritativa en lugar de esta página.

Seleccione **Descargar OpenAPI JSON** en la página de la API para guardar la especificación. Úsela para generar un cliente, para comparar versiones durante una actualización o para ejecutar pruebas de contrato.

La página de la API también enumera lo que cambió en la versión actual, incluidos los cambios de comportamiento que no alteran ninguna ruta o esquema; por ejemplo, una solicitud que antes se aceptaba y se ignoraba silenciosamente ahora se rechaza. Lea esa sección antes de una actualización: un cliente puede dejar de funcionar sin que se haya modificado ningún punto de conexión.

Puntos de conexión utilizados por las extensiones de IDE

Las respuestas de la API de Workspace incluyen los campos `vscode_version_id` y `vscode_version_auto_update`, para que los administradores y las integraciones puedan identificar la versión de VS Code asignada a un espacio de trabajo. Para una descripción de estos campos, consulte Versiones de IDE.

Las extensiones de IDE también pueden usar estos puntos de conexión de espacio de trabajo personal:

- `GET /v1/personal_workspaces/{workspaceId}` devuelve detalles de un espacio de trabajo personal, incluidos los repositorios adjuntos, los puntos de montaje y los depósitos de datos.
- `DELETE /v1/personal_workspaces/{workspaceId}` elimina un espacio de trabajo personal perteneciente al usuario que ha iniciado sesión.

- `GET /v1/personal_workspaces/{workspaceId}/connection_details` devuelve lo que una extensión necesita para abrir una conexión.

`https://<your-sds-hostname>/version.json` es servido por el frontend de la plataforma en lugar de por la API REST. Una extensión puede leerlo para verificar las banderas de capacidad antes de llamar a los puntos de conexión específicos de la versión, sin autenticarse primero.

Administrar versiones de VSCode a través de la API

La API incluye puntos de conexión de versión de VSCode para automatizar los mismos flujos de trabajo de administración de versiones disponibles en la consola. Úselos para estandarizar las versiones de IDE en todos los ámbitos, importar versiones de un registro personalizado y establecer una versión predeterminada como parte de una actualización o una canalización de compilación de entorno.

Las operaciones de versión están disponibles en estas raíces de ámbito:

- Plataforma: `/v1/vscode-versions`
- Organización: `/v1/organizations/{organizationId}/vscode-versions`
- Proyecto: `/v1/projects/{projectId}/vscode-versions`

Cada ámbito admite:

- `GET` para listar versiones.
- `POST` para importar una versión desde un registro por etiqueta de imagen.
- `PATCH /{versionId}/name` para renombrar una versión.
- `DELETE /{versionId}` para eliminar una versión.
- `POST /{versionId}/default` para establecer el valor predeterminado del ámbito.

La gestión de registros personalizados a nivel de plataforma también está disponible a través de `GET /v1/vscode-registries`, `POST /v1/vscode-registries`, `PATCH /v1/vscode-registries/{registryId}/name`, y `DELETE /v1/vscode-registries/{registryId}`.

Los puntos de conexión aplican las mismas comprobaciones de ámbito y permisos que la consola. El nombre de un registro personalizado de VSCode debe ser único dentro de su ámbito, y cada ámbito puede tener un registro personalizado.

Para obtener información sobre cómo se resuelven y utilizan las versiones de IDE en los espacios de trabajo, consulte Versiones de IDE.

Información relacionada

- Seguridad — crear y revocar claves de API
- Licencias — habilitar la API REST
- Roles y permisos — qué puede hacer una clave
- Referencia de SDS CLI

SDS CLI reference

`sds-cli` instala, actualiza y gestiona las implementaciones de Citrix SecurSpaces™. Se ejecuta dentro del Strong Installer contenedor.

Esta página describe los comandos y sus indicadores. Para los procedimientos que los utilizan, consulte Instalar con la CLI de Strong Installer y Actualizar.

> **Nota:**

> Este comando se llamaba anteriormente `strong-cli`. El binario ahora es `sds-cli`. Un enlace simbólico `strong-cli` permanece en el contenedor, por lo que los scripts existentes siguen funcionando, pero use `sds-cli` en el nuevo trabajo.

Ejecutar la CLI

El Strong Installer se publica en Docker Hub. La etiqueta de la imagen coincide con la versión de SecurSpaces que está instalando o a la que está actualizando.

```
docker run -it --rm -v ${PWD}:/strong-network/shared \

    strongnetwork/strong_installer:<version>
```

`${PWD}` se monta en `/strong-network/shared` dentro del contenedor. La CLI escribe archivos de configuración y gráficos de Helm en esa ubicación, para que permanezcan en el host después de que el contenedor salga.

Para ejecutar un comando sin un shell interactivo —por ejemplo, en una canalización—, páselo como argumento:

```
docker run -it --rm -v ${PWD}:/strong-network/shared \

    strongnetwork/strong_installer:<version> \

    <command> [flags]
```

Comandos

COMANDO	PROPÓSITO
`install`	Instalar la plataforma por primera vez.
`upgrade`	Actualizar la plataforma a una nueva versión.
`push-images`	Enviar imágenes de SecurSpaces a un registro.
`create-config`	Crear el archivo de configuración inicial.
`update-config`	Generar un archivo de configuración actualizado a partir de uno existente.
`fetch-access-token`	Obtener un token de acceso de SecurSpaces.
`fetch-helm-chart`	Obtener el gráfico de Helm para una configuración dada.
`helm-upgrade`	Ejecutar `helm upgrade` en una implementación existente.
`get-terraform`	Descargar el proveedor de Terraform de SecurSpaces.
`deploy-demo`	Implementar un entorno de demostración en la nube o en un entorno local.
`stress-test`	Crear espacios de trabajo para pruebas de estrés.

`install` y `upgrade` son los dos comandos utilizados en una implementación normal. Los demás son bloques de construcción que esos dos llaman, y son útiles cuando necesitas ejecutar

una sola etapa por sí misma — por ejemplo, para enviar imágenes desde una máquina que tiene acceso al registro y luego actualizar desde otro lugar.

Grupos de indicadores comunes

La mayoría de los comandos componen los mismos grupos de indicadores. Esta sección describe cada grupo una vez; la entrada de cada comando enumera los grupos que se le aplican.

Archivo de configuración

INDICADOR	DESCRIPCIÓN
`-c`, `--config-file`	Último archivo de configuración implementado, que debe estar en el directorio desde el que inició el contenedor, por ejemplo `config_2026.9.0.yaml`
`--ignore-config`	No leer un archivo de configuración

Cuando utiliza `--ignore-config`, la CLI solicita los valores que de otro modo leería del archivo, como el dominio del host y la URL del registro.

Token de acceso

BANDERA	DESCRIPCIÓN
`-a`, `--access-token`	Token de acceso de SecurSpaces
`--gcp-key-file-path`	Ruta al archivo de clave de cuenta de servicio de SecurSpaces, utilizado para obtener un token
`-d`, `--domain`	Anulación de dominio utilizada al obtener el token

Si no pasa `--access-token`, la CLI obtiene uno utilizando las otras dos banderas o solicita lo que necesita.

Registro de origen

El registro de origen es el registro de Citrix *desde* el que se extraen las imágenes.

BANDERA	DESCRIPCIÓN
`--source-registry-region`	Región desde la que extraer imágenes: `US`, `EU` o `Asia`. No distingue entre mayúsculas y minúsculas.
`--source-registry-url`	URL del registro de origen, anulando la región

Autenticación del registro de destino

El registro de destino es su propio registro, al que se *envían* las imágenes. La CLI detecta el tipo de registro a partir de su URL y solicita las credenciales correspondientes. Utilice estas banderas para proporcionar credenciales de forma no interactiva, por ejemplo, en una canalización que no pueda responder a las solicitudes.

BANDERA	REGISTRO	DESCRIPCIÓN
`--service-account-file-path`	Google	Ruta al archivo de clave de la cuenta de servicio de Google Cloud
`--access-key-id`	AWS	ID de clave de acceso
`--secret-access-key`	AWS	Clave de acceso secreta
`--session-token`	AWS	Token de sesión
`--service-principal-app-id`	Azure	ID de aplicación del principal de servicio
`--service-principal-secret`	Azure	Secreto de cliente del principal de servicio
`--service-principal-tenant-id`	Azure	ID de inquilino del principal de servicio
`--use-docker-login`	Cualquiera	Autenticar con `--registry-username` y `--registry-password` en lugar de usar la autenticación del proveedor de la nube

BANDERA	REGISTRO	DESCRIPCIÓN
`--registry-username`	Cualquiera	Nombre de usuario del registro
`--registry-password`	Cualquiera	Contraseña del registro

Nota:

`--gcp-key-file-path` y `--service-account-file-path` son indicadores diferentes. El primero se autentica contra el registro de origen de Citrix; el segundo se autentica contra su registro de destino.

Selección de imagen

INDICADOR	DESCRIPCIÓN
`-w`, `--workspace-image-tag`	Etiqueta de imagen del espacio de trabajo
`--bitnami-mongo-image-tag`	Etiqueta de imagen de Bitnami MongoDB
`--skip-service-images`	No enviar imágenes de servicio
`--skip-workspace-images`	No enviar imágenes de espacio de trabajo
`--skip-bitnamo-mongodb-image`	No enviar la imagen de Bitnami MongoDB
`--ignore-image`	Imagen a omitir. Repita el indicador para omitir varias imágenes.

Importante:

`--skip-bitnamo-mongodb-image` se escribe como se muestra, con `bitnamo`. Esta es una falta de ortografía conocida en el producto. `--skip-bitnami-mongodb-image` no se reconoce.

Acceso al clúster

Estos indicadores le dicen a la CLI cómo llegar a su clúster cuando ejecuta `kubectl` y `helm`.

INDICADOR	DESCRIPCIÓN
`--ignore-kubectl-setup`	Omitir la configuración de `kubectl` para la autenticación en la nube
`--cluster-name`	Nombre del clúster a usar para la actualización de Helm
`--azure-subscription-id`	ID de suscripción de Azure
`--azure-resource-group`	Grupo de recursos de Azure
`--gcp-project-id`	ID de proyecto de Google Cloud
`--gcp-region`	Región de Google Cloud
`--gcp-zone`	Zona de Google Cloud
`--aws-region`	Región de AWS
`--aws-resource-group`	Grupo de recursos de AWS

Proxy

INDICADOR	DESCRIPCIÓN
`--proxy`	Proxy HTTP o HTTPS
`--proxy-https`	Proxy HTTPS
`--proxy-http`	Proxy HTTP
`--no-proxy`	Hosts que omiten el proxy

Salida y transporte

BANDERA	DESCRIPCIÓN
`--verbose`	Habilitar salida detallada

BANDERA	DESCRIPCIÓN
`--insecure`	Deshabilitar verificación de certificado TLS
`--no-grpc`	Usar REST en lugar de gRPC

instalar

Instala la plataforma por primera vez. El comando solicita los valores de configuración iniciales, para la autenticación del registro y para la URL del registro de destino.

```
sds-cli install [flags]
```

BANDERA	DESCRIPCIÓN	PREDETERMINADO
`-v`, `--version`	Versión de la plataforma a instalar	Valor del archivo `VERSION` en el contenedor

También acepta: archivo de configuración, token de acceso, registro de origen, autenticación del registro de destino, selección de imagen, acceso al clúster, proxy y banderas de salida y transporte.

> **Importante:**

> Después de la autenticación, el archivo del gráfico de Helm se escribe en el directorio compartido. Contiene la configuración de su despliegue y debe protegerse inmediatamente.

actualizar

Prepara un despliegue existente para una nueva versión: descarga el gráfico, actualiza la configuración, imprime el comando de actualización de Helm y sube las imágenes. Aplique el comando de Helm impreso para actualizar el clúster.

```
sds-cli upgrade -c <config-file> [flags]
```

BANDERA	DESCRIPCIÓN	PREDETERMINADO
`-v`, `--version`	Versión de la plataforma a la que actualizar	Valor del archivo `VERSION` en el contenedor

También acepta: archivo de configuración, token de acceso, registro de origen, autenticación del registro de destino, selección de imagen, acceso al clúster y banderas de salida y transporte. `upgrade` no acepta `--insecure`.

Kit de actualización interno de Percona

Para el gráfico con Percona Operator 1.23.0, si `platform.deployPerconaMongoDB` no está configurado o `true`, `upgrade` también copia el kit a `/strong-network/shared/percona-upgrade/`. Contiene `upgrade-percona.sh`, `restore-percona-backup.sh`, `delete-percona-backup.sh`, y los CRD 1.21.2 y 1.22.0. Volver a ejecutar `upgrade` reemplaza el kit para que coincida con la versión del instalador.

Esto no añade ninguna solicitud de CLI. La salida le indica que ejecute `upgrade-percona.sh` antes de Helm y proporciona los comandos de restauración y eliminación. El script en sí solicita confirmación. Actualiza Percona una versión menor a la vez a 1.22.0 y aplica los CRD 1.23; Helm completa el paso a 1.23.0. Las implementaciones externas de MongoDB omiten este comportamiento. Consulte Actualización para ver el procedimiento completo.

Actualización sin un archivo de configuración

Si el archivo de configuración de la implementación anterior no está disponible, pase `--ignore-config`. La CLI entonces solicita cada valor que habría leído del archivo, incluyendo el dominio del host y la URL del registro, y no escribe un nuevo archivo de configuración.

> **Advertencia:**
>
> Sin un archivo de configuración, debe proporcionar cada parámetro de implementación manualmente. Utilice esta opción solo cuando el archivo de configuración no se pueda recuperar.

push-images

Envía imágenes de SecurSpaces a su registro sin instalar ni actualizar.

```
sds-cli push-images [flags]
```

Acepta: archivo de configuración, token de acceso, registro de origen, autenticación de registro de destino, selección de imagen y banderas de salida y transporte.

> **Sugerencia:**
>
> `--use-docker-login` con `--registry-username` y `--registry-password` suprime completamente las solicitudes de autenticación, que es lo que necesita una canalización no interactiva.

create-config

Crea el archivo de configuración inicial.

```
sds-cli create-config [flags]
```

Acepta: token de acceso, registro de origen, proxy y banderas de salida y transporte.

update-config

Genera un archivo de configuración actualizado a partir de uno existente.

```
sds-cli update-config -c <config-file> [flags]
```

BANDERA	DESCRIPCIÓN
`-v`, `--version`	Etiqueta de versión de la plataforma para escribir en el nuevo archivo de configuración

También acepta: archivo de configuración, token de acceso, registro de origen y banderas de salida y transporte.

fetch-access-token

Obtiene un token de acceso de SecurSpaces y lo imprime.

```
sds-cli fetch-access-token [flags]
```

Acepta: archivo de configuración, token de acceso y banderas de salida y transporte.

fetch-helm-chart

Obtiene el gráfico Helm de SecurSpaces para la configuración que proporcione.

```
sds-cli fetch-helm-chart -c <config-file> [flags]
```

Acepta: archivo de configuración, token de acceso, registro de origen y banderas de salida y transporte.

helm-upgrade

Ejecuta `helm upgrade` contra una implementación existente, utilizando un gráfico Helm que ya haya obtenido.

Para una implementación interna existente de Percona que se mueva al gráfico 1.23, primero complete el paso de preparación de Percona. El gráfico bloquea la actualización hasta que la base de datos haya alcanzado la versión 1.22 y se apliquen los CRD 1.23 requeridos; se permiten las actualizaciones posteriores de una implementación que ya esté en la versión 1.23.

```
sds-cli helm-upgrade -c <config-file> --helm-chart-file-name <chart>
[flags]
```

BANDERA	DESCRIPCIÓN
`-c`, `--config-file`	Último archivo de configuración desplegado
`--helm-chart-file-name`	Archivo de gráfico Helm a usar para la actualización
`--verbose`	Habilitar salida detallada

También acepta los indicadores de acceso al clúster.

get-terraform

Descarga el **proveedor de Terraform de SecurSpaces** en el directorio compartido. A pesar del nombre del comando, esto no descarga el binario de Terraform en sí — instale Terraform por separado.

Para saber qué gestiona el proveedor y cómo configurarlo, consulte proveedor de Terraform.

```
sds-cli get-terraform [flags]
```

INDICADOR	DESCRIPCIÓN	PREDETERMINADO
`-c`, `--config-file-name`	Último archivo de configuración desplegado	
`-v`, `--version`	Versión del proveedor a obtener	Última versión
`-d`, `--domain`	Dominio del host	
`--src-reg-key-file`	Ruta al archivo de clave de cuenta de servicio de SecurSpaces	

También acepta los indicadores de salida y transporte.

Nota:

Este comando usa `--config-file-name`, no el `--config-file` usado por los otros comandos. La `-c` abreviatura es la misma.

deploy-demo

Despliega un entorno de demostración. Úselo para evaluación, no para producción.

```
sds-cli deploy-demo [flags]
```

INDICADOR	DESCRIPCIÓN	PREDETERMINADO
`--deployment-location`	Dónde desplegar: `cloud` o `local`	`cloud`
`--helm-chart-version-tag`	Versión del archivo del gráfico Helm para descargar	
`--helm-chart-registry`	Registro desde el que extraer el gráfico Helm	
`--skip-version-check`	No comprobar que la etiqueta de versión existe en el registro	`false`
`-v`, `--version`	Etiqueta de versión de la plataforma	

También acepta: archivo de configuración, token de acceso, registro de origen, proxy y banderas de salida y transporte.

stress-test

Crea espacios de trabajo para probar la carga de una implementación. Esta es una herramienta de prueba, no forma parte de la instalación u operación de una implementación de producción.

```
sds-cli stress-test --domain <domain> --test-name <name> --workspaces <n>
[flags]
```

`--domain` y `--test-name` son obligatorios para el comando y todos sus subcomandos. `--workspaces` es obligatorio para `stress-test` en sí.

INDICADOR	DESCRIPCIÓN	PREDETERMINADO
`--domain`	Dominio del host. Obligatorio.	
`--api-key`	Clave de API de la plataforma. También se puede establecer con la variable de entorno `STRONG_API_KEY`.	

INDICADOR	DESCRIPCIÓN	PREDETERMINADO
`--test-name`	Nombre base que identifica la prueba, la organización, el proyecto y los espacios de trabajo. Obligatorio.	`stress-test`
`--concurrency`	Número máximo de solicitudes de espacio de trabajo concurrentes	
`--delay`	Segundos entre solicitudes de creación secuenciales cuando `--concurrency` es 1	`0`
`--heartbeat-interval`	Envía un latido cada N segundos desde dentro del espacio de trabajo después del inicio. `0` lo deshabilita.	`0`
`--workspaces`	Número de espacios de trabajo a crear. Obligatorio.	`0`
`--image-name`	Imagen del espacio de trabajo a usar	
`--region`	Región en la que crear espacios de trabajo	Región predeterminada
`--per-region`	Crear espacios de trabajo en todas las regiones disponibles	`false`
`--no-cleanup`	No limpiar los recursos cuando la prueba finaliza o se interrumpe	`false`
`--memory`	Memoria en MB para cada espacio de trabajo	
`--vcpu`	vCPU en MHz para cada espacio de trabajo	

INDICADOR	DESCRIPCIÓN	PREDETERMINADO
`--disk`	Tamaño de disco en GB para cada espacio de trabajo	
`--gpu`	Número de GPU para cada espacio de trabajo	
`--state-on-create`	Estado inicial del espacio de trabajo: `CREATE_AS_RUNNING` o `CREATE_AS_PAUSED`	
`--users`	Número de usuarios para crear y asignar espacios de trabajo	`0`
`--user-email-prefix`	Prefijo de correo electrónico para usuarios de prueba de estrés	Valor de `--test-name`
`--user-role`	Rol de proyecto asignado a los usuarios creados	`developer`

Subcomandos de prueba de estrés

SUBCOMANDO	PROPÓSITO
`cleanup`	Limpiar los recursos creados por una prueba de estrés
`create-users`	Crear usuarios y añadirlos a un nuevo proyecto de prueba de estrés, sin crear espacios de trabajo
`delete-users`	Eliminar usuarios de prueba de estrés persistentes, sin eliminar espacios de trabajo, proyecto u organización
`pause`	Pausar todos los espacios de trabajo en un proyecto

SUBCOMANDO	PROPÓSITO
`resume`	Reanudar todos los espacios de trabajo en un proyecto
`pause-resume`	Pausar y luego reanudar todos los espacios de trabajo en un proyecto

Información relacionada

- Instalar con la CLI de Strong Installer
- Actualizar
- Requisitos

Supported IDEs

Qué editores funcionan con Citrix SecurSpaces™, y cómo se conecta cada uno.

IDE en la nube

VS Code para Web es el único IDE en la nube que la plataforma ofrece. Se ejecuta en una pestaña del navegador y no requiere nada instalado localmente.

Si su equipo necesita un IDE diferente basado en navegador, se puede integrar en una imagen de espacio de trabajo personalizada. Consulte Requisitos de la imagen del contenedor.

IDEs locales a través de SSH

IDE	MÉTODO DE CONEXIÓN
VS Code de escritorio	Extensión de SecurSpaces, un clic desde la consola
Cursor	Extensión de SecurSpaces, un clic desde la consola
Windsurf	Extensión de SecurSpaces, un clic desde la consola
Kiro	Extensión de SecurSpaces, un clic desde la consola

IDE	MÉTODO DE CONEXIÓN
JetBrains Gateway	Configuración de SSH a través de la interfaz de Gateway
Otros editores compatibles con SSH	Par de claves SSH manual

Para el procedimiento de conexión, consulte Conectarse a través de SSH.

Para saber dónde residen el código fuente, las credenciales y los datos de la extensión cuando se utiliza un IDE local, consulte Trabajar desde un IDE local.

Extensiones

Hay una extensión para instalar. **Citrix Secure Developer Spaces - Remote SSH** se publica en el VS Code Marketplace y en Open VSX. Su propia documentación se refiere a ella como **Citrix SDS - Remote SSH**.

Tiene dos partes, y no es necesario instalar ni gestionar la segunda.

PARTE	SE EJECUTA EN	PROPORCIONA
La extensión que instala	Su máquina local	La barra lateral, el inicio de sesión, la lista de espacios de trabajo, las conexiones SSH y la barra de estado. Su token de acceso permanece en su máquina y nunca se coloca en el espacio de trabajo.
Un componente complementario, empaquetado en su interior	Dentro del espacio de trabajo	Informa de la actividad, de modo que un espacio de trabajo que esté utilizando activamente no se pausa por detección de inactividad y responde a las mediciones de calidad de la red.

El componente complementario se instala automáticamente en el espacio de trabajo cuando se conecta.

Barra lateral de extensiones

La barra lateral se titula **Secure Developer Spaces**. Los espacios de trabajo se agrupan por proyecto, y cada proyecto tiene un botón de añadir. Una sección de **Enlaces rápidos** en la parte inferior proporciona **Abrir consola SDS**, **Editar configuración del perfil**, y **Solucionar problemas de conexión**.

Estados del espacio de trabajo

ESTADO	SIGNIFICADO
En ejecución	El espacio de trabajo está en ejecución, pero su IDE no está conectado a él
Conectado	Su IDE está conectado a este espacio de trabajo. La fila está resaltada.
Pausado	El espacio de trabajo está pausado

Controles de fila del espacio de trabajo

CONTROL	DISPONIBLE CUANDO
Conectar	El espacio de trabajo está en ejecución y no conectado
Iniciar (icono de reproducción)	El espacio de trabajo está en pausa
Pausar (icono de pausa)	El espacio de trabajo está en ejecución o conectado

Menú contextual del espacio de trabajo

Haz clic con el botón derecho en una fila del espacio de trabajo.

ACCIÓN	DISPONIBLE CUANDO	NOTAS
Conectar en la ventana actual	El espacio de trabajo está en ejecución y no conectado	
Conectar en una nueva ventana	El espacio de trabajo está en ejecución y no conectado	

ACCIÓN	DISPONIBLE CUANDO	NOTAS
Editar espacio de trabajo	Siempre	Abre la configuración del espacio de trabajo en la consola de SecurSpaces, en su navegador
Eliminar espacio de trabajo	Siempre	Elimina permanentemente el espacio de trabajo y sus datos

La conexión requiere que SSH esté habilitado en el espacio de trabajo. Consulte Conectar a través de SSH.

Contenido del espacio de trabajo

Expanda un espacio de trabajo para ver lo que contiene: sus aplicaciones de espacio de trabajo, sus repositorios clonados y sus puntos de montaje. Los puntos de montaje en los que no puede escribir están etiquetados como de solo lectura.

Información relacionada

- Conectar a través de SSH
- Desarrollar en un espacio de trabajo
- Publicar JetBrains Gateway como aplicación de Citrix DaaS(/es-es/securspaces/administer/integrations/publish-jetbrains-gateway.html)

System requirements

Lo que una implementación de Citrix SecurSpaces™ necesita de su infraestructura. Para saber cuánto, consulte Dimensionamiento.

Para las direcciones externas a las que debe llegar la implementación, consulte Destinos de red.

Cada requisito a continuación está marcado con lo que sucede si no lo tiene:

NIVEL	SIGNIFICADO
Obligatorio	La implementación no se completa sin él.

NIVEL	SIGNIFICADO
Recomendado	La implementación se completa. Planifique esto antes de que el entorno realice un trabajo real.
Predeterminado	SecurSpaces ya lo proporciona. No se necesita ninguna acción para empezar.
Condicional	Necesario solo en las circunstancias mencionadas.

Antes del día de la implementación

Todo lo marcado como Obligatorio, en el orden en que lo necesitará:

- Un modelo de despliegue elegido y una cuenta con permisos para aprovisionarlo
- Un clúster de Kubernetes dedicado, `amd64`, no compartido con otras cargas de trabajo
- Un controlador de entrada (ingress controller) y un clúster que aplica la API de Network Policy
- Dos dominios DNS, el segundo un subdominio comodín del primero
- Almacenamiento persistente a través de la API de Persistent Volume Claim
- La CLI de Helm, disponible para quien ejecute el despliegue
- Acceso saliente al servidor de licencias, Docker Hub y Google Artifact Registry

Si el entorno está aislado (air-gapped) o tiene salida restringida, confirme primero este último elemento. Es el que con mayor frecuencia detiene un despliegue el día de la operación, y la solución —cambios en el firewall o una licencia sin conexión— es la que más tiempo tarda en gestionarse. Consulte Destinos de red.

> **Nota:**
>
> Los espacios de trabajo son contenedores Linux. No se admite el desarrollo que requiera macOS o hardware de Apple, como aplicaciones de iOS o macOS aplicaciones.

Kubernetes

REQUISITO	VALOR	NIVEL
Versión de Kubernetes	1.34 o posterior	Obligatorio
Clúster	Dedicado a SecurSpaces. No lo comparta con otras aplicaciones.	Obligatorio
Arquitectura de nodo	`amd64`. `arm64` no es compatible.	Obligatorio
Sistema operativo de nodo en AWS	Amazon Linux	Obligatorio
Tamaño del clúster	Un solo nodo es suficiente para empezar. La alta disponibilidad y los nodos múltiples no son necesarios para una prueba de concepto.	Predeterminado

Nota:

Ejecute una versión de Kubernetes que aún sea compatible con el upstream en lugar de fijarse en este mínimo. Una versión que ha dejado de ser compatible deja de recibir correcciones de seguridad, y la ventana de soporte se mueve con cada ciclo de lanzamiento de Kubernetes ciclo de lanzamiento.

Plataformas compatibles

Elija una implementación de Kubernetes nativa de la nube, local o aislada, y asegúrese de que su cuenta tenga los permisos de infraestructura que ese entorno necesita.

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift

- VMware Tanzu Kubernetes Grid (TKG)
- Nutanix Kubernetes Platform (NKP)

Redes

REQUISITO	DETALLE	NIVEL
Pasarela de entrada	Se recomienda NetScaler CPX, y el gráfico de SecurSpaces puede implementarlo por usted. NGINX, HAProxy y la API de Kubernetes Gateway también son compatibles. Consulte Ingress.	Obligatorio
API de política de red	`networking.k8s.io/v1`. Si su clúster no la implementa, instale Calico o Cilium.	Obligatorio
Dominios DNS	Dos dominios DNS, el segundo un subdominio comodín del primero	Obligatorio
Certificados TLS	Certificados válidos para ambos dominios	Recomendado

> **Importante:**
>
> La API de política de red no es opcional si depende de las políticas de red o del aislamiento del espacio de trabajo. Sin un complemento de red que la aplique, esas políticas son aceptadas por el servidor de API y no hacen nada. Consulte Límites de confianza.

Dominios

El segundo dominio debe ser un subdominio comodín del primero. Por ejemplo:

- `example.com`
- `*.proxy.example.com`

Los certificados son opcionales para las implementaciones de prueba de concepto, pero muy recomendables.

Almacenamiento

Proporcione almacenamiento persistente a través de la API de Kubernetes Persistent Volume Claim. Esto es **obligatorio**: confirme que el clúster de destino es compatible con la API de PVC antes de la implementación.

Herramientas de implementación

HERRAMIENTA	PROPÓSITO	NIVEL
Helm CLI	Implementa SecurSpaces desde el gráfico de Helm proporcionado. Debe estar instalado y accesible para quien ejecute la implementación.	Obligatorio
cert-manager	Necesario solo si el gráfico renderiza recursos de cert-manager `Certificate`. Si su clúster no usa cert-manager, establezca `platform.useCertManager: false`.	Condicional

Lo que SecurSpaces proporciona por defecto

No es necesario organizar ninguna de estas opciones antes de una prueba de concepto. SecurSpaces se implementa con ambas ya funcionando, y cada una tiene una ruta de producción a la que puede pasar más tarde.

ÁREA	PREDETERMINADO	RUTA DE PRODUCCIÓN
Base de datos	Percona Server para MongoDB, implementado por el gráfico y ejecutándose en su clúster	Un servicio externo de MongoDB, como MongoDB Atlas. Consulte Base de datos.

ÁREA	PREDETERMINADO	RUTA DE PRODUCCIÓN
Identidad y acceso	Autenticación por correo electrónico y contraseña	Un proveedor de identidad que utilice SAML u OIDC, como Okta. Consulte Identidad.

La base de datos interna es compatible en producción, incluso para implementaciones aisladas y locales. Lo que cambia es la propiedad: las copias de seguridad, la alta disponibilidad y el escalado pasan a ser responsabilidad suya. Un servicio externo traslada ese trabajo al proveedor. Consulte Base de datos para la comparación.

VM de 1 clic

La VM de 1 clic ejecuta toda la plataforma en una única máquina virtual para evaluación. Tiene sus propios requisitos, que reemplazan los requisitos de Kubernetes en esta página. Para saber cuánta capacidad necesita, consulte Dimensionamiento.

Host de destino

REQUISITO	VALOR	NIVEL
Sistema operativo	Ubuntu 22.04 Desktop o Ubuntu 24.04 Desktop	Obligatorio
CPU	x86_64 con el conjunto de instrucciones AVX, expuesto al invitado. Los procesadores Intel Celeron no lo admiten.	Obligatorio
Software	Una instalación limpia, sin Docker, Kubernetes, K3s ni software de contenedor relacionado	Obligatorio
Red	Acceso a internet saliente y una dirección IP a la que puedan acceder los dispositivos cliente. Una dirección privada es válida.	Obligatorio

REQUISITO	VALOR	NIVEL
Acceso	Una cuenta de usuario con permisos `sudo` completos	Obligatorio
Hipervisor	XenServer, Hyper-V, otro hipervisor o metal desnudo. Las VM en la nube son creadas por el instalador.	Predeterminado

Estos sistemas operativos no son compatibles con el host de destino: Ubuntu Server, imágenes mínimas y en la nube de Ubuntu, Debian y otras distribuciones basadas en Debian, Red Hat Enterprise Linux, CentOS, Rocky Linux y otras distribuciones basadas en RPM.

Host del instalador

REQUISITO	VALOR	NIVEL
Máquina	Separado del host de destino	Obligatorio
Docker	Instalado y en ejecución, capaz de extraer de Docker Hub. En Windows, Docker Desktop con contenedores Linux.	Obligatorio
Red	Acceso HTTPS saliente a Docker Hub y a los registros de imágenes de SecurSpaces	Obligatorio
Disco	20 GB libres	Obligatorio

Qué contiene la VM de 1 clic

COMPONENTE	DETALLE
Clúster	K3s de nodo único
Entrada	NetScaler CPX (`netscaler-cpx-ingress`)
Plataforma	Servicios y base de datos de SecurSpaces

COMPONENTE	DETALLE
URL	Un nombre de host HTTPS bajo `try.sds.citrix.com`
Licencia	Una licencia de evaluación, válida por 6 meses
Certificado TLS	Válido por 90 días
Datos de ejemplo	La **Organización Fast Cars**, con usuarios de ejemplo y un espacio de trabajo de ejemplo

Límites

- No compatible con cargas de trabajo de producción, clústeres multinodo o pruebas de escalabilidad.
- No se puede actualizar ni migrar a una instalación de producción.
- La licencia de evaluación caduca después de 6 meses, y el certificado TLS después de 90 días.
- Implementaciones locales: la asociación DNS debe completarse en el plazo de 1 hora desde la generación del script de implementación.

Información relacionada

- Destinos de red
- Puertos y protocolos
- Instalar con la CLI de Strong Installer
- Licencia
- Dimensionamiento
- Dimensionamiento de la base de datos

Release notes

PÁGINA	¿QUÉ CUBRE?
Novedades	Funciones y cambios por versión
Problemas resueltos	Defectos resueltos por versión y categoría, incluidas las correcciones de seguridad
Novedades en SecurSpaces Flex	Cambios en la oferta gestionada
Historial del documento	Cambios en esta documentación

> **Nota:**
>
> Las correcciones de seguridad se enumeran en Problemas resueltos bajo la categoría **Seguridad**. Si las rastrea para su revisión, esa página es el registro.

What's new

Las actualizaciones mejoran continuamente su experiencia con Citrix SecurSpaces™. Cada versión introduce nuevas funciones, mejoras y correcciones para garantizar que siempre tenga acceso a las últimas innovaciones y mejoras de rendimiento. Este artículo destaca las capacidades nuevas y actualizadas disponibles en esta versión, así como los problemas resueltos.

Para obtener detalles sobre compatibilidad y rendimiento, consulte Requisitos técnicos.

SecurSpaces 2026.9

Copias de seguridad sin clave de Google Cloud Storage para Percona MongoDB interno

Las implementaciones internas de Percona MongoDB ahora utilizan Percona Operator para MongoDB 1.23.0. Esta versión añade soporte nativo para copias de seguridad de Google Cloud Storage con Workload Identity Federation para Google Kubernetes Engine, de modo que los

equipos de plataforma puedan almacenar copias de seguridad en Google Cloud Storage sin claves de cuenta de servicio estáticas ni credenciales HMAC credenciales.

El instalador incluye un kit de actualización de Percona para implementaciones que comenzaron en SecurSpaces 2026.9. Ejecute `sds-cli upgrade` primero, luego ejecute el script `percona-upgrade/upgrade-percona.sh` suministrado antes de aplicar el comando Helm impreso por el instalador. El script realiza una copia de seguridad de la base de datos, actualiza a través de las versiones intermedias de Percona requeridas, aplica las definiciones de recursos personalizados necesarias y prepara la implementación para la actualización final de Helm al operador 1.23.0.

Las capacidades clave incluyen:

- Actualice Percona MongoDB interno del operador 1.20.1 a 1.23.0 con un script proporcionado por el instalador.
- Configure el almacenamiento de copias de seguridad, los programas, la retención y la recuperación a un momento dado en los valores de Helm.
- Seleccione la cuenta de servicio de Kubernetes de la base de datos utilizada por los agentes de Percona Backup para MongoDB.
- Utilice copias de seguridad sin clave de Google Cloud Storage en Google Kubernetes Engine con Workload Identity.
- Restaure desde la copia de seguridad de la actualización o desde los recursos de copia de seguridad de Percona Backup para MongoDB.

Para obtener más información, consulte Copia de seguridad de la base de datos y Actualizar.

Tamaños de espacio de trabajo gestionados para SecurSpaces Flex

SecurSpaces Flex ahora utiliza un catálogo de tamaños de espacio de trabajo gestionado por Citrix. Citrix publica los niveles de tamaño disponibles y sus versiones a través de la plataforma, y las implementaciones de Flex concilian ese catálogo durante las actualizaciones. Esto mantiene el tamaño del espacio de trabajo alineado con el catálogo de servicios, al tiempo que preserva la configuración de disponibilidad para cada nivel.

Los administradores aún pueden decidir qué organizaciones y proyectos pueden usar cada nivel. La definición de recursos del nivel es gestionada por Citrix, por lo que los desarrolladores eligen entre tamaños aprobados en lugar de editar los valores subyacentes de CPU, memoria, almacenamiento y clase de almacenamiento.

Las capacidades clave incluyen:

- Ver los niveles de tamaño de espacio de trabajo gestionados con el estado de versión y ciclo de vida.
- Mantener la configuración de disponibilidad cuando Citrix publique una versión de nivel más reciente.
- Solicitar a los espacios de trabajo afectados que se actualicen cuando su versión de nivel ya no esté actualizada.
- Previsualizar y aplicar actualizaciones masivas que mueven los espacios de trabajo a la versión actual del mismo nivel.
- Evitar que los nuevos espacios de trabajo utilicen versiones de nivel retiradas mientras los espacios de trabajo existentes permanecen visibles.
- Mantener el mismo identificador de versión de nivel gestionado en todos los inquilinos de Flex cuando Citrix fije el identificador.
- Auditar los cambios exitosos de disponibilidad de nivel y las actualizaciones masivas de versión de nivel con el usuario, la hora y el resultado.

Para obtener más información, consulte Plantillas de espacio de trabajo de SecurSpaces Flex.

Registro de auditoría para cambios de nivel de Flex gestionados

SecurSpaces Flex ahora registra los cambios exitosos de disponibilidad de nivel gestionado y las actualizaciones masivas de versión de nivel en el registro de auditoría. Esto proporciona a los administradores un registro más claro de quién cambió un nivel de tamaño de espacio de trabajo gestionado, cuándo ocurrió la acción y qué cambió.

Utilice el registro de auditoría para revisar cuándo se habilitó o deshabilitó un nivel, o cuándo una actualización masiva movió espacios de trabajo a la versión actual de un nivel gestionado. Los intentos rechazados de modificar las definiciones de nivel gestionadas por Citrix continúan registrándose.

Para obtener más información, consulte Catálogo de eventos de auditoría.

Soporte de la API REST para la gestión de versiones de IDE

La API REST ahora incluye la gestión de versiones de IDE. Los equipos de plataforma pueden automatizar las operaciones de versión de VSCode que anteriormente requerían la consola, lo que ayuda a mantener los entornos de SecurSpaces reproducibles en todos los proyectos y pipelines de despliegue.

La API puede listar, importar, renombrar, eliminar y establecer la versión predeterminada de VSCode a nivel de plataforma, organización y ámbito de proyecto. Los administradores de plataforma también pueden listar, añadir, renombrar y eliminar registros personalizados de VSCode a nivel de plataforma.

Utilice estos puntos finales cuando desee estandarizar las versiones de IDE en muchos ámbitos, importar una etiqueta de imagen probada desde un registro personalizado, o establecer una versión como predeterminada como parte de un flujo de trabajo de actualización.

Para obtener más información, consulte API REST. Para conceptos de versiones de IDE, consulte Versiones de IDE.

Actualizaciones más seguras de Percona MongoDB

Las actualizaciones de Helm con el despliegue interno de Percona MongoDB ahora reutilizan las contraseñas de base de datos existentes por defecto. Anteriormente, una renderización con valores de contraseña vacíos podía generar nuevas credenciales, lo que provocaba que MongoDB y los servicios de la plataforma no coincidieran en la contraseña activa durante una actualización.

En las actualizaciones de Helm del lado del servidor, SecurSpaces reutiliza la contraseña ya almacenada en el `<release>-psmdb-secrets` Secret activo a menos que establezca explícitamente un nuevo valor. Cuando la credencial del administrador de la base de datos cambia, los servicios de la plataforma que la consumen ahora se reinician para que lean el Secret actualizado.

La renderización del lado del cliente todavía no puede leer el Secret activo, por lo que `helm template`, la renderización GitOps del lado del cliente, y `--dry-run=client` aún pueden producir nuevos valores generados. Utilice las actualizaciones de Helm del lado del servidor para el despliegue interno de Percona, o fije las contraseñas de la base de datos en su archivo de valores.

Para obtener más información, consulte La base de datos de SecurSpaces.

Soporte de entrada de Istio

Los clústeres que ya utilizan Istio como punto de entrada ahora pueden exponer SecurSpaces a través de una puerta de enlace de entrada de Istio. Establezca `platform.useIstio` y el gráfico renderizará recursos de Istio Gateway, VirtualService y DestinationRule en lugar de recursos de Kubernetes Ingress.

La puerta de enlace de entrada de Istio termina el TLS público y luego abre una segunda conexión TLS a los servicios de SecurSpaces, de modo que el tráfico permanece cifrado a través del clúster.

Al igual que con NGINX, el gráfico no crea una entrada SSH cuando Istio está habilitado.

Para obtener más información, consulte Istio.

Informes más claros cuando un espacio de trabajo se queda sin memoria

Un espacio de trabajo detenido por exceder su límite de memoria ahora informa `OOMKilled` en los detalles de su fallo, con orientación sobre la memoria que necesitaba. Anteriormente, el mismo fallo mostraba `Reason: Unknown` y sugería actualizar la imagen del espacio de trabajo, lo que dirigía a los usuarios al lugar equivocado.

El cuadro de diálogo de error del espacio de trabajo ahora señala la tarea que consumió la memoria, o la posibilidad de pasar a una especificación con un límite superior, en lugar de la imagen. Los fallos de extracción de imágenes mantienen su orientación existente.

Para obtener más información, consulte Solución de problemas.

Nombre del producto actualizado a Citrix SecurSpaces

Citrix SecurSpaces es el nuevo nombre de producto para Citrix Secure Developer Spaces. El nombre actualizado aparece ahora en toda la interfaz del producto, el título del navegador, los metadatos del paquete, las plantillas de correo electrónico y la documentación de la API generada.

Este cambio ayuda a alinear la experiencia del producto con la nomenclatura actual de Citrix, al tiempo que preserva los flujos de trabajo y las rutas de implementación existentes.

Las URL de la documentación se han movido de `/es-es/secure-developer-spaces/` a `/es-es/securspaces/`. Cada dirección anterior redirige a la página correspondiente, por lo que los enlaces y marcadores existentes siguen funcionando, pero la nueva forma es la que se debe usar en adelante.

Para obtener más información, consulte Descripción general.

Configuración de estado deseado para plantillas de espacio de trabajo

Las plantillas de espacio de trabajo ahora mantienen una relación activa con los espacios de trabajo creados a partir de ellas. Cada espacio de trabajo registra la versión de la plantilla a partir de la cual se creó, de modo que los propietarios del proyecto pueden ver qué espacios de trabajo se han desviado del estándar actual y actualizarlos.

Anteriormente, una plantilla se aplicaba una sola vez en el momento de la creación y el espacio de trabajo no mantenía ninguna conexión con ella. Los propietarios del proyecto no tenían forma de saber qué espacios de trabajo seguían alineados con la configuración actual, y cualquier cambio en un repositorio, secreto, extensión o política tenía que coordinarse manualmente con cada desarrollador.

Las capacidades clave incluyen:

- Vea cuántos espacios de trabajo están en prueba, desactualizados o sin versión directamente en la página Plantillas.
- Abra la ventana Espacios de trabajo asociados para revisar los espacios de trabajo agrupados por versión de plantilla y exporte la lista a CSV.
- Establezca una versión de plantilla predeterminada para señalar la configuración deseada para un proyecto.
- Permitir a los propietarios del espacio de trabajo aplicar la actualización desde una ventana de actualización que previsualiza los cambios de configuración, sin perder sus datos persistentes.
- Requerir que un espacio de trabajo obsoleto se actualice antes de que su configuración pueda ser editada.
- Evitar la eliminación de una plantilla o versión de plantilla mientras los espacios de trabajo aún la utilicen.

Para obtener más información, consulte Plantillas.

Observabilidad de IA para el uso de IA por parte de los desarrolladores

El tráfico de IA que SecurSpaces enruta a través de un AI Gateway ahora se etiqueta con el usuario, el proyecto y el espacio de trabajo que lo produjo. Los equipos de plataforma pueden informar sobre el volumen de solicitudes de IA, el uso del modelo y el consumo de tokens en toda la organización, y atribuir ese uso a los equipos y desarrolladores responsables de ello.

La adopción empresarial del desarrollo asistido por IA ha dificultado la contabilidad del gasto en tokens. Los paneles de control de los proveedores son específicos de un único proveedor y no pueden mostrar el uso en todas las herramientas y modelos que una organización de desarrollo utiliza realmente. Esta versión ofrece a los clientes una vista única e independiente del proveedor.

Las capacidades clave incluyen:

- Añadir metadatos de usuario, proyecto y espacio de trabajo a las solicitudes de IA reenviadas al AI Gateway.

- Informar sobre el uso de IA independientemente del proveedor de LLM que atiende cada solicitud.
- Desglosar el consumo de tokens y el volumen de solicitudes por proyecto, por usuario y por modelo para respaldar la refacturación.
- Comprobar el estado del AI Gateway y elegir si el tráfico de IA lo omite o falla cuando no está disponible.
- Importar un panel de control de Grafana de ejemplo que cubra los totales de tokens, las tasas de uso, los tiempos de respuesta y las vistas por proyecto, por usuario y por modelo.

SecurSpaces documenta una pila de referencia validada de Envoy AI Gateway, Prometheus y Grafana. Dado que el gateway exporta métricas estándar, también puede enviar estos datos a su infraestructura de monitoreo existente.

Para obtener más información, consulte Configurar el enrutamiento de AI Gateway.

Archivos dot para la personalización del espacio de trabajo

Los desarrolladores ahora pueden conectar un repositorio personal de archivos dot desde **Perfil > Configuración > Archivos dot**. SecurSpaces clona el repositorio en cada espacio de trabajo seleccionado y ejecuta un script de instalación compatible para que las preferencias de shell, editor y herramientas se puedan aplicar automáticamente.

Los archivos dot se configuran por usuario y utilizan la integración de Git conectada de ese usuario. Los desarrolladores pueden aplicar la configuración a todos los espacios de trabajo o solo a los seleccionados, elegir el tiempo de espera del script de instalación y revisar la salida de los archivos dot en los registros de inicio del espacio de trabajo.

Las capacidades clave incluyen:

- Utilice repositorios privados de GitHub, GitLab, Bitbucket o Azure DevOps para los archivos dot.
- Aplique los archivos dot cuando un espacio de trabajo se inicie o se reanude con nuevas confirmaciones de repositorio.
- Ejecute **Personalizar entorno** para volver a aplicar los archivos dot a un espacio de trabajo existente.
- Mantenga el inicio del espacio de trabajo sin bloqueo si un script de archivos dot falla o agota el tiempo de espera.

Para obtener más información, consulte Configuración.

Lista de verificación de configuración para la incorporación guiada de proyectos

La consola del proyecto ahora incluye una Lista de verificación de configuración que guía a los propietarios y desarrolladores del proyecto a través de los primeros pasos comunes. La lista de verificación aparece como un panel lateral plegable en las páginas del proyecto y mantiene el progreso a través de la navegación para que los usuarios puedan volver a su siguiente tarea de configuración.

Los propietarios del proyecto ven los pasos para revisar imágenes, agregar repositorios y secretos, crear plantillas y agregar usuarios. Los desarrolladores ven los pasos para revisar su perfil, configurar integraciones, personalizar su entorno, agregar credenciales y crear un espacio de trabajo. Los desarrolladores que regresan ven una lista de verificación más corta centrada en la preparación específica del proyecto.

Los administradores de la plataforma pueden habilitar o deshabilitar las listas de verificación de propietarios de proyectos y desarrolladores desde la incorporación ajustes.

Para obtener más información, consulte Configuración general.

Puntos de montaje de AWS para almacenamiento compartido del espacio de trabajo

Los puntos de montaje ahora admiten el almacenamiento de Amazon Web Services además del almacenamiento de archivos de Azure. Los propietarios de proyectos pueden crear o adjuntar almacenamiento compartido respaldado por Amazon Elastic File System (EFS) o Amazon S3 Files, y luego ponerlo a disposición de los espacios de trabajo a través del flujo existente de **Acceso a recursos**.

Utilice los puntos de montaje de AWS cuando los equipos necesiten archivos compartidos en vivo para artefactos de compilación, grandes conjuntos de datos o datos de proyectos colaborativos sin copiar esos datos en cada espacio de trabajo. Los administradores habilitan primero los tipos de almacenamiento disponibles, y los propietarios de proyectos eligen si crear un nuevo almacenamiento o adjuntar un almacenamiento que un equipo de infraestructura ya haya preparado.

Las capacidades clave incluyen:

- Crear nuevos puntos de montaje respaldados por AWS a partir de clases de almacenamiento elegibles.
- Adjuntar almacenamiento existente de Amazon EFS o Amazon S3 Files a un proyecto.
- Utilizar acceso de solo lectura o de lectura/escritura al adjuntar puntos de montaje a espacios de trabajo.

- Ver una validación y una guía de eliminación más claras cuando un punto de montaje todavía está siendo utilizado por espacios de trabajo activos o eliminados.

Para obtener más información, consulte Puntos de montaje.

Amazon EFS y Amazon S3 Files requieren recursos de AWS que SecurSpaces no crea, incluidos el sistema de archivos, los destinos de montaje por zona de disponibilidad, los roles de IAM y las clases de almacenamiento de Kubernetes. Para conocer los pasos de configuración del administrador, consulte Preparar almacenamiento de AWS para puntos de montaje.

Extensión de IDE rediseñada para VS Code e IDE compatibles

La extensión de SecurSpaces para VS Code, Cursor, Windsurf y Kiro ha sido rediseñada en torno a una barra lateral que actúa como punto de entrada de SecurSpaces dentro del IDE. Los desarrolladores que comienzan su día desde un IDE local, una aplicación web progresiva o un enlace de inicio rápido ya no tienen que volver a la consola para realizar acciones rutinarias.

Anteriormente, la extensión listaba los espacios de trabajo y ofrecía poco más allá de iniciar, pausar y conectar. Los desarrolladores que trabajaban principalmente desde su IDE no tenían forma de ver lo que contenía un espacio de trabajo o de acceder a las acciones de la consola que necesitaban, lo que significaba un cambio constante de contexto.

Las capacidades clave incluyen:

- Explorar espacios de trabajo agrupados por proyecto, con el espacio de trabajo conectado resaltado y ordenado en la parte superior.
- Iniciar, pausar, conectar en la ventana actual o en una nueva, y cambiar entre espacios de trabajo.
- Expandir un espacio de trabajo para abrir sus repositorios clonados, puntos de montaje adjuntos y aplicaciones de espacio de trabajo en ejecución.
- Abrir una carpeta en un terminal, o copiar la URL de una aplicación de espacio de trabajo, desde el menú contextual.
- Ver la calidad de la conexión en la barra de estado, con el tiempo de ida y vuelta y el ancho de banda estimado.
- Ir a la consola para crear, editar o eliminar un espacio de trabajo, o para acceder a las páginas de perfil y solución de problemas.

La extensión ahora se ejecuta en su máquina local, y una pequeña extensión complementaria se ejecuta dentro del espacio de trabajo para informar la actividad y responder a las mediciones de conexión. Su token de acceso permanece en su máquina local.

Las acciones que dependen de características de plataforma más recientes se ocultan cuando la extensión está conectada a una plataforma SecurSpaces más antigua, y la barra lateral explica el motivo.

Para obtener más información, consulte Conectarse a un espacio de trabajo a través de SSH.

Recupere sus propios espacios de trabajo antes de que se eliminen

Los espacios de trabajo eliminados por una acción personalizada de inactividad ahora son visibles para su propietario antes de que desaparezcan definitivamente. **Perfil > Resumen > Espacios de trabajo** separa los **Espacios de trabajo activos** de los **Espacios de trabajo pendientes de eliminación**, y la lista de pendientes muestra la fecha límite de eliminación permanente en UTC con acciones para restaurar o eliminar permanentemente.

SecurSpaces también envía un correo electrónico al propietario del espacio de trabajo cuando un espacio de trabajo se mueve a la papelera de reciclaje, y de nuevo 24 horas antes de que se elimine permanentemente. Anteriormente, un espacio de trabajo podía desaparecer sin previo aviso y sin una forma de autoservicio para recuperarlo, lo que era una fuente común de solicitudes de soporte.

Para obtener más información, consulte Resumen del perfil.

Iniciar un espacio de trabajo cuenta como uso

Un espacio de trabajo que se inicia regularmente ya no se considera inactivo. Iniciar un espacio de trabajo desde la consola, la API REST o la extensión IDE ahora cuenta para la condición de **Espacio de trabajo inactivo**, por lo que un espacio de trabajo en el que alguien confía no se elimina por una política de inactividad simplemente porque nunca abrió una sesión dentro de él.

Iniciar un espacio de trabajo todavía no pospone el tiempo de espera de inactividad que lo pausa, por lo que los ahorros de costos por la pausa por inactividad no cambian.

Para obtener más información, consulte Acciones personalizadas.

Creación guiada de espacios de trabajo y una forma de requerir plantillas

La creación de un espacio de trabajo ahora comienza con un diálogo que pregunta cómo desea crearlo: a partir de una plantilla, desde cero o copiando un espacio de trabajo existente. **Crear desde plantilla** está marcado como recomendado. Esto reemplaza el botón dividido, donde las opciones de plantilla y copia estaban ocultas en un menú desplegable y eran fáciles de pasar por alto.

Los administradores de la plataforma ahora también pueden requerir plantillas. Un nuevo permiso **Requerir plantillas para la creación de espacios de trabajo** en un rol restringe a todos los que tienen ese rol a crear espacios de trabajo a partir de una plantilla; las opciones personalizadas y de copia se muestran pero están deshabilitadas, con una información sobre herramientas que explica el motivo. Úselo cuando cada espacio de trabajo en un proyecto deba ser reproducible y consistente.

Para obtener más información, consulte Crear un espacio de trabajo y Roles y permisos.

Archivar plantillas de espacio de trabajo

Las plantillas de espacio de trabajo ahora se pueden archivar y restaurar. Archive una plantilla para evitar que se use para nuevos espacios de trabajo mientras conserva los espacios de trabajo existentes que se crearon a partir de ella.

Una plantilla archivada no se puede seleccionar en el flujo de creación de espacio de trabajo ni a través de un enlace de inicio rápido, y está oculta de la lista de Plantillas a menos que elija mostrar las plantillas archivadas. Dado que una plantilla no se puede eliminar mientras los espacios de trabajo aún la utilizan, el archivado es la forma admitida de retirar una plantilla que todavía está en uso.

Para obtener más información, consulte Plantillas.

Recuperación de espacios de trabajo eliminados

Los espacios de trabajo eliminados ahora se mueven a un área recuperable de **Espacios de trabajo eliminados** antes de la eliminación permanente. Esto proporciona a los usuarios un período de seguridad para restaurar un espacio de trabajo que se eliminó accidentalmente y ayuda a los administradores a gestionar el período de retención.

Los propietarios de proyectos pueden restaurar o eliminar permanentemente espacios de trabajo desde la vista de configuración del proyecto. Los administradores de la plataforma pueden revisar los espacios de trabajo eliminados en todos los proyectos y ajustar cuántos días permanecen recuperables los espacios de trabajo eliminados antes de que se eliminen permanentemente.

Para obtener más información, consulte Descripción general del perfil.

Mejoras en la configuración de instalación e ingreso

Los administradores tienen más opciones de implementación en esta versión. Los valores de Helm ahora admiten la configuración de licencias durante la implementación o actualización, las

anotaciones de ingreso de HAProxy y una opción para omitir la representación de recursos de certificado de cert-manager para clústeres que no usan cert-manager.

Estas opciones reducen el trabajo manual posterior a la instalación y ayudan a adaptar SecurSpaces a una gama más amplia de entornos de Kubernetes.

Para obtener más información, consulte Requisitos técnicos.

SecurSpaces 2026.4

Las respuestas de usuario y grupo de SCIM incluyen detalles de membresía

Las respuestas SCIM ahora incluyen información más completa sobre la membresía de grupos para proveedores de identidad que validan la membresía a través de la API SCIM de SecurSpaces. El endpoint `/Users` devuelve los grupos directos a los que pertenece un usuario, y el endpoint de lista `/Groups` devuelve los miembros de cada grupo sin necesidad de una búsqueda de grupo filtrada por separado.

Esta mejora ayuda a los administradores a conectar SecurSpaces con proveedores SCIM que esperan que los datos de membresía de usuarios y grupos estén disponibles durante las comprobaciones de sincronización. Los usuarios sin membresías de grupo siguen omitiendo el atributo `groups`, por lo que no se añaden datos de grupo vacíos a su respuesta de usuario SCIM.

Para obtener más información, consulte SCIM.

Gestión de enlaces Quickstart en la API de REST

Los equipos de plataforma ahora pueden gestionar los enlaces Quickstart de las plantillas de espacio de trabajo a través de la API REST. Esto ayuda a los equipos a automatizar enlaces Quickstart para portales de desarrolladores, archivos README de repositorios y otros flujos de trabajo de incorporación sin copiar manualmente enlaces de la consola de SecurSpaces.

La API puede habilitar, recuperar y revocar el enlace Quickstart de una plantilla. Las respuestas incluyen la URL y fragmentos de inserción de Markdown y HTML listos para usar, para que la automatización pueda mantener el contenido del portal sincronizado con el enlace de la plantilla actual.

Las capacidades clave incluyen:

- Habilitar, recuperar y revocar enlaces Quickstart para plantillas de espacio de trabajo

- Recuperar la URL sin procesar, el fragmento de Markdown y el fragmento de HTML para un enlace Quickstart
- Usar estilos de botón de inserción claros u oscuros para los fragmentos generados
- Crear espacios de trabajo a partir de enlaces Quickstart a través del mismo flujo que los enlaces generados por la interfaz de usuario

Para obtener más información, consulte API de REST y Plantillas.

Elementos de acceso personalizados en la API REST

Los elementos de acceso personalizados ahora están disponibles a través de la API REST para espacios de trabajo y plantillas de espacios de trabajo. Esto proporciona a los equipos de plataforma paridad de API con la consola de SecurSpaces para añadir entradas de acceso con un solo clic a herramientas o servicios internos que se ejecutan dentro de un espacio de trabajo.

Los llamadores de API pueden incluir elementos de acceso personalizados al crear espacios de trabajo y plantillas, actualizar el conjunto completo de elementos en un espacio de trabajo existente, y leer los elementos configurados de las respuestas de espacios de trabajo y plantillas. Cada elemento puede definir un nombre de visualización, puerto, comando, icono opcional y sonda de estado opcional.

Las capacidades clave incluyen:

- Añadir elementos de acceso personalizados al crear un espacio de trabajo o una plantilla de espacio de trabajo
- Actualizar o eliminar elementos de acceso personalizados en un espacio de trabajo existente
- Leer el estado y las URL de los elementos de acceso personalizados de las respuestas de la API del espacio de trabajo
- Recibir errores de validación legibles por máquina para puertos no válidos, nombres duplicados, comandos faltantes o iconos no compatibles

Para obtener más información, consulte API REST y Crear un espacio de trabajo.

Documentación de la versión autoalojada

La documentación del producto SecurSpaces ahora se incluye con cada versión y se sirve desde el plano de control. Esto ayuda a las implementaciones con aislamiento de red y de red restringida a mantener la documentación disponible sin depender del acceso a internet externo.

Los usuarios pueden abrir la documentación incluida desde el entorno de SecurSpaces en `/docs/`. La versión también incluye un formato `llms.txt` para que las herramientas de IA puedan leer la misma documentación correspondiente a la versión cuando su organización permita ese acceso.

Las capacidades clave incluyen:

- Acceder a la documentación del producto correspondiente a la versión desde el entorno de SecurSpaces implementado
- Mantener la documentación disponible en entornos sin acceso directo a internet
- Proporcionar documentación legible por IA a través de `llms.txt`

Para obtener más información, consulte Conceder acceso a la documentación de SecurSpaces a su asistente de IA.

Actualizaciones de la API de Workspace para extensiones de IDE

Las API de workspace ahora incluyen más información y operaciones para las integraciones de extensiones de IDE. Estas actualizaciones ayudan a las extensiones de IDE a mostrar detalles más completos del workspace y a gestionar workspaces personales sin requerir que los usuarios vuelvan a la consola de SecurSpaces.

El nuevo soporte de API incluye detalles del workspace para repositorios adjuntos, puntos de montaje y depósitos de datos. Las extensiones de IDE también pueden usar indicadores de capacidad de `/version.json` para habilitar funciones solo cuando la versión de SecurSpaces implementada las admita.

Las capacidades clave incluyen:

- Recuperar detalles del workspace personal de `GET /v1/personal_workspaces/{workspace_id}`
- Eliminar un workspace personal con `DELETE /v1/personal_workspaces/{workspace_id}`
- Usar indicadores de capacidad `/version.json` para la gestión de funciones de extensión
- Leer campos de versión de VSCode en las respuestas de la API de workspace

Para obtener más información, consulte API REST y Versiones de VSCode.

Enrutamiento de AI Gateway desde valores de Helm

Los administradores de la plataforma ahora pueden configurar el enrutamiento de AI Gateway directamente en los valores de Helm de SecurSpaces. Esta actualización permite que las implementaciones intercepten dominios de servicio de IA seleccionados y enruten ese tráfico a través de un servicio interno de AI Gateway.

Utilice esta configuración cuando su organización desee un control centralizado para el acceso de proveedores de IA desde los workspaces. Los valores de Helm admiten tanto la configuración a nivel de plataforma como las anulaciones específicas de la región para regiones externas.

Las capacidades clave incluyen:

- Configurar la dirección del servicio interno de AI Gateway con `platform.aiGateway.address`
- Listar los puntos finales DNS del proveedor de IA para interceptar con `platform.aiGateway.dnsEndpoints`
- Anular los valores de toda la plataforma por región con `region.aiGateway`

Para obtener más información, consulte Configurar el enrutamiento de AI Gateway.

Autenticación X.509 para MongoDB externo

SecurSpaces ahora puede conectarse a una implementación externa de MongoDB utilizando la autenticación de certificado X.509. Esto ofrece a las organizaciones una alternativa a la autenticación de nombre de usuario y contraseña para servicios externos de MongoDB como MongoDB Atlas.

Los administradores pueden seleccionar el mecanismo de autenticación `MONGODB-X509` en los valores de Helm y proporcionar el certificado de cliente, la clave privada, y el paquete de autoridad de certificación opcional, ya sea como valores codificados en base64 o desde un Secret de Kubernetes existente.

Para obtener más información, consulte External MongoDB X.509.

Orientación para conexiones SSH salientes bloqueadas

Cuando un espacio de trabajo intenta iniciar una conexión SSH saliente y no hay ningún método SSH configurado para el host de destino, SecurSpaces ahora muestra un mensaje de terminal procesable antes de cerrar la conexión. Anteriormente, el usuario solo veía que la conexión SSH se cerraba.

El mensaje explica que un administrador debe habilitar la Identidad SSH personal o un Servicio SSH conectado antes de que el espacio de trabajo pueda conectarse a hosts externos a través de SSH.

Para obtener más información, consulte Conectarse a servidores y servicios externos a través de SSH.

Detección de inactividad del espacio de trabajo más inteligente

SecurSpaces ahora utiliza un enfoque híbrido para determinar si un espacio de trabajo está realmente inactivo antes de pausarlo. Anteriormente, una conexión SSH abierta era suficiente para mantener un espacio de trabajo en ejecución indefinidamente, incluso cuando nadie estaba trabajando activamente. Esto generaba costos de infraestructura innecesarios, por ejemplo, cuando los desarrolladores dejaban su IDE abierto durante la noche o el fin de semana.

El nuevo motor de detección de inactividad introduce tres capas de inteligencia:

- **Las señales de actividad del IDE tienen prioridad.** Cuando la extensión IDE de SecurSpaces está activa, el sistema utiliza señales de entrada granulares, como la actividad del teclado y el ratón, para determinar si un usuario está presente. Una conexión SSH abierta pero sin usar por sí sola ya no impide que un espacio de trabajo se pause.
- **Respaldo SSH para IDE no compatibles.** Para los desarrolladores que utilizan IDE que no son compatibles con la extensión de SecurSpaces, el sistema recurre a la lógica anterior basada en SSH, de modo que el trabajo activo no se interrumpe.
- **Anulación manual.** Los responsables de seguridad pueden desactivar la detección de inactividad para espacios de trabajo seleccionados con el fin de admitir servicios de larga duración, como herramientas o componentes de desarrollo compartidos. Cuando se activa, el espacio de trabajo sigue ejecutándose incluso sin la entrada directa del usuario.

Para obtener más información, consulte Detección de inactividad del espacio de trabajo para espacios de trabajo conectados por SSH

Puntos de montaje de almacenamiento compartido

Los equipos que trabajan con grandes conjuntos de datos compartidos, como datos de entrenamiento de ML, artefactos de modelos o resultados de experimentos, ahora pueden montar almacenamiento externo directamente en sus espacios de trabajo. Esta nueva capacidad, denominada Puntos de montaje, elimina la necesidad de copiar datos en el clúster antes de que sean accesibles.

Anteriormente, SecurSpaces solo ofrecía cubos de datos, que funcionan como instantáneas puntuales. Aunque son útiles para el control de versiones, las instantáneas duplican los datos en el clúster, requieren un espacio en disco considerable, tardan mucho en replicarse para grandes conjuntos de datos e impiden la colaboración en tiempo real porque las actualizaciones requieren un ciclo de publicación manual.

Con los puntos de montaje:

- **Administradores de plataforma** habilitan la función globalmente en Configuración > Integraciones.
- **Propietarios de proyectos** configuran los puntos de montaje especificando los detalles del almacenamiento, incluida la dirección del servidor, el nombre del recurso compartido, la ruta de montaje predeterminada y los permisos de acceso (solo lectura o lectura-escritura).
- **Desarrolladores** adjuntan los puntos de montaje disponibles al crear un espacio de trabajo o una plantilla de espacio de trabajo. La ruta de montaje se puede personalizar por espacio de trabajo, y el sistema evita conflictos de ruta.

Esta versión inicial solo es compatible con el almacenamiento basado en archivos de Azure.

Para obtener más información, consulte Compartir datos entre usuarios - Puntos de montaje.

Acceso unificado con Citrix DaaS (Vista previa técnica)

SecurSpaces ahora se integra con Citrix DaaS y Citrix Workspace para proporcionar una experiencia de acceso unificado en entornos de desarrollo Linux, Windows y macOS. Hasta ahora, SecurSpaces solo admitía espacios de trabajo de Kubernetes basados en Linux, excluyendo a los equipos que dependen de herramientas de Windows o macOS, como Xcode, Visual Studio completo o herramientas de simulación específicas de la plataforma.

Con esta integración, los desarrolladores pueden acceder tanto a los espacios de trabajo tradicionales de SecurSpaces como a los escritorios y aplicaciones virtuales basados en Citrix desde una única consola. Los usuarios solo necesitan iniciar sesión una vez en la consola de SecurSpaces, y todos los recursos basados en SecurSpaces y Citrix se pueden acceder sin problemas y sin autenticación adicional.

Esta característica proporciona:

- Acceso unificado a aplicaciones y espacios de trabajo basados en Kubernetes y Citrix desde la consola de SecurSpaces
- Autenticación integrada con inicio de sesión único

- Acceso a aplicaciones y escritorios virtuales con la aplicación nativa de Citrix Workspace

Esta característica permite a las organizaciones incorporar más equipos de desarrolladores a una plataforma segura, aprovechando su infraestructura y licencias de Citrix existentes.

Para obtener más información, consulte Integración de Citrix DaaS.

Gestión independiente de versiones de VS Code

Las actualizaciones de VS Code ya no están vinculadas a las versiones de la plataforma SecurSpaces. Anteriormente, los clientes tenían que esperar una actualización completa de SecurSpaces para obtener una versión más reciente de VS Code, lo que podía retrasar el acceso a nuevas funciones del editor y la compatibilidad con complementos.

Con esta versión, VS Code se entrega y actualiza de forma independiente de la plataforma SecurSpaces. Las capacidades clave incluyen:

- **Actualizaciones controladas y reversión.** Los administradores pueden adoptar nuevas versiones de VS Code cuando estén listos y revertir a una versión anterior si surgen problemas.
- **Soporte sin conexión y con aislamiento de red.** Las organizaciones que restringen el acceso a internet desde el plano de control o los espacios de trabajo pueden alojar los archivos de actualización de VS Code en un punto de distribución interno, como un repositorio de artefactos o un recurso compartido de red.
- **Notificaciones integradas.** Los administradores de SecurSpaces y los oficiales de seguridad reciben notificaciones a través del sistema de notificación integrado cuando hay una nueva versión de VS Code disponible.
- **Actualizaciones controladas por el usuario.** Los desarrolladores pueden controlar cuándo se aplica la actualización de VS Code a cada uno de sus espacios de trabajo, de forma similar al flujo de actualización de espacios de trabajo existente.

Para obtener más información, consulte Versiones de VSCode.

Soporte nativo para Kiro IDE

Kiro ahora es compatible como IDE para conexiones de espacio de trabajo basadas en SSH, uniéndose a VS Code Desktop, JetBrains Gateway, Cursor y Windsurf. Anteriormente, los usuarios de Kiro tenían que configurar manualmente las conexiones SSH y las instalaciones de extensiones para acceder a sus espacios de trabajo de SecurSpaces.

Con esta actualización, el modal Conectar a través de SSH en la consola de SecurSpaces incluye Kiro como opción de lanzamiento. Al seleccionarlo, se abre Kiro en la máquina local del desarrollador, se instala o activa automáticamente la extensión de SecurSpaces y se establece la conexión SSH remota al espacio de trabajo de destino.

Para obtener más información, consulte Conectarse a un espacio de trabajo a través de SSH

Flujo de incorporación de usuarios mejorado

El flujo de Añadir usuario para proyectos se ha rediseñado para reducir errores y acelerar la incorporación. Los propietarios de proyectos ahora pueden añadir usuarios de forma masiva pegando una lista de direcciones de correo electrónico, con validación en línea y comentarios claros sobre errores. La búsqueda de un solo usuario se limita a los usuarios de la plataforma que aún no están en el proyecto, evitando confusiones. Al añadir usuarios externos, el flujo guía al administrador a través de los detalles adicionales requeridos antes de completar la operación.

Para obtener más información, consulte Añadir y eliminar usuarios y grupos - Añadir usuarios de forma masiva

Instalación automática de la extensión de SecurSpaces para conexiones SSH

Al conectarse a un espacio de trabajo a través de SSH desde VS Code Desktop, SecurSpaces ahora instala automáticamente la extensión de SecurSpaces requerida en el espacio de trabajo remoto. Esto elimina un paso manual anterior y reduce los fallos en la configuración de la conexión.

Recursos de espacio de trabajo fantasma configurables a través de Helm

Las especificaciones de recursos del espacio de trabajo fantasma ahora se pueden configurar a través del gráfico de Helm, lo que brinda a los administradores más control sobre la asignación de recursos para los espacios de trabajo preaprovisionados.

Soporte de Kubernetes PriorityClass para pods de espacio de trabajo

Los administradores ahora pueden asignar una Kubernetes PriorityClass a los pods del espacio de trabajo a través de un nuevo campo de configuración opcional de Helm. Cuando se establece, todos los pods del espacio de trabajo recién creados se asignan a la clase de prioridad especificada, lo que permite a los programadores de Kubernetes y a herramientas como Karpenter tomar mejores decisiones de escalado y programación. Cuando se omite la configuración, el comportamiento existente no cambia.

Imagen de escritorio Debian con acceso desde el navegador

Ahora está disponible una nueva imagen de contenedor preconfigurada basada en Debian con NoVNC, que proporciona un entorno de escritorio completo directamente accesible en el navegador. Esta opción es útil para equipos que necesitan herramientas basadas en GUI o entornos de prueba dentro de sus espacios de trabajo de SecurSpaces.

VS Code actualizado a 1.114

SecurSpaces ahora incluye VS Code 1.114, lo que aporta las últimas características del editor y mejoras en la compatibilidad de complementos.

Descargas mejoradas para grandes exportaciones de análisis

Las exportaciones de mediciones del espacio de trabajo ahora pueden manejar de forma fiable archivos de informes grandes. Los administradores y los oficiales de seguridad pueden descargar análisis del espacio de trabajo filtrados por organización, proyecto y rango de fechas, incluso cuando los archivos resultantes son demasiado grandes para una llamada API estándar. El mecanismo de descarga ahora utiliza una ruta de transferencia optimizada para admitir archivos de gran tamaño.

Para obtener más información, consulte Información sobre el uso de recursos del espacio de trabajo - Acceder a las mediciones del espacio de trabajo

Opción de proxy para conservar el host para aplicaciones de espacio de trabajo

Las aplicaciones del espacio de trabajo ahora incluyen una opción de proxy para conservar el host (Preserve Host). Cuando está habilitada, el proxy reenvía la URL pública de la aplicación del espacio de trabajo en el encabezado Host, alineándola con los encabezados Origin y X-Forwarded-Host. Esto permite que herramientas como Jupyter Notebook y pgAdmin funcionen detrás del servicio de proxy de SecurSpaces sin una configuración de proxy personalizada por herramienta. La opción está desactivada de forma predeterminada para evitar interrumpir los flujos de trabajo de desarrollo local que esperan localhost.

Para obtener más información, consulte Aplicaciones del espacio de trabajo - Anular encabezado de host

Descargas de especificaciones OpenAPI de autoservicio

La página de documentación de la API REST de SecurSpaces ahora incluye un botón para descargar la especificación OpenAPI. La especificación OpenAPI se empaqueta y se envía automáticamente con cada versión menor y mayor de SecurSpaces, para que los equipos de

ingeniería de la plataforma puedan descargar la especificación que coincida con su versión de SecurSpaces actualmente implementada sin ponerse en contacto con Citrix.

URL de documentación personalizada

Los administradores de la plataforma ahora pueden reemplazar el enlace de documentación predeterminado de SecurSpaces con una URL personalizada que apunte a la documentación interna de su organización. Cuando se habilita en Configuración > General > Documentación, el enlace personalizado se aplica globalmente y actualiza la entrada de Documentación en el menú del perfil de usuario para todos los usuarios, proyectos y organizaciones. Cuando se deshabilita, el enlace vuelve a la documentación predeterminada de SecurSpaces.

Para obtener más información, consulte Configuración general - Documentación

Marketplace OpenVSX personalizado para extensiones de VS Code

Los administradores de la plataforma ahora pueden apuntar todos los espacios de trabajo de VS Code a un marketplace OpenVSX personalizado en Configuración > General > OpenVSX Marketplace, reemplazando el enfoque anterior de variable de entorno manual `EXTENSIONS_GALLERY`. La configuración se hereda en todas las organizaciones, proyectos y espacios de trabajo. Los nuevos espacios de trabajo utilizan el marketplace configurado inmediatamente; los espacios de trabajo existentes adoptan el cambio después de su próximo reinicio.

Para obtener más información, consulte General Settings - OpenVSX Marketplace

Mejoras de la interfaz de usuario

Versionado más sencillo de plantillas de espacio de trabajo

Las acciones de Editar, Publicar y Establecer como predeterminado ahora están directamente disponibles en la lista de versiones de plantillas, lo que hace que los pasos de versionado sean más rápidos y fáciles de descubrir.

Flujo de trabajo optimizado para añadir imágenes

El flujo de importación de imágenes de contenedor ahora comienza con la URL de la imagen, rellena automáticamente los campos cuando es posible, admite la entrada de credenciales en línea e incluye descripciones y sugerencias más claras.

Ordenación alfabética para espacios de trabajo y plantillas

Las listas de espacios de trabajo y plantillas ahora se ordenan alfabéticamente de forma predeterminada.

Control independiente para las guías en la aplicación

La configuración de Análisis de uso ahora permite a los administradores mantener los análisis habilitados mientras desactivan las guías en la aplicación de forma independiente.

Mejor búsqueda en los menús desplegables

Los menús desplegables más grandes ahora muestran un campo de búsqueda visible que se enfoca al abrirse, con las opciones ordenadas alfabéticamente.

Componentes de selección coherentes

SecurSpaces ahora utiliza un componente de selección unificado con un comportamiento de búsqueda y ordenación coherente en toda la consola.

Establecer como predeterminado más claro para imágenes de contenedor

La acción Establecer como predeterminado ahora se muestra de forma más selectiva en la lista de versiones de imágenes de contenedor, lo que reduce el desorden visual y mantiene la acción accesible.

Descripción de los scripts de inicio

El paso Scripts de inicio en el asistente de espacios de trabajo y plantillas ahora incluye una descripción que explica cuándo y por qué usar scripts de inicio.

Selector de idioma movido al perfil de usuario

La selección de idioma se ha movido del pie de página a la configuración del perfil de usuario, y ahora se etiqueta con los nombres de los idiomas en lugar de banderas.

Advertencia de salida del asistente coherente

SecurSpaces ahora siempre advierte a los usuarios antes de que salgan del asistente de espacios de trabajo o plantillas, independientemente de la ruta de navegación, y utiliza etiquetas de diálogo más claras.

Mensaje mejorado para secretos vacíos

Cuando no existen secretos, el asistente ahora muestra una guía sobre cómo añadir uno en lugar de implicar que un filtro no arrojó resultados.

Mensajes más claros de «sin resultados» del filtro

Las listas filtradas ahora muestran un mensaje contextual de «sin resultados» con una acción Borrar filtros para que los usuarios puedan distinguir entre resultados vacíos y datos faltantes.

Componentes de interfaz de usuario y descripciones emergentes estandarizados

Los iconos, las descripciones emergentes y los patrones de estilo son ahora más coherentes en toda la consola de SecurSpaces.

Corrección de errores

Los menús contextuales se cierran al desplazarse

Los menús contextuales ahora se cierran automáticamente cuando el usuario se desplaza, evitando artefactos visuales por el reposicionamiento continuo.

El banner de mantenimiento permanece alineado durante el desplazamiento

El banner de notificación de mantenimiento ya no se desliza brevemente bajo la barra de menú al desplazarse por páginas largas.

La marca de verificación de validación ya no aparece en entradas vacías

El campo de entrada del nombre secreto ya no muestra una marca de verificación de éxito cuando el campo está vacío o es inválido.

Programación consistente de la caché de imágenes en todos los nodos

Los pods de caché de imágenes ahora se programan con antiafinidad a nivel de nodo, asegurando que un pod se ejecute en cada nodo de espacio de trabajo gestionado por Karpenter en lugar de uno por zona de disponibilidad. Esto restaura el comportamiento predecible de los nodos cálidos en clústeres multi-AZ.

SecurSpaces 2025.10

Esta versión contiene las siguientes características nuevas:

Advertencia de renovación para certificados CA

SecurSpaces ahora muestra una advertencia cuando un certificado CA está próximo a caducar, lo que permite a los administradores tomar medidas oportunas para renovar los certificados y evitar interrupciones del servicio.

Información sobre el uso de recursos del espacio de trabajo

SecurSpaces ahora proporciona información histórica sobre el consumo de CPU y RAM del espacio de trabajo. Estos datos se recopilan y almacenan automáticamente en la base de datos de SecurSpaces, y se pueden acceder a través de las API workspace-measurements y workspace-measurement-samples para respaldar el análisis de dimensionamiento correcto y las tendencias a largo plazo.

El sistema recopila la siguiente información:

- Uso de CPU a lo largo del tiempo
- Uso de RAM a lo largo del tiempo

Los datos se conservan durante 7 días.

Para obtener más información, consulte Información sobre el uso de recursos del espacio de trabajo

Detección de inactividad mejorada para sesiones SSH

Cuando los usuarios se conectan a un espacio de trabajo de SecurSpaces a través de SSH con el complemento SecurSpaces/Strong Network, SecurSpaces ahora puede supervisar la actividad con mayor precisión. Esto permitirá que el sistema pause los espacios de trabajo inactivos de forma más fiable, mejorando la eficiencia de costes sin interrumpir las sesiones activas. A los usuarios que no tengan el complemento SecurSpaces/Strong Network instalado en su IDE local se les pedirá que lo instalen mediante una notificación dentro de la consola de SecurSpaces. Los administradores pueden usar la API de SecurSpaces `/v1/metrics/ssh-workspaces-no-extension-usage` para determinar una lista de usuarios que se conectan a través de SSH sin el complemento instalado.

> Nota:
>
> La versión inicial de esta publicación no cambiará el comportamiento del programador de SecurSpaces para minimizar las interrupciones a los usuarios existentes. Una futura versión menor habilitará los cambios del programador.

Creación mejorada de espacios de trabajo de inicio rápido

Se ha mejorado la interfaz de inicio rápido, utilizada al crear un nuevo espacio de trabajo a través de un enlace de inicio rápido. Antes del aprovisionamiento, los usuarios ahora pueden revisar:

- La imagen y la plantilla utilizadas para crear el espacio de trabajo
- La ubicación organizativa donde se implementará el espacio de trabajo

Además, los usuarios pueden seleccionar la versión de la plantilla y la ubicación de implementación geográfica, lo que proporciona un mayor control y transparencia durante la configuración del espacio de trabajo.

Para obtener más información, consulte Inicio rápido

Compatibilidad con Azure Cosmos DB

SecurSpaces ahora es compatible con Azure Cosmos DB como opción de base de datos administrada, además de MongoDB Atlas. Esto brinda a los equipos una mayor flexibilidad para elegir el servicio de base de datos que mejor se adapte a sus cargas de trabajo y entorno de nube.

Flujo de plantillas de espacio de trabajo: Añadir funcionalidad de borrador y promoción

Las nuevas versiones de plantillas de espacio de trabajo ahora se crean en estado de borrador. Los borradores se pueden modificar y probar hasta que se promocionen explícitamente a la versión predeterminada. Este flujo de trabajo simplifica el proceso de iteración en las plantillas, al tiempo que evita que los usuarios utilicen inadvertidamente versiones que no están listas para producción.

Para obtener más información, consulte Crear una nueva versión de una plantilla

Duplicación de plantillas en la consola de SecurSpaces

Los propietarios de proyectos ahora pueden duplicar plantillas de espacio de trabajo existentes directamente dentro de la consola de SecurSpaces. Esto facilita la creación de nuevas plantillas que comparten la misma pila de herramientas e integraciones que las existentes, al tiempo que permite una configuración ajustada para satisfacer las necesidades específicas de los desarrolladores.

Visibilidad y clasificación de recursos del espacio de trabajo

La vista Proyecto/Espacio de trabajo ahora muestra la configuración completa de recursos (CPU, RAM y almacenamiento) para cada espacio de trabajo en un proyecto. Los espacios de trabajo también se pueden ordenar por estos atributos, lo que permite a los propietarios de proyectos identificar rápidamente las asignaciones de recursos elevadas y apoyar las actividades de ajuste de tamaño.

Nuevos filtros en la vista Proyecto/Espacios de trabajo

Se ha añadido una nueva opción de filtro a la vista Proyecto/Espacios de trabajo, lo que facilita la identificación de espacios de trabajo con características específicas dentro de proyectos grandes. Los criterios de filtro disponibles incluyen:

- Propietario – propietario del espacio de trabajo
- Imagen – imagen base utilizada para el espacio de trabajo
- Fecha de creación – fecha de creación
- Estado – estado actual del espacio de trabajo
- CPU, RAM, Almacenamiento – recursos asignados

Esta mejora agiliza la gestión del espacio de trabajo y ayuda a localizar rápidamente los espacios de trabajo relevantes.

Para más información, consulte Filtrado de espacios de trabajo

Capacidad de respuesta de la consola optimizada

Hemos optimizado significativamente la forma en que la consola de SecurSpaces carga los datos, lo que resulta en una experiencia de usuario mucho más receptiva y fluida.

- Navegación casi instantánea: Las acciones que antes tenían un pequeño retraso ahora son casi instantáneas. Por ejemplo, navegar desde el nivel de la plataforma a un proyecto específico es notablemente más rápido.
- Flujo de trabajo mejorado: Esta mejora fundamental minimiza los tiempos de espera, mejorando su flujo de trabajo general y haciendo que la consola se sienta más fluida y eficiente.

Guías de incorporación interactivas

Al acceder a la consola web de SecurSpaces por primera vez, los usuarios ahora ven guías de incorporación interactivas. Estas guías resaltan las funcionalidades clave y explican los primeros pasos importantes, ayudando a los nuevos usuarios a empezar a trabajar más rápidamente.

Versión actualizada de Visual Studio Code

Los espacios de trabajo de SecurSpaces ahora incluyen Visual Studio Code v1.105.1, lo que proporciona las últimas características, mejoras y correcciones.

Flujo de trabajo mejorado para la creación de espacios de trabajo

Los campos de entrada para crear un nuevo espacio de trabajo a partir de una plantilla se han reorganizado para reducir el número de clics necesarios. Además, el nombre propuesto del espacio de trabajo ahora se genera automáticamente utilizando el formato `<First Name><First 3 letters of Surname>-<TemplateName>`, lo que agiliza el proceso de configuración y garantiza una nomenclatura coherente.

Por ejemplo: Espacio de trabajo StevenGal-Frontend

UX mejorada para espacios de trabajo sin límites de recursos

SecurSpaces ahora permite a los clientes crear espacios de trabajo sin límites de CPU o RAM, lo que permite una escalabilidad totalmente elástica. Los espacios de trabajo configurados con recursos ilimitados mostrarán un símbolo de infinito para el recurso afectado, proporcionando un indicador visual claro de esta configuración.

Selección predeterminada del usuario actual para la propiedad de los recursos

Siempre que SecurSpaces solicita un propietario para un recurso recién creado, el usuario actual aparece ahora en la parte superior de la lista de usuarios. Este cambio agiliza los flujos de trabajo comunes y acelera el proceso de creación de recursos.

Página de detalles de usuario mejorada

La página de detalles del usuario ahora muestra los programas de espacio de trabajo configurados por el usuario y enumera todos los espacios de trabajo con programas personalizados. Esta página también es accesible para los propietarios de proyectos, además de para los oficiales de seguridad. La vista mejorada proporciona una mayor visibilidad del contexto del usuario y de las configuraciones especiales, lo que facilita la resolución de problemas y la gestión del espacio de trabajo.

Plugin de Backstage para SecurSpaces

SecurSpaces ahora ofrece un plugin para Backstage, que permite a los usuarios listar y acceder a todos los espacios de trabajo asociados con un proyecto de software específico, así como crear nuevos espacios de trabajo directamente desde Backstage. Para las organizaciones que utilizan un Portal de Desarrolladores Integrado basado en Backstage, esta integración agiliza los flujos de trabajo de los desarrolladores y simplifica la gestión de los espacios de trabajo.

Para obtener más información, consulte Plugin de espacios de trabajo de SecurSpaces para Backstage

Integración de HashiCorp Vault para la gestión de secretos

SecurSpaces ahora se integra con HashiCorp Vault, la solución líder en gestión de secretos. Cuando está habilitado, todos los secretos almacenados previamente en la base de datos de SecurSpaces se almacenan de forma segura en Vault. Esto incluye:

- Secretos de la plataforma: Clave privada SSH de la plataforma, secretos de la aplicación OAuth, secretos del gateway de correo electrónico y credenciales del registro de imágenes del espacio de trabajo
- Secretos de usuario: Identidad personal SSH del usuario, claves SSH privadas y claves GPG

Esta integración mejora la seguridad al centralizar la gestión de secretos y aprovechar los sólidos controles de acceso y las capacidades de auditoría de Vault.

Para obtener más información, consulte Usar HashiCorp Vault como gestor de secretos

Telemetría de uso

SecurSpaces ahora recopila telemetría de uso para ayudar a mejorar la plataforma. Esta telemetría se utiliza para comprender la adopción de funciones e identificar áreas de mejora en el rendimiento y la usabilidad. No se recopilan datos personales y toda la información se maneja de acuerdo con las políticas de privacidad de la organización.

Integración de Pendo para orientación y análisis en la aplicación

SecurSpaces ahora recopila telemetría de uso para ayudar a mejorar la plataforma. Esta telemetría se utiliza para comprender la adopción de funciones e identificar áreas para mejoras de rendimiento y usabilidad. No se recopilan datos personales y toda la información se maneja de acuerdo con las políticas de privacidad de la organización. `https://FQDN/platform/settings/analytics/usage_analytics`

Para obtener más información, consulte Análisis de uso

Fixed issues

Citrix SecurSpaces™ 2026.9 incluye los siguientes problemas solucionados

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
October 06, 2026	2026.9.4	Nuevas funciones	Se añadió soporte para actualizar

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			implementaciones internas de Percona MongoDB de Percona Operator 1.20.1 a 1.23.0 con un kit de actualización proporcionado por el instalador. El gráfico actualizado también expone la configuración de copia de seguridad de Percona para destinos de almacenamiento, programaciones, retención, recuperación a un momento dado y la cuenta de servicio de base de datos utilizada por los agentes de copia de seguridad.
		Nuevas funciones	Se añadió soporte para copias de seguridad sin clave de Google Cloud Storage para Percona MongoDB interno en Google Kubernetes Engine utilizando la Federación de Identidades de Carga de Trabajo.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		Seguridad	Se actualizaron los paquetes base de la imagen sidecar del espacio de trabajo y containerd para abordar vulnerabilidades de alta gravedad.
		Seguridad	Se actualizó el gráfico del controlador de entrada de NetScaler CPX de 4.1.17 a 4.2.26 para abordar vulnerabilidades conocidas del controlador de entrada.
September 29, 2026	2026.9.3	Nuevas funciones	Se ha añadido compatibilidad con valores `specification_id` estables en las definiciones de niveles administrados de Citrix SecurSpaces Flex. Una versión de nivel administrado ahora puede mantener el mismo identificador en todos los inquilinos cuando Citrix fija el valor en los valores de implementación.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se ha resuelto un problema por el que los cambios correctos de disponibilidad de niveles administrados de Citrix SecurSpaces Flex y las actualizaciones masivas de versiones de niveles no aparecían en el registro de auditoría. El registro de auditoría ahora registra quién realizó la acción, cuándo ocurrió y el resultado.
		General	Se ha resuelto un problema por el que la guía de SSH saliente que se mostraba en los espacios de trabajo apuntaba a la URL de documentación anterior. La guía ahora abre la documentación actual de servicios externos de SecurSpaces.
September 28, 2026	2026.9.2	Nuevas funciones	Se ha añadido compatibilidad con Citrix SecurSpaces Flex para los niveles

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			de especificación de espacios de trabajo administrados por Citrix, incluidas las versiones de niveles administrados, las etiquetas de ciclo de vida, las solicitudes de actualización de espacios de trabajo y las actualizaciones masivas de versiones de niveles.
		Nuevas funciones	Se ha añadido compatibilidad con la API de REST para administrar versiones de VSCode en el ámbito de la plataforma, la organización y el proyecto. La API puede enumerar, importar, renombrar, eliminar y establecer valores predeterminados para las versiones, y administrar registros de VSCode a nivel de plataforma.
		General	Se ha resuelto un problema por el que las actualizaciones de Helm con la implementación interna de Percona MongoDB podían

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			regenerar las contraseñas de la base de datos e impedir que los servicios de la plataforma se autenticaran. Las actualizaciones del lado del servidor ahora reutilizan las contraseñas existentes a menos que un operador establezca un nuevo valor, y los cambios de credenciales reinician los servicios que las utilizan.
		General	Se ha resuelto un problema por el que un espacio de trabajo podía permanecer con una imagen de sidecar antigua después de una actualización de la plataforma sin mostrar un aviso de actualización. Los espacios de trabajo ahora muestran una actualización cuando la imagen de sidecar almacenada difiere de la versión enviada por la implementación.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se ha resuelto un problema por el que **Personas > Más detalles** del proyecto podía abrir la ruta de detalles de usuario incorrecta o mostrar la organización incorrecta en las migas de pan. El flujo de detalles de usuario del proyecto ahora mantiene el contexto del proyecto y la organización alineados.
		General	Se ha resuelto un problema por el que las imágenes de servicio de lanzamiento podían tener diferentes resúmenes de manifiesto dependiendo del registro regional utilizado. Las futuras imágenes de lanzamiento ahora utilizan capas comprimidas consistentes en todas las regiones de lanzamiento.
		General	Se ha resuelto un problema por el que las actualizaciones

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			concurrentes de Kubernetes podían hacer que las operaciones de inicio, reinicio o edición del espacio de trabajo fallaran con un conflicto de StatefulSet. Las actualizaciones de StatefulSet ahora reintentan en caso de conflicto.
September 21, 2026	2026.9.1	General	Se ha resuelto un problema por el que un espacio de trabajo detenido por exceder su límite de memoria informaba de `Reason: Unknown` y aconsejaba actualizar la imagen del espacio de trabajo. El fallo ahora se informa como `OOMKilled`, con orientación específica sobre la memoria.
		General	Se ha resuelto un problema por el que el aprovisionamiento SCIM almacenaba la dirección de correo electrónico de un usuario como nombre de pila y

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			apellido. `name.givenName` y `name.familyName` ahora se asignan al nombre del usuario.
		General	Se resolvió un problema por el que las extensiones de marketplace preconfiguradas en una plantilla de espacio de trabajo no se instalaban.
		General	Se resolvió un problema por el que una lista de selección múltiple con capacidad de búsqueda borraba el texto de búsqueda mientras el usuario escribía.
		General	Se actualizó la imagen predeterminada del espacio de trabajo a `2.3.9`.
August 13, 2026	2026.9.0	Seguridad	Se actualizaron las dependencias y las imágenes para abordar vulnerabilidades conocidas.
		Seguridad	Se resolvió un problema por el que algunas solicitudes

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			de API protegidas por roles podían eludir las comprobaciones de acceso.
		Seguridad	Se resolvió un problema por el que algunos flujos podían aceptar un tipo de token incorrecto.
		Seguridad	Se resolvió un problema por el que las acciones de gestión de usuarios podían afectar a usuarios fuera del ámbito del llamante.
		Seguridad	Se resolvió un problema por el que los secretos locales podían copiarse sin verificar la propiedad del contenedor.
		Seguridad	Se resolvió un problema por el que la transmisión de archivos sidecar podía exponer archivos de espacio de trabajo no deseados.
		Seguridad	Se resolvió un problema por el que el manejo de Git del sidecar podía aceptar argumentos

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			de comando inseguros.
		Seguridad	Se resolvió un problema por el que el acceso a Docker del espacio de trabajo era más amplio de lo necesario.
		Seguridad	Se resolvió un problema por el que el creador de imágenes se ejecutaba con más privilegios de los necesarios. Ahora utiliza BuildKit sin privilegios de root.
		Seguridad	Se eliminaron las claves de licencia de prueba de las imágenes de producción.
		Seguridad	Se rotaron las credenciales que se habían enviado al repositorio y se añadió una guía de recuperación para el operador.
		Seguridad	Se ha reforzado el ciclo de vida de los puntos de montaje de AWS, incluyendo la conexión,

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			actualización y eliminación.
		Seguridad	Se ha reforzado el manejo de los puntos de montaje: las clases de almacenamiento sin TLS están ocultas, se bloquea la eliminación de la papelera de reciclaje y los mensajes de error ya no revelan detalles internos.
		Seguridad	Se ha reforzado la documentación servida desde el plano de control en `/docs/`.
		Nuevas funciones	Se ha añadido compatibilidad con puntos de montaje de AWS para el almacenamiento de archivos de Amazon EFS y Amazon S3.
		Nuevas funciones	Se ha añadido una barra lateral de extensión de IDE rediseñada con repositorios, puntos de montaje y aplicaciones de espacio de trabajo.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		Nuevas funciones	Se ha añadido la supervisión de la calidad de la conexión en la barra de estado del IDE.
		Nuevas funciones	Se han añadido metadatos de usuario, proyecto y espacio de trabajo a las solicitudes de IA reenviadas a una puerta de enlace de IA.
		Nuevas funciones	Se añadió la comprobación de estado de AI Gateway con un comportamiento de apertura en caso de fallo configurable.
		Nuevas funciones	Se añadió un panel de Grafana de ejemplo para la elaboración de informes sobre el uso de la IA y el consumo de tokens.
		Nuevas funciones	Se añadió el seguimiento de la configuración del estado deseado de la versión de plantilla utilizada por cada espacio de trabajo.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		Nuevas funciones	Se añadieron indicadores de estado de la versión de plantilla y una ventana de Espacios de trabajo asociados con exportación a CSV.
		Nuevas funciones	Se añadió un flujo de actualización de espacio de trabajo que alinea un espacio de trabajo con la versión de plantilla predeterminada.
		Nuevas funciones	Se añadió el archivado y la restauración para plantillas de espacio de trabajo que aún tienen espacios de trabajo asociados.
		Nuevas funciones	Se añadieron archivos de configuración en **Perfil > Configuración** para la configuración de espacios de trabajo personales.
		Nuevas funciones	Se añadió una lista de comprobación de configuración en las páginas del proyecto para una

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			incorporación guiada.
		Nuevas funciones	Se añadió la recuperación de espacios de trabajo eliminados durante el período de retención configurado.
		Nuevas funciones	Se añadió compatibilidad con Helm para aplicar una licencia de plataforma durante la implementación o actualización.
		Nuevas funciones	Se añadió compatibilidad con la entrada de HAProxy y la representación opcional de certificados de cert-manager.
		Nuevas funciones	Se añadió compatibilidad con GitHub Copilot para espacios de trabajo detrás de una puerta de enlace de IA.
		General	Se actualizó la interfaz del producto y las plantillas de correo electrónico para usar el nombre

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			de producto Citrix SecurSpaces.
		General	Se resolvió un problema por el que las cargas de depósitos de datos podían iniciarse desde espacios de trabajo no elegibles.
		General	Se resolvió un problema por el que el estado de carga del depósito de datos podía ser engañoso.
		General	Se resolvió un problema por el que el modal de carga del bucket de datos podía mostrar datos de bucket obsoletos.
		General	Se resolvió un problema por el que la importación de imágenes podía usar credenciales o URL de imagen incorrectas.
		General	Se resolvió un problema por el que una importación de imagen fallida podía convertirse en la etiqueta de imagen predeterminada.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvió un problema por el que los espacios de trabajo podían iniciarse con la etiqueta de imagen de contenedor incorrecta.
		General	Se resolvió un problema por el que las etiquetas de imagen reutilizadas podían dejar contenido de imagen de espacio de trabajo obsoleto.
		General	Se resolvió un problema por el que la configuración de la versión de VSCode podía perderse en los flujos de trabajo.
		General	Se resolvió un problema por el que una URL de registro privado de VSCode podía quedar obsoleta.
		General	Se resolvió un problema por el que las operaciones de Git firmadas podían fallar con `commit.gpgsign=true`.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvió un problema por el que el inicio del espacio de trabajo podía quedarse bloqueado durante los scripts de inicio del sistema.
		General	Se resolvió un problema por el que los espacios de trabajo podían permanecer en `Pending` debido a la configuración de almacenamiento.
		General	Se resolvió un problema por el que un socket IPC sidecar obsoleto podía causar `CrashLoopBackOff` .
		General	Se resolvió un problema por el que las programaciones de espacios de trabajo con una hora de inicio `00:00` no se guardaban.
		General	Se resolvió un problema por el que las acciones manuales de **Ejecutar** no se contaban como actividad.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvió un problema por el que las direcciones SSH de la página de perfil podían omitir la región del espacio de trabajo.
		General	Se resolvió un problema por el que las comprobaciones de roles de la organización no se aplicaban a las páginas protegidas.
		General	Se resolvió un problema por el que las referencias de roles deshabilitados podían interrumpir la carga del proyecto.
		General	Se resolvió un problema por el que el modal Deshabilitar rol mostraba `-1` en lugar de un marcador de posición.
		General	Se resolvió un problema por el que **Conectar a GitHub** no iniciaba OAuth para los nuevos usuarios.
		General	Se resolvió un problema por el que

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			los borradores de versiones de plantillas de espacio de trabajo podían ordenarse de forma impredecible.
		General	Se resolvió un problema por el que la opción crear a partir de existente mostraba valores de especificación incorrectos.
		General	Se resolvió un problema por el que las selecciones de servicios conectados HTTP y SSH no persistían.
		General	Se resolvió un problema por el que se podían perder las restricciones de la plantilla de especificación del espacio de trabajo.
		General	Se resolvió un problema por el que aparecían acciones de actualización del espacio de trabajo cuando no había ninguna actualización disponible.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvió un problema por el que las acciones del ciclo de vida de las plantillas podían dejar estados de espacio de trabajo huérfanos.
		General	Se resolvió un problema por el que **Añadir a favoritos** permanecía abierto después de la selección.
		General	Se resolvió un problema por el que la opción de filtro **Seleccionar todo** de la página de auditoría no se aplicaba.
		General	Se resolvió un problema por el que los totales de tokens del panel de IA eran inconsistentes.
		General	Se resolvió un problema por el que el tráfico de IA de los espacios de trabajo SSH carecía de metadatos de observabilidad.
		General	Se resolvió un problema por el que

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			la implementación de demostración con 1 clic podía fallar en escenarios comunes de reintento.
		General	Se resolvió un problema por el que los puntos de montaje de AWS de solo lectura no se podían montar.
		General	Se resolvió un problema por el que los puntos de montaje de Azure Files presentaban varios defectos que afectaban a la conexión y la actualización.
		General	Se resolvió un problema por el que un espacio de trabajo podía informar brevemente de un estado `DESTROYED` mientras se estaba creando.
		General	Se resolvió un problema por el que el asistente del espacio de trabajo podía quedarse atascado después de **Descartar**.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvió un problema por el que la edición de una especificación de espacio de trabajo no llegaba a los espacios de trabajo, pods y plantillas en ejecución.
		General	Se resolvió un problema por el que la sustitución de una plantilla de especificación podía escribir fuera de su ámbito previsto.
		General	Se resolvió un problema por el que la activación de la licencia de Community Edition podía fallar.
		General	Se resolvió un problema por el que el gráfico de uso de recursos de Insights mostraba huecos, colores inestables y una información sobre herramientas imprecisa.
		General	Se resolvió un problema por el que la actualización de las propiedades del espacio de trabajo

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			podía causar un error de backend.
		General	Se resolvió un problema por el que el cuadro de diálogo de actualización del espacio de trabajo mostraba un estado incorrecto para una versión de plantilla.
		General	Se resolvió un problema por el que la autorización de una clave SSH no mostraba los espacios de trabajo propiedad del usuario sin el permiso de gestión.
		General	Se resolvió un problema por el que se incluían repositorios no válidos en la comprobación de rutas duplicadas.
		General	Se resolvió un problema por el que la búsqueda de usuarios respondía lentamente.
		General	Se resolvió un problema por el que los registros de compilación de

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			imágenes no se podían transmitir.
		General	Se resolvió un problema por el que las compilaciones de imágenes podían fallar cuando el clúster utilizaba un proxy externo.
		General	Se resolvió un problema por el que la plataforma no se recuperaba rápidamente después de perder su bloqueo de elección de líder.

Citrix SecurSpaces 2026.4 incluye los siguientes problemas resueltos

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
August 24, 2026	2026.4.10	Seguridad	Se actualizaron los contextos de seguridad del gráfico de Helm para impedir la escalada de privilegios para los contenedores de servicios de plataforma y el contenedor de inicialización de permisos de syslog.
		General	Se resolvió un problema por el que

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			las respuestas de usuario de SCIM no incluían la pertenencia a grupos y las respuestas de lista de grupos de SCIM omitían a los miembros a menos que se solicitara un grupo específico. `/Users` ahora devuelve la pertenencia directa a grupos y las respuestas de lista de `/Groups` incluyen a los miembros.
August 14, 2026	2026.4.9	Nuevas funciones	Se añadió compatibilidad con la entrada de HAProxy.
		General	Se resolvió un problema por el que la creación de proyectos podía fallar después de que se deshabilitara el rol de **Propietario del proyecto**.
		General	Se resolvió un problema por el que la implementación de demostración de Azure con un solo clic podía fallar y dejar reglas de red incompletas.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvió un problema por el que la entrada de NetScaler podía fallar en Google Cloud.
		General	Se resolvió un problema por el que las sondas de Google Kubernetes Engine 1.35 podían agotar el tiempo de espera demasiado rápido.
July 20, 2026	2026.4.8	Seguridad	Se actualizaron las dependencias y las imágenes para abordar las vulnerabilidades conocidas.
		Nuevas funciones	Se añadió compatibilidad con la API de REST para gestionar los enlaces de inicio rápido de las plantillas de espacio de trabajo.
		Nuevas funciones	Se añadió compatibilidad con la API de REST para elementos de acceso personalizados en espacios de trabajo y plantillas.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvió un problema por el que las respuestas de la API REST de plantillas omitían los scripts de configuración.
		General	Se resolvió un problema por el que los registros del registro de VSCode podían pasarse por alto o quedar obsoletos.
July 2, 2026	2026.4.7	Seguridad	Se actualizaron las dependencias para abordar vulnerabilidades conocidas.
		Nuevas funciones	Se añadió la documentación de SecurSpaces servida desde el plano de control en `/docs/` para implementaciones aisladas.
		Nuevas funciones	Se añadió compatibilidad con la API de extensión de IDE para puntos finales de espacio de trabajo personales y campos de versión de VSCode.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		General	Se resolvieron los errores de confirmación de Git firmados cuando se configuró `commit.gpgsign=true`.
		General	Se resolvieron los fallos de acceso al repositorio de artefactos de JFrog para usuarios sin un token configurado.
		General	Se resolvió un problema por el que los límites de recursos de CPU y memoria podían perderse después de las operaciones de edición del espacio de trabajo.
		General	Se resolvió un problema por el que las respuestas de la API de creación de espacios de trabajo podían carecer de campos esperados.
		General	Se resolvió un problema por el que los repositorios adjuntos no aparecían en las respuestas de la API

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			del espacio de trabajo personal.
		General	Se resolvió un problema por el que el inicio de sesión rápido de la extensión IDE no redirigía a rutas que no eran de proyecto.
June 9, 2026	2026.4.6	Seguridad	Se actualizó el entorno de ejecución de Go y la cadena de herramientas de compilación para abordar vulnerabilidades conocidas.
		Nuevas características	Se añadió soporte de enrutamiento de AI Gateway a través de valores de Helm para dominios de servicios de IA seleccionados.
		Nuevas funciones	Se añadió la autenticación de certificados X.509 para las conexiones de SecurSpaces a implementaciones externas de MongoDB.
		General	Se resolvió el problema de las conexiones SSH salientes que se

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			cerraban sin explicación cuando no se configuraba ningún método SSH.
		General	Se resolvió un problema por el que el icono de añadir en la tarjeta de creación de la página de inicio vacía aparecía aplanado.
		General	Se resolvió un problema por el que las sesiones de la guía integrada de Pendo podían continuar después de cerrar la sesión.
June 4, 2026	2026.4.5	Seguridad	Se resolvió el problema de los tokens anónimos de JFrog aceptados durante el inicio de sesión de OAuth.
		General	Se resolvió un pánico nulo en el trabajo de rotación de secretos de cliente de OAuth cuando no se configuraba ninguna aplicación de OAuth.
		General	Se resolvió un problema por el que la acción de eliminación

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			automática utilizaba un tiempo de último uso del espacio de trabajo incorrecto.
		General	Se resolvió que las opciones de configuración de GPU estuvieran ocultas para el rol de oficial de seguridad en las plantillas de espacio de trabajo.
		Nuevas funciones	Se añadió compatibilidad con el espejo del registro de Docker del espacio de trabajo a través del valor Helm `workspaceDockerRegistryMirrors`.
May 29, 2026	2026.4.4	Seguridad	Se actualizaron las versiones de la cadena de herramientas de Go y Docker para abordar vulnerabilidades conocidas.
		Seguridad	Se actualizó la imagen de contenedor de MongoDB para abordar vulnerabilidades conocidas.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
		Seguridad	Se actualizó la imagen predeterminada del espacio de trabajo a `2.3.6` para abordar vulnerabilidades conocidas.
		General	Se resolvió un problema por el que el icono de "actualización disponible" persistía después de que se completara una actualización del espacio de trabajo.
		General	Se ha resuelto la asignación de color no determinista en los gráficos de asignación de recursos. Los colores ahora se ordenan por región.
		General	Se ha resuelto un problema por el que las condiciones de las Acciones personalizadas no se aplicaban correctamente.
		General	Se ha resuelto un problema por el que la página de Perfil mostraba un error al

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			actualizar para los usuarios con el rol de Desarrollador.
		General	Se han resuelto las unidades incorrectas para la memoria y el disco al editar los límites de recursos.
		General	Se ha resuelto el problema de que los registros de estado del espacio de trabajo no se inicializaban para los espacios de trabajo clonados o creados a partir de plantillas.
		General	Se ha resuelto el problema de que el menú desplegable **Avanzado** aparecía vacío para algunos roles en la configuración del espacio de trabajo.
May 12, 2026	2026.4.3	General	Se resolvió un problema de coste del clúster de Kubernetes causado por el preaprovisionamiento de nodos en caliente.
		General	Se resolvió un problema de caché de pods de imagen

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			realineando la antiafinidad de nodos a `kubernetes.io/hostname`.
		Nuevas características	Se añadió una configuración de plataforma para configurar una URL ascendente personalizada para la Galería de Extensiones de VS Code.
		Nuevas características	Se aumentaron los límites máximos configurables de especificación del espacio de trabajo para CPU, GPU, memoria y disco.

SecurSpaces 2025.10 incluye los siguientes problemas solucionados

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
April 30, 2026	2025.10.21	Seguridad	Se resolvió un problema por el que una aprobación SSH de espacio de trabajo rechazada seguía autorizando la clave pública presentada, lo que permitía que una conexión posterior con la misma clave

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			tuviera éxito. Las claves SSH ahora solo se autorizan cuando se acepta la solicitud de aprobación.
		Seguridad	Se han restringido los permisos de archivos y directorios en el instalador. Los directorios generados, los archivos de variables de Terraform y el paquete de certificados CA ahora se crean con acceso solo para el propietario para abordar los hallazgos de Mend SAST (CWE-732).
		Seguridad	Se actualizó la imagen del contenedor de MongoDB para abordar las vulnerabilidades conocidas reportadas por Mend.
		Seguridad	Se actualizó la imagen predeterminada del espacio de trabajo a `2.3.6` para abordar las

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			vulnerabilidades conocidas.
		General	Se resolvió el rendimiento lento de las consultas para las colecciones `ip_pod_assignment` y `workspaces_v5` que podría provocar eventos de proxy `OOMKilled`. Se añadió un índice compuesto en `(ip, region_id)` para `ip_pod_assignment` y un índice `team_id` en `workspaces_v5`.
		General	Se resolvió un retraso al cambiar a la pestaña Espacios de trabajo en la interfaz de usuario.
		General	Se resolvió un problema por el que el componente de tabla no mostraba su estado de carga en la recuperación inicial de datos.
		General	Se resolvió un problema por el que la información sobre herramientas de

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			copiar al portapapeles no aparecía en la primera acción de pasar el ratón o copiar.
		General	Se resolvió un problema por el que al abrir una sesión de terminal desde el menú desplegable se iniciaba una ventana duplicada en lugar de enfocar la existente.
April 23, 2026	2025.10.20	Seguridad	Esta versión incluye varias correcciones de vulnerabilidades en los servicios principales de la plataforma.
		Seguridad	Se actualizó el tiempo de ejecución del lenguaje Go a la versión 1.25.9 y se resolvieron las CVE de frontend notificadas por Mend.
		General	Se resolvió un problema por el que los scripts de configuración del espacio de trabajo se perdían al crear un espacio de trabajo a través de la

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			API REST. Los scripts de configuración ahora se conservan al crearlos.
		General	Se resolvió un problema de la interfaz de usuario por el que el icono del elemento de acceso al espacio de trabajo aparecía más alto de lo esperado.
April 14, 2026	2025.10.19	General	Se resolvió un problema por el que el aprovisionamiento de VM con 1 clic fallaba al dirigirse a un grupo de recursos de Azure existente.
April 13, 2026	2025.10.18	Seguridad	Esta versión incluye varias correcciones de vulnerabilidades en los servicios principales de la plataforma.
		General	Se resolvió un problema en el flujo de autenticación de OAuth2 por el que las direcciones de correo electrónico que contenían letras mayúsculas causaban fallos de autenticación o

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			discrepancias en las cuentas.
April 1, 2026	2025.10.17	Seguridad	Esta versión incluye varias correcciones de vulnerabilidades en los servicios principales de la plataforma.
March 30, 2026	2025.10.16	General	Se resolvió un error crítico del índice de CosmosDB que causaba fallos en la actualización del backend. Esta corrección garantiza que las actualizaciones del esquema de la base de datos y las operaciones de indexación se completen correctamente durante las implementaciones de la plataforma, evitando interrupciones del servicio durante el ciclo de actualización.
		General	Se han añadido espacios de trabajo acelerados por GPU con aceleración de hardware para aprendizaje

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			automático, ciencia de datos y cargas de trabajo con uso intensivo de gráficos.
March 17, 2026	2025.10.15	Seguridad	Esta versión incluye varias correcciones de vulnerabilidades en los servicios principales de la plataforma.
March 9, 2026	2025.10.14	Redes	Se ha resuelto un problema por el que el acceso HTTP entre espacios de trabajo no funcionaba.
February 19, 2026	2025.10.13	General	Se ha resuelto un problema con Git Large File Storage (LFS) que afectaba a los repositorios de GitLab al usar SSH para la autenticación.
February 11, 2026	2025.10.12	Seguridad	Esta versión incluye varias correcciones de vulnerabilidades en los servicios centrales de la plataforma.
February 11, 2026	2025.10.11	General	Se resolvió un problema por el que el trabajo cron de medición generaba un mensaje de error engañoso para los

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			espacios de trabajo sin pods activos, como los que se encuentran en estado de pausa.
January 30, 2026	2025.10.10	Seguridad	Esta versión incluye varias correcciones de vulnerabilidades en los servicios centrales de la plataforma.
January 28, 2026	2025.10.9	General	Se resolvió un problema con la Galería de extensiones de VS Code que impedía el descubrimiento y la instalación de extensiones.
		Nuevas características	Se actualizó el NetScaler Ingress Controller (NetScaler CPX) de la versión 3.2.22 a la 3.3.2. Esta actualización proporciona una estabilidad mejorada y un mayor rendimiento para la gestión del tráfico de entrada.
January 23, 2026	2025.10.8	Seguridad	Esta versión incluye varias correcciones de vulnerabilidades en los servicios

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			principales de la plataforma.
January 15, 2026	2025.10.7	Seguridad	Se refactorizó la configuración RBAC del Helm Chart para mejorar la postura de seguridad de la plataforma mediante principios de mínimo privilegio. El ClusterRole previamente unificado se ha dividido en dos ámbitos específicos: el rol con ámbito de espacio de nombres (Namespace-scoped Role) gestiona recursos específicos de la carga de trabajo, incluidos pods, trabajos y secretos; el ClusterRole mínimo (Minimal ClusterRole) está restringido a recursos esenciales de todo el clúster, como nodos, clases de almacenamiento y métricas.
December 18, 2025	2025.10.6	General	Se corrigió un error en entornos de VM de 1 clic que utilizaban integración OAuth que impedía

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			que los IDE locales se conectaran correctamente a través de extensiones y complementos SSH. Esta resolución garantiza que los desarrolladores puedan utilizar herramientas IDE locales, como VS Code Desktop o JetBrains Gateway, dentro de la sesión de espacio de trabajo autenticada.
December 15, 2025	2025.10.5	General	Se ha añadido compatibilidad con las anotaciones de F5 NGINX. Los administradores de la plataforma pueden habilitar la compatibilidad con controladores dedicados con `platform.useF5NginxController: true`.
		Seguridad	Se ha actualizado el tiempo de ejecución del lenguaje Go a la versión 1.25.5, que aborda vulnerabilidades de seguridad conocidas.

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
December 2, 2025	2025.10.4	General	Se ha corregido un problema de permisos que impedía a los usuarios con el rol de oficial de seguridad deshabilitar las funciones de análisis en la página de configuración de la plataforma.
		General	Se ha resuelto un problema que provocaba que el componente de la API de Workspace entrara en estado CrashLoopBackOff cuando el sistema gestionaba un gran número de espacios de trabajo activos o desmantelados.
		Nuevas características	Se ha añadido una nueva opción de configuración para deshabilitar la detección de modo automático de Amazon EKS durante la configuración del clúster. Los administradores pueden establecer `region.clusterConfig.disableAutoM`

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			`odeCheck: true` para un control más granular en entornos de implementación específicos.
		Nuevas características	Se ha introducido la compatibilidad con Terraform para la gestión de grupos de usuarios, lo que permite a los administradores aprovisionar, actualizar y gestionar grupos de usuarios de espacios de trabajo utilizando prácticas de Infraestructura como código.
November 26, 2025	2025.10.3	General	Se ha corregido un problema por el que algunas dependencias de Visual Studio Code fallaban debido a un requisito subyacente de la biblioteca estándar de C. La versión mínima requerida de `glibc` es ahora la 2.28 para garantizar la estabilidad y compatibilidad con la funcionalidad remota de VS Code en las

FECHA DE LANZAMIENTO	VERSIÓN	CATEGORÍA	DESCRIPCIÓN
			distribuciones de Linux compatibles.
		Seguridad	Se ha actualizado el tiempo de ejecución del lenguaje Go a la versión 1.25.4, que aborda vulnerabilidades de seguridad conocidas.
November 21, 2025	2025.10.2	General	Se ha resuelto el rendimiento lento de la migración de bases de datos. Una optimización del motor de migración de bases de datos reduce significativamente el tiempo necesario para ejecutar actualizaciones de bases de datos durante los lanzamientos de productos y las actualizaciones de versión.
November 14, 2025	2025.10.1	General	Se ha eliminado la dependencia de la biblioteca estándar de C (`libc`). Los componentes principales del espacio de trabajo ya no requieren `libc` en tiempo de ejecución.

What's new in SecurSpaces Flex

Este artículo resume las nuevas funciones, mejoras y correcciones para Citrix SecurSpaces™ Flex. Para el historial de versiones de Citrix SecurSpaces autohospedado, consulte Novedades de Citrix SecurSpaces.

Septiembre de 2026

Catálogo de tamaños de espacio de trabajo administrado

Citrix SecurSpaces Flex ahora utiliza un catálogo de tamaños de espacio de trabajo administrado por Citrix. Citrix publica los niveles de tamaño de espacio de trabajo disponibles y sus versiones, y las implementaciones de Flex concilian ese catálogo durante las actualizaciones de la plataforma.

Esta versión añade el estado del ciclo de vida para las versiones de nivel administrado. Los administradores pueden ver las versiones de nivel actuales, anteriores y retiradas, mantener la configuración de disponibilidad de la organización y del proyecto, y actualizar los espacios de trabajo afectados a la versión actual del mismo nivel.

Las capacidades clave incluyen:

- Niveles de tamaño de espacio de trabajo administrados Light, Medium y Heavy con estado de versión.
- Controles de disponibilidad de la organización y del proyecto que permanecen disponibles para los administradores.
- Mensajes de actualización del espacio de trabajo cuando un espacio de trabajo utiliza una versión de nivel administrado anterior.
- Actualizaciones masivas de versiones de nivel que mueven los espacios de trabajo a la versión actual del mismo nivel.
- Versiones de nivel retiradas que están ocultas para la creación de nuevos espacios de trabajo, mientras que los espacios de trabajo existentes permanecen visibles.

Para obtener más información, consulte Plantillas de espacio de trabajo de SecurSpaces Flex.

Identificadores de nivel administrado estables y de auditoría

Los niveles de tamaño de espacio de trabajo administrado ahora proporcionan un registro operativo más claro. Cuando un administrador habilita o deshabilita un nivel administrado, o aplica una actualización masiva para mover espacios de trabajo a la versión de nivel actual,

SecurSpaces registra la acción exitosa en el registro de auditoría con el actor, la hora y el resultado.

Citrix también puede fijar el identificador de una versión de nivel administrado en los valores de implementación. Esto mantiene el mismo identificador de versión de nivel administrado en todos los inquilinos de Flex, mientras que las implementaciones existentes sin un valor fijado continúan recibiendo un identificador generado.

Agosto de 2026

Disponibilidad general: Citrix SecurSpaces Flex

Citrix SecurSpaces Flex ya está disponible de forma general como un servicio administrado por Citrix dentro de Citrix Platform Flex que ofrece espacios de trabajo Linux seguros para equipos de desarrollo. Ofrecido a través de Citrix Cloud, este servicio proporciona entornos de desarrollador alojados sin infraestructura de cliente que configurar o mantener. En esta versión, Citrix SecurSpaces Flex solo es aplicable a entornos de Azure. Para obtener más información, consulte Descripción general de Citrix SecurSpaces Flex.

Funciones nuevas y mejoradas

- **Plano de control administrado por Citrix** — Citrix opera la infraestructura de Azure Kubernetes Service (AKS) y Azure Cosmos DB.
- **Tamaño del espacio de trabajo por perfil** — Ligero (2 vCPU / 8 GB RAM), Medio (4 vCPU / 16 GB RAM) y Pesado (8 vCPU / 32 GB RAM), cada uno asignado a una tarifa de crédito de Platform Flex publicada.
- **Tamaño y plantilla de espacio de trabajo desacoplados** — Una única plantilla de espacio de trabajo se puede emparejar con cualquier perfil de computación bajo demanda.
- **Compatibilidad con varias regiones** — Se aprovisiona una región principal de Azure en el momento de la implementación, y su equipo de Citrix puede añadir regiones secundarias más adelante.
- **Administración de versiones** — Citrix administra las actualizaciones de versión para su entorno, incluida la programación de ventanas de mantenimiento.
- **Conectividad de red** — Conecte los espacios de trabajo a sistemas propiedad del cliente a través del emparejamiento de Azure vNET o la puerta de enlace VPN.
- **DLP, RBAC y registro de auditoría nativos** — Controles integrados para la prevención de pérdida de datos, la gobernanza de acceso y el cumplimiento.

- **Compatibilidad con agentes de IA en entornos aislados** — Los agentes de codificación de IA se ejecutan dentro de los espacios de trabajo bajo el mismo plano de control y marco de políticas que las sesiones de desarrolladores humanos.
- **Modelo de crédito de Platform Flex** — Los créditos de Citrix SecurSpaces Flex provienen del mismo grupo que Citrix DaaS Flex, sin un ciclo de adquisición independiente.

Más información

- Descripción general de Citrix SecurSpaces Flex
- Licencias para Citrix Platform Flex