



Enregistrement de session 2210

Contents

Enregistrement de session 2210	5
Nouveautés	6
Problèmes résolus	6
Problèmes connus	6
Avis de tiers	7
Configuration système requise	8
Mise en route	11
Planifier votre déploiement	12
Recommandations de sécurité	15
Considérations sur la capacité à monter en charge	21
Installer, mettre à niveau et désinstaller	37
Enregistrement de session dynamique	71
Configurer	77
Configurer les paramètres de l'agent d'enregistrement de session	77
Activer ou désactiver l'enregistrement	78
Configurer la connexion au serveur d'enregistrement de session	79
Changer votre protocole de communication	81
Configurer les paramètres sur le serveur d'enregistrement de session	83
Autoriser les utilisateurs	83
Configurer le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP)	85
Personnaliser les messages de notification	90
Activer ou désactiver les signatures numériques	90
Rapports de stockage d'enregistrement de session	91

Spécifier la taille du fichier pour les enregistrements	93
Spécifier l'emplacement du stockage des enregistrements	96
Stratégies	102
Configurer les stratégies d'enregistrement de session	104
Configurer des stratégies de visionnage d'enregistrement	117
Configurer les stratégies de détection d'événements	123
Configurer les stratégies de réponse aux événements	155
Haute disponibilité et équilibrage de charge	166
Équilibrer la charge des serveurs d'enregistrement de session	167
Configurer la haute disponibilité de base de données	170
Afficher les enregistrements	172
Lecteur d'enregistrement de session	172
Lancer le lecteur d'enregistrement de session	173
Activer ou désactiver la lecture de session active	175
Activer ou désactiver la protection de lecture	176
Rechercher des enregistrements	176
Imposer des restrictions d'accès aux enregistrements	179
Ouvrir et lire des enregistrements	182
Enregistrements en cache	190
Afficher les périodes d'inactivité	191
Utiliser des événements et des signets	191
Lecteur Web d'enregistrement de session	194
Accéder au lecteur Web	195
Masquer ou afficher le contenu sur la page d'accueil du lecteur Web	202

Rechercher des enregistrements	205
Imposer des restrictions d'accès aux enregistrements	206
Ouvrir et lire des enregistrements	209
Configurer les préférences	213
Augmenter la taille du paquet de transport pour le lecteur Web	214
Afficher les périodes d'inactivité	214
Utiliser les événements et les commentaires	216
Partager les URL des enregistrements	219
Afficher les statistiques d'événements graphiques pour chaque enregistrement	221
Afficher les points de données relatifs à chaque session enregistrée	225
Gérer les enregistrements	226
Gérer et interroger les journaux de l'administrateur	233
Recommandations	239
Configurer l'équilibrage de charge dans un déploiement existant	239
Déployer et équilibrer la charge de l'enregistrement de session sur Azure	288
Dépanner	322
Échec de l'installation des composants du serveur	322
Le test de la connexion à la base de données échoue lors de l'installation	323
L'agent ne peut pas se connecter au serveur	323
Le serveur ne peut pas se connecter à la base de données	325
Échec de l'enregistrement des sessions	326
Impossible d'afficher la lecture de session active	328
Les enregistrements sont endommagés ou incomplets	329
Vérifier les connexions des composants	329

Échec de la recherche d'enregistrements à l'aide du lecteur

333

Enregistrement de session 2210

April 27, 2023

Important :

La stratégie de cycle de vie du produit des versions Current Releases (CR) et Long Term Service Releases (LTSR) est décrite dans [Étapes du cycle de vie](#).

L'enregistrement de session enregistre, catalogue et archive les sessions pour en permettre la récupération et la lecture.

L'enregistrement de session offre des stratégies flexibles pour déclencher l'enregistrement automatique de sessions d'application et de bureau. L'enregistrement de session prend également en charge l'enregistrement de session dynamique. L'enregistrement de session permet aux services informatiques de vérifier et d'examiner l'activité des utilisateurs, et assure ainsi un contrôle interne à des fins de conformité à la réglementation et de surveillance de la sécurité. De même, l'enregistrement de session facilite également le travail du support technique en accélérant l'identification et la résolution des problèmes.

Avantages

Sécurité renforcée grâce à la journalisation et à la surveillance. L'enregistrement de session permet aux entreprises d'enregistrer l'activité des utilisateurs à l'écran pour les applications qui traitent des informations sensibles, de surveiller et de prévenir la fuite d'informations sensibles des sessions virtuelles. La prévention des fuites d'informations sensibles est particulièrement importante dans les secteurs réglementés tels que la santé et les finances.

Puissante surveillance des activités. L'enregistrement de session capture et met en archive les mises à jour d'écran, notamment les activités de la souris et le résultat visible de frappes clavier afin de fournir un enregistrement des activités d'utilisateurs, d'applications et de serveurs spécifiques.

L'enregistrement de session n'est pas conçu pour la collecte de preuves dans le cadre de procédures judiciaires. Toutefois, les organisations peuvent utiliser l'enregistrement de session avec d'autres techniques pour la collecte de preuves, telles que des enregistrements vidéo conventionnels combinés avec des outils d'eDiscovery traditionnels.

Réduction de la durée de résolution de problèmes. Lorsque les utilisateurs appellent au sujet d'un problème difficile à reproduire, le personnel de support technique peut activer les enregistrements des sessions utilisateur. Si le problème se reproduit, l'enregistrement de session fournit un enregistrement visuel horodaté de l'erreur, qui peut être utilisé ensuite pour une résolution plus rapide des problèmes.

Nouveautés

December 21, 2022

Nouveautés dans la version 2210

Cette version comprend la nouvelle fonctionnalité suivante et résout un [problème](#) afin d'améliorer l'expérience utilisateur :

Prise en charge de l'installation sur la session 0

Cette version introduit l'argument **AllowSession0Install** qui vous permet d'automatiser l'installation des composants d'administration de l'enregistrement de session dans la session 0. Pour plus d'informations, consultez [Automatiser l'installation](#).

Nouveautés dans les versions précédentes

Pour connaître les nouvelles fonctionnalités incluses dans les versions qui ont été mises à disposition après la version 1912 LTSR jusqu'à la version 2209 CR, consultez l'article [Historique des nouveautés](#).

Problèmes résolus

December 21, 2022

Comparé à : Enregistrement de session 2209

L'enregistrement de session 2210 ajoute les corrections suivantes :

- Des erreurs de dépassement de délai peuvent se produire lorsque vous sélectionnez plus de 40 enregistrements à la fois pour modifier les restrictions d'accès. [SRT-8496]

Problèmes connus

April 3, 2024

Les problèmes suivants ont été identifiés dans cette version :

- Si vous utilisez des [signatures Citrix Web App Firewall \(WAF\) pour atténuer partiellement la vulnérabilité CVE-2021-44228](#), l'enregistrement de session risque de ne pas fonctionner comme prévu. Pour résoudre le problème, excluez les adresses IP des serveurs d'enregistrement de session de la stratégie **mitigate_cve_2021_44228** du côté de NetScaler. [CVADHELP-24365]
- Un utilisateur de domaine disposant de privilèges d'administrateur local sur la console de stratégie d'enregistrement de session peut ajouter des utilisateurs locaux et des utilisateurs de domaine auxquels s'applique l'action d'une règle de stratégie. Toutefois, un utilisateur local disposant de privilèges d'administrateur local peut ajouter uniquement des utilisateurs locaux, mais pas des utilisateurs de domaine. [SRT-5769]
- Le lecteur Web peut ne pas fonctionner correctement si vous le mettez à niveau à partir de la version 2009 ou antérieure. Pour résoudre le problème, effacez le cache de votre navigateur. [SRT-5624]
- Les stratégies personnalisées des règles peuvent être perdues après la mise à jour de l'enregistrement de session à partir de la version incluse dans XenApp and XenDesktop 7.6 LTSR vers la dernière version. Comme solution de contournement, mettez à jour le logiciel vers la version incluse dans la dernière CU de XenApp and XenDesktop 7.15 LTSR, puis mettez-le à jour vers la dernière version. [SRT-4546]
- Lorsque Machine Creation Services (MCS) ou Citrix Provisioning (PVS) crée des VDA avec Microsoft Message Queuing (MSMQ) installé, ces VDA peuvent disposer de la même **QMID** dans certaines conditions. Cette condition peut entraîner divers problèmes, par exemple :
 - Les sessions peuvent ne pas être enregistrées, même si l'accord d'enregistrement est accepté.
 - Le serveur d'enregistrement de session peut ne pas pouvoir recevoir les signaux de fermeture de session, par conséquent les sessions peuvent être toujours actives.

Pour trouver une solution à ce problème, consultez la section [Installer, mettre à niveau et désinstaller](#). [#528678]

Avis de tiers

February 20, 2024

[Enregistrement de session version 2210](#) (téléchargement de PDF)

Cette version d'Enregistrement de session peut inclure des logiciels tiers distribués sous licence selon les conditions définies dans ce document.

Configuration système requise

February 28, 2023

L'enregistrement de session inclut les composants de l'administration d'enregistrement de session, l'agent d'enregistrement de session et le lecteur d'enregistrement de session. Vous pouvez installer les composants de l'administration d'enregistrement de session (base de données d'enregistrement de session, serveur d'enregistrement de session et console de stratégie d'enregistrement de session) sur un serveur unique ou sur des serveurs différents. La section suivante détaille les exigences pour chacun des composants d'enregistrement de session.

Pour plus d'informations sur l'utilisation de cette version Current Release (CR) dans un environnement Long Term Service Release (LTSR) et d'autres questions fréquemment posées, consultez cet [article du centre de connaissances](#).

Base de données d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Versions Microsoft SQL Server prises en charge :

- Microsoft SQL Server 2019 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2017 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2016 SP2 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2016 SP1 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2014 SP2 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2012 SP3 éditions Enterprise, Express et Standard
- Microsoft SQL Server 2008 R2 SP3 éditions Enterprise, Express et Standard

Services de base de données Azure SQL pris en charge :

- Azure SQL Managed Instance
- SQL Server sur machines virtuelles Azure (VM)
(Utilisez les versions prises en charge de Microsoft SQL Server indiquées précédemment.)

Services de base de données AWS RDS pris en charge :

- SQL Server

Configuration requise : .NET Framework 4.7.2

Serveur d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Autres éléments requis :

- Internet Information Services (IIS) 10, 8.5, 8.0 ou 7.5
- .NET Framework version 4.7.2
- Si le serveur d'enregistrement de session utilise HTTPS comme protocole de communication, ajoutez un certificat valide. L'enregistrement de session utilise HTTPS par défaut, selon les recommandations de Citrix.
- Microsoft Message Queuing (MSMQ), avec intégration Active Directory désactivée et la prise en charge de MSMQ HTTP activée.
- Journalisation de l'administrateur : dernière version de Chrome, Firefox ou Internet Explorer 11.

Console de stratégie d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Configuration requise : .NET Framework 4.7.2

Agent d'enregistrement de session

Installez l'agent d'enregistrement de session sur chaque agent VDA (Windows Virtual Delivery Agent) sur lequel vous souhaitez enregistrer des sessions.

Systèmes d'exploitation pris en charge :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- Windows 10, version minimale 1607
- Windows 10 Entreprise pour postes de travail virtuels

Exigences :

- Citrix Virtual Apps and Desktops 7 2203 avec licence Premium
- Citrix Virtual Apps and Desktops 7 1912 LTSR CU4 ou version ultérieure avec licence Platinum
- XenApp et XenDesktop 7.15 LTSR CU8 avec licence Platinum
- .NET Framework 4.7.2
- Microsoft Message Queuing (MSMQ), avec intégration Active Directory désactivée et la prise en charge de MSMQ HTTP activée

Remarque :

L'enregistrement de session prend actuellement en charge les éditions Advanced, Advanced Plus, Premium et Premium Plus de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

Lecteur d'enregistrement de session

Systèmes d'exploitation pris en charge :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- Windows 10 64 bits, version minimale 1607

Configuration requise : .NET Framework 4.7.2

Remarque :

Sous Windows 10 32 bits, vous pouvez installer le lecteur uniquement à l'aide du fichier Session-RecordingPlayer.msi. Le fichier msi se trouve sur l'image ISO de Citrix Virtual Apps and Desktops sous **\layout\image-full\x86\Session Recording**.

Pour obtenir des résultats optimaux, installez le lecteur d'enregistrement de session sur une station de travail disposant des caractéristiques suivantes :

- Résolution d'écran de 1024 x 768.
- Profondeur de couleur d'au moins 32 bits.
- 2 Go de RAM minimum ; des ressources supplémentaires en RAM et UC/GPU peuvent améliorer les performances lors de la lecture d'enregistrements riches en graphiques ; plus particulièrement si les enregistrements contiennent beaucoup d'animations.

Le délai de réponse de la recherche dépend de la taille de l'enregistrement et des spécifications matérielles de votre ordinateur.

Mise en route

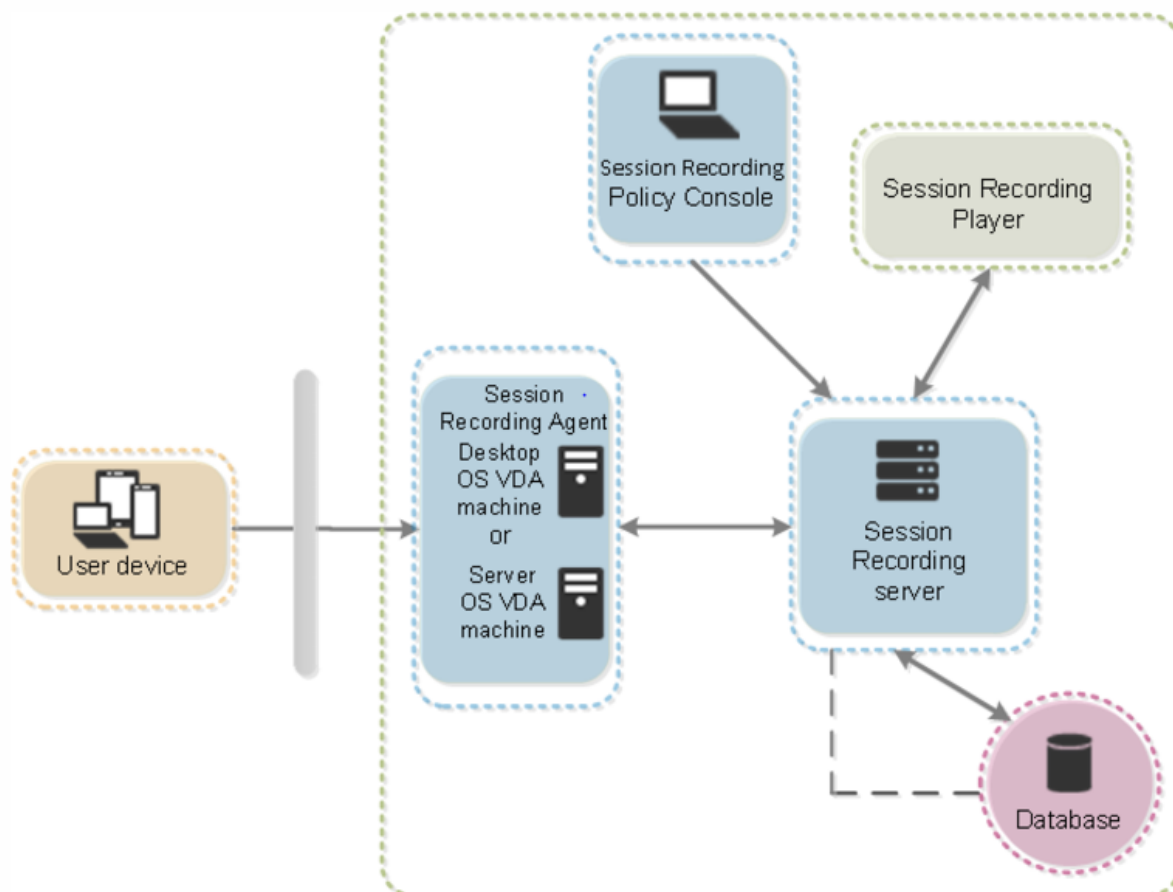
February 20, 2024

L'enregistrement de session se compose de cinq composants :

- **Agent d'enregistrement de session.** Composant installé sur chaque VDA pour OS multi-session ou OS mono-session pour activer l'enregistrement. Il est responsable de l'enregistrement des données de session.
- **Serveur d'enregistrement de session.** Il s'agit d'un serveur hébergeant ce composant :
 - Le broker. Une application Web IIS 6.0+ hébergée dont les objectifs sont les suivants :
 - * Gestion des requêtes de recherche et des demandes de téléchargement de fichiers à partir du lecteur et du lecteur Web d'enregistrement de session
 - * Gestion des demandes d'administration des stratégies depuis la console de stratégie d'enregistrement de session
 - * Évaluation des stratégies d'enregistrement pour chaque session Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
 - Le gestionnaire de stockage. Service Windows qui gère les fichiers de sessions enregistrées reçues de chaque VDA d'enregistrement de session.
 - Journalisation de l'administrateur. Sous-composant facultatif installé avec le serveur d'enregistrement de session pour consigner les activités d'administration. Toutes les données de journalisation sont stockées dans une base de données SQL Server nommée **CitrixSessionRecordingLogging** par défaut. Vous pouvez personnaliser le nom de la base de données.
- **Lecteur d'enregistrement de session.** Il s'agit d'une interface utilisateur à laquelle les utilisateurs accèdent depuis une station de travail pour lire des fichiers de session enregistrées.
- **Base de données d'enregistrement de session.** Composant qui gère la base de données SQL Server pour stocker les données de sessions enregistrées. Lorsque ce composant est installé, il crée une base de données appelée **CitrixSessionRecording** par défaut. Vous pouvez personnaliser le nom de la base de données.
- **Console de stratégie d'enregistrement de session.** Console utilisée pour créer des stratégies afin de spécifier les sessions à enregistrer.

Dans l'exemple de déploiement représenté par cette illustration, tous les composants d'enregistrement de session résident sous la protection d'un pare-feu de sécurité. L'agent d'enregistrement de session est installé sur un VDA pour OS multi-session ou OS mono-session. Un second serveur héberge la console de stratégie d'enregistrement de session, un troisième remplit les fonctions de serveur d'enregistrement de session, tandis qu'un quatrième serveur héberge la base de données d'enregistrement de session. Le lecteur d'enregistrement de session est installé sur une station

de travail séparée. Une machine cliente, située en-dehors du pare-feu, communique avec le VDA pour OS de serveur sur lequel l'agent d'enregistrement de session est installé. À l'intérieur du pare-feu, l'agent, la console de stratégie, le lecteur et la base de données d'enregistrement de session communiquent tous avec le serveur d'enregistrement de session.



Planifier votre déploiement

February 20, 2024

Limitations et restrictions

L'enregistrement de session ne prend pas en charge le mode d'affichage de redirection Desktop Composition (DCR). Par défaut, l'enregistrement de session désactive le DCR dans une session à enregistrer. Vous pouvez configurer ce comportement dans les **propriétés de l'agent d'enregistrement de session**.

Lorsque vous parcourez les URL configurées dans la [stratégie Redirection du contenu du navigateur](#) dans Internet Explorer, les activités graphiques ne sont pas enregistrées.

Enregistrement de session ne prend pas en charge le mode d'affichage Framehawk. Les sessions en mode d'affichage Framehawk ne peuvent pas être enregistrées ni lues correctement. Les sessions enregistrées dans le mode d'affichage Framehawk peuvent ne pas contenir les activités de session.

L'enregistrement de session ne peut pas enregistrer la vidéo provenant de la webcam Lync lors de l'utilisation du pack d'optimisation HDX RealTime.

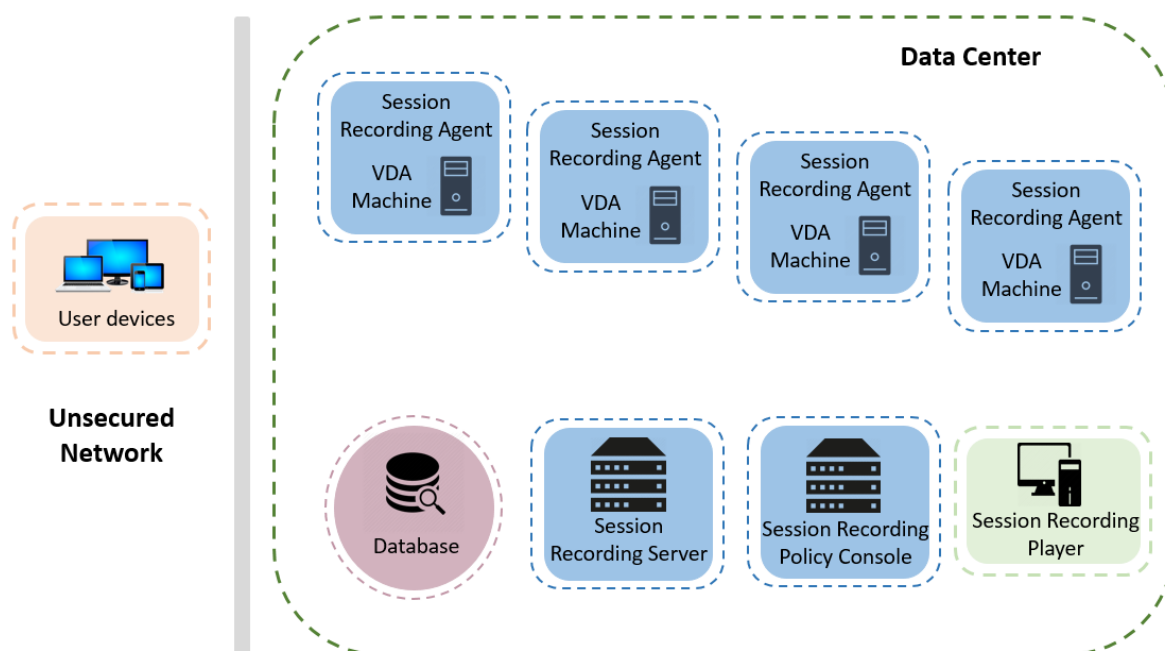
En fonction de votre environnement, vous pouvez déployer les composants d'enregistrement de session selon des scénarios différents.

Un déploiement d'enregistrement de session ne se limite pas nécessairement à un seul site. À l'exception de l'agent d'enregistrement de session, tous les composants sont indépendants du site de serveur. Vous pouvez par exemple configurer plusieurs sites pour utiliser un serveur d'enregistrement de session unique.

Un seul serveur d'enregistrement de session peut être soumis à des demandes de performances élevées. Par exemple, vous pouvez disposer d'un site de grande taille comptant de nombreux agents et prévoir d'enregistrer un grand nombre d'applications au graphisme intensif (applications AutoCAD par exemple). Pour atténuer les problèmes de performances, vous pouvez installer plusieurs serveurs d'enregistrement de session et configurer l'équilibrage de charge.

Suggestion de déploiement d'un site de serveurs

Utilisez ce type de déploiement pour l'enregistrement de sessions pour un ou plusieurs sites. L'agent d'enregistrement de session est installé sur chaque VDA dans un site. Le site réside dans un centre de données protégé par un pare-feu de sécurité. Les composants d'administration de l'enregistrement de session sont installés sur d'autres serveurs et le lecteur d'enregistrement de session est installé sur une station de travail, l'ensemble étant protégé par le pare-feu.



Remarques importantes sur le déploiement

- Pour activer les composants d'enregistrement de session de manière à ce qu'ils communiquent entre eux, installez-les dans le même domaine ou à travers des domaines de confiance. Le système ne peut pas être installé sur un groupe de travail ou à travers des domaines ayant une relation de confiance externe.
- En raison de sa nature graphique intensive et de l'utilisation de mémoire lors de la lecture des enregistrements de grande taille, nous déconseillons d'installer le lecteur d'enregistrement de session en tant qu'application publiée.
- L'installation de l'enregistrement de session est configurée pour la communication TLS/HTTPS. Installez un certificat sur le serveur d'enregistrement de session. Assurez-vous que les composants d'enregistrement de session fassent confiance à l'autorité de certification racine (CA).
- Si vous installez le serveur d'enregistrement de session sur un serveur autonome exécutant SQL Server, activez le protocole TCP/IP et exécutez le service SQL Server Browser. Ces paramètres sont désactivés par défaut, mais vous devez les activer pour que le serveur d'enregistrement de session puisse communiquer avec la base de données. Pour plus d'informations, consultez les articles Microsoft [Activer le protocole réseau TCP/IP pour SQL Server](#) et [SQL Server Browser service](#).
- Considérez les effets du partage de session lors de la planification de votre déploiement d'enregistrement de session. Le partage de session pour les applications publiées peut entrer en conflit avec les règles de stratégie d'enregistrement de session pour les applications publiées. L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'

un utilisateur ouvre. Après que l'utilisateur ouvre la première application, toute application suivante ouverte au cours de la même session continue d'observer la stratégie en vigueur pour la première application. Par exemple, si une stratégie indique que seul Outlook doit être enregistré, l'enregistrement commence lorsque l'utilisateur ouvre Outlook. Si l'utilisateur ouvre ensuite une autre application Microsoft Word publiée (pendant qu'Outlook est ouvert), Word est également enregistré. Inversement, si la stratégie active ne spécifie pas d'enregistrer Word et que l'utilisateur lance Word avant Outlook, Outlook n'est pas enregistré.

- Bien que vous puissiez installer le serveur d'enregistrement de session sur un Delivery Controller, nous ne recommandons pas de le faire en raison de problèmes de performances.
- Vous pouvez installer la console de stratégie d'enregistrement de session sur un Delivery Controller.
- Vous pouvez installer le serveur d'enregistrement de session et la console de stratégie d'enregistrement de session sur le même système.
- Assurez-vous que le nom NetBIOS du serveur d'enregistrement de session ne dépasse pas la limite de 15 caractères. Microsoft limite la longueur du nom d'hôte à 15 caractères.
- PowerShell 5.1 ou version ultérieure est requis pour la journalisation d'événements personnalisée. Mettez à niveau PowerShell si vous installez l'agent d'enregistrement de session sur Windows Server 2012 R2 sur lequel PowerShell 4.0 est installé. Le non-respect de cette consigne peut provoquer l'échec d'appels d'API.

Recommandations de sécurité

February 20, 2024

L'enregistrement de session est déployé au sein d'un réseau sécurisé ; son accès est réservé aux administrateurs et par conséquent il est lui-même sécurisé. Le déploiement prêt à l'emploi est conçu dans un souci de simplicité et les fonctionnalités de sécurité, telles que la signature et le cryptage numériques peuvent être configurés en option.

La communication entre les composants d'enregistrement de session est assurée par les Services Internet (IIS) et Microsoft Message Queuing (MSMQ). IIS fournit la liaison de communication des services Web entre les composants d'enregistrement de session. MSMQ fournit un mécanisme fiable de transport des données pour l'envoi des données de session de l'agent d'enregistrement de session vers le serveur d'enregistrement de session.

Avertissement :

Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de

résoudre les problèmes provenant d'une mauvaise utilisation de l'**Éditeur du Registre**. Vous assumez l'ensemble des risques liés à l'utilisation de l'**Éditeur du Registre**. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Tenez compte des recommandations de sécurité suivantes lors de la planification de votre déploiement :

- Configurez Microsoft Internet Information Services (IIS).

Vous pouvez configurer Enregistrement de session avec une configuration IIS limitée. Sur chaque serveur d'enregistrement de session, ouvrez le Gestionnaire des services Internet (IIS) et définissez les limites de recyclage suivantes pour chaque pool d'applications IIS :

- **Limite de la mémoire virtuelle** : définissez la valeur sur 4 294 967 295.
- **Limite de la mémoire privée** : définissez la valeur sur la mémoire physique du serveur d'enregistrement de session. Par exemple, si la mémoire physique est de 4 Go, définissez la valeur sur 4 194 304.
- **Nombre limite de demandes** : nous vous recommandons de ne pas spécifier ce paramètre. Ou, vous pouvez définir la valeur sur 4 000 000 000.

Conseil :

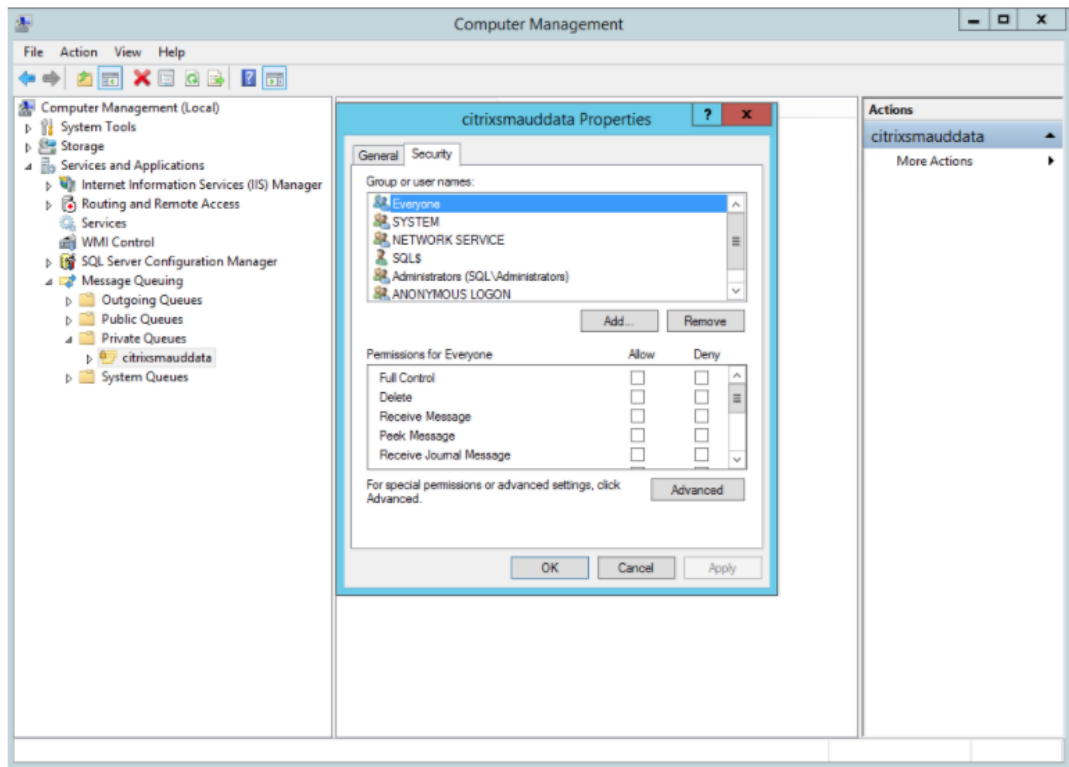
Pour accéder aux paramètres précédents, mettez en surbrillance chaque pool d'applications, sélectionnez **Paramètres avancés** dans le volet **Actions**, puis faites défiler l'écran jusqu'à la section **Recyclage** de la boîte de dialogue **Paramètres avancés**.

- Assurez-vous que vous isolez correctement les différents rôles administrateur dans le réseau de l'entreprise, dans le système d'enregistrement de session ou sur des machines individuelles. Sinon, vous vous exposez à des risques de sécurité qui peuvent avoir un impact sur la fonctionnalité du système ou entraîner une utilisation abusive du système. Nous vous recommandons d'affecter différents rôles d'administrateur à différentes personnes ou comptes. N'accordez pas aux utilisateurs de session générale des privilèges d'administrateur sur le système VDA.
 - N'accordez le rôle d'administrateur local VDA à aucun utilisateur d'applications ou de bureaux publiés. Si le rôle d'administrateur local est requis, protégez les composants de l'agent d'enregistrement de session à l'aide de mécanismes Windows ou de solutions tierces.
 - Attribuez séparément l'administrateur de base de données d'enregistrement de session et l'administrateur de stratégie d'enregistrement de session.
 - N'attribuez pas de privilèges d'administrateur VDA aux utilisateurs de sessions, particulièrement lors de l'utilisation de Remote PC Access.
 - Le compte d'administrateur local de serveur d'enregistrement de session doit être un compte à protection élevée.

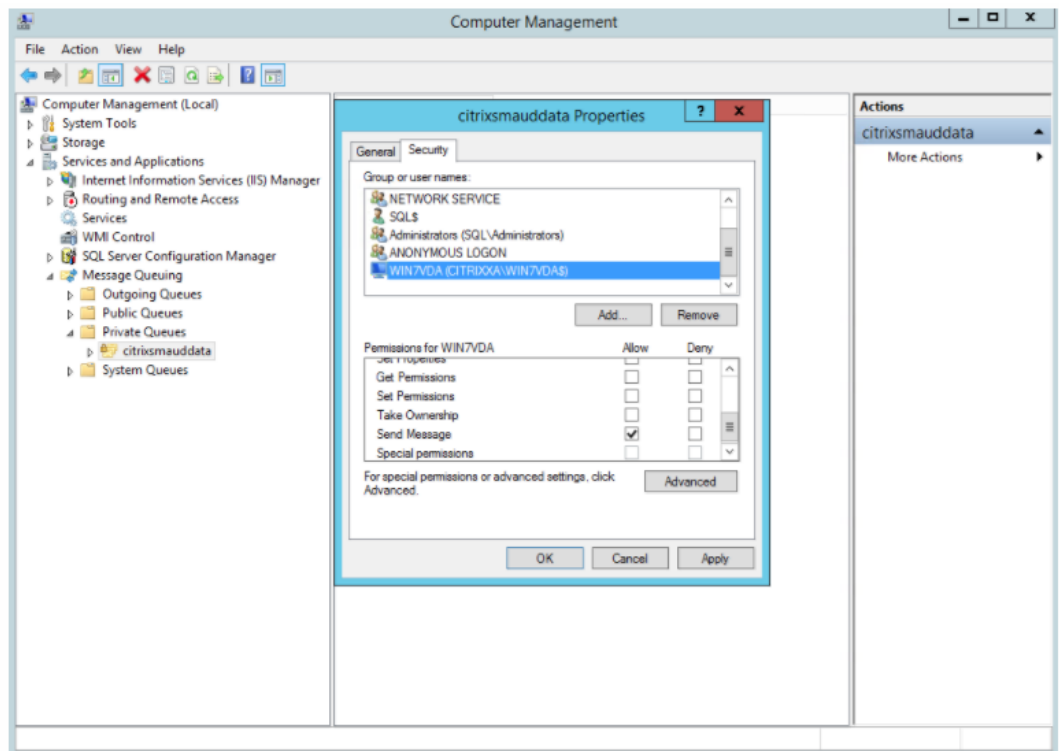
- Contrôlez l'accès aux machines sur lesquelles le lecteur d'enregistrement de session est installé. Si un utilisateur ne dispose pas du rôle Lecteur, n'accordez pas à cet utilisateur le rôle d'administrateur local pour une machine lecteur. Désactivez l'accès anonyme.
 - Nous recommandons d'utiliser une machine physique en tant que serveur de stockage pour l'enregistrement de session.
- L'enregistrement de session enregistre les activités graphiques des sessions sans tenir compte de la confidentialité des données. Dans certaines circonstances, des données sensibles (notamment, mais pas exclusivement, des informations d'identification d'utilisateur, des informations personnelles et des écrans de tierce partie) peuvent être enregistrées involontairement. Prenez les mesures suivantes pour éviter tout risque :
 - Désactivez l'image mémoire principale pour les VDA sauf pour un dépannage spécifique. Pour désactiver l'image mémoire principale :
 1. Cliquez avec le bouton droit sur **Poste de travail**, puis sélectionnez **Propriétés**.
 2. Cliquez sur l'onglet **Avancé**, puis dans la section **Démarrage et récupération**, cliquez sur **Paramètres**.
 3. Sous **Écriture des informations de débogage**, sélectionnez **(aucune)**.
Consultez l'article Microsoft sur <https://support.microsoft.com/en-us/kb/307973>.
 - Les propriétaires de session avertissent les participants que les logiciels de réunion en ligne et d'assistance à distance peuvent être enregistrés si une session de bureau est enregistrée.
 - Assurez-vous que les informations d'identification d'ouverture de session ou les informations personnelles ne s'affichent pas dans les applications locales et Web publiées ou utilisées à l'intérieur de l'entreprise. Sinon elles sont enregistrées par l'enregistrement de session.
 - Fermez toutes les applications qui pourraient exposer des informations confidentielles avant de basculer vers une session ICA distante.
 - Nous vous recommandons d'autoriser uniquement les méthodes d'authentification automatiques (par exemple, l'authentification unique, la carte à puce) pour accéder à des bureaux ou à des applications SaaS publiés.
 - L'enregistrement de session s'appuie sur des matériels et une infrastructure matérielle spécifiques (par exemple, des périphériques de réseau d'entreprise, un système d'exploitation) pour fonctionner correctement et pour satisfaire aux exigences en termes de sécurité. Prenez des mesures aux différents niveaux des infrastructures pour empêcher l'endommagement ou l'abus de ces infrastructures et sécuriser la fonction d'enregistrement de session.
 - Protégez correctement l'infrastructure réseau sur laquelle repose l'enregistrement de session et assurez sa disponibilité.
 - Nous recommandons d'utiliser une solution de sécurité tierce ou un mécanisme Windows pour protéger les composants d'enregistrement de session. Les composants d'

enregistrement de session sont les suivants :

- * Sur le serveur d'enregistrement de session
 - Processus : SsRecStoragemanager.exe et SsRecAnalyticsService.exe
 - Services : CitrixSsRecStorageManager et CitrixSsRecAnalyticsService
 - Tous les fichiers du dossier d'installation du serveur d'enregistrement de session
 - Valeurs de registre dans HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\
- * Sur l'agent d'enregistrement de session
 - Processus : SsRecAgent.exe
 - Service : CitrixSmAudAgent
 - Tous les fichiers du dossier d'installation de l'agent d'enregistrement de session
 - Valeurs de registre sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent
- Définissez la liste de contrôle d'accès (ACL) pour Message Queuing (MSMQ) sur le serveur d'enregistrement de session afin de restreindre les machines VDA ou VDI qui peuvent envoyer des données MSMQ au serveur d'enregistrement de session et empêcher les machines non autorisées d'envoyer des données au serveur d'enregistrement de session.
 1. Installez la fonctionnalité serveur Intégration du service d'annuaire sur chaque serveur d'enregistrement de session et la machine VDA ou VDI sur laquelle l'enregistrement de session est activé. Puis redémarrez le service Message Queuing.
 2. Dans le menu **Démarrer** de Windows sur chaque serveur d'enregistrement de session, ouvrez la fenêtre **Outils d'administration** > **Gestion de l'ordinateur**.
 3. Ouvrez **Services et applications** > **Message Queuing** > **Files d'attente privées**.
 4. Cliquez sur la file d'attente privée **citrixsmduddata** pour ouvrir la page **Propriétés** et sélectionnez l'onglet **Sécurité**.



5. Ajoutez les groupes d'ordinateurs ou les groupes de sécurité des VDA qui envoient des données MSMQ à ce serveur et accordez-leur l'autorisation **Envoyer un message**.



- Protégez correctement le journal d'événements du serveur d'enregistrement de session et des agents d'enregistrement de session. Nous recommandons l'utilisation d'une solution de journalisation à distance Windows ou tierce pour protéger le journal d'événements ou rediriger le journal d'événements vers le serveur distant.
- Veillez à ce que les serveurs exécutant les composants d'enregistrement de session sont physiquement sécurisés. Si possible, verrouillez ces ordinateurs dans une pièce sécurisée dont l'accès direct ne peut être accordé qu'au personnel autorisé.
- Isolez les serveurs exécutant les composants d'enregistrement de session sur un sous-réseau ou domaine séparé.
- Protégez les données de sessions enregistrées des utilisateurs accédant à d'autres serveurs en installant un pare-feu entre le serveur d'enregistrement de session et les autres serveurs.
- Actualisez fréquemment le serveur d'administration de l'enregistrement de sessions et la base de données SQL avec les dernières mises à jour de sécurité de Microsoft.
- Interdisez les non-administrateurs de se connecter à la machine d'administration.
- Limitez strictement les personnels autorisés à modifier les stratégies d'enregistrement et à afficher les sessions enregistrées.
- Installez des certificats numériques, utilisez la fonctionnalité de signature de fichiers d'enregistrement de session et paramétrez les communications TLS dans IIS.
- Configurez MSMQ pour utiliser HTTPS en tant que transport. Pour ce faire, définissez le protocole MSMQ figurant dans **Propriétés de l'Agent d'enregistrement de session** sur HTTPS. Pour obtenir davantage d'informations, veuillez consulter la section [Résolution des problèmes de MSMQ](#).
- Utilisez TLS 1.1 ou TLS 1.2 (recommandé) et désactivez SSLv2, SSLv3, TLS 1.0 sur le serveur d'enregistrement de session et la base de données d'enregistrement de session.
- Désactivez les suites de chiffrement RC4 pour TLS sur le serveur d'enregistrement de session et la base de données d'enregistrement de session.
 1. Dans l'éditeur de stratégie de groupe Microsoft, accédez à **Configuration ordinateur > Modèles d'administration > Réseau > Paramètres de configuration SSL**.
 2. Définissez la stratégie **Ordre des suites de chiffrement SSL politique** sur **Activé**. Par défaut, cette stratégie est définie sur **Non configuré**.
 3. Supprimez toutes les suites de chiffrement RC4.
- Utilisez la fonction Protection de lecture. La fonction Protection de lecture est une fonction de l'enregistrement de session qui crypte des fichiers enregistrés avant de les télécharger sur le lecteur d'enregistrement de session. Par défaut, cette option est activée et se trouve dans les **propriétés du serveur d'enregistrement de session**.

- Suivez les recommandations du NSIT pour la longueur des clés cryptographiques et les algorithmes cryptographiques.
- Configurez la prise en charge de TLS 1.2 pour l'enregistrement de session.

Nous recommandons TLS 1.2 comme protocole de communication pour assurer la sécurité de bout en bout des composants d'enregistrement de session.

Pour configurer la prise en charge TLS 1.2 de l'enregistrement de session :

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session. Installez le composant client et le pilote SQL Server appropriés et définissez une cryptographie forte pour `.NET Framework` (version 4 et ultérieure).
 - a) Installez le pilote Microsoft ODBC 11 (ou une version ultérieure) pour SQL Server.
 - b) Appliquez la dernière correction Hotfix Rollup de `.NET Framework`.
 - c) Installez `ADO.NET - SqlClient` en fonction de votre version de `.NET Framework`. Pour de plus amples informations, consultez <https://support.microsoft.com/en-us/kb/3135244>.
 - d) Ajoutez une valeur `DWORD SchUseStrongCrypto=1` sous `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQL Server\{InstanceName}\Client` et `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NetFramework\v4.0.30319`.
 - e) Redémarrez la machine.
2. Ouvrez une session sur la machine exécutant la console de stratégie d'enregistrement de session. Appliquez le dernier Hotfix Rollup de `.NET Framework` et définissez une cryptographie forte pour `.NET Framework` (version 4 et versions ultérieures). La méthode permettant de définir une cryptographie forte est la même que celle décrite dans les sous-étapes 1–4 et 1–5. Il n'est pas nécessaire d'effectuer ces étapes si vous choisissez d'installer la console de stratégie d'enregistrement de session sur le même ordinateur que le serveur d'enregistrement de session.

Pour configurer la prise en charge TLS 1.2 de SQL Server avec les versions antérieures à 2016, consultez <https://support.microsoft.com/en-us/kb/3135244>. Pour utiliser TLS 1.2, configurez HTTPS comme protocole de communication pour les composants d'enregistrement de session.

Considérations sur la capacité à monter en charge

February 20, 2024

L'enregistrement de session est un système hautement évolutif qui gère des milliers, voire des dizaines de milliers de sessions. L'installation et l'exécution de l'enregistrement de session nécessitent quelques ressources supplémentaires au-delà des éléments de base nécessaires à l'exécution de Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops

Service). Cependant, nous vous recommandons toujours de prendre en compte les performances de votre système si vous prévoyez d'enregistrer un grand nombre de sessions. Les sessions que vous prévoyez d'enregistrer peuvent également produire des fichiers de session volumineux (par exemple, des applications exigeant d'importantes ressources graphiques).

Cet article explique comment vous pouvez optimiser la capacité à monter en charge de l'enregistrement de session et comment vous pouvez tirer le meilleur parti de votre système d'enregistrement à moindre coût.

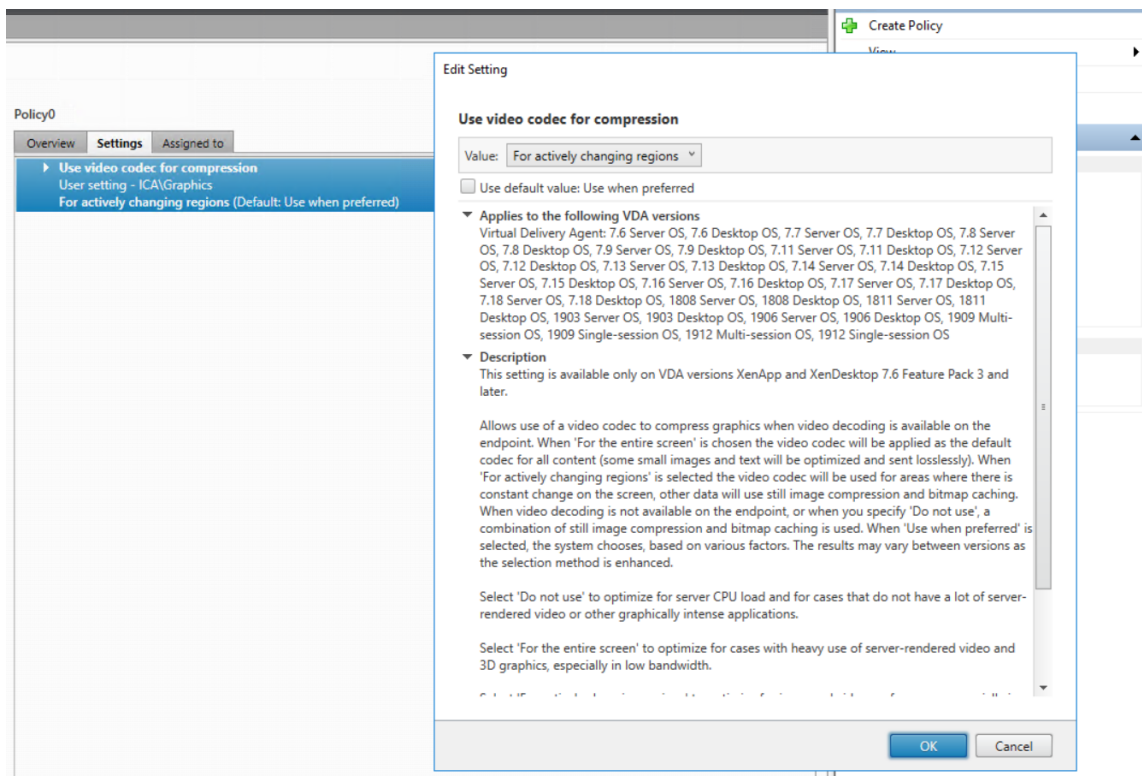
Capacité à monter en charge de l'enregistrement de session

Il y a deux raisons principales pour lesquelles l'enregistrement de session est plus performant que les produits concurrents :

- Taille des fichiers

Un fichier de session enregistrée créé avec l'enregistrement de session est très compact. Il est beaucoup plus petit qu'un enregistrement vidéo équivalent effectué avec des solutions de capture de données d'écran. La bande passante réseau, l'espace disque et le nombre d'E/S par seconde de disque nécessaires au transport et au stockage de chaque fichier de session enregistrée sont généralement au moins 10 fois inférieur qu'avec un fichier vidéo équivalent.

La petite taille des fichiers de sessions enregistrées permet un rendu plus rapide et plus fluide des images vidéo. Les enregistrements sont également sans aucune perte et ne présentent pas la pixelisation souvent observée dans la plupart des formats vidéo compacts. Le texte des enregistrements est aussi facile à lire que pendant les sessions d'origine. Pour obtenir des fichiers de petite taille, l'enregistrement de session n'enregistre pas les trames clés à l'intérieur des fichiers. L'enregistrement de session peut ignorer les paquets H.264 lors de l'enregistrement de sessions qui ont des vidéos en cours d'exécution et ainsi réduire la taille des fichiers d'enregistrement. Pour utiliser cette fonctionnalité, définissez `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\DropH264Enabled` sur 1 sur l'agent d'enregistrement de session et définissez la valeur **Utiliser codec vidéo pour la compression** sur **Pour les zones changeant constamment**.



- Faible traitement requis pour générer des fichiers

Un fichier de session enregistrée contient les données du protocole ICA d'une session, extraites virtuellement dans leur format natif. Le fichier capture le flux de données du protocole ICA utilisé pour communiquer avec l'application Citrix Workspace. Il n'est pas nécessaire d'exécuter des composants logiciels coûteux de transcodage ou d'encodage pour modifier le format des données en temps réel. La faible quantité de traitement est également importante pour la capacité à monter en charge du VDA et garantit que l'expérience de l'utilisateur final reste satisfaisante lorsque de nombreuses sessions sont enregistrées à partir du même VDA.

De plus, seuls les canaux virtuels ICA qui peuvent être lus sont enregistrés, ce qui est un facteur d'optimisation supplémentaire. Par exemple, les canaux de mappage des imprimantes et des lecteurs clients ne sont pas enregistrés car ils peuvent générer des volumes élevés de données sans bénéfice pour la lecture vidéo.

Estimer les taux d'entrée et de traitement des données

Le serveur d'enregistrement de session est le point central de collecte des fichiers de sessions enregistrées. Chaque ordinateur qui exécute un VDA avec OS multi-session alors que l'enregistrement de session est activé envoie des données de sessions enregistrées au serveur d'enregistrement de session. L'enregistrement de session peut gérer des volumes élevés de données et tolérer les rafales et les défaillances, mais il existe des limites physiques quant à la quantité de données qu'un serveur

peut gérer.

Considérez le volume de données que vous envoyez à chaque serveur d'enregistrement de session et la rapidité des délais de traitement et de stockage de ces données par les serveurs. Le taux auquel votre système peut stocker les données entrantes doit être supérieur au taux d'entrée des données.

Pour estimer votre taux d'entrée de données, effectuez le calcul suivant :

1. Multipliez le nombre de sessions enregistrées par la taille moyenne des sessions.
2. Divisez le produit par la durée d'enregistrement des sessions.

Par exemple, vous pouvez enregistrer 5 000 sessions Microsoft Outlook de 20 Mo chacune sur une durée de 8 heures par jour ouvrable. Dans ce cas, le taux d'entrée des données est d'environ 3,5 Mbit/s (5 000 sessions x 20 Mo, divisé par 8 heures, divisé par 3 600 secondes par heure). Un serveur d'enregistrement de session standard connecté à un réseau local de 100 Mbit/s avec suffisamment d'espace disque pour stocker les données enregistrées peut traiter les données à une vitesse d'environ 5,0 Mbit/s. Ce taux correspond au taux de traitement en fonction des limites physiques imposées par le nombre d'E/S par seconde sur le disque et le réseau. Dans l'exemple, le taux de traitement (5,0 Mbit/s) est supérieur au taux d'entrée (3,5 Mbit/s), ce qui rend possible l'enregistrement des 5 000 sessions Outlook.

La quantité de données par session varie considérablement en fonction de ce qui est enregistré. D'autres facteurs tels que la résolution de l'écran, la profondeur des couleurs et le mode graphique ont également un impact. Une session dans laquelle une application CAO est en cours d'exécution génère probablement un enregistrement beaucoup plus important qu'une session au cours de laquelle l'utilisateur envoie et reçoit des e-mails dans Outlook. Par conséquent, l'enregistrement du même nombre de sessions CAO peut générer un taux d'entrée élevé et nécessiter l'utilisation d'un plus grand nombre de serveurs d'enregistrement de session.

Rafales et défaillances

L'exemple précédent suppose un débit uniforme simple de données, mais n'explique pas comment le système traite de courtes périodes d'activité plus élevée, appelées rafales. Une rafale peut se produire lorsque tous les utilisateurs se connectent à la même heure le matin, appelée la pointe de 9 heures, ou lorsqu'ils reçoivent le même courrier électronique simultanément dans leur boîte de réception Outlook. Le taux de traitement de 5,0 Mbit/s du serveur d'enregistrement de session est très insuffisant pour faire face à cette demande soudaine.

L'agent d'enregistrement de session s'exécutant sur chaque VDA utilise Microsoft Message Queuing (MSMQ) pour envoyer des données enregistrées au Gestionnaire de stockage s'exécutant sur le serveur central d'enregistrement de session. Les données sont envoyées selon une méthode de stockage et de transfert similaire à la manière dont un e-mail est transmis entre l'expéditeur, le serveur de messagerie et le destinataire. Si le serveur d'enregistrement de session ou le réseau

ne peut pas gérer le taux élevé de données dans une rafale, les données enregistrées sont temporairement stockées. Le message de données peut être stocké temporairement dans la file d'attente sortante sur le VDA si le réseau est encombré. Il se peut également que les données aient traversé le réseau mais que le Gestionnaire de stockage soit toujours occupé à traiter d'autres messages. Dans ce cas, le message de données est stocké dans la file d'attente de réception du serveur d'enregistrement de session.

MSMQ sert également de mécanisme de tolérance aux pannes. Si le serveur d'enregistrement de session tombe en panne ou si la liaison est interrompue, les données enregistrées sont conservées dans la file d'attente sortante de chaque VDA. Lorsque la défaillance est résolue, toutes les données mises en file d'attente sont envoyées ensemble. L'utilisation de MSMQ vous permet également de mettre un serveur hors connexion pour la mise à niveau ou la maintenance sans interrompre l'enregistrement de session ni perdre de données.

La principale limitation de MSMQ est que l'espace disque pour le stockage temporaire des messages de données n'est pas infini. Cette limitation limite le temps que peut durer une rafale, une défaillance ou un événement de maintenance avant que les données ne soient perdues. Le système global peut continuer après la perte de données, mais dans ce cas, des morceaux de données manquent dans les enregistrements individuels. Un fichier avec des données manquantes est toujours lisible, mais seulement jusqu'au point où les données ont été perdues. Tenez compte de ce qui suit :

- L'ajout d'espace disque à chaque serveur, en particulier au serveur d'enregistrement de session, et sa mise à disposition pour MSMQ peuvent augmenter la tolérance aux rafales et aux défaillances.
- Il est important de configurer le paramètre Durée de validité des messages pour chaque agent d'enregistrement de session sur un niveau approprié (sous l'onglet **Connexions** dans Propriétés de l'Agent d'enregistrement de session). La valeur par défaut est 7 200 secondes (deux heures). Cela signifie que chaque message de données enregistré dispose de deux heures pour atteindre le Gestionnaire de stockage avant qu'il ne soit ignoré et que les fichiers d'enregistrement soient endommagés. Avec plus d'espace disque disponible (ou moins de sessions à enregistrer), vous pouvez choisir d'augmenter cette valeur. La valeur maximale est 365 jours.

Autre limitation de MSMQ : lorsque les données en attente s'accumulent, un nombre d'E/S par seconde supplémentaire est nécessaire dans la file d'attente pour lire et écrire les messages de données. Dans des conditions normales, le Gestionnaire de stockage reçoit et traite les données du réseau directement sans que le message de données soit écrit sur le disque. Le stockage des données implique une seule opération d'écriture sur le disque qui ajoute le fichier de session enregistrée. Lorsque les données s'accumulent, le nombre d'E/S par seconde du disque triple : chaque message doit être écrit sur le disque, lu sur le disque et écrit dans un fichier. Le Gestionnaire de stockage étant fortement lié aux E/S par seconde, le taux de traitement du serveur d'enregistrement de session diminue jusqu'à ce que la file d'attente des messages soit vide. Pour atténuer les effets de ces E/S par seconde supplémentaires, adoptez les recommandations suivantes :

- Assurez-vous que le disque sur lequel MSMQ stocke les messages est différent des dossiers de stockage de fichiers d'enregistrement. Même si le trafic des bus E/S par seconde triple, la baisse du taux de traitement réel n'est jamais aussi forte.
- Planifiez les arrêts aux heures creuses seulement. Si votre budget vous le permet, suivez des approches courantes pour créer des serveurs à haute disponibilité. Ces approches incluent l'utilisation d'UPS (Uninterruptible Power Supply), de cartes réseau doubles, de commutateurs redondants, de mémoire et de disques remplaçables à chaud.

Prévoir la capacité de réserve

Il est peu probable que le taux de données des sessions enregistrées soit uniforme, des rafales et des défaillances peuvent se produire, et le traitement des messages en attente consomme beaucoup d'E/S par seconde. Pour cette raison, concevez chaque serveur d'enregistrement de session avec beaucoup de capacité de réserve. Ajoutez d'autres serveurs ou améliorez la spécification des serveurs existants, comme décrit dans les sections suivantes, pour une capacité supplémentaire. La règle générale consiste à exécuter chaque serveur d'enregistrement de session à un maximum de 50 % de sa capacité totale. Dans l'exemple précédent, si le serveur est capable de traiter 5,0 Mbit/s, configurez le système pour qu'il s'exécute uniquement à 2,5 Mbit/s. Au lieu d'enregistrer 5 000 sessions Outlook qui génèrent 3,5 Mbit/s sur un serveur d'enregistrement de session, réduisez ce nombre à 3 500 sessions qui génèrent seulement 2,5 Mbit/s.

Files d'attente et lecture active

Un réviseur peut ouvrir un enregistrement de session pour le lire alors que la session est toujours active, cela s'appelle la lecture active. Pendant la lecture active, l'agent d'enregistrement de session responsable de la session passe en mode streaming pour cette session. Les données d'enregistrement sont immédiatement envoyées au Gestionnaire de stockage sans mise en mémoire tampon interne. Étant donné que le fichier d'enregistrement est constamment mis à jour, le lecteur peut continuer à être alimenté avec les dernières données de la session active. Toutefois, les données envoyées par l'agent au Gestionnaire de stockage le sont via MSMQ, donc les règles de mise en file d'attente décrites précédemment s'appliquent. Un problème peut se produire dans ce scénario. Lorsque MSMQ accumule un retard, les nouvelles données enregistrées disponibles pour la lecture active sont mises en file d'attente comme tous les autres messages de données. Le réviseur peut toujours lire le fichier, mais l'affichage des dernières données enregistrées en direct est retardé. Si la lecture active est une fonctionnalité importante pour les réviseurs, minimisez la probabilité de retard. Vous pouvez concevoir une capacité de réserve et une tolérance aux pannes dans votre déploiement.

Scalabilité du système

L'enregistrement de session ne réduit jamais les performances de session et n'arrête jamais les sessions en réponse à des retards de données enregistrées. Il est primordial de préserver l'expérience utilisateur final et la capacité à monter en charge d'un seul serveur lors de la conception du système d'enregistrement de session. Si le système d'enregistrement devient surchargé de façon irréversible, les données de session enregistrées sont supprimées. L'impact de l'enregistrement des sessions ICA sur les performances et la capacité à monter en charge des VDA est faible. L'importance de l'impact dépend de la plate-forme, de la mémoire disponible et de la nature graphique des sessions enregistrées. Avec la configuration suivante, vous pouvez vous attendre à un impact de 1 % à 5 % sur la capacité à monter en charge d'un serveur unique. En d'autres termes, si un serveur peut héberger 100 utilisateurs sans que l'enregistrement de session soit installé, il peut héberger 95 à 99 utilisateurs après l'installation :

- Serveur 64 bits avec 8 Go de RAM exécutant un VDA avec OS multi-session
- Toutes les sessions exécutant des applications de productivité Office, telles que Outlook et Excel
- L'utilisation des applications est active et soutenue
- Toutes les sessions sont enregistrées selon la configuration des stratégies d'enregistrement de session

Si moins de sessions sont enregistrées ou si l'activité est moins soutenue et plus sporadique, l'impact est moindre. Dans de nombreux cas, l'impact sur la capacité à monter en charge est négligeable et la densité utilisateur par serveur reste la même. Comme mentionné précédemment, le faible impact est dû aux exigences de traitement simples des composants d'enregistrement de session sur chaque VDA. Les données enregistrées sont extraites de la pile de sessions ICA et envoyées telles quelles au serveur d'enregistrement de session via MSMQ. Il n'y a pas de codage coûteux des données.

Il y a une surcharge mineure de l'utilisation de l'enregistrement de session même lorsqu'aucune session n'est enregistrée. Si vous n'allez pas enregistrer de session à partir d'un serveur particulier, vous pouvez désactiver l'enregistrement sur ce serveur. La suppression de l'enregistrement de session est une façon de procéder. Une approche moins invasive consiste à désactiver la case à cocher **Activer l'enregistrement de session pour cette machine VDA** sous l'onglet **Enregistrement de session** dans **Propriétés de l'Agent d'enregistrement de session**. Si l'enregistrement de session est nécessaire à l'avenir, réactivez cette case à cocher.

Mesure du débit

Vous pouvez mesurer le débit des données de session enregistrées depuis le VDA d'envoi vers le serveur d'enregistrement de session de réception. Une approche simple et efficace consiste à observer la taille des fichiers d'enregistrement et la fréquence à laquelle l'espace disque sur le serveur d'enregistrement de session est consommé. Le volume de données écrites sur le disque reflète

étroitement le volume de trafic réseau généré. L'Analyseur de performances Windows (perfmon.exe) propose des compteurs système standard qui peuvent être observés en plus de certains compteurs fournis par l'enregistrement de session. Les compteurs peuvent être utilisés pour mesurer le débit et identifier les goulots d'étranglement et les problèmes de système. Le tableau suivant présente certains des compteurs de performances les plus utiles.

Objet de performance	Nom du compteur	Description
Agent d'enregistrement de session Citrix	Active Recording Count	Nombre de sessions en cours d'enregistrement sur un VDA particulier.
Agent d'enregistrement de session Citrix	Bytes read from the Session Recording Driver	Nombre d'octets lus à partir des composants du noyau responsables de l'acquisition des données de session. Utile pour déterminer la quantité de données générée par un seul VDA pour toutes les sessions enregistrées sur ce serveur.
Gestionnaire de stockage d'enregistrement de session Citrix	Active Recording Count	Similaire au compteur Agent d'enregistrement de session Citrix, à l'exception du serveur d'enregistrement de session. Indique le nombre total de sessions en cours d'enregistrement pour tous les serveurs.
Gestionnaire de stockage d'enregistrement de session Citrix	Message bytes/sec	Débit de toutes les sessions enregistrées. Peut être utilisé pour déterminer le taux de traitement des données par le gestionnaire de stockage. Si MSMQ a accumulé les messages en file d'attente, le Gestionnaire de stockage s'exécute à pleine vitesse. Cette valeur peut être utilisée pour indiquer le taux de traitement maximal du Gestionnaire de stockage.

Objet de performance	Nom du compteur	Description
Disque LogicalDisk	Disk Write Bytes/sec	Peut être utilisé pour mesurer les performances d'écriture sur disque. Ceci est important pour que le serveur d'enregistrement de session puisse atteindre une capacité à monter en charge élevée. Les performances des lecteurs individuels peuvent également être observées.
File d'attente MSMQ	Bytes in Queue	Peut être utilisé pour déterminer la quantité de données en attente dans la file de messages CitrixSmAudData. Si cette valeur augmente au fil du temps, le taux de données enregistrées reçues depuis le réseau est supérieur à celui auquel le gestionnaire de stockage peut traiter les données. Ce compteur est utile pour observer l'effet des rafales de données et des défaillances.
File d'attente MSMQ	Message in Queue	Similaire au compteur Octets dans la file d'attente, mais mesure le nombre de messages.

Objet de performance	Nom du compteur	Description
Interface réseau	Bytes Total/sec	Peut être utilisé pour mesurer les deux côtés du lien pour observer la quantité de données générées lors de l'enregistrement des sessions. Lorsqu'il est mesuré sur le serveur d'enregistrement de session, ce compteur indique le taux de réception des données entrantes. Différent du compteur Gestionnaire de stockage d'enregistrement de session Citrix Message bytes/sec qui mesure le taux de traitement des données. Si le débit du réseau est supérieur à cette valeur, les messages s'accumulent dans la file d'attente des messages.
Processeur	% Processor Time	Il peut être utile de le surveiller même si le processeur est peu susceptible d'être un goulot d'étranglement.

Matériel du serveur d'enregistrement de session

Vous pouvez augmenter la capacité de votre déploiement en sélectionnant soigneusement le matériel du serveur d'enregistrement de session. Vous avez deux choix : mettre à niveau (en augmentant la capacité de chaque serveur) ou monter en charge (en ajoutant plus de serveurs). En faisant l'un ou l'autre des choix, votre objectif est d'augmenter la capacité à monter en charge au moindre coût.

Augmentation de la capacité

Si vous envisagez un serveur d'enregistrement de session unique, tenez compte des meilleures pratiques suivantes pour garantir des performances optimales selon le budget disponible. Le système

dépend des opérations d'E/S par seconde qui peuvent garantir un débit élevé de données enregistrées depuis le réseau sur le disque. Il est donc important d'investir dans le matériel de réseau et de disque approprié. Pour un serveur d'enregistrement de session hautes performances, un processeur double ou double cœur est recommandé, mais une spécification plus élevée n'a pas beaucoup d'intérêt. L'architecture de processeur 64 bits est recommandée, mais un type de processeur x86 convient également. 4 Go de RAM est recommandé mais encore une fois, il y a peu d'avantages à en ajouter plus.

Montée en charge

Même avec les meilleures pratiques de montée en charge, il existe des limites de performances et de capacité avec un seul serveur d'enregistrement de session lors de l'enregistrement d'un grand nombre de sessions. Il peut être nécessaire d'ajouter des serveurs supplémentaires pour faire face à la charge. Vous pouvez installer des serveurs d'enregistrement de session supplémentaires sur des ordinateurs différents de manière à ce que les serveurs d'enregistrement de session fonctionnent en tant que pool d'équilibrage de charge. Dans ce type de déploiement, les serveurs d'enregistrement de session partagent le stockage et la base de données. Pour répartir la charge, dirigez les agents d'enregistrement de session vers l'équilibreur de charge responsable de la répartition de la charge de travail.

Capacité du réseau

Une liaison réseau de 100 Mbps convient aux connexions à un serveur d'enregistrement de session. Une connexion Ethernet en Gb peut améliorer les performances, mais ne se traduira pas par des performances de dix fois supérieures à une liaison 100 Mbit/s. En pratique, le gain de débit est moindre.

Veillez à ce que les commutateurs réseau utilisés par l'enregistrement de session ne soient pas partagés avec des applications tierces qui pourraient lui disputer la bande passante réseau disponible. Dans le meilleur des cas, les commutateurs réseau sont dédiés au serveur d'enregistrement de session. Si la congestion du réseau s'avère être le goulot d'étranglement, une mise à niveau du réseau est un moyen relativement peu coûteux d'augmenter la capacité à monter en charge du système.

Stockage

Investir dans du matériel de disque et de stockage est le facteur le plus important de la capacité à monter en charge des serveurs. Plus vite les données peuvent être écrites sur disques, plus élevées sont les performances du système dans son ensemble. Lorsque vous sélectionnez une solution de stockage, donnez priorité aux performances d'écriture plutôt qu'aux performances de lecture.

Stockez les données sur un contrôleur RAID ou un réseau SAN.

Remarque :

Le stockage des données sur un serveur NAS basé sur des protocoles basés sur des fichiers tels que SMB et NFS, peut avoir d'importantes répercussions sur les performances et la sécurité. Utilisez la dernière version du protocole pour éviter toute incidence sur la sécurité et effectuez des tests de scalabilité pour garantir des performances adéquates.

Pour une configuration de lecteur local, recherchez un contrôleur de disque avec mémoire cache intégré. La mise en cache permet au contrôleur d'utiliser le tri en ascenseur pendant la réécriture. Cela permet de minimiser le mouvement de la tête de disque et garantit que les opérations d'écriture sont terminées sans attendre la fin de l'opération du disque physique. Cela peut améliorer considérablement les performances d'écriture à un coût supplémentaire minimale. La mise en cache soulève cependant le problème de la perte de données après une panne de courant. Pour garantir l'intégrité des données et du système de fichiers, envisagez d'utiliser une fonction de sauvegarde sur batterie pour le contrôleur de disque de mise en cache.

Envisagez d'utiliser une solution de stockage RAID appropriée. De nombreux niveaux de RAID sont disponibles en fonction de vos exigences en matière de performances et de redondance. Le tableau suivant spécifie chacun des niveaux de RAID et la manière dont chaque norme est applicable à l'enregistrement de session.

Niveau de RAID	Type	Nombre minimal de disques	Description
RAID 0	Volume agrégé par bandes sans parité	2	Fournit des performances élevées mais pas de redondance. La perte de tout disque détruit la grappe. RAID 0 est une solution peu coûteuse permettant de stocker des fichiers de sessions enregistrées où l'impact de la perte de données est faible. Facile d'augmenter la capacité des performances en ajoutant plus de disques.
RAID 1	Disques en miroir sans parité	2	Aucun gain de performances sur un seul disque, ce qui en fait une solution relativement coûteuse. Utilisez cette solution uniquement si un niveau élevé de redondance est requis.

Niveau de RAID	Type	Nombre minimal de disques	Description
RAID 3	Volume agrégé par bandes avec parité dédiée	3	Fournit des performances d'écriture élevées avec des caractéristiques de redondance similaires à RAID 5. RAID 3 est recommandé pour les applications de production vidéo et de diffusion en direct. L'enregistrement de session correspondant à ce type d'application, le RAID 3 est fortement recommandé, mais il n'est pas courant.

Niveau de RAID	Type	Nombre minimal de disques	Description
RAID 5	Volume agrégé par bandes avec parité distribuée	3	Fournit des performances de lecture élevées avec redondance, mais au détriment de performances d'écriture plus lentes. RAID 5 est l'option la plus courante pour les usages d'ordre général. Mais en raison de la lenteur des performances d'écriture, RAID 5 n'est pas recommandé pour l'enregistrement de session. RAID 3 peut être déployé à un coût similaire, mais avec de meilleures performances d'écriture.
RAID 10	Volume en miroir et volume agrégé par bandes	4	Fournit les caractéristiques de performance du RAID 0 avec les avantages de redondance du RAID 1. Une solution coûteuse qui n'est pas recommandée pour l'enregistrement de session.

RAID 0 et RAID 3 sont les niveaux de RAID les plus recommandés. RAID 1 et RAID 5 sont des normes populaires, mais ne sont pas recommandés pour l'enregistrement de session. RAID 10 offre certains avantages en termes de performances, mais il est trop coûteux pour le gain supplémentaire.

Décidez du type et de la spécification des unités de disque. Les lecteurs IDE/ATA et les lecteurs USB ou Firewire externes ne conviennent pas à l'enregistrement de session. Vous avez principalement le choix entre SATA et SCSI. Les disques SATA offrent des débits de transfert raisonnablement élevés à un coût par Mo réduit par rapport aux disques SCSI. Toutefois, les disques SCSI offrent de meilleures performances et sont plus courants dans les déploiements de serveurs. Les solutions RAID de serveur prennent principalement en charge les disques SCSI, mais certains produits RAID SATA sont maintenant disponibles. Lors de l'évaluation des spécifications des produits d'unités de disque, tenez compte de la vitesse de rotation du disque et d'autres caractéristiques de performance.

Étant donné que l'enregistrement de milliers de sessions par jour peut consommer beaucoup d'espace disque, vous devez choisir entre la capacité globale et les performances. Dans l'exemple précédent, l'enregistrement de 5 000 sessions Outlook sur une journée de travail de 8 heures consomme environ 100 Go d'espace de stockage. Pour stocker 10 jours d'enregistrements (c'est-à-dire 50 000 fichiers de sessions enregistrées), vous avez besoin de 1 000 Go (1 To). Vous pouvez atténuer cette pression sur l'espace disque en raccourcissant la période de rétention avant l'archivage ou la suppression d'anciens enregistrements. Si 1 To d'espace disque est disponible, une période de rétention de sept jours est raisonnable, cela garantit que l'utilisation de l'espace disque reste autour de 700 Go, avec 300 Go restant en mémoire tampon pour les jours plus intenses. Dans l'enregistrement de session, l'archivage et la suppression des fichiers sont pris en charge avec l'utilitaire ICLDB. Ces fonctions ont une période de conservation minimale de deux jours. Vous pouvez planifier une tâche en arrière-plan pour qu'elle s'exécute une fois par jour à une heure creuse. Pour plus d'informations sur les commandes **ICLDB** et l'archivage, reportez-vous à la section [Gérer vos enregistrements de base de données](#).

L'alternative à l'utilisation d'un lecteur local et de contrôleurs consiste à utiliser une solution de stockage SAN basée sur l'accès au disque au niveau du bloc. Sur le serveur d'enregistrement de session, la grappe de disques apparaît en tant que lecteur local. La configuration des SAN est plus coûteuse, mais à mesure que la grappe de disques est partagée, les SAN présentent l'avantage d'une gestion simplifiée et centralisée. Il existe deux principaux types de SAN : Fibre Channel et iSCSI. iSCSI est essentiellement SCSI sur TCP/IP et gagne en popularité par rapport à Fibre Channel depuis l'introduction de Gb Ethernet.

Capacité à monter en charge de la base de données

Le volume de données envoyées à la base de données d'enregistrement de session est minime car celle-ci ne stocke que les métadonnées sur les sessions enregistrées. Pour leur part, les fichiers des sessions enregistrées sont inscrits sur un autre disque. Généralement, chaque session enregistrée ne nécessite qu'environ 1 Ko d'espace dans la base de données, à moins que l'API d'événements de l'enregistrement de session soit utilisé pour insérer des événements avec possibilité de recherche dans la session.

Les éditions Express de Microsoft SQL Server 2019, Microsoft SQL Server 2017, Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012 et Microsoft SQL Server 2008 R2 imposent une limite de taille de base de données de 10 Go. À 1 Ko par session d'enregistrement, la base de données peut cataloguer environ 4 000 000 sessions. D'autres éditions de Microsoft SQL Server n'ont pas de restrictions de taille de base de données et ne sont limitées que par la quantité d'espace disque disponible. À mesure que le nombre de sessions augmente dans la base de données, les performances de la base de données et la vitesse des recherches ne diminuent que faiblement.

Si vous ne faites pas de personnalisations par le biais de l'[API d'événements de l'enregistrement de session](#), chaque session enregistrée génère quatre transactions sur la base de données : deux au démarrage de l'enregistrement, une lorsque l'utilisateur se connecte aux sessions actuellement enregistrées et une à l'arrêt de l'enregistrement. Si vous utilisez l'API d'événements de l'enregistrement de session pour personnaliser des sessions, chaque événement avec possibilité de recherche enregistré génère une transaction. Puisque même le déploiement de base de données le plus élémentaire est en mesure de traiter des centaines de transactions par seconde, la charge de traitement sur la base de données n'est pas considérée comme étant excessivement sollicitée. L'impact est assez minime pour que la base de données d'enregistrement de session puisse s'exécuter sur le même serveur SQL que d'autres bases de données, notamment la base de données du magasin central de Citrix Virtual Apps and Desktops.

Si votre déploiement d'enregistrement de session nécessite de cataloguer plusieurs millions de sessions enregistrées dans la base de données, suivez les consignes de Microsoft pour la montée en charge de SQL Server.

Installer, mettre à niveau et désinstaller

February 20, 2024

Remarque :

Pour configurer la haute disponibilité du serveur via l'équilibrage de charge, consultez la section [Configurer l'équilibrage de charge dans un déploiement existant](#) et [Déployer et équilibrer la charge de l'enregistrement de session sur Azure](#).

Cet article comprend les sections suivantes :

- [Check-list d'installation](#)
- [Utiliser des scripts Citrix pour installer les rôles et fonctionnalités Windows requis](#)
- [Installer les composants de l'administration de l'enregistrement de session](#)
 - [Installer la base de données d'enregistrement de session](#)

- [Installer le serveur d'enregistrement de session](#)
- [Installer l'agent d'enregistrement de session](#)
- [Installer le lecteur d'enregistrement de session et le lecteur Web](#)
- [Automatiser l'installation](#)
- [Mettre à niveau l'enregistrement de session](#)
- [Désinstaller l'enregistrement de session](#)
- [Intégrer à Citrix Analytics for Security](#)

Check-list d'installation

Vous installez les composants d'enregistrement de session à l'aide des fichiers suivants :

- [Broker_PowerShellSnapIn_x64.msi](#)
- [SessionRecordingAdministrationx64.msi](#)
- [SessionRecordingAgentx64.msi](#)
- [SessionRecordingPlayer.msi](#)
- [SessionRecordingWebPlayer.msi](#)

Avant de commencer l'installation, effectuez les tâches de cette liste :

☒	Étape
	<p>Installez les composants requis avant de commencer l'installation. Consultez Configuration système requise et Utiliser des scripts Citrix pour installer les rôles et fonctionnalités Windows requis.</p> <p>Sélectionnez les machines sur lesquelles vous souhaitez installer chaque composant de l'enregistrement de session. Veillez à ce que chaque machine soit conforme aux configurations matérielles et logicielles requises correspondant aux composants à y installer.</p>

☒	Étape
	<p>Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de Citrix Virtual Apps and Desktops et télécharger le fichier du produit. Décompressez le fichier.</p> <p>Pour utiliser le protocole TLS pour les communications entre les composants de l'enregistrement de session, installez les certificats corrects dans votre environnement. Installez toute correction requise pour les composants de l'enregistrement de session. Les corrections sont disponibles auprès du support de Citrix.</p> <p>Configurez Director pour créer et activer des stratégies d'enregistrement de session. Pour de plus amples informations, consultez Configurer Director pour utiliser le serveur d'enregistrement de session.</p>

Remarque :

- Nous vous recommandons de séparer les applications publiées dans des groupes de mise à disposition distincts en fonction des stratégies d'enregistrement. Le partage de session pour les applications publiées peut entrer en conflit avec la stratégie active si elles se trouvent dans le même groupe de mise à disposition. L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre. À compter de la version 7.18, vous pouvez utiliser la fonction d'enregistrement de session dynamique pour démarrer ou arrêter l'enregistrement des sessions à tout moment au cours des sessions. Pour plus d'informations, veuillez consulter la section [Enregistrement de session dynamique](#).
- Si vous prévoyez d'utiliser Machine Creation Services (MCS) ou Citrix Provisioning, préparez une [QMID](#) unique. Si vous ne respectez pas cette consigne, des données d'enregistrement peuvent être perdues.
- SQL Server requiert que TCP/IP soit activé, que le service SQL Server Browser soit exécuté et que l'authentification Windows soit utilisée.
- Pour utiliser HTTPS, configurez des certificats de serveur pour TLS/HTTPS.
- Assurez-vous que les utilisateurs sous `Local Users and Groups > Groups >`

Users disposent d'une autorisation d'écriture dans le dossier C:\windows\Temp.

Utiliser des scripts Citrix pour installer les rôles et fonctionnalités Windows requis

Pour que l'enregistrement de session fonctionne correctement, utilisez les scripts Citrix suivants pour installer les rôles et fonctionnalités Windows nécessaires avant d'installer l'enregistrement de session :

- InstallPrereqsforSessionRecordingAdministration.ps1

```
1 <#
2 .Synopsis
3     Installs Prereqs for Session Recording Administration
4 .Description
5     Supports Windows Server 2022, Windows Server 2019 and Windows
6     Server 2016.
7     Install below windows feature on this machine:
8     -Application Development
9     -Security - Windows Authentication
10    -Management Tools - IIS 6 Management Compatibility
11        IIS 6 Metabase Compatibility
12        IIS 6 WMI Compatibility
13        IIS 6 Scripting Tools
14        IIS 6 Management Console
15    -Microsoft Message Queuing (MSMQ), with Active Directory
16        integration disabled, and MSMQ HTTP support enabled.
17 #>
18 function AddFeatures($featurename)
19 {
20     try
21     {
22         $feature=Get-WindowsFeature | ? {
23     $_.DisplayName -eq $featurename -or $_.Name -eq $featurename }
24
25         Add-WindowsFeature $feature
26     }
27
28     catch
29     {
30
31         Write-Host "Addition of Windows feature $featurename
32             failed"
33         Exit 1
34     }
35
36     Write-Host "Addition of Windows feature $featurename
37         succeeded"
```

```
38
39 $system= gwmi win32_operatingSystem | select name
40
41 if (-not (($system -Like '*Microsoft Windows Server 2022*') -or
    ($system -Like '*Microsoft Windows Server 2019*') -or (
    $system -Like '*Microsoft Windows Server 2016*')))
42 {
43
44     Write-Host("This is not a supported server platform.
    Installation aborted.")
45     Exit
46 }
47
48
49 # Start to install Windows feature
50 Import-Module ServerManager
51
52 AddFeatures('Web-Asp-Net45') #ASP.NET 4.5
53 AddFeatures('Web-Mgmt-Console') #IIS Management Console
54 AddFeatures('Web-Windows-Auth') # Windows Authentication
55 AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility
56 AddFeatures('Web-WMI') #IIS 6 WMI Compatibility
57 AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools
58 AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console
59 AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
60 AddFeatures('web-websockets') #IIS Web Sockets
61 AddFeatures('NET-WCF-HTTP-Activation45') #http activate
62 <!--NeedCopy-->
```

- InstallPrereqsforSessionRecordingAgent.ps1

```
1 <#
2 .Synopsis
3     Installs Prereqs for Session Recording Agent
4 .Description
5     Supports Windows Server 2022, Windows Server 2019, Windows
6     Server 2016, windows 11, and Windows 10.
7     Install below windows feature on this machine:
8     -Microsoft Message Queuing (MSMQ), with Active Directory
9     integration disabled, and MSMQ HTTP support enabled.
10
11 #>
12 function AddFeatures($featurename)
13 {
14
15     try
16     {
17         $feature=Get-WindowsFeature | ? {
18             $\.DisplayName -eq $featurename -or $\.Name -eq $featurename }
19         Add-WindowsFeature $feature
20     }
```

```
21     catch
22     {
23
24         Write-Host "Addition of Windows feature $featurename
                failed"
25         Exit 1
26     }
27
28     Write-Host "Addition of Windows feature $featurename
                succeeded"
29 }
30
31
32 # Start to install Windows feature
33 $system= gwmi win32_operatingSystem | select name
34
35 if (-not (($system -Like '*Microsoft Windows Server 2022*') -or
        ($system -Like '*Microsoft Windows Server 2019*') -or (
        $system -Like '*Microsoft Windows Server 2016*') -or (
        $system -Like '*Microsoft Windows 11*') -or ($system -Like '
        *Microsoft Windows 10*'))
36 {
37
38     Write-Host("This is not a supported platform. Installation
                aborted.")
39     Exit
40 }
41
42
43 if ($system -Like '*Microsoft Windows Server*')
44 {
45
46     Import-Module ServerManager
47     AddFeatures('MSMQ') #Message Queuing
48     AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support
49 }
50
51 else
52 {
53
54     try
55     {
56
57         dism /online /enable-feature /featurename:MSMQ-HTTP /all
58     }
59
60     catch
61     {
62
63         Write-Host "Addition of Windows feature MSMQ HTTP Support
                failed"
64         Exit 1
65     }
```

```
66
67     write-Host "Addition of Windows feature MSMQ HTTP Support
        succeeded"
68   }
69
70 <!--NeedCopy-->
```

Pour installer les rôles et fonctionnalités Windows requis, procédez comme suit :

1. Sur l'ordinateur sur lequel vous prévoyez d'installer les composants d'administration de l'enregistrement de session :

- a) Vérifiez que la stratégie d'exécution est définie sur **RemoteSigned** ou **Unrestricted** dans PowerShell.

```
1 Set-ExecutionPolicy RemoteSigned
2 <!--NeedCopy-->
```

- b) Démarrez une invite de commande en tant qu'administrateur et exécutez la commande `powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1`:

Le script affiche les fonctionnalités qui ont été ajoutées avec succès et s'arrête.

- c) Une fois le script exécuté, assurez-vous que la stratégie d'exécution est définie sur une valeur correcte en fonction de la stratégie de votre entreprise.

2. Sur l'ordinateur sur lequel vous prévoyez d'installer le composant Agent d'enregistrement de session :

- a) Vérifiez que la stratégie d'exécution est définie sur **RemoteSigned** ou **Unrestricted** dans PowerShell.

```
1 Set-ExecutionPolicy RemoteSigned
2 <!--NeedCopy-->
```

- b) Démarrez une invite de commande en tant qu'administrateur et exécutez la commande `powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1`:

Le script affiche les fonctionnalités qui ont été ajoutées avec succès et s'arrête.

- c) Une fois le script exécuté, assurez-vous que la stratégie d'exécution est définie sur une valeur correcte en fonction de la stratégie de votre entreprise.

Installer les composants de l'administration de l'enregistrement de session

Remarque :

À partir de la version 2110, avant d'installer les composants de l'administration de l'enregistrement de session sur Windows Server 2016 sur lequel TLS 1.0 est désactivé, procédez comme suit :

1. Installez le pilote Microsoft OLE DB pour SQL Server.
2. Sous la clé de Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\v4.0.30319`, ajoutez la valeur DWORD `SchUseStrongCrypto` (32 bits) et définissez les données de la valeur sur 1.
3. Redémarrez.

Nous vous recommandons d'installer les composants Administration de l'enregistrement de session, Agent d'enregistrement de session et Lecteur d'enregistrement de session sur des serveurs distincts.

Les composants de l'administration de l'enregistrement de session sont les suivants : base de données d'enregistrement de session, serveur d'enregistrement de session et console de stratégie d'enregistrement de session. Vous pouvez choisir le composant à installer sur un serveur.

Remarque :

À partir de la version 2110, avant d'installer les composants de l'administration de l'enregistrement de session sur Windows Server 2016 sur lequel TLS 1.0 est désactivé, procédez comme suit :

1. Installez le pilote Microsoft OLE DB pour SQL Server.
2. Sous la clé de Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\v4.0.30319`, ajoutez la valeur DWORD `SchUseStrongCrypto` (32 bits) et définissez les données de la valeur sur 1.
3. Redémarrez Windows Server 2016.

1. Installez **Broker_PowerShellSnapIn_x64.msi**.

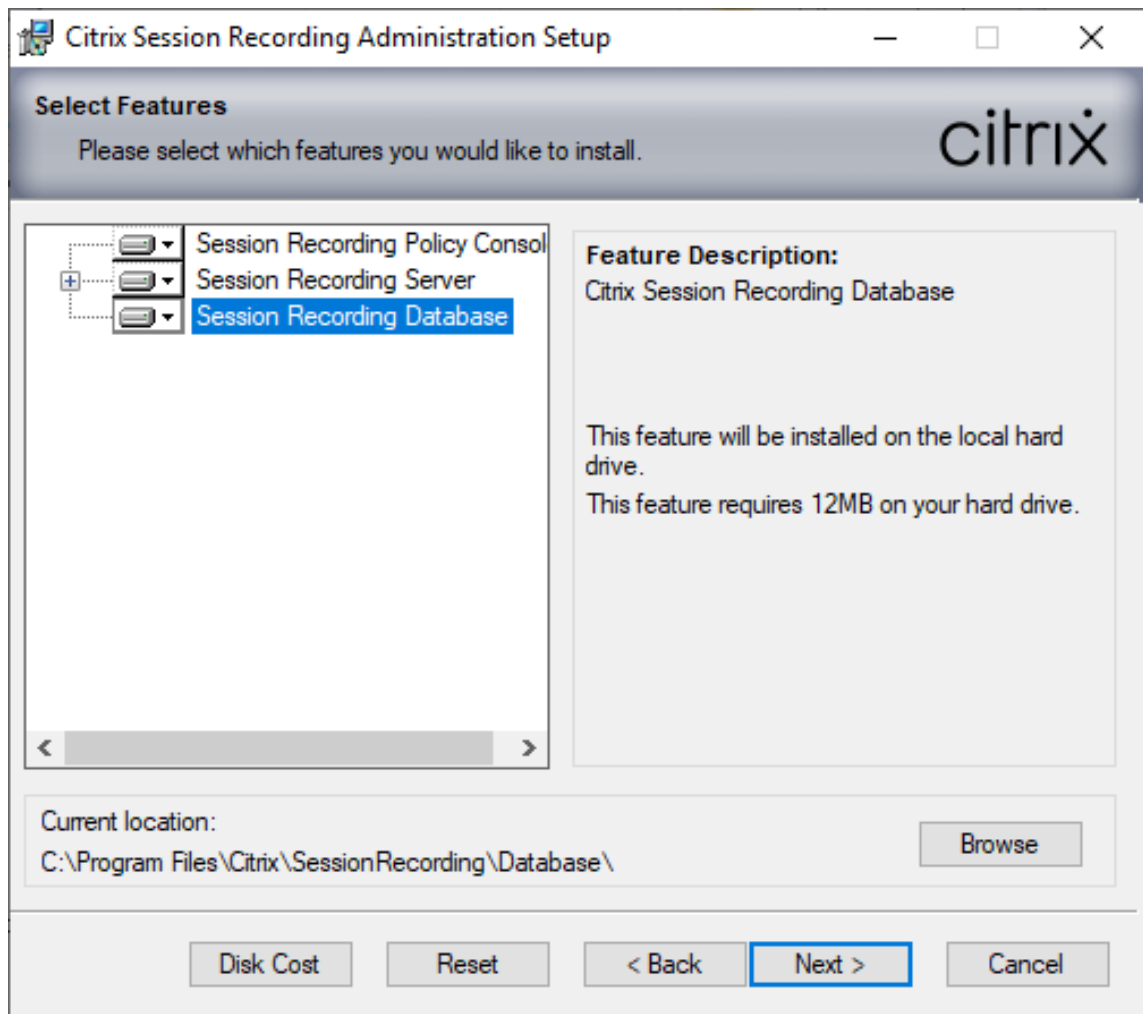
Important :

pour utiliser la console de stratégie d'enregistrement de session, installez le logiciel enfichable Broker PowerShell (`Broker_PowerShellSnapIn_x64.msi`) manuellement. Accédez au logiciel enfichable dans le fichier ISO de Citrix Virtual Apps and Desktops (`\layout\image-full\x64\Citrix Desktop Delivery Controller`) et suivez les instructions pour l'installer. Si vous ne respectez pas cette consigne, cela peut entraîner une erreur.

2. Démarrez l'invite de commandes Windows en tant qu'administrateur, puis exécutez la

commande `msiexec /i SessionRecordingAdministrationx64.msi` ou double-cliquez sur le fichier .msi.

3. Sur l'interface utilisateur d'installation, sélectionnez **Suivant** et acceptez le contrat de licence.
4. Sur l'écran **d'installation de l'administration de l'enregistrement de session**, sélectionnez les composants d'administration de l'enregistrement de session que vous voulez installer.



Remarque :

L'installation de tous les composants d'administration de l'enregistrement de session sur un seul serveur est adaptée à une preuve de concept. Toutefois, pour un environnement de production de grande taille, nous vous recommandons d'installer la Console de stratégie d'enregistrement de session sur un serveur distinct et les composants Serveur d'enregistrement de session, Journalisation de l'Administrateur d'enregistrement de session et Base de données d'enregistrement de session sur un autre serveur. La journalisation de l'administrateur d'enregistrement de session est un sous-composant facultatif du serveur d'enregistrement de session. Sélectionnez le serveur d'enregistrement de session avant

de pouvoir sélectionner la journalisation de l'administrateur d'enregistrement de session.

Installer la base de données d'enregistrement de session

Remarque :

- La base de données d'enregistrement de session n'est pas une véritable base de données. Il s'agit d'un composant permettant de créer et de configurer les bases de données requises dans l'instance Microsoft SQL Server. L'enregistrement de session prend en charge trois solutions pour la haute disponibilité de base de données basée sur Microsoft SQL Server. Pour plus d'informations, consultez la section [Haute disponibilité de la base de données](#).
- Vous pouvez déployer la base de données d'enregistrement de session sur Azure SQL Managed Instance, sur SQL Server sur des machines virtuelles Azure et sur AWS RDS. Pour plus d'informations, consultez [Déployer la base de données d'enregistrement de session sur Azure SQL Managed Instance ou sur AWS RDS](#) et [Déployer la base de données d'enregistrement de session sur SQL Server sur des machines virtuelles Azure](#).

Il existe généralement trois types de déploiement pour la base de données d'enregistrement de session et Microsoft SQL Server :

- Déploiement 1 : Installer le serveur d'enregistrement de session et la base de données d'enregistrement de session sur la même machine et la base de données Microsoft SQL Server sur une machine distante. (**Recommandé**)
 - Déploiement 2 : Installer le serveur d'enregistrement de session, la base de données d'enregistrement de session et la base de données Microsoft SQL Server sur la même machine.
 - Déploiement 3 : Installer le serveur d'enregistrement de session sur une machine et installer la base de données d'enregistrement de session et Microsoft SQL Server sur une autre machine. (**Non recommandé**).
1. Sur la page **Configuration de la base de données et du serveur**, spécifiez le nom de l'instance et le nom de la base de données de la base de données d'enregistrement de session et le compte d'ordinateur du serveur d'enregistrement de session. Cliquez sur **Suivant**.
 - **Nom de l'instance** : si l'instance de base de données n'est pas une instance nommée, vous pouvez uniquement utiliser le nom de l'ordinateur du serveur SQL Server. Si vous avez nommé l'instance, utilisez nom-ordinateur\nom-instance comme nom d'instance de la base de données. Pour déterminer le nom de l'instance du serveur que vous utilisez, exécutez **select @@servername** sur SQL Server. La valeur renvoyée est le nom exact de l'instance de base de données. Si votre serveur SQL écoute un port personnalisé autre que le port par défaut 1433, définissez le port d'écoute personnalisé en ajoutant une virgule au nom de l'instance. Par exemple, tapez **DXSBC-SRD-1,2433** dans la zone de texte **Nom de l'instance**, où 2433, après la virgule, indique le port d'écoute personnalisé.

- **Nom de la base de données** : entrez un nom de base de données personnalisé dans la zone de texte **Nom de la base de données** ou utilisez le nom de base de données par défaut en sélectionnant Utiliser le nom par défaut de la base de données. Cliquez sur **Tester la connexion** pour tester la connectivité avec l'instance de SQL Server et la validité du nom de base de données.

Important :

Un nom de base de données personnalisé doit contenir uniquement les caractères A-Z, a-z, les chiffres 0-9 et des traits de soulignement, et ne doit pas dépasser 123 caractères.

- Vous devez disposer des autorisations de rôle de serveur **securityadmin** et **dbcreator** sur la base de données. Si vous ne disposez pas des autorisations, vous pouvez :
 - * Demander à l'administrateur de base de données d'attribuer les permissions pour l'installation. Une fois l'installation terminée, les autorisations de rôle de serveur **securityadmin** et **dbcreator** ne sont plus nécessaires et peuvent être supprimées.
 - * Ou durant l'installation du msi, une boîte de dialogue s'affiche, demandant les informations d'identification d'un administrateur de base de données avec les autorisations de rôle de serveur **securityadmin** et **dbcreator**. Entrez les informations d'identification correctes et cliquez sur **OK** pour continuer l'installation.

L'installation crée la nouvelle base de données d'enregistrement de session et ajoute le compte de machine du serveur d'enregistrement de session en tant que **db_owner**.

- **Compte d'ordinateur du serveur d'enregistrement de session :**

- **Déploiements 1 et 2** : entrez la valeur **localhost** dans la zone de texte **Compte d'ordinateur du serveur d'enregistrement de session**.
- **Déploiement 3** : entrez le nom de la machine hébergeant le serveur d'enregistrement de session dans le format domaine\nom-ordinateur. Le compte d'ordinateur du serveur d'enregistrement de session est le compte utilisateur utilisé pour accéder à la base de données d'enregistrement de session.

Remarque :

Les tentatives d'installation des composants d'Administration de l'enregistrement de session peuvent échouer avec le code d'erreur 1603 lorsqu'un nom de domaine est défini dans la zone de texte **Compte d'ordinateur du Serveur d'enregistrement de session**. Pour contourner le problème, tapez **localhost** ou le nom de domaine NetBIOS\nom de machine dans la zone de texte **Compte d'ordinateur du Serveur d'enregistrement de session**. Pour obtenir le nom de domaine NetBIOS, exécutez `$env`

:`userdomain` dans PowerShell ou `echo %UserDomain%` dans l'invite de commandes sur la machine sur laquelle vous avez installé le serveur d'enregistrement de session.

2. Suivez les instructions pour terminer l'installation.

Installer le serveur d'enregistrement de session

1. Sélectionnez **Serveur d'enregistrement de session** et **Journalisation de l'administrateur d'enregistrement de session**.

Remarque :

- La journalisation de l'administrateur d'enregistrement de session est un sous-composant facultatif du serveur d'enregistrement de session. Sélectionnez le serveur d'enregistrement de session avant de pouvoir sélectionner la journalisation de l'administrateur d'enregistrement de session.
- Nous vous recommandons d'installer la journalisation de l'administrateur d'enregistrement de session ainsi que le serveur d'enregistrement de session en même temps. Si vous ne souhaitez pas que la fonctionnalité de journalisation de l'administrateur soit activée, vous pouvez la désactiver sur une page ultérieure.

2. Sur la page **Configuration de la base de données et du serveur**, spécifiez les paramètres.

- **Nom de l'instance** : entrez le nom de votre serveur SQL Server dans la case **Nom de l'instance**. Si vous utilisez une instance nommée, entrez `nom-ordinateur\nom-instance` ; sinon, entrez un nom-ordinateur uniquement. Si votre serveur SQL écoute un port personnalisé autre que le port par défaut 1433, définissez le port d'écoute personnalisé en ajoutant une virgule au nom de l'instance. Par exemple, tapez **DXSBC-SRD-1,2433** dans la zone de texte **Nom de l'instance**, où 2433, après la virgule, indique le port d'écoute personnalisé.
- **Nom de la base de données** : entrez un nom de base de données personnalisé dans la zone de texte **Nom de la base de données** ou utilisez le nom de base de données par défaut **CitrixSessionRecording** qui est prédéfini dans la zone de texte. Vous devez disposer des autorisations de rôle de serveur **securityadmin** et **dbcreator** sur la base de données. Si vous ne disposez pas des autorisations, vous pouvez :
 - Demander à l'administrateur de base de données d'attribuer les permissions pour l'installation. Une fois l'installation terminée, les autorisations de rôle de serveur **securityadmin** et **dbcreator** ne sont plus nécessaires et peuvent être supprimées.

- Ou durant l'installation du msi, une boîte de dialogue s'affiche, demandant les informations d'identification d'un administrateur de base de données avec les autorisations de rôle de serveur **securityadmin** et **dbcreator**. Entrez les informations d'identification correctes et cliquez sur **OK** pour continuer l'installation.
 - Après avoir entré le nom d'instance et le nom de base de données corrects, cliquez sur **Tester la connexion** pour tester la connectivité à la base de données d'enregistrement de session.
 - Entrez le compte d'ordinateur du serveur d'enregistrement de session, puis cliquez sur **Suivant**.
3. Sur la page **Configuration de la journalisation d'administration**, spécifiez les configurations pour la fonctionnalité de journalisation de l'administration.
- **La base de données de journalisation est installée sur l'instance SQL Server** : cette zone de texte n'est pas modifiable. Le nom d'instance SQL Server de la base de données de journalisation d'administration est récupéré automatiquement à partir du nom d'instance que vous avez tapé sur la page **Configuration de base de données et de serveur**.
 - **Nom de la base de données de journalisation** : entrez un nom de base de données personnalisé pour la base de données de journalisation de l'administrateur dans la zone de texte ou utilisez le nom de la base de données par défaut **CitrixSessionRecordingLogging** prédéfini dans la zone de texte.
- Remarque :**

Le nom de la base de données de journalisation de l'administrateur doit être différent du nom de la base de données d'enregistrement de session défini dans la zone de texte **Nom de la base de données** sur la page **Configuration de la base de données et du serveur** précédente.
- **Utiliser nom par défaut de la BDD** : cette option utilise le nom de base de données de journalisation par défaut.
 - **Activer service de journalisation** : par défaut, la fonctionnalité de journalisation de l'administration est activée. Vous pouvez la désactiver en désélectionnant la case à cocher.
 - **Activer blocage obligatoire** : par défaut, le blocage obligatoire est activé. Les fonctionnalités normales peuvent être bloquées si la journalisation échoue. Vous pouvez désactiver le blocage obligatoire en désélectionnant la case à cocher.
4. Cliquez sur **Suivant** pour terminer l'installation.

Remarque :

l'installation du serveur d'enregistrement de session utilise par défaut HTTPS/TLS pour sécuriser les communications. Si TLS n'est pas configuré sur le site IIS par défaut du serveur d'enregistrement de session, utilisez HTTP. Pour ce faire, annulez la sélection de SSL dans la console de gestion IIS. Accédez au site Broker d'enregistrement de session, ouvrez les paramètres SSL et désactivez la case à cocher **Require SSL**.

Installer l'agent d'enregistrement de session

Installez l'agent d'enregistrement de session sur la machine VDA ou VDI sur laquelle vous voulez enregistrer les sessions.

1. Sur la page **Configuration de l'agent d'enregistrement de session** : si vous avez déjà installé le serveur d'enregistrement de session, tapez le nom de l'ordinateur sur lequel vous avez installé le serveur d'enregistrement de session. Entrez les informations de protocole et de port pour la connexion au serveur d'enregistrement de session. Si vous n'avez pas encore installé Enregistrement de session, vous pouvez modifier ces informations ultérieurement dans **Propriétés de l'Agent d'enregistrement de session**.
2. Suivez les instructions pour terminer l'installation.

Remarque :

lorsque Machine Creation Services (MCS) ou Citrix Provisioning Services (PVS) crée des VDA avec Microsoft Message Queuing (MSMQ) installé, ces VDA peuvent disposer de la même **QMID** dans certaines conditions. Ce cas peut entraîner plusieurs problèmes, par exemple :

- Les sessions peuvent ne pas être enregistrées, même si l'accord d'enregistrement est accepté.
- Le serveur d'enregistrement de session peut ne pas recevoir les signaux de fermeture de session, par conséquent les sessions peuvent être toujours actives.

Une solution consiste à créer une **QMID** unique pour chaque VDA et elle varie selon les méthodes de déploiement.

Aucune action supplémentaire n'est requise pour les VDA avec OS mono-session créés à l'aide de PVS 7.7 ou version ultérieure et de MCS 7.9 ou version ultérieure en mode bureau statique.

Pour les VDA avec OS multi-session créés avec MCS ou PVS et les VDA avec OS mono-session qui sont configurés pour supprimer toutes les modifications lorsque l'utilisateur ferme sa session, utilisez le script **GenRandomQMID.ps1** pour modifier la **QMID** au démarrage du système. Modifiez la stratégie de gestion de l'alimentation pour vous assurer qu'un nombre suffisant de VDA sont en cours d'exécution avant la connexion des utilisateurs.

Pour utiliser le script GenRandomQMID.ps1, procédez comme suit :

1. Vérifiez que la stratégie d'exécution est définie sur **RemoteSigned** ou **Unrestricted** dans PowerShell.

```
1 Set-ExecutionPolicy RemoteSigned
```

2. Créez une tâche planifiée, définissez le déclencheur sur Au démarrage du système et exécutez le compte SYSTEM sur la machine avec l'image principale PVS ou MCS.

3. Ajoutez la commande en tant que tâche de démarrage.

```
1 powershell .exe -file C:\\GenRandomQMID.ps1
```

Résumé du script GenRandomQmid.ps1 :

1. Supprimez la QMIId actuelle du registre.
2. Ajoutez SysPrep = 1 à HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters.
3. Arrêtez les services associés, notamment CitrixSmAudAgent et MSMQ.
4. Pour générer une QMIId aléatoire, démarrez les services arrêtés précédemment.

Exemple de GENRANDOMQMID.PS1 :

```
1 # Remove old QMIId from registry and set SysPrep flag for MSMQ
2
3 Remove-ItemProperty -Path >HKLM:Software\Microsoft\MSMQ\Parameters\
  MachineCache -Name QMIId -Force
4
5 Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -
  Name >"SysPrep" -Type DWord -Value 1
6
7 # Get dependent services
8
9 $depServices = Get-Service -name MSMQ -dependentservices | Select -
  Property Name
10
11 # Restart MSMQ to get a new QMIId
12
13 Restart-Service -force MSMQ
14
15 # Start dependent services
16
17 if ($depServices -ne $null) {
18
19     foreach ($depService in $depServices) {
20
21
22
```

```
23     $startMode = Get-WmiObject win32_service -filter "NAME = '$
($depService.Name)'" | Select -Property StartMode
24
25     if ($startMode.StartMode -eq "Auto") {
26
27         Start-Service $depService.Name
28     }
29 }
30
31 }
32
33
34 }
35
36 <!--NeedCopy-->
```

Installer le lecteur d'enregistrement de session et le lecteur Web

Installez le lecteur d'enregistrement de session sur le serveur d'enregistrement de session ou sur des postes de travail du domaine. Installez le lecteur Web uniquement sur le serveur d'enregistrement de session.

Double-cliquez sur [SessionRecordingPlayer.msi](#) et [SessionRecordingWebPlayer.msi](#) et suivez les instructions pour terminer l'installation.

Automatiser l'installation

L'enregistrement de session prend en charge l'installation silencieuse avec des options. Écrivez un script qui utilise l'installation silencieuse et exécutez les commandes requises.

Automatiser l'installation des composants d'administration de l'enregistrement de session

Installez l'ensemble des composants de l'administration d'enregistrement de session à l'aide d'une seule commande Par exemple, l'une des deux commandes suivantes installe l'ensemble des composants d'administration de l'enregistrement de session et crée un fichier journal pour capturer les informations d'installation.

```
1 msiexec /i "c:\SessionRecordingAdministrationx64.msi" AddLocal="
SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
DatabaseInstance="WNBIO-SRD-1" DatabaseName="CitrixSessionRecording"
LoggingDatabaseName="CitrixSessionRecordingLogging" DatabaseUser="
localhost" AllowSession0Install="1" /q /l*vx "YourInstallationLog"
2 <!--NeedCopy-->
```

```
1 msiexec /i "SessionRecordingAdministrationx64.msi" AddLocal="
    SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
    DatabaseInstance="CloudSQL" DatabaseName="CitrixSessionRecording"
    LoggingDatabaseName="CitrixSessionRecordingLogging"
    AzureSQLServiceSupport="1" AzureUsername="CloudSQLAdminName"
    AzurePassword="CloudSQLAdminPassword" AllowSession0Install="1" /q /l
    *vx "c:\WithLogging.log"
2 <!--NeedCopy-->
```

Remarque :

Le fichier `SessionRecordingAdministrationx64.msi` se trouve sur l'image ISO de Citrix Virtual Apps and Desktops sous `\layout\image-full\x64\Session Recording`.

Où :

- **AddLocal** fournit les fonctionnalités que vous pouvez sélectionner. Vous pouvez sélectionner plusieurs options. **SsRecServer** est le serveur d'enregistrement de session. **PolicyConsole** est la Console de stratégie d'enregistrement de session. **SsRecLogging** est la fonctionnalité de journalisation de l'administrateur. **StorageDatabase** est la base de données d'enregistrement de session. La journalisation de l'administrateur d'enregistrement de session est un sous-composant facultatif du serveur d'enregistrement de session. Sélectionnez le serveur d'enregistrement de session avant de pouvoir sélectionner la journalisation de l'administrateur d'enregistrement de session.
- **DatabaseInstance** est le nom de l'instance de la base de données d'enregistrement de session. Par exemple, `.\SQLEXPRESS,computer-name\SQLEXPRESS,computer-name` ou `tcp:srt-sql-support.public.ca7b16b60789.database.windows.net,3342` si vous utilisez Azure SQL Managed Instance.
- **DatabaseName** est le nom de la base de données de l'enregistrement de session.
- **LoggingDatabaseName** est le nom de la base de données de journalisation de l'administrateur.
- **AzureSQLServiceSupport** détermine si Cloud SQL est pris en charge. Pour utiliser Cloud SQL, définissez la valeur sur 1.
- **DatabaseUser** est le compte d'ordinateur du serveur d'enregistrement de session.
- **AzureUsername** est le nom d'administrateur Cloud SQL.
- **AzurePassword** est le mot de passe d'administration Cloud SQL.
- **AllowSession0Install** détermine s'il faut installer les composants de l'administration de l'enregistrement de session dans la session 0. Pour installer les composants de l'administration de l'enregistrement de session dans la session 0, ajoutez cet argument à la commande et définissez-le sur 1. Avant d'exécuter la commande, assurez-vous d'ajouter votre compte d'ordinateur en tant que login à SQL Server et de lui attribuer le rôle **sysadmin**.
- **/q** spécifie le mode silencieux.
- **/l*v** spécifie l'enregistrement détaillé.
- **votre_journal_installation** est l'emplacement de votre fichier journal d'installation.

Créer une image principale pour le déploiement du serveur d'enregistrement de session Il se peut que la base de données d'enregistrement de session et la base de données de journalisation d'administration soient déjà en place à partir d'un déploiement existant. Pour de tels scénarios, vous pouvez désormais renoncer aux vérifications de base de données lorsque vous installez les composants d'administration d'enregistrement de session à l'aide de `SessionRecordingAdministrationX64.msi`. Vous pouvez créer une image principale pour déployer facilement le serveur d'enregistrement de session sur de nombreuses autres machines. Après avoir déployé le serveur sur les machines cibles à l'aide de l'image principale, exécutez une commande sur chaque machine pour vous connecter à la base de données d'enregistrement de session et à la base de données de journalisation d'administration existante. Cette prise en charge de l'image principale facilite le déploiement et minimise l'impact potentiel des erreurs humaines. Elle s'applique uniquement aux nouvelles installations et comprend les étapes suivantes :

1. Démarrez une invite de commande et exécutez une commande similaire à la suivante :

```
1 msixexec /i "SessionRecordingAdministrationx64.msi" AddLocal="
  SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
  DatabaseInstance="sqlnotexists" DatabaseName="
  CitrixSessionRecording2" LoggingDatabaseName="
  CitrixSessionRecordingLogging2" DatabaseUser="localhost" /q /l*
  vx "c:\WithLogging.log" IgnoreDBCheck="True"
2 <!--NeedCopy-->
```

Cette commande installe les composants d'administration d'enregistrement de session sans configurer ni tester la connectivité à la base de données d'enregistrement de session et à la base de données de journalisation d'administration.

Définissez le paramètre **IgnoreDBCheck** sur **True** et utilisez des valeurs aléatoires pour **DatabaseInstance**, **DatabaseName** et **LoggingDatabaseName**.

2. Créez une image principale sur la machine que vous utilisez.
3. Déployez l'image principale sur d'autres machines pour déployer le serveur d'enregistrement de session.
4. Sur chacune des machines, exécutez des commandes similaires aux suivantes :

```
1 .\SsRecUtils.exe -modifydbconnectionpara DATABASEINSTANCE
  DATABASENAME LOGGINGDATABASENAME
2
3 iisreset /noforce
4 <!--NeedCopy-->
```

Les commandes connectent le serveur d'enregistrement de session installé précédemment à une base de données d'enregistrement de session et à une base de données de journalisation d'administration existantes.

Le fichier `SsRecUtils.exe` est stocké dans `\Citrix\SessionRecording\Server\`

`bin\`. Définissez les paramètres **DatabaseInstance**, **DatabaseName** et **LoggingDatabaseName** si nécessaire.

Conserver les bases de données lors de la désinstallation des composants de l'administration de l'enregistrement de session Lorsque le paramètre **KeepDB** est défini sur **True**, la commande suivante conserve la base de données d'enregistrement de session et la base de données de journalisation d'administration lors de la désinstallation des composants d'administration d'enregistrement de session :

```
1 msiexec /x "SessionRecordingAdministrationx64.msi" KeepDB="True"
2 <!--NeedCopy-->
```

Automatiser l'installation du lecteur et du lecteur Web d'enregistrement de session

Par exemple, les commandes suivantes installent respectivement le lecteur d'enregistrement de session et le lecteur Web d'enregistrement de session.

```
1 msiexec /i "c:\SessionRecordingPlayer.msi" /q /l*\vx "
  yourinstallationlog"
2 <!--NeedCopy-->
```

```
1 msiexec /i "c:\SessionRecordingWebPlayer.msi" /q /l*vx "
  yourinstallationlog"
2 <!--NeedCopy-->
```

Remarque :

Le fichier `SessionRecordingPlayer.msi` se trouve sur l'image ISO de Citrix Virtual Apps and Desktops sous `\layout\image-full\x86\Session Recording`.

Le fichier `SessionRecordingWebPlayer.msi` se trouve sur l'image ISO de Citrix Virtual Apps and Desktops sous `\layout\image-full\x64\Session Recording`.

Où :

- **/q** spécifie le mode silencieux.
- **/l*v** spécifie l'enregistrement détaillé.
- **votre_journal_installation** est l'emplacement de votre fichier journal d'installation.

Automatiser l'installation de l'agent d'enregistrement de session Par exemple, la commande suivante installe l'agent d'enregistrement de session et crée un fichier journal pour capturer les informations d'installation.


```
1 msiexec /i SessionRecordingAgentx64.msi /q /l*v yourinstallationlog
   SESSIONRECORDINGSERVERNAME=yourservername
2 SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol
   SESSIONRECORDINGBROKERPORT=yourbrokerport
3 <!--NeedCopy-->
```

Remarque :

Le fichier `SessionRecordingAgentx64.msi` se trouve sur l'image ISO de Citrix Virtual Apps and Desktops sous `\layout\image-full\x64\Session Recording`.

Où :

- **nom_de_votre_serveur** correspond au nom NetBIOS ou au nom de domaine complet de la machine hébergeant le serveur d'enregistrement de session. Si elle n'est pas précisée, cette valeur prend par défaut la valeur **localhost**.
- **protocole_de_votre_broker** est le protocole, HTTP ou HTTPS que l'agent d'enregistrement de session utilise pour communiquer avec le broker d'enregistrement de session. Si elle n'est pas précisée, cette valeur prend par défaut la valeur HTTPS.
- **port_de_votre_broker** est le numéro de port que l'agent d'enregistrement de session utilise pour communiquer avec le broker d'enregistrement de session. Si elle n'est pas précisée, la valeur par défaut de cette valeur est zéro, qui amène l'agent d'enregistrement de session à utiliser le numéro de port par défaut pour le protocole sélectionné : 80 pour HTTP ou 443 pour HTTPS.
- **/q** spécifie le mode silencieux.
- **/l*v** spécifie l'enregistrement détaillé.
- **vosre_journal_installation** est l'emplacement de votre fichier journal d'installation.

Mettre à niveau l'enregistrement de session

Vous pouvez mettre à niveau certains déploiements vers des versions ultérieures sans devoir d'abord configurer les nouvelles machines ou sites. Vous pouvez mettre à niveau la dernière mise à jour cumulative de l'enregistrement de session 7.15 LTSR, et n'importe quelle version ultérieure, vers la dernière version de l'enregistrement de session.

Remarque :

Lorsque vous mettez à niveau Administration de l'enregistrement de session depuis la version 7.6 vers 7.13 ou version ultérieure et choisissez **Modifier** pour ajouter le service de journalisation de l'administrateur, le nom de l'instance SQL Server ne s'affiche pas sur la page de **configuration de la journalisation d'administrateur**. Le message d'erreur suivant s'affiche lorsque vous cliquez sur **Suivant : Le test de la connexion à la base de données a échoué. Entrez un nom**

d'instance de base de données correct. Pour contourner le problème, ajoutez le droit en lecture pour les utilisateurs localhost dans le dossier de registre de serveur SmartAuditor suivant : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.

Vous ne pouvez pas mettre à niveau à partir d'une version Technical Preview.

Configuration requise, préparation et limites

- Utilisez l'interface graphique ou l'interface de ligne de commande du programme d'installation de l'enregistrement de session pour mettre à niveau les composants d'enregistrement de session.
- Avant de procéder à toute activité de mise à niveau, sauvegardez la base de données nommée CitrixSessionRecording dans l'instance de SQL Server. De cette façon, vous pouvez la restaurer en cas de problème après la mise à niveau de la base de données.
- En plus d'être un utilisateur du domaine, vous devez être un administrateur local sur les machines sur lesquelles vous mettez à niveau les composants d'enregistrement de session.
- Si le serveur d'enregistrement de session et la base de données d'enregistrement de session ne sont pas installés sur le même serveur, vous devez disposer de l'autorisation de rôle de base de données pour mettre à niveau la base de données d'enregistrement de session. Sinon, vous pouvez :
 - Demander à l'administrateur de base de données d'attribuer les autorisations de rôle de serveur **securityadmin** et **dbcreator** pour la mise à niveau. Une fois la mise à niveau terminée, les autorisations de rôle de serveur **securityadmin** et **dbcreator** ne sont plus nécessaires et peuvent être supprimées pour l'utilisateur actuel.
 - Ou, utilisez le fichier `SessionRecordingAdministrationx64.msi` pour effectuer la mise à niveau. Durant la mise à niveau msi, une boîte de dialogue s'affiche, demandant les informations d'identification d'un administrateur de base de données avec les autorisations de rôle de serveur **securityadmin** et **dbcreator**. Entrez les informations d'identification correctes et cliquez sur **OK** pour continuer la mise à niveau.
- L'agent d'enregistrement de session 7.6.0 et les versions ultérieures sont compatibles avec la dernière version du serveur d'enregistrement de session. Cependant, certaines nouvelles fonctionnalités et des corrections de bogues risquent de ne pas être appliquées.
- Les sessions démarrées durant la mise à niveau du serveur d'enregistrement de session ne sont pas enregistrées.
- L'option **Réglage graphique** dans **Propriétés de l'agent d'enregistrement de session** est activée par défaut après une nouvelle installation ou mise à niveau pour maintenir la compatibilité avec le mode Redirection de composition du Bureau. Vous pouvez désactiver cette option manuellement après une nouvelle installation ou mise à niveau.
- La fonctionnalité de journalisation de l'administrateur n'est pas installée après la mise à niveau

de l'enregistrement de session à partir d'une version précédente où la fonctionnalité n'est pas disponible. Pour ajouter cette fonctionnalité, modifiez l'installation après la mise à niveau.

- S'il existe des sessions d'enregistrement actives lorsque le processus de mise à niveau démarre, l'enregistrement ne pourra probablement pas se terminer.
- Vérifiez la séquence de mise à niveau suivante afin de pouvoir planifier et réduire tout problème potentiel.

Séquence de mise à niveau

1. Lorsque la base de données d'enregistrement de session et le serveur d'enregistrement de session sont installés sur des serveurs différents, arrêtez le service Gestionnaire de stockage d'enregistrement de session manuellement sur le serveur d'enregistrement de session. Ensuite, mettez à niveau la base de données d'enregistrement de session.
2. Via le Gestionnaire des services Internet Information Services (IIS), assurez-vous que le broker d'enregistrement de session est exécuté. Mettez à niveau le serveur d'enregistrement de session. Si la base de données d'enregistrement de session et le serveur d'enregistrement de session sont installés sur le même serveur, la base de données d'enregistrement de session est également mise à niveau.
3. Le service d'enregistrement de session est automatiquement reconnecté lorsque la mise à niveau du serveur d'enregistrement de session est terminée.
4. Mettez à niveau l'agent d'enregistrement de session (sur l'image principale).
5. Mettez à niveau la console de stratégie d'enregistrement de session avec ou après le serveur d'enregistrement de session.
6. Mettez à niveau le lecteur d'enregistrement de session.

Déployer la base de données d'enregistrement de session sur les services de base de données Cloud SQL

Cette section décrit comment déployer la base de données d'enregistrement de session sur Azure SQL Managed Instance, sur AWS RDS et sur SQL Server sur des machines virtuelles Azure.

Déployer la base de données d'enregistrement de session sur Azure SQL Managed Instance ou sur AWS RDS

Conseil :

Vous pouvez également exécuter une seule commande similaire à la suivante pour déployer la base de données d'enregistrement de session sur Azure SQL Managed Instance et sur AWS RDS. Pour plus d'informations, reportez-vous à la section [Automatiser l'installation](#) précédente dans

cet article.

```
1 msixexec /i "SessionRecordingAdministrationx64.msi" AddLocal="
  SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
  DatabaseInstance="CloudSQL" DatabaseName="CitrixSessionRecording
  " LoggingDatabaseName="CitrixSessionRecordingLogging"
  AzureSQLServiceSupport="1" AzureUsername="CloudSQLAdminName"
  AzurePassword="CloudSQLAdminPassword" /q /l*vx "c:\WithLogging.
  log"
2 <!--NeedCopy-->
```

1. Créez une instance Azure SQL Managed Instance ou créez une instance SQL Server via la console Amazon RDS.
2. (Pour Azure SQL uniquement) Conservez un enregistrement des chaînes **Server** qui apparaissent dans le panneau des propriétés. Ces chaînes représentent le nom d'instance de la base de données d'enregistrement de session. Pour obtenir un exemple, consultez la capture d'écran suivante.

[ADO.NET](#) [JDBC](#) [ODBC](#) [PHP](#)

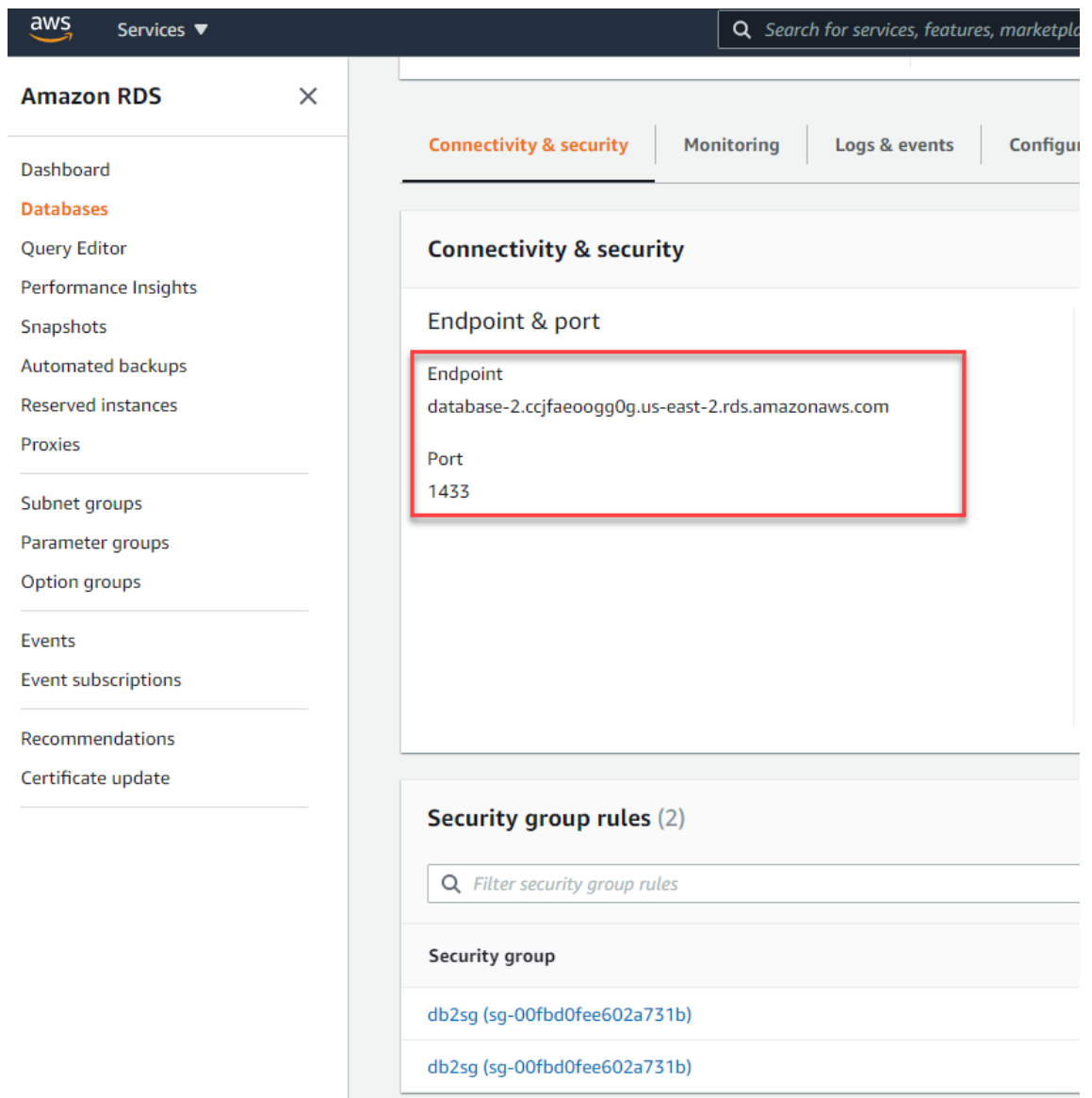
ADO.NET (SQL authentication) - private endpoint

```
Server=tcp:sr-sqlinstance.3141e49e4d94.database.windows.net,1433;Persist Security Info=False;User ID={your_username};Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
```

ADO.NET (SQL authentication) - public endpoint

```
Server=tcp:sr-sqlinstance.public.3141e49e4d94.database.windows.net,3342;Persist Security Info=False;User ID={your_username};Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
```

3. (Pour AWS RDS uniquement) Conservez un enregistrement des informations **Endpoint** et **Port**. Nous utilisons ces informations comme nom d'instance de votre base de données, au format **<Endpoint, Port>**.



4. Exécutez SessionRecordingAdministrationx64.msi pour installer la base de données d'enregistrement de session.

Activez la case à cocher **Activer Cloud SQL** et entrez le nom et le mot de passe administrateur Cloud SQL. Effectuez les autres configurations requises.

The screenshot shows a Windows-style dialog box titled "Citrix Session Recording Administration Setup" with a sub-header "Database and Server Configuration" and the Citrix logo. The main text reads: "Specify the instance name and database name of the Session Recording Database and the computer account of the Session Recording Server." The form contains several input fields and checkboxes:

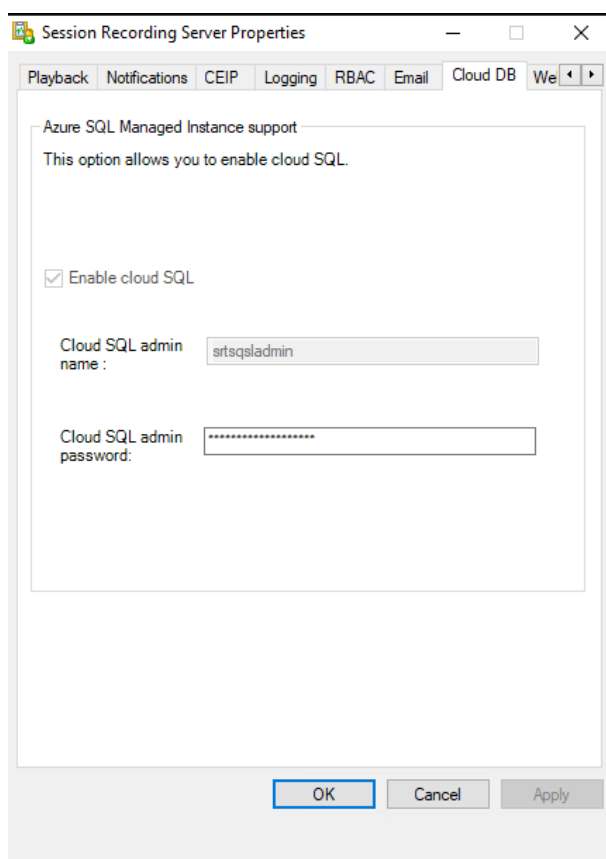
- Instance name:** A text input field with an example below: ".\SQLEXPRESS, computer-name\SQLEXPRESS, computer-name, tcp:xxxx.database.windows.net, 3342".
- Enable cloud SQL:** A checked checkbox.
- Database name:** A text input field with an unchecked checkbox labeled "Use default database name".
- Cloud SQL admin name:** A text input field.
- Cloud SQL admin password:** A text input field.
- Session Recording Server computer account:** A text input field with an example below: "localhost, domain\computer-name".

At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

Remarque :

Si vous modifiez le mot de passe administrateur Cloud SQL, vous devez mettre à jour le mot de passe dans **Propriétés du serveur d'enregistrement de session**. Lorsque vous ouvrez **Propriétés du serveur d'enregistrement de session**, un message d'erreur s'affiche. Cliquez sur **OK** pour continuer, sélectionnez l'onglet **Base de données de cloud** et tapez le nouveau mot de passe administrateur Cloud SQL. Redémarrez le service Analytics d'enregistrement de session Citrix, le service Gestionnaire de stockage d'enregistrement de session Citrix et le service IIS.

L'authentification Azure AD n'est pas prise en charge.



Migrer une base de données locale vers Cloud SQL Managed Instance

1. Migrez votre base de données locale en suivant les instructions de <https://docs.microsoft.com/en-us/data-migration/> et <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-microsoft-sql-server-database-to-amazon-rds-for-sql-server.html>.
2. Pour que l'enregistrement de session fonctionne correctement après la migration, exécutez `SsRecUtils.exe` sur le serveur d'enregistrement de session.

```
C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe -modifyazuredbconnectionpara { Database Instance } { Session Recording Database Name } { Session Recording Logging Database Name } { AzureAdminName } { AzureAdminPassword } iisreset /noforce
```

3. Sur le serveur d'enregistrement de session, redémarrez le service Analyse de l'enregistrement de session Citrix, le service Gestionnaire de stockage d'enregistrement de session Citrix et le service IIS.

Migrer une base de données de production depuis Azure SQL Managed Instance vers une base de données locale

1. Migrez la base de données en suivant les instructions de <https://docs.microsoft.com/en-us/dta-migration/>.
2. Pour que l'enregistrement de session fonctionne correctement après la migration, exécutez `SsRecUtils.exe` sur le serveur d'enregistrement de session.

```
C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe -modifydbconnectionpara { Database Instance } { Session Recording Database Name } { Session Recording Logging Database Name } iisreset /noforce
```

3. Sur le serveur d'enregistrement de session, redémarrez le service Analyse de l'enregistrement de session Citrix, le service Gestionnaire de stockage d'enregistrement de session Citrix et le service IIS.

Déployer la base de données d'enregistrement de session sur SQL Server sur des machines virtuelles Azure

Sur SQL Server sur des VM Azure, vous pouvez déployer la base de données d'enregistrement de session.

1. Extrayez une machine virtuelle Azure SQL.
2. Configurez la machine virtuelle et ajoutez-la au domaine où vous installez les composants d'enregistrement de session.
3. Utilisez le nom de domaine complet de la machine virtuelle comme nom d'instance lors de l'installation de la base de données d'enregistrement de session.

Remarque : lorsque vous utilisez `SessionRecordingAdministrationx64.msi` pour l'installation, désactivez la case à cocher **Activer Cloud SQL**.

4. Suivez les instructions pour terminer l'installation.

Désinstaller l'enregistrement de session

Pour supprimer tous les composants d'enregistrement de session d'un serveur ou d'une station de travail, utilisez la capacité de désinstallation ou de suppression des programmes disponible au travers du Panneau de configuration Windows. Pour supprimer la base de données d'enregistrement de session, vous devez avoir les mêmes droits d'administrateur système SQL Server **securityadmin** et **dbcreator** que lorsque vous l'avez installée.

Pour des raisons de sécurité, la base de données de Journalisation de l'administrateur n'est pas supprimée après la désinstallation des composants.

Intégrer à Citrix Analytics for Security

Vous pouvez configurer des serveurs d'enregistrement de session pour envoyer des [événements](#) utilisateur à Citrix Analytics for Security, qui traite les événements utilisateur afin de fournir des insights exploitables sur les comportements des utilisateurs.

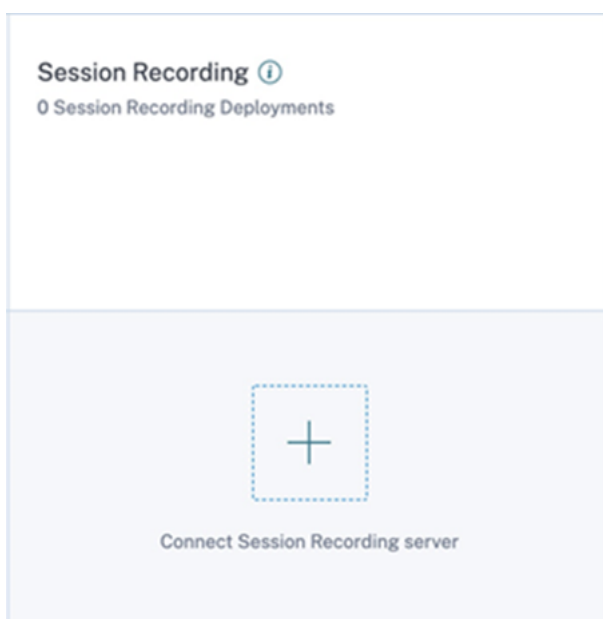
Pré-requis

Avant de commencer, les conditions préalables suivantes doivent être remplies :

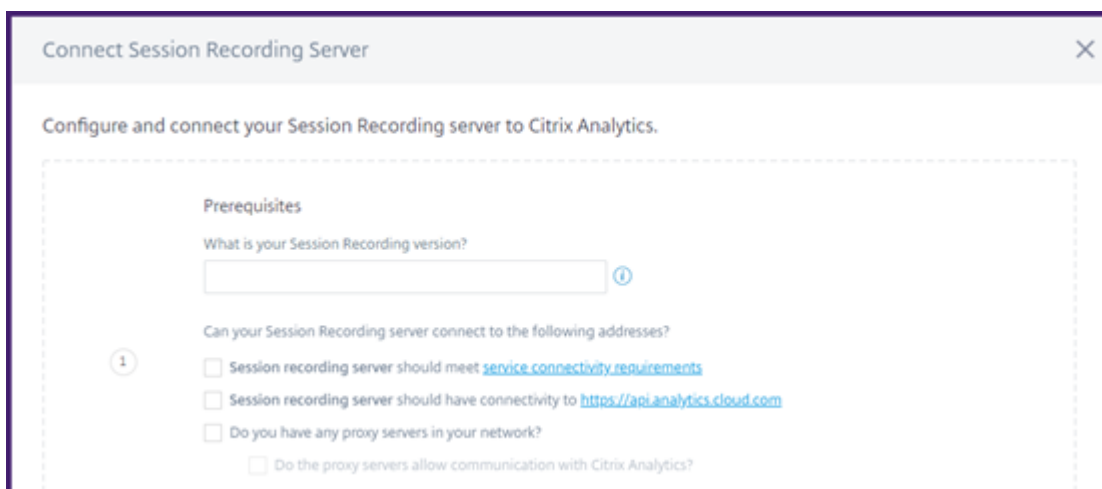
- Le serveur d'enregistrement de session peut se connecter aux adresses suivantes :
 - https://*.cloud.com
 - https://*.citrixdata.com
 - <https://api.analytics.cloud.com>
- Le port 443 du déploiement d'enregistrement de session est ouvert pour les connexions Internet sortantes. Tous les serveurs proxy du réseau doivent autoriser cette communication avec Citrix Analytics for Security.
- Si vous utilisez Citrix Virtual Apps and Desktops 7 1912 LTSR, la version d'enregistrement de session prise en charge est 2103 ou ultérieure.

Connecter votre serveur d'enregistrement de session à Citrix Analytics for Security

1. Connectez-vous à Citrix Cloud.
2. Trouvez Citrix Analytics for Security et cliquez sur **Gérer**.
3. Dans la barre supérieure, cliquez sur **Paramètres > Sources de données**.
4. Sur la carte de site **Virtual Apps and Desktops - Enregistrement de session**, cliquez sur **Connecter Serveur d'enregistrement de session**.



5. Sur la page **Connecter Serveur d'enregistrement de session**, consultez la liste de contrôle et sélectionnez toutes les conditions obligatoires. Si vous ne sélectionnez aucune condition obligatoire, l'option **Télécharger le fichier** est désactivée.



6. Si votre réseau comporte des serveurs proxy, entrez l'adresse proxy dans le fichier *SsRecStorageManager.exe.config* de votre serveur d'enregistrement de session.

Le fichier de configuration se trouve sous <Session Recording server installation path>\bin\SsRecStorageManager.exe.config

Par exemple : C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageManager.exe.config

7. Cliquez sur **Télécharger le fichier** pour télécharger le fichier *SessionRecordingConfigurationFile.json*.

Remarque :

Le fichier contient des informations sensibles. Conservez le fichier dans un endroit sûr et sécurisé.

8. Copiez le fichier sur le serveur d'enregistrement de session que vous souhaitez connecter à Citrix Analytics for Security.

Si votre déploiement comporte plusieurs serveurs d'enregistrement de session, vous devez copier le fichier sur chaque serveur auquel vous souhaitez vous connecter et suivre les étapes de configuration pour chaque serveur.

9. Sur le serveur d'enregistrement de session, exécutez la commande suivante pour importer les paramètres :

```

1 <Session Recording server installation path>\bin\SsRecUtils.exe -
  Import_SRCAsConfigurations <configuration file path>
2 <!--NeedCopy-->
    
```

Par exemple :

```

1 C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
  exe -Import_SRCAsConfigurations C:\Users\administrator \
  Downloads\SessionRecordingConfigurationFile.json
2 <!--NeedCopy-->
    
```

10. Redémarrez les services suivants :

- Service d'analyse de l'enregistrement de session Citrix
- Gestionnaire de stockage d'enregistrement de session Citrix

11. Une fois la configuration terminée, accédez à Citrix Analytics for Security pour afficher le serveur d'enregistrement de session connecté. Cliquez sur **Turn On Data Processing** pour autoriser Citrix Analytics for Security à traiter les données.

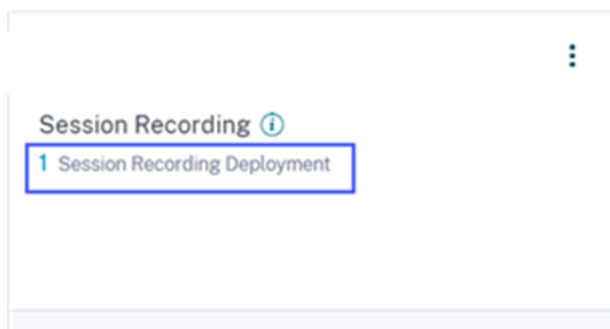
Remarque :

Si vous utilisez le serveur d'enregistrement de session version 2103 ou 2104, vous devez d'abord lancer une session Virtual Apps and Desktops pour afficher le serveur d'enregistrement de session connecté sur Citrix Analytics for Security. Sinon, le serveur d'enregistrement de session connecté ne s'affiche pas. Cette exigence ne s'applique pas aux versions 2106 et ultérieures du serveur d'enregistrement de session.

Afficher les déploiements connectés

Les déploiements de serveurs apparaissent sur la carte de site Enregistrement de session uniquement si la configuration est réussie. La carte de site indique le nombre de serveurs configurés qui ont établi des connexions avec Citrix Analytics for Security.

Si vous ne voyez pas vos serveurs d'enregistrement de session même après la réussite de la configuration, reportez-vous à la section de dépannage [Le serveur d'enregistrement de session configuré ne parvient pas à se connecter](#).



Sur la carte de site, cliquez sur le nombre de déploiements pour afficher les groupes de serveurs connectés avec Citrix Analytics for Security. Par exemple, cliquez sur **1 déploiement d'enregistrement de session** pour afficher le ou les groupes de serveurs connectés. Chaque serveur d'enregistrement de session est représenté par une URL de base et un ServerGroupID.

Session recording servers

^ Session Recording deployment

The Session recording server is successfully configured and connected.

BASE URL	SESSION RECORDING DEPLOYMENT	CONFIGURATION STATUS	LAST UPDATED
Site-2-v2103.smarttools.cim	[REDACTED]	Success	Sep 21 2021 11:26 AM

Showing 1-1 of 1 items Page 1 of 1 5 rows

Afficher les événements reçus

La carte de site affiche les déploiements d'enregistrement de session connectés et les événements reçus de ces déploiements au cours de la dernière heure, qui est la période sélectionnée par défaut. Vous pouvez également sélectionner 1 semaine (1 W) et afficher les données. Cliquez sur le nombre d'événements reçus pour afficher les événements sur la page de recherche en libre-service.

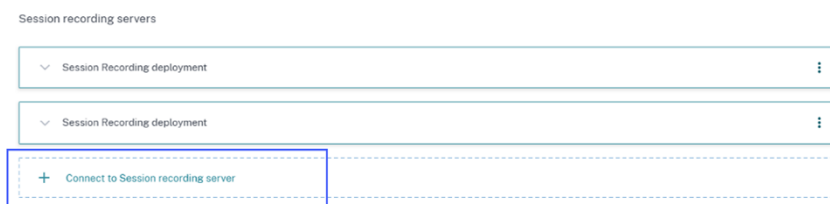
Une fois que vous avez activé le traitement des données, la carte de site peut afficher l'état **No data received** (Aucune donnée reçue). Cet état apparaît pour deux raisons :

1. Si vous avez activé le traitement des données pour la première fois, les événements mettent un certain temps à atteindre le hub d'événements dans Citrix Analytics. Lorsque Citrix Analytics reçoit les événements, l'état passe à **Data processing on** (Traitement des données activé). Si l'état ne change pas après un certain temps, actualisez la page des sources de données.
2. Citrix Analytics n'a reçu aucun événement de la source de données au cours de la dernière heure.

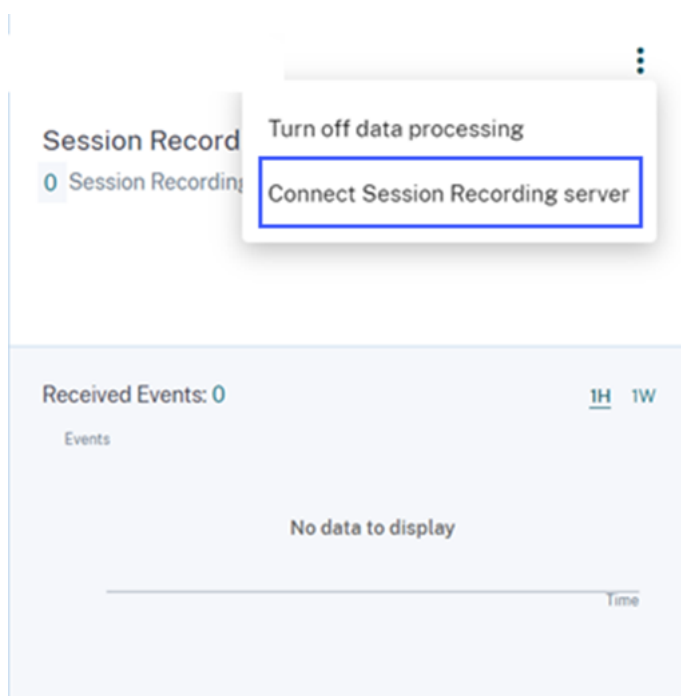
Ajouter des serveurs d'enregistrement de session

Pour ajouter un serveur d'enregistrement de session, effectuez l'une des opérations suivantes :

- Sur la page des **déploiements d'enregistrement de session connectés**, cliquez sur **Connecter Serveur d'enregistrement de session**.



- Sur la carte de site **Virtual Apps and Desktops - Enregistrement de session**, cliquez sur les points de suspension verticaux (⋮), puis sélectionnez **Connecter Serveur d'enregistrement de session**.

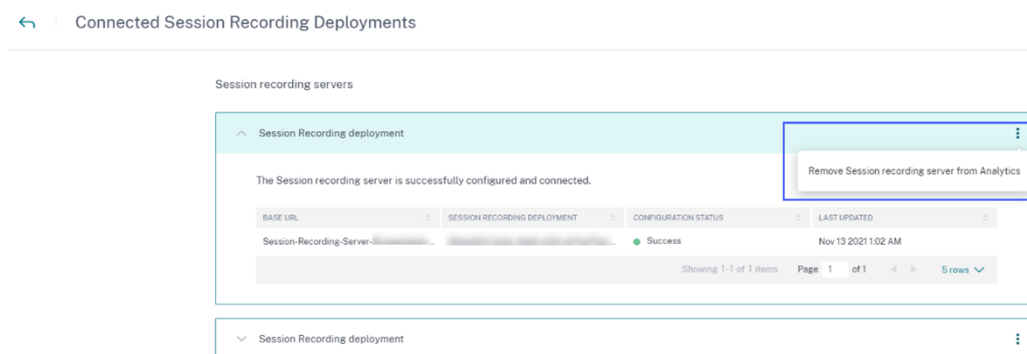


Suivez les étapes pour télécharger le fichier de configuration et configurer un serveur d'enregistrement de session.

Supprimer les serveurs d'enregistrement de session

Pour supprimer un serveur d'enregistrement de session :

1. Sur Citrix Analytics for Security, accédez à la page des **déploiements d'enregistrement de session connectés** et sélectionnez le déploiement de serveur que vous souhaitez supprimer.
2. Cliquez sur les points de suspension verticaux (⋮) et sélectionnez **Remove Session Recording server from Analytics**.



3. Sur le serveur d'enregistrement de session que vous avez supprimé de Citrix Analytics, exécutez la commande suivante :

```
1 <Session Recording server installation path>\bin\SsRecUtils.exe -  
  Remove_SRCasConfigurations  
2 <!--NeedCopy-->
```

Par exemple :

```
1 C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.  
  exe -Remove_SRCasConfigurations  
2 <!--NeedCopy-->
```

Activer ou désactiver le traitement des données sur la source de données

Vous pouvez arrêter le traitement des données à tout moment pour une source de données particulière : Director et l'application Workspace. Sur la carte de site de la source de données, cliquez sur les points de suspension verticaux (⋮), puis sélectionnez **Turn off data processing**. Citrix Analytics arrête le traitement des données pour cette source de données. Vous pouvez également arrêter le traitement des données à partir de la carte de site Virtual Apps and Desktops. Cette option s'applique à la fois aux sources de données de Director et de l'application Workspace.

Pour réactiver le traitement des données, cliquez sur **Turn On Data Processing**.

Le serveur d'enregistrement de session configuré ne parvient pas à se connecter

Votre serveur d'enregistrement de session ne parvient pas à se connecter à Citrix Analytics après la configuration. Par conséquent, le serveur configuré n'apparaît pas sur la carte de site **Enregistrement de session**.

Pour résoudre ce problème, procédez comme suit :

1. Sur votre serveur d'enregistrement de session configuré, exécutez la commande PowerShell suivante pour vérifier l'identification de la machine cliente (CMID) :

““

```
Get-WmiObject -class SoftwareLicensingService | select Clientmachineid
```

““

2. Si CMID est vide, ajoutez les fichiers de registre suivants dans les chemins spécifiés :

Nom de Registre	Chemin du registre	Type de clé	Valeur
AuditorUniqueID	Computer\ HKEY_LOCAL_MACHINE \SOFTWARE\ Citrix\ SmartAuditor\ Server\ Computer\ HKEY_LOCAL_MACHINE	Chaîne	Entrez votre UUID.
EnableCASUseAuditor	/SOFTWARE/ Citrix/ SmartAuditor/ Server/	REG_DWORD	1

3. Redémarrez les services suivants :

- Service d'analyse de l'enregistrement de session Citrix
- Gestionnaire de stockage d'enregistrement de session Citrix

Enregistrement de session dynamique

February 20, 2024

Auparavant, l'enregistrement de session commençait strictement au tout début des sessions qui répondaient aux stratégies d'enregistrement et s'arrêtait strictement à la fin de ces sessions.

À partir de la version 7.18, Citrix introduit l'enregistrement de session dynamique. Grâce à cette fonctionnalité, vous pouvez démarrer ou arrêter l'enregistrement d'une session ou de sessions spécifiques qu'un utilisateur spécifique lance, à tout moment au cours des sessions.

Remarque :

Pour que cette fonctionnalité fonctionne comme prévu, mettez à niveau l'enregistrement de session, le VDA et le Delivery Controller vers la version 7.18 ou une version ultérieure.

Désactiver ou activer l'enregistrement de session dynamique

Sur l'agent d'enregistrement de session, une valeur de registre est ajoutée pour activer ou désactiver cette fonctionnalité. La valeur de registre est définie par défaut sur **1**, ce qui signifie que la fonction est activée par défaut.

Pour activer ou désactiver la fonctionnalité, procédez comme suit :

1. Une fois l'installation de l'enregistrement de session terminée, connectez-vous en tant qu'administrateur à la machine sur laquelle vous avez installé l'agent d'enregistrement de session.
2. Ouvrez l'Éditeur de Registre.
3. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor`.
4. Définissez la valeur de **DynamicControlAllowed** sur **0** ou utilisez la valeur par défaut, **1**.
1 : activer l'enregistrement dynamique
0 : désactiver l'enregistrement dynamique
5. Redémarrez l'agent d'enregistrement de session pour que votre paramètre prenne effet.
Si vous utilisez MCS ou PVS pour le déploiement, modifiez le paramètre sur votre image principale et effectuez une mise à jour pour que vos modifications prennent effet.

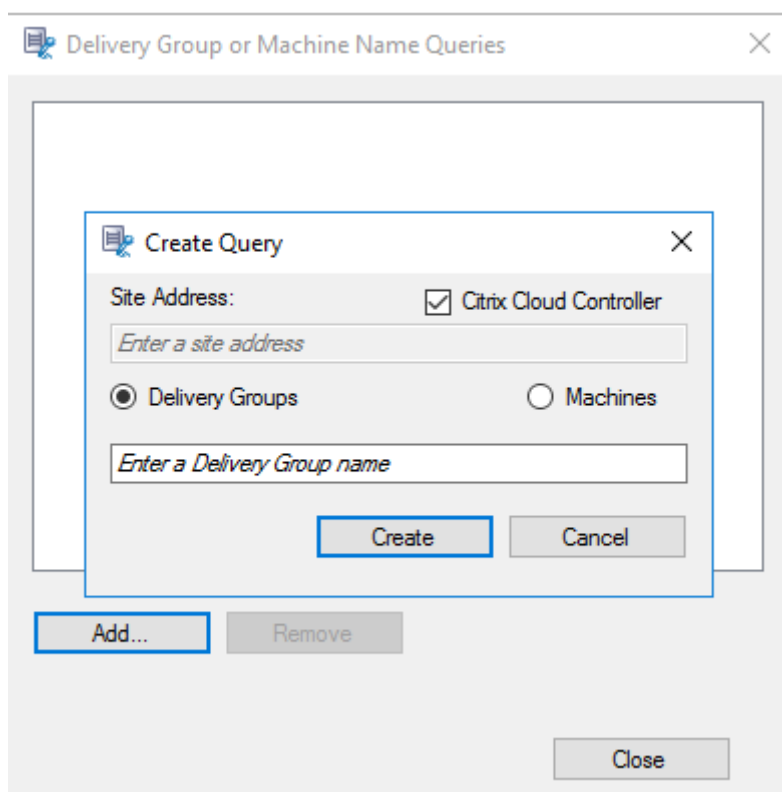
Avertissement :

La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Démarrer ou arrêter dynamiquement l'enregistrement à l'aide des commandes PowerShell dans les SDK Citrix

Vous pouvez utiliser la fonctionnalité d'enregistrement de session dynamique dans des environnements locaux et Citrix Cloud. Pour utiliser la fonctionnalité dans un environnement local, utilisez le SDK PowerShell Citrix Virtual Apps and Desktops. Pour utiliser la fonctionnalité dans un environnement Citrix Cloud, utilisez le SDK Citrix DaaS Remote PowerShell (anciennement SDK Citrix Virtual Apps and Desktops Remote PowerShell).

Pour déterminer quel SDK installer et utiliser, tenez compte du Delivery Controller que vous avez spécifié lors de la création de votre stratégie d'enregistrement. Si vous sélectionnez l'option **Citrix Cloud Controller** pour enregistrer les sessions dans un environnement Citrix Cloud, vous devez valider vos informations d'identification Citrix Cloud.

**Remarque :**

N'installez pas le SDK Citrix DaaS PowerShell Remote sur une machine Citrix Cloud Connector. Vous pouvez installer le SDK Remote PowerShell sur n'importe quelle machine appartenant au domaine dans le même emplacement de ressources. Nous vous recommandons de ne pas exécuter les applets de commande de ce SDK sur les Cloud Connector. Le fonctionnement du SDK n'implique pas les Cloud Connector.

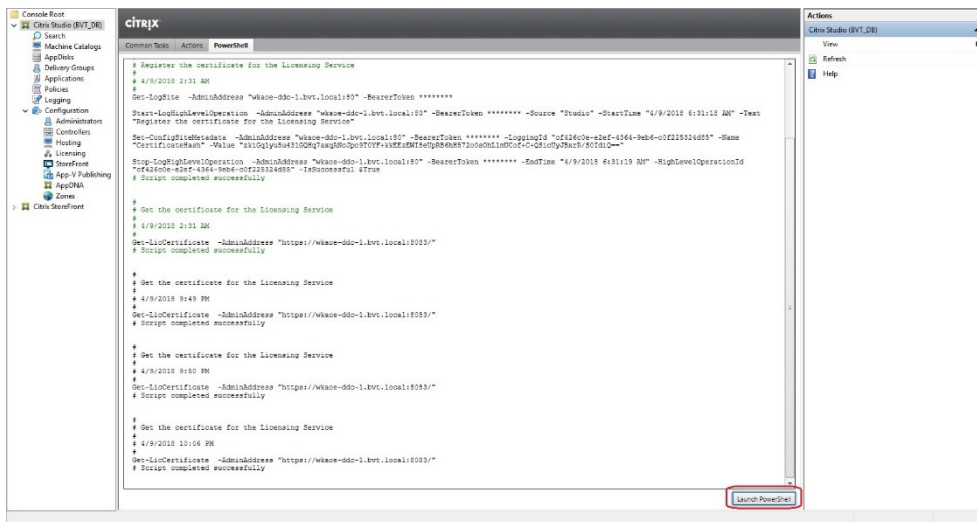
Le tableau suivant répertorie trois commandes PowerShell que les deux SDK Citrix fournissent pour la fonctionnalité d'enregistrement de session dynamique.

Commande	Description
Start-BrokerSessionRecording	Permet de commencer à enregistrer une session active spécifique, une liste de sessions actives ou des sessions lancées par un utilisateur spécifique. Pour plus d'informations, exécutez <code>Get-Help Start-BrokerSessionRecording</code> pour afficher l'aide en ligne de la commande.

Commande	Description
Stop-BrokerSessionRecording	Permet d'arrêter d'enregistrer une session active spécifique, une liste de sessions actives ou des sessions lancées par un utilisateur spécifique. Pour plus d'informations, exécutez Get-Help Stop-BrokerSessionRecording pour afficher l'aide en ligne de la commande.
Get-BrokerSessionRecordingStatus	Permet d'obtenir le statut d'enregistrement d'une session active spécifique. Pour plus d'informations, exécutez Get-Help Get-BrokerSessionRecordingStatus pour afficher l'aide en ligne de la commande.

Par exemple, lorsqu'un utilisateur signale un problème et nécessite une assistance immédiate, vous pouvez utiliser cette fonctionnalité pour démarrer dynamiquement l'enregistrement des sessions actives de l'utilisateur. Vous pouvez également visionner l'enregistrement actif pour procéder au dépannage. Vous pouvez effectuer les opérations suivantes :

1. (Pour le SDK PowerShell Citrix Virtual Apps and Desktops uniquement) Lancez PowerShell à partir de la console Citrix Studio.



2. Utiliser la commande [Get-BrokerSession](#) pour obtenir toutes les sessions actives de l'utilisateur cible.

```

Select Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\Powershell.exe
PS C:\Program Files\Citrix\Desktop Studio> $sessions=get-brokersession -username WKAOE\testuser6
24
25
PS C:\Program Files\Citrix\Desktop Studio> $sessions.sessionstate
Active
Active
PS C:\Program Files\Citrix\Desktop Studio> $sessions.sessiontype
Desktop
Application
PS C:\Program Files\Citrix\Desktop Studio> $sessions.ostype
Windows 2016
Windows 2016
PS C:\Program Files\Citrix\Desktop Studio>
    
```

3. Utiliser la commande `Get-BrokerSessionRecordingStatus` pour obtenir l'état d'enregistrement de la session spécifiée.

```

PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSessionRecordingStatus -Session 24
SessionNotRecorded
PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSessionRecordingStatus -Session 25
SessionNotRecorded
PS C:\Program Files\Citrix\Desktop Studio>
    
```

Remarque :

Le paramètre **-Session** ne peut accepter qu'un seul UID de session à la fois.

4. Utilisez la commande `Start-BrokerSessionRecording` pour démarrer l'enregistrement. Par défaut, un message de notification apparaît pour informer les utilisateurs que la session est enregistrée.

Le tableau suivant indique les méthodes courantes d'utilisation de la commande `Start-BrokerSessionRecording`:

Commande	Description
<code>Start-BrokerSessionRecording -User DomainA \ UserA</code>	Lance l'enregistrement de toutes les sessions de l'utilisateur UserA dans le domaine appelé DomainA et notifie UserA.
<code>Start-BrokerSessionRecording -User DomainA \ UserA -NotifyUser \$false</code>	Lance l'enregistrement de toutes les sessions de l'utilisateur UserA dans le domaine appelé DomainA et ne notifie pas UserA.
<code>Start-BrokerSessionRecording -Sessions \$SessionObject</code>	Lance l'enregistrement de toutes les sessions de l'objet appelé \$SessionObject et notifie l'utilisateur. Pour obtenir l'objet \$SessionObject, exécutez <code>\$SessionObject=Get-BrokerSession -username UserA</code> . Le nom d'un objet est préfixé d'un signe de dollar \$. Pour plus d'informations, voir Étape 2 et l'aide en ligne de la commande.
<code>Start-BrokerSessionRecording -Sessions uid1,uid2,...,uidn</code>	Lance l'enregistrement des sessions UID1, UID2, ...et UIDn et notifie les utilisateurs.

5. Utiliser la commande `Get-BrokerSessionRecordingStatus` pour obtenir l'état d'enregistrement de chaque session cible. L'état est censé être **SessionBeingRecorded**.
6. Visionnez les enregistrements **Actif** ou **Terminé** et procédez au dépannage.

Remarque :

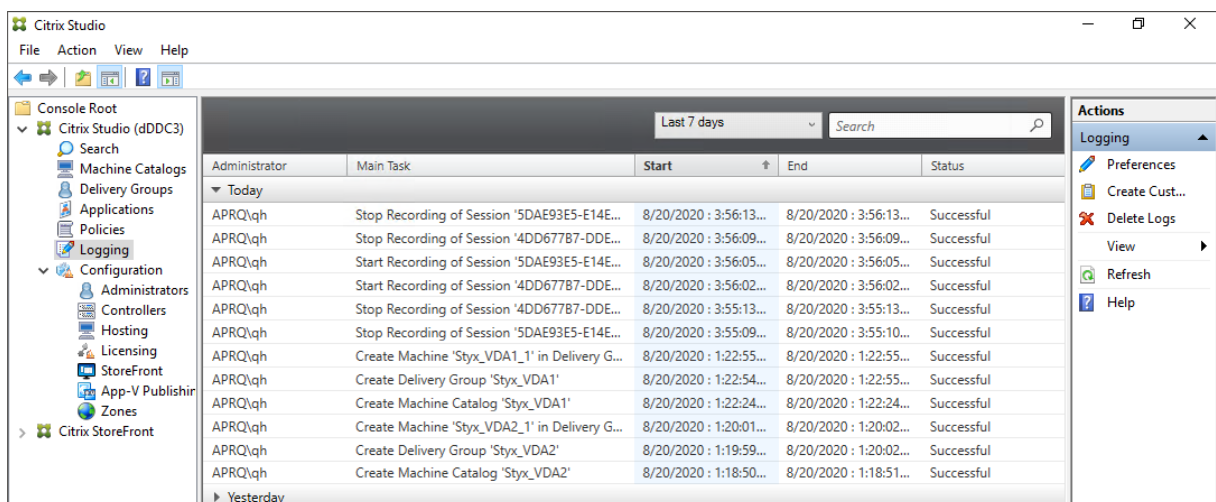
La dernière section de la chronologie de la barre de progression du lecteur peut apparaître grisée lorsque vous visionnez un enregistrement **Terminé** qui a été arrêté par la commande `Stop-BrokerSessionRecording` et que la dernière section de la session enregistrée est inactive. Il est difficile de savoir quand la session enregistrée a des activités constantes.

7. Utilisez la commande `Stop-BrokerSessionRecording` pour arrêter l'enregistrement lorsque le problème signalé a été trié ou résolu.

Le tableau suivant indique les méthodes courantes d'utilisation de cette commande :

Commande	Description
<code>Stop-BrokerSessionRecording -User DomainA \ UserA</code>	Arrête l'enregistrement de toutes les sessions de l'utilisateur UserA dans le domaine appelé DomainA.
<code>Stop-BrokerSessionRecording -Sessions \$SessionObject</code>	Arrête l'enregistrement de toutes les sessions dans \$SessionObject.
<code>Stop-BrokerSessionRecording -Sessions uid1,uid2,...,uidn</code>	Arrête l'enregistrement des sessions UID1, UID2, ...et UIDn.

Dans l'écran **Journalisation** de Citrix Studio, vous pouvez afficher les journaux des commandes `Start-BrokerSessionRecording` et `Stop-BrokerSessionRecording`.



Configurer

December 21, 2022

Cette section fournit des instructions pour configurer les paramètres suivants :

- Paramètres de l'agent d'enregistrement de session
 - Activer ou désactiver l'enregistrement
 - Configurer la connexion au serveur d'enregistrement de session
 - Configurer le protocole de communication
- Paramètres sur le serveur d'enregistrement de session
 - Autoriser les utilisateurs
 - Personnaliser les messages de notification
 - Spécifier l'emplacement du stockage des enregistrements
 - Spécifier la taille du fichier pour les enregistrements
 - Activer ou désactiver les signatures numériques
 - Configurer le programme CEIP
- Stratégies
 - Configurer les stratégies d'enregistrement de session
 - Configurer des stratégies de visionnage d'enregistrement
 - Configurer les stratégies de détection d'événements
 - Configurer les stratégies de réponse aux événements
- Haute disponibilité et équilibrage de charge
 - Équilibrer la charge des serveurs d'enregistrement de session
 - Configurer la haute disponibilité de base de données

Configurer les paramètres de l'agent d'enregistrement de session

December 21, 2022

Cette section décrit les paramètres suivants :

- Activer ou désactiver l'enregistrement
- Configurer la connexion au serveur d'enregistrement de session
- Configurer le protocole de communication

Activer ou désactiver l'enregistrement

December 23, 2022

L'installation de l'agent d'enregistrement de session s'effectue sur chaque VDA pour OS multi-session pour lequel vous souhaitez enregistrer des sessions. Chaque agent est équipé d'un paramètre permettant d'activer les enregistrements pour le VDA sur lequel il est installé. Après l'activation de la fonction d'enregistrement, l'enregistrement de session évalue la stratégie d'enregistrement active qui détermine les sessions à enregistrer.

Nous vous recommandons de désactiver l'enregistrement de session sur les VDA qui ne sont pas enregistrés. Il existe un impact minime sur les performances, même si aucun enregistrement n'a lieu.

Activer ou désactiver l'enregistrement sur un VDA

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Sous l'option **Enregistrement de session**, sélectionnez ou effacez le contenu de la case **Activer l'enregistrement de session pour cette machine VDA** afin de spécifier si les sessions de ce VDA peuvent être enregistrées.
4. À l'invite, redémarrez le service de l'agent d'enregistrement de session pour accepter la modification.

Remarque :

Lorsque vous installez l'enregistrement de session, la stratégie active est **Ne pas enregistrer** (aucune session n'est enregistrée, sur aucun serveur). Pour commencer à enregistrer, utilisez la console de stratégie d'enregistrement de session pour activer une stratégie différente.

Activer l'enregistrement d'événement personnalisé

L'enregistrement de session vous permet d'utiliser des applications tierces pour insérer des données personnalisées (des événements) dans des sessions enregistrées. Ces événements apparaissent lors de la lecture de la session enregistrée. Ils font partie du fichier de la session enregistrée et ne peuvent pas être modifiés une fois la session enregistrée.

Par exemple, un événement peut contenir le texte suivant : « Ouverture de navigateur par l'utilisateur ». Chaque fois qu'un utilisateur ouvre un navigateur pendant une session en cours d'enregistrement, le texte s'insère dans l'enregistrement à ce point. Lorsqu'un observateur lit la session enregistrée, il peut localiser et compter le nombre de fois où l'utilisateur a ouvert un navigateur en notant le nombre de marqueurs.

Pour insérer des événements personnalisés dans les enregistrements sur un serveur :

- Utilisez la fenêtre **Propriétés de l'Agent d'enregistrement de session** pour activer un paramètre sur chaque serveur dans lequel vous souhaitez insérer des événements personnalisés. Activez chaque serveur séparément. Vous ne pouvez pas activer globalement tous les serveurs d'un site.
- Générez des applications sur l'API d'enregistrement d'événements s'exécutant dans chaque session virtuelle des utilisateurs (pour injecter les données dans l'enregistrement).

L'installation de l'enregistrement de session comprend une interface d'application COM (API) vous permettant d'insérer du texte provenant d'applications tierces dans un enregistrement. Vous pouvez utiliser l'API de nombreux langages de programmation, notamment Visual Basic, C++ ou C#. Pour plus d'informations, consultez l'article [CTX226844](#) du centre de connaissances. Le fichier .dll API des événements d'enregistrement de session est installé dans le cadre de l'installation de l'enregistrement de session. Vous pouvez le trouver sur `C:\rogram Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll`.

Pour activer l'enregistrement d'événements personnalisés sur un serveur, procédez comme suit :

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Dans la fenêtre **Propriétés de l'Agent d'enregistrement de session**, cliquez sur l'onglet **Enregistrement**.
4. Sous **Enregistrement d'événement personnalisé**, cochez la case **Permettre aux applications tierces d'enregistrer des données personnalisées sur ce serveur**.

Configurer la connexion au serveur d'enregistrement de session

December 21, 2022

Configurer la connexion du lecteur d'enregistrement de session au serveur d'enregistrement de session

Avant qu'un lecteur d'enregistrement de session puisse lire des sessions, configurez-le de manière à ce qu'il puisse se connecter au serveur d'enregistrement de session qui stocke les sessions enregistrées. Chaque lecteur peut être configuré avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, mais ne peut se connecter qu'à un seul serveur d'enregistrement de session à la fois. Si le lecteur est configuré avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, les utilisateurs peuvent changer de serveur d'enregistrement de session auquel connecter le lecteur.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Démarrez le lecteur d'enregistrement de session.
3. Dans la barre de menu du lecteur d'enregistrement de session, choisissez **Outils > Options**.
4. Dans l'onglet **Connexions**, cliquez sur **Ajouter**.
5. Dans le champ **Nom de l'hôte**, entrez le nom ou l'adresse IP de la machine hébergeant le serveur d'enregistrement de session et sélectionnez le protocole. L'enregistrement de session est configuré par défaut pour utiliser HTTPS/SSL afin de sécuriser les communications. Si SSL n'est pas configuré, sélectionnez HTTP.
6. Pour configurer le lecteur d'enregistrement de session avec la capacité de se connecter à plusieurs serveurs d'enregistrement de session, répétez les étapes 4 et 5 pour chaque serveur d'enregistrement de session.
7. Veillez à cocher la case correspondant au serveur d'enregistrement de session auquel vous souhaitez vous connecter.

Configurer la connexion de l'agent d'enregistrement de session au serveur d'enregistrement de session

La connexion est généralement configurée lorsque l'agent d'enregistrement de session est installé. Pour configurer cette connexion après l'installation de l'agent d'enregistrement de session, utilisez les **propriétés de l'agent d'enregistrement de session**.

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Cliquez sur l'onglet **Connexions**.
4. Dans le champ **Serveur d'enregistrement de session**, saisissez le nom de domaine complet du serveur d'enregistrement de session.

Remarque :

Pour utiliser le service Message Queuing sur HTTPS (TCP est utilisé par défaut), entrez un nom de domaine complet dans le champ **Serveur d'enregistrement de session**. Sinon, l'enregistrement de session échoue.

5. Dans la section **File d'attente des messages du gestionnaire de stockage d'enregistrement de session**, sélectionnez le protocole utilisé par le gestionnaire de stockage d'enregistrement de session pour communiquer et changer le numéro de port par défaut, si nécessaire.

Remarque :

Pour utiliser Message Queuing sur HTTP et HTTPS, installez toutes les fonctionnalités

recommandées par IIS.

6. Dans le champ **Durée de validité des messages**, acceptez la valeur par défaut de 7200 secondes (deux heures) ou tapez une nouvelle valeur pour indiquer la durée en secondes pendant laquelle chaque message est conservé dans la file d'attente en cas de panne de communication. À l'issue de cette période, le message est supprimé et le fichier n'est lisible que jusqu'au point où la perte des données s'est produite.
7. Dans la section **Broker d'enregistrement de session**, sélectionnez le protocole de communication que le broker d'enregistrement de session utilise pour communiquer et changer le numéro de port par défaut, si nécessaire.
8. À l'invite, redémarrez le **service de l'agent d'enregistrement de session** pour accepter les modifications.

Changer votre protocole de communication

December 21, 2022

Pour des raisons de sécurité, Citrix déconseille d'utiliser HTTP comme protocole de communication. L'installation de l'enregistrement de session est configurée pour utiliser le mode HTTPS. Pour utiliser HTTP au lieu de HTTPS, vous devez modifier plusieurs paramètres.

Utiliser HTTP comme protocole de communication

1. Connectez-vous à la machine hébergeant le serveur d'enregistrement de session et désactivez les connexions sécurisées pour le broker d'enregistrement de session dans IIS.
2. Changez le paramètre du protocole de HTTPS à HTTP dans **Propriétés de l'agent d'enregistrement de session** sur chaque serveur sur lequel l'Agent d'enregistrement de session est installé :
 - a) Ouvrez une session sur chaque serveur sur lequel l'agent d'enregistrement de session est installé.
 - b) À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
 - c) Dans la boîte de dialogue **Propriétés de l'Agent d'enregistrement de session**, choisissez l'onglet **Connexions**.
 - d) Dans la zone **Broker d'enregistrement de session**, sélectionnez **HTTP** dans la liste déroulante **Protocole** et choisissez **OK** pour accepter la modification. Si vous êtes invité à redémarrer le service, choisissez **Oui**.

3. Modifiez le paramètre de protocole de HTTPS à HTTP dans les paramètres du lecteur d'enregistrement de session :
 - a) Ouvrez une session sur chaque poste de travail sur lequel le lecteur d'enregistrement de session est installé.
 - b) Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
 - c) Dans la barre de menu **Lecteur d'enregistrement de session**, choisissez **Outils > Options > Connexions**, sélectionnez le serveur et choisissez **Modifier**.
 - d) Sélectionnez **HTTP** dans la liste déroulante **Protocole** et cliquez deux fois sur **OK** pour accepter le changement et quitter la boîte de dialogue.
4. Modifiez le paramètre de protocole de HTTPS à HTTP dans la console de stratégie d'enregistrement de session :
 - a) Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
 - b) À partir du menu **Démarrer**, choisissez **Console de stratégie d'enregistrement de session**.
 - c) Sélectionnez **HTTP** dans la liste déroulante **Protocole** et cliquez sur **OK** pour vous connecter. Si la connexion est établie, ce paramètre est mémorisé lorsque vous lancez la console de stratégie d'enregistrement de session la fois suivante.

Rétablir HTTPS en tant que protocole de communication

1. Connectez-vous à la machine hébergeant le serveur d'enregistrement de session et activez les connexions sécurisées pour le broker d'enregistrement de session dans IIS.
2. Changez le paramètre du protocole de HTTP à HTTPS dans chaque boîte de dialogue **Propriétés de l'agent d'enregistrement de session** :
 - a) Ouvrez une session sur chaque serveur sur lequel l'agent d'enregistrement de session est installé.
 - b) À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
 - c) Dans la boîte de dialogue **Propriétés de l'Agent d'enregistrement de session**, choisissez l'onglet **Connexions**.
 - d) Dans la zone **Broker d'enregistrement de session**, sélectionnez **HTTPS** dans la liste déroulante **Protocole** et choisissez **OK** pour accepter la modification. Si vous êtes invité à redémarrer le service, choisissez **Oui**.
3. Modifiez le paramètre de protocole de HTTP à HTTPS dans les paramètres du lecteur d'enregistrement de session :

- a) Ouvrez une session sur chaque poste de travail sur lequel le lecteur d'enregistrement de session est installé.
 - b) Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
 - c) Dans la barre de menu **Lecteur d'enregistrement de session**, choisissez **Outils > Options > Connexions**, sélectionnez le serveur et choisissez **Modifier**.
 - d) Sélectionnez **HTTPS** dans la liste déroulante **Protocole** et cliquez deux fois sur **OK** pour accepter le changement et quitter la boîte de dialogue.
4. Modifiez le paramètre de protocole de HTTP à HTTPS dans la console de stratégie d'enregistrement de session :
- a) Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
 - b) À partir du menu **Démarrer**, choisissez **Console de stratégie d'enregistrement de session**.
 - c) Sélectionnez **HTTPS** dans la liste déroulante **Protocole** et cliquez sur **OK** pour vous connecter. Si la connexion est établie, ce paramètre est mémorisé lorsque vous lancez la console de stratégie d'enregistrement de session la fois suivante.

Configurer les paramètres sur le serveur d'enregistrement de session

December 21, 2022

Cette section décrit les paramètres suivants :

- [Autoriser les utilisateurs](#)
- [Personnaliser les messages de notification](#)
- [Spécifier l'emplacement du stockage des enregistrements](#)
- [Spécifier la taille du fichier pour les enregistrements](#)
- [Activer ou désactiver les signatures numériques](#)
- [Configurer le programme CEIP](#)

Autoriser les utilisateurs

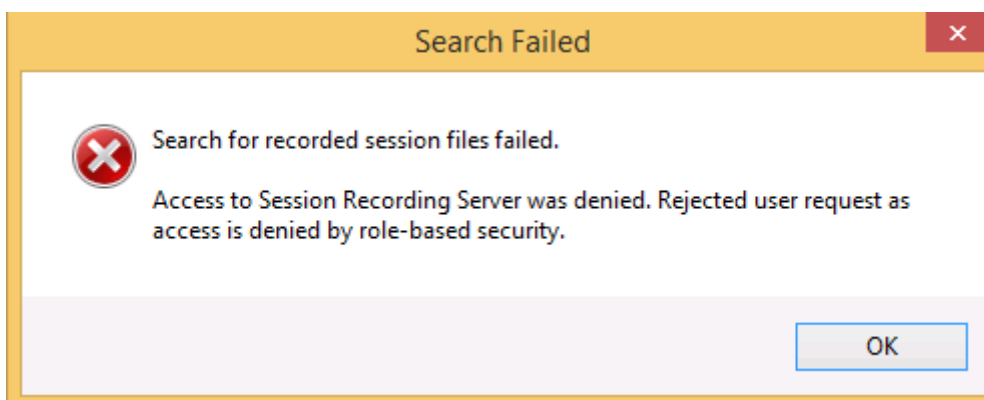
February 20, 2024

Pour accorder des droits aux utilisateurs, vous leur attribuez des rôles par le biais de la console d'autorisation d'enregistrement de session sur le serveur d'enregistrement de session. Cinq rôles sont disponibles :

Important :

pour des raisons de sécurité, veillez à accorder uniquement aux utilisateurs les droits nécessaires à l'accomplissement de fonctions précises, comme l'affichage de sessions enregistrées par exemple.

- **PolicyAdministrator.** Ce rôle donne le droit d'afficher, de créer, de modifier, de supprimer et d'activer les stratégies d'enregistrement. Par défaut, les administrateurs de la machine hébergeant le serveur d'enregistrement de session sont membres de ce rôle.
- **PolicyQuery.** Cette option permet aux serveurs hébergeant l'agent d'enregistrement de session de demander des évaluations de stratégie d'enregistrement. Par défaut, les utilisateurs authentifiés sont membres de ce rôle.
- **LoggingWriter.** Ce rôle donne le droit d'écrire dans les journaux de l'administrateur. Par défaut, le groupe Administrateurs local et le groupe Service réseau sont membres de ce rôle. La modification de l'appartenance à **LoggingWriter** par défaut peut entraîner l'échec de la journalisation.
- **LoggingReader.** Ce rôle donne le droit d'interroger les journaux de l'administrateur. Ce rôle n'est rattaché à aucune appartenance par défaut.
- **PrivilegedPlayer.** Accorde le droit d'imposer et de supprimer des restrictions d'accès aux enregistrements et le droit d'archiver et de supprimer des enregistrements.
- **Lecteur.** Accorde le droit d'afficher les sessions Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) enregistrées. Ce rôle n'est rattaché à aucune appartenance par défaut. Lorsque vous installez l'enregistrement de session, aucun utilisateur n'est autorisé à lire les sessions enregistrées. Un utilisateur qui n'est pas autorisé à lire des sessions enregistrées reçoit le message d'erreur suivant lorsqu'il essaye de lire une session enregistrée :



Pour attribuer des utilisateurs à un rôle, procédez comme suit :

1. Ouvrez une session en tant qu'administrateur sur la machine hébergeant le serveur d'enregistrement de session.
2. Démarrez la console d'autorisation d'enregistrement de session.
3. Sélectionnez le rôle que vous souhaitez attribuer aux utilisateurs.
4. Dans la barre de menu, choisissez **Action > Attribuer des utilisateurs et des groupes**.
5. Ajoutez les utilisateurs et les groupes.

L'enregistrement de session prend en charge les utilisateurs et les groupes définis dans Active Directory.

Toute modification apportée à la console prend effet au cours de la mise à jour, qui se produit toutes les minutes. En outre, à partir de la version 1906, vous pouvez utiliser la console de stratégie d'enregistrement de session pour créer des stratégies de visionnage d'enregistrement. Pour de plus amples informations, consultez la section [Stratégies de visionnage d'enregistrement](#).

Configurer le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP)

April 3, 2024

Lorsque vous participez au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP), des données de configuration et d'utilisation anonymes sont collectées et envoyées à Citrix. Ces données contribuent à améliorer la qualité et les performances du produit. En outre, une copie des données anonymes est envoyée à Google Analytics pour une analyse rapide et efficace.

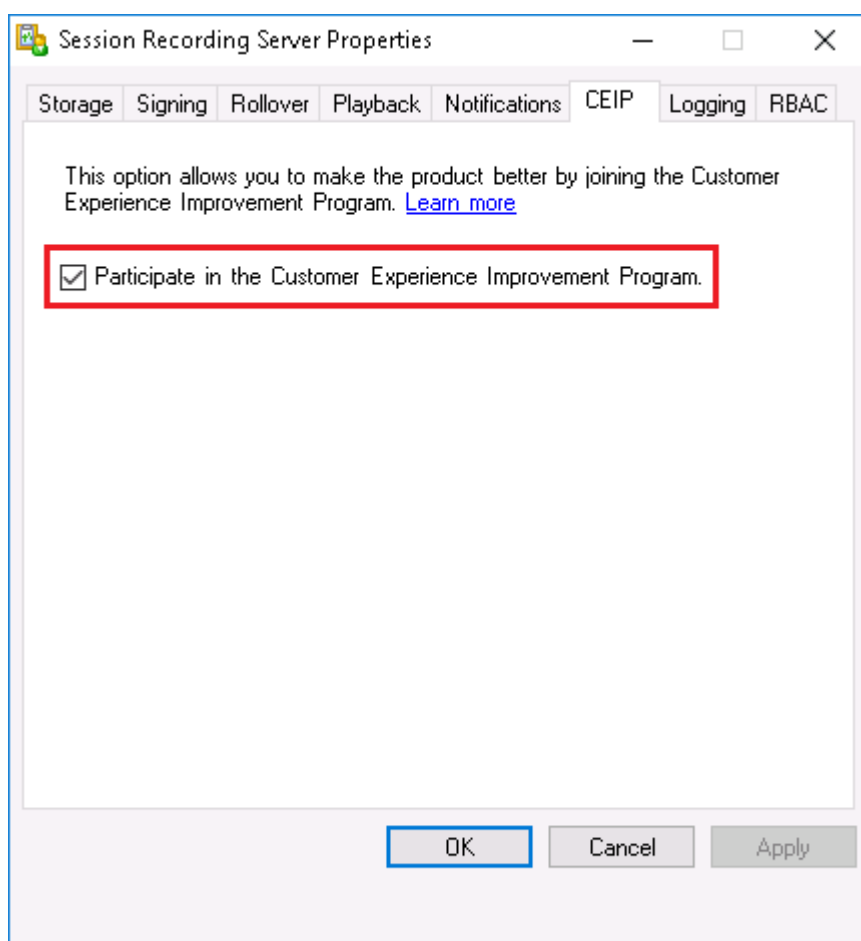
Paramètres

Paramètre du programme CEIP

Par défaut, vous participez automatiquement au programme CEIP lorsque vous installez l'enregistrement de session. Le premier chargement de données se produit approximativement sept jours après l'installation de l'enregistrement de session. Pour vous désabonner de CEIP, procédez comme suit :

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **CEIP**.
4. Désactivez la case à cocher **Participer au programme d'amélioration de l'expérience utilisateur**.

5. Redémarrez le **service d'analyse de l'enregistrement de session Citrix** pour que le paramètre prenne effet.



Paramètre Google Analytics

Lorsque Google Analytics est activé, les données de pulsation entre Google Analytics et le serveur d'enregistrement de session sont collectées toutes les 5 heures. Des données sur le comportement des utilisateurs sur le lecteur Web sont également envoyées à Google Analytics. Le comportement de l'utilisateur inclut des activités telles que l'ouverture du lecteur Web et la lecture ou la recherche d'enregistrements qu'il contient.

Paramètre de Registre qui active ou désactive Google Analytics (valeur par défaut = 0) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\

Nom : CeipHeartBeatDisable

Valeur : 1 = désactivé, 0 = activé

Lorsqu'aucune valeur n'est spécifiée, Google Analytics est activé.

Pour désactiver Google Analytics :

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. Ouvrez l'**Éditeur du Registre**.
3. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\`.
4. Ajoutez une valeur de registre et nommez-la **CeipHeartBeatDisable**.
5. Définissez les données de la valeur de **CeipHeartBeatDisable** sur 1.
6. Redémarrez le service d'analyse de l'enregistrement de session Citrix pour que le paramètre prenne effet.

Données collectées à partir du serveur d'enregistrement de session

Le tableau suivant présente un exemple de types d'informations anonymes collectées. Les données ne contiennent aucun détail permettant d'identifier le client.

Point de données	Nom de la clé	Description
GUID de machine	<code>machine_guid</code>	Identification de la machine d'où les données proviennent. Lorsque Google Analytics est activé, les données de pulsation sont envoyées à Google Analytics, que le programme CEIP soit activé ou non.
Version du système d'exploitation	<code>OS_version</code>	Chaîne de texte indiquant le système d'exploitation de la machine. Lorsque Google Analytics est activé, les données de pulsation sont envoyées à Google Analytics, que le programme CEIP soit activé ou non.

Point de données	Nom de la clé	Description
Version du serveur d'enregistrement de session	<code>SRS_version</code>	Chaîne de texte indiquant la version installée du serveur d'enregistrement de session. Lorsque Google Analytics est activé, les données de pulsation sont envoyées à Google Analytics, que le programme CEIP soit activé ou non.
Nombre d'enregistrements associés à l'application	<code>application-recording-number</code>	Entier indiquant le nombre de fichiers d'enregistrement associés à l'application. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Nombre d'enregistrements	<code>recording-number</code>	Entier indiquant le nombre de fichiers d'enregistrement associés à l'application et au bureau. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Nombre d'enregistrements dynamiques	<code>dynamic-recording-number</code>	Entier indiquant le nombre de fichiers enregistrés dynamiquement. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Nombre d'agents hébergeant des sessions enregistrées	<code>recorded-agent-number</code>	Entier indiquant le nombre de VDA hébergeant des sessions enregistrées. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Nombre d'agents hébergeant des sessions enregistrées contenant des événements journalisés	<code>event-logging-enabled-agent-number</code>	Entier indiquant le nombre de VDA hébergeant des sessions enregistrées contenant des événements journalisés. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.

Point de données	Nom de la clé	Description
Nombre d'enregistrements contenant des événements journalisés	<code>event-logging-recording-number</code>	Entier indiquant le nombre de fichiers d'enregistrement contenant des événements journalisés. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Activation de la journalisation de l'administrateur	<code>admin-logging-status</code>	Chiffre indiquant l'activation de la journalisation de l'administrateur. 1 = activé ; 0 = désactivé. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Nombre d'événements journalisés	<code>collected-events-number</code>	Entier indiquant le nombre d'événements journalisés. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Nombre de stratégies personnalisées	<code>customized-policies-number</code>	Entier indiquant le nombre de stratégies personnalisées pour l'enregistrement de session et la journalisation d'événements. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Activation de l'équilibrage de charge	<code>load-balancing-status</code>	Chiffre indiquant l'activation de l'équilibrage de charge. 1 = activé ; 0 = désactivé. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.
Activation de la stratégie de visionnage d'enregistrement	<code>rbac-status</code>	Chiffre indiquant l'activation de la stratégie de visionnage d'enregistrement. 1 = activé ; 0 = désactivé. Les données sont envoyées lorsque Google Analytics et CEIP sont activés.

Personnaliser les messages de notification

April 4, 2024

Si la stratégie d'enregistrement active enregistre des sessions avec notification, les utilisateurs reçoivent des notifications d'enregistrement après avoir saisi leurs informations d'identification. Le message de notification par défaut est : **Votre activité relative au bureau ou aux programmes démarrés récemment est enregistrée. Si vous y êtes opposé, fermez le bureau ou les programmes en question.** Les utilisateurs peuvent cliquer sur **OK** pour fermer la fenêtre et pour continuer leurs sessions.

Le message de notification par défaut s'affiche dans la langue du système d'exploitation du VDA.

Vous pouvez créer des notifications personnalisées dans les langues que vous choisissez. Cependant, vous ne pouvez avoir qu'un seul message de notification pour chaque langue. Vos utilisateurs voient les messages de notification dans la langue correspondant à leurs paramètres locaux préférés.

Créer un message de notification

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Notifications**.
4. Cliquez sur **Ajouter**.
5. Choisissez la langue du message et tapez le nouveau message. Vous ne pouvez créer qu'un seul message par langue.

Une fois accepté et activé, le nouveau message s'affiche dans la boîte Messages de notification en langues étrangères.

Activer ou désactiver les signatures numériques

December 21, 2022

Vous pouvez installer des certificats sur les machines sur lesquelles vous avez installé le serveur d'enregistrement de session et le lecteur d'enregistrement de session. La sécurité de votre déploiement peut être renforcée lorsque vous attribuez des signatures numériques à l'enregistrement de session.

Par défaut, la fonction de signature numérique est désactivée. Après avoir sélectionné le certificat utilisé pour signer les enregistrements, l'enregistrement de session accorde une autorisation d'accès en lecture au Gestionnaire de stockage d'enregistrement de session.

Activer les signatures numériques

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du serveur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Signature**.
4. Recherchez le certificat qui permet la communication sécurisée entre les machines sur lesquelles vous avez installé les composants d'enregistrement de session.

Désactiver les signatures numériques

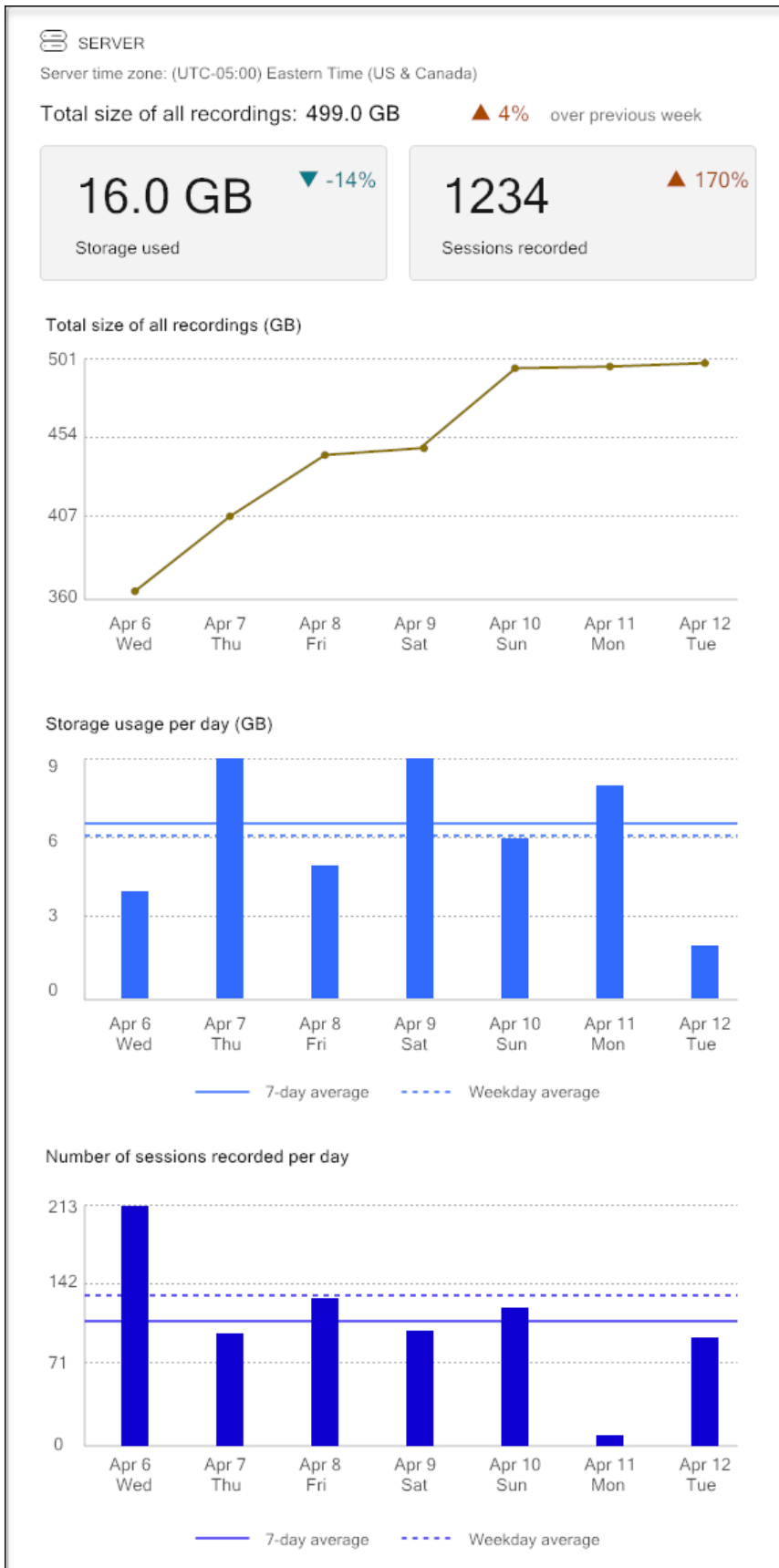
1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du serveur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Signature**.
4. Cliquez sur **Effacer**.

Rapports de stockage d'enregistrement de session

February 20, 2024

Vue d'ensemble

Un rapport de stockage d'enregistrement de session fournit des statistiques hebdomadaires sur les enregistrements d'écran d'un ou de plusieurs serveurs d'enregistrement de session à charge équilibrée. Il vous est envoyé par e-mail et contient des diagrammes condensés similaires aux suivants :

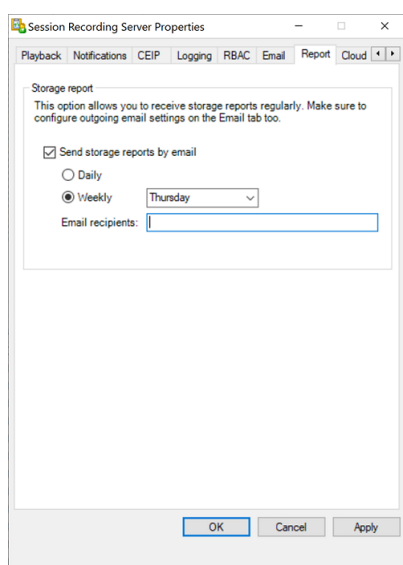


Configuration

Pour recevoir des rapports de stockage d'enregistrement de session par e-mail une fois par jour ou une fois par semaine, planifiez des rapports via les propriétés du serveur d'enregistrement de session. Assurez-vous également de configurer les paramètres des e-mails sortants dans l'onglet **E-mail**.

Remarque :

Si vos serveurs d'enregistrement de session sont configurés de manière à équilibrer la charge, planifiez les rapports sur l'un des serveurs. Sinon, créez une planification sur chacun de vos serveurs d'enregistrement de session.



Spécifier la taille du fichier pour les enregistrements

February 20, 2024

À mesure que la taille des enregistrements augmente, les fichiers d'enregistrement prennent plus longtemps à se télécharger et réagissent plus lentement lorsque vous utilisez le curseur de recherche pour naviguer pendant la lecture. Pour contrôler la taille des fichiers, spécifiez un seuil limite. Lorsque l'enregistrement atteint cette limite, l'enregistrement de session ferme le fichier et crée un fichier supplémentaire afin de poursuivre l'enregistrement. Cette action s'appelle une substitution.

Vous pouvez préciser deux seuils pour une substitution :

- **Taille du fichier.** Le fichier en cours se ferme lorsqu'il atteint cette taille et un nouveau fichier s'ouvre. Par défaut, la substitution se produit lorsque la taille dépasse 50 Mo. Valeurs prises en charge : 10 à 300.

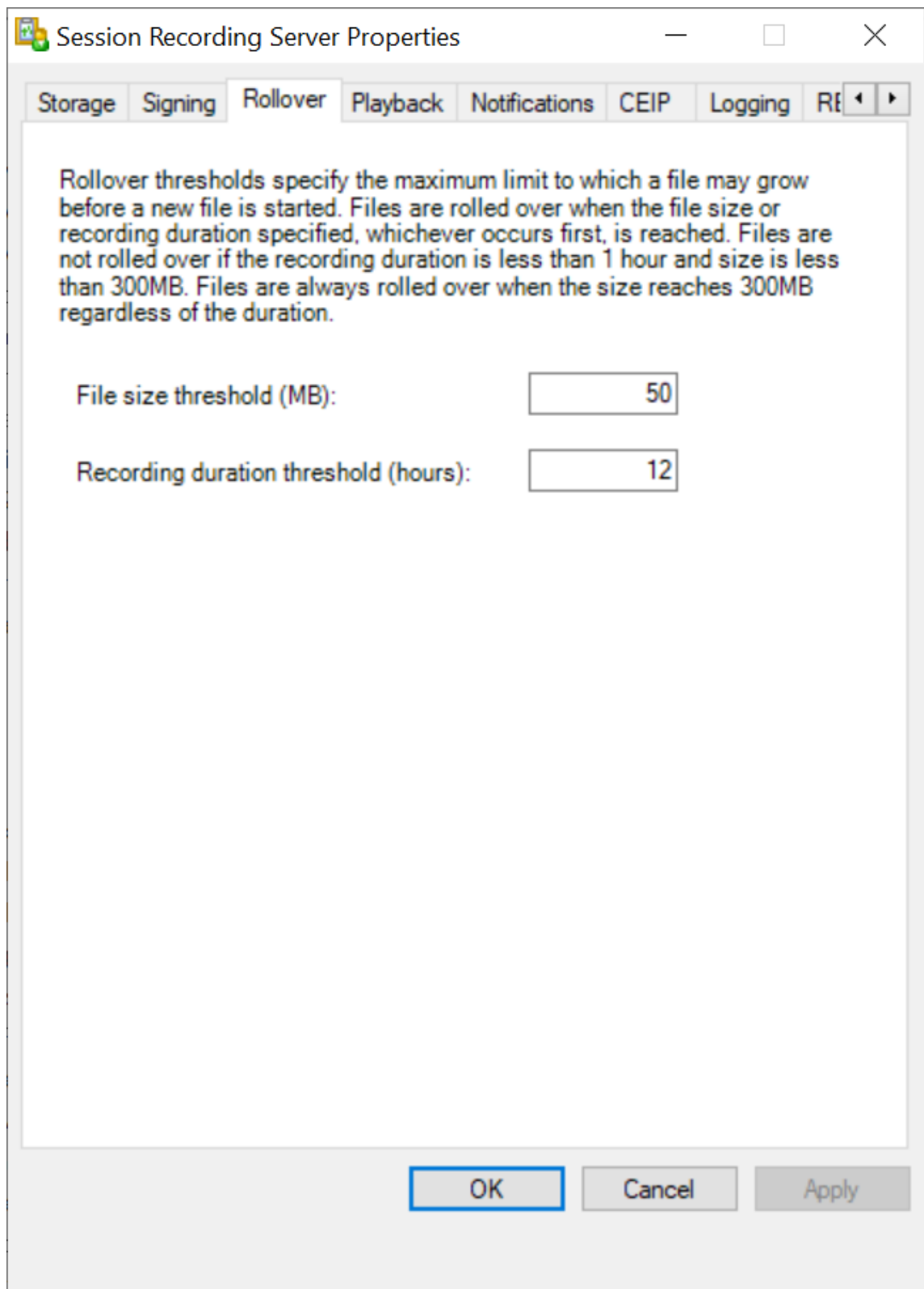
- **Durée.** Lorsque la durée est atteinte, le fichier en cours se ferme et un nouveau fichier s'ouvre. Par défaut, la substitution se produit lorsque la session enregistre pendant 12 heures. Valeurs prises en charge : 1 à 24.

Les substitutions se produisent lorsque la première des deux conditions ci-dessus est remplie. Par exemple, vous pouvez spécifier 17 Mo pour la taille du fichier et 6 heures pour la durée. Lorsque votre enregistrement atteint 17 Mo en 3 heures, l'enregistrement de session ferme le fichier et en ouvre un nouveau.

Pour éviter de créer trop de fichiers de petite taille, l'enregistrement de session ne procède à aucune substitution avant qu'une heure au moins ne se soit écoulée, quelle que soit la valeur spécifiée pour la taille de fichier. L'exception à cette règle est si la taille du fichier dépasse 300 Mo.

Définir la taille maximale des fichiers pour les enregistrements

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du serveur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Substitution**.



4. Entrez un nombre entier compris entre 10 et 300 pour spécifier la taille maximale des fichiers, en Mo.

5. Entrez un nombre entier compris entre 1 et 24 pour spécifier la durée maximale des enregistrements, en heures.

Spécifier l'emplacement du stockage des enregistrements

February 20, 2024

Utilisez la fenêtre **Propriétés du serveur d'enregistrement de session** pour spécifier l'emplacement du stockage des enregistrements et l'emplacement de restauration des enregistrements restaurés pour la lecture.

Vous pouvez stocker des enregistrements sur un lecteur local, un volume réseau SAN et un chemin réseau UNC complet. À partir de la version 2103, vous pouvez stocker des enregistrements dans des partages de fichiers Azure. Pour de plus amples informations, consultez la section [Configurer un partage de fichiers Azure pour stocker des enregistrements](#) plus loin dans cet article.

Remarque :

- Le stockage des données sur un serveur NAS basé sur des protocoles basés sur des fichiers tels que SMB et NFS, peut avoir d'importantes répercussions sur les performances et la sécurité. Utilisez la dernière version du protocole pour éviter toute incidence sur la sécurité et effectuez des tests de scalabilité pour garantir des performances adéquates.
- Pour archiver les fichiers ou restaurer les fichiers supprimés, utilisez la commande [ICLDB](#).

Spécifier un ou plusieurs dossiers pour stocker les enregistrements et un dossier pour restaurer les enregistrements archivés

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du serveur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Stockage**.
4. Utilisez la liste **Répertoire de stockage des fichiers** pour gérer les dossiers dans lesquels les enregistrements sont stockés.

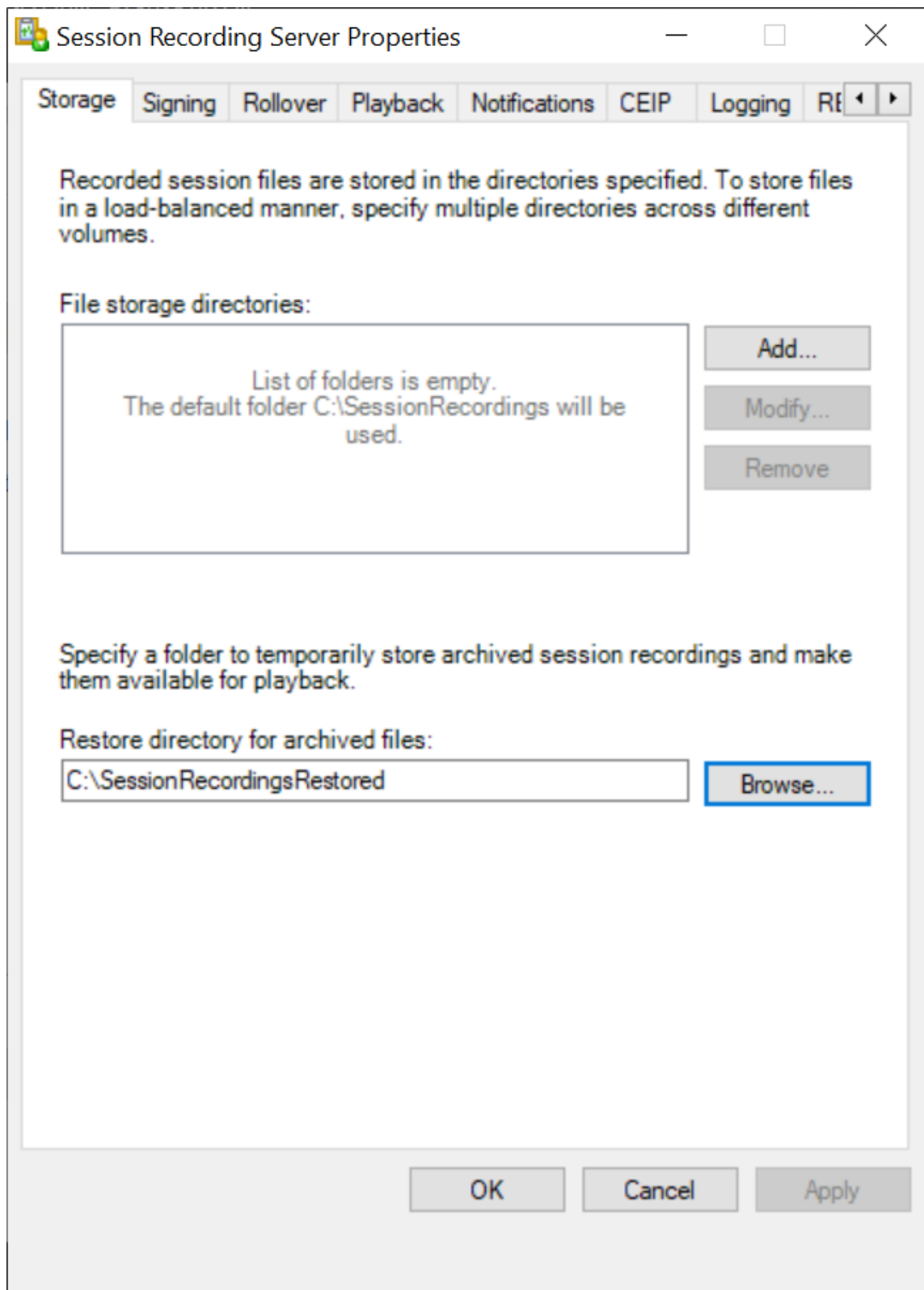
Après la sélection des dossiers, l'enregistrement de session accorde à son service les autorisations de contrôle total sur ces dossiers.

Par défaut, les enregistrements sont stockés dans le dossier **<drive>:SessionRecordings** de la machine hébergeant le serveur d'enregistrement de session. Vous pouvez modifier le dossier de stockage des enregistrements, ajouter des dossiers supplémentaires afin d'équilibrer la

charge sur plusieurs volumes ou utiliser plus d'espace. La présence de plusieurs dossiers dans la liste indique que l'équilibrage de la charge s'applique dans les dossiers pour les enregistrements. L'équilibrage de charge passe successivement dans tous les dossiers.

5. Dans le champ **Restaurer le répertoire des fichiers archivés**, tapez le dossier dans lequel restaurer les enregistrements archivés.

Par défaut, les enregistrements archivés sont restaurés dans le dossier **<drive>:SessionRecordingsRestore** de la machine hébergeant le serveur d'enregistrement de session. Vous pouvez modifier le dossier.



Configurer un partage de fichiers Azure pour stocker des enregistrements

Pour créer un partage de fichiers Azure pour stocker des enregistrements, procédez comme suit :

1. Dans le [portail Azure](#), créez un compte de stockage, puis créez un partage de fichiers Azure.

Pour obtenir un guide de démarrage rapide, consultez la section [Créer et gérer des partages de fichiers Azure avec le portail Azure](#). Le tableau suivant vous recommande de prendre en considération ces configurations.

Taille du fichier d'enregistrement Mo/heure	Nombre de sessions	Type de partage de fichiers	Quota de partage de fichiers (To)	Nombre de serveur d'enregistrement de session	Taille du serveur d'enregistrement de session
< 6.37	< 1,000	Disque standard HDD (StorageV2)	2	1	Standard D4as_v4
< 6.37	1,000–2,000	SSD Premium	3	1	Standard D4as_v4
< 6.37	2,000–3,000	SSD Premium	5	1	Standard D4as_v4
< 6.37	3,000–4,000	SSD Premium	6	1	Standard D4as_v4
Environ 10	< 1,000	Disque standard HDD (StorageV2)	3	1	Standard D4as_v4
Environ 10	1,000–2,500	SSD Premium	6	1	Standard D4as_v4
Environ 10	2,500–4,000	SSD Premium	10	2	Standard D4as_v4

Le quota de partage de fichiers est calculé en fonction de huit heures par jour, de 23 jours ouvrables par mois et d'une période de conservation d'un mois pour chaque fichier d'enregistrement.

2. Ajoutez les informations d'identification du partage de fichiers Azure à l'hôte sur lequel vous avez installé le serveur d'enregistrement de session.
 - a) Démarrez une invite de commandes en tant qu'administrateur et remplacez le lecteur dans le dossier **<chemin d'installation du serveur d'enregistrement de session>\Bin**.
Par défaut, le serveur d'enregistrement de session est installé dans `C:\Program Files\Citrix\SessionRecording\Server`.

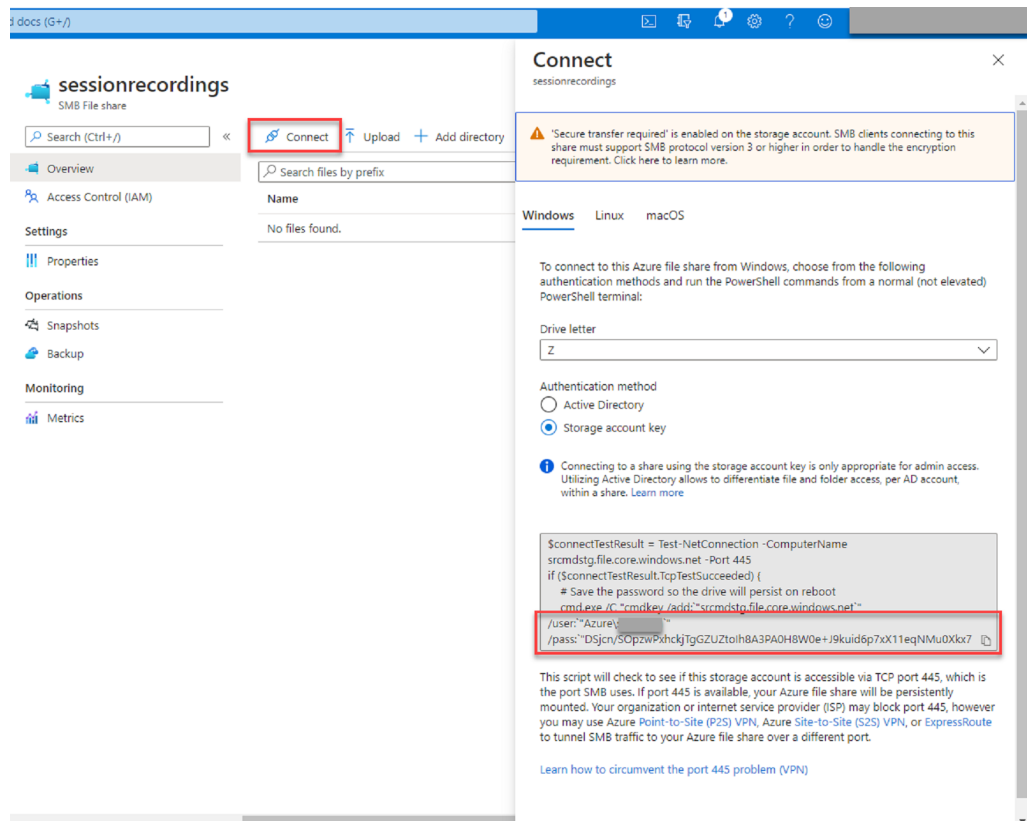
b) Exécutez la commande **SsRecUtils.exe -AddAzureFiles <storageAccountName> <file-ShareName> <accesskey>**

Où,

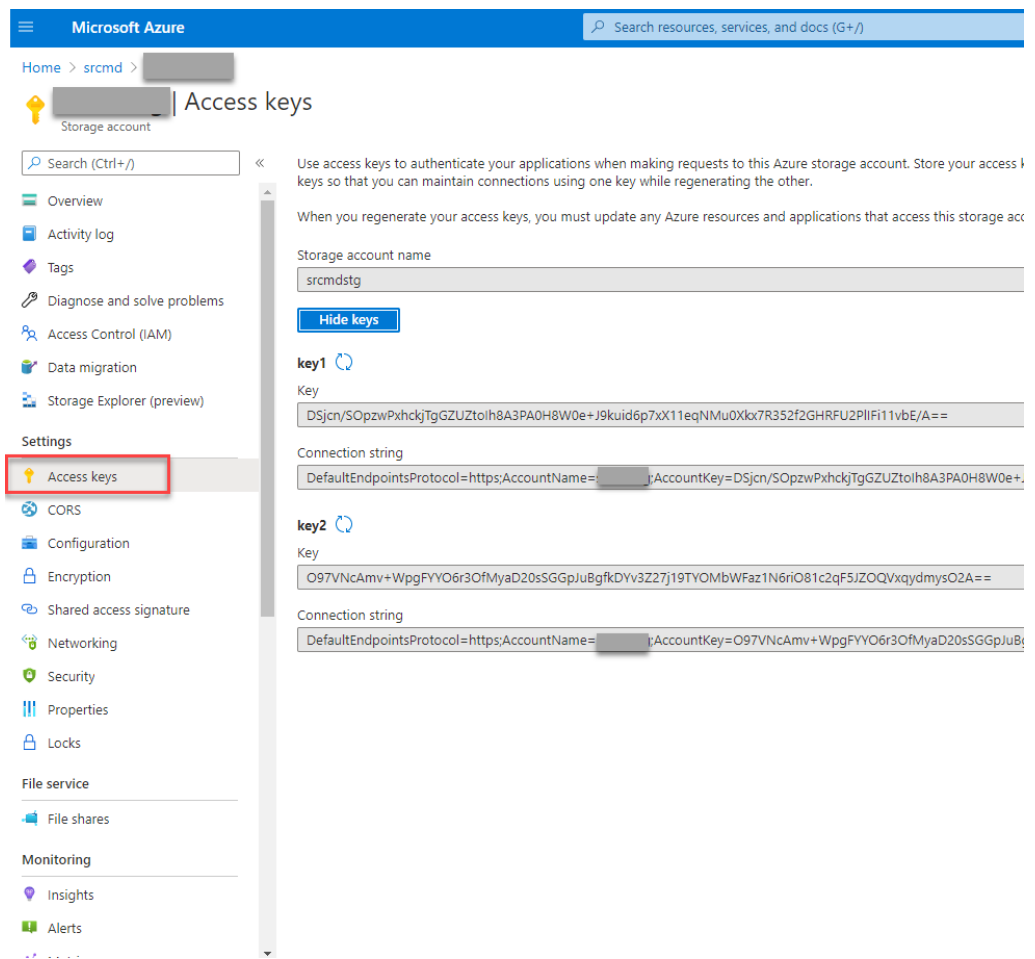
- **<storageaccountname>** est le nom de votre compte de stockage dans Azure.
- **<filesharename>** est le nom du partage de fichiers contenu dans votre compte de stockage.
- **<accesskey>** est votre clé de compte de stockage qui peut être utilisée pour accéder au partage de fichiers.

Il existe deux façons d'obtenir votre clé de compte de stockage :

- Vous pouvez obtenir votre clé de compte de stockage à partir de la chaîne de connexion qui apparaît lorsque vous cliquez sur le bouton **Connecter** sur votre page de partage de fichiers.

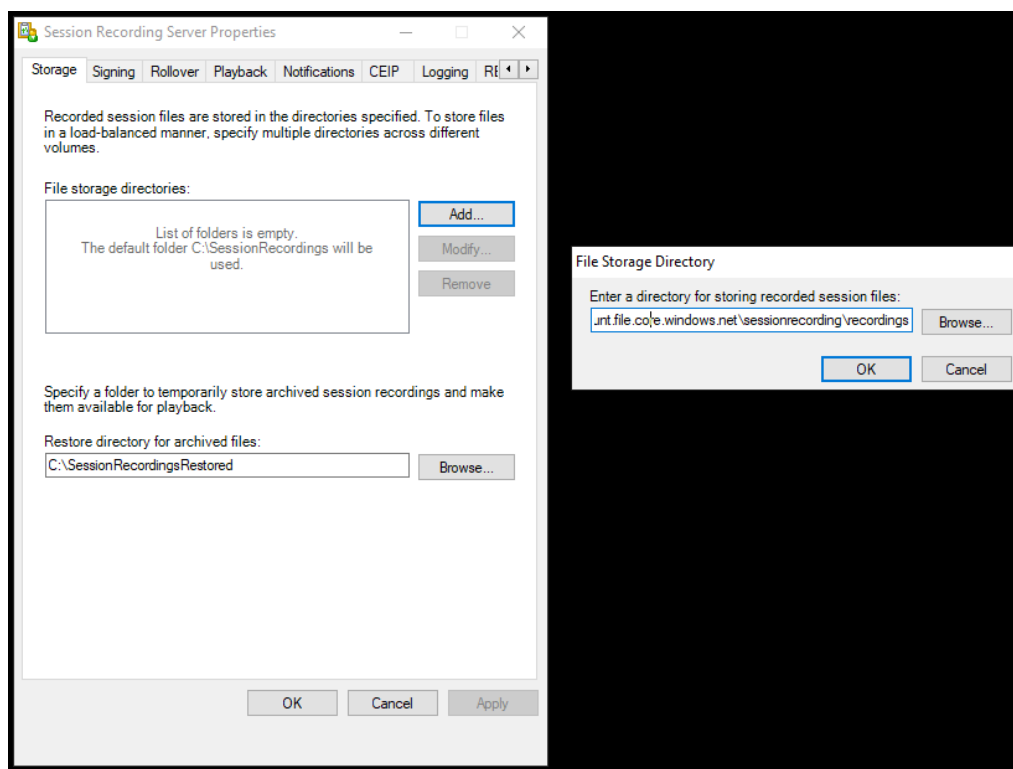


- Vous pouvez également obtenir votre clé de compte de stockage en cliquant sur **Clés d'accès** dans le panneau de navigation de gauche de la page de votre compte de stockage.

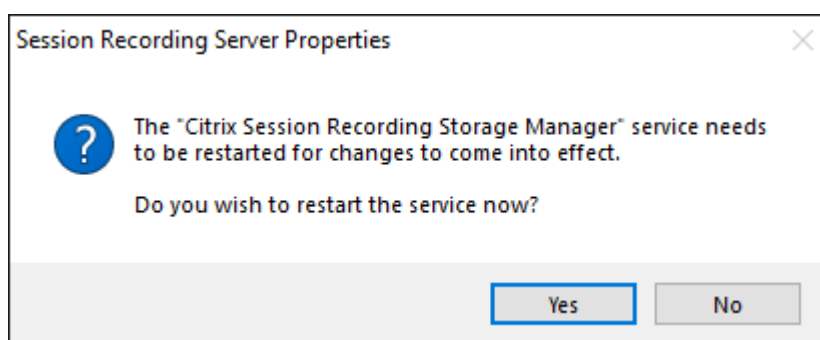


- c) Montez le partage de fichiers Azure sur l'hôte sur lequel vous avez installé le serveur d'enregistrement de session.
- i. Ouvrez **Propriétés du serveur d'enregistrement de session**.
 - ii. Cliquez sur **Ajouter** sur l'onglet **Stockage**.
 - iii. Entrez le chemin UNC au format `\\<storageaccountname>.file.core.windows.net\\<filessharename>`

Spécifiez un sous-dossier sous le partage de fichiers pour stocker vos fichiers d'enregistrement. Le serveur d'enregistrement de session crée automatiquement le sous-dossier.



- iv. Cliquez sur **OK** dans la boîte de dialogue **Répertoire de stockage des fichiers**.
- v. Cliquez sur **Appliquer** dans la fenêtre **Propriétés du serveur d'enregistrement de session**.
- vi. Cliquez sur **OK** une fois que l'option **Appliquer** devient grisée.
- vii. Cliquez sur **Oui** lorsque vous êtes invité à redémarrer le service Gestionnaire de stockage d'enregistrement de session.



Stratégies

April 3, 2024

Utilisez la console de stratégie d'enregistrement de session pour créer des stratégies d'enregistrement, des stratégies de détection d'événements, des stratégies de réponse aux événements et des stratégies de visionnage d'enregistrement. Lors de la création de stratégies, vous pouvez spécifier des Delivery Controller à partir des environnements locaux et Citrix Cloud.

Important :

Pour utiliser la console de stratégie d'enregistrement de session, le Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) ou le SDK Citrix DaaS Remote PowerShell (Citrix-PoshSdk.exe) doit être installé manuellement. Recherchez le composant logiciel enfichable Broker PowerShell sur l'ISO Citrix Virtual Apps and Desktops (`\\layout\image-full\x64\Citrix Desktop Delivery Controller`). Vous pouvez également télécharger le [SDK Citrix DaaS Remote PowerShell](#) à partir de la [page de téléchargement de Citrix DaaS \(anciennement Citrix Virtual Apps and Desktops Service\)](#).

Conseil :

Vous pouvez modifier le Registre de façon à éviter la perte de fichiers d'enregistrement au cas où votre serveur d'enregistrement de session pourrait échouer de façon inattendue. Ouvrez une session en tant qu'administrateur sur la machine sur laquelle vous avez installé l'agent d'enregistrement de session, ouvrez l'Éditeur du Registre et ajoutez une valeur DWORD `DefaultRecordActionOnError=1` sous `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent`.

Activer une stratégie

1. Ouvrez une session en tant qu'administrateur sur la machine sur laquelle vous avez installé la console de stratégie d'enregistrement de session.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si la fenêtre **Se connecter au serveur d'enregistrement de session** s'affiche, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur **OK**.
4. Dans la console de stratégie d'enregistrement de session, développez le type de stratégie cible.
5. Sélectionnez la stratégie que vous souhaitez activer.
6. Dans la barre de menu, choisissez **Activer la stratégie**.

Modifier une stratégie

1. Ouvrez une session en tant qu'administrateur sur la machine sur laquelle vous avez installé la console de stratégie d'enregistrement de session.
2. Démarrez la console de stratégie d'enregistrement de session.

3. Si la fenêtre **Se connecter au serveur d'enregistrement de session** s'affiche, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur **OK**.
4. Dans la console de stratégie d'enregistrement de session, développez le type de stratégie cible.
5. Sélectionnez la stratégie que vous souhaitez modifier. Les règles de cette stratégie s'affichent dans le volet droit.
6. Pour ajouter, modifier ou supprimer une règle :
 - Dans la barre de menu, choisissez **Ajouter une nouvelle règle**. Si cette stratégie est active, une fenêtre indépendante s'affiche pour demander confirmation de l'action entreprise. Utilisez l'assistant **Règles** pour créer une règle.
 - Sélectionnez la règle que vous souhaitez modifier, cliquez avec le bouton droit de la souris et choisissez **Propriétés**. Utilisez l'assistant **Règles** pour modifier la règle.
 - Sélectionnez la règle que vous souhaitez supprimer, cliquez avec le bouton droit de la souris et choisissez **Supprimer la règle**.

Supprimer une stratégie

Remarque :

Vous ne pouvez pas supprimer une stratégie définie par le système ou une stratégie active.

1. Ouvrez une session en tant qu'administrateur sur la machine sur laquelle vous avez installé la console de stratégie d'enregistrement de session.
2. Démarrez la console de stratégie d'enregistrement de session.
3. Si la fenêtre **Se connecter au serveur d'enregistrement de session** s'affiche, veillez à ce que le nom du serveur d'enregistrement de session, le protocole et le port sont corrects. Cliquez sur **OK**.
4. Dans la console de stratégie d'enregistrement de session, développez le type de stratégie cible.
5. Dans le panneau gauche, sélectionnez la stratégie que vous souhaitez supprimer. Si la stratégie est active, vous devez en activer une autre.
6. Dans la barre de menu, choisissez **Supprimer la stratégie**.
7. Sélectionnez **Oui** pour confirmer l'action.

Configurer les stratégies d'enregistrement de session

February 20, 2024

Vous pouvez activer les stratégies d'enregistrement définies par le système ou créer et activer vos propres stratégies personnalisées. Les stratégies d'enregistrement définies par le système appliquent

une seule règle à des sessions entières. Les stratégies d'enregistrement personnalisées spécifient les sessions qui sont enregistrées.

La stratégie d'enregistrement active détermine quelles sessions sont enregistrées. Une seule stratégie d'enregistrement peut être active à la fois.

Stratégies d'enregistrement définies par le système

L'enregistrement de session fournit les stratégies d'enregistrement définies par le système suivantes :

- **Ne pas enregistrer.** Stratégie par défaut. Si vous ne précisez pas d'autre stratégie, aucune session n'est enregistrée.
- **Enregistrer uniquement les événements (pour tous, avec notification).** Cette stratégie enregistre uniquement les événements spécifiés par votre stratégie de détection d'événements. Elle n'enregistre pas d'écrans. Les utilisateurs reçoivent des notifications d'enregistrement à l'avance.
- **Enregistrer uniquement les événements (pour tous, sans notification).** Cette stratégie enregistre uniquement les événements spécifiés par votre stratégie de détection d'événements. Elle n'enregistre pas d'écrans. Les utilisateurs ne reçoivent pas de notifications d'enregistrement.
- **Enregistrer sessions entières (pour tous, avec notification).** Cette stratégie enregistre des sessions entières (écrans et événements). Les utilisateurs reçoivent des notifications d'enregistrement à l'avance.
- **Enregistrer sessions entières (pour tous, sans notification).** Cette stratégie enregistre des sessions entières (écrans et événements). Les utilisateurs ne reçoivent pas de notifications d'enregistrement.

Vous ne pouvez pas modifier ou supprimer les stratégies d'enregistrement définies par le système.

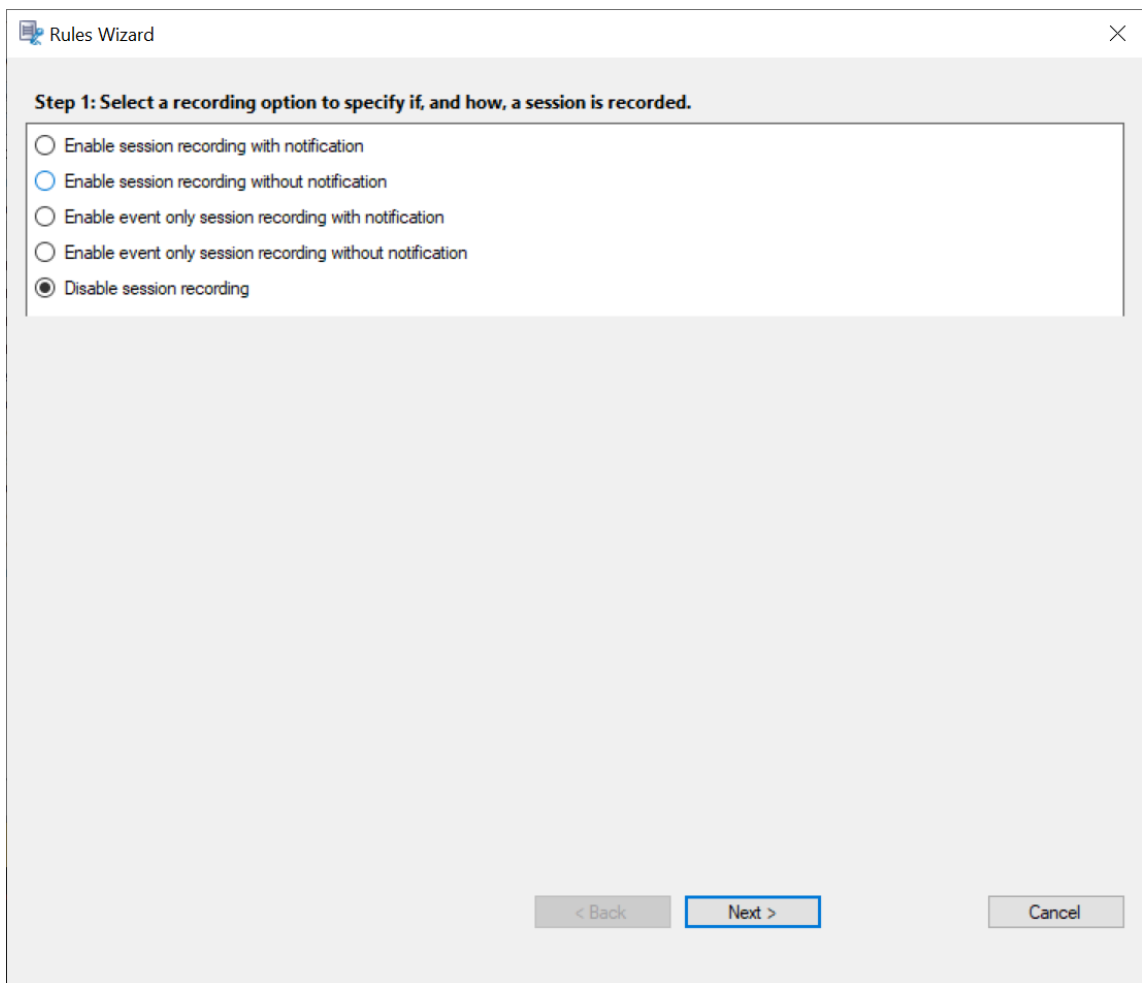
Créer une stratégie d'enregistrement personnalisée

Vous pouvez enregistrer des sessions spécifiques à des utilisateurs ou des groupes définis, à des applications ou des bureaux publiés, à des groupes de mise à disposition ou des machines VDA, ainsi qu'aux adresses IP du client de l'application Citrix Workspace. Un assistant intégré à la console de stratégie d'enregistrement de session vous aide à créer des règles. Pour obtenir la liste des applications publiées ou des bureaux publiés, ainsi que la liste des groupes de mise à disposition ou des machines VDA, vous devez disposer d'autorisations d'accès en lecture de l'administrateur du site. Configurez l'autorisation de lecture de l'administrateur sur le Delivery Controller du site.

Pour chaque règle que vous créez, vous spécifiez une action d'enregistrement et un critère de règle. L'action d'enregistrement s'applique aux sessions qui correspondent au critère de règle.

Pour chaque règle, choisissez une action d'enregistrement :

- **Activer l'enregistrement de session avec notification.** Cette option enregistre des sessions entières (écrans et événements). Les utilisateurs reçoivent des notifications d'enregistrement à l'avance.
- **Activer l'enregistrement de session sans notification.** Cette option enregistre des sessions entières (écrans et événements). Les utilisateurs ne reçoivent pas de notifications d'enregistrement.
- **Activer l'enregistrement de session d'événement uniquement avec notification.** Cette option enregistre uniquement les événements spécifiés par votre stratégie de détection d'événements au cours des sessions. Elle n'enregistre pas d'écrans. Les utilisateurs reçoivent des notifications d'enregistrement à l'avance.
- **Activer l'enregistrement de session d'événement uniquement sans notification.** Cette option enregistre uniquement les événements spécifiés par votre stratégie de détection d'événements au cours des sessions. Elle n'enregistre pas d'écrans. Les utilisateurs ne reçoivent pas de notifications d'enregistrement.
- **Désactiver l'enregistrement de session.** Cette option signifie qu'aucune session n'est enregistrée.



Pour chaque règle, choisissez au moins l'une des règles suivantes pour créer les critères de règle :

- **Utilisateurs ou groupes.** Crée une liste d'utilisateurs ou de groupes auxquels l'action de la règle s'applique. L'enregistrement de session vous permet d'[utiliser les groupes Active Directory](#) et de [placer des utilisateurs sur liste blanche](#).
- **Applications ou bureaux publiés.** Crée une liste d'applications ou de bureaux publiés à laquelle l'action de la règle s'applique. Dans l'assistant **Règles**, choisissez les sites Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) sur lesquels les applications ou bureaux sont disponibles.
- **Groupes de mise à disposition ou machines.** Crée une liste de groupes de mise à disposition ou de machines auxquels l'action de la règle s'applique. Dans l'assistant **Règles**, choisissez l'emplacement des groupes de mise à disposition ou machines.
- **Adresse IP ou plage d'adresses IP.** Crée une liste d'adresses IP ou de plages d'adresses IP auxquelles l'action de la règle s'applique. Dans la boîte de dialogue **Sélectionner IP et plage d'adresses IP**, ajoutez une adresse IP ou une plage d'adresses IP valide pour lesquelles l'enregistrement est activé ou désactivé. Les adresses IP mentionnées ici sont les adresses IP des

applications Citrix Workspace.

The screenshot shows a 'Rules Wizard' dialog box with two main sections. The first section, 'Step 2: Select the rule criteria.', contains four unchecked checkboxes: 'Users or Groups', 'Published Applications or Desktop', 'Delivery Groups or Machines', and 'IP Address or IP Range'. The second section, 'Step 3: Edit the rule criteria.', contains a text box with the instruction: 'Selecting a rule criterion above activates the option here. To edit, click the underlined value.' Below this, there are four lines of text: 'Users / Groups: All Users', 'Published Resources: All Applications and Desktop', 'Delivery Groups / Machines: All Delivery Groups and Machines', and 'IP Address / IP Range: All IP Addresses'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

Remarque :

La console de stratégie d'enregistrement de session prend en charge la configuration de plusieurs critères au sein d'une règle unique. Lorsqu'une règle s'applique, les opérateurs logiques « ET » et « OU » sont utilisés pour calculer l'action finale. Généralement, l'opérateur « OU » est utilisé entre les éléments au sein d'un critère, et l'opérateur « ET » est quant à lui utilisé entre les critères distincts. Si le résultat est true, le moteur de stratégie d'enregistrement de session entreprend l'action de la règle. Sinon, il passe à la règle suivante et répète le processus.

Lorsque vous créez plus d'une règle dans une stratégie d'enregistrement, il est possible que certaines sessions correspondent aux critères de plusieurs de ces règles. Dans ces cas de figure, la règle ayant la plus haute priorité est celle appliquée aux sessions.

L'action d'enregistrement d'une règle en détermine la priorité :

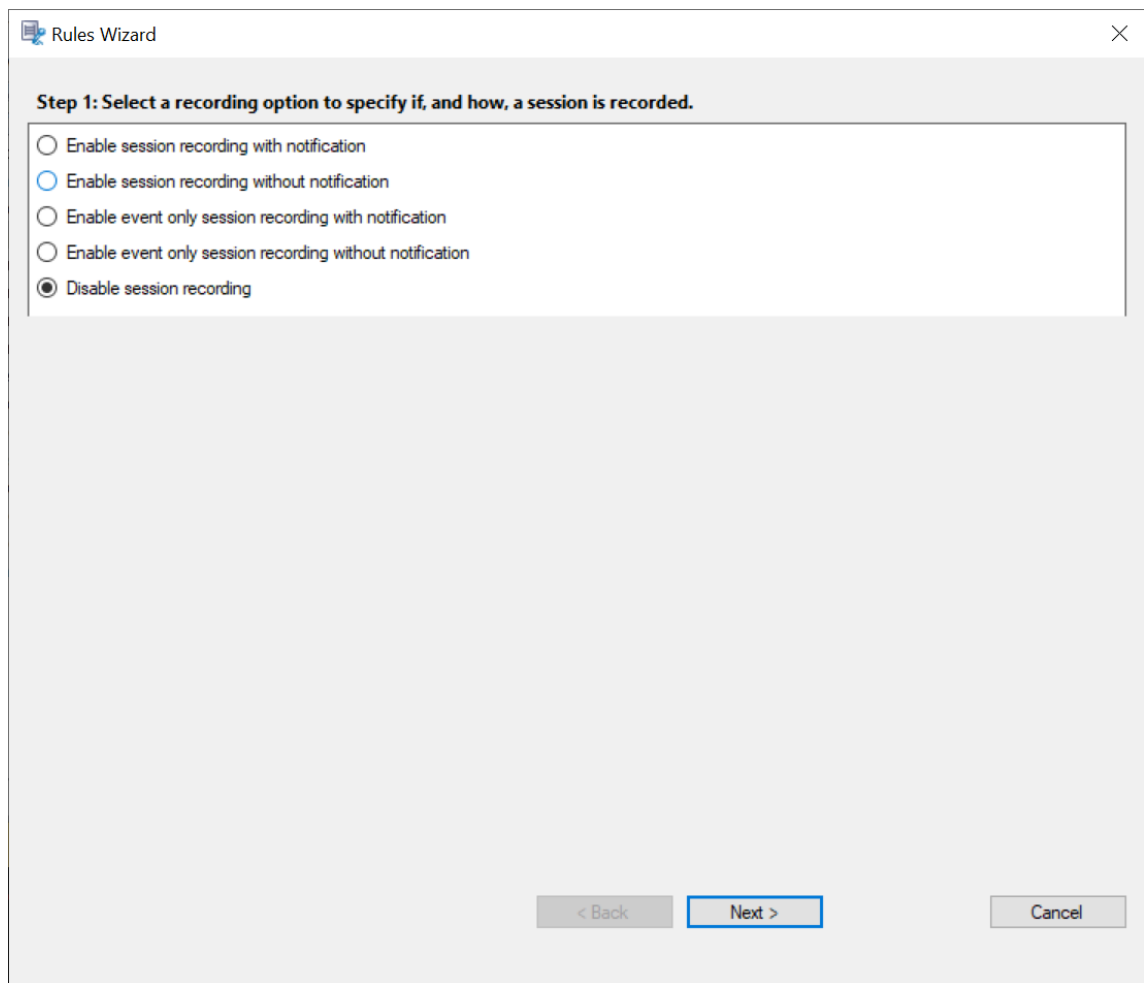
- Les règles avec l'action **Ne pas enregistrer** ont la plus haute priorité.
- Les règles avec l'action **Enregistrer avec notification** ont la seconde plus haute priorité.

- Les règles avec l'action **Enregistrer sans notification** ont la seconde plus faible priorité.
- Les règles avec l'action **Activer l'enregistrement de session d'événement uniquement avec notification** ont la priorité moyenne.
- Les règles avec l'action **Activer l'enregistrement de session d'événement uniquement sans notification** ont la priorité la plus faible.

Il se peut que certaines sessions ne correspondent à aucun critère de règle d'une stratégie d'enregistrement. Pour ces sessions, l'action de la règle de repli des stratégies s'applique. L'action de la règle de repli est toujours **Ne pas enregistrer**. Vous ne pouvez pas modifier ou supprimer la règle de repli.

Pour créer une stratégie d'enregistrement personnalisée :

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session et sélectionnez **Stratégies d'enregistrement** dans le panneau gauche. Dans la barre de menu, choisissez **Ajouter une nouvelle stratégie**.
3. Cliquez avec le bouton droit sur **Nouvelle stratégie** et sélectionnez **Ajouter une règle**.
4. Dans l'assistant de règles, sélectionnez une option d'enregistrement, puis cliquez sur **Suivant**.



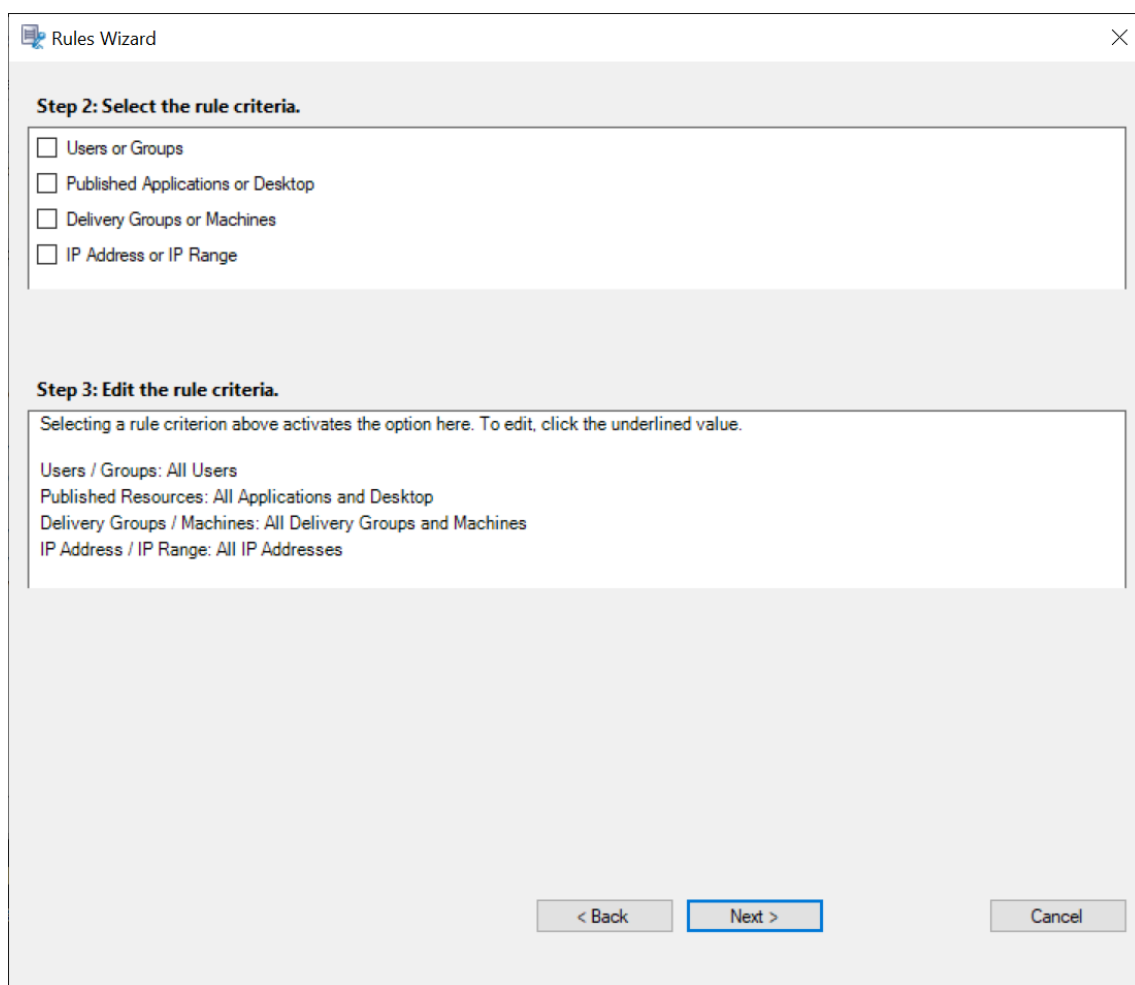
5. Sélectionnez les critères de la règle : vous pouvez choisir une ou plusieurs critères de règle :

Utilisateurs ou Groupes

Applications ou bureaux publiés

Groupes de mise à disposition ou Machines

Adresse IP ou Plage d'adresses IP



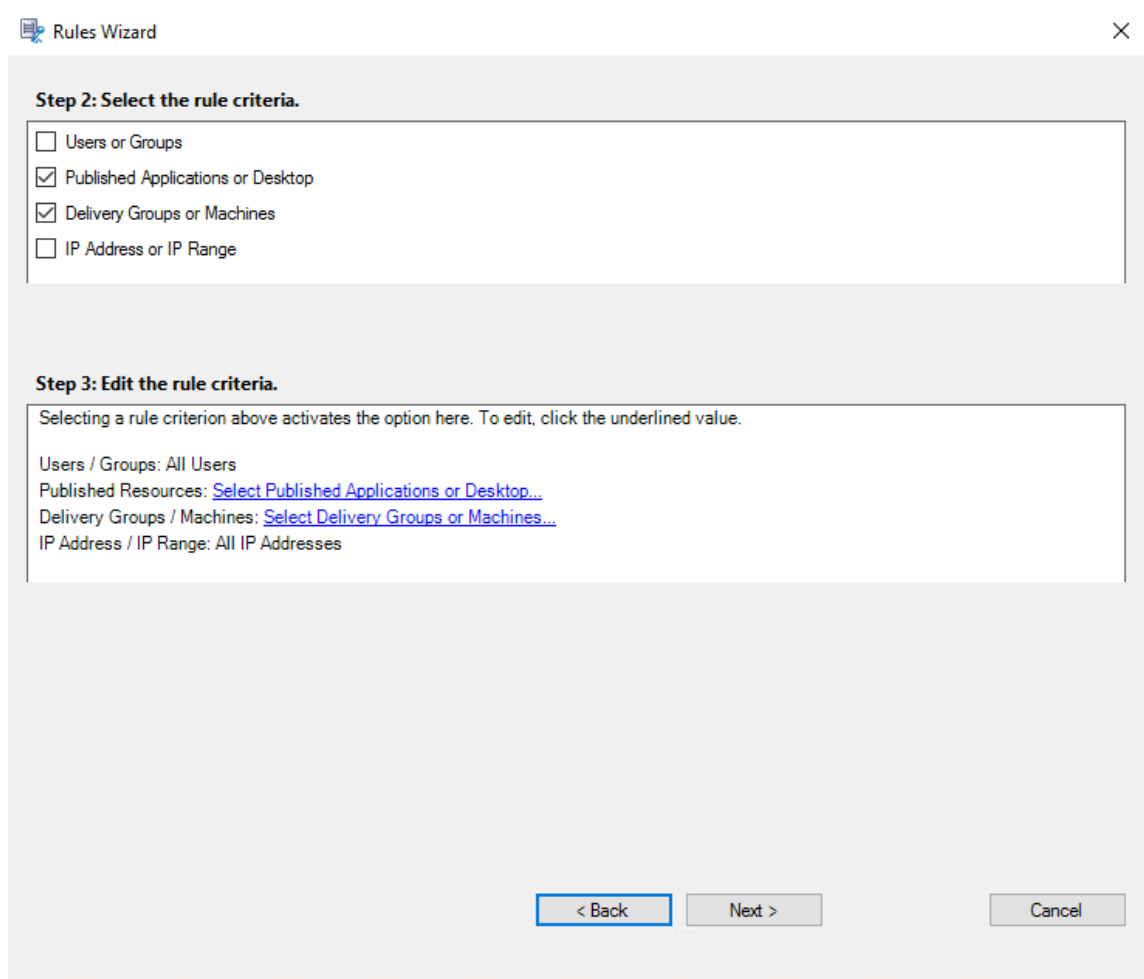
6. Modifiez les critères de la règle : pour modifier, cliquez sur les valeurs soulignées. Les valeurs sont soulignées en fonction des critères que vous avez choisis dans l'étape précédente.

Remarque :

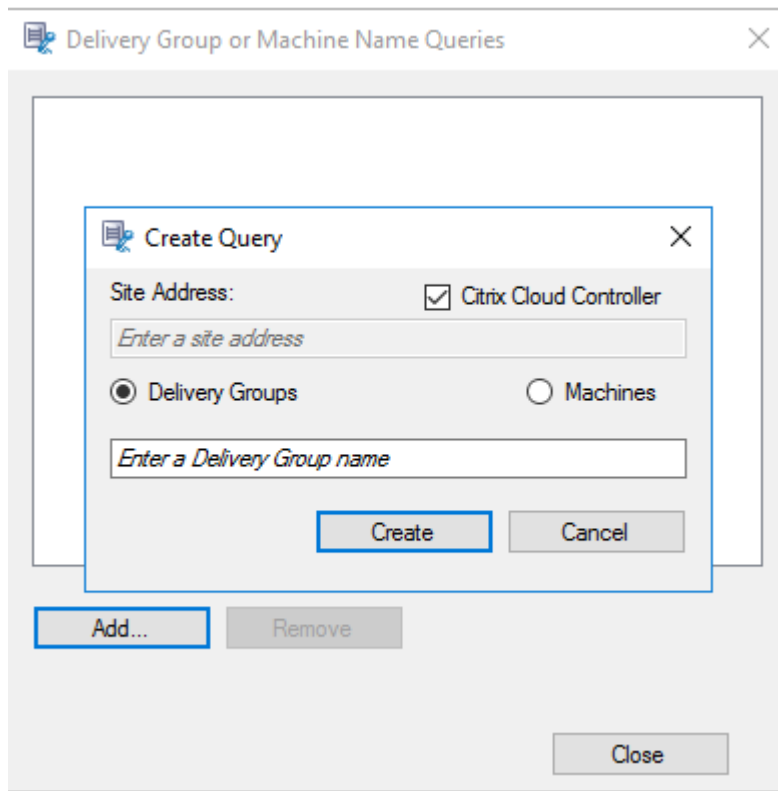
Si vous choisissez la valeur soulignée **Applications ou bureaux publiés**, l'**adresse du site** est l'adresse IP, une adresse URL ou un nom de machine si le Contrôleur se trouve sur un réseau local. La liste **Nom de l'application** indique le nom d'affichage.

Lorsque vous choisissez **Applications ou bureaux publiés** ou **Groupes de mise à disposition ou Machines**, spécifiez le Delivery Controller avec lequel votre console de stratégie d'enregistrement de session va communiquer.

La console de stratégie d'enregistrement de session est le seul canal qui communique avec les Delivery Controller à partir d'environnements locaux ou Citrix Cloud.



Par exemple, lorsque vous choisissez **Groupes de mise à disposition ou machines**, cliquez sur le lien hypertexte correspondant à l'étape 3 de la capture d'écran précédente et cliquez sur **Ajouter** pour ajouter des requêtes au Controller.



Pour obtenir une description des cas d'utilisation qui couvrent les Delivery Controller Citrix Cloud et locaux, consultez le tableau suivant :

Cas d'utilisation	Action requise
Delivery Controller locaux	a) Installez Broker_PowerShellSnapin_x64.msi. 2. Désactivez la case à cocher Citrix Cloud Controller .
Delivery Controller Citrix Cloud	a) Installez le kit de développement logiciel distant SDK Remote PowerShell Citrix DaaS. 2. Validez les informations d'identification du compte Citrix Cloud. 3. Sélectionnez la case à cocher Citrix Cloud Controller .

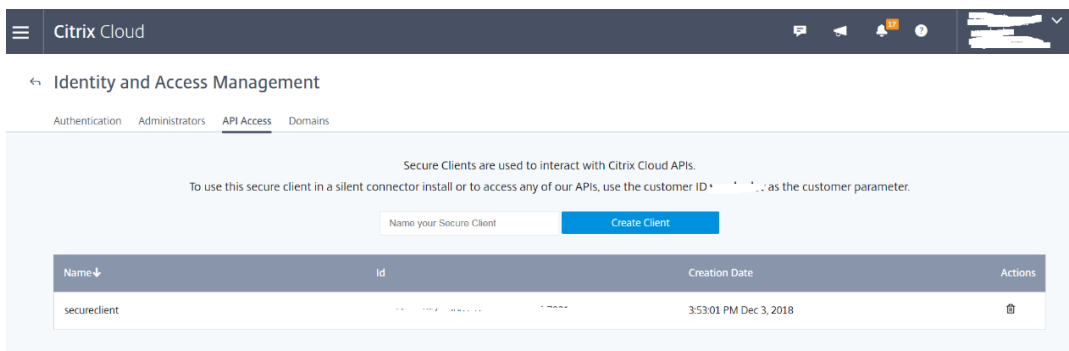
Cas d'utilisation	Action requise
Passer d'un Delivery Controller local à un Delivery Controller Citrix Cloud	a) Désinstallez Broker_PowerShellSnapin_x64.msi et redémarrez l'ordinateur. 2. Installez le kit de développement logiciel distant SDK Remote PowerShell Citrix DaaS. 3. Validez les informations d'identification du compte Citrix Cloud. 4. Sélectionnez la case à cocher Citrix Cloud Controller .
Passer d'un Delivery Controller Citrix Cloud à un Delivery Controller local	a) Désinstallez le SDK Remote PowerShell Citrix DaaS et redémarrez l'ordinateur. 2. Installez Broker_PowerShellSnapin_x64.msi. 3. Désactivez la case à cocher Citrix Cloud Controller .

Validation des informations d'identification de Citrix Cloud

Pour interroger les Delivery Controller hébergés dans Citrix Cloud, validez manuellement vos informations d'identification Citrix Cloud sur l'ordinateur sur lequel la console de stratégie d'enregistrement de session est installée. Le non-respect de ces conditions peut provoquer une erreur et votre console de stratégie d'enregistrement de session peut ne pas fonctionner comme prévu.

Pour effectuer la validation manuelle :

- a) Connectez-vous à la console Citrix Cloud et recherchez **Gestion des identités et des accès > Accès aux API**. Créez un client sécurisé pour accéder aux API afin d'obtenir un profil d'authentification capable de contourner les invites d'authentification de Citrix Cloud. Téléchargez votre client sécurisé, renommez-le et enregistrez-le dans un emplacement sécurisé. Le nom de fichier est défini par défaut sur secureclient.csv.



- b) Ouvrez une session PowerShell et exécutez la commande suivante pour que le profil d'authentification (obtenu à l'étape précédente) prenne effet.

```
1 asnp citrix.*
2 Set-XDCredentials -CustomerId "citrixdemo" -SecureClientFile
   "c:\temp\secureclient.csv" -ProfileType CloudAPI -
   StoreAs "default"
3
4 <!--NeedCopy-->
```

Définissez **CustomerID** et **SecureClientFile** si nécessaire. La commande précédente crée un profil d'authentification par défaut pour le client `citrixdemo` afin de contourner les invites d'authentification dans les sessions PowerShell en cours et à venir.

7. Suivez les instructions de l'assistant pour terminer la configuration.

Remarque : Veuillez noter les limitations suivantes concernant les sessions d'application pré-lancées :

- Si la stratégie active essaie d'établir une correspondance avec le nom d'une application, elle ne peut pas le faire avec des applications qui sont ouvertes au cours d'une session pré-lancée. Par conséquent, la session pré-lancée ne peut pas être enregistrée.
- Si la stratégie active enregistre chaque application et que le pré-lancement de session est activé, une notification d'enregistrement apparaît lorsqu'un utilisateur ouvre une session sur l'application Citrix Workspace pour Windows. La session pré-lancée (vide) et toutes les applications à lancer dans cette session sont enregistrées.

Une solution consiste à publier les applications dans des groupes de mise à disposition séparés en fonction de leurs stratégies d'enregistrement. N'utilisez pas de nom d'application en tant que condition d'enregistrement. Cette approche garantit que les sessions pré-lancées peuvent être enregistrées. Toutefois, les notifications continuent à s'afficher.

Utiliser des groupes Active Directory

L'enregistrement de session vous permet d'utiliser les groupes Active Directory lorsque vous créez des stratégies. Utiliser les groupes Active Directory au lieu d'utilisateurs individuels simplifie la création et la gestion des règles et des stratégies. Par exemple, si les utilisateurs du service financier de votre société sont réunis dans un groupe Active Directory intitulé **Finance**, vous pouvez créer une règle concernant tous les membres de ce groupe en sélectionnant le groupe **Finance** dans l'assistant **Règles**.

Utilisateurs sur liste blanche

Vous pouvez créer des stratégies d'enregistrement de session qui font en sorte que certains utilisateurs de votre organisation ne sont jamais enregistrés. Cela s'appelle *mettre ces utilisateurs sur liste blanche*. La liste blanche est utile pour les utilisateurs qui gèrent des informations relatives à la confidentialité ou lorsque votre organisation ne souhaite pas enregistrer les sessions d'une certaine classe d'employés.

Par exemple, si tous les managers d'une entreprise sont membres d'un groupe Active Directory intitulé **Cadres supérieurs**, vous pouvez faire en sorte que les sessions de ces utilisateurs ne sont jamais enregistrées en créant une règle désactivant l'enregistrement de sessions pour le groupe **Cadres supérieurs**. Lorsque la stratégie contenant cette règle est active, aucune session des membres du groupe Cadres supérieurs n'est enregistrée. Les sessions des autres membres de votre organisation sont enregistrées en fonction d'autres règles de la stratégie active.

Configurer Director pour utiliser le serveur d'enregistrement de session

Vous pouvez utiliser la console Director pour créer et activer des stratégies d'enregistrement.

1. Dans le cas d'une connexion HTTPS, installez le certificat destiné à approuver le serveur d'enregistrement de session dans les certificats racines de confiance du serveur Director.
2. Pour configurer le serveur Director en vue d'utiliser le serveur d'enregistrement de session, exécutez la commande `C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording`.
3. Entrez l'adresse IP ou le nom de domaine complet du serveur d'enregistrement de session, le numéro de port et le type de connexion (HTTP/HTTPS) que l'agent d'enregistrement de session utilise pour se connecter au broker d'enregistrement de session sur le serveur Director.

Comportement de substitution - définitions

Lorsque vous activez une stratégie, la stratégie précédemment active reste en vigueur jusqu'à ce que la session en cours d'enregistrement se termine ou que le fichier de session enregistrée soit substitué. Les fichiers sont substitués lorsqu'ils atteignent la taille maximale. Pour plus d'informations sur la taille maximale des fichiers pour les enregistrements, consultez la section [Définir la taille des fichiers pour les enregistrements](#).

Le tableau suivant illustre en détail les événements qui se produisent lorsque vous appliquez une nouvelle stratégie d'enregistrement pendant qu'une session est en cours d'enregistrement et qu'une substitution a lieu :

Stratégie d'enregistrement précédente	Nouvelle stratégie d'enregistrement	Stratégie d'enregistrement après substitution
Ne pas enregistrer	Toute autre stratégie	Pas de modification. La nouvelle stratégie ne prend effet que lorsque l'utilisateur ouvre une nouvelle session. L'enregistrement s'arrête.
Enregistrer sans notification	Ne pas enregistrer	L'enregistrement s'arrête.
Enregistrer sans notification	Enregistrer avec notification	L'enregistrement continue et un message de notification s'affiche.
Enregistrer avec notification	Ne pas enregistrer	L'enregistrement s'arrête.
Enregistrer avec notification	Enregistrer sans notification	L'enregistrement continue. Aucun message ne s'affiche avant que l'utilisateur ouvre une nouvelle session.

Configurer des stratégies de visionnage d'enregistrement

February 20, 2024

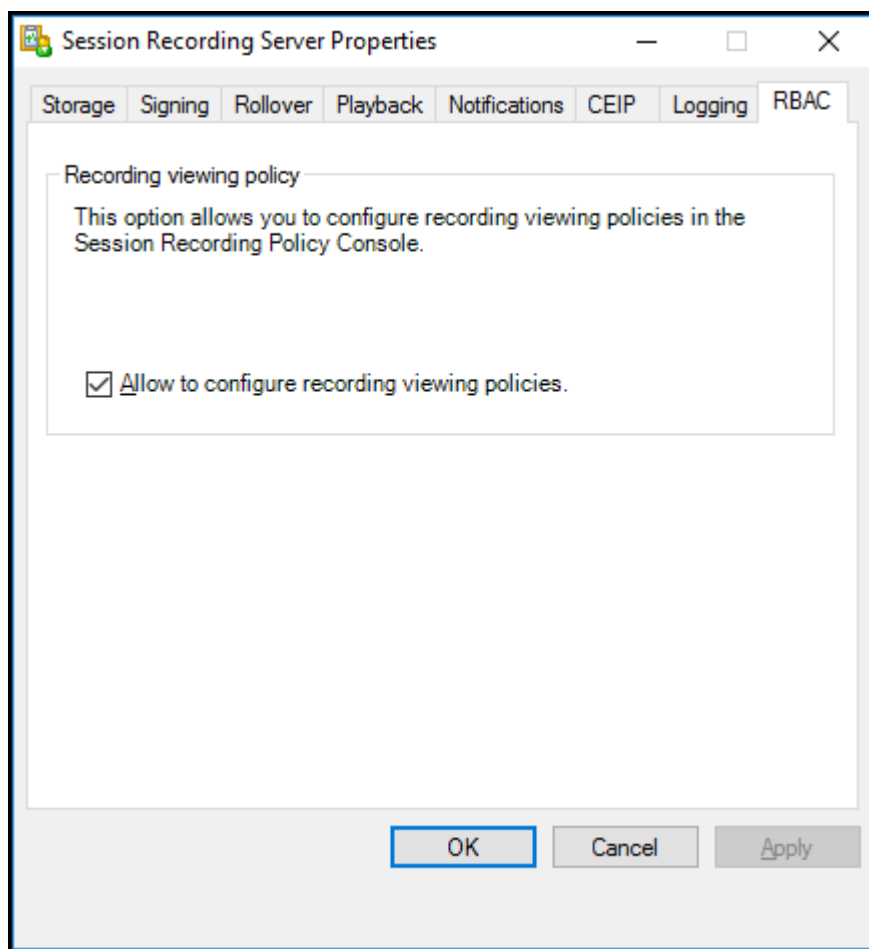
L'enregistrement de session prend en charge le contrôle d'accès basé sur les rôles. Vous pouvez créer des stratégies de visionnage d'enregistrement dans la console de stratégie d'enregistrement de session et ajouter plusieurs règles à chaque stratégie. Chaque règle vous permet de sélectionner un utilisateur ou un groupe d'utilisateurs comme visionneur d'enregistrements et de définir quels enregistrements sont visibles par le visionneur.

Créer une stratégie de visionnage d'enregistrement personnalisée

Avant de pouvoir créer des stratégies de visionnage d'enregistrement, activez la fonctionnalité comme suit :

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du serveur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **RBAC**.

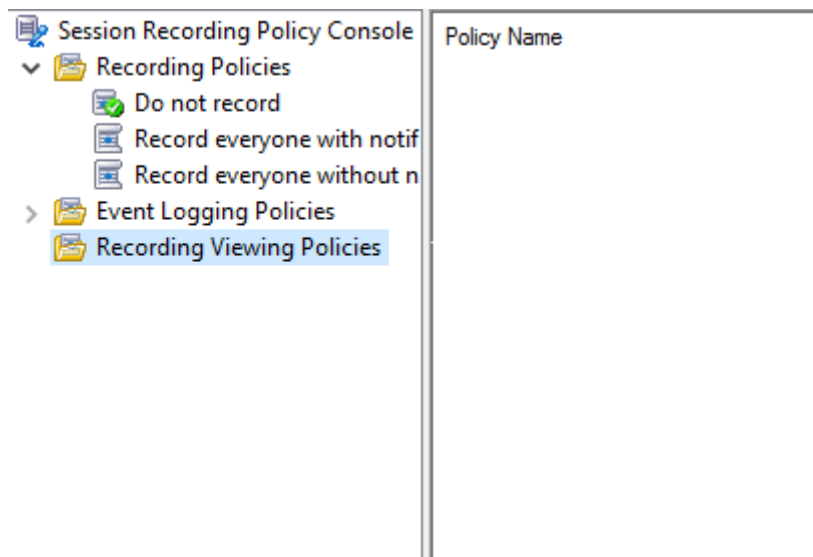
4. Cochez la case **Autoriser la configuration de stratégies de visionnage d'enregistrement**.



Pour créer une stratégie de visionnage d'enregistrement personnalisée :

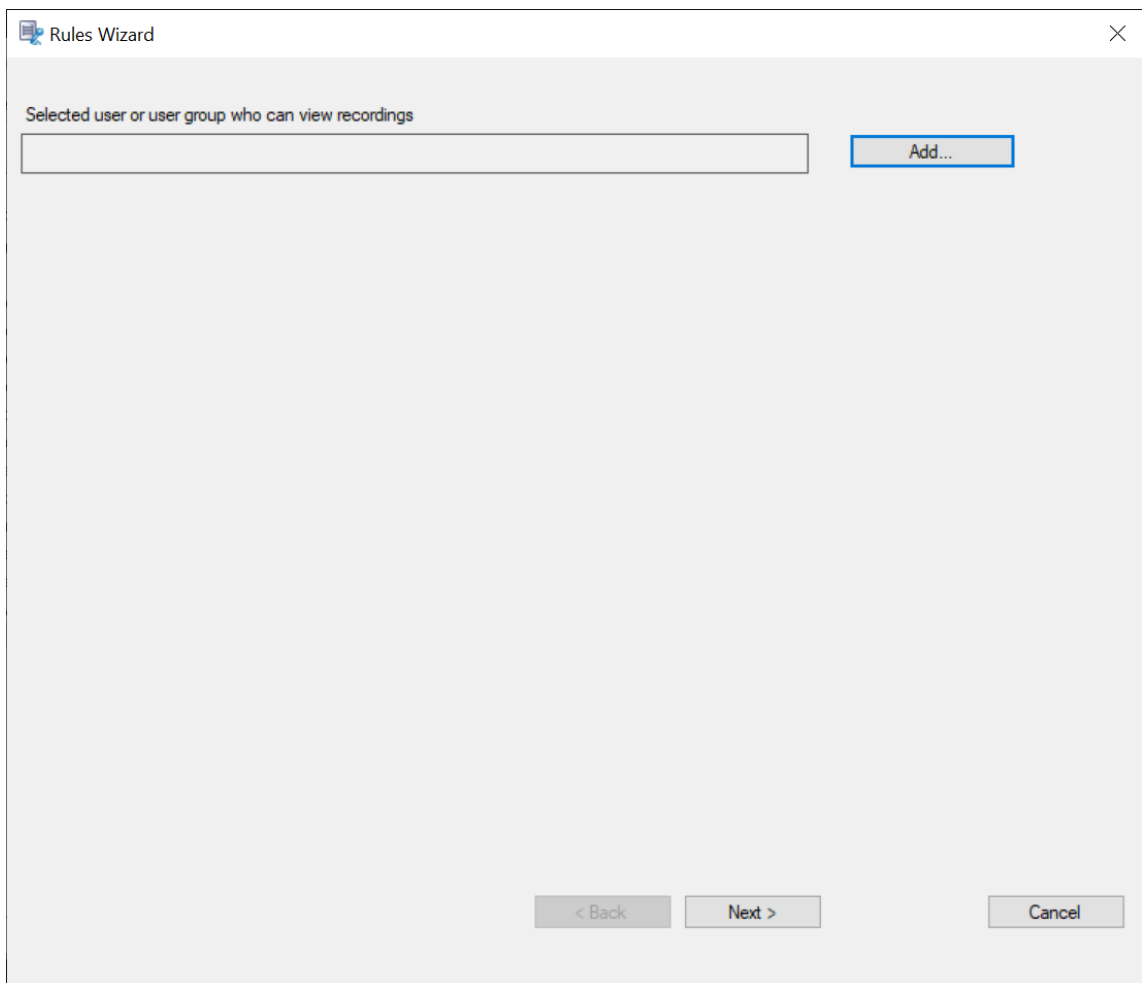
Remarque : Différente des stratégies d'enregistrement et des stratégies de détection d'événements, une stratégie de visionnage d'enregistrement (y compris toutes les règles qui y ont été ajoutées) est active immédiatement lors de sa création. Vous n'avez pas besoin de l'activer.

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session. Par défaut, il n'y a pas de stratégie de visionnage d'enregistrement.



Remarque : le menu **Stratégies de visionnage d'enregistrement** n'est disponible que si vous avez activé la fonctionnalité dans **Propriétés du serveur d'enregistrement de session**.

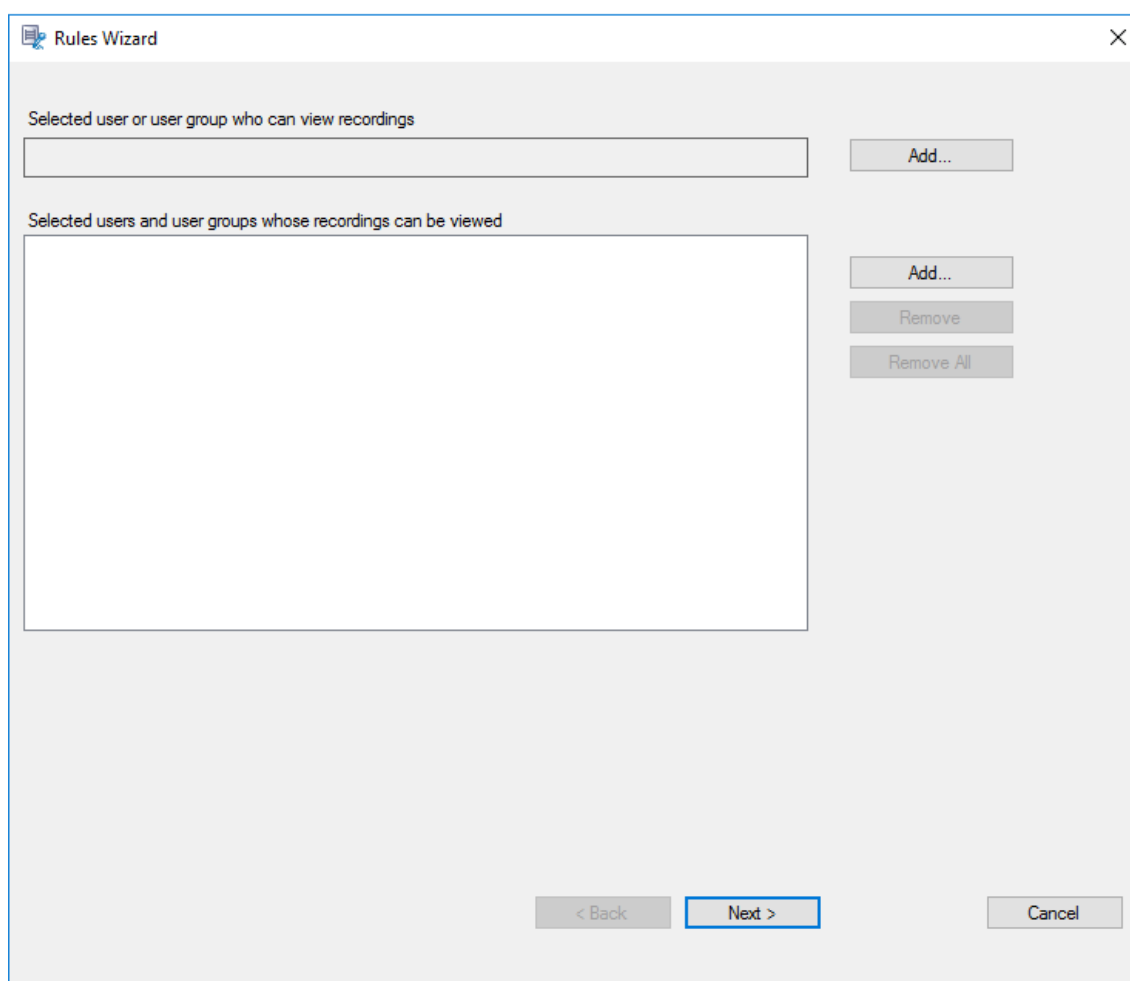
3. Sélectionnez **Stratégies de visionnage d'enregistrement** dans le volet gauche. Dans la barre de menu, choisissez **Ajouter une nouvelle stratégie** pour créer une stratégie de visionnage d'enregistrement.
4. (Facultatif) Cliquez avec le bouton droit de la souris sur la nouvelle stratégie et renommez-la.
5. Cliquez avec le bouton droit sur la nouvelle stratégie et sélectionnez **Ajouter une règle**.



6. Cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Sélectionnez des utilisateurs ou des groupes d'utilisateurs**, sélectionnez un utilisateur ou un groupe d'utilisateurs comme observateur d'enregistrement.

Remarque :

Un observateur doit avoir le rôle Lecteur pour afficher les sessions enregistrées. Pour de plus amples informations, consultez la section [Autoriser les utilisateurs](#).



Remarque :

Dans chaque règle, vous ne pouvez sélectionner qu'un seul utilisateur ou groupe d'utilisateurs comme personne autorisée à visionner un enregistrement. Si vous sélectionnez plusieurs utilisateurs ou groupes d'utilisateurs, seule votre sélection la plus récente prend effet et apparaît dans la zone de texte.

Lorsque vous autorisez un utilisateur à visionner des enregistrements (rôle Observateur), assurez-vous d'avoir affecté ce dernier au rôle Lecteur. Un utilisateur qui n'est pas autorisé à lire des sessions enregistrées reçoit un message d'erreur lorsqu'il essaye de lire une session enregistrée. Pour de plus amples informations, consultez la section [Autoriser les utilisateurs](#).

8. Cliquez sur **OK**, puis sur **Suivant**. La boîte de dialogue de définition des critères de règle apparaît.
9. Sélectionnez et modifiez les critères de règle pour spécifier les enregistrements qui sont visibles par l'utilisateur autorisé spécifié précédemment :
 - **Utilisateurs ou groupes**

- **Applications ou bureaux publiés**
- **Groupes de mise à disposition ou machines**

The screenshot shows a dialog box titled "Rules Wizard" with a close button (X) in the top right corner. The dialog is divided into two main sections. The first section, "Step 2: Select the rule criteria.", contains three unchecked checkboxes: "Users or Groups", "Published Applications or Desktop", and "Delivery Groups or Machines". The second section, "Step 3: Edit the rule criteria.", contains three lines of text: "Users / Groups: All Users", "Published Resources: All Applications and Desktop", and "Delivery Groups / Machines: All Delivery Groups and Machines". At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

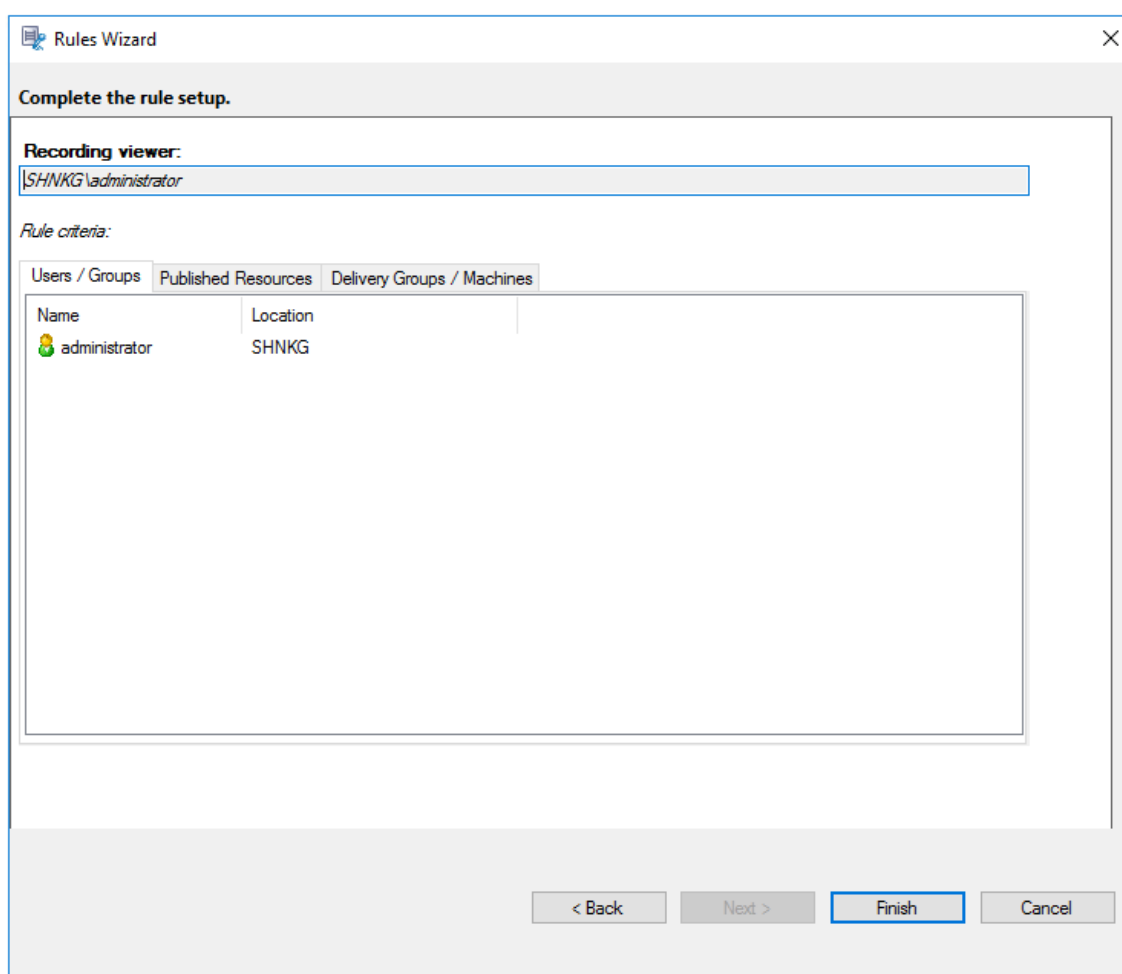
Remarque :

L'opérateur logique « OU » est utilisé à la fois entre les éléments d'un critère de règle et entre les critères de règle distincts.

Si vous ne spécifiez pas les critères de règle, l'utilisateur autorisé spécifié précédemment ne peut visionner aucun enregistrement.

10. Suivez les instructions de l'assistant pour terminer l'installation.

Par exemple :



Configurer les stratégies de détection d'événements

February 20, 2024

L'enregistrement de session prend en charge la configuration centralisée des stratégies de détection d'événements. Vous pouvez créer des stratégies dans la console de stratégie d'enregistrement de session pour consigner divers événements.

Événements pouvant être détectés

L'enregistrement de session détecte les événements cibles et marque ces événements dans les enregistrements en vue de faciliter leur recherche et lecture ultérieurement. Vous pouvez rechercher des événements d'intérêt au sein d'un grand nombre d'enregistrements et localiser les événements pendant la lecture.

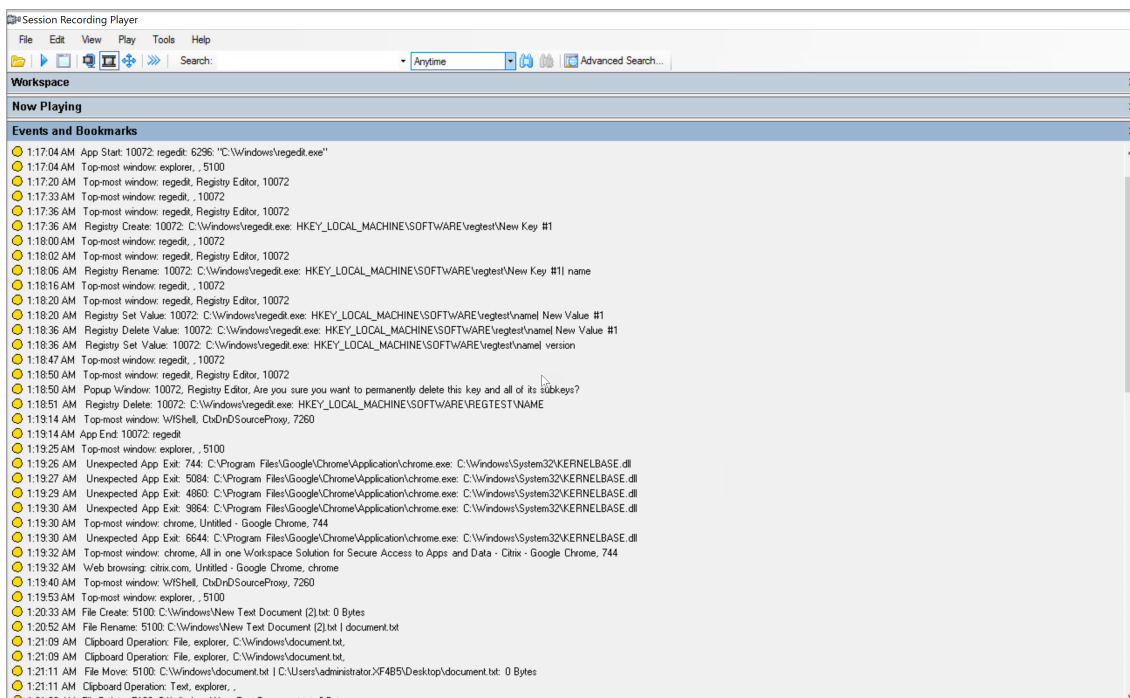
Événements définis par le système

L'enregistrement de session peut détecter et journaliser les événements définis par le système suivants qui se produisent pendant les sessions enregistrées :

- Insertion des périphériques de stockage de masse USB
- Démarrages et fins d'applications
- Défaillances d'application
- Installations et désinstallations d'applications
- Opérations de changement de nom, de création, de suppression et de déplacement de fichier lors de sessions
- Transferts de fichiers entre les hôtes de session (VDA) et les machines clientes (y compris les lecteurs clients mappés et les périphériques de stockage de masse génériques redirigés)
- Activités de navigation sur le Web
- Événements de la fenêtre principale
- Activités du presse-papiers
- Modifications du registre Windows
- Modifications du compte utilisateur
- Connexions RDP
- Données de performance (points de données liés à la session enregistrée)
- Événements de fenêtre contextuelle

Par exemple :

- Événements d'un enregistrement d'événement uniquement dans le lecteur Web :

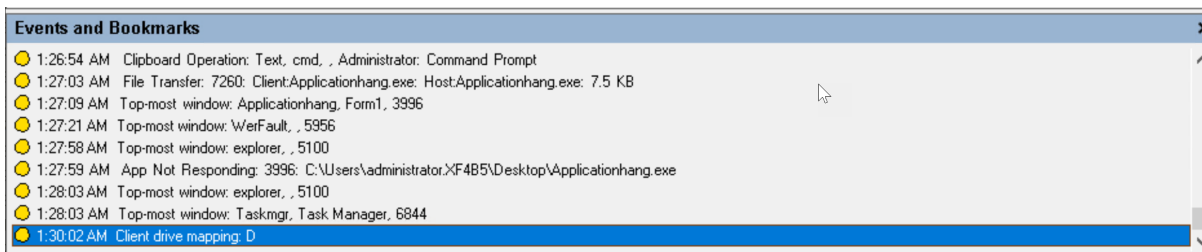


Pour plus en savoir plus sur les événements dans le lecteur d'enregistrement de session, consultez les descriptions des événements plus loin dans cet article.

Remarque :

Les applications créées par PowerBuilder peuvent se fermer de manière inattendue lorsque des stratégies actives détectent les activités de navigation Web et les événements de la fenêtre principale. Pour éviter ce problème, utilisez PowerBuilder 2019 R3 pour créer vos applications.

Insertion des périphériques de stockage de masse USB L'enregistrement de session peut détecter l'insertion d'un périphérique de stockage de masse USB redirigé générique ou mappé (CDM) sur un client sur lequel l'application Citrix Workspace pour Windows ou Mac est installée. Enregistrement de session marque ces événements dans l'enregistrement.



Remarque :

Pour utiliser un périphérique de stockage de masse USB inséré et détecter les événements d'insertion, définissez la stratégie **Redirection de périphérique USB client** sur **Autorisé** dans Citrix

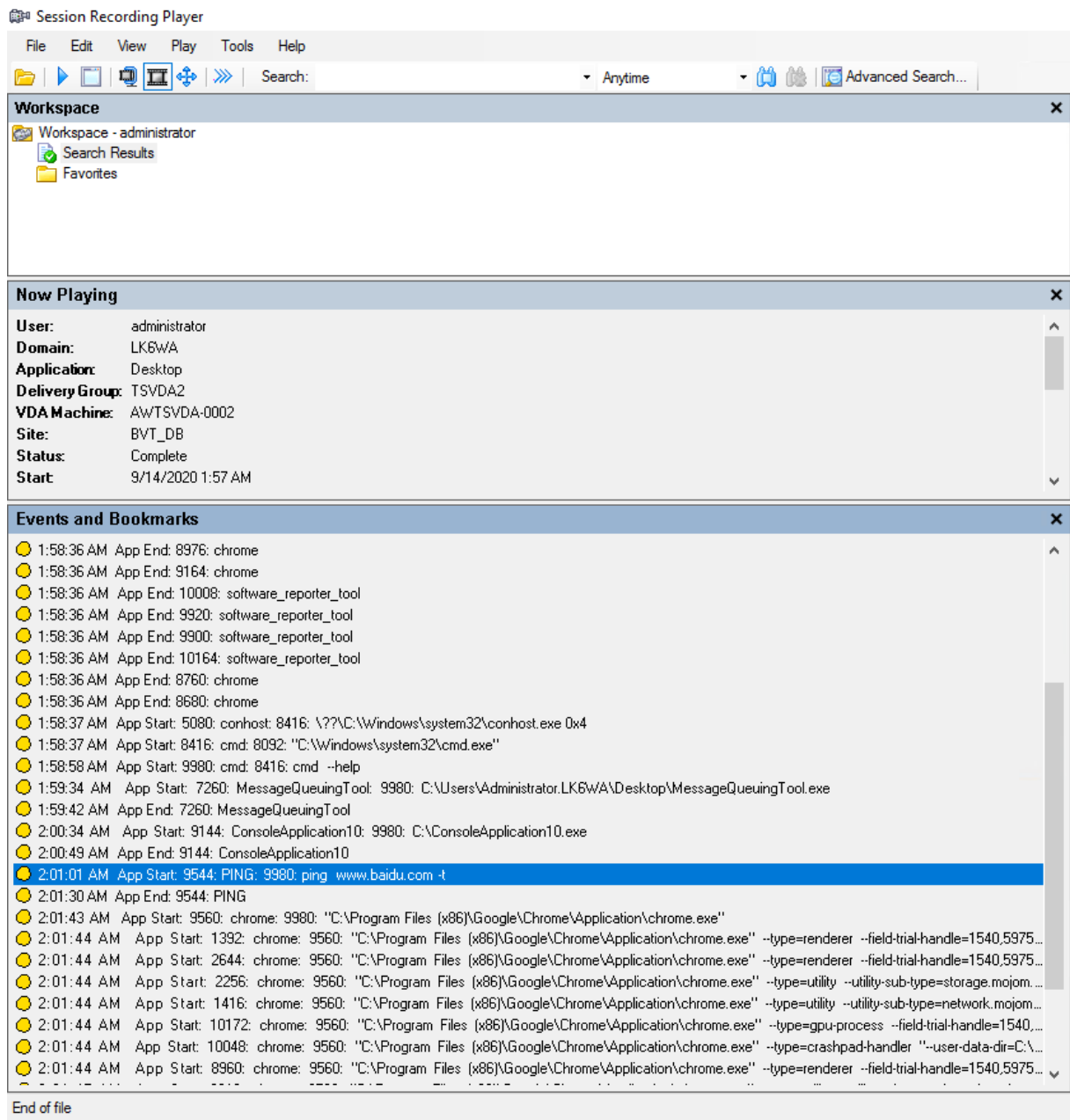
Studio.

Actuellement, seule l'insertion de périphériques de stockage de masse USB (Classe USB 08) peut être détectée.

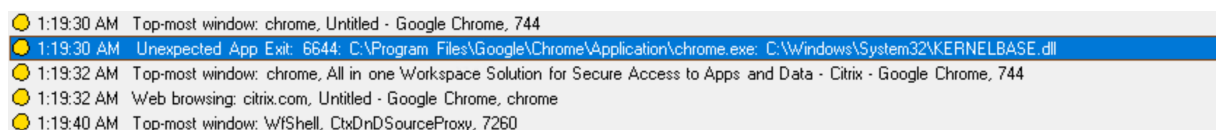
Démarrages et fins d'applications L'enregistrement de session prend en charge la détection des démarrages et des arrêts d'applications. Lorsque vous ajoutez un processus à la **liste de surveillance des applications**, les applications lancées par le processus ajouté et ses processus enfants sont surveillées. Les processus enfants d'un processus parent qui démarre avant l'exécution de l'enregistrement de session peuvent également être capturés.

Par défaut, Enregistrement de session ajoute les noms des processus, `cmd.exe`, `powershell.exe` et `wsl.exe`, à la **liste de surveillance des applications**. Si vous sélectionnez **Consigner les événements de démarrage d'application** et **Consigner les événements de fin d'application** pour une stratégie de détection des événements, les démarrages et les fins des applications Invite de commandes, PowerShell et Sous-système Windows pour Linux (WSL) sont consignés, que vous ajoutiez ou non manuellement leurs noms de processus à la **liste de surveillance des applications**. Les noms de processus par défaut ne sont pas visibles dans la **liste de surveillance des applications**.

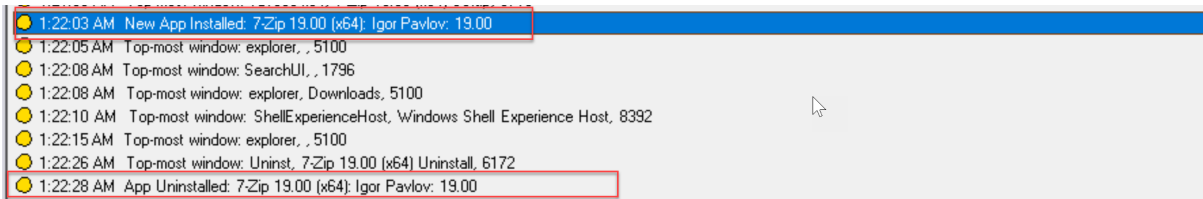
En outre, Enregistrement de session fournit une ligne de commande complète pour chaque événement de démarrage d'application consigné.



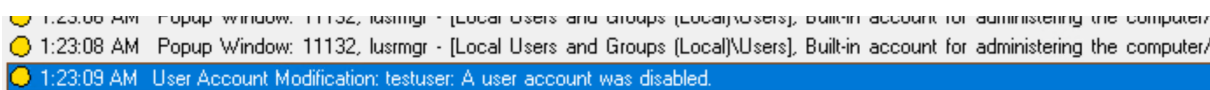
Échecs applicatifs L’enregistrement de session détecte les fermetures d’applications et les applications qui ne répondent pas si vous sélectionnez **Consigner défaillances d’application** lors de la création de votre stratégie de détection d’événements. La **règle Consigner défaillances d’application** s’applique à toutes les applications.



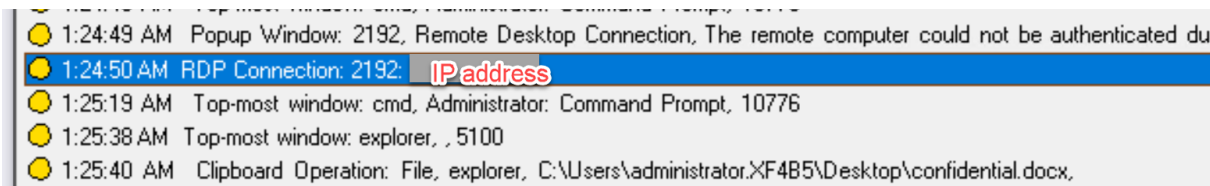
Installations et désinstallations d'applications La règle **Consigner installations et désinstallations d'applications** s'applique à toutes les applications.



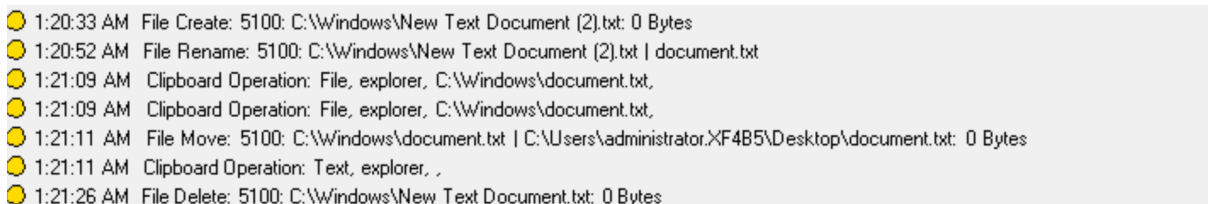
Modifications du compte utilisateur L'enregistrement de session peut détecter la création, l'activation, la désactivation, la suppression, les changements de nom et les tentatives de modification du mot de passe de compte.

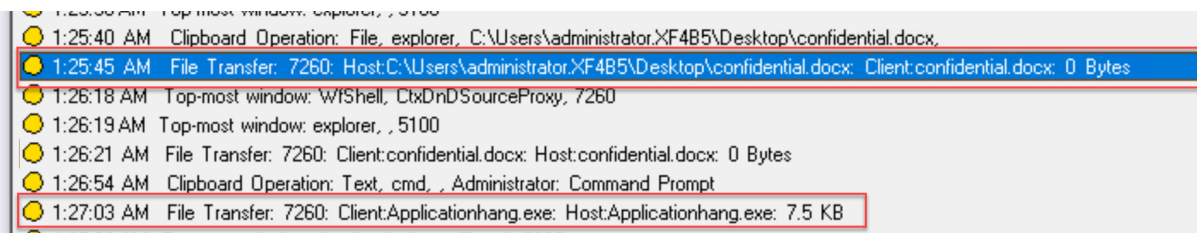


Connexions RDP L'enregistrement de session peut détecter les connexions RDP initiées à partir du VDA hébergeant la session enregistrée.



Opérations de changement de nom, de création, de suppression et de déplacement de fichiers dans les sessions et les transferts de fichiers entre les hôtes de session (VDA) et les machines clientes L'enregistrement de session peut détecter les opérations de changement de nom, de création, de suppression et de déplacement sur les fichiers et dossiers cibles que vous spécifiez dans la **Liste de surveillance des fichiers**. L'enregistrement de session peut également détecter les transferts de fichiers entre les hôtes de session (VDA) et les machines clientes (y compris les lecteurs clients mappés et les périphériques de stockage de masse génériques redirigés). La sélection de l'option **Consigner les événements de fichiers sensibles** déclenche la détection des transferts de fichiers, que vous spécifiez ou non la **Liste de surveillance des fichiers**.





Remarque :

Pour activer le glisser-déplacer de fichier et capturer les événements de glisser-déplacer, définissez la stratégie **Glisser-déposer** sur **Activé** dans Citrix Studio.

Activités de navigation sur le Web L'enregistrement de session peut détecter les activités des utilisateurs sur les navigateurs pris en charge et marquer les événements dans l'enregistrement. Le nom du navigateur, l'URL et le titre de la page sont enregistrés. Pour obtenir un exemple, consultez la capture d'écran suivante.



Lorsque vous éloignez votre curseur d'une page Web qui a le focus, votre navigation sur cette page Web est marquée sans afficher le nom du navigateur. Cette fonctionnalité peut être utilisée pour estimer combien de temps un utilisateur reste sur une page Web. Pour obtenir un exemple, consultez la capture d'écran suivante.



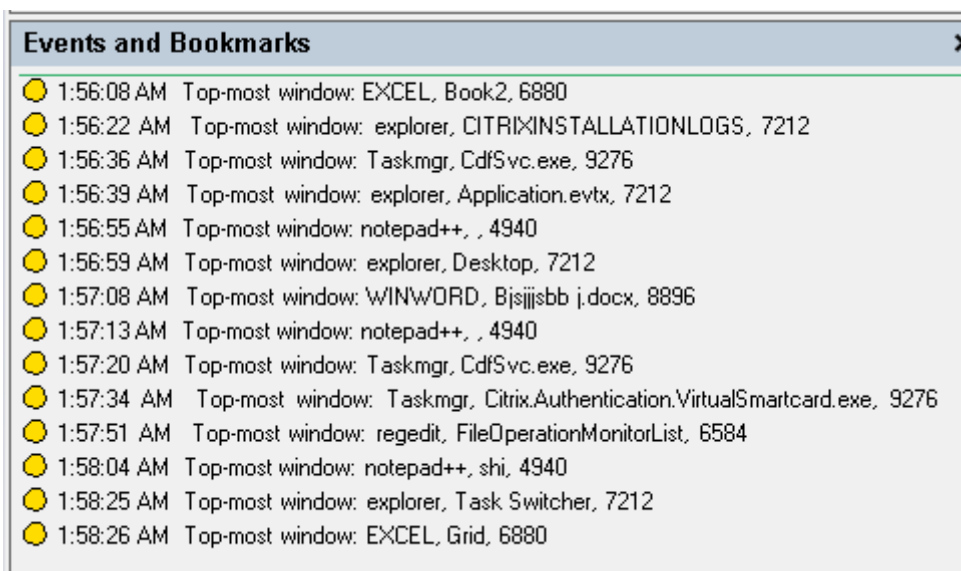
Liste des navigateurs pris en charge :

Navigateur	Version
Chrome	69 et versions ultérieures
Internet Explorer	11
Firefox	61 et versions ultérieures

Remarque :

Cette fonctionnalité nécessite Enregistrement de session version 1906 ou ultérieure.

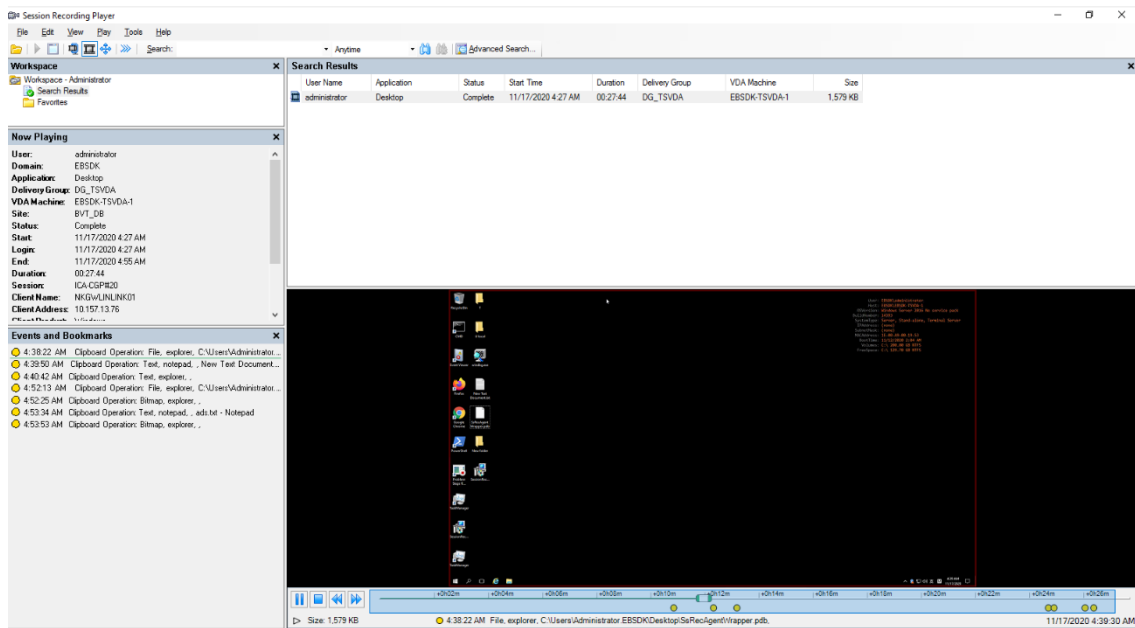
Événements de la fenêtre principale L'enregistrement de session peut détecter les événements lorsque la fenêtre d'une application est au-dessus de tous les autres fenêtres. Le nom, le titre et le numéro du processus sont consignés.



Activités du presse-papiers L'enregistrement de session peut détecter les opérations de copie de texte, d'images et de fichiers à l'aide du presse-papiers. Le nom du processus et le chemin d'accès du fichier sont consignés pour une copie de fichier. Le titre et le nom du processus sont consignés pour une copie de texte. Le nom du processus est consigné pour une copie d'image.

Remarque : Le contenu du texte copié n'est pas consigné par défaut. Pour consigner le contenu du texte, accédez à l'Agent d'enregistrement de session et définissez `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\CaptureClipboardContent` sur `1` (la valeur par défaut est `0`).

Enregistrement de session 2210



Modifications du registre Windows À partir de la version 2109, l'enregistrement de session peut détecter et journaliser les modifications apportées au registre suivantes lors de l'enregistrement de sessions :

Modification du registre	Événement correspondant
Ajouter une clé	Créer registre
Ajouter une valeur	Définir valeur du registre
Renommer une clé	Renommer registre
Renommer une valeur	Supprimer valeur du registre et Définir valeur du registre
Modifier une valeur existante	Définir valeur du registre
Supprimer une clé	Supprimer registre
Supprimer une valeur	Supprimer valeur du registre

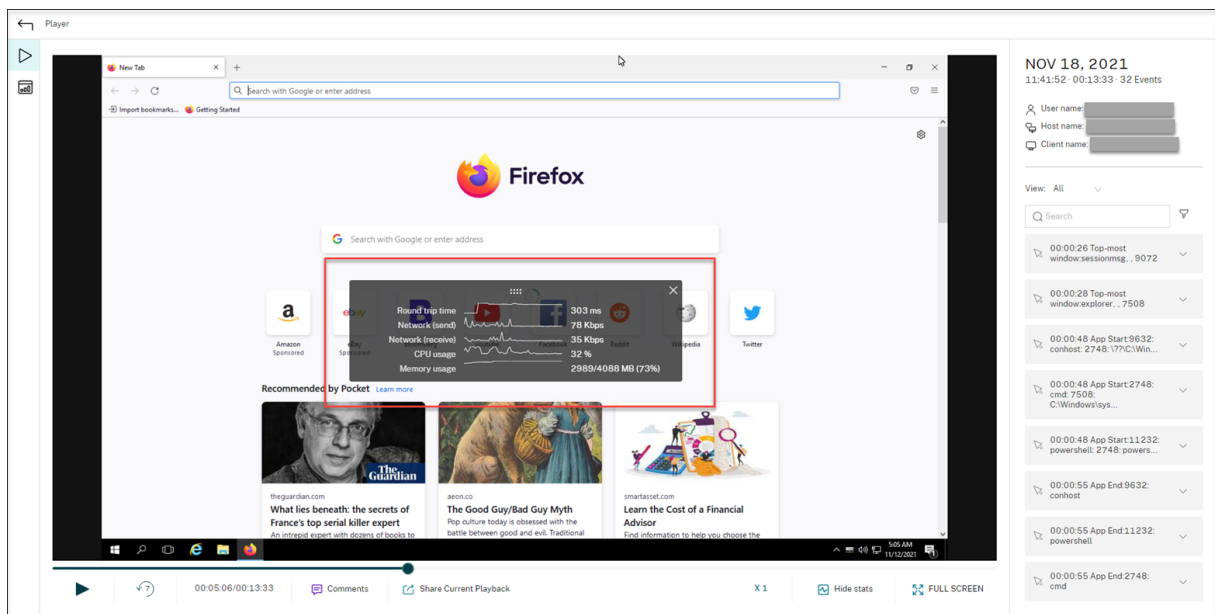
Par exemple :

Events and Bookmarks	
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Tablet PC IsTabletPC
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Tablet PC
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Windows6432Node\Microsoft\Windows\Tablet PC IsTabletPC
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Windows6432Node\Microsoft\Windows\Tablet PC
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation LastOrientation
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation\NonPreserve LastAutoRequest
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation\NonPreserve
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation LastOrientation
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation
10:30:55 PM	Registry Set Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3\LLIndicator LLIndicator
10:30:55 PM	Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3 SessionHeight
10:30:55 PM	Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3 SessionWidth
10:30:55 PM	Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3 NumMonitors
10:30:55 PM	Registry Create: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3

Pour activer cette fonctionnalité de surveillance du registre, sélectionnez l’option **Consigner les modifications du registre** pour votre stratégie de détection d’événements.

Données de performance (points de données liés à la session enregistrée) Lors de la création de votre stratégie de détection des événements, sélectionnez **Enregistrer les données de performances** pour activer la fonctionnalité de superposition des données de session. Cette fonctionnalité introduit une superposition d’écran pendant la lecture de la session dans le lecteur Web. Il s’agit d’une superposition semi-transparente que vous pouvez déplacer et masquer. La superposition comporte les points de données suivants liés à la session enregistrée :

- Durée des boucles
- Réseau (envoi)
- Réseau (réception)
- Utilisation du processeur
- Utilisation de la mémoire



Événements de fenêtre contextuelle Lorsque les utilisateurs ouvrent ou ferment un fichier confidentiel ou accèdent à un dossier, une fenêtre contextuelle peut apparaître, affichant une invite ou demandant un mot de passe. L'enregistrement de session peut désormais surveiller ces événements de fenêtre contextuelle lors de l'enregistrement des sessions. Notez que les fenêtres contextuelles des navigateurs Web ne sont pas surveillées.

Les attributs d'un événement de fenêtre contextuelle sont enregistrés, y compris le nom du processus et le contenu de l'invite.

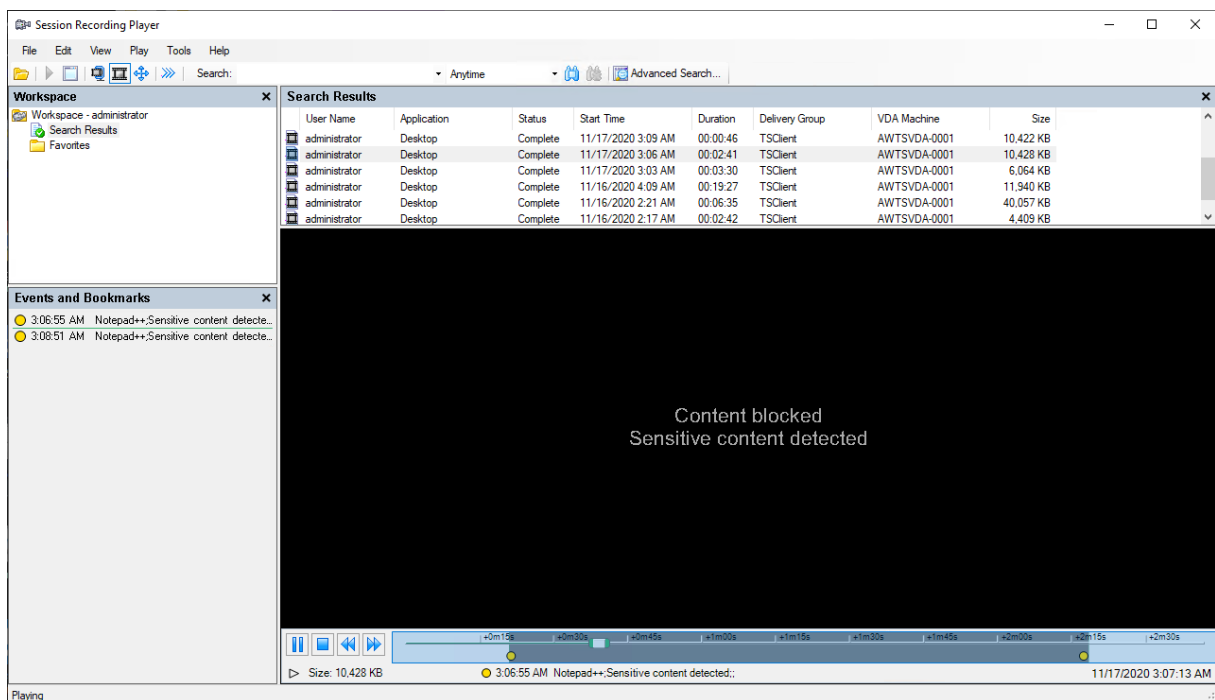
```

1:23:48 AM Popup Window: 2192, Remote Desktop Connection, Connecting to [IP address] Initiating remote connection...
1:24:05 AM Popup Window: 2192, Remote Desktop Connection, Remote Desktop can't connect to the remote computer for one of these reasons:\n\n1) Remote access to the server is not enabled\n2) The remote computer is turned off\n3) The remote...
    
```

Événements personnalisés

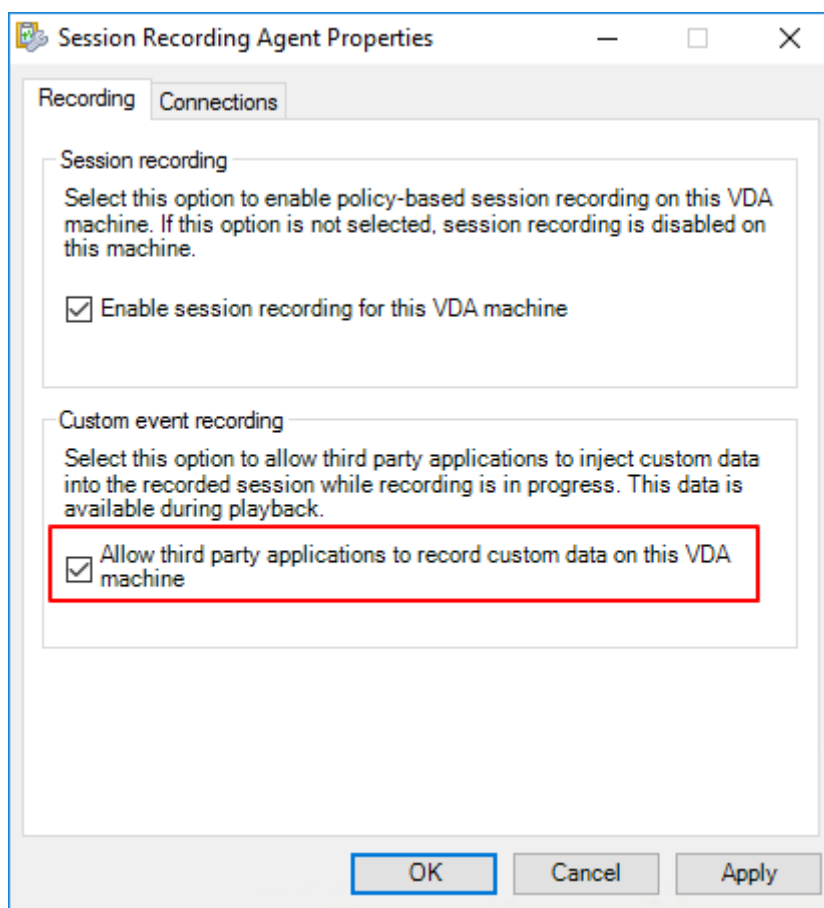
L'agent d'enregistrement de session fournit l'interface COM IUserAPI que les applications tierces peuvent utiliser pour ajouter des données d'événement spécifiques à l'application dans les sessions enregistrées. En fonction de la personnalisation de l'événement, l'enregistrement de session peut bloquer les informations sensibles et consigner les événements de pause et de reprise de session en conséquence.

Blocage d'informations sensibles L'enregistrement de session vous permet d'ignorer certaines périodes lors de l'enregistrement de l'écran et de bloquer les informations sensibles pendant ces périodes au cours de la lecture de session. Pour utiliser cette fonctionnalité, utilisez Enregistrement de session 2012 et versions ultérieures.



Pour utiliser cette fonctionnalité, procédez comme suit :

1. Dans **Propriétés de l'Agent d'enregistrement de session**, activez la case à cocher **Autoriser les applications tierces à enregistrer des données personnalisées sur cette machine VDA** et cliquez sur **Appliquer**.

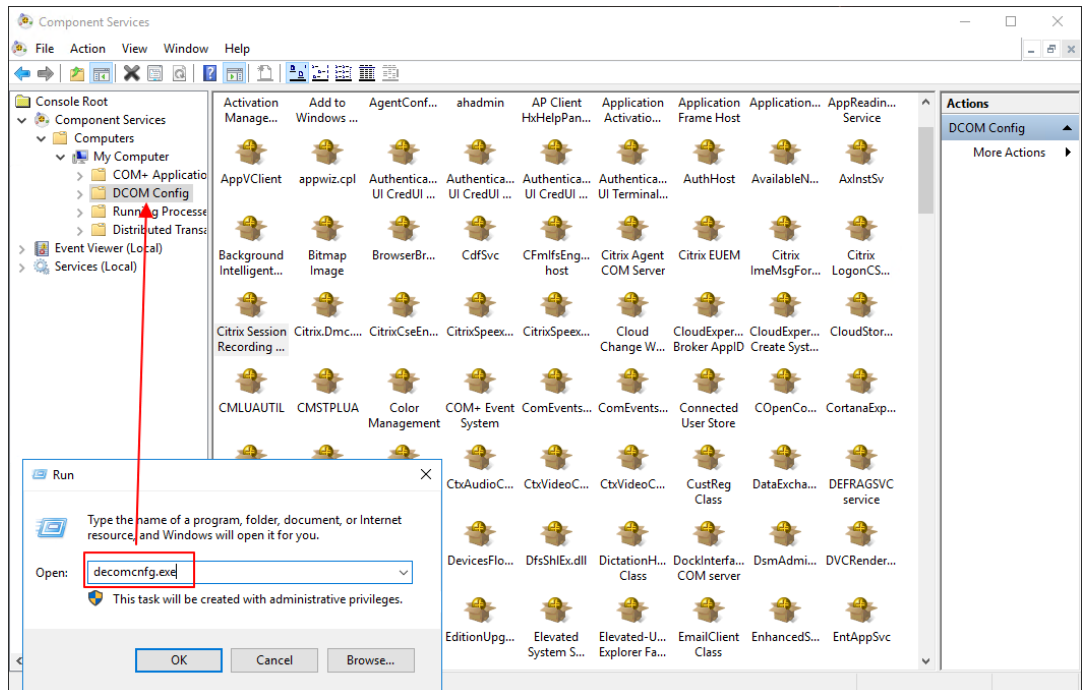


2. Accordez aux utilisateurs l'autorisation d'appeler l'API d'événements de l'enregistrement de session (interface COM IUserAPI).

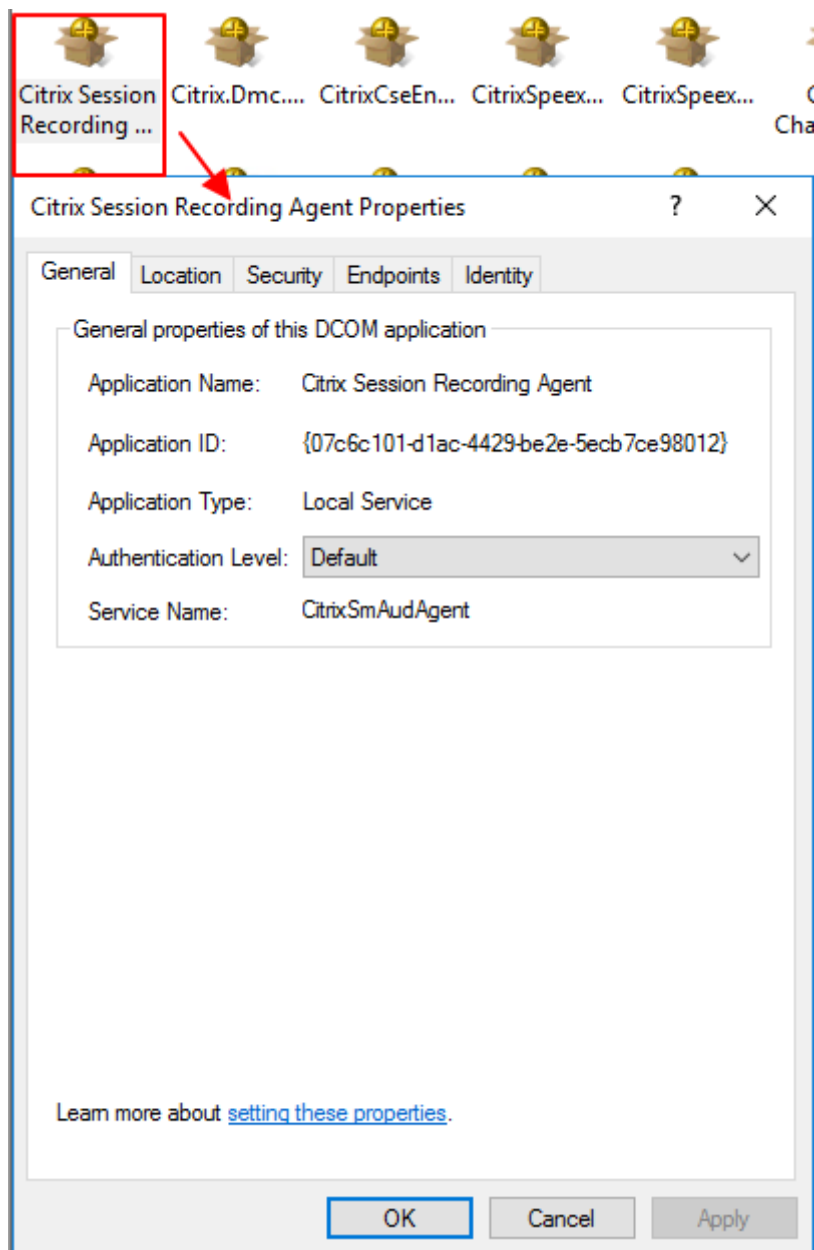
L'enregistrement de session a ajouté le contrôle d'accès à l'interface COM API d'événement dans la version 7.15. Seuls les utilisateurs autorisés peuvent invoquer la fonctionnalité pour insérer des métadonnées d'événement dans un enregistrement.

Les administrateurs locaux bénéficient de cette autorisation par défaut. Pour accorder cette autorisation à d'autres utilisateurs, utilisez l'outil de configuration Windows DCOM :

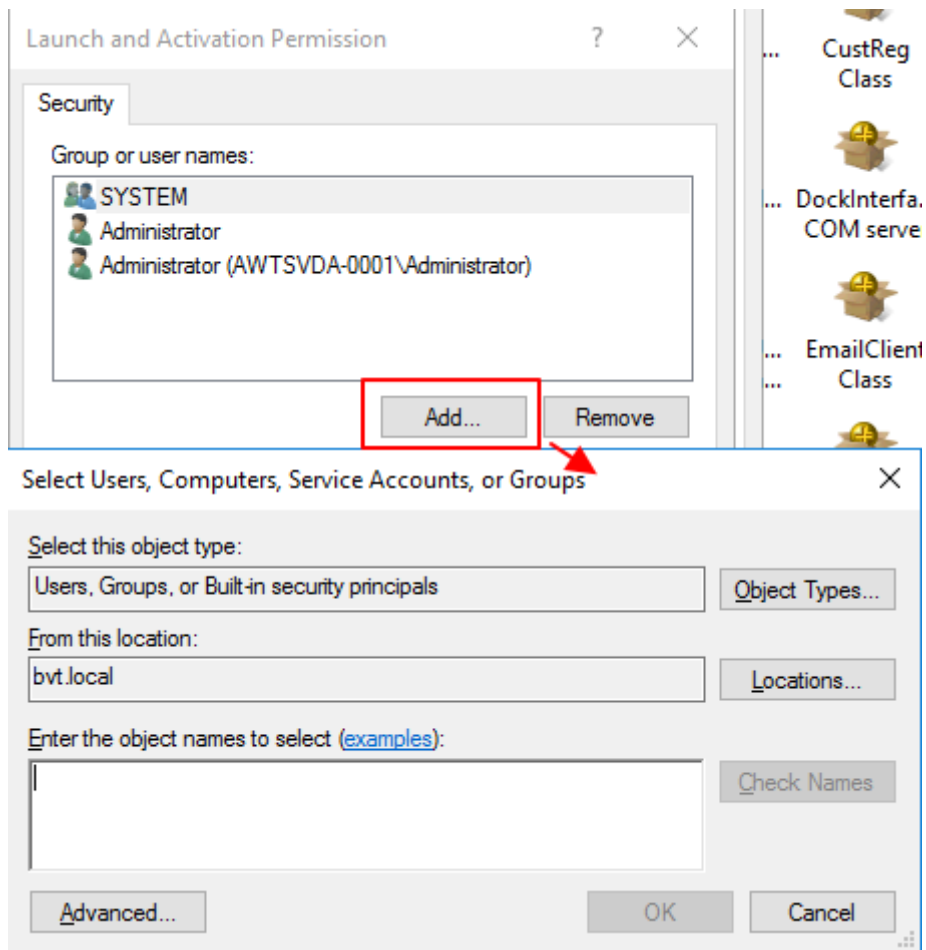
- a) Ouvrez l'outil de configuration Windows DCOM sur l'agent d'enregistrement de session en exécutant `dcomcnfg.exe`.

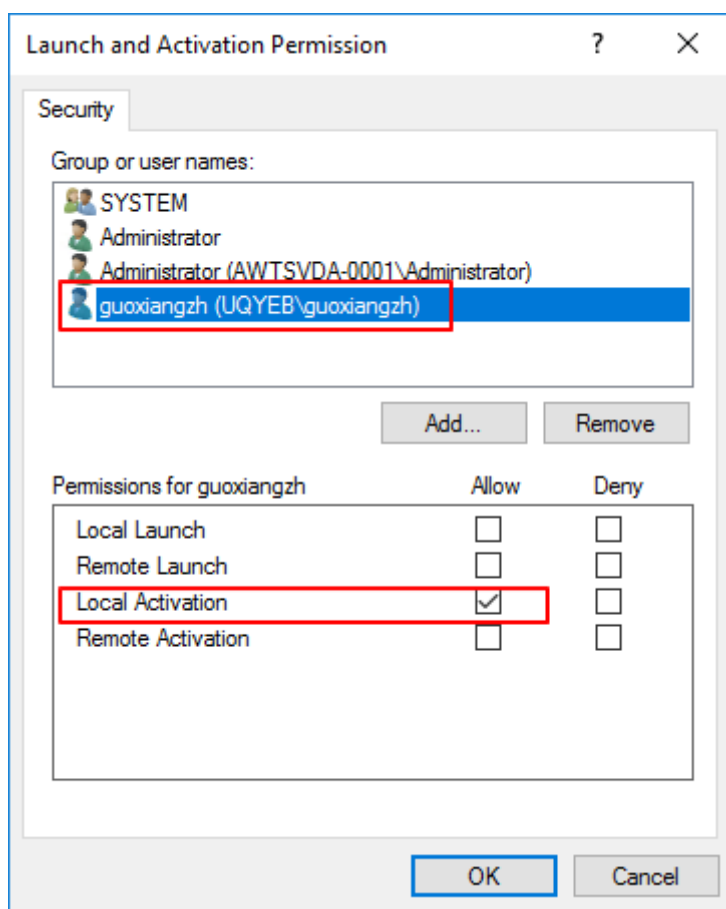


- b) Cliquez avec le bouton droit sur **Agent d'enregistrement de session Citrix** et choisissez **Propriétés**.



- c) Sélectionnez l'onglet **Sécurité**, puis cliquez sur **Modifier** pour ajouter des utilisateurs disposant de l'autorisation **Activation locale** dans la section **Autorisations d'exécution et d'activation**.



**Remarque :**

la configuration DCOM prend effet immédiatement. Il n'est pas nécessaire de redémarrer les services ou la machine.

- Démarrez une session virtuelle Citrix.
- Démarrez PowerShell et modifiez le lecteur actuel vers le dossier **<chemin d'installation de l'Agent d'enregistrement de session>\Bin** pour importer le module SRUserEventHelper-Snapin.dll.
- Exécutez les applets de commande `Session-Pause` et `Session-Resume` pour définir les paramètres de déclenchement du blocage des informations sensibles.

Paramètre	Description	Requis ou facultatif
-APP	Nom de l'application qui appelle l'applet de commande.	Obligatoire

Paramètre	Description	Requis ou facultatif
-Reason	Raison pour laquelle le contenu est bloqué. Si vous laissez ce paramètre non spécifié, la valeur par défaut s’affiche, indiquant Contenu bloqué et Du contenu sensible a été détecté et bloqué.. Si vous définissez ce paramètre, la raison que vous spécifiez s’affiche lorsque vous accédez à la période bloquée pendant la lecture de session.	Facultatif

Par exemple, vous pouvez exécuter `Session-Pause` de la manière suivante :

```

Select Administrator: PowerShell
PS C:\Program Files\Citrix\SessionRecording\Agent\Bin> man Session-Pause

NAME
    Session-Pause

SYNOPSIS
    Session-Pause [-App] <string> [[-Reason] <string>] [<CommonParameters>]

SYNTAX
    Session-Pause [-App] <string> [[-Reason] <string>] [<CommonParameters>]

DESCRIPTION
    User can use it to pause current session.

RELATED LINKS

REMARKS
    To see the examples, type: "get-help Session-Pause -examples".
    For more information, type: "get-help Session-Pause -detailed".
    For technical information, type: "get-help Session-Pause -full".

PS C:\Program Files\Citrix\SessionRecording\Agent\Bin> Session-Pause -App Notepad++ -Reason 'Sensitive content detected'
Getting type from local machine...
Creating instance...
Querying IUserApi interface...
*** Connected ***

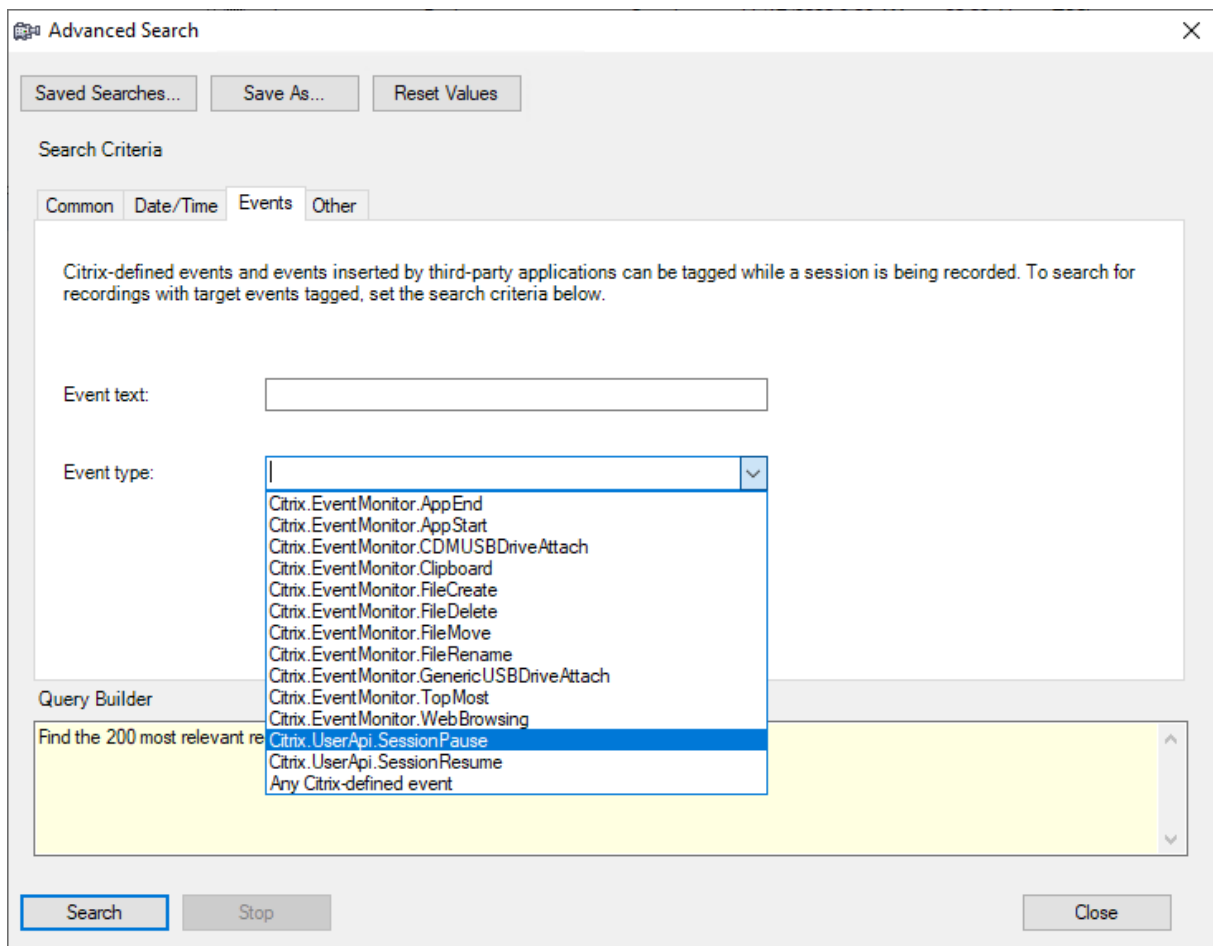
Formatting data for send...
Calling IUserApi.LogDataWithExtData...
*** Call Success ***
PS C:\Program Files\Citrix\SessionRecording\Agent\Bin>
    
```

Rechercher et visualiser des enregistrements avec des événements marqués

Rechercher des enregistrements avec des événements marqués Le lecteur d’enregistrement de session vous permet d’effectuer des recherches avancées sur des enregistrements avec événements marqués.

1. Dans le lecteur d'enregistrement de session, cliquez sur **Recherche avancée** dans la barre d'outils ou choisissez **Outils > Recherche avancée**.
2. Définissez vos critères de recherche dans la boîte de dialogue **Recherche avancée**.

L'onglet **Événements** vous permet de rechercher des événements marqués dans les sessions par **texte d'événement**, **type d'événement** ou les deux. Vous pouvez combiner les filtres **Événements**, **Commun**, **Date/Heure** et **Autre** pour rechercher des enregistrements répondant à vos critères.



Remarque :

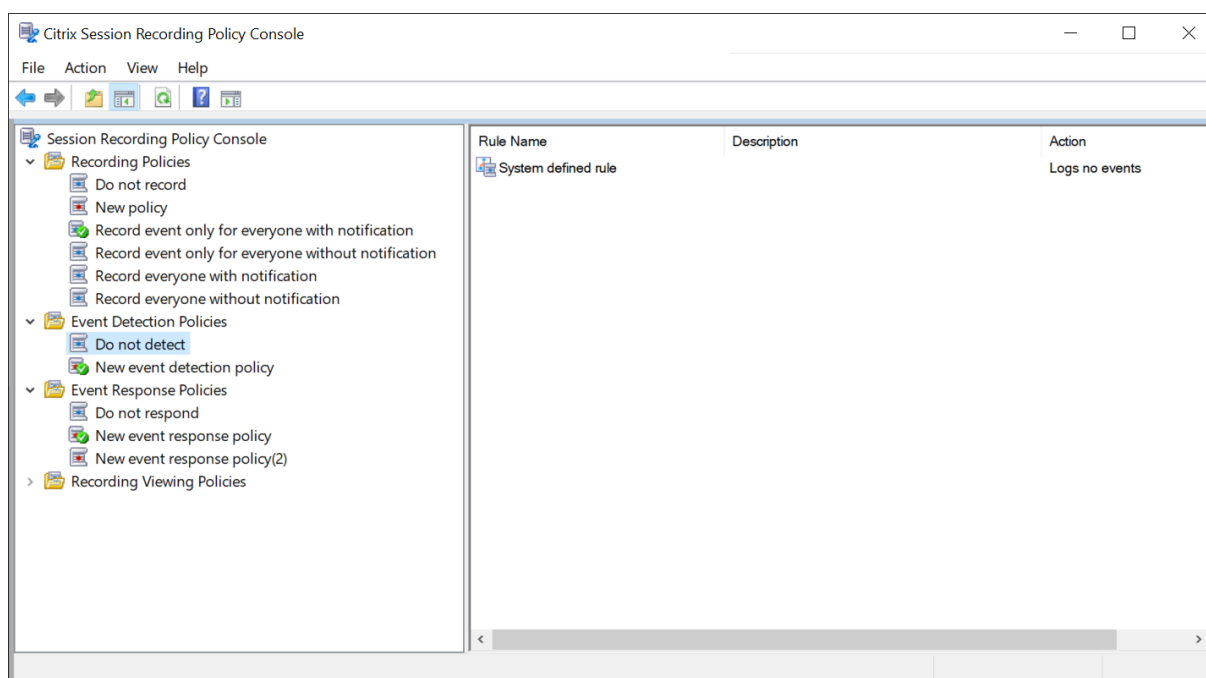
- La liste **Type d'événement** répertorie tous les types d'événements. Vous pouvez sélectionner un type d'événement à rechercher. La sélection de **Tout événement défini par Citrix** équivaut à rechercher tous les enregistrements avec tout type d'événement consigné par l'enregistrement de session Citrix.
- Le filtre **Texte de l'événement** prend en charge la correspondance partielle. Les caractères génériques ne sont pas pris en charge.
- Le filtre **Texte de l'événement** n'est pas sensible à la casse lors de la correspondance.
- Pour les types d'événements, les mots **App Start**, **App End**, **Client drive**

mapping et File Rename ne donnent pas de résultat lors d'une recherche par **Texte de l'événement**. Par conséquent, lorsque vous tapez App Start, App End, Client drive mapping ou File Rename dans la zone **Texte de l'événement**, aucun résultat ne peut être trouvé.

Vous pouvez utiliser les événements pour naviguer dans une session enregistrée ou passer directement aux points où les événements sont marqués.

Stratégie de détection d'événements définie par le système

La stratégie de détection d'événements définie par le système est **Ne pas détecter**. Elle est inactive par défaut. Lorsque cette stratégie est active, aucun événement n'est journalisé.



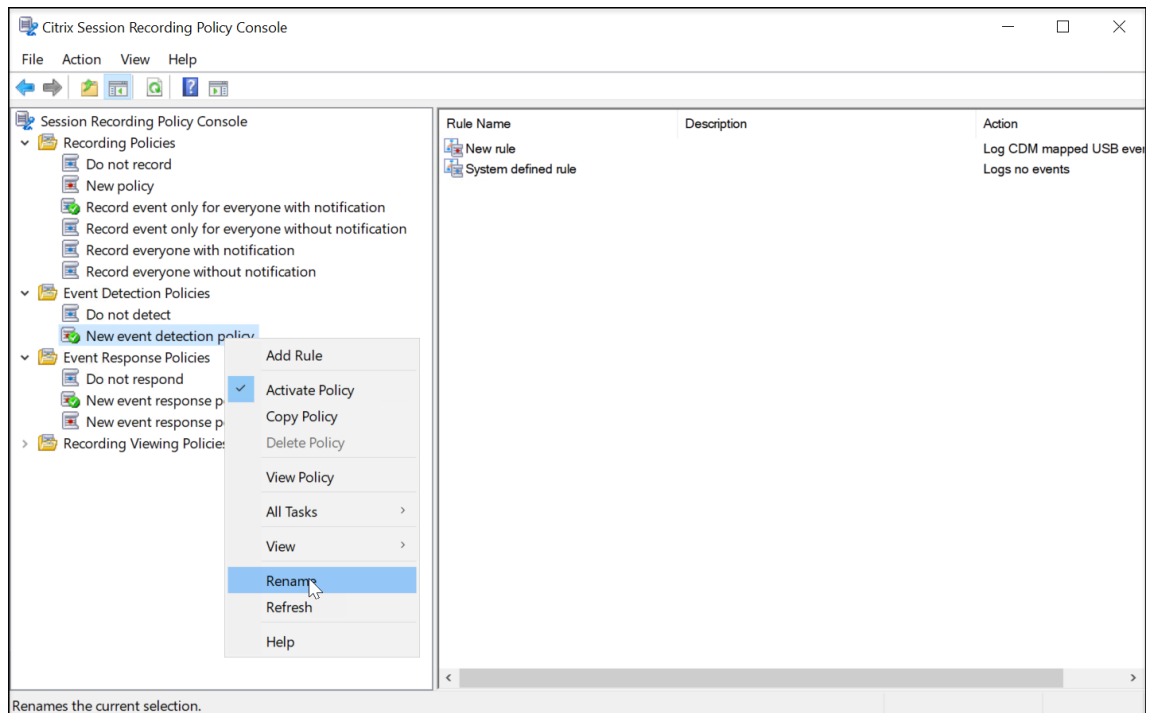
Vous ne pouvez pas modifier ou supprimer les stratégies de détection définies par le système.

Créer une stratégie de détection d'événements personnalisée

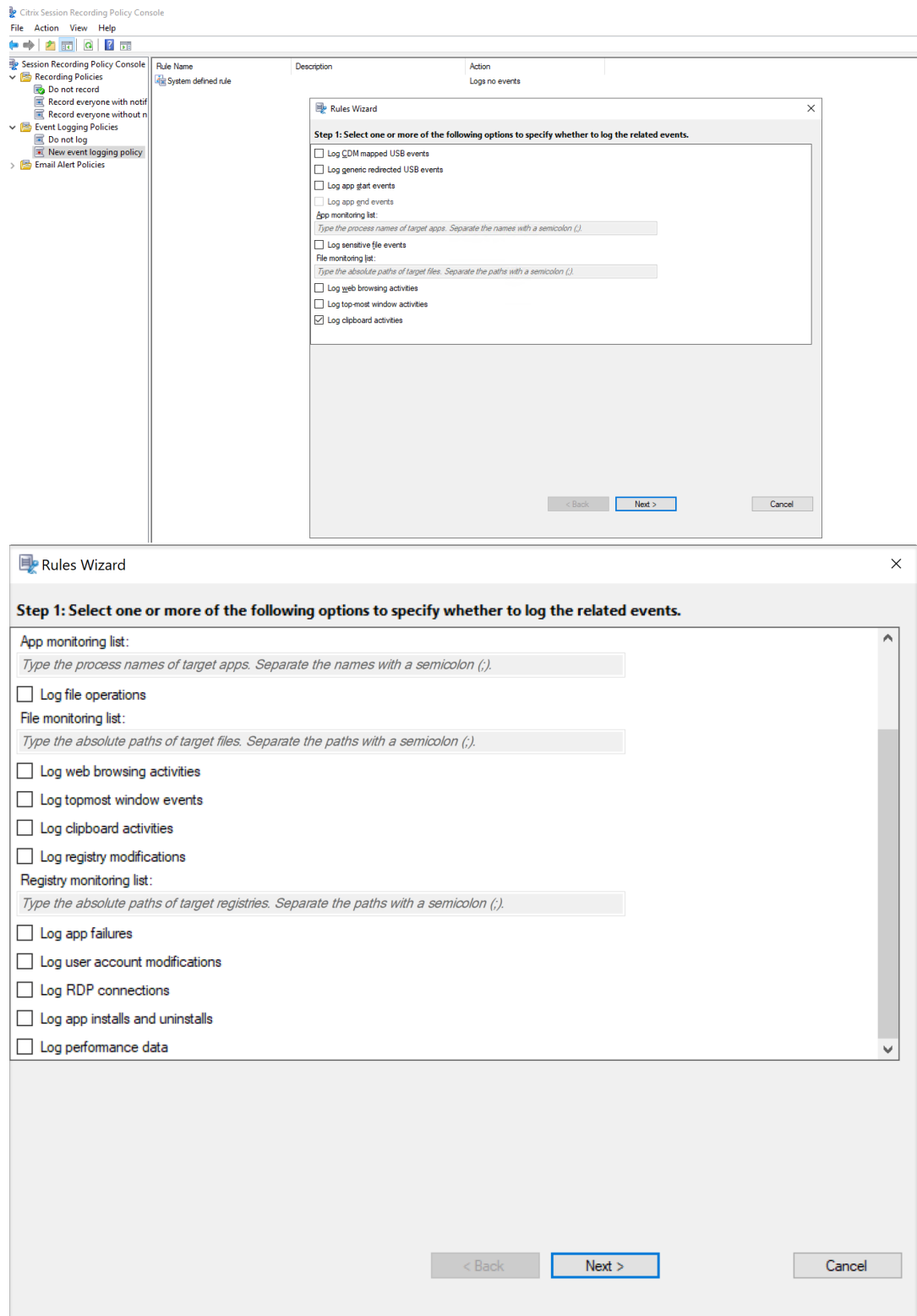
Pour créer une stratégie de détection d'événements personnalisée :

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session.
Par défaut, il n'existe pas de stratégie de détection d'événements active.

3. Sélectionnez **Stratégies de détection d'événements** dans le volet gauche. Dans la barre de menu, choisissez **Ajouter une nouvelle stratégie** pour créer une stratégie de détection d'événements.
4. (Facultatif) Cliquez avec le bouton droit de la souris sur la nouvelle stratégie et renommez-la.



5. Cliquez avec le bouton droit sur la nouvelle stratégie de détection d'événements et sélectionnez **Ajouter une règle**.
 - a) Spécifiez un ou plusieurs événements cibles à surveiller en cochant la case en regard de chaque type d'événement. Faites défiler la fenêtre vers le bas pour afficher tous les types d'événements disponibles.



- **Consigner les événements USB mappés par CDM** : journalise l'insertion d'un périphérique de stockage de masse mappé (CDM) sur un client sur lequel l'application Citrix Workspace pour Windows ou Mac est installée.

- **Consigner la redirection USB générique** : journalise l'insertion d'un périphérique de stockage de masse redirigé générique sur un client sur lequel l'application Citrix Workspace pour Windows ou Mac est installée.
- **Consigner les événements de démarrage d'application** : enregistre les événements de démarrage des applications cibles.
- **Consigner les événements de fin d'application** : enregistre les événements de fin des applications cibles.

Remarque :

La case à cocher **Consigner les événements de fin d'application** est grisée si l'option **Consigner les événements de démarrage d'application** n'est pas sélectionnée.

- **Liste de surveillance des applications** : lorsque vous sélectionnez **Consigner les événements de démarrage d'application** et **Consigner les événements de fin d'application**, utilisez la **liste de surveillance des applications** pour spécifier les applications cibles à surveiller et éviter qu'une quantité excessive d'événements ne sature les enregistrements.

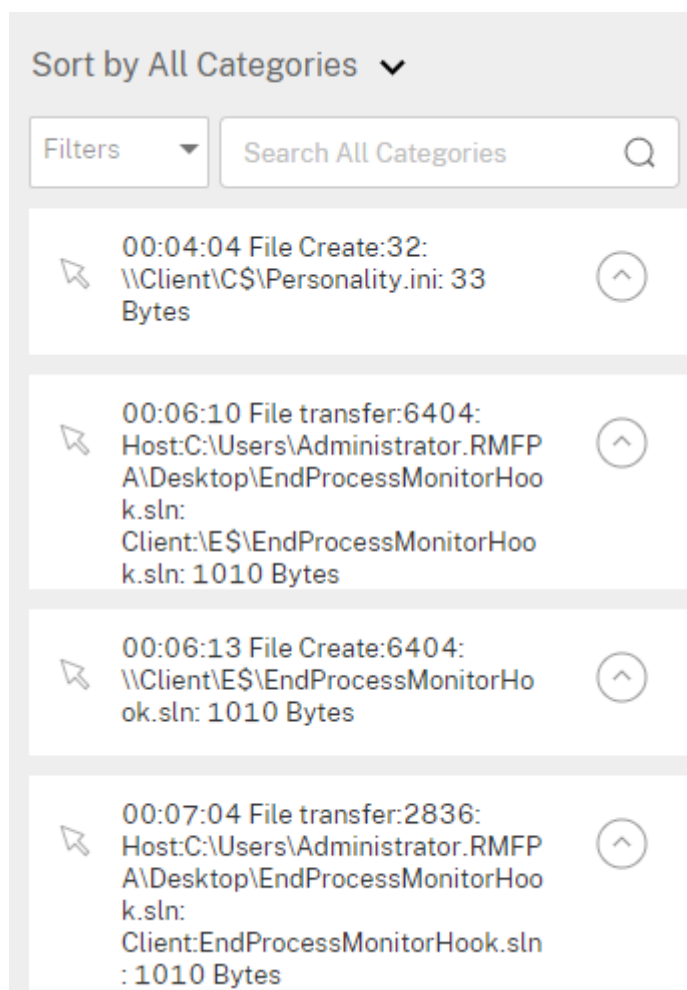
Remarque :

- Pour capturer le démarrage et la fin d'une application, ajoutez le nom du processus de l'application dans la **liste de surveillance des applications**. Par exemple, pour capturer le démarrage de la fonction Connexion Bureau à distance, ajoutez le nom du processus `mstsc.exe` dans la **liste de surveillance des applications**. Lorsque vous ajoutez un processus à la **liste de surveillance des applications**, les applications lancées par le processus ajouté et ses processus enfants sont surveillées. Par défaut, Enregistrement de session ajoute les noms des processus, `cmd.exe`, `powershell.exe` et `wsl.exe`, à la **liste de surveillance des applications**. Si vous sélectionnez **Consigner les événements de démarrage d'application** et **Consigner les événements de fin d'application** pour une stratégie de détection des événements, les démarrages et les fins des applications Invite de commandes, PowerShell et Sous-système Windows pour Linux (WSL) sont consignés, que vous ajoutiez ou non manuellement leurs noms de processus à la **liste de surveillance des applications**. Les noms de processus par défaut ne sont pas visibles dans la **liste de surveillance des applications**.
- Séparez les noms de processus par un point-virgule (;).
- Seule la correspondance exacte est prise en charge. Les caractères génériques ne sont pas pris en charge.

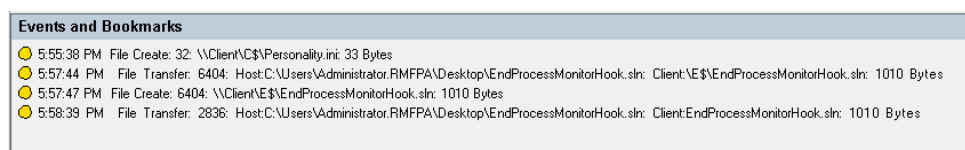
- Les noms des processus que vous ajoutez ne sont pas sensibles à la casse.
- Pour éviter qu'une quantité excessive d'événements ne sature les enregistrements, n'ajoutez aucun nom de processus système (par exemple, explorer.exe) et de navigateurs Web au registre.

- **Consigner les opérations de fichiers** : journalise les opérations sur les fichiers cibles dans la **Liste de surveillance des fichiers** et journalise les transferts de fichiers entre les hôtes de session (VDA) et les machines clientes (y compris les lecteurs clients mappés et les périphériques de stockage de masse génériques redirigés). La sélection de cette option déclenche la journalisation des transferts de fichiers, que vous spécifiez ou non la **Liste de surveillance des fichiers**.

- Événements de fichiers présentés dans le lecteur Web



- Événements de fichiers présentés dans le lecteur d'enregistrement de session



- **Liste de surveillance des fichiers** : lorsque vous sélectionnez **Consigner les opérations de fichiers**, utilisez la **liste de surveillance des fichiers** pour spécifier les fichiers cibles à surveiller. Vous pouvez spécifier les dossiers dans lesquels capturer tous les fichiers. Aucun fichier n'est spécifié par défaut, ce qui signifie qu'aucun fichier n'est capturé par défaut.

Remarque :

- Pour capturer les opérations de changement de nom, de création, de suppression ou de déplacement sur un fichier, ajoutez la chaîne de chemin du dossier de fichiers (et non le nom de fichier ou le chemin racine du dossier de fichiers) dans la **liste de surveillance des fichiers**. Par exemple, pour capturer les opérations de changement de nom, de création, de suppression et de déplacement sur le fichier `sharing.ppt` dans `C:\User\File`, ajoutez la chaîne de chemin `C:\User\File` dans la **liste de surveillance des fichiers**.
- Les chemins de fichiers locaux et les chemins de dossiers partagés distants sont pris en charge. Par exemple, pour capturer les opérations sur le fichier `RemoteDocument.txt` dans le dossier `\\remote.address\Documents`, ajoutez la chaîne de chemin `\\remote.address\Documents` dans la **liste de surveillance des fichiers**.
- Séparez les chemins à surveiller par un point-virgule (;).
- Seules les correspondances exactes sont prises en charge. Les caractères génériques ne sont pas pris en charge.
- Les chaînes de chemin sont insensibles à la casse.

Limitations :

- La copie de fichiers ou de dossiers d'un dossier local surveillé vers un dossier local non surveillé n'est pas capturée.
- Lorsque la longueur du chemin d'accès d'un fichier ou d'un dossier, y compris le nom du fichier ou du dossier, dépasse 260 caractères, les opérations sur le fichier ou le dossier ne sont pas capturées.
- Faites attention à la taille de la base de données. Pour empêcher la capture d'un grand nombre d'événements, sauvegardez ou supprimez régulièrement la table « Événement ».
- Lorsqu'un grand nombre d'événements est capturé pendant une courte période, le lecteur n'affiche qu'un seul événement et la base de données ne stocke qu'un seul événement pour chaque type afin d'éviter un engorgement du stockage.

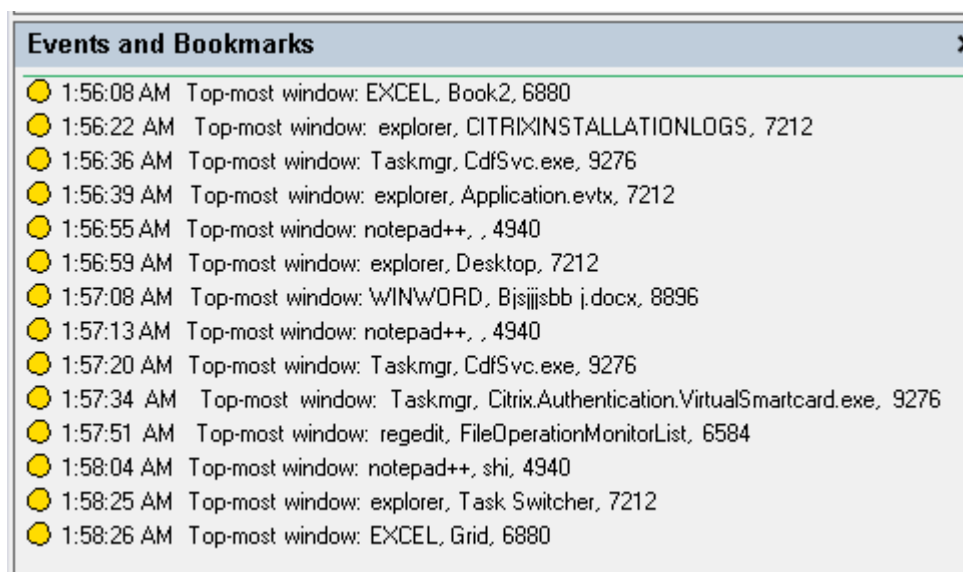
- **Consigner les activités de navigation sur le Web** : consigne les activités des utilisateurs sur les navigateurs pris en charge et identifie le nom du navigateur, l'URL et le titre de la page dans l'enregistrement.



Liste des navigateurs pris en charge :

Navigateur	Version
Chrome	69 et versions ultérieures
Internet Explorer	11
Firefox	61 et versions ultérieures

- **Consigner les événements de la fenêtre principale** : consigne les événements de la fenêtre principale et ajoute une balise au nom, au titre et au numéro du processus dans l'enregistrement.



- **Enregistrer les activités du presse-papiers** : consigne les opérations de copie de texte, d'images et de fichiers à l'aide du Presse-papiers. Le nom du processus et le chemin d'accès du fichier sont consignés pour une copie de fichier. Le titre et le nom du processus sont consignés pour une copie de texte. Le nom du processus est consigné pour une copie d'image.
- **Consigner les modifications du registre** : enregistre les modifications du registre Windows, notamment l'ajout d'une clé ou d'une valeur, le changement de nom d'

une clé ou d'une valeur, la modification d'une valeur existante et la suppression d'une clé ou d'une valeur.

- **Liste de surveillance du registre:** lorsque vous sélectionnez **Consigner les modifications du registre**, entrez les chemins d'accès absolus des registres cibles que vous souhaitez surveiller et séparez les chemins par un point-virgule (;). Démarrez un chemin d'accès par HKEY_USERS, HKEY_LOCAL_MACHINE ou HKEY_CLASSES_ROOT. Par exemple, vous pouvez entrer `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows;HKEY_CLASSES_ROOT\GuestStateVDev`. Si vous ne spécifiez pas cette liste, aucune modification du registre n'est capturée.
- **Consigner défaillances d'application :** enregistre les fermetures inattendues des applications et les applications qui ne répondent pas. Cette règle s'applique à toutes les applications.
- **Enregistrer les modifications du compte utilisateur :** enregistre les modifications du compte utilisateur, notamment la création, l'activation, la désactivation, la suppression, le verrouillage, les changements de nom et les tentatives de modification du mot de passe du compte.
- **Consigner les connexions RDP :** enregistre les connexions RDP initiées à partir du VDA hébergeant la session enregistrée.
- **Consigner installations et désinstallations d'applications :** enregistre les installations et les désinstallations d'applications au cours de la session enregistrée. Cette règle s'applique à toutes les applications.
- **Enregistrer les données de performances :** active la fonctionnalité de superposition des données de session. Activez cette case à cocher pour afficher les points de données liés à la session enregistrée.
- **Fenêtres contextuelles de journal :** enregistre les fenêtres contextuelles qui peuvent apparaître lorsque les utilisateurs ouvrent ou ferment un fichier confidentiel ou accèdent à un dossier.

b) Sélectionnez et modifiez les critères de règle.

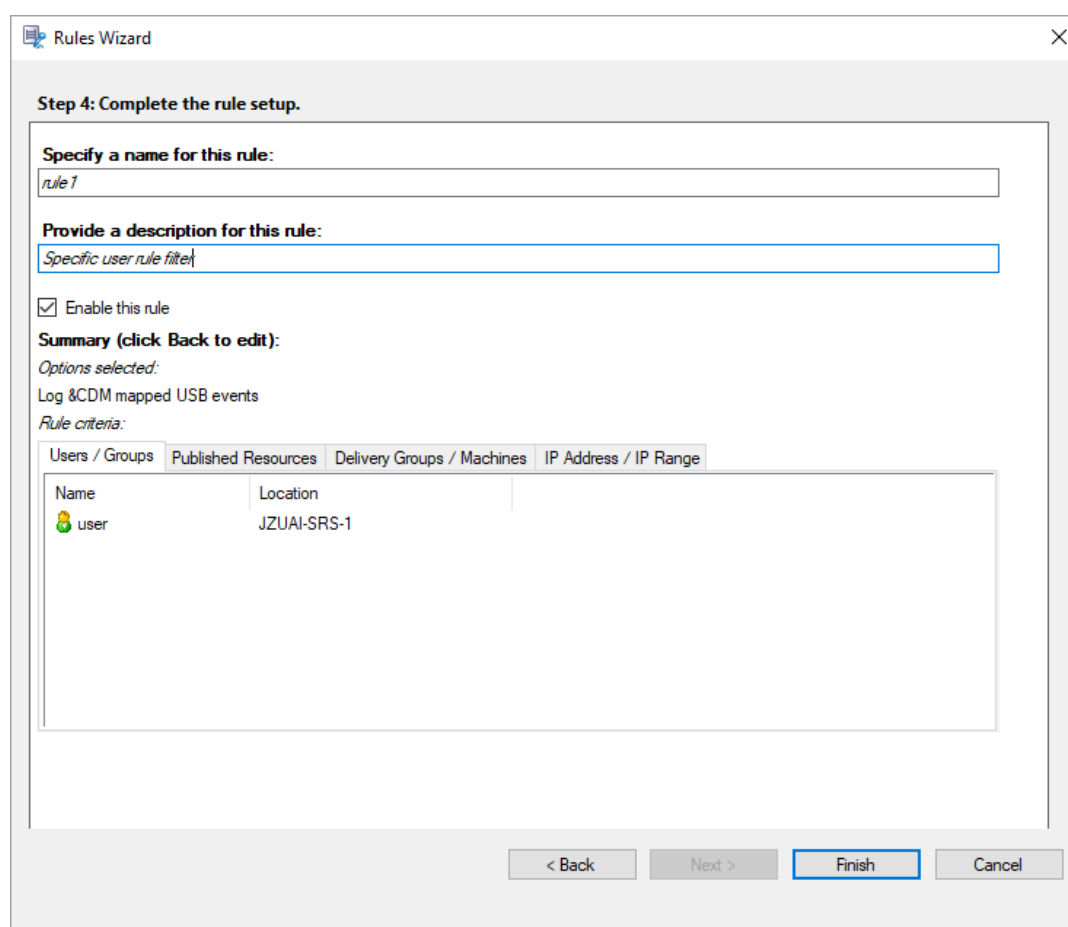
De la même façon que vous avez créé une stratégie d'enregistrement personnalisée, sélectionnez un ou plusieurs critères de règle : **Utilisateurs ou Groupes, Applications ou bureaux publiés, Groupes de mise à disposition ou Machines** et **Adresse IP ou Plage d'adresses IP**. Pour obtenir la liste des applications publiées ou des bureaux publiés, ainsi que la liste des groupes de mise à disposition ou des machines VDA, vous devez disposer d'autorisations d'accès en lecture de l'administrateur du site. Configurez l'autorisation de lecture de l'administrateur sur le Delivery Controller du site.

Pour plus d'informations, consultez les instructions de la section [Créer une stratégie d'enregistrement personnalisée](#).

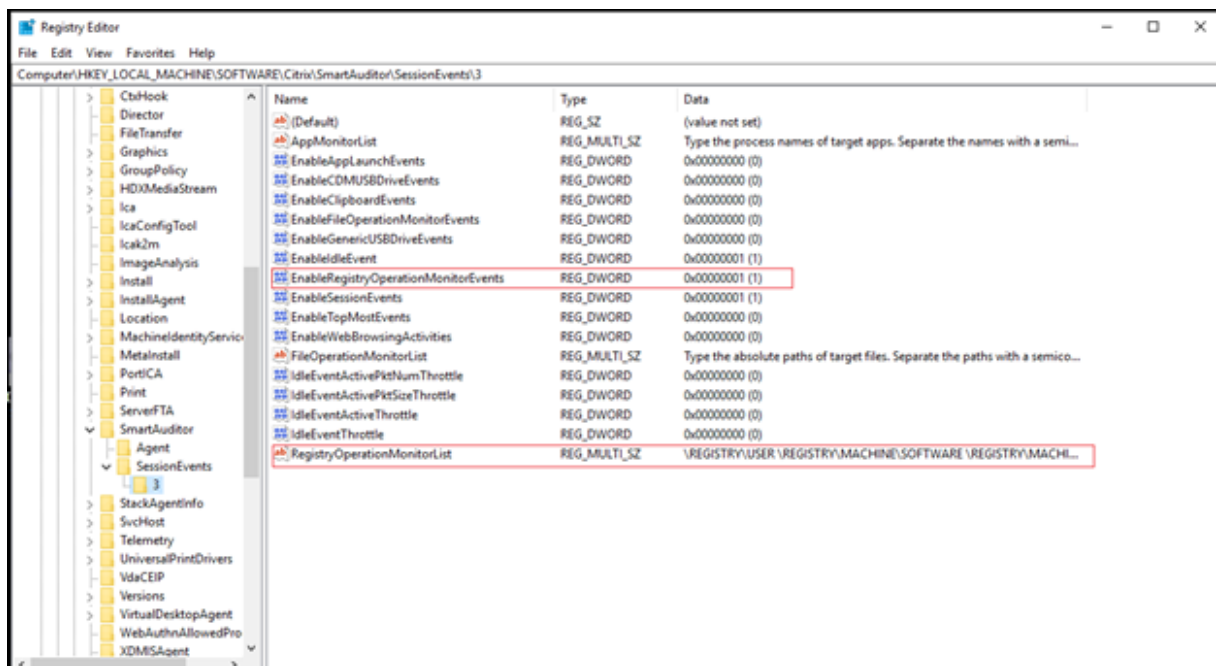
Remarque :

Il se peut que certaines sessions ne correspondent à aucun critère de règle d'une stratégie de détection d'événements. Pour ces sessions, l'action de la règle de repli s'applique ; celle-ci est toujours définie sur **Ne pas détecter**. Vous ne pouvez pas modifier ou supprimer la règle de repli.

c) Suivez les instructions de l'assistant pour terminer l'installation.



Après le démarrage d'une session correspondant à une stratégie de détection d'événements, l'ID de session et ses valeurs de registre d'événements s'affichent dans l'agent d'enregistrement de session. Par exemple :



Compatibilité avec les configurations de registre

Lorsque l'enregistrement de session est récemment installé ou mis à niveau, aucune stratégie de détection d'événements active n'est disponible par défaut. Dans ce cas, chaque agent d'enregistrement de session respecte les valeurs de registre sous `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEvents` pour déterminer si des événements spécifiques doivent être journalisés. Pour obtenir une description des valeurs de registre, consultez le tableau suivant :

Valeur de registre

Description

EnableSessionEvents

1 : active la détection d'événements de manière globale ; **0** : désactive la détection d'événements de manière globale (données de valeur par défaut).

EnableAccountChangeEvents

1 : active la détection des modifications du compte utilisateur ; **0** : désactive la détection des modifications du compte utilisateur (données de valeur par défaut).

Valeur de registre	Description
EnableAppChangeEvents	1 : active la détection des installations et des désinstallations d'applications ; 0 : désactive la détection des installations et des désinstallations d'applications (données de valeur par défaut).
EnableAppFaultEvents	1 : active la détection des défaillances des applications ; 0 : désactive la détection des défaillances des applications (données de valeur par défaut).
EnableAppLaunchEvents	1 : active la détection des démarrages d'applications uniquement ; 2 : active la détection des démarrages et des fins d'applications ; 0 : désactive la détection des démarrages et des fins d'applications (données de valeur par défaut)
AppMonitorList	Spécifie les applications cibles à surveiller. Aucune application n'est spécifiée par défaut, ce qui signifie qu'aucune application n'est capturée par défaut.

Valeur de registre	Description
EnableCDMUSBDriveEvents	1 : active la détection de l'insertion de périphériques de stockage de masse USB mappés CDM ; 0 : désactive la détection de l'insertion de périphériques de stockage de masse USB mappés CDM (données de valeur par défaut).
EnableClipboardEvents	1 : active la détection des activités du presse-papiers ; 0 : désactive la détection des activités du presse-papiers (données de valeur par défaut).
EnableFileOperationMonitorEvents	1 : active les opérations de détection de fichiers ; 0 : désactive les opérations de détection de fichiers (données de valeur par défaut).
FileOperationMonitorList	Spécifie les dossiers cibles à surveiller. Aucun dossier n'est spécifié par défaut, ce qui signifie qu'aucune opération de fichier n'est capturée par défaut.
EnableGenericUSBDriveEvents	1 : active la détection de l'insertion de périphériques de stockage de masse USB génériques redirigés ; 0 : désactive la détection de l'insertion de périphériques de stockage de masse USB génériques redirigés (données de valeur par défaut).

Valeur de registre	Description
EnablePerfDataEvents	1 : active la fonction de superposition des données de session ; 0 : désactive la fonction de superposition des données de session (données de valeur par défaut).
EnablePopupWindowEvents	1 : active la détection des événements de fenêtre contextuelle ; 0 : désactive la détection des événements de fenêtre contextuelle (données de valeur par défaut).
EnableRDPConnectionEvents	1 : active la détection des connexions RDP ; 0 : désactive la détection des connexions RDP (données de valeur par défaut).
EnableRegistryOperationMonitorElement	1 : active la détection des modifications du registre Windows ; 0 : désactive la détection des modifications du registre Windows (données de valeur par défaut).
RegistryOperationMonitorList	Spécifie les registres cibles à surveiller. Aucun registre n'est spécifié par défaut, ce qui signifie qu'aucune modification du registre n'est capturée par défaut.
EnableWebBrowsingActivities	1 : active la détection des activités de navigation sur Internet ; 0 : désactive la détection des activités de navigation sur Internet (données de valeur par défaut).

Vous trouverez ci-dessous plusieurs scénarios compatibles :

- Si l'enregistrement de session est récemment installé ou mis à niveau à partir d'une version antérieure à 1811 qui ne prend pas en charge la détection (journalisation) d'événements, les valeurs de registre associées sur chaque agent d'enregistrement de session sont les valeurs par défaut. Par défaut, il n'existe pas de stratégie de détection d'événements active ; aucun événement n'est donc journalisé.
- Si l'enregistrement de session est mis à niveau à partir d'une version antérieure à 1811 qui prend en charge la détection d'événements mais dont la fonctionnalité est désactivée avant la mise à niveau, les valeurs de registre associées sur chaque agent d'enregistrement de session restent les valeurs par défaut. Par défaut, il n'existe pas de stratégie de détection d'événements active ; aucun événement n'est donc journalisé.
- Si l'enregistrement de session est mis à niveau à partir d'une version antérieure à 1811 qui prend en charge la détection d'événements et dont la fonctionnalité est partiellement ou entièrement activée avant la mise à niveau, les valeurs de registre associées sur chaque agent d'enregistrement de session restent les valeurs par défaut. Par défaut, il n'existe pas de stratégie de détection d'événements active ; le comportement de la détection d'événements reste donc le même.
- Si l'enregistrement de session est mis à niveau à partir de 1811, les stratégies de détection (journalisation) des événements configurées dans la console de stratégie restent en fonction.

Attention :

Lorsque vous activez la stratégie de détection d'événements définie par le système ou personnalisée, les paramètres de registre pertinents sur chaque agent d'enregistrement de session sont ignorés. Dans ce cas, vous ne pouvez plus utiliser les paramètres de registre pour la détection des événements.

Configurer les stratégies de réponse aux événements

February 20, 2024

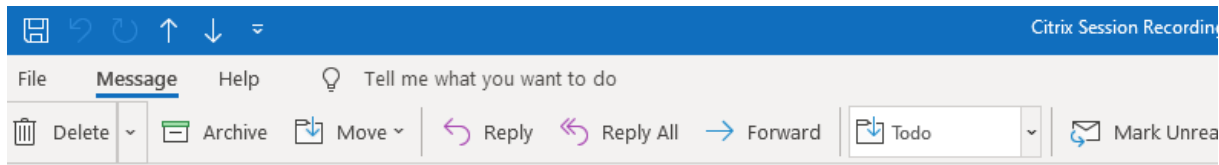
Ce paramètre de stratégie vous permet d'effectuer les actions suivantes en réponse aux événements consignés dans les sessions enregistrées :

- Envoyer des alertes par e-mail
- Lancer immédiatement l'enregistrement d'écran
- Verrouiller la session
- Fermer la session


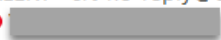
- Déconnecter la session

La seule stratégie de réponse aux événements définie par le système est **Ne pas répondre**. Vous pouvez créer des stratégies de réponse aux événements personnalisées si nécessaire. Une seule stratégie de réponse aux événements peut être active à la fois.

Pour obtenir un exemple d'alerte par e-mail, consultez la capture d'écran suivante.



Citrix Session Recording Alert: A TopMost was detected. VDAMachine: AWTSVDA-0002;


 SR-ALERT <srt-no-reply@outlook.com>
To: 

[CAUTION - EXTERNAL EMAIL] DO NOT REPLY

Hi, @citrix.com

This email comes from Citrix Session Recording to notify you that a **TopMost** was detected:

Session Details

User Name	administrator
Domain Name	X8X7E
Start Time	11/9/2020 3:15:06 AM
Delivery Group	Rds DesktopAndAppGroup
Application	###Desktop,
VDA Machine	
Playback URL	<a data-bbox="900 1240 1054 1270" href="https:// /webplayer/#/player/">https://  /webplayer/#/player/
Event Text	TopApp: reedit
Event Time	11/9/2020 3:17:51 AM

You can find the session recording video and more information [here](#).

This is an automated email from Citrix Session Recording. Do not reply.

Conseil :

Cliquez sur l'URL de lecture pour ouvrir la page de lecture de la session enregistrée dans le lecteur Web. Cliquez [ici](#) pour ouvrir la page **Tous les enregistrements** dans le lecteur Web.

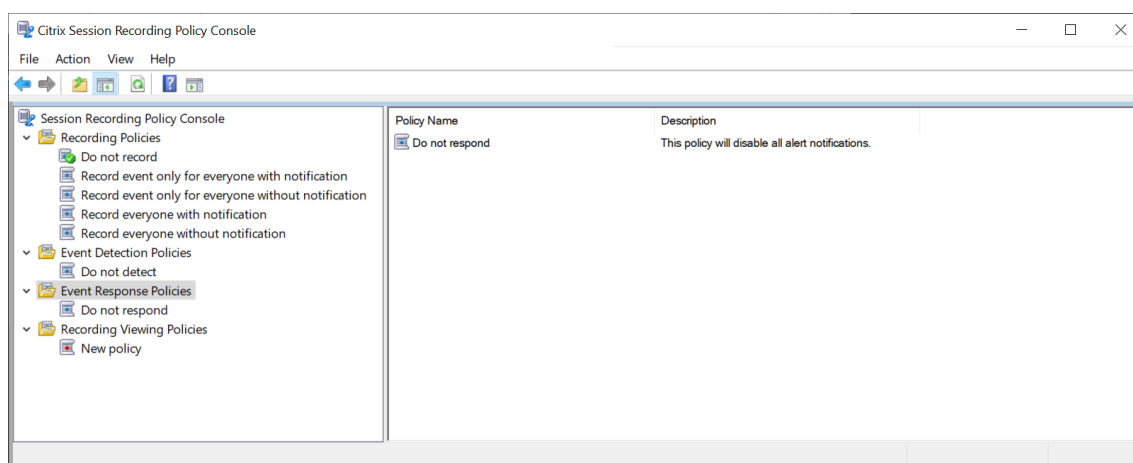
Stratégie de réponse aux événements définie par le système

Enregistrement de session fournit une stratégie de réponse aux événements définie par le système :

- **Ne pas répondre**. Par défaut, aucune action n'est prise en réponse aux événements consignés dans vos enregistrements.

Créer une stratégie de réponse personnalisée aux événements

1. Ouvrez une session en tant qu'administrateur de stratégie autorisé sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Démarrez la console de stratégie d'enregistrement de session. Par défaut, il n'existe pas de stratégie de réponse aux événements active.



3. Sélectionnez **Stratégies de réponse aux événements** dans le volet gauche. Dans la barre de menu, choisissez **Ajouter une nouvelle stratégie**.
4. (Facultatif) Cliquez avec le bouton droit de la souris sur la nouvelle stratégie de réponse aux événements et renommez-la.
5. Cliquez avec le bouton droit sur la nouvelle stratégie de réponse aux événements et sélectionnez **Ajouter une règle**.
6. Sélectionnez **Envoyer alerte par e-mail lorsqu'un démarrage de session est détecté** et **Utiliser des déclencheurs d'événements pour spécifier comment réagir lorsqu'un événement de session est détecté** en fonction de vos besoins.

Rules Wizard

Step 1-1: Select one or more of the following options.

- Email alert when a session start is detected.
- Trigger response actions when a session event is detected

Configure event triggers and responses

Step 1-2: Enter email addresses for the alert recipients and set time spans for dynamic screen recording.

Email recipients:
Type the email addresses who will receive alerts according to this rule. Separate the addresses with a semicolon (;).

Screen recording time span after we detect an event:
How many minutes do you want us to record the screen after we detect an event?

Screen recording time span before we detect an event (available only for virtual desktop sessions):
How many seconds of the screen recording do you want us to keep before we detect an event?

Time interval between a session operation notice and its execution (available for session lock, log off, and disconnection)
How many seconds do you want us to hold a session operation after we issue the notice?

< Back Next > Cancel

7. (Facultatif) Définissez les destinataires des e-mails et les propriétés de l'expéditeur.
 - a) Saisissez les adresses e-mail des destinataires des alertes dans l'assistant **Règles**.
 - b) Configurez les paramètres de messagerie sortante dans **Propriétés du serveur d'enregistrement de session**.

Session Recording Server Properties

Rollover Playback Notifications CEIP Logging RBAC Email

SMTP server: smtp.office365.com

Port: 587 Enable SSL

Display name: Citrix Session Recording

Email address: srt-no-reply@outlook.com

Password:

Email title

- User name
- Domain name
- Start time
- Delivery group
- Application
- VDA Machine

Email body

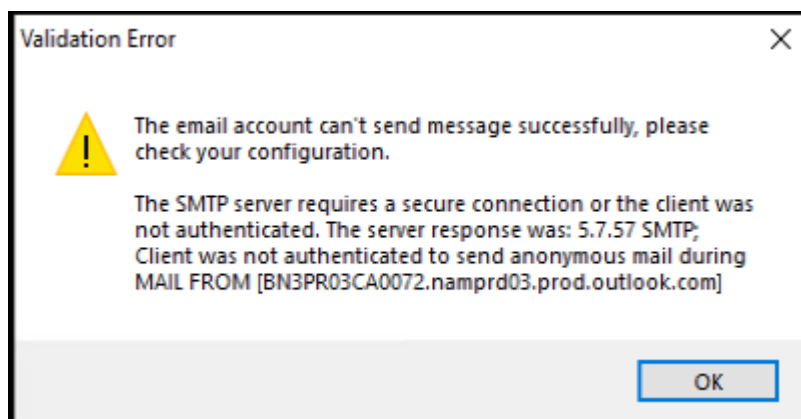
- User name
- Domain name
- Start time
- Delivery group
- Application
- VDA Machine
- Recording URL

Allow sending email notifications

OK Cancel Apply

Remarque :

si vous sélectionnez plus de deux options dans la section **Titre de l'e-mail**, une boîte de dialogue vous avertit que l'objet de l'e-mail peut être trop long. Une fois que vous avez sélectionné **Autoriser l'envoi de notifications par e-mail** et cliqué sur **Appliquer**, Enregistrement de session envoie un e-mail pour vérifier vos paramètres de messagerie. Si un paramètre est incorrect, par exemple un mot de passe ou un port incorrect, Enregistrement de session renvoie un message d'erreur avec les détails de l'erreur.



Vos paramètres de messagerie mettent environ cinq minutes à être appliqués. Pour que vos paramètres de messagerie prennent effet immédiatement ou pour résoudre le problème d'e-mails qui ne sont pas envoyés conformément aux paramètres, redémarrez le service Gestionnaire de stockage (*CitrixSsRecStorageManager*). Vous devez également redémarrer le service Gestionnaire de stockage si vous effectuez une mise à niveau vers la version actuelle à partir de la version 2006 et antérieure.

c) Modifiez le registre pour accéder au lecteur Web.

Pour que les URL de lecture de vos e-mails d'alerte fonctionnent comme prévu, accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` et procédez comme suit :

- Définissez les données de valeur de **LinkHost** sur l'URL du domaine que vous utilisez pour accéder au lecteur Web. Par exemple, pour accéder à un lecteur Web sur `https://example.com/webplayer/#/player/`, définissez les données de valeur de **LinkHost** sur `https://example.com`.
- Ajoutez une valeur, **EmailThreshold**, et définissez ses données sur un nombre compris entre 1 et 100. Les données de valeur déterminent le nombre maximal d'e-mails d'alerte qu'un compte d'envoi d'e-mails envoie en une seconde. Ce paramètre permet de ralentir le nombre d'e-mails envoyés et donc de réduire l'utilisation de l'UC. Si vous ne spécifiez pas de données de valeur ou si vous les définissez sur un nombre hors plage, les données de valeur sont ramenées à 25.

Remarque :

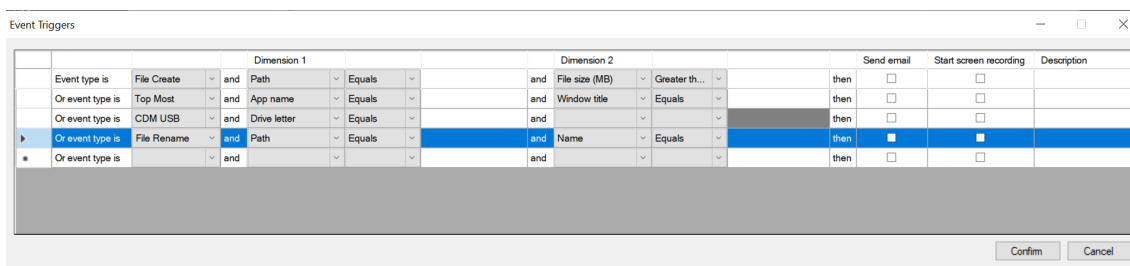
- Votre serveur de messagerie peut traiter un compte d'envoi d'e-mails comme bot de spam et l'empêcher d'envoyer des e-mails. Avant qu'un compte ne soit autorisé à envoyer des e-mails, un client de messagerie tel qu'Outlook peut vous demander de vérifier que le compte est utilisé par un utilisateur humain.

- Il y a une limite pour l'envoi d'e-mails dans un délai donné. Par exemple, lorsque la limite journalière est atteinte, vous ne pouvez pas envoyer d'e-mails avant le début de la journée suivante. Dans ce cas, assurez-vous que la limite est supérieure au nombre de sessions enregistrées au cours de la période.

8. (Facultatif) Configurez les déclencheurs d'événements et les réponses.

Une fois que vous avez sélectionné **Déclencher des actions de réponse lorsqu'un événement de session est détecté**, le bouton **Configurer déclencheurs et réponses aux événements** devient disponible. Cliquez dessus pour spécifier les événements consignés susceptibles de déclencher les actions de réponse suivantes :

- Envoyer des alertes par e-mail
- Lancer immédiatement l'enregistrement d'écran
- Verrouiller la session
- Fermer la session
- Déconnecter la session



Remarque :

Si la langue de votre système est l'allemand, le français ou l'espagnol, assurez-vous que la résolution horizontale de votre machine est égale ou supérieure à 1 700 pixels. Dans le cas contraire, le texte est tronqué et les colonnes du tableau **Déclencheurs d'événements** ne sont pas complètement affichées.

Vous devez sélectionner les types d'événements que la stratégie de détection d'événements active consigne. Cliquez sur **Confirmer** lorsque vous avez terminé.

Sélectionnez les types d'événements dans la liste déroulante et définissez des règles d'événement selon les deux dimensions pouvant être combinées à l'aide de l'opérateur AND logique. Vous pouvez configurer jusqu'à sept déclencheurs d'événements pour chaque règle de stratégie. Vous pouvez également définir vos déclencheurs d'événements dans la colonne **Description** ou laisser la colonne vide. La description définie d'un déclencheur d'événement est fournie dans les e-mails d'alerte si vous avez sélectionné **Envoyer un e-mail** et si les événements de ce type sont journalisés. Si **Démarrer enregistrement d'écran** est sélectionné, l'enregistrement dynamique de l'écran démarre automatiquement lorsque certains évé-

ments se produisent pendant un enregistrement d'événement uniquement. Définissez les durées d'enregistrement d'écran dynamique.

- **Durée d'enregistrement d'écran après la détection d'un événement de session** : vous pouvez configurer le nombre de minutes pendant lesquelles vous souhaitez enregistrer l'écran après la détection d'événements. Si vous ne spécifiez pas la durée, l'enregistrement d'écran se poursuit jusqu'à la fin de la session enregistrée.
- **Durée d'enregistrement d'écran avant la détection d'un événement de session** : vous pouvez configurer le nombre de secondes de l'enregistrement d'écran que vous souhaitez conserver avant la détection des événements. Cette fonctionnalité n'est disponible que pour les sessions de bureau virtuel. La valeur est comprise entre 1 et 120. Si vous définissez la valeur entre 1 et 10, la valeur 10 est effective. Si vous ne spécifiez pas la valeur, la fonction n'est pas appliquée. La durée réelle de l'enregistrement d'écran conservé par l'enregistrement de session peut être un peu plus longue que votre configuration.

The screenshot shows the 'Rules Wizard' dialog box with two steps. Step 1-1 offers two options: 'Email alert when a session start is detected.' and 'Use event triggers to specify how to respond when a session event is detected.' A 'Configure event triggers (0)' button is below. Step 1-2 is for email recipients and time spans. It includes a text field for email addresses, a field for 'Screen recording time span after we detect an event' (in minutes), and a field for 'Screen recording time span before we detect an event' (in seconds, available only for virtual desktop sessions). Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

Pour obtenir la liste complète des types d'événements pris en charge, reportez-vous au tableau suivant.

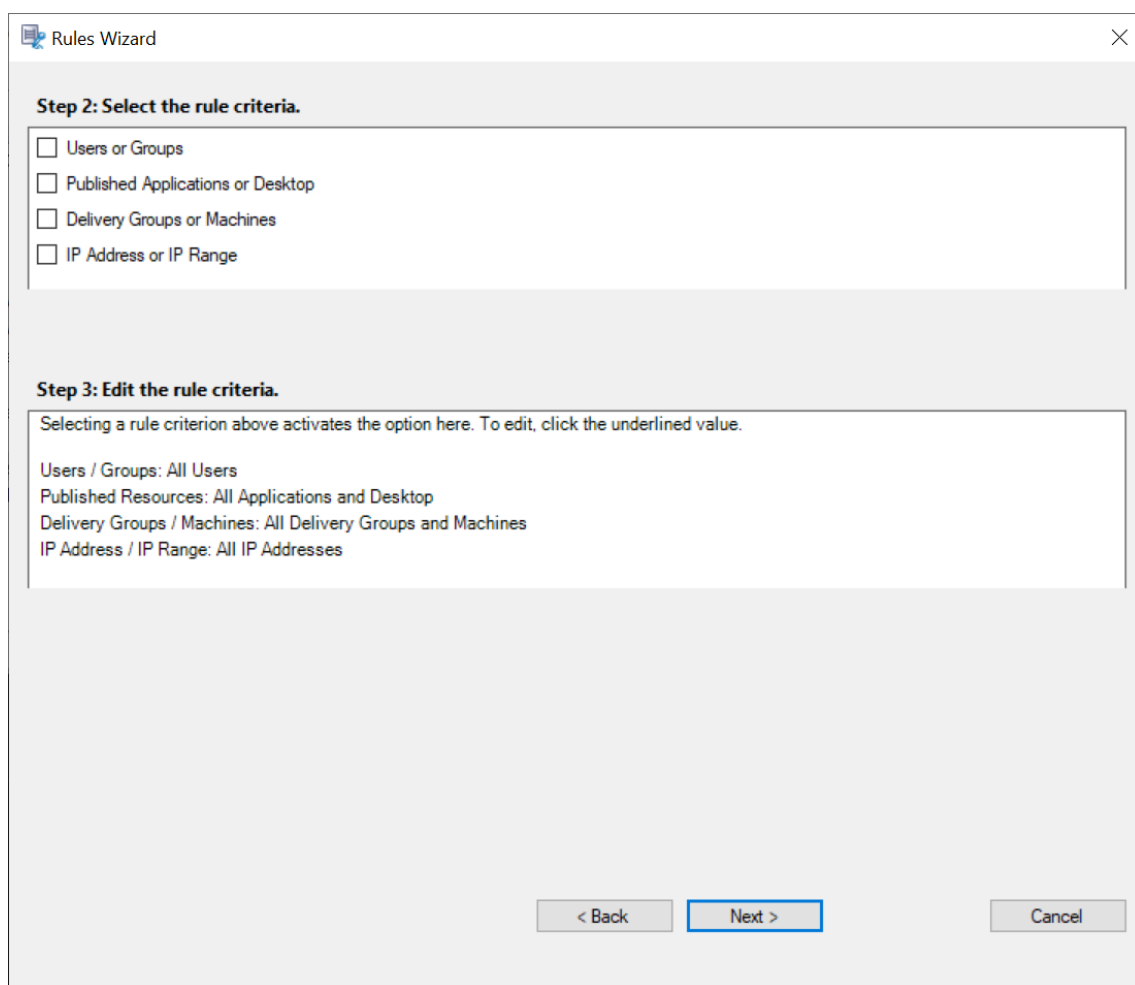
Type d'événement	Dimension	Option
Démarrage de l'application		Nom de l'application Ligne de commande complète
Fin de l'application		Nom de l'application
Principaux		Nom de l'application Titre de la fenêtre
Navigation sur le Web		URL Titre de l'onglet Nom du navigateur
Création de fichier		Path Taille du fichier (Mo)
Changement de nom du fichier		Path Nom
Déplacement de fichier		Chemin d'accès source Chemin de destination Taille du fichier (Mo)
Suppression de fichier		Path Taille du fichier (Mo)
USB CDM		Lettre de lecteur
USB générique		Nom de l'appareil

Type d'événement	Dimension	Option
Inactif		Durée d'inactivité (heures)
Transfert de fichiers		Source du fichier Taille du fichier (Mo) Nom du fichier
Créer registre		Nom de la clé
Supprimer registre		Nom de la clé
Définir valeur du registre		Nom de la clé Nom de la valeur
Supprimer valeur du registre		Nom de la clé Nom de la valeur
Renommer registre		Nom de la clé
Modification du compte utilisateur		Nom d'utilisateur
Fermeture inattendue de l'application		Nom de l'application
L'application ne répond pas		Nom de l'application
Nouvelle application installée		Nom de l'application
Application désinstallée		Nom de l'application

Type d'événement	Dimension	Option
Connexion RDP		Adresse IP
Fenêtre contextuelle		Nom du processus Contenu de la fenêtre
Données de performances		Utilisation UC (%) Utilisation de mémoire (%) Envoi réseau (Mo) Réception réseau (Mo) RTT (ms)
Opération du presse-papiers		Type de données Nom du processus Contenu

9. Cliquez sur **Suivant** pour sélectionner et modifier les critères de règle.

De la même façon que vous avez créé une stratégie d'enregistrement personnalisée, sélectionnez un ou plusieurs critères de règle : **Utilisateurs ou Groupes, Applications ou bureaux publiés, Groupes de mise à disposition ou Machines et Adresse IP ou Plage d'adresses IP.** Pour plus d'informations, consultez les instructions de la section [Créer une stratégie d'enregistrement personnalisée](#).



Remarque :

Lorsqu’une session ou un événement rencontre plusieurs règles dans une seule stratégie de réponse aux événements, la règle la plus ancienne prend effet.

10. Suivez les instructions de l’assistant pour terminer l’installation.
11. Activez la nouvelle stratégie de réponse aux événements.

Haute disponibilité et équilibrage de charge

December 21, 2022

Cette section décrit les paramètres suivants :

- [Équilibrer la charge des serveurs d’enregistrement de session](#)
- [Configurer la haute disponibilité de base de données](#)

Équilibrer la charge des serveurs d'enregistrement de session

December 23, 2022

L'enregistrement de session prend en charge l'**équilibrage de charge** entre les serveurs d'enregistrement de session. Cet article résume la configuration d'**équilibrage de charge** en utilisant Citrix ADC comme exemple. Pour de plus amples informations, consultez la section [Configurer l'équilibrage de charge dans un déploiement existant](#) et [Déployer et équilibrer la charge de l'enregistrement de session sur Azure](#).

Vous pouvez synchroniser les configurations d'**équilibrage de charge** entre tous les serveurs d'enregistrement de session.

Remarque :

Cette fonctionnalité d'**équilibrage de charge** nécessite la version 7.16 ou ultérieure du serveur d'enregistrement de session et de l'agent d'enregistrement de session.

Modifications apportées à l'enregistrement de session pour prendre en charge l'équilibrage de charge :

- Tous les serveurs d'enregistrement de session partagent un dossier pour stocker les fichiers d'enregistrement.
- Tous les serveurs d'enregistrement de session partagent une base de données d'enregistrement de session.
- (Recommandé) Installez une seule console de stratégie d'enregistrement de session et tous les serveurs d'enregistrement de session partagent cette console.

Configurer l'équilibrage de charge

Pour utiliser cette fonctionnalité, effectuez les étapes suivantes sur Citrix ADC et sur les différents composants de l'enregistrement de session :

Configurer l'équilibrage de charge (dans Citrix ADC)

Configurer les serveurs d'équilibrage de charge Ajoutez les serveurs d'enregistrement de session aux **serveurs d'équilibrage de charge** dans Citrix ADC.

Configurer les services d'équilibrage de charge

1. Ajoutez un **service d'équilibrage de charge** pour chaque protocole nécessaire sur chaque serveur d'enregistrement de session.
2. (Recommandé) Sélectionnez le protocole de surveillance approprié pour lier chaque service de surveillance.

Configurer les serveurs virtuels d'équilibrage de charge

1. Créez des serveurs virtuels avec la même adresse VIP Citrix ADC selon les protocoles nécessaires et liez les serveurs virtuels avec les **services d'équilibrage de charge** appropriés.
2. Configurez la persistance sur chaque serveur virtuel.
3. (Recommandé) Choisissez LEASTBANDWIDTH ou LEASTPACKETS en tant que **méthode d'équilibrage de charge** plutôt que la méthode par défaut (LEASTCONNECTION).
4. Créez un certificat pour activer le serveur virtuel HTTPS.

Configurer l'équilibrage de charge (dans l'enregistrement de session)

Sur chaque serveur sur lequel vous avez installé le serveur d'enregistrement de session, procédez comme suit

1. (Recommandé) Entrez le même nom de base de données d'enregistrement de session que pendant l'installation du serveur d'enregistrement de session.
2. Si vous choisissez la fonctionnalité de journalisation de l'administrateur, nous vous recommandons d'entrer le même nom de base de données de journalisation de l'administrateur lorsque vous installez chaque serveur d'enregistrement de session.
3. Accordez l'autorisation de lecture/écriture du dossier de stockage de fichiers à tous les comptes de machine du serveur d'enregistrement de session. Modifiez ensuite les paramètres pour utiliser le dossier de stockage de fichiers en tant que dossier partagé dans **Propriétés du serveur d'enregistrement de session**. Pour plus d'informations, consultez la section [Spécifier l'endroit où les enregistrements sont restaurés](#).
4. Ajoutez une valeur à la clé de registre du serveur d'enregistrement de session se trouvant sous `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.
Nom de la valeur : **EnableLB**
Données de la valeur : **1** (DWORD, signifie activer)
5. Si vous choisissez le protocole HTTP ou HTTPS pour la file d'attente des messages du gestionnaire de stockage d'enregistrement de session, créez un enregistrement d'hôte pour l'adresse VIP Citrix ADC, ajoutez les redirections dans `C:\Windows\System32\msmq\Mapping\sample_map`. Redémarrez ensuite le service Message Queuing.

La redirection est similaire à ceci :

```

1 <redirections xmlns="msmq-queue-redirections.xml">
2   <redirection>
3     <from>http://<ADCHost>*/msmq/private$/
      CitrixSmAudData</from>
4     <to>http://<LocalFqdn>/msmq/private$/
      CitrixSmAudData</to>
5   </redirection>
6   <redirection>
7     <from>https://<ADCHost>*/msmq/private$/
      CitrixSmAudData</from>
8     <to>https://<LocalFqdn>/msmq/private$/
      CitrixSmAudData</to>
9   </redirection>
10 </redirections>
11 <!--NeedCopy-->

```

Où **<ADCHost>** est le nom de domaine complet créé depuis l'adresse VIP Citrix ADC, et **<LocalFqdn>** le nom de domaine complet de l'hôte local.

6. (Recommandé) Après avoir configuré un registre de serveur d'enregistrement de session, vous pouvez utiliser le script **<chemin d'installation du serveur d'enregistrement de session>\Scripts\SrServerConfigurationSync.ps1** pour exporter les configurations de ce registre de serveur et importer le registre dans les autres registres du serveur d'enregistrement de session. Vous pouvez également utiliser le script **SrServerConfigurationSync.ps1** pour ajouter un mappage de redirection pour la mise en file d'attente des messages.
 - a) Sur un serveur d'enregistrement de session, après avoir configuré la valeur de registre **EnableLB**, démarrez une invite de commande en tant qu'administrateur et exécutez la commande **powershell.exe -file SrServerConfigurationSync.ps1 -Action Export,AddRedirection -ADCHost <ADCHost>**, où **<ADCHost>** est le nom de domaine complet créé de l'adresse VIP Citrix ADC.
 - b) Après l'exécution du script, un fichier de registre exporté nommé **SrServerConfig.reg** est généré et un fichier **sr_lb_map.xml** est ajouté au chemin **C:\Windows\System32\msmq\Mapping**.
 - c) Sur d'autres serveurs d'enregistrement de session, copiez le fichier généré **SrServerConfig.reg** dans l'étape qui précède, démarrez une invite de commande en tant qu'administrateur et exécutez la commande **powershell.exe -file SrServerConfigurationSync.ps1 -Action Import,AddRedirection -ADCHost <ADCHost>**, où **<ADCHost>** est le nom de domaine complet créé de l'adresse VIP Citrix ADC.
 - d) Une fois le script exécuté, la valeur **EnableLB** est ajoutée aux autres clés de registre du serveur d'enregistrement de session et un fichier **sr_lb_map.xml** est ajouté au chemin **C:\Windows\System32\msmq\Mapping**.

Sur la machine sur laquelle vous avez installé l'agent d'enregistrement de session, effectuez ce qui suit dans les propriétés de l'agent d'enregistrement de session

- Si vous choisissez le protocole HTTP ou HTTPS pour la file d'attente de messages du gestionnaire de stockage d'enregistrement de session, entrez le nom de domaine complet de l'adresse VIP Citrix ADC dans la zone de texte **Serveur d'enregistrement de session**.
- Si vous choisissez le protocole TCP par défaut pour la file d'attente de messages du gestionnaire de stockage d'enregistrement de session, entrez l'adresse VIP Citrix ADC dans la zone de texte **Serveur d'enregistrement de session**.

Sur la machine sur laquelle vous avez installé le lecteur d'enregistrement de session, effectuez ce qui suit Ajoutez l'adresse VIP Citrix ADC ou son nom de domaine complet comme serveur d'enregistrement de session connecté.

Sur le serveur SQL Server sur lequel vous avez installé la base de données d'enregistrement de session, effectuez ce qui suit Ajoutez tous les comptes de machines de serveur d'enregistrement de session à la base de données d'enregistrement de session partagée et attribuez-leur l'autorisation **db_owner**.

Configurer la haute disponibilité de base de données

December 21, 2022

L'enregistrement de session prend en charge les solutions suivantes pour la haute disponibilité de base de données basée sur Microsoft SQL Server. Les bases de données peuvent basculer automatiquement lorsque le matériel ou le logiciel d'un serveur SQL Server principal échoue.

- Groupes de disponibilité AlwaysOn

La fonctionnalité Groupes de disponibilité AlwaysOn est une solution de haute disponibilité et de récupération d'urgence qui offre une alternative pour la mise en miroir de base de données. Elle optimise la disponibilité d'un ensemble de bases de données utilisateur pour une entreprise. Elle nécessite que les instances SQL Server résident les nœuds WSFC (Windows Server Failover Clustering). Pour de plus amples informations, consultez la section [Groupes de disponibilité AlwaysOn : une solution de haute disponibilité et de récupération d'urgence](#).

- Mise en cluster SQL Server

La technologie de mise en cluster SQL de Microsoft permet à un serveur d'assurer automatiquement la reprise des tâches et des responsabilités du serveur en échec. Toutefois, cette solution est complexe à mettre en place et le basculement automatique est généralement plus lent qu'

avec les autres méthodes, comme la mise en miroir de la base de données SQL Server. Pour de plus amples informations, consultez la section [Instances de cluster de basculement AlwaysOn \(SQL Server\)](#).

- Mise en miroir de base de données SQL Server

La mise en miroir de base de données garantit qu'un basculement automatique se produit en quelques secondes si le serveur de base de données actif échoue. Cette solution est plus coûteuse que les deux autres solutions car des licences complètes de SQL Server sont requises sur chaque serveur de base de données. Vous ne pouvez pas utiliser l'édition SQL Server Express dans un environnement de mise en miroir. Pour de plus amples informations, consultez la section [Mise en miroir de bases de données \(SQL Server\)](#).

Méthodes de configuration de l'enregistrement de session avec une haute disponibilité de base de données

Pour configurer l'enregistrement de session avec une haute disponibilité de base de données, suivez l'une des procédures suivantes :

- Commencez par installer les composants du serveur d'enregistrement de session, puis configurez une haute disponibilité de base de données pour les bases de données créées. Vous pouvez installer les composants d'administration d'enregistrement de session avec les bases de données configurées pour être installées sur l'instance de SQL Server préparée. Configurez ensuite une haute disponibilité de base de données pour les bases de données créées.
 - Pour les groupes de disponibilité AlwaysOn et la mise en cluster, définissez le nom de l'instance SQL Server sur le nom de l'écouteur du groupe de disponibilité ou du réseau SQL Server dans `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance`.
 - Pour la mise en miroir de base de données, vous devez ajouter les partenaires de basculement pour les bases de données dans `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner` et `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner`.
- Commencez par configurer une haute disponibilité de base de données pour des bases de données vides, puis installez les composants d'administration d'enregistrement de session. Vous pouvez créer deux bases de données vides en tant que base de données d'enregistrement de session et base de données de journalisation de l'administrateur dans l'instance de SQL Server principale attendue et configurer la haute disponibilité. Entrez le nom de l'instance SQL Server lors de l'installation des composants du serveur d'enregistrement de session :

- Pour utiliser la solution Groupes de disponibilité AlwaysOn, entrez le nom de votre écouteur de groupe de disponibilité.
- Pour utiliser la solution de mise en miroir de base de données, entrez le nom de votre SQL Server principal.
- Pour utiliser la solution de mise en cluster, entrez le nom du réseau de votre SQL Server.

Afficher les enregistrements

December 21, 2022

Utilisez le lecteur d'enregistrement de session ou le lecteur Web d'enregistrement de session pour afficher, rechercher et créer des signets pour les sessions enregistrées.

Si les sessions sont enregistrées avec la fonctionnalité de lecture active, vous pouvez afficher les sessions en cours, avec un délai de quelques secondes.

Les sessions dont la durée ou la taille de fichier sont supérieures aux limites configurées apparaissent dans plusieurs fichiers de session.

Remarque :

Accordez aux utilisateurs le droit d'accéder aux sessions enregistrées des VDA.

Lecteur d'enregistrement de session

December 23, 2022

Le lecteur d'enregistrement de session est une interface utilisateur à laquelle vous accédez depuis une station de travail pour lire des fichiers de session enregistrées. Cette section fournit des instructions pour effectuer les opérations suivantes :

- [Lancer le lecteur d'enregistrement de session](#)
- [Activer ou désactiver la lecture de session active](#)
- [Activer ou désactiver la protection de lecture](#)
- [Rechercher des enregistrements](#)
- [Ouvrir et lire des enregistrements](#)
- [Enregistrements en cache](#)
- [Afficher les périodes d'inactivité](#)
- [Utiliser des événements et des signets](#)

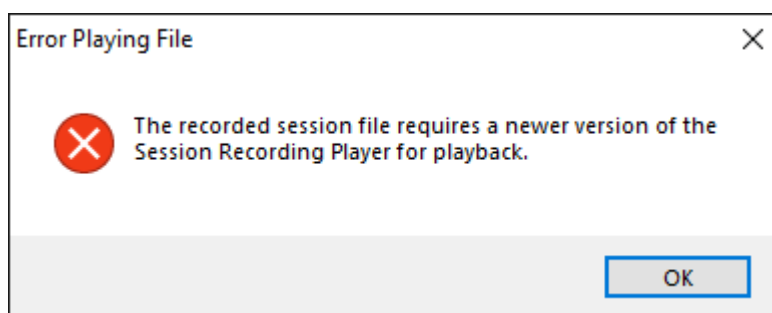
Lancer le lecteur d'enregistrement de session

February 20, 2024

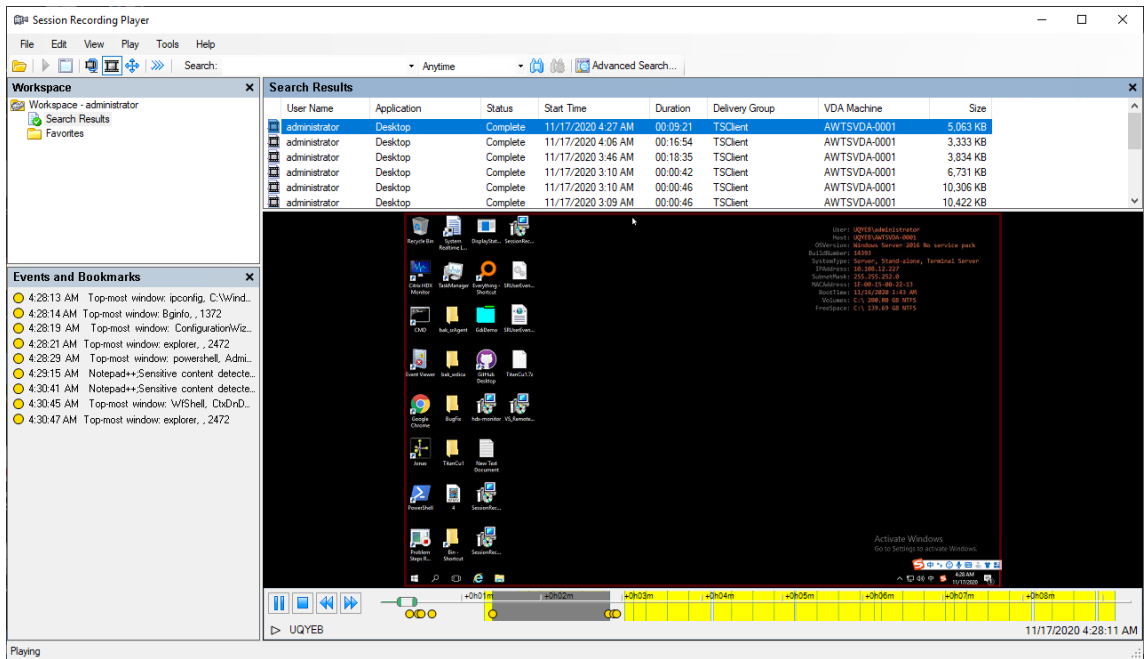
Lancer le lecteur d'enregistrement de session

Remarque :

- Si un enregistrement contient du contenu bloqué, l'enregistrement de session l'ignore. Toutefois, si vous accédez à la période bloquée, votre lecture affiche un écran noir et un message indiquant que ce contenu est bloqué. Pour utiliser cette fonctionnalité, utilisez Enregistrement de session 2012 et versions ultérieures.
- Si vous utilisez le Lecteur d'enregistrement de session 2009 et versions antérieures pour lire un enregistrement, le message d'erreur suivant s'affiche. Le lecteur Web n'est pas affecté.

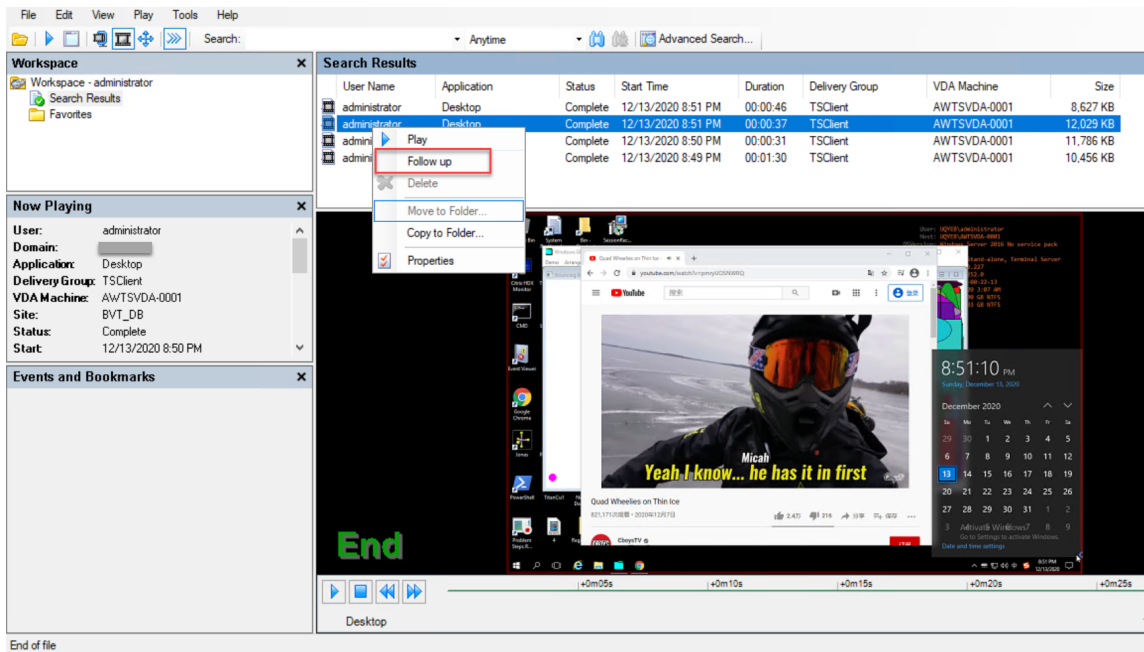


1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**. Le lecteur d'enregistrement de session s'affiche.



Conseil : la colonne **Événement uniquement** indique un enregistrement d'écran ou un enregistrement d'événement uniquement.

Pour afficher tous les fichiers d'enregistrement d'une session enregistrée, cliquez avec le bouton droit de la souris sur un enregistrement dans la liste et choisissez **Suivi**.



Afficher ou masquer les éléments de fenêtre

Le lecteur d'enregistrement de session possède des éléments de fenêtre que vous activez et désactivez.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Affichage**.
4. Choisissez les éléments que vous souhaitez afficher. La sélection d'un élément entraîne l'affichage immédiat. Un élément sélectionné est indiqué par la case correspondante cochée.

Se connecter au serveur d'enregistrement de session souhaité

Vous pouvez configurer votre lecteur d'enregistrement de session pour qu'il se connecte à plusieurs serveurs d'enregistrement de session, puis sélectionner un serveur d'enregistrement de session auquel il se connecte. Le lecteur d'enregistrement de session ne peut se connecter qu'à un seul serveur d'enregistrement de session à la fois.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du lecteur d'enregistrement de session**, choisissez ****Outils > Options > Connexions**.
4. Sélectionnez le serveur d'enregistrement de session auquel vous connecter.

Activer ou désactiver la lecture de session active

December 21, 2022

Si les sessions sont enregistrées avec la fonction de lecture active activée, vous pouvez voir une session après ou pendant son enregistrement. L'affichage d'une session en cours d'enregistrement est similaire à la visualisation d'actions se déroulant en direct. Toutefois, il existe un délai de 1-2 secondes lorsque les données se propagent à partir du VDA.

Certaines fonctionnalités ne sont pas disponibles lorsque vous affichez des sessions de lecture actives :

- Vous ne pouvez pas attribuer de signature numérique ni consulter le certificat tant que l'enregistrement n'est pas terminé.

- La protection en lecture ne peut pas s'appliquer tant que l'enregistrement n'est pas terminé. Si la protection de lecture est activée, vous pouvez afficher les sessions de lecture actives. Cependant, elles ne sont pas cryptées tant que la session n'est pas terminée.
- Vous ne pouvez pas mettre en cache un fichier tant que l'enregistrement n'est pas terminé.

Par défaut, la lecture de session active est activée.

1. Ouvrez une session sur l'ordinateur exécutant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du serveur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Lecture**.
4. Cochez ou désélectionnez la case **Autoriser la lecture d'une session active**.

Activer ou désactiver la protection de lecture

December 21, 2022

Par mesure de sécurité, l'enregistrement de session crypte automatiquement les fichiers enregistrés qui sont téléchargés pour être affichés dans le lecteur. Les fichiers cryptés ne peuvent pas être copiés ou lus sur une autre station de travail ou par un autre utilisateur. Les fichiers cryptés sont identifiés par une extension `.icle`. Les fichiers non cryptés sont identifiés par une extension `.icl`. Les fichiers demeurent cryptés tant qu'ils résident dans `%localAppData%\Citrix\SessionRecording\Player\Cache` sur le lecteur et ce jusqu'à ce qu'ils soient ouverts par un utilisateur autorisé.

Nous vous recommandons d'utiliser HTTPS pour protéger le transfert de données.

Par défaut, la protection de lecture est désactivée.

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. À partir du menu **Démarrer**, choisissez **Propriétés du lecteur d'enregistrement de session**.
3. Dans la fenêtre **Propriétés du serveur d'enregistrement de session**, cliquez sur l'onglet **Lecture**.
4. Cochez ou désélectionnez la case **Crypter les fichiers d'enregistrement de session téléchargés pour les lire**.

Rechercher des enregistrements

December 21, 2022

Le lecteur d'enregistrement de session vous permet d'effectuer des recherches rapides et avancées et de spécifier des options s'appliquant à toutes les recherches. Le résultat des recherches s'affiche dans la zone Résultats de la recherche du lecteur d'enregistrement de session.

Remarque :

L'installation du lecteur vous permet généralement de configurer une connexion entre le lecteur d'enregistrement de session et un serveur d'enregistrement de session. Si vous ne parvenez pas à établir la connexion, vous êtes invité à le faire la première fois que vous effectuez une recherche de fichiers.

Pour afficher toutes les sessions enregistrées disponibles, jusqu'au nombre maximum de sessions pouvant s'afficher dans une recherche, effectuez une recherche sans spécifier de paramètre de recherche précis.

Effectuer une recherche rapide

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Définissez vos critères de recherche :
 - Entrez un critère de recherche dans le champ **Rechercher**.
 - Faites glisser le pointeur de la souris sur l'étiquette **Rechercher** pour afficher une liste de paramètres à utiliser à titre indicatif.
 - Cliquez sur la flèche à droite du champ **Rechercher** pour afficher le texte des 64 dernières recherches que vous avez effectuées.
 - Utilisez la liste déroulante située à droite du champ **Rechercher** pour sélectionner une période ou une durée pour l'enregistrement de la session.
4. Cliquez sur l'icône binoculaire à droite de la liste déroulante pour lancer la recherche.

Effectuer une recherche avancée

Les recherches avancées peuvent prendre jusqu'à 20 secondes pour renvoyer des résultats contenant plus de 150 000 entités. Citrix vous recommande d'utiliser des critères de recherche plus précis comme une plage de dates ou un utilisateur afin de réduire le nombre de résultats.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.

3. Dans la fenêtre **Lecteur d'enregistrement de session**, cliquez sur **Recherche avancée** dans la barre d'outils ou choisissez **Outils > Recherche avancée**.
4. Définissez vos critères de recherche dans les onglets de la boîte de dialogue **Recherche avancée** :
 - **Commun** vous permet de faire une recherche par domaine ou autorité de compte, par site, groupe, VDA pour OS multi-session, application ou identificateur de fichier.
 - **Date/Heure** vous permet de faire une recherche en fonction de la date, du jour de la semaine et de l'heure.
 - **Événements** vous permet de rechercher des événements définis par Citrix et personnalisés qui sont insérés dans les sessions.
 - **Autre** vous permet de faire une recherche par nom de session, nom de client, adresse de client et durée d'enregistrement. Cet onglet vous permet aussi de spécifier, pour cette recherche, le nombre maximum de résultats affichés et d'inclure ou non les fichiers archivés.

À mesure que vous précisez les critères de recherche, la requête que vous créez s'affiche dans le volet situé au bas de la boîte de dialogue.
5. Cliquez sur **Recherche** pour lancer la recherche.

vous pouvez enregistrer et récupérer les requêtes de recherche avancée. Cliquez sur **Enregistrer** dans la boîte de dialogue **Recherche avancée** pour enregistrer la requête actuelle. Cliquez sur **Ouvrir** dans la boîte de dialogue **Recherche avancée** pour extraire une requête enregistrée. Les requêtes sont enregistrées sous forme de fichiers avec l'extension `.isq`.

Paramétrer les options de recherche

Les options de recherche du lecteur d'enregistrement de session vous permettent de limiter le nombre maximum d'enregistrements de sessions qui s'affichent dans les résultats de la recherche et de spécifier si ces résultats peuvent inclure les fichiers de sessions archivés.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Outils > Options > Recherche**.
4. Dans le champ **Nombre maximum de résultats à afficher**, tapez le nombre de résultats de recherche que vous souhaitez afficher. Un maximum de 500 résultats peuvent être affichés.
5. Pour définir si les fichiers archivés doivent ou non être inclus dans les recherches, sélectionnez ou désélectionnez **Inclure les fichiers archivés**.

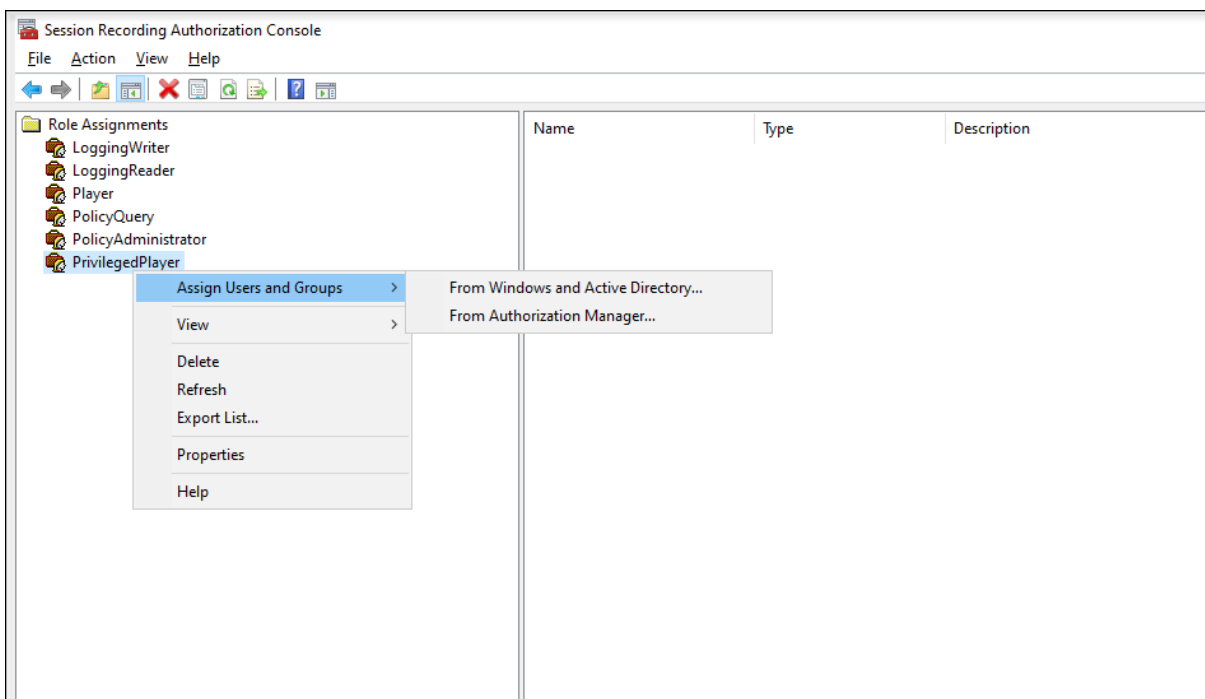
Imposer des restrictions d'accès aux enregistrements

February 20, 2024

Vous imposez des restrictions d'accès aux enregistrements cibles en plus du contrôle d'accès basé sur les rôles par le biais de [stratégies de visionnage d'enregistrement](#). Les enregistrements restreints ne sont accessibles qu'aux utilisateurs et aux groupes d'utilisateurs auxquels le rôle **PrivilegedPlayer** est attribué via la console d'autorisation d'enregistrement de session.

Remarque :

Il n'est pas possible d'imposer des restrictions d'accès aux enregistrements en direct.

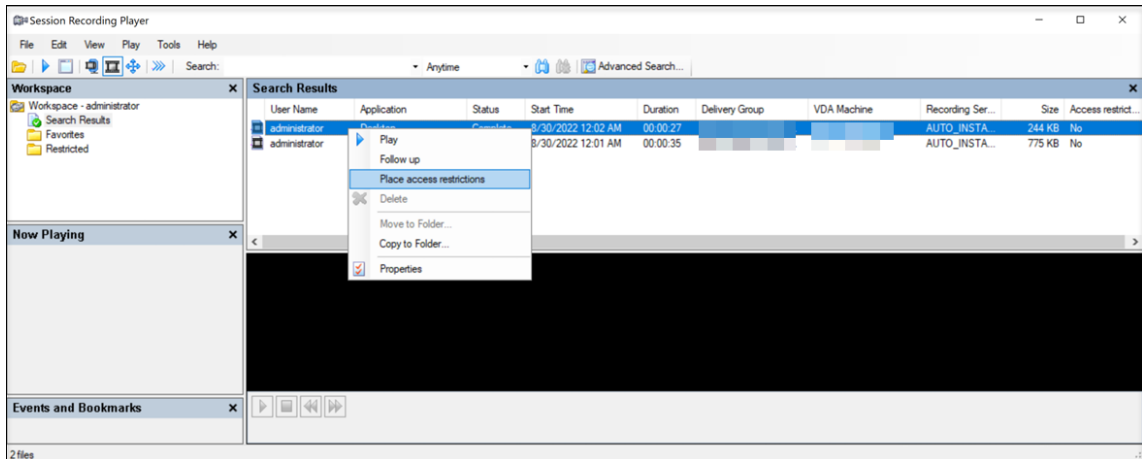


La section suivante vous explique comment placer et supprimer des restrictions d'accès sur les enregistrements cibles.

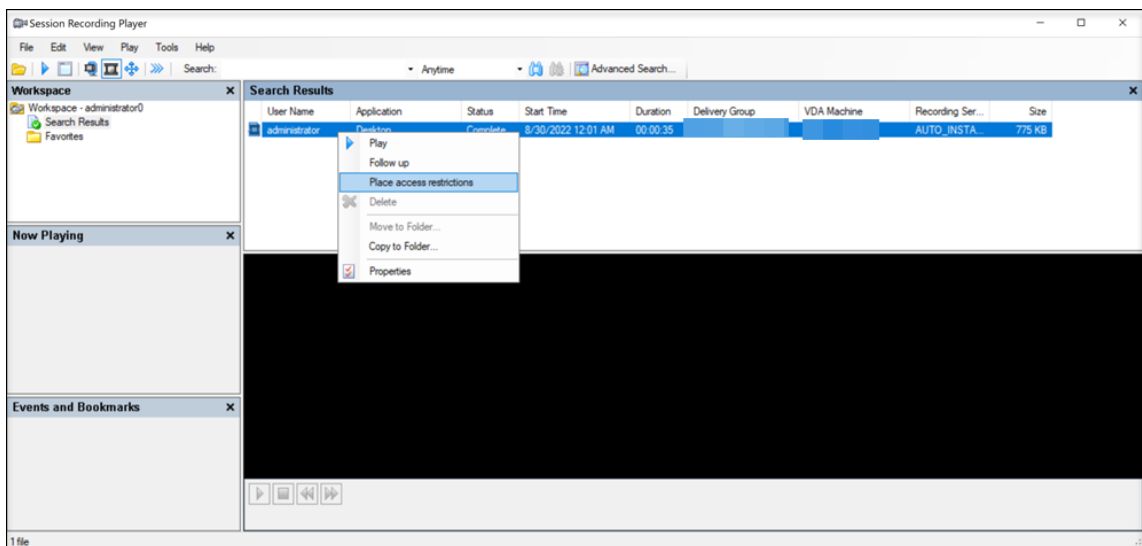
1. Ouvrez une session sur la machine sur laquelle le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Sélectionnez **Résultats de recherche** dans le volet **Espace de travail**.
4. Dans la zone **Résultats de recherche**, sélectionnez un ou plusieurs enregistrements cibles.
5. Cliquez avec le bouton droit et sélectionnez **Imposer restrictions d'accès**.

Les utilisateurs et les groupes d'utilisateurs auxquels est attribué le rôle **Player** ou **Privileged-Player** sont autorisés à imposer des restrictions d'accès aux enregistrements. Le menu **Restraint** n'est disponible que pour les utilisateurs et les groupes d'utilisateurs auxquels le rôle **PrivilegedPlayer** a été attribué.

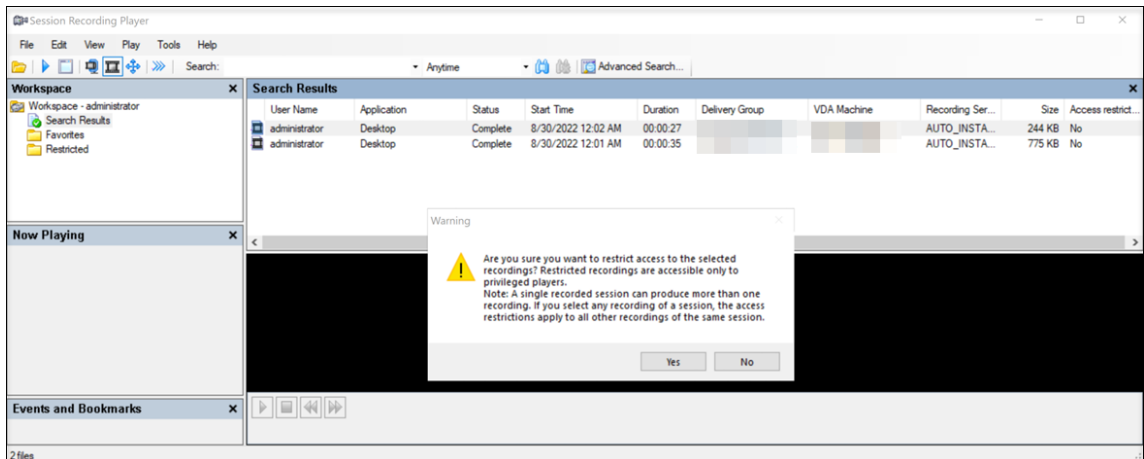
Vue pour le rôle **PrivilegedPlayer** :



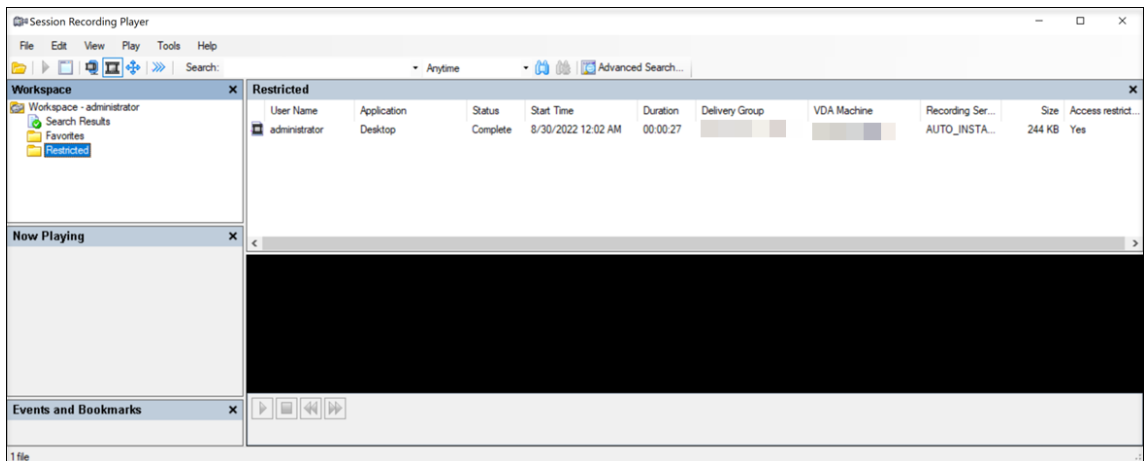
Vue pour le rôle **Player** :



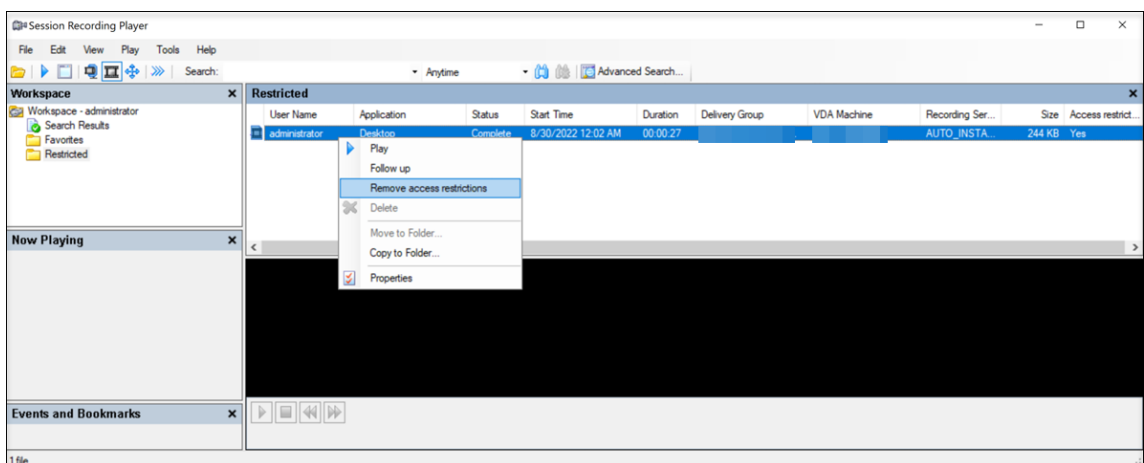
6. Cliquez sur **Oui**.



7. Vérifiez que les enregistrements sélectionnés pour lesquels vous avez imposé des restrictions d'accès sont déplacés de la zone **Résultats de recherche** vers la zone **Restreint**.



8. Dans la zone **Restreint**, supprimez des restrictions d'accès si nécessaire. Une fois les restrictions d'accès supprimées, les enregistrements sont replacés dans la zone **Résultats de recherche**.



Ouvrir et lire des enregistrements

February 20, 2024

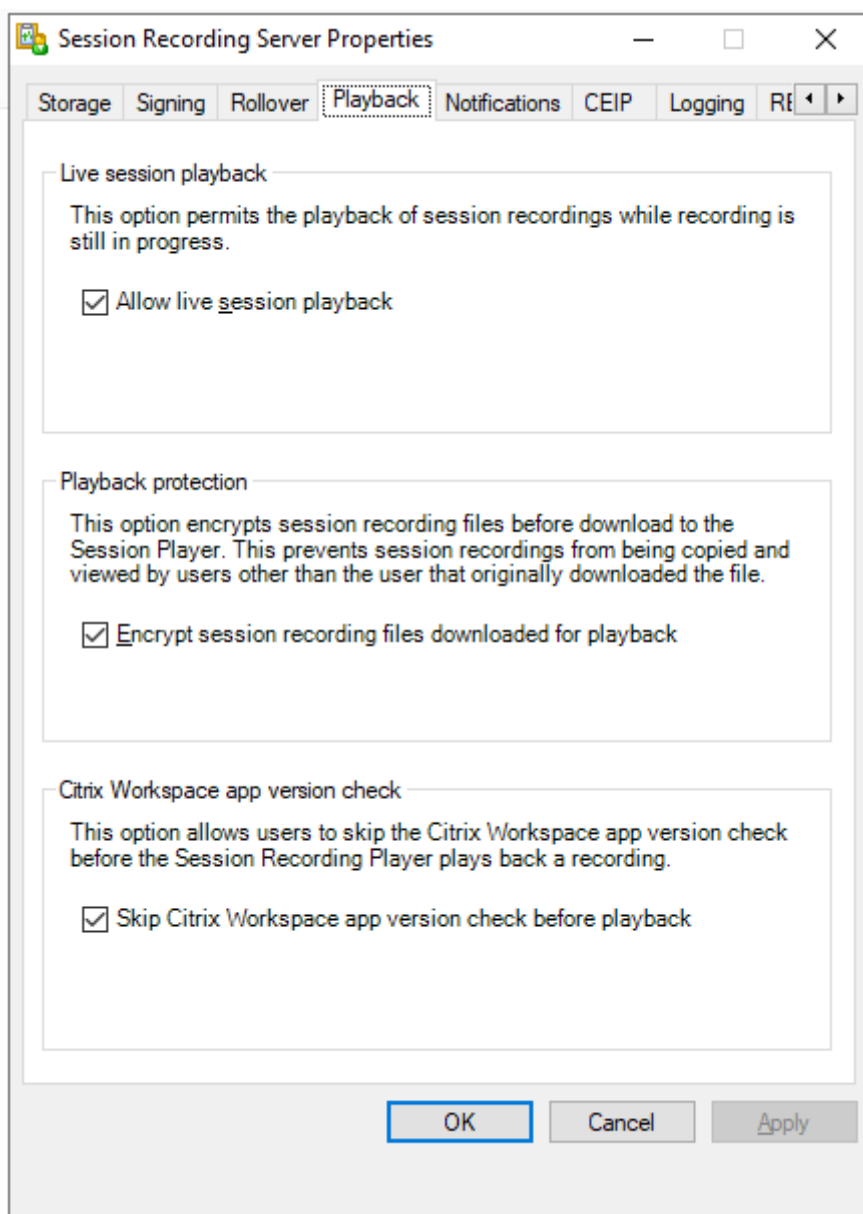
Ouvrir des enregistrements

Vous pouvez utiliser trois méthodes différentes pour ouvrir des enregistrements de session dans le lecteur d'enregistrement de session :

- Effectuez une recherche à l'aide du lecteur d'enregistrement de session. Les sessions enregistrées correspondant aux critères de recherche s'affichent dans la zone des résultats de la recherche.
- Accédez aux fichiers de session enregistrée directement sur votre disque dur local ou sur un lecteur partagé.
- Accédez aux fichiers de session enregistrée à partir d'un dossier Favoris.

Lorsque vous ouvrez un fichier enregistré sans signature numérique, un message d'avertissement s'affiche. Il indique que l'origine et l'intégrité du fichier n'ont pas été vérifiées. Si vous avez confiance dans l'intégrité du fichier, cliquez sur **Oui** dans la fenêtre d'avertissement pour ouvrir le fichier.

Le lecteur d'enregistrement de session vérifie la version de l'application Citrix Workspace avant de lire une session enregistrée. Si le lecteur ne prend pas en charge la version de l'application Citrix Workspace, une erreur est renvoyée. Pour éliminer l'erreur, sélectionnez **Ignorer la vérification de la version de l'application Citrix Workspace** dans **Propriétés du serveur d'enregistrement de session**.

**Remarque :**

la fonctionnalité Journalisation de l'administrateur de l'enregistrement de session vous permet de consigner les téléchargements d'enregistrement dans le lecteur d'enregistrement de session. Pour de plus amples informations, consultez [Journalisation de l'administrateur](#).

Ouvrir un enregistrement dans la zone de résultats de la recherche

1. Ouvrez une session sur la machine sur laquelle le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.

3. Effectuez une recherche rapide.
4. Si la zone des résultats de la recherche n'est pas visible, sélectionnez **Résultats de la recherche** dans le volet Espace de travail.
5. Dans la zone des résultats de la recherche, sélectionnez la session que vous souhaitez lire.
6. Effectuez une des actions suivantes :
 - Double-cliquez sur la session.
 - Cliquez avec le bouton droit et sélectionnez **Propriétés**.
 - Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture > Vitesse de lecture**.

Ouvrir un enregistrement en accédant au fichier

Le nom d'un fichier d'enregistrement commence par `i_`, suivi d'un identifiant alphanumérique de fichier unique, suivi d'une extension de fichier `.icl` et `.icle`. L'extension `.icl` désigne les enregistrements sans protection de lecture. L'extension `.icle` désigne les enregistrements avec protection de lecture. Les fichiers de sessions enregistrées sont enregistrés dans un dossier incorporant la date à laquelle les sessions ont été enregistrées. Par exemple, le fichier d'une session enregistrée le 22 décembre 2014 est enregistré dans le chemin de dossier `2014\12\22`.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Effectuez une des actions suivantes :
 - Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Fichier > Ouvrir** et recherchez le fichier.
 - À l'aide de Windows Explorer, naviguez jusqu'au fichier et glissez-déplacez le fichier dans la fenêtre **Lecteur**.
 - À l'aide de Windows Explorer, naviguez jusqu'au fichier et double-cliquez dessus.
 - Si vous avez créé des favoris dans le volet Espace de travail, sélectionnez **Favoris** et ouvrez le fichier à partir de la zone Favoris de la même manière que vous ouvrez des fichiers à partir de la zone de résultats de recherche.

Utiliser des favoris

La création des dossiers **Favoris** vous permet d'accéder rapidement à des enregistrements que vous visionnez fréquemment. Ces dossiers **Favoris** répertorient des fichiers de sessions enregistrées qui sont stockés sur votre station de travail ou sur un lecteur réseau. Vous pouvez importer et exporter ces fichiers vers d'autres stations de travail et partager ces dossiers avec d'autres utilisateurs du lecteur d'enregistrement de session.

Remarque :

Seuls les utilisateurs disposant des droits d'accès au lecteur d'enregistrement de session peuvent télécharger les fichiers de sessions enregistrées associés aux dossiers **Favoris**. Pour plus d'informations sur les droits d'accès, veuillez contacter votre administrateur d'enregistrement de session.

Pour créer un sous-dossier **Favoris** :

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la fenêtre **Lecteur d'enregistrement de session**, sélectionnez le dossier **Favoris** de votre volet Espace de travail.
4. Dans la barre de menu, choisissez **Fichier > Dossier > Nouveau dossier**. Un nouveau dossier apparaît sous le dossier **Favoris**.
5. Tapez le nom du dossier, puis appuyez sur **Entrer** ou cliquez n'importe où pour accepter le nouveau nom.

Vous pouvez utiliser les autres options qui s'affichent dans le menu **Fichier > Dossier** pour supprimer, renommer, copier, importer et exporter les dossiers.

Lire des enregistrements

Après avoir ouvert une session enregistrée dans le lecteur d'enregistrement de session, vous pouvez parcourir les sessions enregistrées en utilisant les méthodes suivantes :

- Utilisez les contrôles du lecteur pour lire, arrêter, mettre en pause et pour augmenter ou réduire la vitesse de lecture.
- Utilisez le curseur de recherche pour avancer ou reculer.

Vous pouvez également parcourir la session enregistrée en accédant aux marqueurs insérés et aux événements personnalisés.

Remarque :






- un second pointeur de souris peut apparaître pendant la lecture d'une session enregistrée. Le deuxième pointeur s'affiche dans l'enregistrement lorsque l'utilisateur navigue dans Internet Explorer, puis clique sur une image qui était à l'origine plus grande que l'écran, mais avait été automatiquement réduite par Internet Explorer. Bien qu'un seul pointeur apparaisse au cours de la session, deux peuvent apparaître pendant la lecture.
- Cette version de l'enregistrement de session ne prend pas en charge l'accélération multi-média SpeedScreen et le paramètre de stratégie de réglage de la qualité Flash. Lorsque

cette option est activée, la lecture affiche un carré noir.

- Lors de l'enregistrement d'une session avec une résolution supérieure ou égale à 4 096 x 4 096, des fragments peuvent apparaître dans l'apparence de l'enregistrement.

Utiliser les contrôles du lecteur

Vous pouvez cliquer sur les contrôles du lecteur dans la partie inférieure de la fenêtre Lecteur ou y accéder en choisissant **Lecture** dans la barre de menu du **lecteur d'enregistrement de session**.

Contrôle du lecteur	Fonction
	Lit le fichier de session sélectionné.
	Suspend la lecture.
	Arrête la lecture. Si vous cliquez sur Arrêter , puis Lire , l'enregistrement reprend au début du fichier.
	Réduit la vitesse de lecture actuelle jusqu'à un quart minimum de la vitesse normale.
	Double la vitesse de lecture actuelle jusqu'à 32 fois maximum la vitesse normale.

Utiliser le curseur de recherche

Utilisez le curseur de recherche situé dans la partie inférieure de la fenêtre Lecteur pour sauter directement à une position différente dans la session enregistrée. Vous pouvez faire glisser le curseur de recherche jusqu'au point de l'enregistrement que vous souhaitez afficher ou vous pouvez cliquer n'importe où sur la barre du curseur pour vous déplacer dans cette direction.

Vous pouvez aussi utiliser les touches clavier suivantes pour contrôler le curseur de recherche :

Touche du clavier	Fonction
Début	Recherche depuis le début.
Fin	Recherche jusqu'à la fin.
Flèche droite	Recherche en avant (cinq secondes).
Flèche gauche	Recherche en arrière (cinq secondes).

Touche du clavier	Fonction
Déplacement de la roulette de la souris d'un cran vers le bas	Recherche en avant (15 secondes).
Déplacement de la roulette de la souris d'un cran vers le haut	Recherche en arrière (15 secondes).
Ctrl + Flèche droite	Recherche en avant (30 secondes).
Ctrl + Flèche gauche	Recherche en arrière (30 secondes).
Pg suiv.	Recherche en avant (une minute).
Pg préc.	Recherche en arrière (une minute).
Ctrl + Déplacement de la roulette de la souris d'un cran vers le bas	Recherche en avant (90 secondes).
Ctrl + Déplacement de la roulette de la souris d'un cran vers le haut	Recherche en arrière (90 secondes).
Ctrl + Page suivante	Recherche en avant (six minutes).
Ctrl + Page précédente	Recherche en arrière (six minutes).

Pour régler la vitesse du curseur de recherche : dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Outils > Options > Lecteur** et faites glisser le curseur pour augmenter ou réduire le délai de réponse de la recherche. Un temps de réponse plus rapide sollicite plus de mémoire. La réponse peut être lente en fonction de la taille des enregistrements et du matériel de votre ordinateur.

Modifier la vitesse de lecture

Vous pouvez définir une vitesse de lecture en incréments exponentiels allant d'un quart à 32 fois la vitesse de lecture normale.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture > Vitesse de lecture**.
4. Choisissez une option de vitesse.

La vitesse s'adapte immédiatement. Le texte indiquant le taux exponentiel s'affiche rapidement en vert dans la partie inférieure de la fenêtre Lecteur.

Afficher les périodes d'inactivité des sessions enregistrées

Les périodes d'inactivité d'une session enregistrée sont les parties pendant lesquelles aucune action n'a lieu. Le lecteur d'enregistrement de session peut indiquer les périodes d'inactivité des sessions enregistrées lors de la lecture. L'option par défaut est **Activé**. Pour de plus amples informations, consultez la section [Afficher les périodes d'inactivité](#).

Ignorer les espaces sans action

Le mode de révision rapide vous permet de configurer le lecteur pour qu'il ignore les parties de sessions enregistrées pendant lesquelles aucune action n'a lieu. Ce réglage permet d'économiser du temps pour la lecture. Cependant, il ne permet pas d'ignorer les séquences animées comme les mouvements de souris, les clignotements de curseur ou les horloges affichées et leurs aiguilles en mouvement.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture > Mode de consultation rapide**.

L'option passe de l'état activée à désactivée et vice-versa. Chaque fois que vous le choisissez, le statut s'affiche rapidement en vert dans la fenêtre Lecteur.

Modifier l'affichage de la lecture

Pour modifier l'affichage des sessions enregistrées dans la fenêtre du lecteur, procédez comme suit :

- Faire défiler et mettre à l'échelle l'image
- Afficher la lecture en plein écran
- Afficher la fenêtre du lecteur dans une fenêtre séparée
- Afficher une bordure rouge autour de la session enregistrée pour la différencier de l'arrière-plan de la fenêtre du lecteur

Afficher la fenêtre du lecteur en plein écran

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.

3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Afficher > Lecteur en plein écran**.
4. Pour revenir à la taille originale, appuyez sur **Échap** ou **F11**.

Afficher la fenêtre du lecteur dans une fenêtre séparée

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Affichage > Lecteur dans une fenêtre séparée**. Une nouvelle fenêtre s'affiche ; elle contient la fenêtre du lecteur. Vous pouvez faire glisser et redimensionner la fenêtre.
4. Pour incorporer la fenêtre Lecteur dans la fenêtre principale, choisissez **Affichage > Lecteur dans une fenêtre séparée** ou appuyez sur **F10**.

Mettre l'écran de lecture de session à l'échelle de la fenêtre Lecteur

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture > Panorama et mise à l'échelle > Mise à l'échelle**.
 - **Mise à l'échelle (rendu rapide)** rétrécit les images tout en fournissant une bonne qualité. Les images sont créées plus rapidement qu'avec l'option Haute qualité, mais les images et le texte ne sont pas aussi nets. Utilisez cette option si vous avez des problèmes de performances en utilisant le mode Haute qualité.
 - **Mise à l'échelle (haute qualité)** rétrécit les images tout en fournissant une haute qualité. L'emploi de cette option peut se traduire par plus de lenteur dans la création des images qu'avec l'option Rendu rapide.

Réaliser un panorama de l'image

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Lecture > Panorama et mise à l'échelle > Panorama**. Le pointeur se transforme en main. Une représentation de l'écran en taille réduite s'affiche dans le coin supérieur droit de la fenêtre Lecteur.

4. Faites glisser l'image. La représentation de taille réduite indique où vous vous trouvez dans l'image.
5. Pour arrêter le panorama, choisissez l'une des options de mise à l'échelle.

Afficher une bordure rouge autour de l'enregistrement de session

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Outils > Options > Lecteur**.
4. Sélectionnez la case **Afficher le pourtour de l'enregistrement de la session**.
Si la case **Afficher le pourtour de l'enregistrement de session** n'est pas cochée, vous pouvez afficher temporairement le pourtour rouge en cliquant sur le bouton gauche de la souris et en le maintenant enfoncé pendant que le pointeur se trouve dans la fenêtre du lecteur.

Enregistrements en cache

December 21, 2022

Chaque fois que vous ouvrez un fichier de session enregistrée, le lecteur d'enregistrement de session télécharge le fichier de l'emplacement de stockage des enregistrements. Si vous téléchargez les mêmes fichiers régulièrement, vous pouvez gagner du temps en mettant les fichiers en cache sur votre station de travail. Les fichiers mis en cache sont stockés sur votre station de travail dans ce dossier :

userprofile**AppData\Local\Citrix\SessionRecording\Player\Cache**

Vous pouvez spécifier la quantité d'espace disque utilisée pour le cache. Lorsque les enregistrements atteignent le volume d'espace disque spécifié, l'enregistrement de session supprime les enregistrements les plus anciens et les moins utilisés pour faire de la place aux nouveaux enregistrements. Vous pouvez vider le cache à tout moment pour libérer de l'espace disque.

Activer la mise en cache

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du lecteur d'enregistrement de session**, choisissez **Outils > Options > Cache**.
4. Cochez la case **Mettre en cache les fichiers téléchargés sur la machine locale**.

5. Pour limiter le volume d'espace disque utilisé pour la mise en cache, cochez la case **Limiter le volume d'espace disque utilisable** et faites glisser le curseur ou entrez le nombre de mégaoctets à utiliser pour le cache.
6. Cliquez sur **OK**.

Purger les caches

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du lecteur d'enregistrement de session**, choisissez ****Outils > Options > Cache**.
4. Cochez la case **Mettre en cache les fichiers téléchargés sur la machine locale**.
5. Dans le lecteur d'enregistrement de session, choisissez **Outils > Options > Cache**.
6. Cliquez sur **Purger le cache**, puis sur **OK** pour confirmer l'action.

Afficher les périodes d'inactivité

December 21, 2022

Les périodes d'inactivité d'une session enregistrée sont les parties pendant lesquelles aucune action n'a lieu. Le lecteur d'enregistrement de session peut indiquer les périodes d'inactivité des sessions enregistrées lors de la lecture. L'option par défaut est **Activé**.

Remarque : les périodes d'inactivité ne sont pas affichées lors de la lecture de sessions actives à l'aide du lecteur d'enregistrement de session.

Pour afficher les périodes d'inactivité des sessions enregistrées, procédez comme suit :

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Dans la barre de menu du lecteur d'enregistrement de session**, choisissez ****Affichage > Périodes inactives** et cochez ou décochez la case.

Utiliser des événements et des signets

December 21, 2022

Vous pouvez utiliser les événements et les signets pour vous aider à naviguer à travers les sessions enregistrées.

Les événements définis par Citrix sont insérés dans les sessions pendant l'enregistrement des sessions. Vous pouvez également utiliser l'API Event et une application tierce pour insérer des événements personnalisés. Les événements sont enregistrés comme faisant partie du fichier de session. Vous ne pouvez pas les supprimer ou les modifier à l'aide du lecteur d'enregistrement de session.

Les signets sont des marqueurs que vous insérez dans une session enregistrée au cours de la lecture de la session à l'aide du lecteur d'enregistrement de session. Une fois insérés, les signets sont associés à la session enregistrée jusqu'à ce que vous les supprimiez. Cependant, ils ne sont pas enregistrés comme faisant partie du fichier de session, mais stockés sous forme de fichiers `.icl` distincts dans le dossier en cache **Signets** sur le lecteur d'enregistrement de session, par exemple, `C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks`, avec les mêmes noms de fichier que le fichier d'enregistrement `.icl`. Pour lire un fichier d'enregistrement contenant des signets sur un autre lecteur, copiez les fichiers `.icl` dans le dossier en cache **Signets** sur ce lecteur. Par défaut, chaque signet est accompagné de l'étiquette « Signet », mais vous pouvez changer ce nom pour le texte d'annotation de votre choix (avec une limite maximale de 128 caractères).

Les événements s'affichent sous forme de points jaunes et les signets sous forme de carrés bleus dans la partie inférieure de la fenêtre Lecteur. Déplacer la souris sur ces points et carrés permet d'afficher le texte de l'étiquette qui leur est associé. Vous pouvez aussi afficher les événements et les signets dans la liste **Événements et signets** du lecteur d'enregistrement de session. Ils s'affichent dans cette liste avec leur étiquette et l'heure de la session enregistrée à laquelle ils apparaissent, dans l'ordre chronologique.

Vous pouvez utiliser les événements et les signets pour vous aider à naviguer à travers les sessions enregistrées. En allant à un événement ou un signet, vous pouvez atteindre directement le point de la session enregistrée où l'événement ou signet a été inséré.

Afficher les événements et les signets dans la liste

La liste **Événements et signets** contient les événements et les signets insérés dans la session enregistrée en cours de lecture. Elle peut afficher les événements, les signets seulement ou elle peut afficher les deux.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Déplacez le pointeur de la souris dans la zone de la liste **Événements et signets** et cliquez avec le bouton droit pour afficher le menu.

4. Choisissez **Afficher les événements seulement**, **Afficher les signets seulement** ou **Afficher tout**.

Insérer un signet

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez la lecture de la session enregistrée à laquelle vous souhaitez ajouter un signet.
4. Déplacez le curseur de recherche sur le point d'insertion souhaité pour le signet.
5. Déplacez le pointeur de la souris dans la zone de la fenêtre Lecteur et cliquez avec le bouton droit pour afficher le menu.
6. Ajoutez un signet avec l'étiquette **Signet** par défaut ou créez une annotation :
 - Pour ajouter un signet avec l'étiquette **Signet** par défaut, choisissez **Ajouter un signet**.
 - Pour ajouter un signet avec un texte descriptif que vous créez, choisissez **Ajouter une annotation**. Entrez le texte de l'étiquette que vous souhaitez attribuer au signet, d'une longueur maximale de 128 caractères. Cliquez sur **OK**.

Ajouter ou modifier une annotation

Après avoir créé un signet, vous pouvez y ajouter une annotation ou en modifier une.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez la lecture de la session enregistrée contenant le signet.
4. Assurez-vous que la liste **Événements et signets** affiche des signets.
5. Sélectionnez le signet dans la liste **Événements et signets** et cliquez avec le bouton droit pour afficher le menu.
6. Choisissez **Modifier l'annotation**.
7. Dans la fenêtre qui apparaît, tapez la nouvelle annotation et cliquez sur **OK**.

Supprimer un signet

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez la lecture de la session enregistrée contenant le signet.
4. Assurez-vous que la liste **Événements et signets** affiche des signets.

5. Sélectionnez le signet dans la liste **Événements et signets** et cliquez avec le bouton droit pour afficher le menu.
6. Choisissez **Supprimer**.

Aller à un événement ou un signet

Lorsque vous accédez à un événement ou un signet, cela signifie que le lecteur d'enregistrement de session accède au point de la session enregistrée où l'événement ou le signet a été inséré.

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Dans le menu **Démarrer**, choisissez **Lecteur d'enregistrement de session**.
3. Commencez à lire un enregistrement de session contenant des événements ou des signets.
4. Allez à un événement ou un signet.
 - Dans la partie inférieure de la fenêtre du lecteur, cliquez sur le point ou carré représentant l'événement ou le signet que vous souhaitez consulter.
 - Dans la liste **Événements et signets**, double-cliquez sur un élément pour vous y rendre. Pour accéder à l'événement ou au favori suivant, sélectionnez-le dans la liste, cliquez dessus avec le bouton droit de la souris pour afficher le menu, puis choisissez **Rechercher jusqu'au signet**.

Lecteur Web d'enregistrement de session

December 21, 2022

Le lecteur Web vous permet d'utiliser un navigateur Web pour afficher et lire des sessions enregistrées.

Le lecteur Web vous permet de :

- Rechercher des enregistrements à l'aide de filtres
- Afficher et lire des enregistrements actifs et terminés avec des événements marqués répertoriés dans le panneau droit
- Configurer la mémoire cache pour stocker des enregistrements lors de la lecture
- Afficher les périodes d'inactivité
- Laisser des commentaires sur un enregistrement et définir la sévérité des commentaires
- Partager les URL des enregistrements
- Afficher les statistiques d'événements graphiques pour chaque enregistrement

- Afficher les points de données liés à chaque session enregistrée

Accéder au lecteur Web

February 20, 2024

L'URL du site Web du lecteur Web est `http(s)://<FQDN of Session Recording server>/WebPlayer`. Pour garantir l'utilisation de HTTPS, ajoutez une liaison SSL au site Web sur IIS et mettez à jour le fichier de configuration `SsRecWebSocketServer.config`.

Remarque :

- Lors de la connexion au site Web du lecteur Web, les utilisateurs de domaine n'ont pas besoin d'entrer leurs informations d'identification, alors que les utilisateurs n'appartenant pas à un domaine doivent le faire.
- Les navigateurs pris en charge incluent Google Chrome, Microsoft Edge et Firefox.
- Pour que le lecteur Web fonctionne correctement, assurez-vous d'activer WebGL dans Firefox.

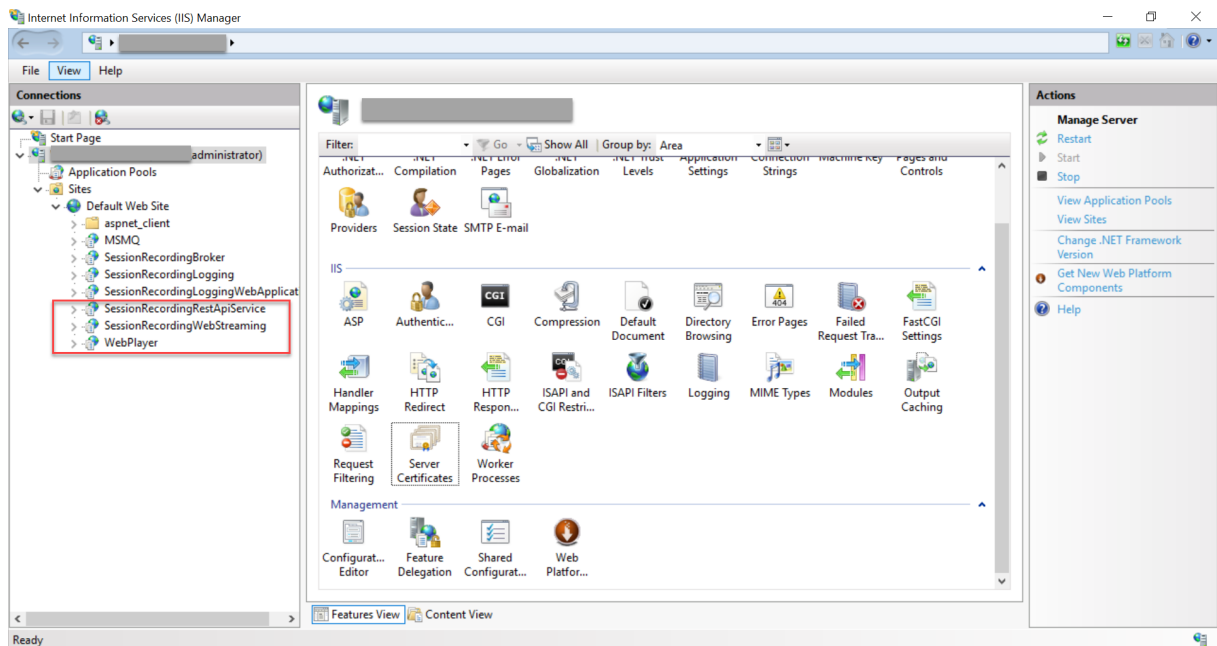
Cet article vous guide tout au long du processus d'installation et d'activation du lecteur Web, ainsi que le processus de configuration du protocole HTTPS.

Installer le lecteur Web

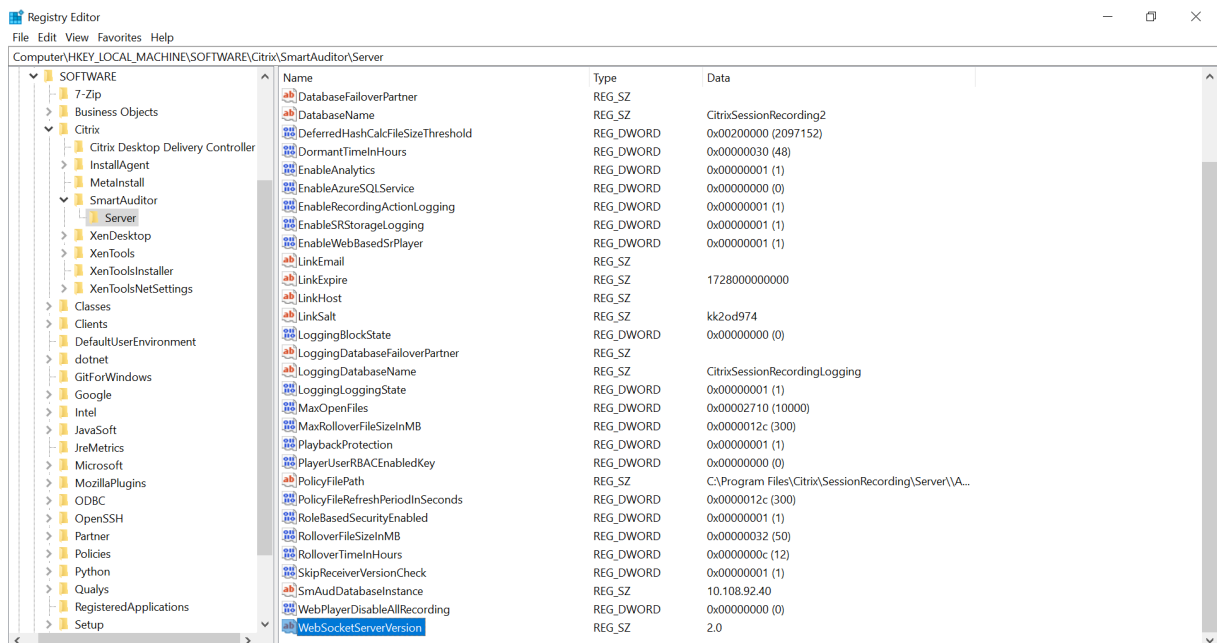
Installez le lecteur Web uniquement sur le serveur d'enregistrement de session. Cliquez deux fois sur `SessionRecordingWebPlayer.msi` puis suivez les invites pour terminer votre installation. Pour plus d'informations sur l'installation de l'enregistrement de session, consultez la section [Installer, mettre à niveau et désinstaller](#).

À partir de la version 2103, l'enregistrement de session migre le serveur WebSocket vers IIS. Une fois le lecteur Web installé, les applications **SessionRecordingRestApiService**, **SessionRecordingWeb-Streaming** et **WebPlayer** apparaissent sur IIS.

Enregistrement de session 2210



Une nouvelle installation de l'enregistrement de session 2103 et versions ultérieures connecte votre navigateur Web au serveur WebSocket hébergé sur IIS lorsque vous accédez au site Web du lecteur Web. Le serveur WebSocket hébergé sur IIS dispose de la version gérée 2.0, comme indiqué par la valeur de registre **WebSocketServerVersion** sous la clé de registre sur `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.



Une installation de mise à niveau à partir d'une version antérieure vers l'enregistrement de session 2103 et versions ultérieures connecte votre navigateur Web au serveur WebSocket basé sur Python. Pour vous connecter au serveur WebSocket hébergé sur IIS, exécutez la commande **<chemin d'instal-**

lacion du serveur d'enregistrement de session>\Bin\SsRecUtils.exe -enablestreamingservice. Pour vous reconnecter au serveur WebSocket basé sur Python, exécutez la commande **<chemin d'installation du serveur d'enregistrement de session>\Bin\SsRecUtils.exe - disablestreamingservice.** Le serveur WebSocket basé sur Python dispose de la version gérée 1.0.

Activer le lecteur Web

Le lecteur Web est activé par défaut.

- Pour désactiver le lecteur Web, démarrez une invite de commande Windows et exécutez la commande `<Session Recording Server installation path>\Bin\SsRecUtils.exe -disablewebplayer.`
- Pour activer le lecteur Web, démarrez une invite de commande Windows et exécutez la commande `<Session Recording Server installation path>\Bin\SsRecUtils.exe -enablewebplayer.`

Configurer le protocole HTTPS

L'URL du site Web du lecteur Web est `http(s)://<FQDN of Session Recording server>/WebPlayer.` Pour garantir l'utilisation de HTTPS, ajoutez une liaison SSL au site Web sur IIS et mettez à jour le fichier de configuration `SsRecWebSocketServer.config.`

Remarque :

Lors de la connexion au site Web du lecteur Web, les utilisateurs de domaine n'ont pas besoin d'entrer leurs informations d'identification, alors que les utilisateurs n'appartenant pas à un domaine doivent le faire.

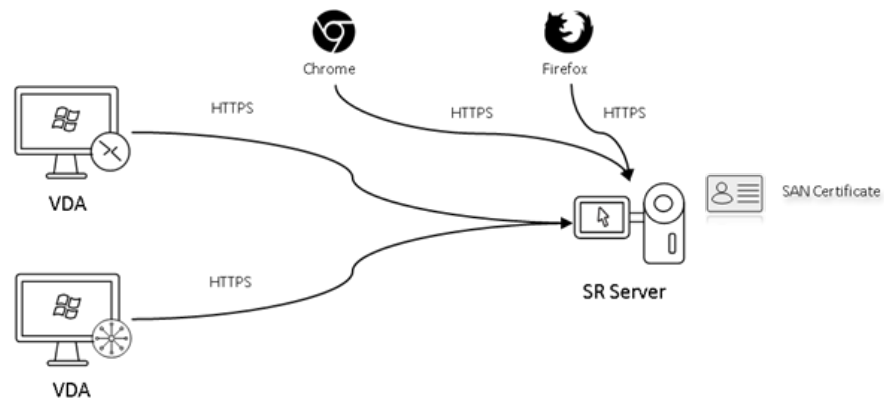
Pour utiliser HTTPS pour accéder au site Web du lecteur Web, procédez comme suit :

1. Ajoutez une liaison SSL sur IIS.
 - a) Obtenez un certificat SSL au format PEM auprès d'une autorité de certification (CA) de confiance.

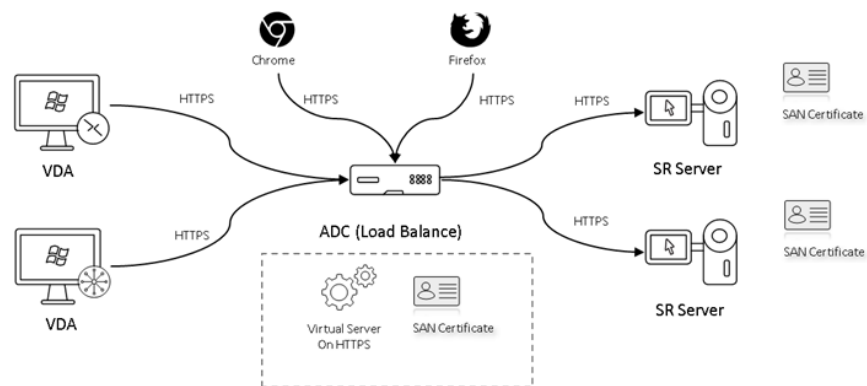
Remarque :

La plupart des navigateurs populaires tels que Google Chrome et Firefox ne prennent plus en charge l'utilisation du nom commun dans une demande de signature de certificat (CSR). Ils appliquent en effet l'utilisation du nom SAN (Autre nom de l'objet) dans tous les certificats approuvés publiquement. Pour utiliser le lecteur Web sur HTTPS, procédez comme suit :

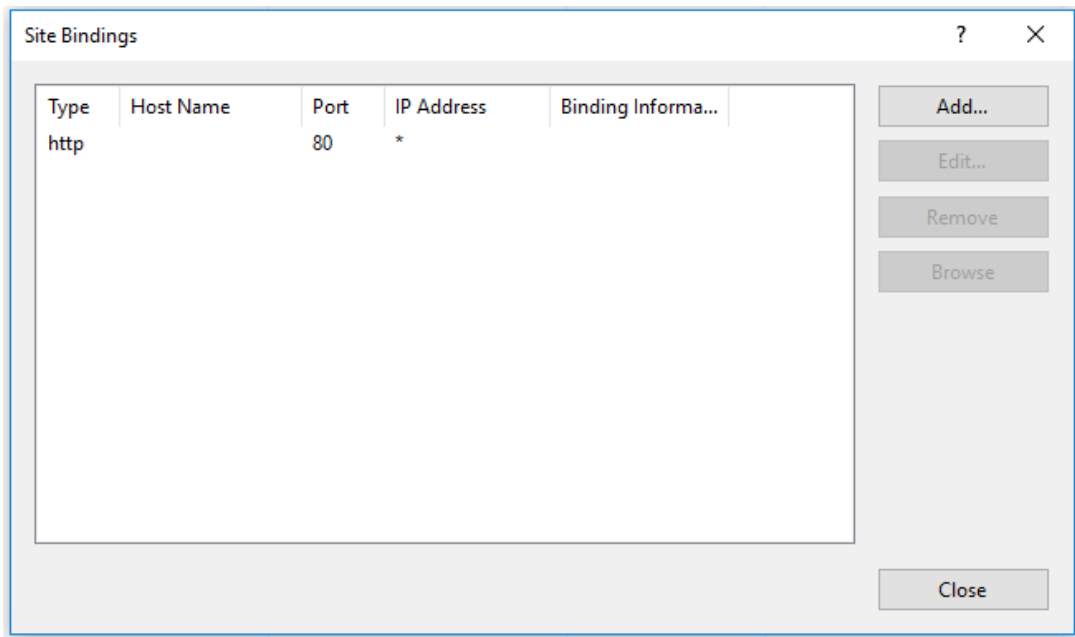
- Lorsqu'un seul serveur d'enregistrement de session est utilisé, mettez à jour le certificat du serveur d'enregistrement de session vers un certificat SAN.



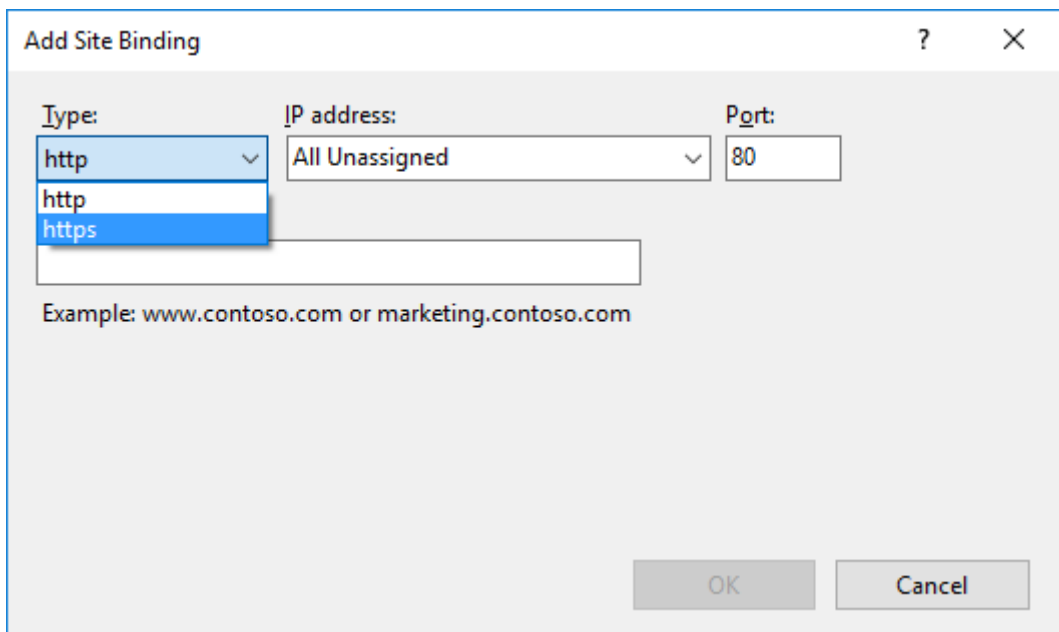
- Lorsque l'équilibrage de charge est utilisé, assurez-vous qu'un certificat SAN est disponible à la fois sur Citrix ADC et sur chaque serveur d'enregistrement de session.



- b) Dans IIS, cliquez avec le bouton droit de la souris sur le site Web et sélectionnez **Ajouter des liaisons**. La boîte de dialogue **Liaisons de sites** s'affiche.



- c) Cliquez sur **Ajouter** dans le coin supérieur droit. La boîte de dialogue **Ajouter la liaison de site** s'affiche.
- d) Sélectionnez **https** dans la liste **Type** et sélectionnez votre certificat SSL.



The screenshot shows a dialog box titled "Add Site Binding". It contains the following elements:

- Type:** A dropdown menu set to "https".
- IP address:** A dropdown menu set to "All Unassigned".
- Port:** A text box containing "443".
- Host name:** An empty text box.
- Require Server Name Indication:** An unchecked checkbox.
- SSL certificate:** A dropdown menu with "Not selected" selected. A list is open below it showing "Not selected" and "test".
- Select...:** A button to the right of the SSL certificate dropdown.
- View...:** A button to the right of the "Select..." button.
- OK:** A button at the bottom right.
- Cancel:** A button at the bottom right, to the right of the "OK" button.

e) Cliquez sur **OK**.

2. Mettez à jour le fichier de configuration `SsRecWebSocketServer.config`.

a) Recherchez et ouvrez le fichier de configuration `SsRecWebSocketServer.config`.

Le fichier de configuration `SsRecWebSocketServer.config` se trouve généralement dans le dossier `<Session Recording Server installation path>\Bin\`.

b) (Facultatif) Pour l'enregistrement de session 2103 et versions ultérieures qui hébergent le serveur WebSocket sur IIS, activez TLS en modifiant `TLSEnable=1` et ignorez les champs **ServerPort**, **SSLCert** et **SSLKey**.

c) (Facultatif) Pour l'enregistrement de session 2012 et les versions antérieures, activez TLS en modifiant `TLSEnable=1` et entrez les chemins d'accès au certificat SSL et à sa clé, respectivement.

Remarque :

Seul le format PEM des certificats SSL et des fichiers de clés est pris en charge.

Le champ **ServerPort** indique le numéro de port utilisé par le lecteur Web pour collecter les fichiers d'enregistrement. Dans la capture d'écran suivante, ce champ est défini sur la valeur par défaut (22334).

```
SsRecWebSocketServer.exe.config - Notepad
File Edit Format View Help
#1-enable TLS
#0-disable TLS
TLSEnable=0
#default-enable web socket server on all ip address
#x.x.x.x-only enable server on the given ip address
ServerAddress=default
#default-enable web socket server on tcp port 22334
#[0-65535]-enable server on the given tcp port
ServerPort=default
#cert file path and name, only config it when TLSEnable=1
SSLCert=C:\aSRS2.pem
#key file path and name, only config it when TLSEnable=1
SSLKey=C:\newaSRS2key.pem
```

Pour extraire des fichiers de certificat et de clé distincts utilisés dans la configuration du serveur WebSocket, procédez comme suit :

- i. Assurez-vous que OpenSSL est installé sur votre serveur d'enregistrement de session qui contient le certificat SSL.
- ii. Exportez le certificat SSL en tant que fichier .pfx. Le fichier .pfx inclut à la fois le certificat et la clé privée.
- iii. Ouvrez l'invite de commandes et accédez au dossier contenant le fichier .pfx.
- iv. Démarrez OpenSSL à partir du dossier OpenSSL\bin.
- v. Exécutez la commande suivante pour extraire le certificat :

```
1 openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out [
  aSRS2.pem]
2 <!--NeedCopy-->
```

Entrez le mot de passe d'importation que vous avez créé lors de l'exportation du fichier .pfx.

- vi. Exécutez la commande suivante pour extraire la clé privée :

```
1 openssl pkcs12 -in [yourfile.pfx] -nocerts -out [
  newaSRS2keyWithPassword.pem]
2 <!--NeedCopy-->
```

Entrez le mot de passe d'importation que vous avez créé lors de l'exportation du fichier .pfx. Fournissez un nouveau mot de passe pour protéger votre fichier de clé lorsque vous êtes invité à entrer la phrase secrète PEM.

- vii. Exécutez la commande suivante pour décrypter la clé privée :

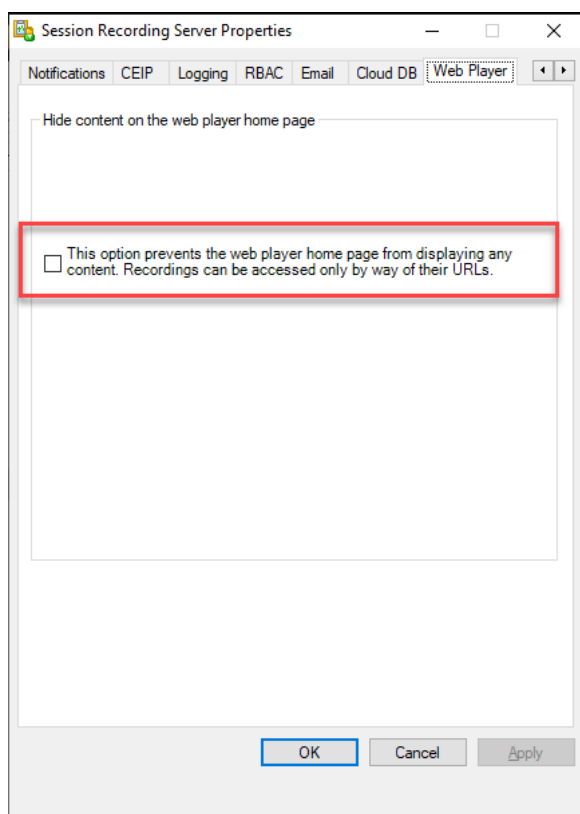
```
1 openssl rsa -in [newaSRS2keyWithPassword.pem] -out [
  newaSRS2key.pem]
2 <!--NeedCopy-->
```

- d) Enregistrez vos modifications.
- e) Vérifiez les paramètres de pare-feu. Autorisez SsRecWebSocketServer.exe à utiliser le port TCP (22334 par défaut) et autorisez l'accès à l'URL du lecteur Web.
- f) Exécutez la commande `SsRecUtils -stopwebsocketserver`.

Masquer ou afficher le contenu sur la page d'accueil du lecteur Web

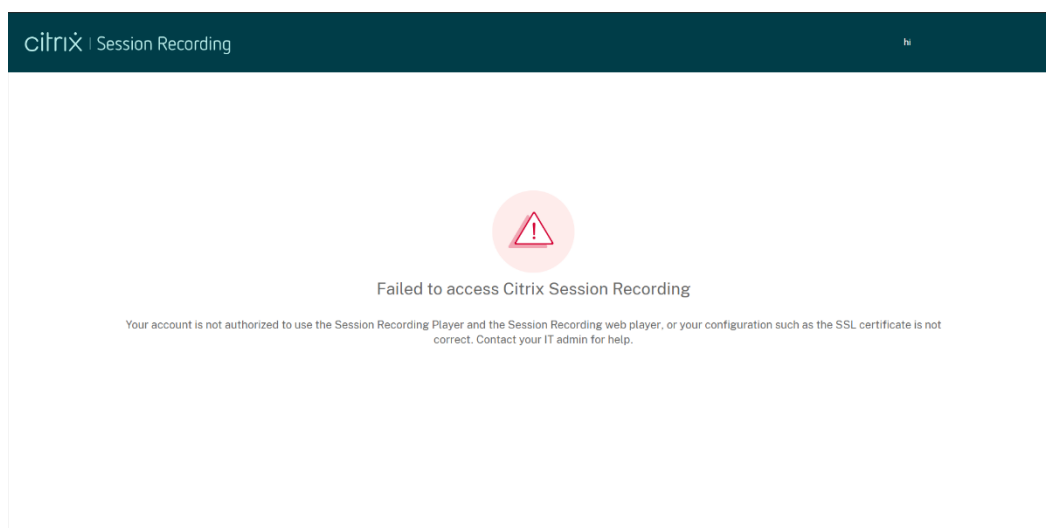
February 20, 2024

Une fois que vous ouvrez une session, la page d'accueil du lecteur Web peut masquer ou afficher le contenu selon que l'option suivante est sélectionnée dans **Propriétés du serveur d'enregistrement de session**.



- Lorsque l'option est sélectionnée, la page d'accueil du lecteur Web masque tout le contenu. Il est uniquement possible d'accéder aux enregistrements via leurs URL. Les URL d'enregistrement sont fournies dans les alertes envoyées par e-mail à des destinataires spécifiés.

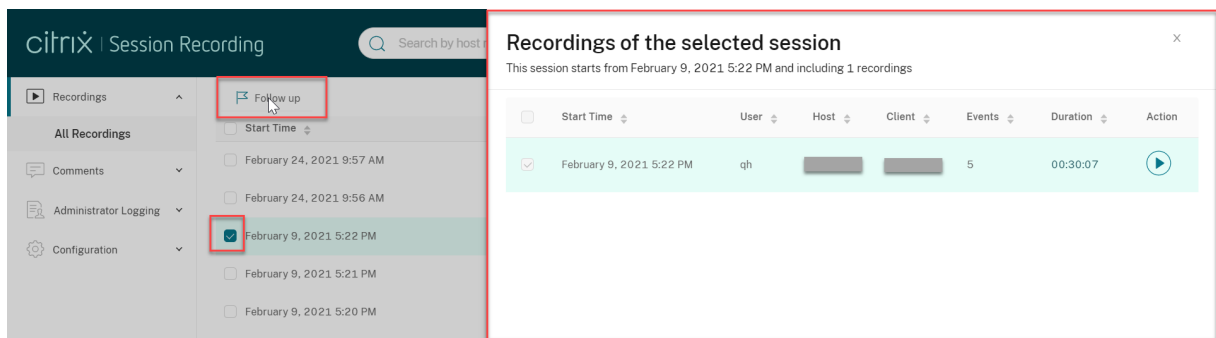
Pour plus d'informations sur les alertes e-mail, consultez [Configurer les stratégies de réponse aux événements](#). Vous pouvez également partager des URL d'enregistrement via la commande **Partager lecture en cours** sur les pages de lecture d'enregistrement. Consultez les descriptions plus loin dans cet article.



- Si l'option est désactivée, la page d'accueil du lecteur Web affiche un contenu similaire à la capture d'écran suivante. Cliquez sur **Tous les enregistrements** dans le panneau de navigation de gauche pour actualiser la page et afficher les nouveaux enregistrements. Vous pouvez faire défiler la page Web vers le bas pour sélectionner des enregistrements à afficher ou utiliser des filtres pour personnaliser vos résultats de recherche. Pour les enregistrements actifs, la colonne **Durée** affiche l'état **Actif** et le bouton de lecture s'affiche en vert.

	Start Time	User	Host	Client	Events	Duration	Action
<input type="checkbox"/>	February 23, 2021 3:17 PM	administrator			0	Live	
<input type="checkbox"/>	February 23, 2021 3:05 PM	administrator			0	00:08:14	
<input type="checkbox"/>	February 23, 2021 2:55 PM	qh			0	00:03:12	
<input type="checkbox"/>	February 23, 2021 2:50 PM	qh			0	00:01:54	
<input type="checkbox"/>	February 23, 2021 2:43 PM	qh			0	Live	

Pour afficher tous les fichiers d'enregistrement d'une session enregistrée, sélectionnez un enregistrement dans la liste et cliquez sur l'icône **Suivi**. L'icône **Suivi** est disponible uniquement lorsqu'un enregistrement est sélectionné.



Pour obtenir une description des éléments d'enregistrement, consultez le tableau suivant :

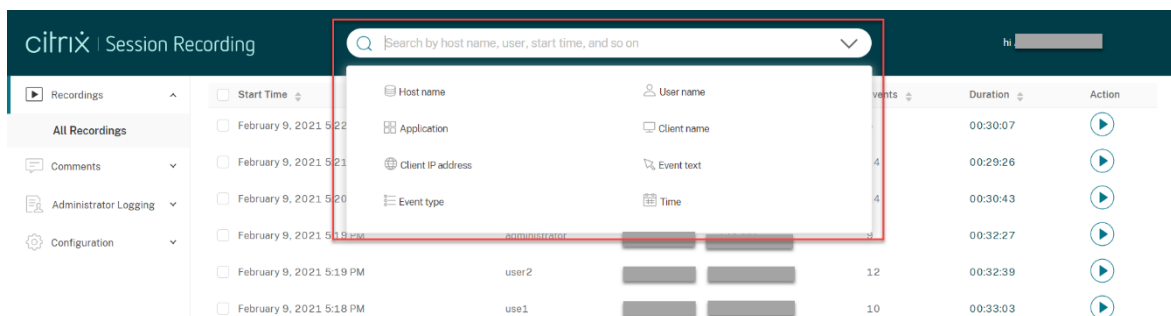
Élément	Description
Heure de début	Heure de début de l'enregistrement. Cliquez sur les flèches vers le haut/vers le bas pour afficher les enregistrements dans l'ordre chronologique.
Utilisateur	Utilisateur dont la session a été enregistrée. Cliquez sur les flèches vers le haut/vers le bas pour afficher les enregistrements d'un utilisateur sur la liste et trier les utilisateurs par ordre alphabétique.
Hôte	Nom d'hôte du VDA dans lequel la session enregistrée a été hébergée. Cliquez sur les flèches vers le haut/vers le bas pour afficher les noms d'hôtes du VDA par ordre alphabétique.
Client	Nom de la machine cliente sur laquelle la session a été exécutée. Cliquez sur les flèches vers le haut/vers le bas pour afficher les noms d'hôte du client par ordre alphabétique.
Événements	Nombre d'événements dans l'enregistrement. Cliquez sur les flèches vers le haut/vers le bas pour afficher les enregistrements dans la liste en fonction du nombre d'événements.
Événements uniquement	Indique un enregistrement d'écran ou un enregistrement d'événement uniquement. Un enregistrement d'événement uniquement lu dans le lecteur Web contient un graphique à secteurs et un histogramme de statistiques d'événements. Le graphique à secteurs et l'histogramme restent statiques tout au long de la lecture.

Élément	Description
Serveur d'enregistrement	Serveur d'enregistrement de session qui traite les données d'enregistrement envoyées à partir des VDA.
Durée	Durée de l'enregistrement. Cliquez sur les flèches vers le haut/vers le bas pour afficher les enregistrements dans la liste en fonction de leur durée.

Rechercher des enregistrements

February 20, 2024

Vous pouvez rechercher des enregistrements à l'aide de filtres du lecteur Web. Les filtres disponibles incluent le nom d'hôte, le nom du client, le nom d'utilisateur, l'application, l'adresse IP du client, le texte de l'événement, le type d'événement et l'heure.



Conseil :

Vous pouvez sélectionner un enregistrement et cliquer sur le bouton **Suivi** pour afficher tous les enregistrements de la session enregistrée.

Par exemple, après avoir sélectionné le filtre de nom d'hôte, la boîte de dialogue suivante apparaît. Tapez le nom d'hôte (du VDA sur lequel les sessions enregistrées sont hébergées) et cliquez sur **Rechercher** pour exclure les enregistrements non pertinents et afficher uniquement les enregistrements pertinents.

FILTER Search Clear All

Host name + X

Vous pouvez passer à un filtre différent en cliquant sur le **nom d'hôte** sélectionné, comme indiqué dans la capture d'écran suivante. Après avoir cliqué sur **Nom d'hôte**, tous les filtres disponibles sont répertoriés. Sélectionnez un filtre différent selon vos besoins.

The screenshot shows a 'FILTER' section with a 'Host name' dropdown menu open. The dropdown list includes: Host name, User name, Application, Client name, Client IP address, Event text, Comments, Event type, and Time. Below the filter menu is a table with columns: User, Host, Client, Events, Duration, and Action. The table contains several rows of data.

User	Host	Client	Events	Duration	Action
qh			5	00:30:07	▶
dzl			14	00:29:26	▶
dlq			14	00:30:43	▶
administrator			9	00:32:27	▶
user2			12	00:32:39	▶

Vous pouvez également cliquer sur le symbole **+** pour ajouter des filtres.

The screenshot shows the 'FILTER' section with a 'Host name' dropdown menu and a search input field. A '+' button is highlighted with a red box, indicating it can be used to add more filters.

Par exemple, vous pouvez ajouter le filtre **Heure** comme indiqué dans l'écran suivant.

The screenshot shows the 'FILTER' section with the 'Time' filter expanded. It includes fields for 'Start date', 'End date', 'Start Time', and 'End time', along with a 'Duration' section with a dropdown menu set to 'At least' and a 'Seconds' dropdown menu. Below the filter section is a table with columns: Start Time, User, Host, Client, Events, Duration, and Action. The table contains one row of data.

Start Time	User	Host	Client	Events	Duration	Action
February 9, 2021 5:22 PM	qh			5	00:30:07	▶

Le filtre **Heure** consiste à enregistrer la date de début, l'heure de début et la durée.

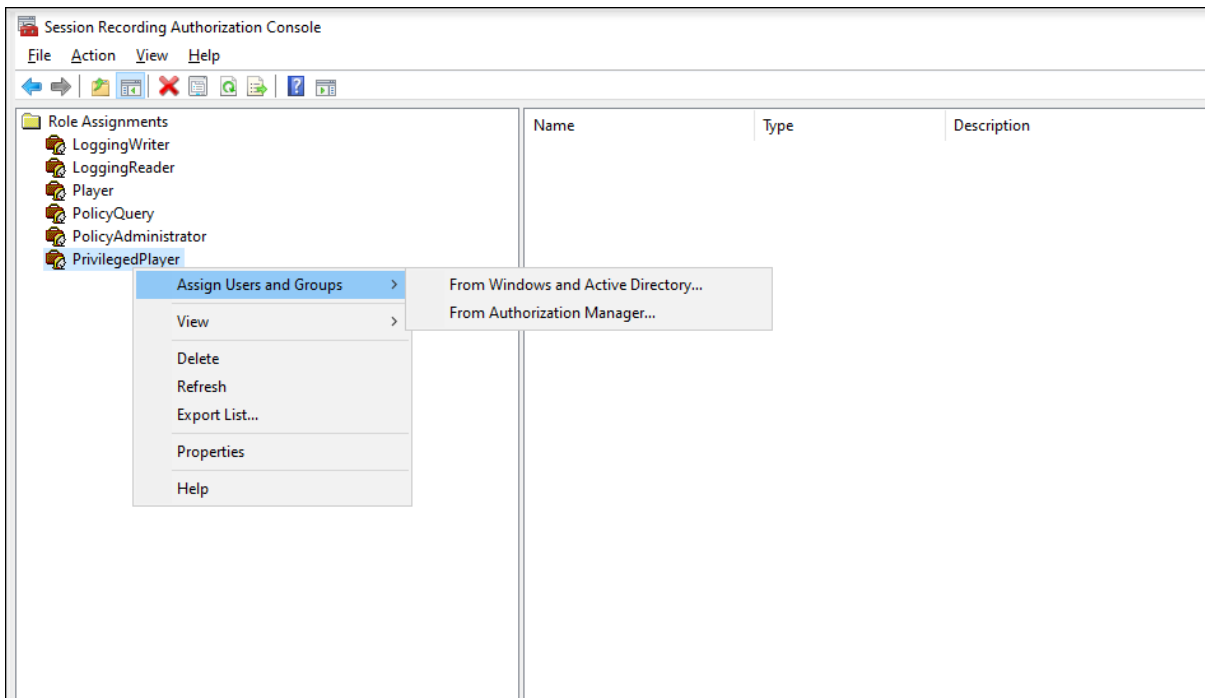
Imposer des restrictions d'accès aux enregistrements

February 20, 2024

Vous imposez des restrictions d'accès aux enregistrements cibles en plus du contrôle d'accès basé sur les rôles par le biais de [stratégies de visionnage d'enregistrement](#). Les enregistrements restreints ne sont accessibles qu'aux utilisateurs et aux groupes d'utilisateurs auxquels le rôle **PrivilegedPlayer** est attribué via la console d'autorisation d'enregistrement de session.

Remarque :

Il n'est pas possible d'imposer des restrictions d'accès aux enregistrements en direct.



La section suivante vous explique comment placer et supprimer des restrictions d'accès sur les enregistrements cibles.

1. Entrez l'URL du site de votre lecteur Web dans la barre d'adresse d'un navigateur compatible.

Le format de l'URL est **http(s)://<Nom de domaine complet du Serveur d'enregistrement de session>/WebPlayer**.

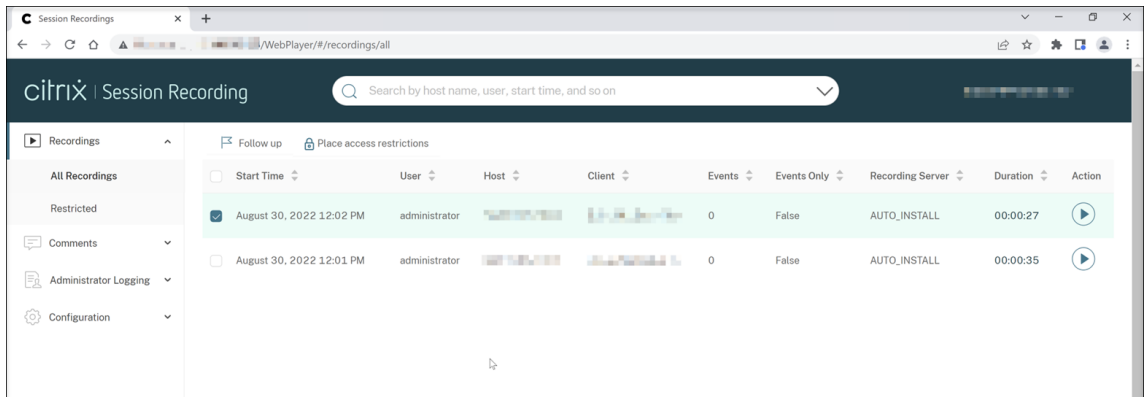
Les navigateurs pris en charge incluent Google Chrome, Microsoft Edge et Firefox.

2. Dans le menu de navigation de gauche de la page du lecteur Web, développez le menu **Enregistrements**.
3. Sur la page **Tous les enregistrements**, sélectionnez un ou plusieurs enregistrements cibles.
4. Cliquez sur l'icône **Imposer restrictions d'accès** en haut de la liste des enregistrements.

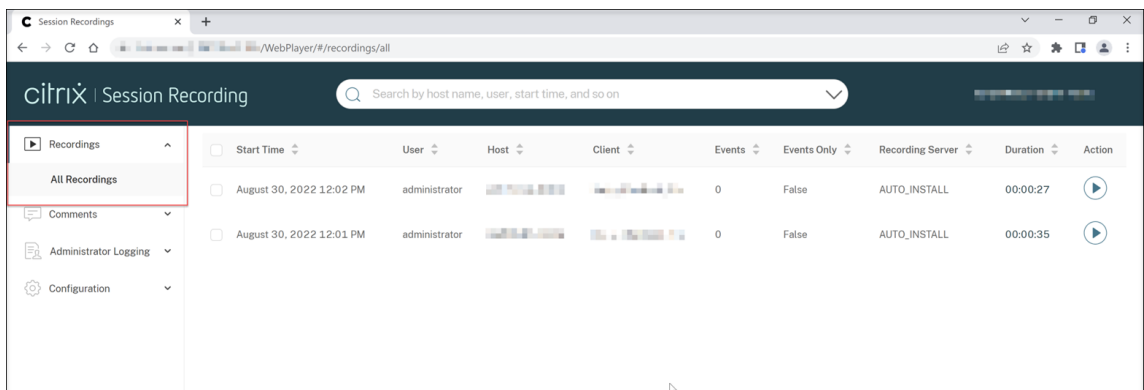
Les utilisateurs et les groupes d'utilisateurs auxquels est attribué le rôle **Player** ou **Privileged-Player** sont autorisés à imposer des restrictions d'accès aux enregistrements. Le menu **Re-**

streint n'est disponible que pour les utilisateurs et les groupes d'utilisateurs auxquels le rôle **PrivilegedPlayer** a été attribué.

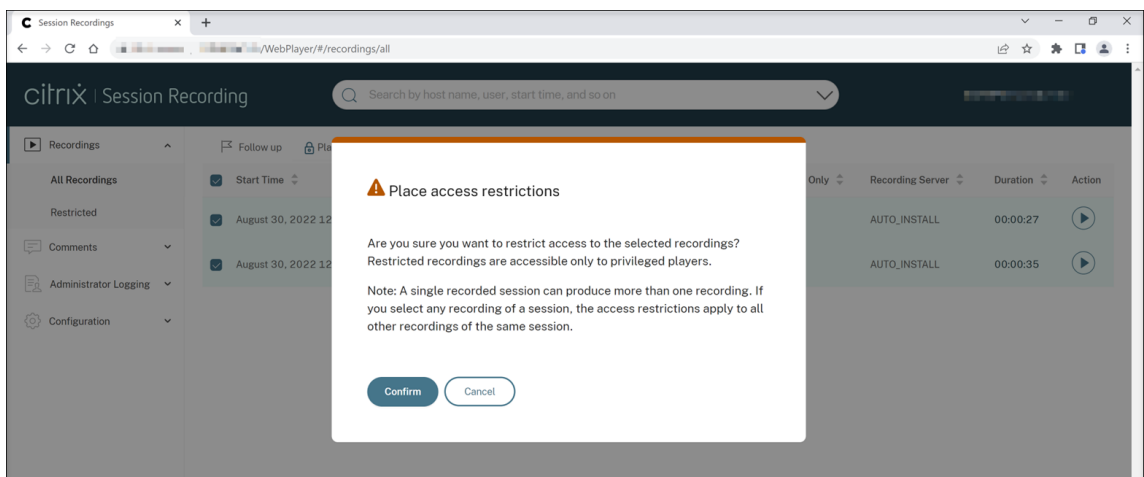
Vue pour le rôle **PrivilegedPlayer** :



Vue pour le rôle **Player** :

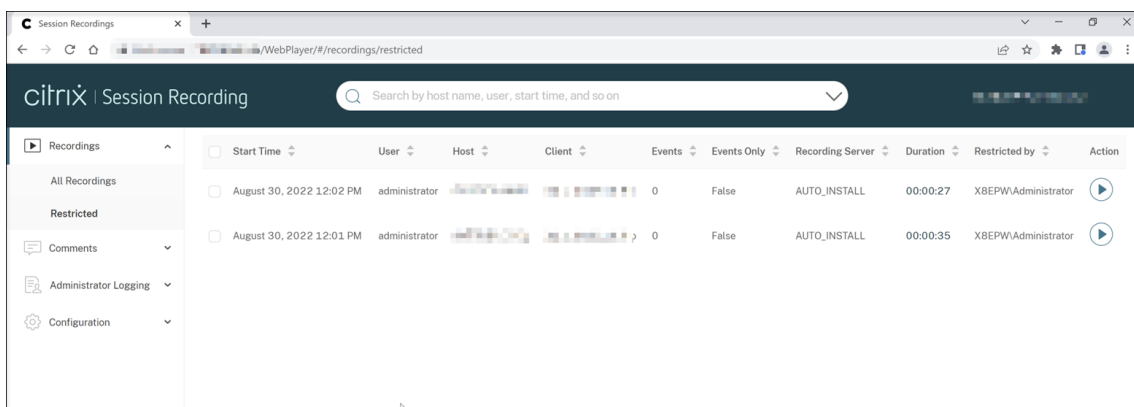


5. Cliquez sur **Confirmer**.



6. Vérifiez que les enregistrements sélectionnés pour lesquels vous avez imposé des restrictions d'accès sont déplacés de la page **Tous les enregistrements** vers la page **Restreint**.

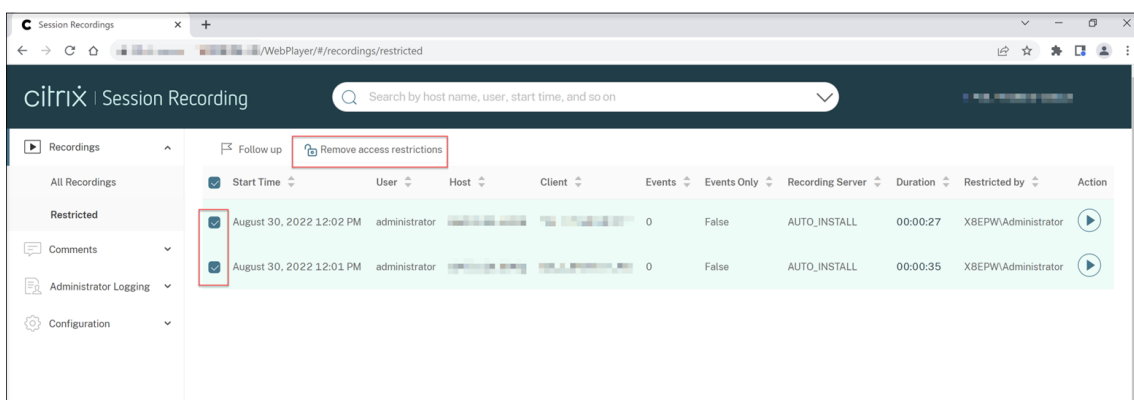
La colonne **Restreint par** indique qui a imposé des restrictions d'accès aux enregistrements concernés.



The screenshot shows the Citrix Session Recording interface. The left sidebar contains navigation options: Recordings, All Recordings, Restricted, Comments, Administrator Logging, and Configuration. The main area displays a table of recordings. The 'Restricted by' column shows 'XBEPW\Administrator' for both entries.

Start Time	User	Host	Client	Events	Events Only	Recording Server	Duration	Restricted by	Action
August 30, 2022 12:02 PM	administrator	[redacted]	[redacted]	0	False	AUTO_INSTALL	00:00:27	XBEPW\Administrator	[play icon]
August 30, 2022 12:01 PM	administrator	[redacted]	[redacted]	0	False	AUTO_INSTALL	00:00:35	XBEPW\Administrator	[play icon]

7. Sur la page **Restreint**, supprimez des restrictions d'accès si nécessaire. Une fois les restrictions d'accès supprimées, les enregistrements réapparaissent sur la page **Tous les enregistrements**.



The screenshot shows the Citrix Session Recording interface with the 'Remove access restrictions' button highlighted in a red box. The table below shows the recordings, with the 'Restricted by' column now empty, indicating that the restrictions have been removed.

Start Time	User	Host	Client	Events	Events Only	Recording Server	Duration	Restricted by	Action
August 30, 2022 12:02 PM	administrator	[redacted]	[redacted]	0	False	AUTO_INSTALL	00:00:27		[play icon]
August 30, 2022 12:01 PM	administrator	[redacted]	[redacted]	0	False	AUTO_INSTALL	00:00:35		[play icon]

Ouvrir et lire des enregistrements

February 20, 2024

Vous pouvez lire des enregistrements actifs et terminés dans le lecteur Web. Sur la page des enregistrements, chaque enregistrement comporte un bouton de lecture sur le côté droit, à côté de l'élément **Durée**.

Recordings	Start Time	User	Host	Client	Events	Duration	Action
All Recordings	February 23, 2021 3:17 PM	administrator			0	Live	▶
Comments	February 23, 2021 3:05 PM	administrator			0	00:08:14	▶
Administrator Logging	February 23, 2021 2:55 PM	qh			0	00:03:12	▶
Configuration	February 23, 2021 2:50 PM	qh			0	00:01:54	▶
	February 23, 2021 2:43 PM	qh			0	Live	▶

Conseil :

Pour le rôle **Player**, le menu **Enregistrements** dans le menu de navigation de gauche affiche uniquement le sous-menu **Tous les enregistrements**.









Pour le rôle **PrivilegedPlayer**, le menu **Enregistrements** affiche à la fois les sous-menus **Tous les enregistrements** et **Restreint**.

Cliquez sur le bouton de lecture. La page de lecture apparaît. La lecture démarre après la mise en cache de la mémoire.

Conseil :

- Lorsque vous cliquez sur l'heure de progression de la session, vous passez à la date/l'heure absolue à laquelle la session a été enregistrée.
- Pour un enregistrement d'événement uniquement, l'icône de lecture dans le coin supérieur gauche n'est pas disponible.

Pour obtenir une description des contrôles du lecteur, consultez le tableau suivant :

Contrôle du lecteur	Description
	<p>Lit le fichier d'enregistrement sélectionné.</p>
	<p>Suspend la lecture.</p>
	<p>Vous pouvez faire glisser la barre de progression pendant la lecture. Les périodes d'inactivité des sessions enregistrées sont mises en surbrillance pendant la lecture.</p>
	<p>Recherche en arrière (7 secondes).</p>
<p>00:00:00/00:02:17</p>	<p>Indique la position actuelle de la lecture de l'enregistrement et la durée totale de l'enregistrement. Le format de l'heure est HH:MM:SS.</p>
 <p>Comments</p>	<p>Permet de cliquer et de laisser un commentaire sur l'enregistrement en cours de lecture.</p>
 <p>Share Current Playback</p>	<p>Permet de cliquer et de copier l'URL de l'enregistrement en cours dans le Presse-papiers.</p>
 <p>Show stats</p>	<p>Affiche la superposition qui présente des points de données liés à la session enregistrée.</p>
 <p>Hide stats</p>	<p>Masque la superposition des données de session.</p>
<p>X 1</p>	<p>Indique la vitesse actuelle de lecture. Cliquez sur l'icône pour basculer entre les options X0.5, X1, X2 et X4.</p>
<p>FULL SCREEN</p>	<p>Affiche la lecture en plein écran.</p>
<p>Exit full screen</p>	<p>Affiche la lecture dans la page Web.</p>

Dans le panneau droit de la page de lecture, les filtres **Événements** et **Commentaires**, la zone de recherche rapide et certaines données d'enregistrement sont disponibles :

The screenshot displays a session recording interface. At the top, it shows the date **FEB 23, 2021** and the session duration **11:10:58 · 00:07:32 · 11 Events**. Below this, there is a circular profile icon with the letter 'Q' and three fields for user information: 'User name:', 'Host name:', and 'Client name:', each followed by a redacted grey box. A 'Sort by All Categories' dropdown menu is visible. Below the menu are search filters: a 'Filters' dropdown and a 'Search All Categories' search bar with a magnifying glass icon. The main area contains a list of events, each with a mouse cursor icon on the left and a dropdown arrow on the right. The events listed are:

- 00:00:00 Alert
Notification:Session Start
- 00:00:59 App Start:5692:
powershell: 8352: "C:\Win...
- 00:01:00 App Start:8416:
conhost: 5692: \??\C:\Win...
- 00:01:36 Session Pause:s;k;;
- 00:02:27 Session Resume:l;;;
- 00:03:02 Session Pause:/help;;;
- 00:03:19 Session Resume:hj;;;

- Date et heure sur la machine du lecteur Web. Dans cet exemple, **AUG 20, 2021** et **18:50:50**.
- Durée de l'enregistrement en lecture. Dans cet exemple, **01:37:00**.
- Nombre d'événements dans l'enregistrement. Dans cet exemple, **359 EVENTS**.
- Nom de l'utilisateur dont la session a été enregistrée.
- Nom d'hôte du VDA dans lequel la session enregistrée a été hébergée.
- Nom de la machine cliente sur laquelle la session a été exécutée.
- Options de tri des résultats de recherche : sélectionnez **Tous**, **Événements** ou **Commentaires** pour trier les résultats de recherche.

- **Filtres d'événements.** Vous pouvez sélectionner plusieurs filtres pour rechercher des événements dans l'enregistrement en cours.

Cliquez sur l'icône pour développer l'affichage des événements. Par exemple :

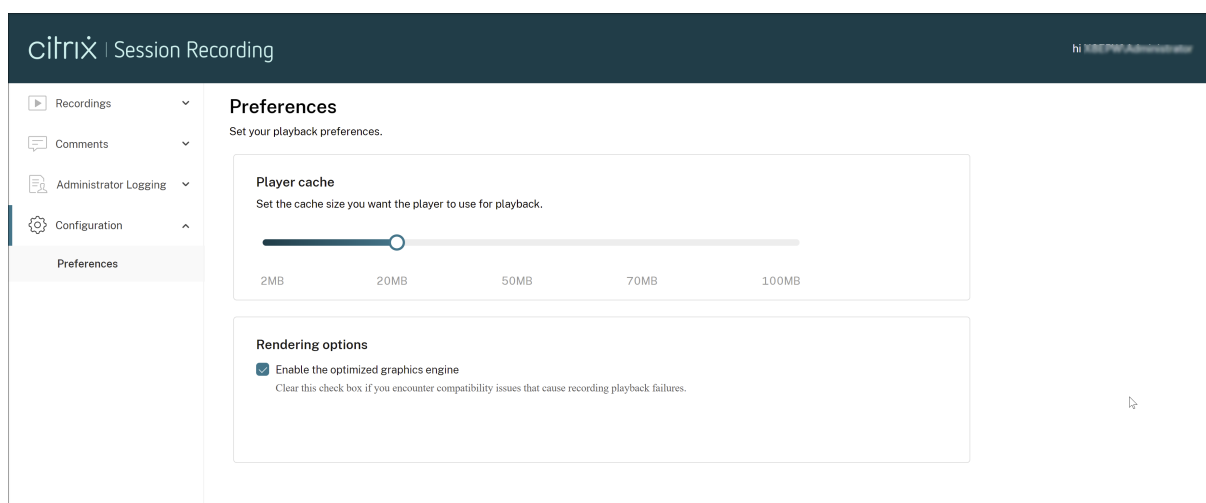


- **Liste des événements.** Lorsque vous cliquez sur un événement dans la liste, vous êtes dirigé vers la position de l'événement dans l'enregistrement.
- **Zone de recherche rapide.** La zone de **recherche rapide des événements** permet de réduire rapidement une liste d'événements dans l'enregistrement en cours.

Configurer les préférences

February 20, 2024

Pour configurer les préférences de votre lecteur Web, accédez à **Configuration > Préférences** sur la page du lecteur Web.



Vous pouvez configurer les préférences suivantes pour votre lecteur Web :

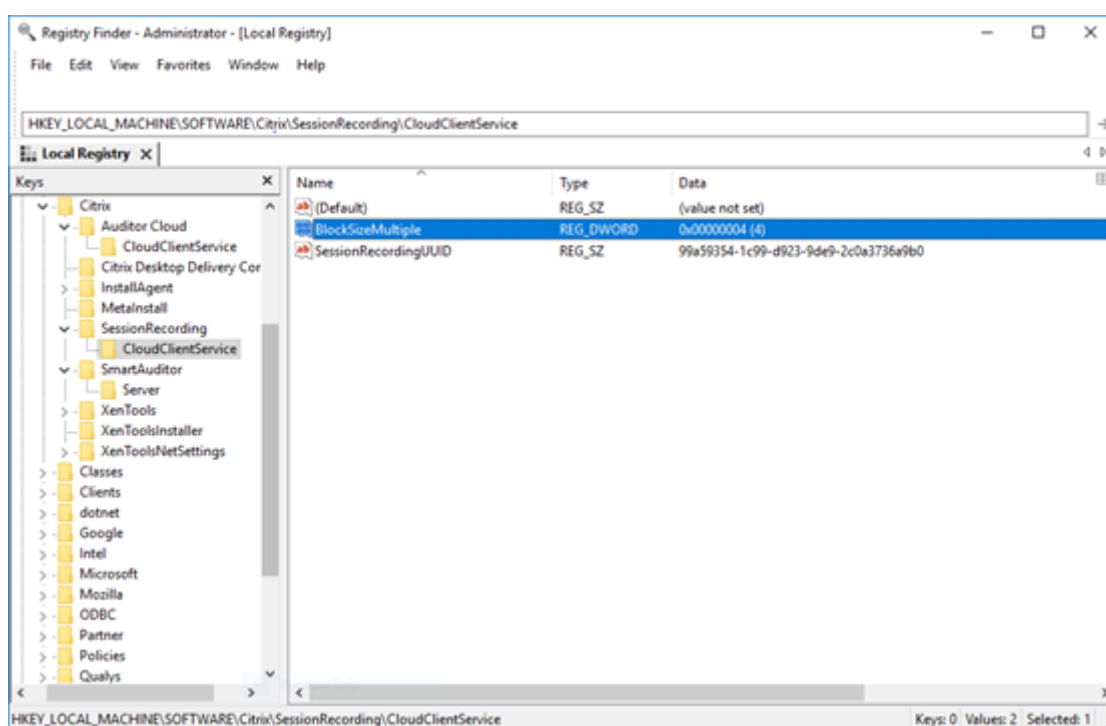
- **Cache du lecteur.** Faites glisser le curseur pour définir la taille du cache que le lecteur doit utiliser pour la lecture.
- **Moteur graphique optimisé.** Nous avons optimisé le moteur graphique pour améliorer les performances du lecteur Web. Le moteur optimisé est activé par défaut. Si vous rencontrez des problèmes de compatibilité ou d'autres problèmes avec le moteur optimisé, vous pouvez le désactiver en désélectionnant la case à cocher.

Augmenter la taille du paquet de transport pour le lecteur Web

December 21, 2022

1. Recherchez le fichier de configuration **Web** sous <Session Recording installation path>/WebSocketServer.
2. Ouvrez le fichier de configuration **Web**.
3. Modifiez la valeur **BlockSizeMultiple**.

La valeur par défaut est 1 (4 Ko). Nous vous recommandons de définir la valeur sur 8 (32 Ko).



Afficher les périodes d'inactivité

December 21, 2022

L'enregistrement de session peut enregistrer les événements inactifs et mettre en surbrillance les périodes d'inactivité dans le lecteur Web.

Conseil :

Les événements inactifs ne sont pas visibles dans le lecteur d'enregistrement de session car les

événements inactifs sont enregistrés dans la base de données d'enregistrement de session, mais pas dans les fichiers d'enregistrement correspondants (fichiers `.icl`).

Pour personnaliser la fonctionnalité d'événements inactifs, définissez les clés de registre suivantes dans `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEvents`.

Clé de registre	Valeur par défaut	Description
<code>DisableIdleEvent</code>	0	Pour désactiver la fonctionnalité d'événement inactif, définissez la valeur sur 1 . Pour activer la fonctionnalité d'événement inactif, définissez la valeur sur 0 .
<code>IdleEventThrottle</code>	30 secondes	S'il n'y a pas d'activité utilisateur (y compris les modifications graphiques et les entrées clavier/souris) pendant une période plus longue que le seuil défini par la clé de registre, un événement inactif est enregistré. La période d'inactivité est mise en surbrillance lorsque la session enregistrée est lue sur le lecteur Web de l'enregistrement de session.
<code>IdleEventActiveThrottle</code>	2 secondes	Seul un nombre spécifique de modifications graphiques dans un laps de temps donné sont considérées comme des activités utilisateur. Par défaut, au moins trois paquets en 2 secondes peuvent être considérés comme des activités utilisateur.

Clé de registre	Valeur par défaut	Description
IdleEventActivePktNumThrottle	3 paquets	Seul un nombre spécifique de modifications graphiques dans un laps de temps donné sont considérées comme des activités utilisateur. Par défaut, au moins trois paquets en 2 secondes peuvent être considérés comme des activités utilisateur.
IdleEventActivePktSizeThrottle	300 octets	Les paquets graphiques inférieurs à la valeur clé sont ignorés et la durée de temps correspondante est considérée comme inactive.

Utiliser les événements et les commentaires

February 20, 2024

Dans le panneau droit de la page de lecture, les filtres **Événements** et **Commentaires** sont disponibles. Vous pouvez utiliser des événements et des commentaires pour vous aider à naviguer à travers les sessions enregistrées dans le lecteur Web.

FEB 23, 2021
11:10:58 · 00:07:32 · 11 Events

User name: [REDACTED]
Host name: [REDACTED]
Client name: [REDACTED]

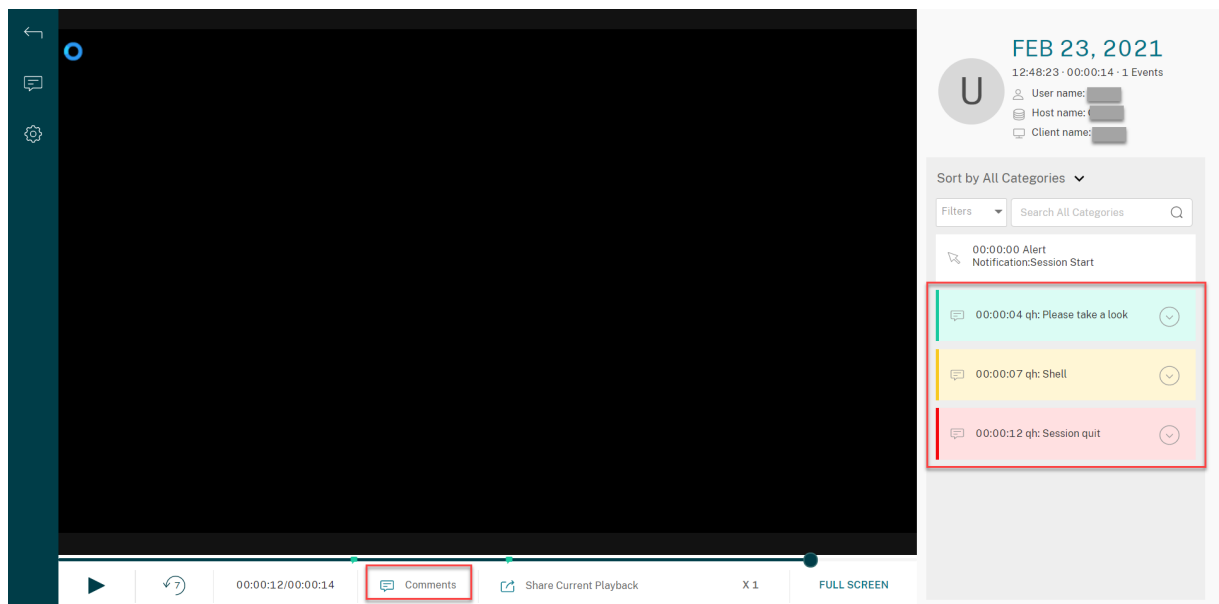
Sort by All Categories ▾

Filters ▾ Search All Categories 🔍

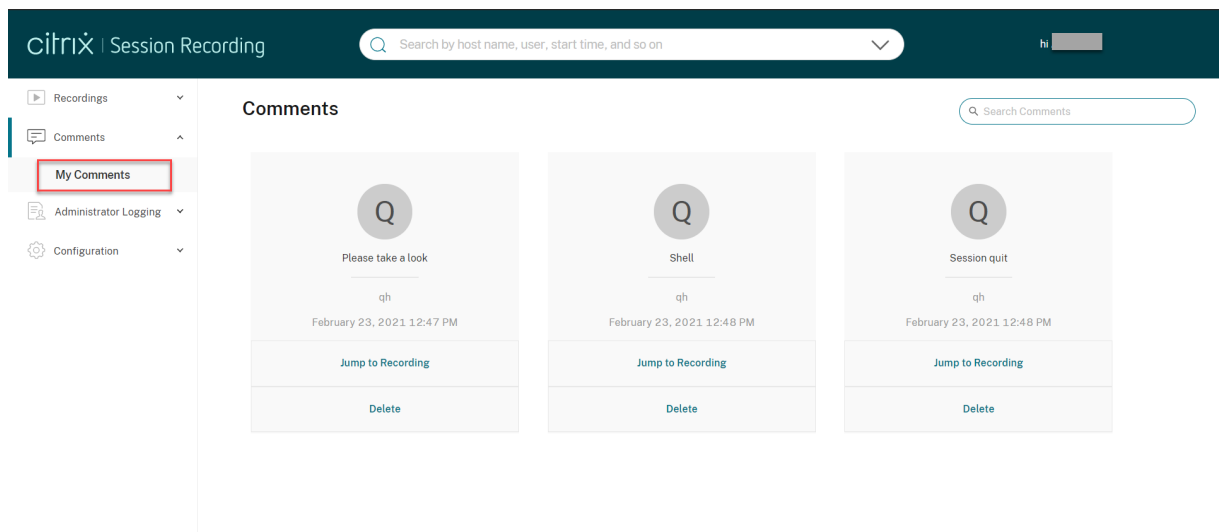
- 00:00:00 Alert
Notification:Session Start
- 00:00:59 App Start:5692:
powershell: 8352: "C:\Win... ⌵
- 00:01:00 App Start:8416:
conhost: 5692: \??\C:\Win... ⌵
- 00:01:36 Session Pause:s;k;;
- 00:02:27 Session Resume:l;;;
- 00:03:02 Session Pause:/help;;;
- 00:03:19 Session Resume:hj;;;

Commentaires sur les enregistrements

Lorsqu'une session enregistrée est en cours de lecture, vous pouvez cliquer sur le contrôle du lecteur **Commentaires** pour laisser des commentaires et définir le niveau de sévérité des commentaires. Les sévérités sont les suivantes : Normal, Moyenne et Grave. Les commentaires de sévérité Grave et Moyenne sont indiqués par des points rouge et orange, respectivement. Durant la lecture de session, vous pouvez afficher tous les commentaires relatifs à un enregistrement. Pour supprimer un commentaire que vous avez laissé, actualisez votre page Web, développez le commentaire, puis cliquez sur **Supprimer**.



En cliquant sur un commentaire, vous pouvez accéder à l'emplacement où le commentaire a été laissé. Vous pouvez afficher tous vos commentaires sur la page **Mes commentaires**.



Remarque :

pour que la fonctionnalité de commentaires fonctionne comme prévu, désactivez la case à cocher **Publication WebDAV** dans l'Assistant **Ajouter des rôles et des fonctionnalités** du Gestionnaire de serveur sur l'ordinateur sur le serveur d'enregistrement de session.

Add Roles and Features Wizard

Select server roles

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- Hyper-V
- MultiPoint Services
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS) (27 of 43 installed)
 - Web Server (21 of 34 installed)
 - Common HTTP Features (5 of 6 installed)
 - Default Document (Installed)
 - Directory Browsing (Installed)
 - HTTP Errors (Installed)
 - Static Content (Installed)
 - HTTP Redirection (Installed)
 - WebDAV Publishing
 - Health and Diagnostics (4 of 6 installed)
 - Performance (Installed)
 - Security (3 of 9 installed)

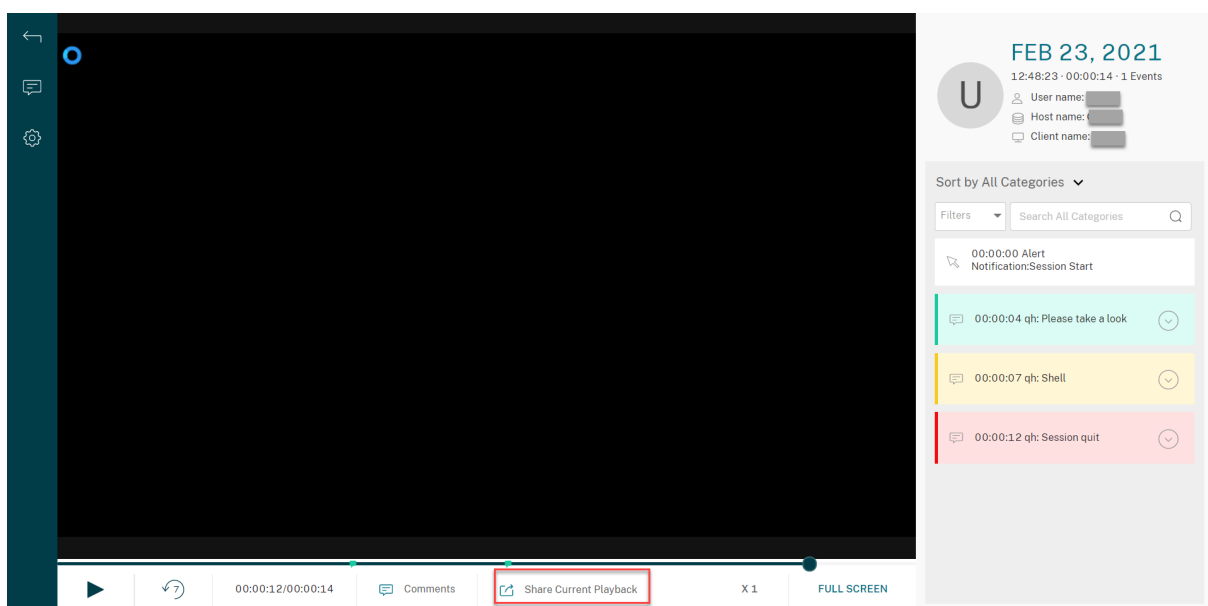
< Previous

Next >

Partager les URL des enregistrements

February 20, 2024

Cliquez sur **Partager lecture en cours** sur la page de lecture d'un enregistrement pour copier l'URL d'enregistrement dans le Presse-papiers. Vous pouvez partager l'URL avec d'autres utilisateurs pour qu'ils accèdent directement à l'enregistrement sans avoir besoin d'effectuer une recherche dans tous les enregistrements.



Après avoir cliqué sur **Partager lecture en cours**, vous verrez l'un des messages suivants indiquant une opération réussie ou ayant échoué respectivement :

- **L'URL de l'enregistrement partagé a été copiée dans le presse-papiers**
- **Le partage de l'URL de l'enregistrement a échoué**

Le collage de l'URL partagée dans la barre d'adresse vous permet d'accéder à l'emplacement où l'URL a été copiée.

Pour un partage sécurisé, définissez les valeurs de registre suivantes sous `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` :

Valeur de registre	Description	Valeur par défaut	Remarques
LinkExpire	Période au-delà de laquelle une URL partagée expire. Comptée en tant que valeur « timetick » dans l'unité de 10 microsecondes.	1 728 000 000 000 (La valeur par défaut est égale à 2 jours.)	-
LinkSalt	Méthode de sécurité pour protéger l'heure d'expiration de l'URL précédente.	Kk2od974	Modifiez la valeur par défaut en une chaîne arbitraire qui se termine de préférence par des chiffres.

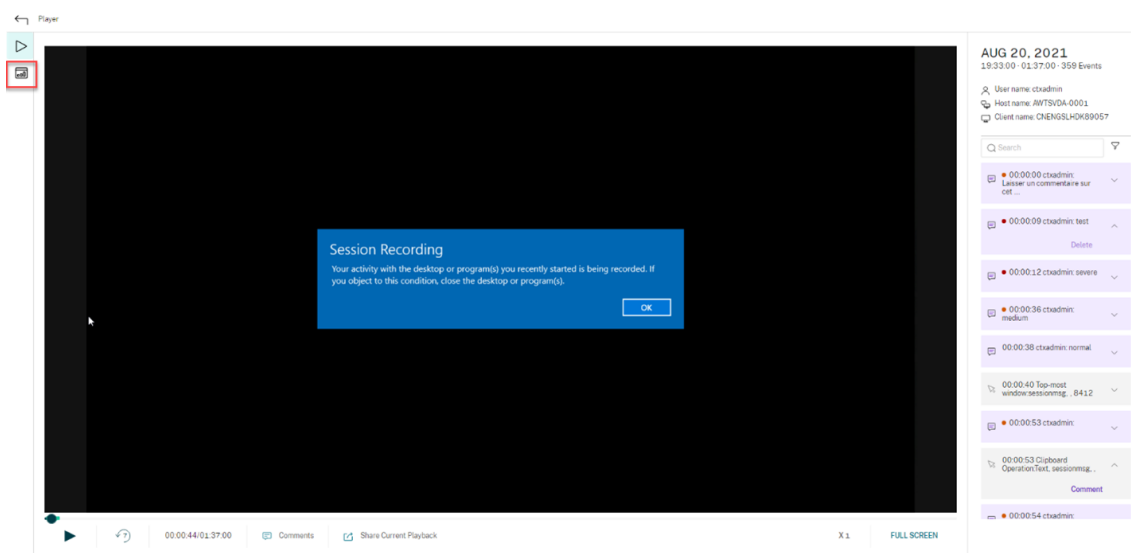
Afficher les statistiques d'événements graphiques pour chaque enregistrement

February 20, 2024

La visualisation des données d'événements est disponible dans le lecteur Web pour chaque enregistrement. Cela permet de fournir des statistiques graphiques sur les événements pour vous permettre de comprendre rapidement les événements insérés dans les enregistrements.

Pour afficher des statistiques d'événements graphiques, procédez comme suit :

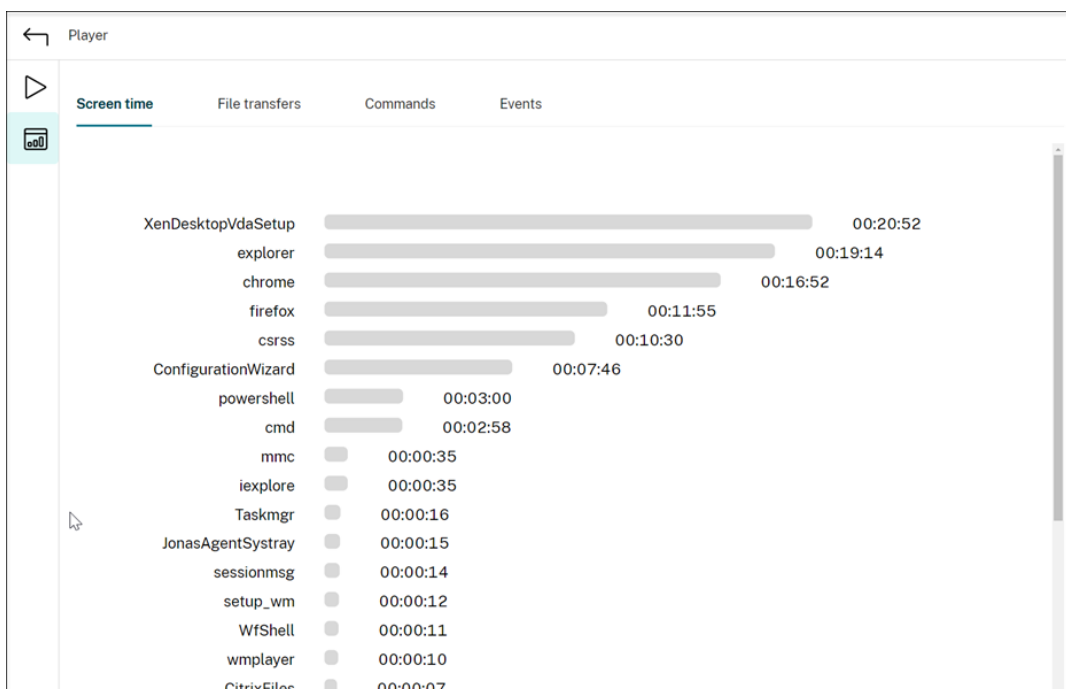
1. Ouvrez et lisez un enregistrement.
2. Dans le coin supérieur gauche de la page de lecture, cliquez sur l'icône Statistiques.



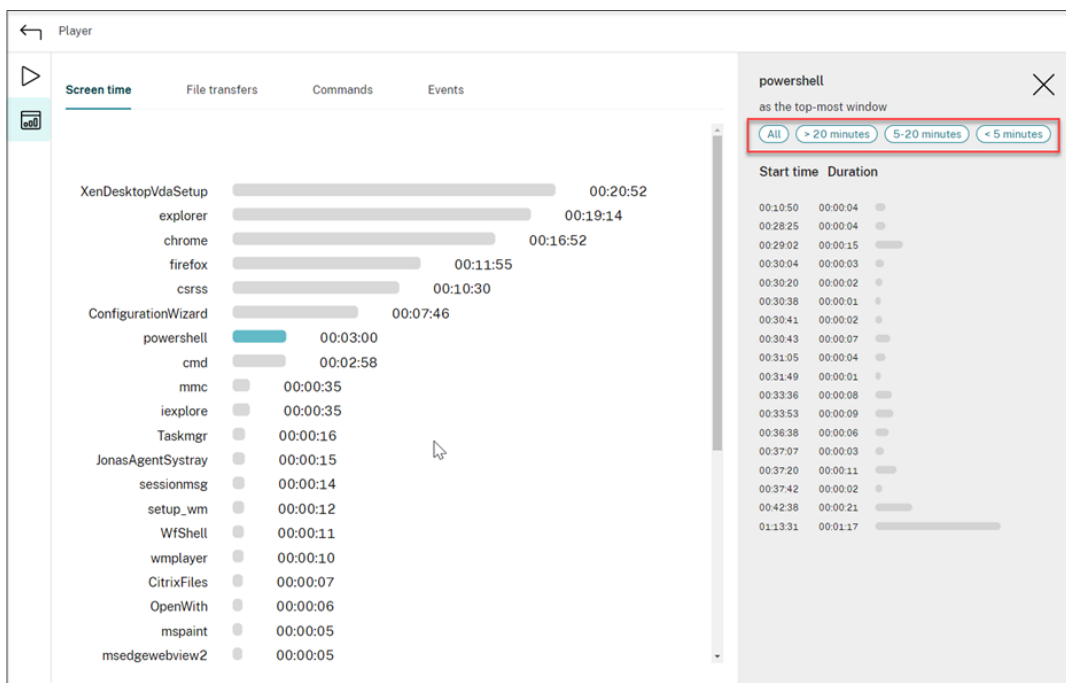
3. Basculez entre les onglets **Temps d'écran**, **Transferts de fichiers**, **Commandes** et **Événements** pour afficher des statistiques d'un point de vue différent.

- **Temps d'écran**

L'onglet **Temps d'écran** vous permet de connaître la durée cumulative pendant laquelle une fenêtre d'application est active.



Une barre de temps horizontale se trouve à côté de chaque application. Cliquez sur la barre pour afficher l'heure de début et la durée chaque fois que l'application devient et reste active, respectivement. Vous pouvez limiter votre plage de recherche en spécifiant une plage de durée autre que l'option par défaut **Tous**. Par exemple :



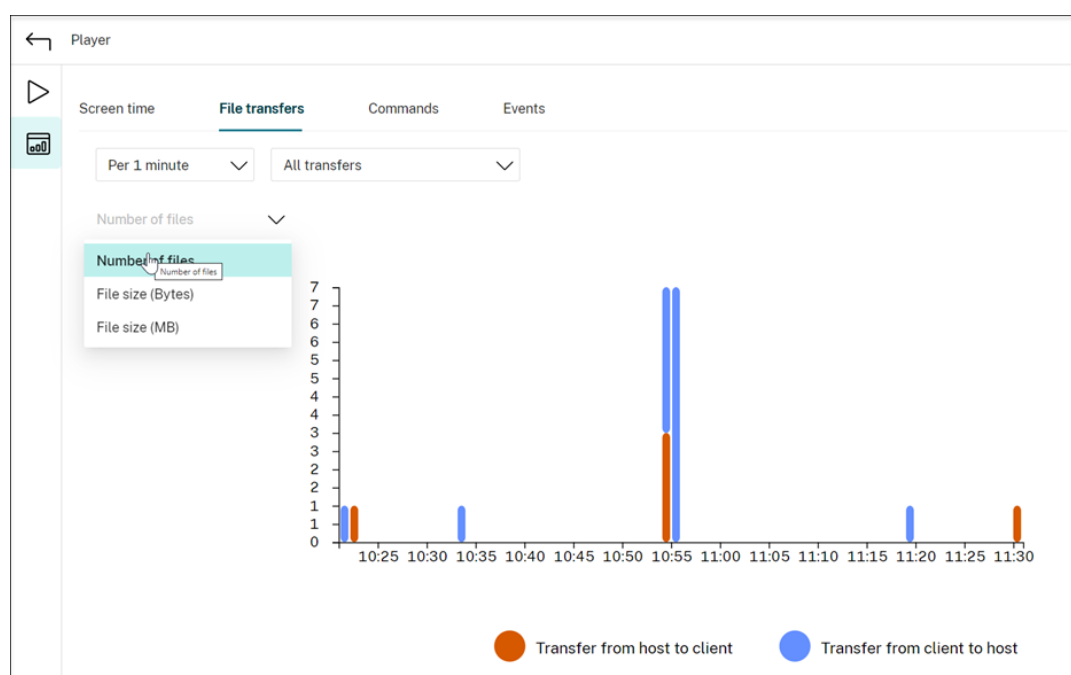
- **Transferts de fichiers**

L'onglet **Transferts de fichiers** fournit des statistiques graphiques sur les transferts

de fichiers bidirectionnels entre le VDA hébergeant la session enregistrée et la machine cliente sur laquelle la session est exécutée. Vous pouvez personnaliser la visualisation à l'aide des paramètres suivants :

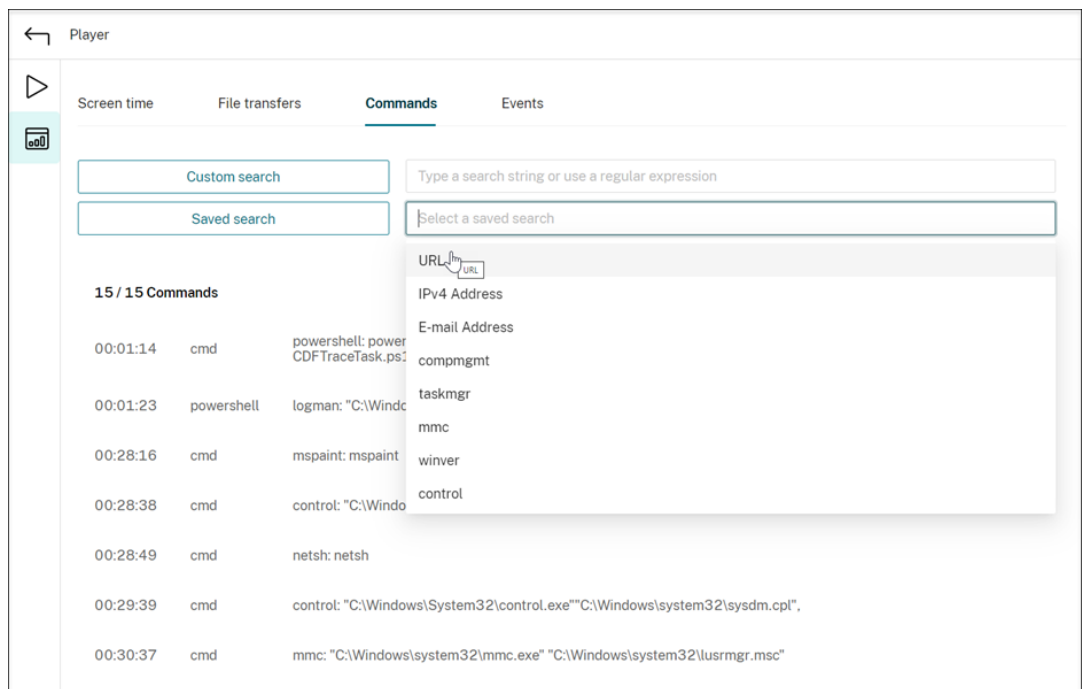
- Précision temporelle : **Par minute, Toutes les 10 minutes, Toutes les heures**
- Destination du transfert de fichiers : **Tous les transferts, Transfert de l'hôte au client, Transfert du client à l'hôte**
- Nombre ou taille (Octets ou Mo) des fichiers transférés

L'axe X représente l'heure absolue dans le système horaire de 24 heures.



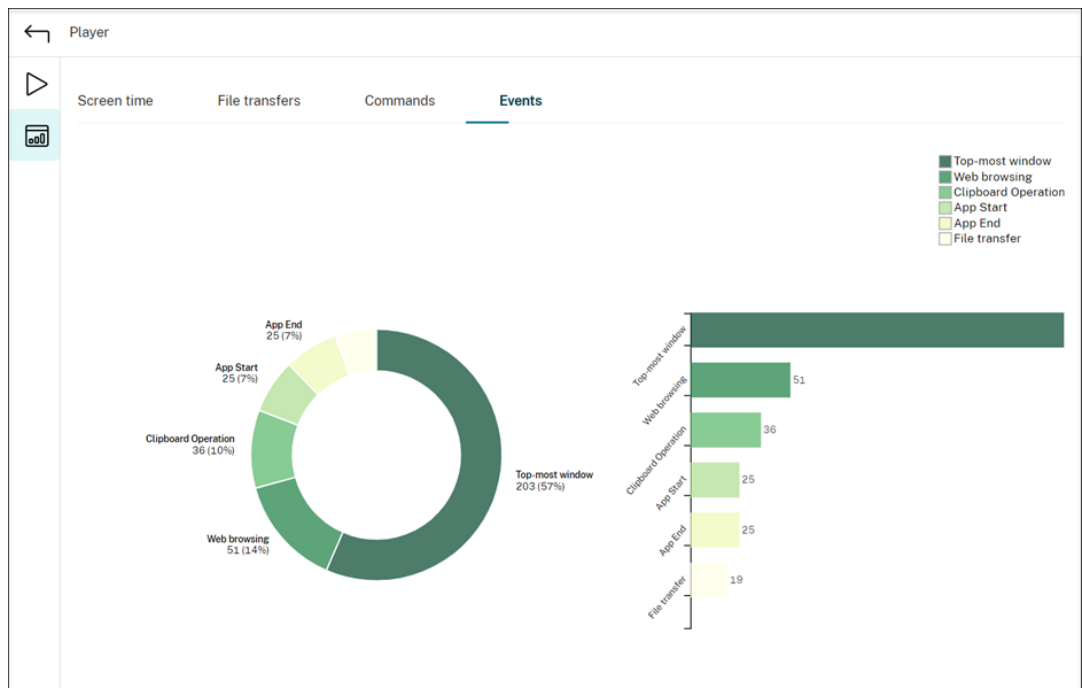
• Commandes

L'onglet **Commandes** affiche les commandes CMD et PowerShell qui sont exécutées pendant la session enregistrée. Vous pouvez personnaliser l'affichage des données en entrant votre recherche personnalisée dans **Recherche personnalisée** ou en sélectionnant une recherche enregistrée dans **Recherche enregistrée**. L'opérateur logique « OU » est utilisé pour calculer l'action finale.



• Événements

L'onglet **Événements** affiche les proportions et le nombre de tous les types d'événements dans la session enregistrée.

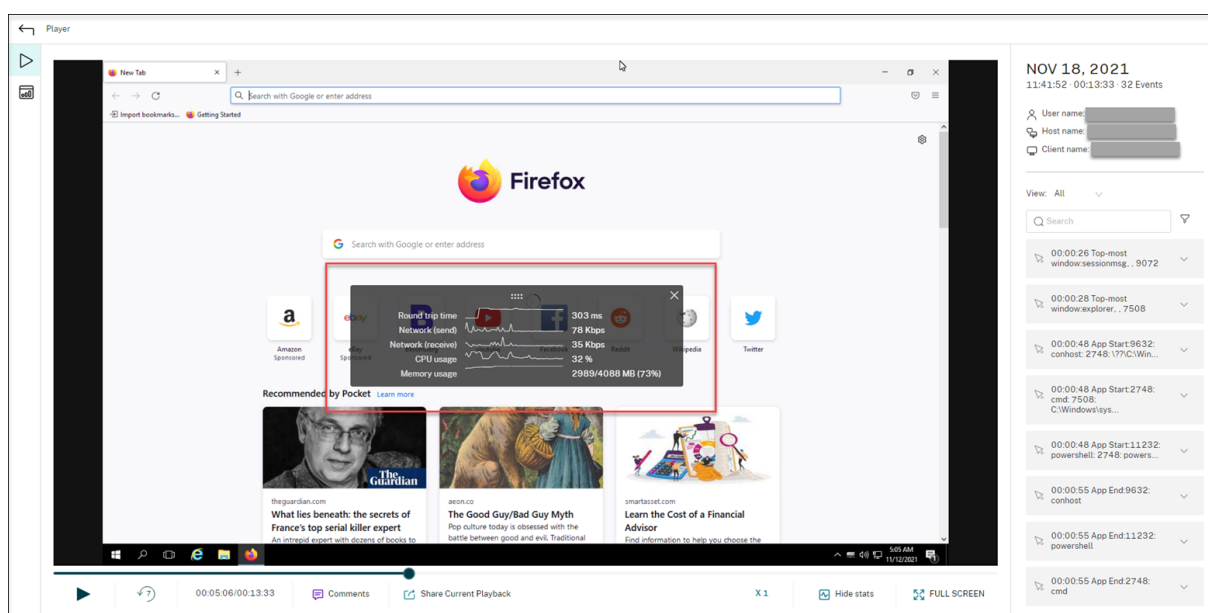


Afficher les points de données relatifs à chaque session enregistrée

February 20, 2024

Pendant la lecture, vous pouvez cliquer sur le contrôle **Afficher les statistiques** pour afficher, sur une superposition, les points de données suivants relatifs à la session enregistrée :

- Durée des boucles
- Réseau (envoi)
- Réseau (réception)
- Utilisation UC
- Utilisation de mémoire



Remarque :

- L'enregistrement de session collecte la durée des boucles toutes les 15 secondes et le reste des points de données toutes les secondes.
- Théoriquement, l'enregistrement de session actualise les données sur les durées des boucles toutes les cinq secondes. Toutefois, les données relatives à la durée des boucles sont actualisées toutes les 15 secondes en raison du cycle de collecte.
- L'enregistrement de session actualise le reste des points de données toutes les 5 secondes et présente leurs valeurs moyennes sur la superposition.

La superposition est **semi-transparente**. Vous pouvez la déplacer et la masquer.

- Pour déplacer la superposition, passez votre souris sur les huit points, puis effectuez un glisser-déposer.

- Pour masquer la superposition, cliquez sur **Masquer les statistiques**.

Vous pouvez activer la superposition en sélectionnant **Enregistrer les données de performances** lors de la création de votre stratégie de détection d'événements. Pour plus d'informations, consultez la section [Configurer les stratégies de détection d'événements](#).

Gérer les enregistrements

December 23, 2022

L'utilitaire de base de données de journalisation ICA (ICLDB) est un utilitaire de ligne de commande pour base de données utilisé pour la manipulation des éléments de base de données constitués d'enregistrements de sessions. Cet utilitaire est installé en même temps que l'enregistrement de session dans le dossier `\Program Files\Citrix\SessionRecording\Server\Bin` du serveur hébergeant le serveur d'enregistrement de session.

Tableau de référence rapide

Le tableau suivant contient la liste des commandes et des options disponibles avec l'utilitaire ICLDB. Tapez les commandes en utilisant le format suivant :

```
icldb [version | locate | dormant | import | archive | remove |  
removeall] command-options [/l] [/f] [/s] [/?]
```

Remarque :

Des instructions plus détaillées sont disponibles dans l'aide associée à l'utilitaire. Pour accéder à l'aide, à partir d'une invite de commandes, entrez le dossier `\Program Files\Citrix\SessionRecording\Server\Bin` et tapez

```
icldb /?. Pour accéder à l'aide de commandes spécifiques, tapez
```

```
icldb *command* /?.
```

Commande	Description
<code>archive</code>	Permet d'archiver les fichiers d'enregistrement de session plus anciens que la période de rétention spécifiée. Utilisez cette commande pour archiver les enregistrements et les événements dans les enregistrements. Les événements sont archivés dans la table de base de données <code>ArchivedEvent</code> .
<code>dormant</code>	Cette commande permet d'afficher ou de compter les fichiers d'enregistrement de session considérés comme dormants. Les fichiers dormants sont des enregistrements de session incomplets en raison d'une perte de données. Utilisez cette commande pour vérifier si vous suspectez une perte de données. Vous pouvez vérifier si les fichiers d'enregistrement de session deviennent dormants pour l'intégralité de la base de données ou si s'il ne s'agit que des enregistrements effectués pendant un certain nombre de jours, d'heures ou de minutes.
<code>import</code>	Permet d'importer les fichiers d'enregistrement de session dans la base de données d'enregistrement de session. Utilisez la commande pour reconstituer la base de données si vous perdez les enregistrements de la base de données. Vous pouvez également utiliser la commande pour fusionner des bases de données (si vous avez deux bases de données, vous pouvez importer les fichiers de l'une des bases de données).
<code>locate</code>	Permet de localiser et d'afficher le chemin complet vers un fichier d'enregistrement de session en utilisant l'identificateur de fichier comme critère. Utilisez cette commande lorsque vous cherchez l'emplacement d'un fichier d'enregistrement de session. Il s'agit aussi d'une manière de vérifier si la base de données est à jour par rapport à un fichier spécifique.

Commande	Description
<code>remove</code>	Permet de supprimer les références à des fichiers d'enregistrement de session de la base de données. Utilisez cette commande (prudemment) pour nettoyer la base de données. Spécifiez la période de rétention à utiliser comme critères. Vous pouvez également supprimer le fichier physique associé.
<code>removeall</code>	Cette commande supprime toutes les références aux fichiers d'enregistrement de session de la base de données d'enregistrement de session et rétablit l'état d'origine de la base de données. Les fichiers physiques ne sont pas supprimés ; il est toutefois impossible de les rechercher dans le lecteur d'enregistrement de session. Utilisez cette commande (prudemment) pour nettoyer la base de données. Les références supprimées ne peuvent être rétablies qu'en effectuant une restauration à partir des fichiers de sauvegarde.
<code>version</code>	Cette commande permet d'afficher la version du schéma de la base de données d'enregistrement de session.
<code>/l</code>	Cette commande enregistre les résultats et les erreurs dans le journal des événements Windows.
<code>/f</code>	Cette commande force l'exécution de la commande sans invites.
<code>/s</code>	Cette commande supprime le message de copyright.
<code>/?</code>	Cette commande affiche l'aide des commandes.

Archiver les anciens fichiers d'enregistrement de session

Pour maintenir un niveau adéquat de capacité de disque disponible dans les emplacements de stockage des enregistrements, archivez régulièrement les fichiers d'enregistrement de session. Les intervalles d'archivage diffèrent en fonction de la quantité d'espace disque disponible et de la taille typique des fichiers d'enregistrement. Les fichiers d'enregistrement de session doivent dater de plus de deux jours à compter de la date de début avant de pouvoir être archivés. Cette règle vise à empêcher

l'archivage d'enregistrements actifs avant qu'ils ne soient terminés.

Deux méthodes sont disponibles lorsque vous archivez des enregistrements de session. L'enregistrement de base de données pour un fichier d'enregistrement peut être mis à jour vers le statut d'archivage tant que le fichier reste à l'emplacement de stockage de l'enregistrement. Cette méthode peut être utilisée pour réduire les résultats de la recherche dans le lecteur. L'autre méthode consiste à mettre à jour l'enregistrement de la base de données d'un fichier d'enregistrement vers le statut archivé et à déplacer le fichier depuis l'emplacement de stockage de l'enregistrement vers un autre emplacement afin de le sauvegarder sur un autre support. Lorsque l'utilitaire ICLDB déplace les fichiers d'enregistrement de session, ceux-ci sont déplacés vers le répertoire spécifié, dans lequel la structure de dossiers d'origine, année/mois/jour, n'existe plus.

L'enregistrement dans la base de données d'enregistrement de session contient deux champs associés à l'archivage : l'heure d'archivage et la note d'archivage. L'heure d'archivage représente la date et l'heure actuelles auxquelles un enregistrement a été archivé. La note d'archivage est une note textuelle facultative qui peut être ajoutée lors de l'archivage. Les deux champs indiquent qu'un enregistrement a été archivé et l'heure d'archivage.

Dans le lecteur d'enregistrement de session, tous les enregistrements de session archivés indiquent l'état Archivé, ainsi que la date et l'heure de l'archivage. Les enregistrements de session archivés peuvent toujours être lus si les fichiers n'ont pas été déplacés. Si un fichier d'enregistrement de session a été déplacé lors de l'archivage, une erreur de fichier introuvable est affichée. Le fichier d'enregistrement de session doit être restauré avant que la session ne puisse être lue. Pour restaurer un fichier d'enregistrement de session, indiquez l'ID du fichier et l'heure d'archivage du fichier d'enregistrement. La restauration de fichiers archivés est abordée plus loin dans la section [Restaurer les fichiers d'enregistrement de session](#).

La commande **archive** de l'utilitaire ICLDB a plusieurs paramètres qui sont décrits comme suit :

- **/RETENTION:<jours>** - Période de rétention, en jours, des enregistrements de session. Les enregistrements plus anciens que le nombre de jours spécifié sont marqués comme archivés dans la base de données d'enregistrement de session. La période de rétention doit être un nombre entier supérieur ou égal à 2 jours.
- **/LISTFILES** –Répertorie le chemin complet et le nom des fichiers d'enregistrement de la session au fur et à mesure de leur archivage. Ce paramètre est facultatif.
- **/MOVETO:<répertoire\>** - Répertoire dans lequel vous déplacez physiquement les fichiers d'enregistrement de session archivés. Le répertoire spécifié doit exister. Ce paramètre est facultatif. Si aucun répertoire n'est spécifié, les fichiers restent dans leur emplacement de stockage d'origine.
- **/NOTE:<note>** - note de texte ajoutée à l'enregistrement de la base de données pour chaque enregistrement de session archivé. Assurez-vous que la note est entourée de guillemets. Ce paramètre est facultatif.

- **/L** - Enregistre les résultats et les erreurs dans le journal des événements Windows du nombre de fichiers d'enregistrement de session archivés. Ce paramètre est facultatif.
- **/F** - Cette commande force l'exécution de la commande sans invites. Ce paramètre est facultatif.

Pour archiver des enregistrements de session dans la base de données d'enregistrement de session et déplacer physiquement les fichiers d'enregistrement de session

1. Ouvrez une session en tant qu'administrateur local sur le serveur sur lequel le serveur d'enregistrement de session est installé.
2. Démarrez une invite de commande.
3. Passez du répertoire de travail actuel au répertoire Bin du chemin d'installation du serveur d'enregistrement de session (<Session Recording server Installation Path>/Server/Bin).
4. Exécutez la commande `ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /MOVETO:<directory> /NOTE:<note> /L` où **days** est la durée de rétention des fichiers d'enregistrement de session, **directory** est le répertoire dans lequel les fichiers d'enregistrement de session archivés sont déplacés, et **note** est la note de texte ajoutée à l'enregistrement de la base de données pour chaque fichier d'enregistrement de session archivé. Entrez **Y** pour confirmer l'archivage.

Pour archiver des enregistrements de session dans la base de données d'enregistrement de session uniquement

1. Ouvrez une session en tant qu'administrateur local sur le serveur sur lequel le serveur d'enregistrement de session est installé.
2. Démarrez une invite de commande.
3. Passez du répertoire de travail actuel au répertoire Bin du chemin d'installation du serveur d'enregistrement de session (<chemin d'installation du serveur d'enregistrement de session>/Server/Bin).
4. Exécutez la commande `ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /NOTE :<note> /L` où **days** est la durée de rétention des fichiers d'enregistrement de session et **note** est la note de texte ajoutée à l'enregistrement de la base de données pour chaque enregistrement de session archivé. Entrez **Y** pour confirmer l'archivage.

Restaurer les fichiers d'enregistrement de session

Pour afficher un fichier d'enregistrement archivé dans la base de données d'enregistrement de session et déplacé depuis l'emplacement de stockage de l'enregistrement, restaurez-le. Les enregistrements de session archivés qui n'ont pas été déplacés depuis l'emplacement de stockage des enregistrements pendant l'archivage sont toujours accessibles dans le lecteur d'enregistrement de session.

Deux méthodes sont disponibles pour restaurer les fichiers d'enregistrement de session qui ont été déplacés. Copiez le fichier d'enregistrement de session requis dans le répertoire de restauration pour fichiers archivés. Vous pouvez également réimporter le fichier d'enregistrement de session requis dans la base de données d'enregistrement de session à l'aide de l'utilitaire ICLDB. Nous vous recommandons la première méthode de restauration des fichiers d'enregistrement de session archivés. Supprimez les fichiers archivés copiés dans le répertoire de restauration lorsque vous n'en avez plus besoin.

Le broker d'enregistrement de session utilise le **répertoire de restauration pour fichiers archivés** lorsqu'un fichier d'enregistrement de session est introuvable dans son emplacement de stockage d'origine. Cela se produit lorsque le lecteur d'enregistrement de session demande la lecture d'un fichier d'enregistrement de session. Le broker d'enregistrement de session tente d'abord de trouver le fichier d'enregistrement de session dans l'emplacement de stockage d'origine. Si le fichier n'est pas trouvé dans l'emplacement de stockage d'origine, le broker vérifie ensuite le **répertoire de restauration pour fichiers archivés**. Si le fichier est présent dans le répertoire de restauration, le broker l'envoie au lecteur d'enregistrement de session pour le lire. Si le fichier n'est pas trouvé, le broker envoie une erreur de fichier non trouvé au lecteur d'enregistrement de session.

L'importation d'un fichier d'enregistrement archivé met à jour la base de données d'enregistrement de session avec les informations d'enregistrement de session du fichier, y compris un nouveau chemin de stockage. L'importation d'un fichier d'enregistrement de session archivé ne le déplace pas vers son emplacement de stockage d'origine lors de l'enregistrement de la session.

Remarque : l'heure d'archivage et la note d'archivage sont effacées dans la base de données d'enregistrement de session d'un fichier importé. Lors de la prochaine exécution de la commande ICLDB [archive](#), le fichier d'enregistrement de session importé peut être à nouveau archivé.

La commande ICLDB **import** est utile pour importer un grand nombre de fichiers d'enregistrement archivés. Elle peut réparer ou mettre à jour des données d'enregistrement de session incorrectes et manquantes dans la base de données d'enregistrement de session. Elle peut également déplacer des fichiers d'enregistrement de session d'un emplacement de stockage à un autre sur le serveur d'enregistrement de session. Vous pouvez utiliser la commande **import** de l'ICLDB pour remplir la base de données d'enregistrement de session avec des enregistrements de session après l'exécution de la commande ICLDB [removeall](#).

La commande **import** de l'utilitaire ICLDB a plusieurs paramètres qui sont décrits comme suit :

- **/LISTFILES** –Répertorie le chemin complet et le nom des fichiers d’enregistrement de la session au fur et à mesure de leur importation. Ce paramètre est facultatif.
- **/RECURSIVE** - Recherche dans tous les sous-répertoires les fichiers d’enregistrement de session. Ce paramètre est facultatif.
- **/L** - Enregistre les résultats et les erreurs dans le journal des événements Windows du nombre de fichiers d’enregistrement de session importés. Ce paramètre est facultatif.
- **/F** –Cette commande force l’exécution de la commande sans invites. Ce paramètre est facultatif.

Pour restaurer des fichiers d’enregistrement de session à l’aide du répertoire de restauration des fichiers archivés

1. Ouvrez une session en tant qu’administrateur local sur le serveur sur lequel le serveur d’enregistrement de session est installé.
2. Dans les propriétés du lecteur d’enregistrement de session, déterminez l’ID de fichier et l’heure d’archivage du fichier d’enregistrement de session archivé.
3. Localisez le fichier d’enregistrement de session dans vos sauvegardes à l’aide de l’ID de fichier spécifié dans les propriétés du lecteur d’enregistrement de session. Chaque enregistrement de session porte le nom de fichier `i_<FileID>.icl`, où FileID est l’ID du fichier d’enregistrement de session.
4. Copiez le fichier d’enregistrement de session de votre sauvegarde dans le répertoire de restauration pour fichiers archivés. Pour déterminer le répertoire de restauration pour fichiers archivés :
 - a) À partir du menu **Démarrer**, choisissez **Démarrer > Tous les programmes > Citrix > Propriétés du lecteur d’enregistrement de session**.
 - b) Dans la fenêtre **Propriétés du serveur d’enregistrement de session**, sélectionnez l’onglet **Stockage**. Le répertoire de restauration actuel apparaît dans le champ **Répertoire de restauration pour les fichiers archivés**.

Pour restaurer des fichiers d’enregistrement de session à l’aide de la commande d’importation ICLDB

1. Ouvrez une session en tant qu’administrateur local sur le serveur sur lequel le serveur d’enregistrement de session est installé.
2. Démarrez une invite de commande.

3. Passez du répertoire de travail actuel au répertoire Bin du chemin d'installation du serveur d'enregistrement de session (<Session Recording server installation path>/Server/Bin).
4. Vous pouvez au choix :
 - Exécutez la commande `ICLDB IMPORT /LISTFILES /RECURSIVE /L <directory>` où **directory** est le nom d'un ou de plusieurs répertoires, séparés par un espace, contenant des fichiers d'enregistrement de session. Entrez **Y** pour confirmer l'importation.
 - Exécutez la commande `ICLDB IMPORT /LISTFILES /L <file>` où **file** est le nom d'un ou de plusieurs fichiers d'enregistrement de session, séparés par un espace. Des caractères génériques peuvent être utilisés pour spécifier des fichiers d'enregistrement de session. Entrez **Y** pour confirmer l'importation.

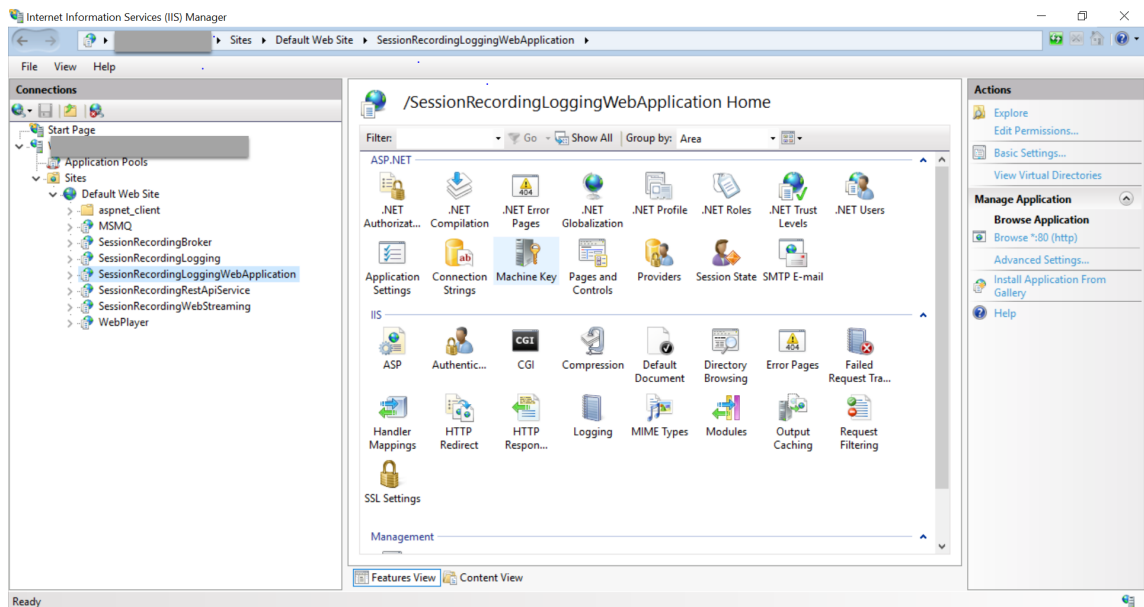
Gérer et interroger les journaux de l'administrateur

February 20, 2024

Interroger les données de la journalisation de l'administrateur

Exigences

- Un administrateur affecté aux rôles **LoggingReader** et **Player** peut consulter la journalisation de l'administrateur. Pour attribuer des utilisateurs aux rôles, accédez à la console d'autorisation d'enregistrement de session.
- La page de journalisation de l'administrateur est intégrée au lecteur Web. Le lecteur Web doit être installé pour pouvoir interroger la journalisation de l'administrateur. Dans le cas contraire, des erreurs 404 (page introuvable) peuvent se produire.
- La langue définie pour le navigateur du lecteur Web doit correspondre à la langue sélectionnée lors de l'installation des composants Administration de l'enregistrement de session.
- Assurez-vous que votre site SessionRecordingLoggingWebApplication sur IIS et le lecteur Web ont les mêmes paramètres SSL. Sinon, des erreurs 403 se produisent lorsque vous demandez l'accès aux données de journalisation de l'administrateur.



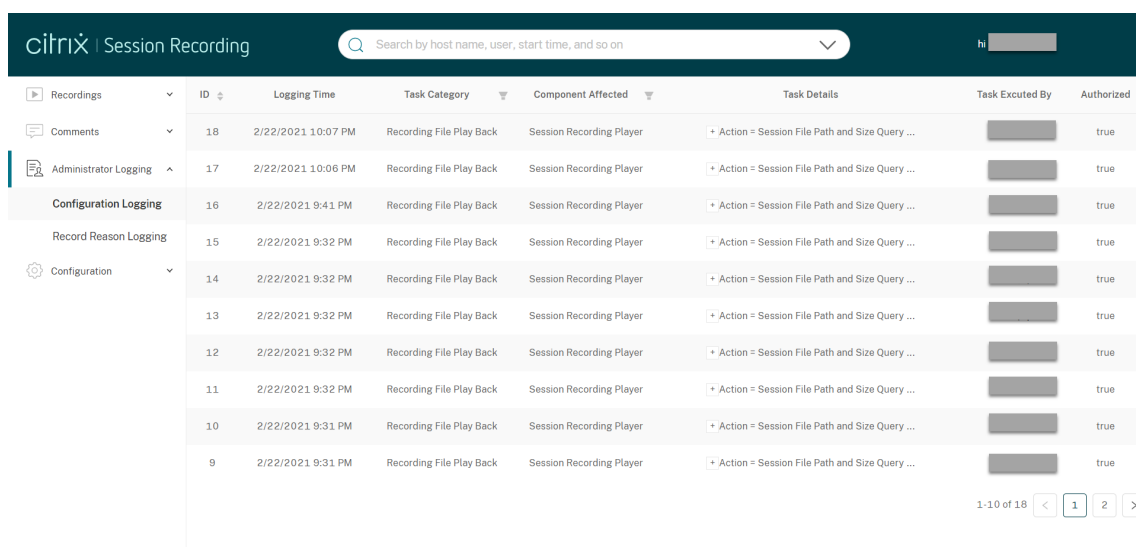
Étapes

Vous pouvez interroger les données de journalisation de l'administrateur concernant un serveur d'enregistrement de session à la fois depuis la machine qui héberge le serveur et depuis d'autres machines :

Sur la machine hébergeant le serveur d'enregistrement de session cible

1. À partir du menu **Démarrer**, choisissez **Journalisation de l'Administrateur d'enregistrement de session**.
2. Entrez les informations d'identification d'un utilisateur **LoggingReader**.

La page Web de journalisation de l'administrateur intégrée au lecteur Web s'affiche.



The screenshot shows the Citrix Session Recording interface. At the top, there is a search bar with the text "Search by host name, user, start time, and so on". Below the search bar is a table with the following columns: ID, Logging Time, Task Category, Component Affected, Task Details, Task Executed By, and Authorized. The table contains 10 rows of data, all with a "Recording File Play Back" task category and "Session Recording Player" component. The "Task Details" column for each row contains the text "+ Action = Session File Path and Size Query ...". The "Task Executed By" column is redacted with a grey box, and the "Authorized" column contains the value "true".

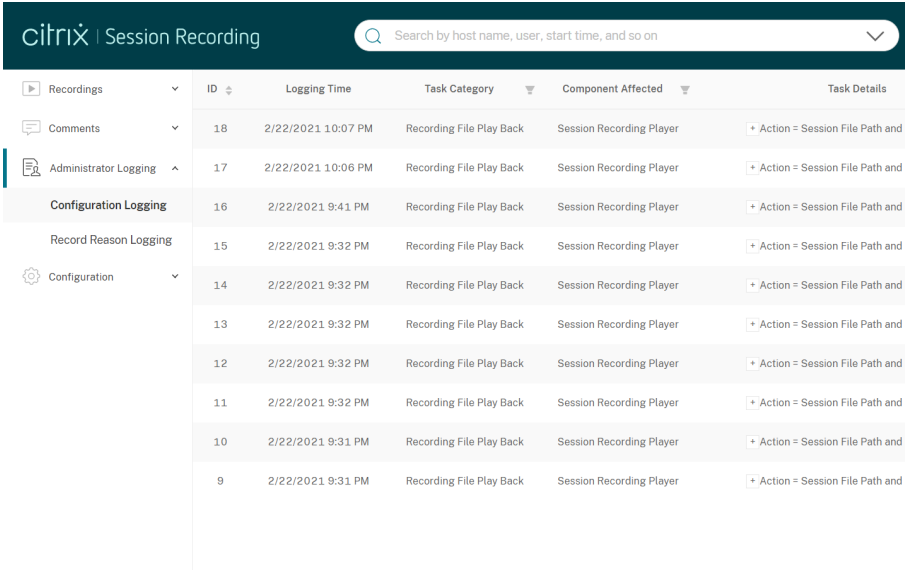
ID	Logging Time	Task Category	Component Affected	Task Details	Task Executed By	Authorized
18	2/22/2021 10:07 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
17	2/22/2021 10:06 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
16	2/22/2021 9:41 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
15	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
14	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
13	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
12	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
11	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
10	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true
9	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...	[Redacted]	true

Sur d'autres machines

1. Ouvrez un navigateur Web et accédez à la page Web de journalisation de l'administrateur.
 - **Pour HTTPS :** <https://servername/WebPlayer/#/logging/config> et <https://servername/WebPlayer/#/logging/record>, où **servername** correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
 - **Pour HTTP :** <http://servername/WebPlayer/#/logging/config> et <http://servername/WebPlayer/#/logging/record>, où **servername** correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
2. Entrez les informations d'identification d'un utilisateur **LoggingReader**.

Présentation des données de journalisation

Les données de journalisation de l'administrateur se composent de deux parties : la journalisation de la configuration et la journalisation du motif d'enregistrement



ID	Logging Time	Task Category	Component Affected	Task Details
18	2/22/2021 10:07 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
17	2/22/2021 10:06 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
16	2/22/2021 9:41 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
15	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
14	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
13	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
12	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
11	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
10	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and
9	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and

Journalisation de la configuration

Cette partie enregistre les activités suivantes de l'administrateur :

- **Modification du document de stratégie** : modifications apportées aux stratégies dans la console de stratégie d'enregistrement de session ou Citrix Director
- **Modification de la configuration du serveur** : modifications apportées aux propriétés du serveur d'enregistrement de session Citrix
- **Lecture du fichier d'enregistrement** : lecture des sessions enregistrées
- **Lecture du journal** : tentatives non autorisées d'accès aux données de journalisation de l'administrateur

Pour enregistrer les activités de l'administrateur, activez la journalisation de l'administrateur sur vos serveurs d'enregistrement de session. Pour plus d'informations, consultez [Désactiver ou activer la journalisation de l'administrateur](#). Pour renforcer la sécurité, vous pouvez également [configurer un compte de service de journalisation de l'administrateur](#).

Conseil :

Vous pouvez activer la journalisation de l'administrateur via le service d'enregistrement de session et via les propriétés du serveur d'enregistrement de session.

ID	Logging Time	Task Category	Component Affected
32	2/9/2021 1:26 AM	Event Logging Reason	Session Recording Agent
31	2/9/2021 1:26 AM	Email Alert Reason	Session Recording Agent
30	2/9/2021 1:26 AM	Record Reason	Session Recording Agent
29	2/9/2021 1:24 AM	Event Logging Reason	Session Recording Agent
28	2/9/2021 1:24 AM	Email Alert Reason	Session Recording Agent
27	2/9/2021 1:24 AM	Record Reason	Session Recording Agent
26	2/9/2021 1:21 AM	Event Logging Reason	Session Recording Agent
25	2/9/2021 1:21 AM	Email Alert Reason	Session Recording Agent
24	2/9/2021 1:21 AM	Record Reason	Session Recording Agent
23	2/9/2021 1:18 AM	Event Logging Reason	Session Recording Agent

Journalisation du motif de l'enregistrement

Cette partie enregistre les stratégies qui ont déclenché des enregistrements.

Pour activer cette fonctionnalité, activez la journalisation de l'administrateur et la journalisation du motif de l'enregistrement sur vos serveurs d'enregistrement de session. Si la journalisation de l'administrateur est désactivée, l'activation de la journalisation du motif de l'enregistrement ne prend pas effet.

Désactiver ou activer la journalisation de l'administrateur

Après l'installation, vous pouvez activer ou désactiver la fonctionnalité Journalisation de l'administrateur dans les **Propriétés du serveur d'enregistrement de session**.

1. Ouvrez une session en tant qu'administrateur sur la machine sur laquelle la journalisation de l'administrateur d'enregistrement de session est installée.
2. À partir du menu **Démarrer**, choisissez **Propriétés du serveur d'enregistrement de session**.
3. Cliquez sur l'onglet **Enregistrement**.

Lorsque la journalisation de l'administrateur d'enregistrement de session est désactivée, aucune nouvelle activité n'est consignée. Vous pouvez consulter les journaux existants à partir de l'interface Web.

Lorsque le **blocage obligatoire** est activé, les activités suivantes sont bloquées si la journalisation échoue. Un événement système est également consigné avec l'ID d'événement 6001 :

- Les modifications apportées aux stratégies d'enregistrement dans la console de stratégie d'enregistrement de session ou Citrix Director.
- Modifications apportées aux propriétés du serveur d'enregistrement de session Citrix

Le paramètre de blocage obligatoire n'a pas d'incidence sur l'enregistrement des sessions.

Configurer un compte de service de journalisation de l'administrateur

Par défaut, la journalisation de l'administrateur est exécutée en tant qu'application Web dans Internet Information Services (IIS) et son identité est Service réseau. Pour améliorer le niveau de sécurité, vous pouvez modifier l'identité de l'application Web vers un compte de service ou un compte de domaine spécifique.

1. Ouvrez une session en tant qu'administrateur sur la machine hébergeant le serveur d'enregistrement de session.
2. Dans le Gestionnaire des services Internet, cliquez sur **Pools d'applications**.
3. Dans **Pools d'applications**, cliquez avec le bouton droit sur **SessionRecordingLoggingApp-Pool**, et choisissez **Paramètres avancés**.
4. Modifiez l'attribut **identité** pour le compte que vous voulez utiliser.
5. Accordez au compte l'autorisation **db_owner** pour la base de données **CitrixSessionRecordingLogging** dans Microsoft SQL Server.
6. Accordez au compte le droit en lecture pour la clé de registre sur **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix**

Avertissement :

Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Désactiver ou activer la journalisation du motif de l'enregistrement

Par défaut, la journalisation de l'administrateur consigne chaque motif d'enregistrement de session une fois que la requête de stratégie est terminée. Ce cas peut générer un grand nombre de journaux. Pour améliorer les performances et économiser le stockage, désactivez ce type de journalisation dans le registre.

1. Ouvrez une session en tant qu'administrateur sur la machine hébergeant le serveur d'enregistrement de session.
2. Ouvrez l'Éditeur de Registre.
3. Accédez à **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.
4. Définissez la valeur de **EnableRecordingActionLogging** sur :
 - 0** : désactive la journalisation du motif de l'enregistrement
 - 1** : active la journalisation du motif de l'enregistrement

Recommandations

December 21, 2022

Vous pouvez consulter la documentation suivante sur les meilleures pratiques pour déployer l'enregistrement de session et configurer l'équilibrage de charge :

- [Configurer l'équilibrage de charge dans un déploiement existant](#)
- [Déployer et équilibrer la charge de l'enregistrement de session sur Azure](#)

Configurer l'équilibrage de charge dans un déploiement existant

February 20, 2024

Vous pouvez ajouter des nœuds d'équilibrage de charge à l'aide de Citrix ADC dans un déploiement d'enregistrement de session existant. Les serveurs suivants sont utilisés à titre d'exemple. Vous pouvez également [déployer et équilibrer la charge de l'enregistrement de session sur Azure](#)

- Enregistrement de session

Nom d'hôte	Rôle de serveur	OS	Adresse IP
SRSrver1	Serveur d'enregistrement de session	Windows Server	10.63.32.55
LBDC	Contrôleur de domaine	Windows Server	10.63.32.82
TSVDA	Agent d'enregistrement de session	Windows Server	10.63.32.215
SRSQL	Base de données d'enregistrement de session et serveur de fichiers	Windows Server	10.63.32.91

Tous les composants de l'enregistrement de session et le contrôleur de domaine partagent un domaine, par exemple, `lb.com`. Le compte d'administrateur de domaine, par exemple `lb\administrator`, est utilisé pour la connexion du serveur.

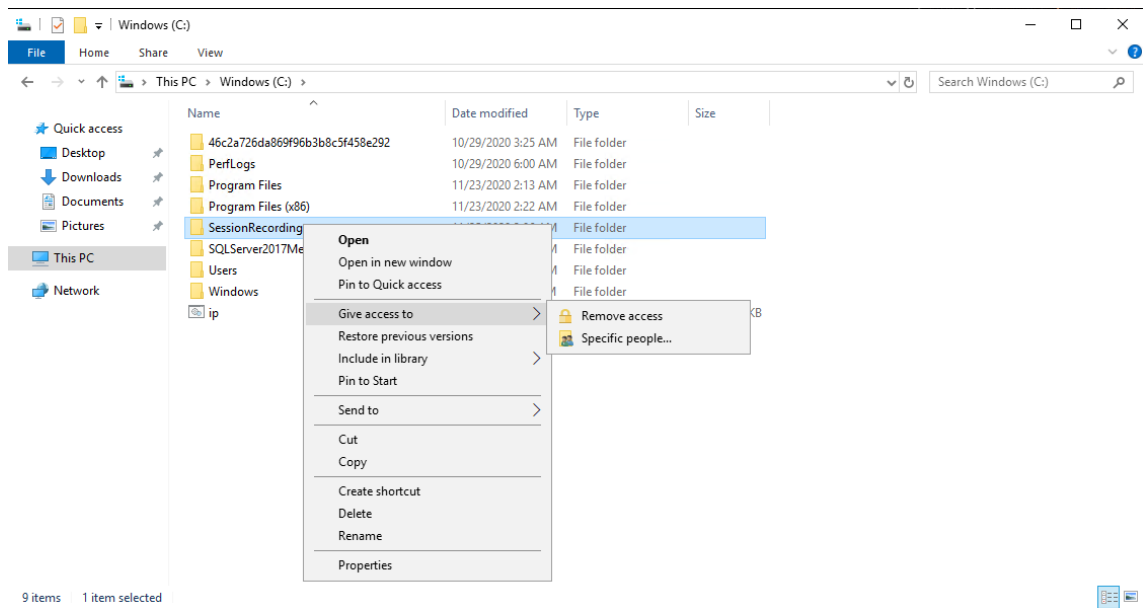
- Citrix ADC

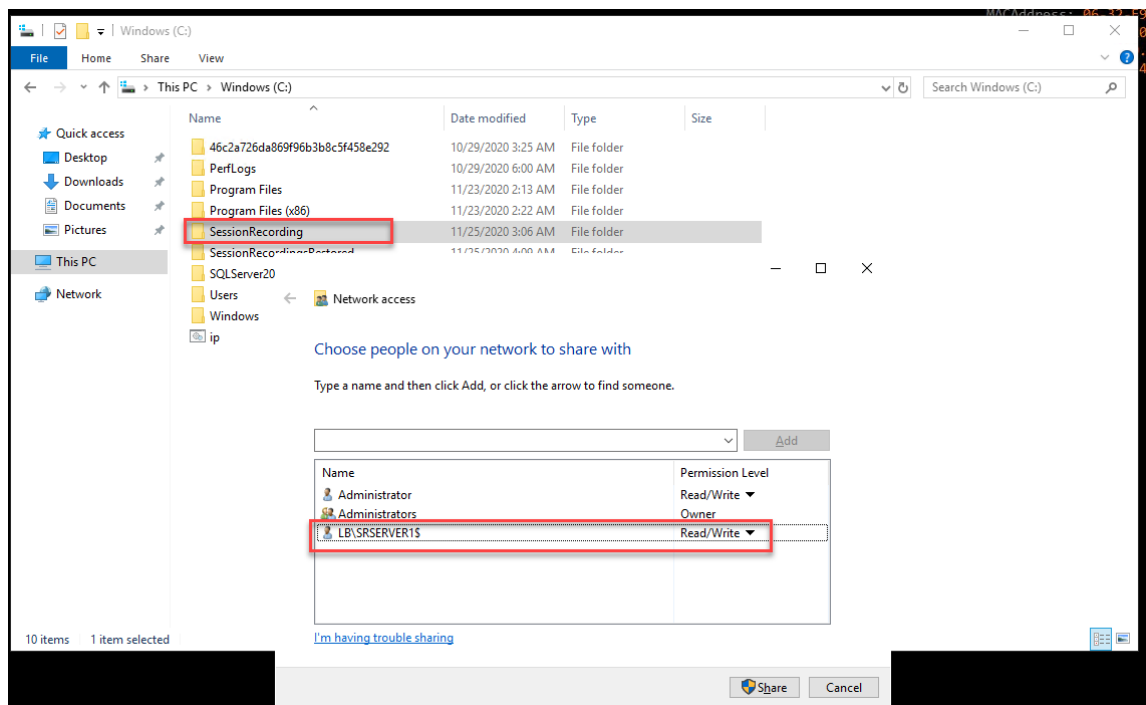
Nom d'hôte	Rôle de serveur	Adresse IP de gestion (NSIP)	Adresse IP du sous-réseau (SNIP)
NetScaler	Instance Citrix ADC VPX	10.63.32.40	10.63.32.109

Pour de plus amples informations, consultez la section [Déployer une instance de Citrix ADC VPX](#).

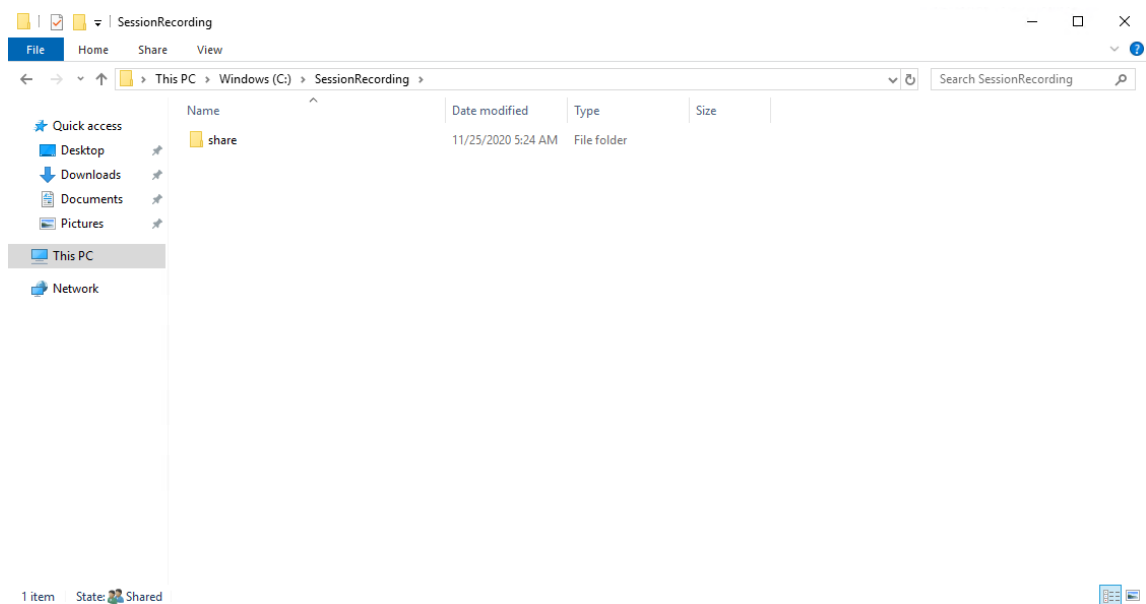
Étape 1 –Créer des dossiers partagés sur le serveur de fichiers

1. Connectez-vous au serveur de fichiers à l'aide d'un compte d'administrateur de domaine, par exemple `lb\administrator`.
2. Créez un dossier pour stocker les enregistrements et nommez le dossier `SessionRecording`, par exemple, `C:\SessionRecording`. Accordez l'autorisation de lecture/écriture du dossier à un serveur d'enregistrement de session. Par exemple, pour `SRServer1`, tapez `LB\SRSERVER1$`. Le signe dollar \$ est requis.





3. Créez un sous-dossier dans le dossier `SessionRecording` et nommez le sous-dossier `share`, par exemple, `C:\SessionRecording\share`.

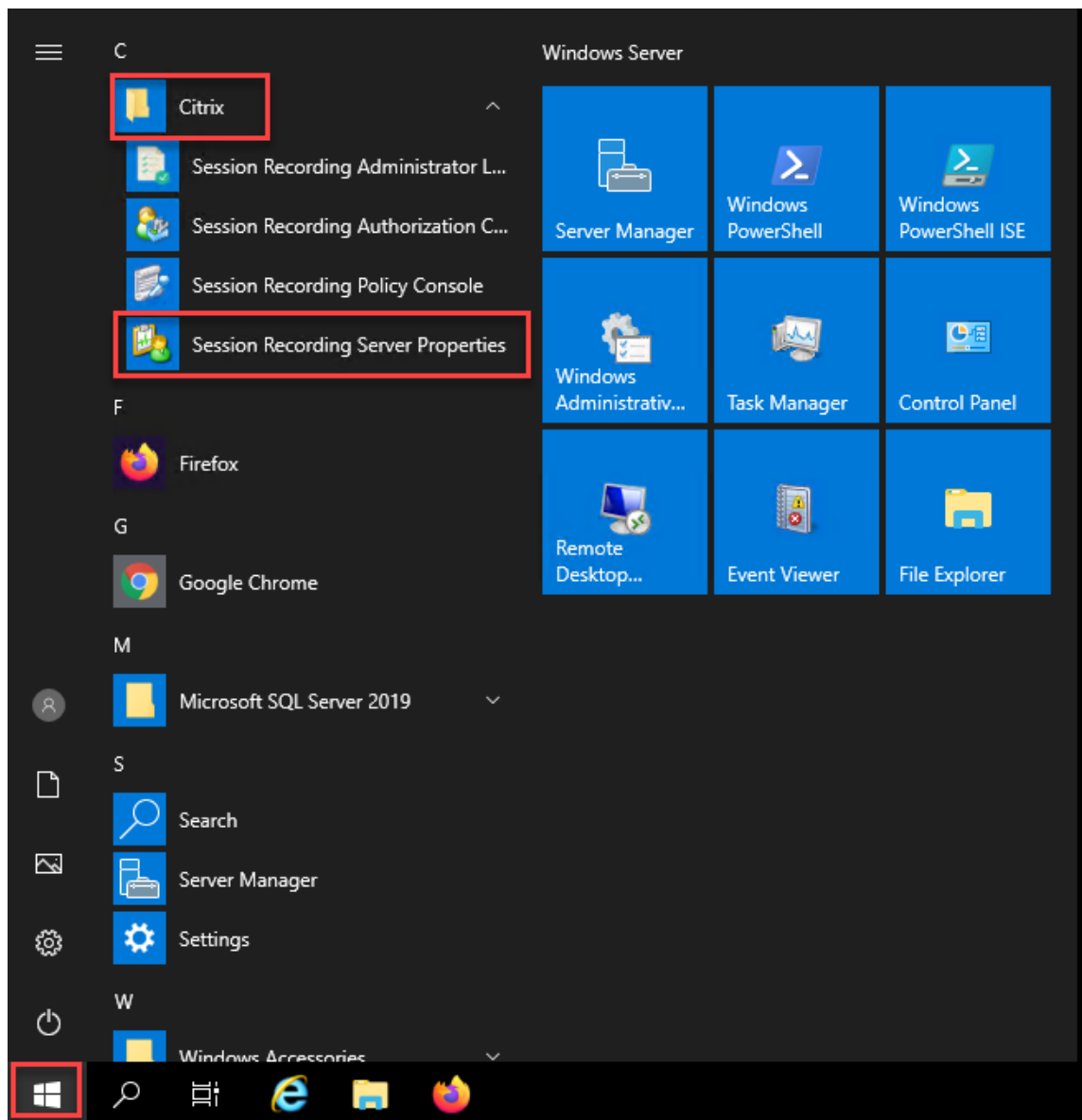


4. Créez un autre dossier pour restaurer les enregistrements archivés et nommez le dossier `SessionRecordingsRestored`, par exemple, `C:\SessionRecordingsRestored`. Accordez l'autorisation de lecture/écriture du dossier à un serveur d'enregistrement de session. Par exemple, pour `SRServer1`, tapez `LB\SRSERVER1$`. Le signe dollar `$` est requis.
5. Créez un sous-dossier dans le dossier `SessionRecordingsRestored` et nommez le sous-dossier `share`, par exemple, `C:\SessionRecordingsRestored\share`.

Étape 2 – Configurer un serveur d'enregistrement de session existant pour prendre en charge l'équilibrage de charge

Cette étape décrit comment configurer un serveur d'enregistrement de session existant pour prendre en charge l'équilibrage de charge. L'[Étape 7](#) détaille la procédure d'ajout d'autres serveurs d'enregistrement de session à votre déploiement existant.

1. Connectez-vous à un serveur d'enregistrement de session à l'aide d'un compte d'administrateur de domaine.
2. Ouvrez **Propriétés du serveur d'enregistrement de session**.

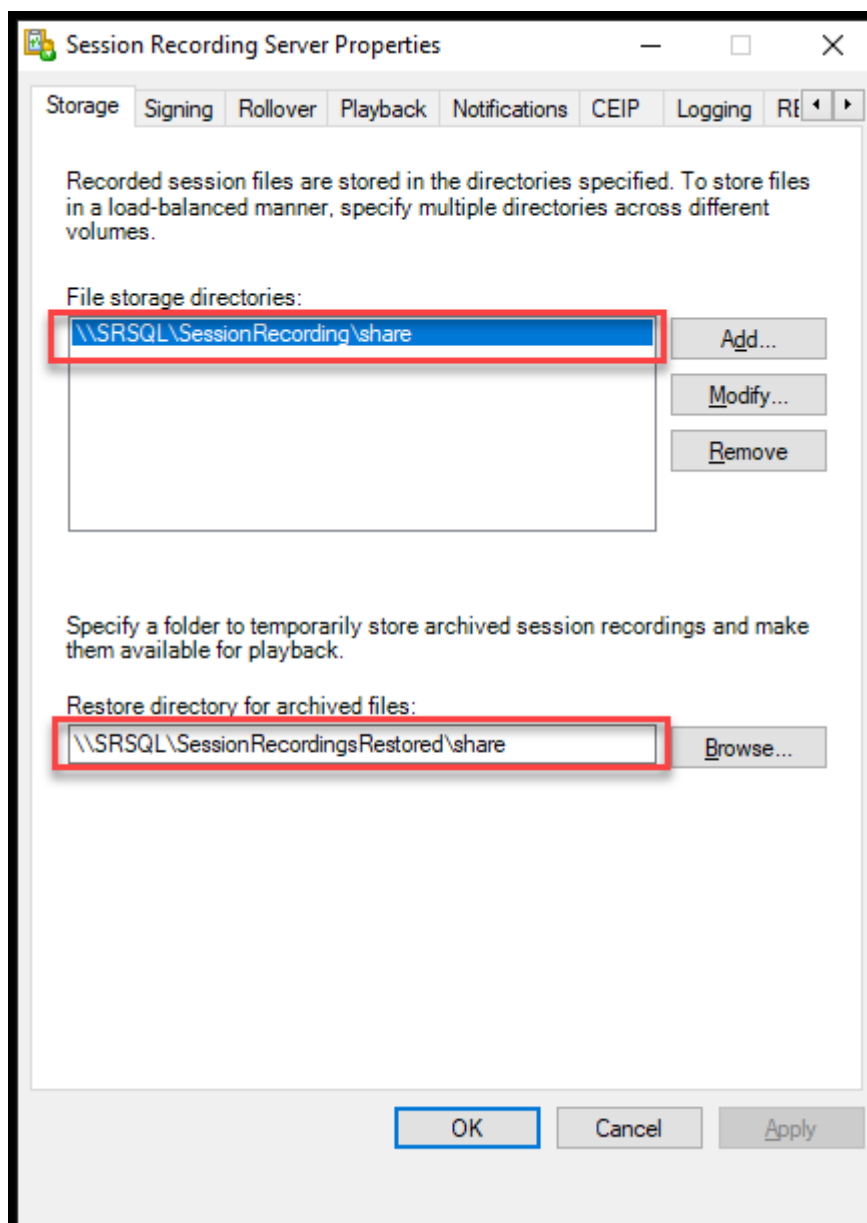


3. Ajoutez les chemins d'accès UNC (Universal Naming Convention) créés dans l'[Étape 1](#) pour stocker et restaurer les fichiers d'enregistrement, dans cet exemple, `\\SRSQL\`

SessionRecording\share et \\SRSQL\SessionRecordingRestored\share. SRSQL correspond au nom d'hôte du serveur de fichiers.

Remarque :

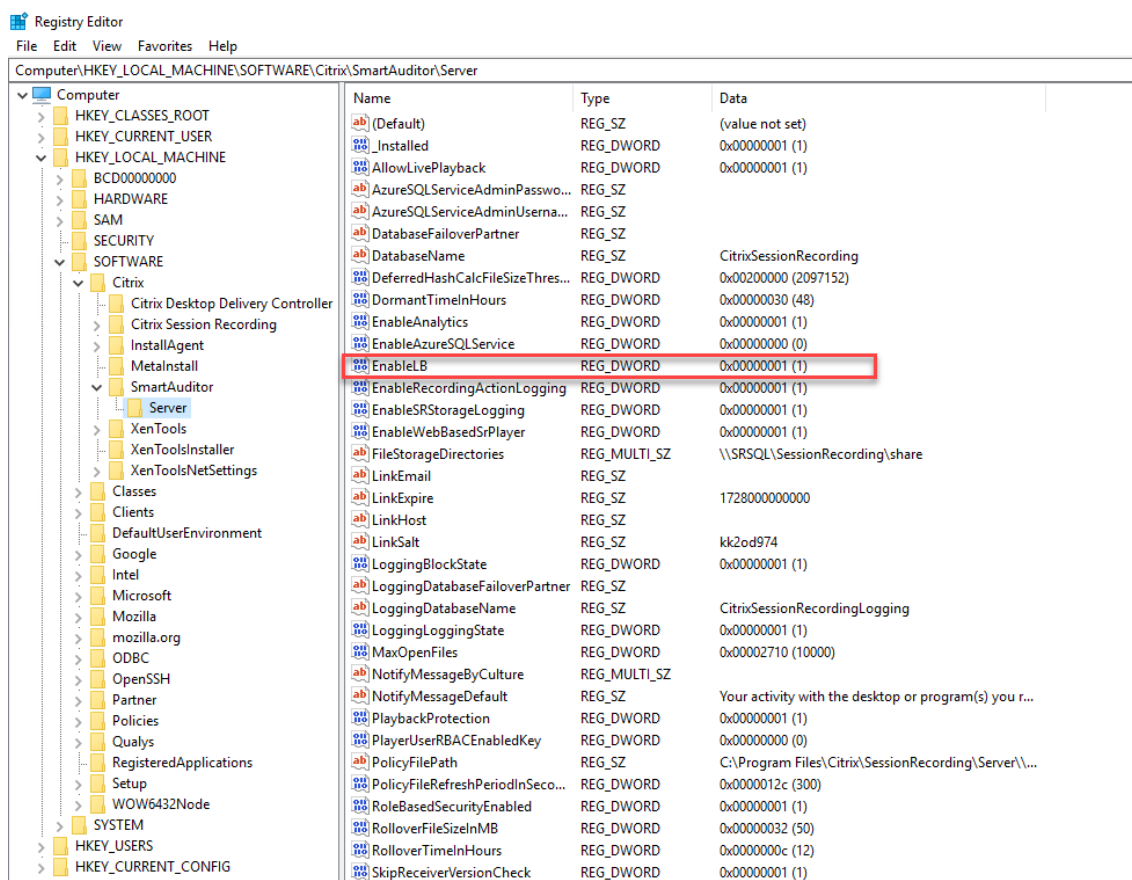
Le lecteur d'enregistrement de session ne peut pas lire les fichiers se trouvant sous un chemin contenant une lettre de lecteur ou un signe dollar (\$). Il y a une exception lorsque vous installez le lecteur et le serveur d'enregistrement de session sur la même machine.



4. Ajoutez une valeur à la clé de registre du serveur d'enregistrement de session se trouvant sous HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.

Nom de la valeur : EnableLB

Données de la valeur : 1 (D_WORD, signifie activer)



5. Redémarrez le service Gestionnaire de stockage d'enregistrement de session Citrix.

Étape 3 – Configurer l'équilibrage de charge dans Citrix ADC

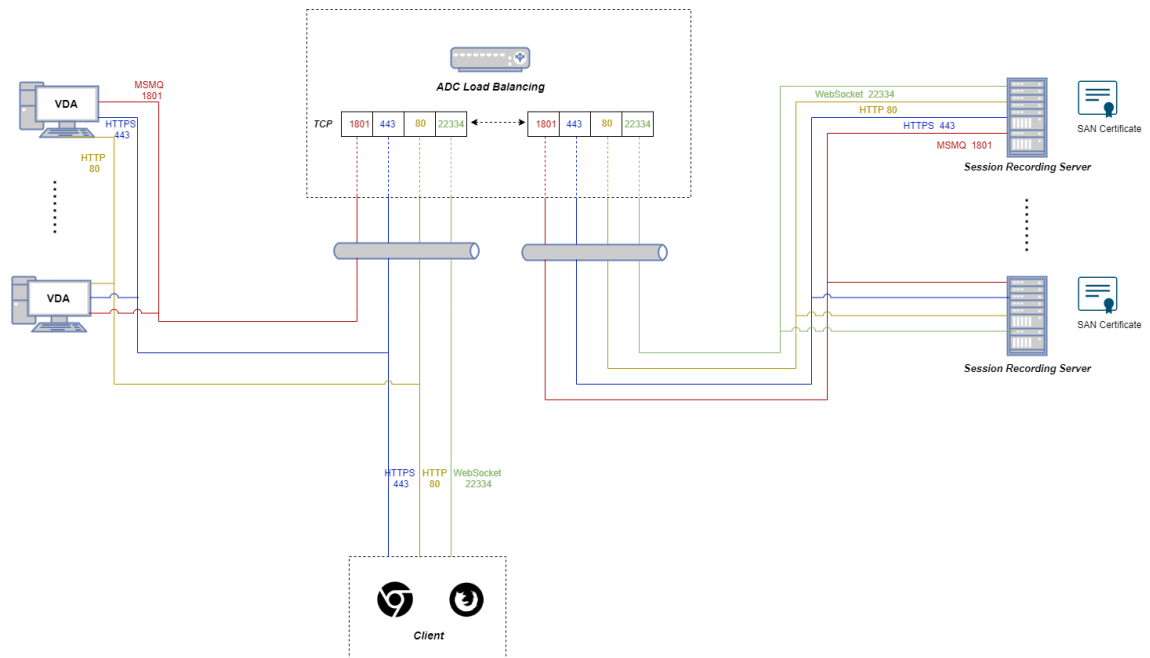
Il existe deux façons de configurer l'équilibrage de charge dans Citrix ADC : le protocole TCP pass-through et le déchargement SSL.

Configurer l'équilibrage de charge via le protocole TCP pass-through

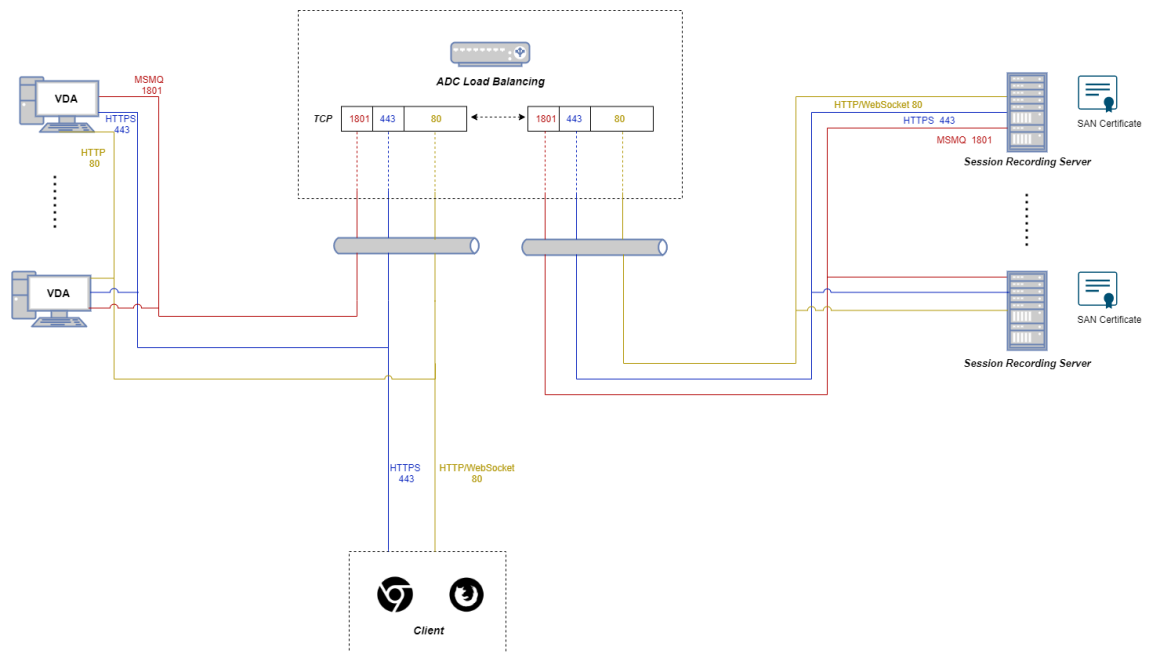
Les topologies suivantes montrent comment configurer l'équilibrage de charge via le protocole **TCP pass-through**.

- Si vous utilisez le serveur WebSocket basé sur Python (version 1.0) :

Enregistrement de session 2210

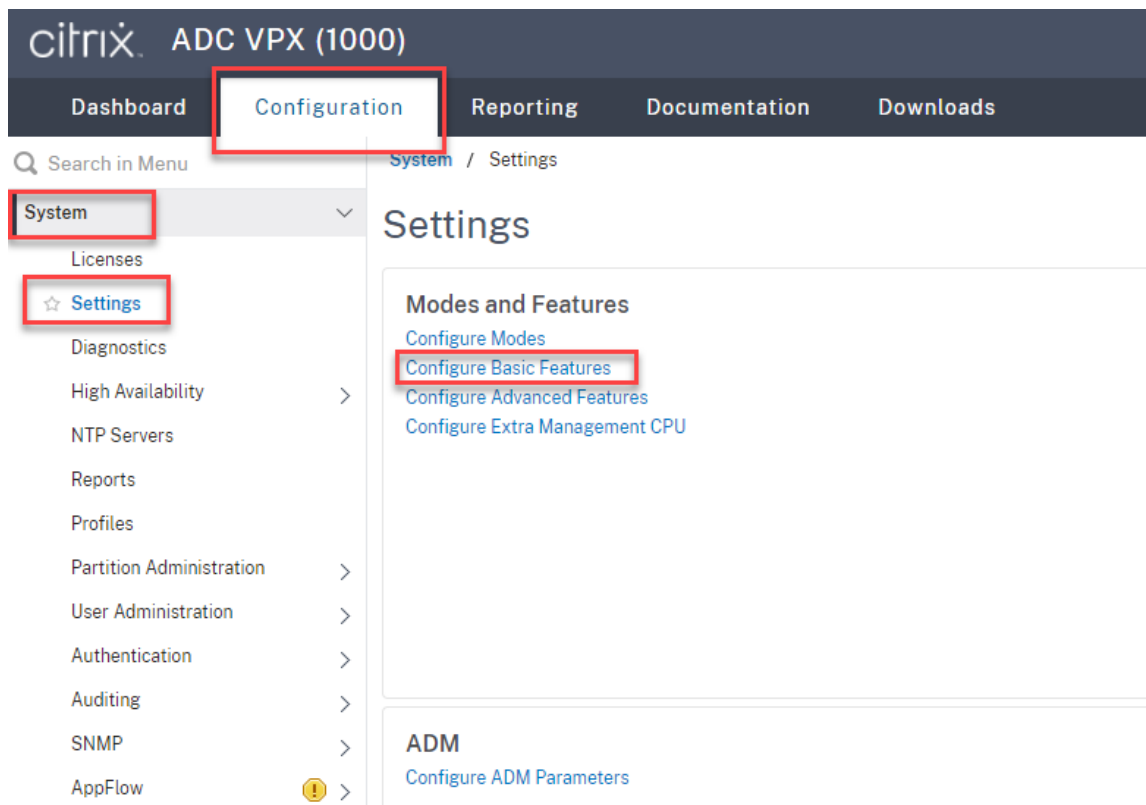


- Si vous utilisez le serveur WebSocket hébergé dans IIS (version 2.0) :

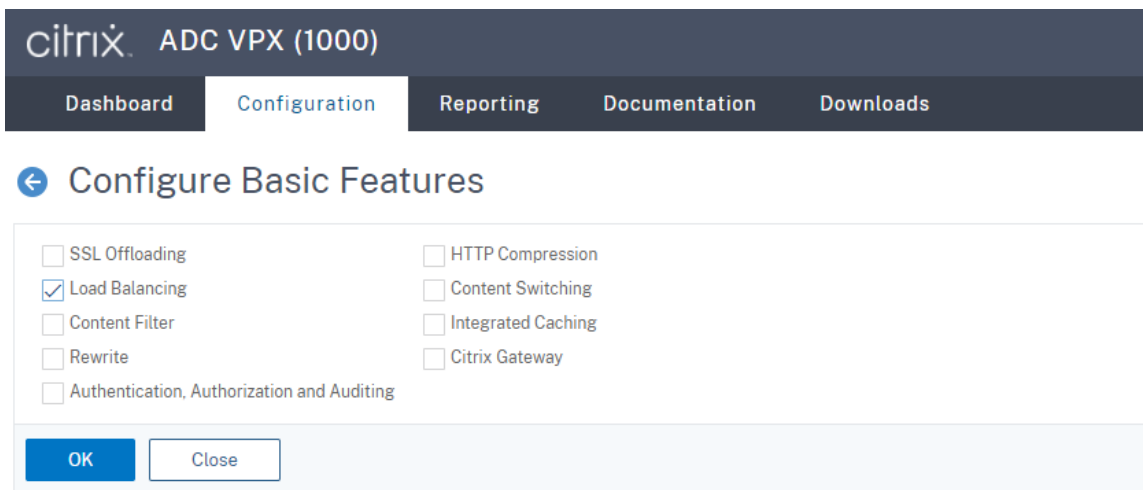


Pour configurer l'équilibrage de charge via le protocole TCP pass-through, procédez comme suit :

1. Connectez-vous à votre instance Citrix ADC VPX.
2. Accédez à **Configuration > System > Settings > Configure Basic Features**.

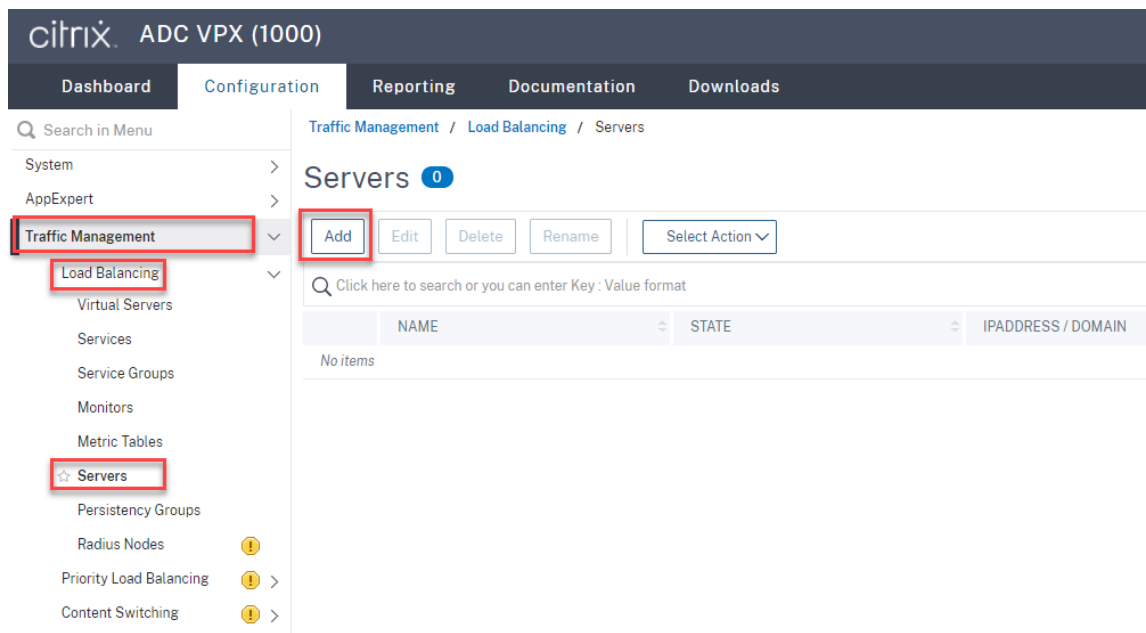


3. Sélectionnez **Load Balancing**, puis cliquez sur **OK**.

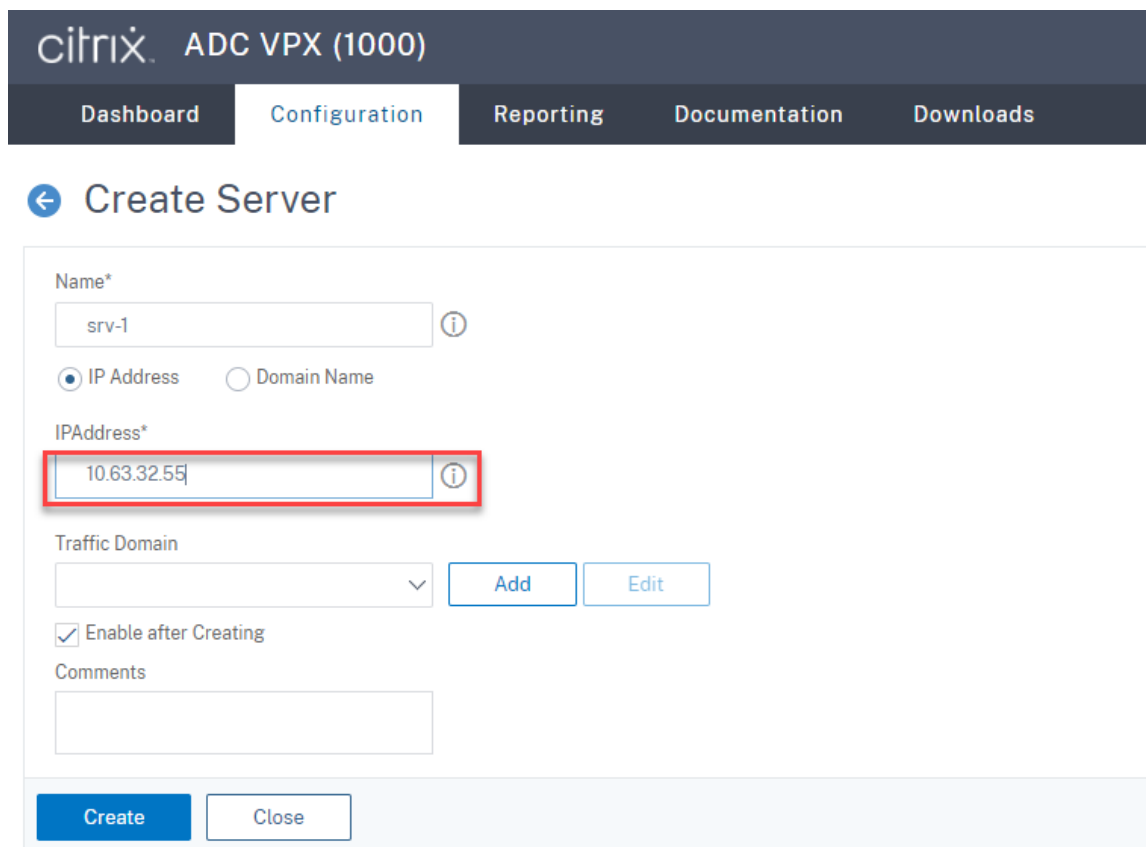


4. Ajoutez des serveurs d'équilibrage de charge.

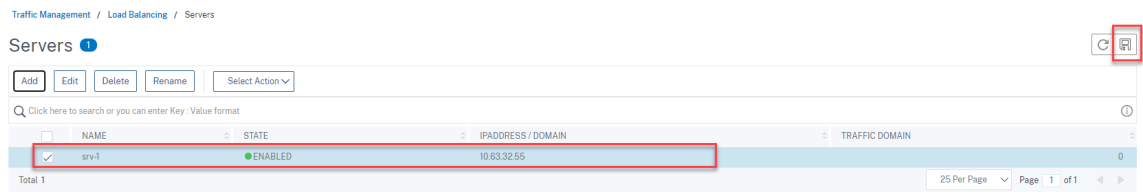
Accédez à **Traffic Management > Load Balancing > Servers** et cliquez sur **Add**.



Tapez le nom et l'adresse IP d'un serveur d'enregistrement de session, puis cliquez sur **Create**. Par exemple :

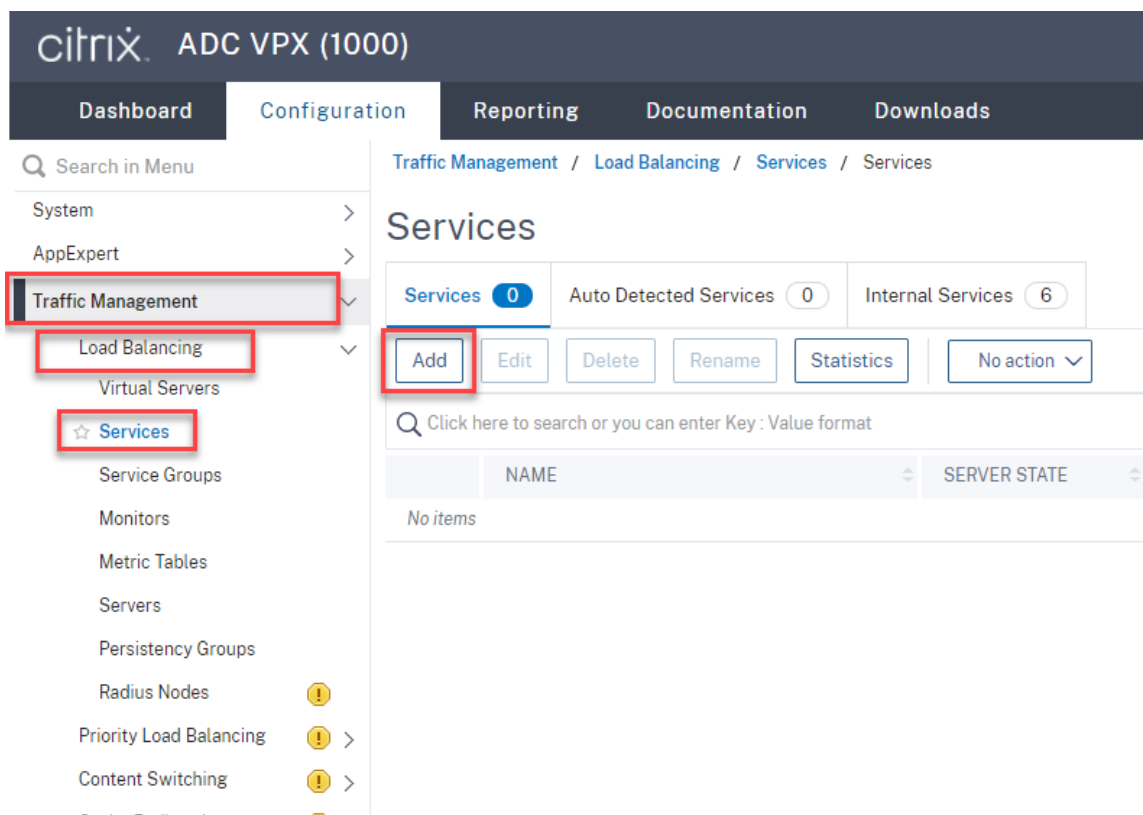


Cliquez sur l'icône Save dans le coin supérieur droit pour enregistrer vos modifications.



5. Pour le serveur WebSocket version 1.0, ajoutez des **services d'équilibrage de charge** pour les ports 80, 1801, 22334 et 443 pour chaque serveur d'enregistrement de session. Pour le serveur WebSocket version 2.0, ajoutez des **services d'équilibrage de charge** pour les ports 80, 1801 et 443 pour chaque serveur d'enregistrement de session.

Accédez à **Traffic Management > Load Balancing > Services** et cliquez sur **Add**.



Tapez un nom pour chaque **service d'équilibrage de charge** que vous ajoutez. Choisissez **Existing Server**, sélectionnez l'adresse IP de votre serveur d'enregistrement de session cible, sélectionnez **TCP** comme protocole de serveur et saisissez un numéro de port. Cliquez sur **OK**.

citrix ADC VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

← Load Balancing Service

Basic Settings

Service Name*
srv-1-80 ⓘ

New Server Existing Server

Server*
srv-1 (10.63.32.55) ▾

Protocol*
TCP ▾ ⓘ

Port*
80 ⓘ

▶ More

OK Cancel

Liez le moniteur de protocole TCP à chaque service d'équilibrage de charge.

The screenshot shows the Citrix ADC VPX (1000) configuration interface. The main panel displays the 'Load Balancing Service' configuration for 'srv-1-80'. The 'Basic Settings' section shows: Service Name: srv-1-80, Server Name: srv-1, IP Address: 10.63.32.55, Server State: DOWN, Protocol: TCP, Port: 80. The 'Monitors' section at the bottom indicates '1 Service to Load Balancing Monitor Binding'. A modal window titled 'Load Balancing Monitor Binding' is open, showing 'Select Monitor*' with 'tcp' selected, 'Binding Details' with 'Weight' set to 1 and 'State' checked, and 'Bind' and 'Close' buttons.

Cliquez sur l'icône Save dans le coin supérieur droit pour enregistrer vos modifications.

Traffic Management / Load Balancing / Services / Services

Services

Services 4 Auto Detected Services 0 Internal Services 6

	Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
<input type="checkbox"/>	srv-1-1801	UP	10.63.32.55	1801	TCP	0	0	SERVER	0
<input type="checkbox"/>	srv-1-22334	UP	10.63.32.55	22334	TCP	0	0	SERVER	0
<input type="checkbox"/>	srv-1-443	UP	10.63.32.55	443	TCP	0	0	SERVER	0
<input checked="" type="checkbox"/>	srv-1-80	UP	10.63.32.55	80	TCP	0	0	SERVER	0

Conseil :

Le **service d'équilibrage de charge** pour le port 22334 est requis uniquement pour le serveur WebSocket version 1.0.

6. Ajoutez des **serveurs virtuels d'équilibrage de charge**.

Pour le serveur WebSocket version 1.0, procédez comme suit pour ajouter des **serveurs virtuels d'équilibrage de charge** pour les ports 80, 443, 1801 et 22334. Pour le serveur

WebSocket version 2.0, ajoutez des **serveurs virtuels d'équilibrage de charge** pour les ports 80, 443 et 1801. Par exemple :

Traffic Management / Load Balancing / Virtual Servers

Virtual Servers

	Add	Edit	Delete	Enable	Disable	Statistics	Action		Search	
	Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health	Traffic Domain
<input type="checkbox"/>	vsvr-80	UP	UP	10.63.32.60	80	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
<input type="checkbox"/>	vsvr-1801	UP	UP	10.63.32.60	1801	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
<input type="checkbox"/>	vsvr-443	UP	UP	10.63.32.60	443	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
<input type="checkbox"/>	vsvr-22334	UP	UP	10.63.32.60	22334	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0

Accédez à **Traffic Management -> Load Balancing -> Virtual Servers** et cliquez sur **Add**.

The screenshot shows the Citrix ADC VPX (1000) configuration interface. The navigation menu on the left includes System, AppExpert, Traffic Management, Load Balancing, Virtual Servers, Services, Service Groups, Monitors, Metric Tables, Servers, Persistency Groups, Radius Nodes, Priority Load Balancing, and Content Switching. The main content area shows the path Traffic Management / Load Balancing / Virtual Servers. The 'Virtual Servers' page has a notification badge '1' and an 'Add' button highlighted with a red box. Below the 'Add' button is a search bar and a table with columns NAME, STATE, EFFECTIVE STATE, and IP ADDRESS. The table currently shows 'No items' and a 'Total 0'.

Ajoutez chaque serveur virtuel avec l'adresse VIP Citrix ADC basée sur le protocole TCP.

Citrix ADC VPX (1000)

[Dashboard](#)
[Configuration](#)
[Reporting](#)
[Documentation](#)
[Downloads](#)

← Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name* ⓘ

Protocol* ⓘ

IP Address Type* ⓘ

IP Address* ⓘ

Port* ⓘ

▶ More

Liez chaque serveur virtuel au **service d'équilibrage de charge** du même port. Par exemple :

Citrix ADC VPX (1000)

[Dashboard](#)
[Configuration](#)
[Reporting](#)
[Documentation](#)
[Downloads](#)

← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings

Name	vsrv-80	Listen Priority	-
Protocol	TCP	Listen Policy Expression	NONE
State	● DOWN	Redirection Mode	IP
IP Address	10.63.32.60	Range	1
Port	80	IPset	-
Traffic Domain	0	RHI State	PASSIV
		AppFlow Logging	ENABL
		Retain Connections on Cluster	NO
		TCP Probe Port	-

Services and Service Groups

A service is a logical representation of an application running on a server.
 A service group enables you to manage a group of services as though it were a single service. After creating a service group, you can bind it to a virtual server, and you can add services.
Note: Bind at least one service or service group to the virtual server.

Click **Continue** to display the advanced settings and select the method, persistence type, and any other configuration detail that you might need.

No Load Balancing Virtual Server Service Binding

No Load Balancing Virtual Server ServiceGroup Binding

The screenshot displays the Citrix ADC VPX (1000) configuration interface. The main navigation bar includes Dashboard, Configuration, Reporting, Documentation, and Downloads. The current view is 'Load Balancing Virtual Server' under the Configuration tab. The interface is divided into two main sections: a left sidebar for settings and a right pane for service binding.

Left Sidebar (Load Balancing Virtual Server):

- Basic Settings:**
 - Name: vsrv-80
 - Protocol: TCP
 - State: DOWN
 - IP Address: 10.63.32.60
 - Port: 80
 - Traffic Domain: 0
- Services and Service Groups:**
 - No Load Balancing Virtual Server Service Binding
 - No Load Balancing Virtual Server ServiceGroup Binding
- Traffic Settings:**
 - Health Threshold: 0
 - Client Idle Time-out: 9000
 - Minimum Autoscale Members: 0
 - Maximum Autoscale Members: 0
 - ICMP Virtual Server Response: PASSIVE

Right Pane (Service Binding / Service):

- Service count: 4
- Buttons: Select, Add (highlighted with a red box), Edit
- Search: Click here to search or you can enter Key : Value format
- Table of services:

<input type="checkbox"/>	NAME
<input type="checkbox"/>	srv-1-80
<input type="checkbox"/>	srv-1-443
<input type="checkbox"/>	srv-1-1801
<input type="checkbox"/>	srv-1-22334

Total 4

Choisissez une méthode d'équilibrage de charge.

Method

Method is a load balancing algorithm that the Citrix ADC uses to s

Load Balancing Method*

LEASTBANDWIDTH ⓘ

New Service Startup Request Rate

0

Backup LB Method*

ROUNDROBIN

New Service Request unit*

PER_SECOND

Increment Interval

Configurez la persistance sur chaque serveur virtuel. Nous vous recommandons de sélectionner **SOURCEIP** comme type de persistance. Pour de plus amples informations, consultez la section [Paramètres de persistance](#).

Persistence

Configure persistence to route all connections from the same user persistence type fails.

Select Persistence Type*

SOURCEIP RULE OTHERS ⓘ

Time-out (mins)*

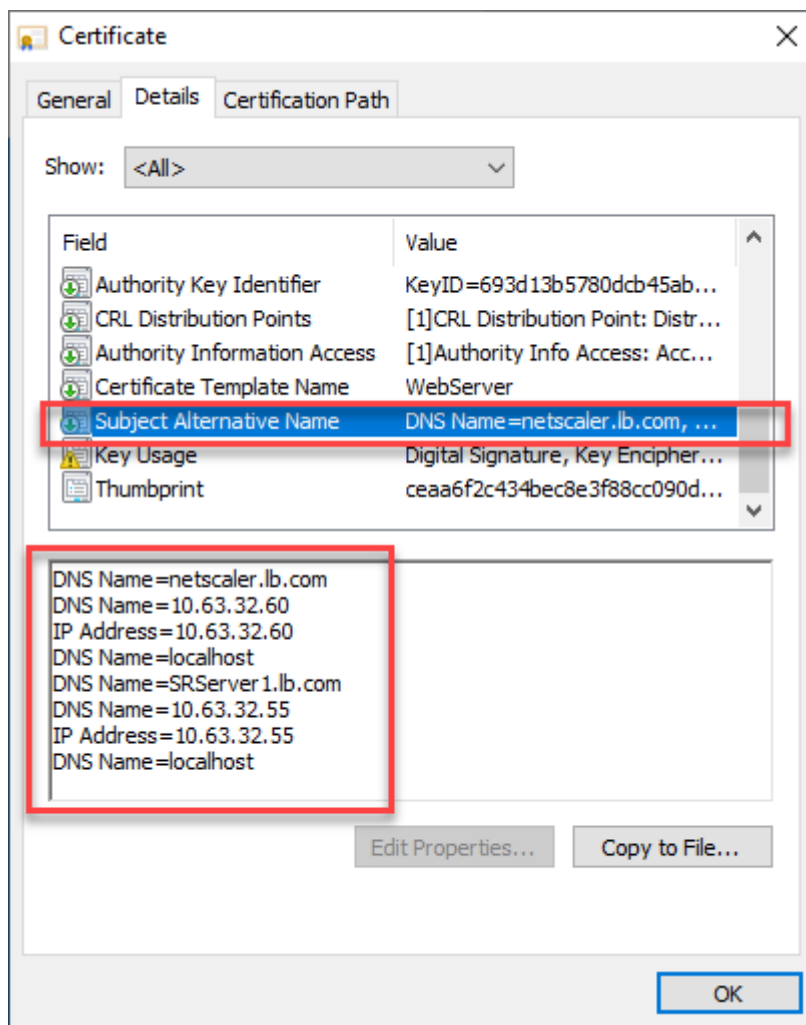
IPv4 Netmask

IPv6 Mask Length

7. Créez un enregistrement hôte pour l'adresse VIP Citrix ADC sur le contrôleur de domaine.

Name	Type	Data	Timestamp
lb.com	Start of Authority (SOA)	[47], lbdc.lb.com., hostma...	static
lb.com	Name Server (NS)	lbdc.lb.com.	static
lb.com	Host (A)	10.63.32.82	11/19/2020 2:00:00 AM
lbdc	Host (A)	10.63.32.82	static
LBDDC	Host (A)	10.63.32.11	11/19/2020 11:00:00 PM
Netscaler	Host (A)	10.63.32.60	static
SRSserver1	Host (A)	10.63.32.55	11/19/2020 2:00:00 AM
SRSserver2	Host (A)	10.63.32.68	11/19/2020 11:00:00 PM
SRSsql	Host (A)	10.63.32.91	11/23/2020 3:00:00 AM
TSVDA	Host (A)	10.63.32.215	11/23/2020 2:00:00 AM

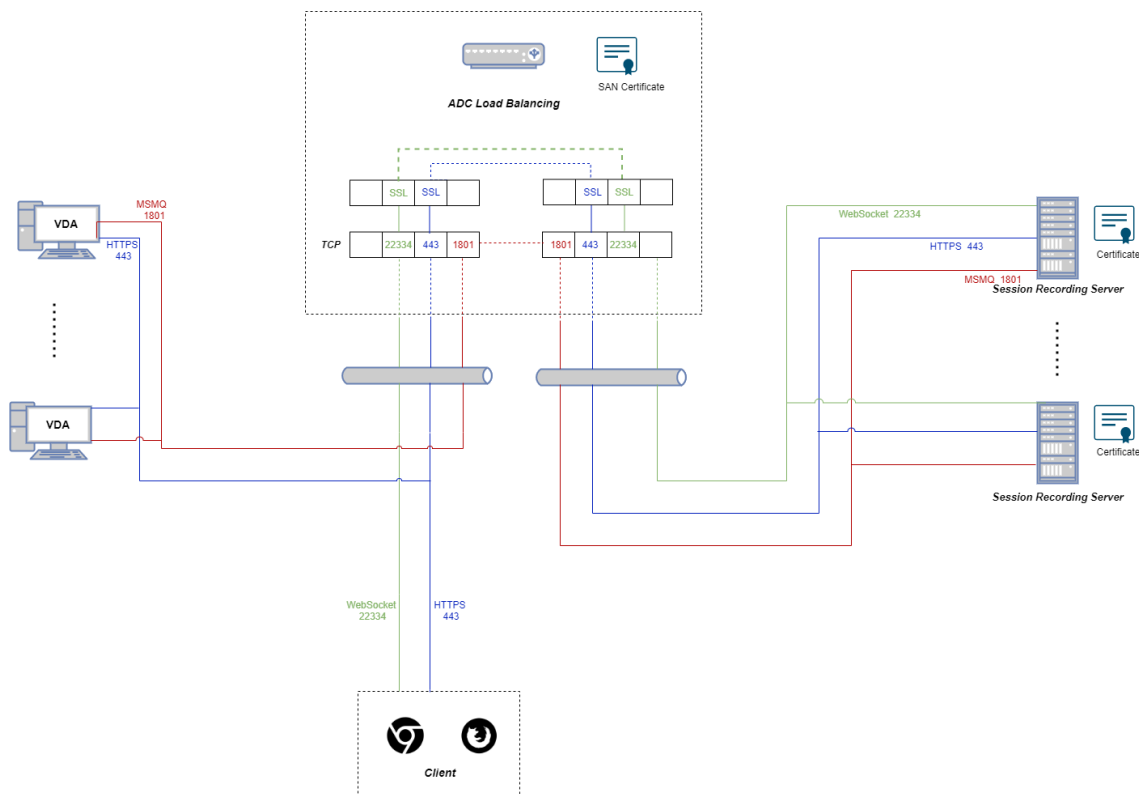
8. Pour accéder au lecteur Web via HTTPS, assurez-vous qu'un certificat SAN est disponible à la fois sur Citrix ADC et sur chaque serveur d'enregistrement de session. Un certificat SAN contient les noms de domaine complets de Citrix ADC et de chaque serveur d'enregistrement de session.



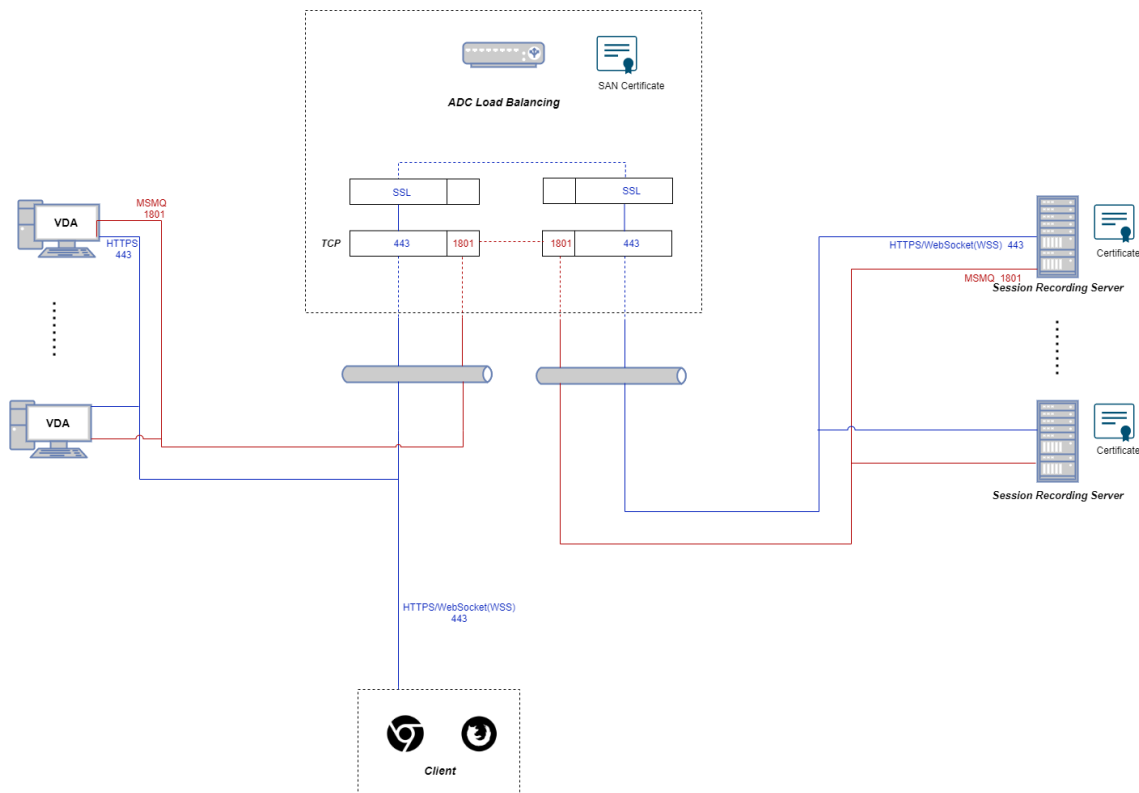
Configurer l'équilibrage de charge via le téléchargement SSL

Les topologies suivantes montrent comment configurer l'équilibrage de charge via le téléchargement SSL.

- Si vous utilisez le serveur WebSocket basé sur Python (version 1.0) :

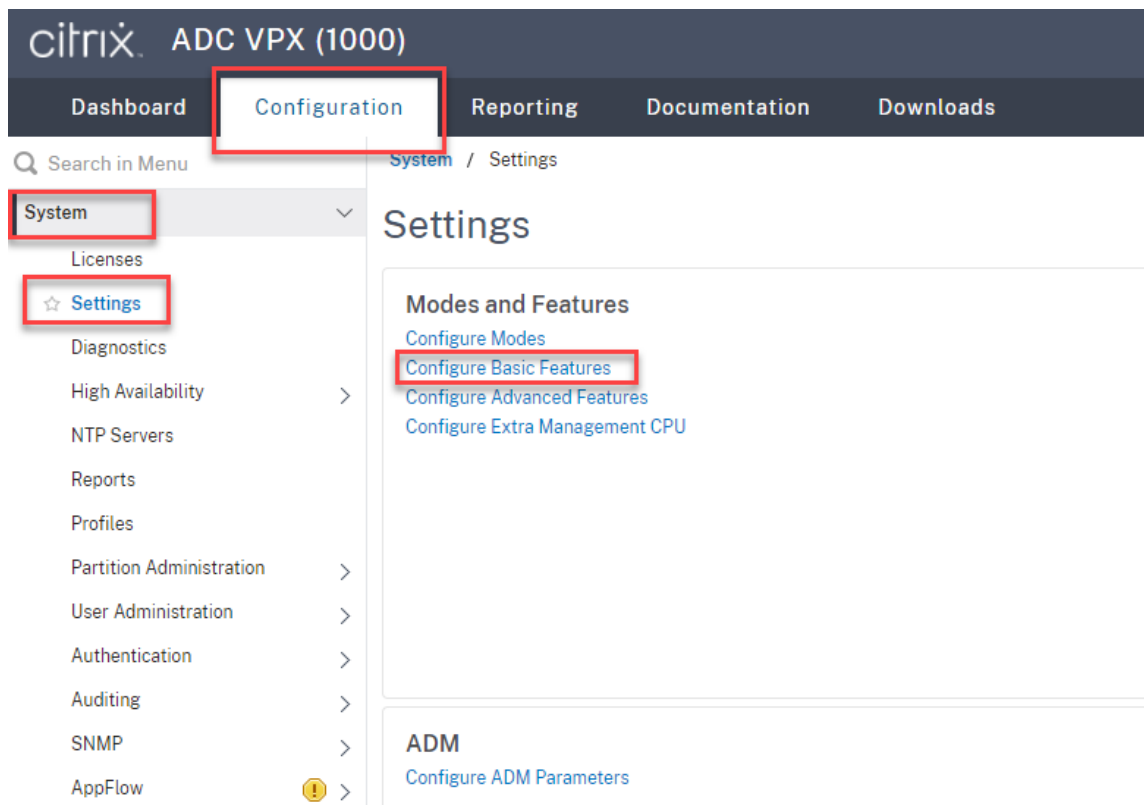


- Si vous utilisez le serveur WebSocket hébergé dans IIS (version 2.0) :

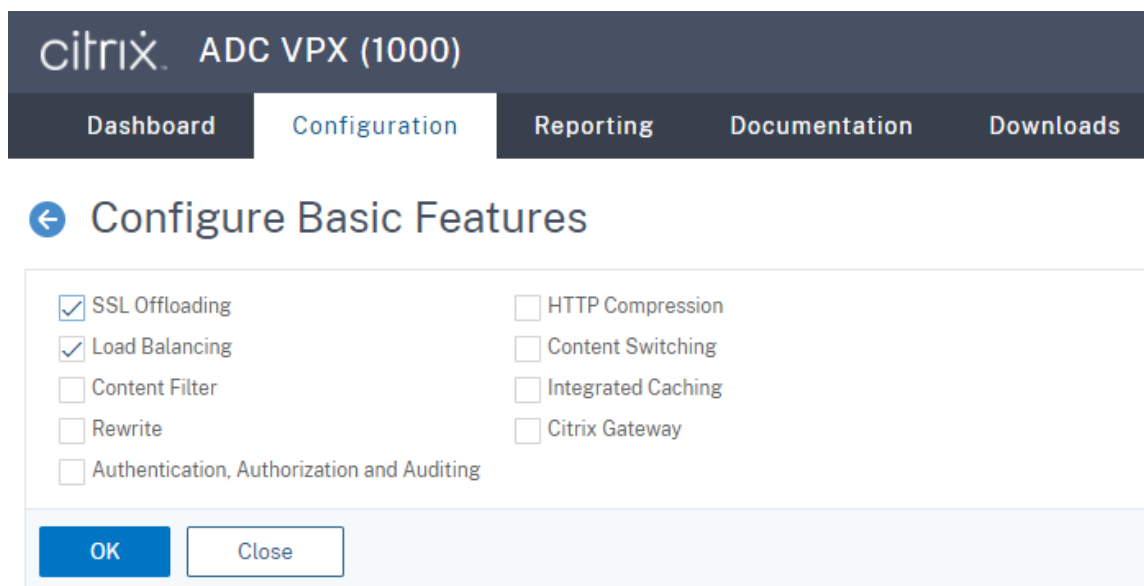


1. Connectez-vous à votre instance Citrix ADC VPX.

2. Accédez à **Configuration > System > Settings > Configure Basic Features**.

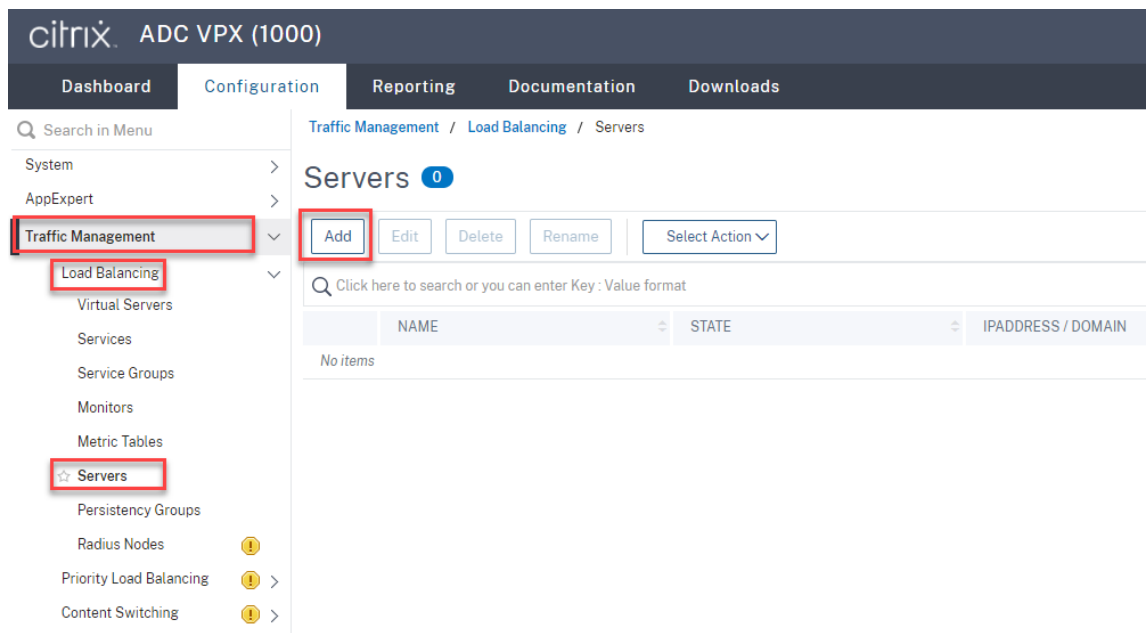


3. Sélectionnez **SSL Offloading** et **Load Balancing**, puis cliquez sur **OK**.

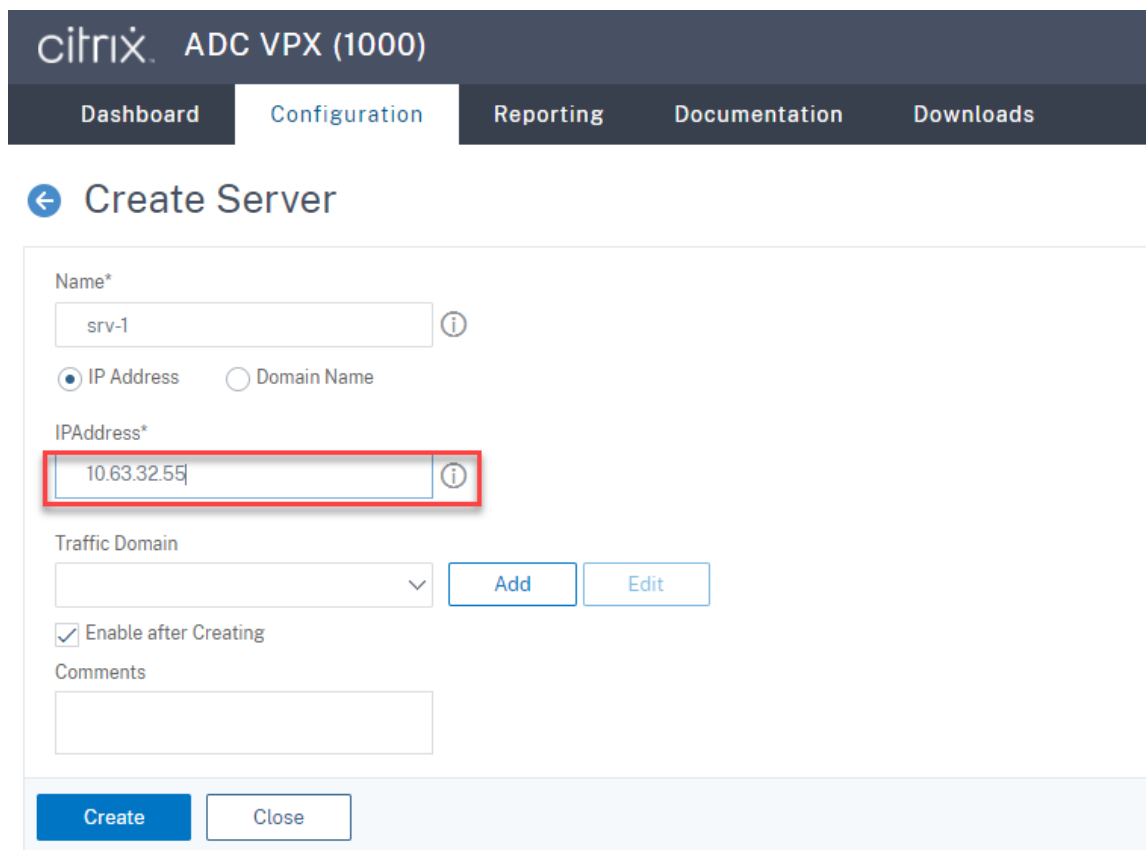


4. Ajoutez des serveurs d'équilibrage de charge.

Accédez à **Traffic Management > Load Balancing > Servers** et cliquez sur **Add**.

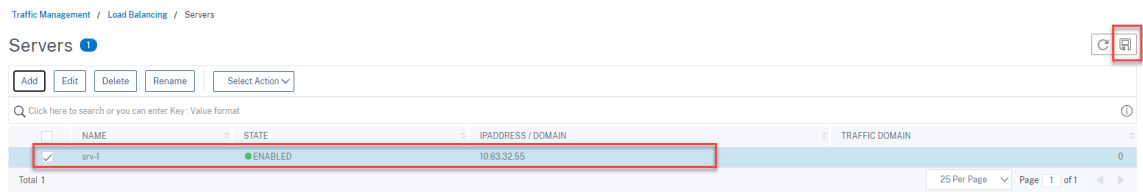


Tapez le nom et l'adresse IP d'un serveur d'enregistrement de session, puis cliquez sur **Create**. Par exemple :



Cliquez sur l'icône Save dans le coin supérieur droit pour enregistrer vos modifications.

Enregistrement de session 2210



5. Ajoutez des **services d'équilibrage de charge** pour chaque serveur d'enregistrement de session que vous avez ajouté à l'étape précédente.

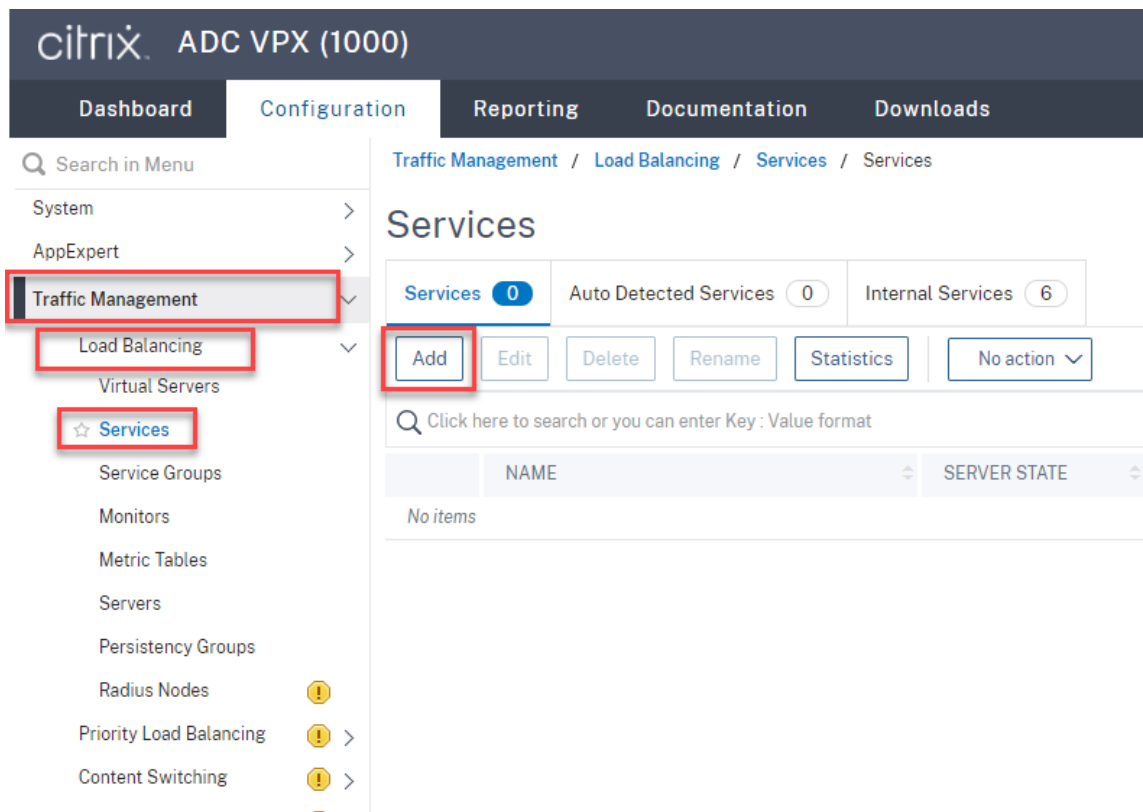
Ajoutez les **services d'équilibrage de charge** suivants pour chaque serveur d'enregistrement de session :

- (Requis uniquement lorsque vous utilisez le serveur WebSocket version 1.0) **Service d'équilibrage de charge SSL** associé au port 22334 qui est liée au moniteur TCP
- **Service d'équilibrage de charge SSL** associé au port 443 qui est lié au moniteur HTTPS
- **Service d'équilibrage de charge TCP** associé au port 1801 qui est lié au moniteur TCP

Par exemple :

Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
srv-1-443	UP	10.63.32.55	443	SSL	0	0	SERVER	0
srv-1-1801	UP	10.63.32.55	1801	TCP	0	0	SERVER	0
srv-1-22334	UP	10.63.32.55	22334	SSL	0	0	SERVER	0

Accédez à **Traffic Management > Load Balancing > Services** et cliquez sur **Add**.



(Requis uniquement lorsque vous utilisez le serveur WebSocket version 1.0) Ajoutez un service d'équilibrage de charge SSL associé au port 22334 pour chaque serveur d'enregistrement de session. Tapez un nom pour le service d'équilibrage de charge, choisissez **Existing Server**, sélectionnez l'adresse IP d'un serveur d'enregistrement de session, sélectionnez **SSL** comme protocole serveur, tapez le numéro de port **22334**, puis cliquez sur **OK**.

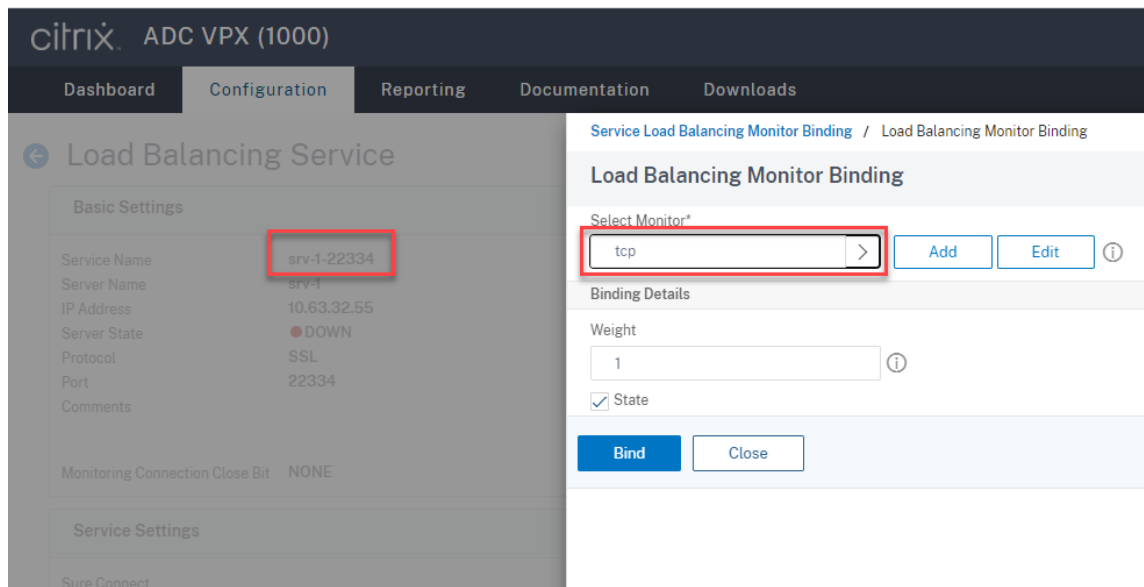
Pour obtenir un exemple, consultez la capture d'écran suivante.

The screenshot shows the Citrix ADC VPX (1000) Configuration page. The navigation tabs are Dashboard, Configuration, Reporting, and Documents. The main heading is "Load Balancing Service" with a back arrow. Below this is a "Basic Settings" section with the following fields:

- Service Name*: srv-1-22334 (with an information icon)
- Radio buttons: New Server, Existing Server
- Server*: srv-1 (10.63.32.55) (dropdown menu)
- Protocol*: SSL (dropdown menu, with an information icon)
- Port*: 22334 (with an information icon)

Below the "Basic Settings" section is a "More" section with a right-pointing arrow. At the bottom of the dialog are two buttons: "OK" (blue) and "Cancel" (white).

Liez le moniteur TCP au **service d'équilibrage de charge SSL** que vous venez d'ajouter.



Ajoutez un service d'équilibrage de charge SSL associé au port 443 pour chaque serveur d'enregistrement de session. Tapez un nom pour le service d'équilibrage de charge, choisissez **Existing Server**, sélectionnez l'adresse IP d'un serveur d'enregistrement de session, sélectionnez **SSL** comme protocole serveur, tapez le numéro de port 443, puis cliquez sur **OK**.

citrix ADC VPX (1000)

Dashboard Configuration Reporting De

← Load Balancing Service

Basic Settings

Service Name*
srv-1-443 ⓘ

New Server Existing Server

Server*
srv-1 (10.63.32.55) ▾

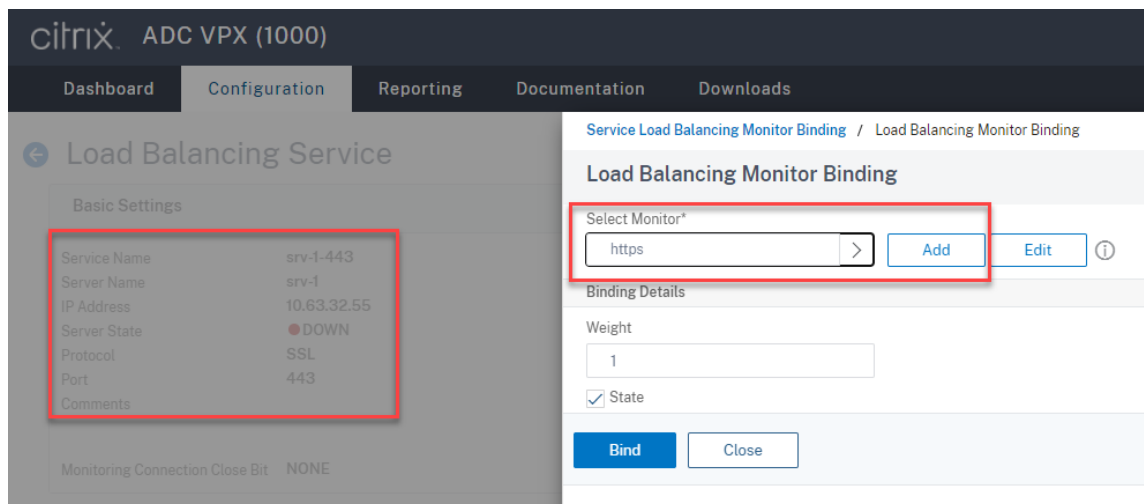
Protocol*
SSL ▾

Port*
443 ⓘ

▶ More

OK Cancel

Liez le moniteur HTTPS au **service d'équilibrage de charge SSL** que vous venez d'ajouter.



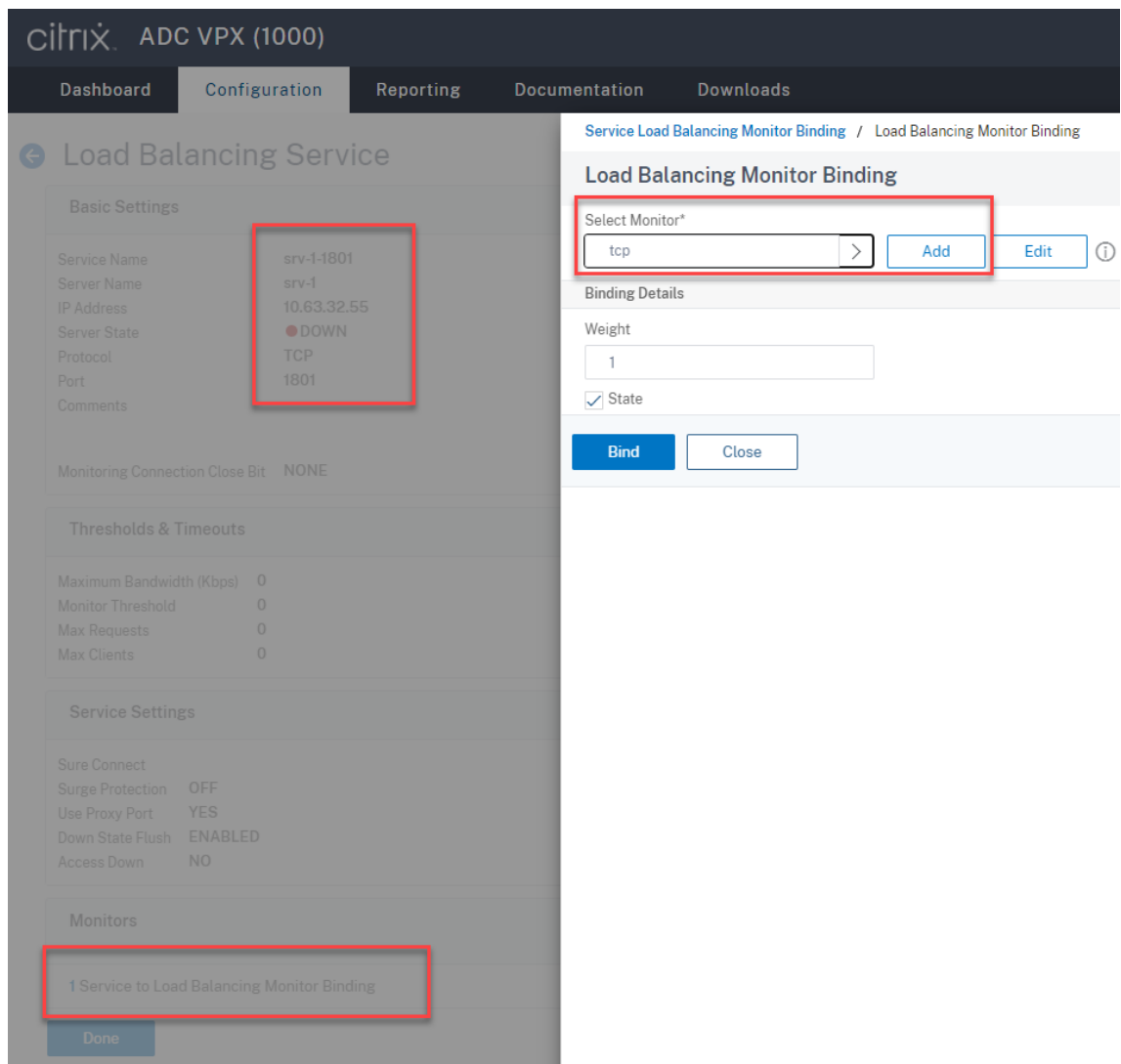
Ajoutez un service d'équilibrage de charge TCP associé au port 1801 pour chaque serveur d'enregistrement de session. Tapez un nom pour le service d'équilibrage de charge, choisissez **Existing Server**, sélectionnez l'adresse IP d'un serveur d'enregistrement de session, sélectionnez **TCP** comme protocole serveur, tapez le numéro de port 1801, puis cliquez sur **OK**.

The screenshot shows the Citrix ADC VPX (1000) Configuration page. The navigation tabs are Dashboard, Configuration, Reporting, and Documentation. The main heading is "Load Balancing Service" with a back arrow. Below this is a "Basic Settings" section with the following fields:

- Service Name*: srv-1-1801 (with an information icon)
- Radio buttons: New Server, Existing Server
- Server*: srv-1 (10.63.32.55) (with a dropdown arrow)
- Protocol*: TCP (with a dropdown arrow and an information icon)
- Port*: 1801 (with an information icon)

Below the "Basic Settings" section is a "More" section with a right-pointing arrow. At the bottom of the dialog are two buttons: "OK" (in a blue box) and "Cancel".

Liez le moniteur TCP au **service d'équilibrage de charge TCP** que vous venez d'ajouter.



6. (Requis uniquement lorsque vous utilisez le serveur WebSocket version 1.0) Ajoutez un profil HTTP pour chaque **service d'équilibrage de charge SSL** associé au port 22334.

Accédez à **System > Profiles > HTTP Profiles** et cliquez sur **Ajouter**.

citrix ADC VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Search in Menu

System

- Licenses
- Settings
- Diagnostics
- High Availability
- NTP Servers
- Reports
- Profiles**
- Partition Administration
- User Administration
- Authentication
- Auditing
- SNMP

System / Profiles / HTTP Profiles

Profiles

TCP Profiles 13 HTTP Profiles 3 Database Profiles 0 SSL Profil

Add Edit Delete

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	DROP INVALID	INVALIDATE HTTP
<input type="checkbox"/>	nshttp_default_profile	✗	✗
<input type="checkbox"/>	nshttp_default_strict_validation	✓	✓
<input type="checkbox"/>	nshttp_default_internal_apps	✓	✓

Total 3

Cochez la case **Enable WebSocket connections** et acceptez les autres paramètres par défaut.

Enregistrement de session 2210

HTTP/2 Initial Window Size	<input type="text" value="65535"/>
HTTP/2 Maximum Concurrent Streams	<input type="text" value="100"/>
HTTP/2 Maximum Frame Size	<input type="text" value="16384"/>
HTTP/2 Minimum Server Connections	<input type="text" value="20"/>
HTTP/2 Maximum Header List Size	<input type="text" value="24576"/>
HTTP/2 Maximum Ping Frames Per Minute	<input type="text"/>
HTTP/2 Maximum Reset Frames Per Minute	<input type="text"/>
HTTP/2 Maximum Empty Frames Per Minute	<input type="text"/>
HTTP/2 Maximum Settings Frames Per Minute	<input type="text"/> ⓘ

<input type="checkbox"/> Alternative Service	<input checked="" type="checkbox"/> Connection Multiplexing	<input type="checkbox"/> Drop invalid HTTP requests
<input type="checkbox"/> Mark HTTP/0.9 requests as invalid	<input type="checkbox"/> Mark CONNECT Requests as Invalid	<input type="checkbox"/> Mark TRACE Requests as Inva
<input type="checkbox"/> Mark RFC7230 Non-Compliant Transaction as Invalid	<input type="checkbox"/> Mark HTTP Header with Extra White Space as Invalid	<input type="checkbox"/> Compression on PUSH packet
<input checked="" type="checkbox"/> Drop extra CRLF	<input checked="" type="checkbox"/> Enable WebSocket connections ⓘ	<input type="checkbox"/> Enable RTSP Tunnel
<input type="checkbox"/> Drop extra data from server	<input checked="" type="checkbox"/> HTTP Weblogging	<input type="checkbox"/> Persistent ETag
<input type="checkbox"/> Adaptive Timeout		

Entrez un nom pour le profil HTTP, par exemple `websocket_SSL`.

Revenez à chaque **service d'équilibrage de charge SSL** associé au port 22334, par exemple, `srv-1-22334`. Cliquez sur **+ Profiles**.

The screenshot shows the Citrix ADC VPX (1000) configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The 'Configuration' tab is active, and the 'Load Balancing Service' page is displayed. The 'Basic Settings' section contains a table with the following data:

Service Name	srv-1-22334	Traffic Domain	0
Server Name	srv-1	Number of Active Connections	-
IP Address	10.63.32.55	Hash ID	-
Server State	● DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	22334	Cache Type	SERVER
Comments		Cacheable	NO
		Health Monitoring	YES
		AppFlow Logging	ENABLED
Monitoring Connection Close Bit	NONE		

The 'Advanced Settings' sidebar on the right includes options for '+ Thresholds & Timeouts', '+ Profiles' (highlighted), '+ Policies', '+ SSL Profile', '+ SSL Policies', and '+ Certificate'. The 'Service Settings' section at the bottom shows 'Use Proxy Port' set to 'YES'.

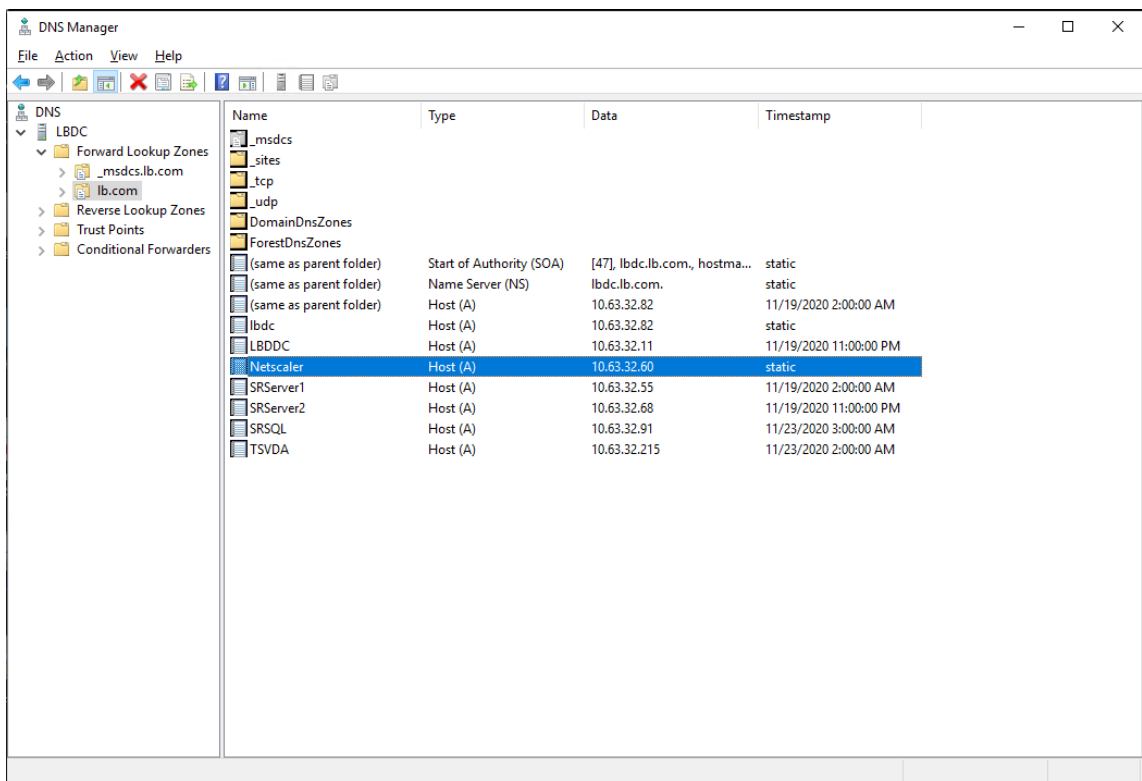
Sélectionnez le profil HTTP, par exemple `websocket_SSL`, puis cliquez sur **OK**, puis sur **Done**.

The screenshot shows the 'Profiles' configuration dialog. It has four dropdown menus with '+' buttons to the right:

- Net Profile: [Empty]
- TCP Profile: [Empty]
- HTTP Profile: `websocket_SSL` (highlighted with a black box)
- DNS Profile Name: [Empty]

At the bottom of the dialog is a blue 'OK' button. Below the dialog is a 'Done' button.

7. (Requis uniquement lorsque vous utilisez le serveur WebSocket version 2.0) Ajoutez un profil HTTP pour chaque **service d'équilibrage de charge SSL** associé au port 443.
8. Créez un enregistrement hôte pour l'adresse VIP Citrix ADC sur le contrôleur de domaine.

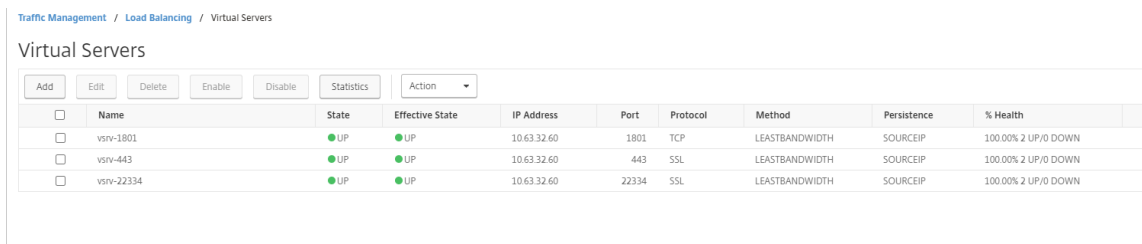


9. Ajoutez des **serveurs virtuels d'équilibrage de charge**.

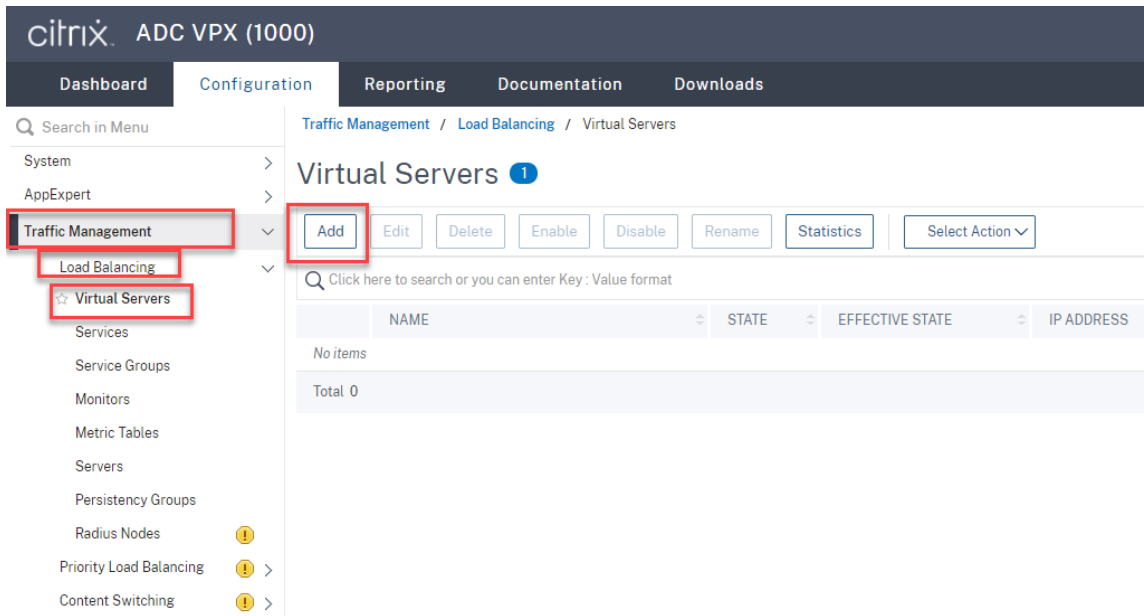
Ajoutez les **serveurs virtuels d'équilibrage de charge** suivants avec l'adresse VIP Citrix ADC.

- (Requis uniquement lorsque vous utilisez le serveur WebSocket version 1.0) **Serveur virtuel d'équilibrage de charge** associé au port 22334 basé sur SSL
- **Serveur virtuel d'équilibrage de charge** associé au port 443 basé sur SSL
- **Serveur virtuel d'équilibrage de charge** associé au port 1801 basé sur TCP

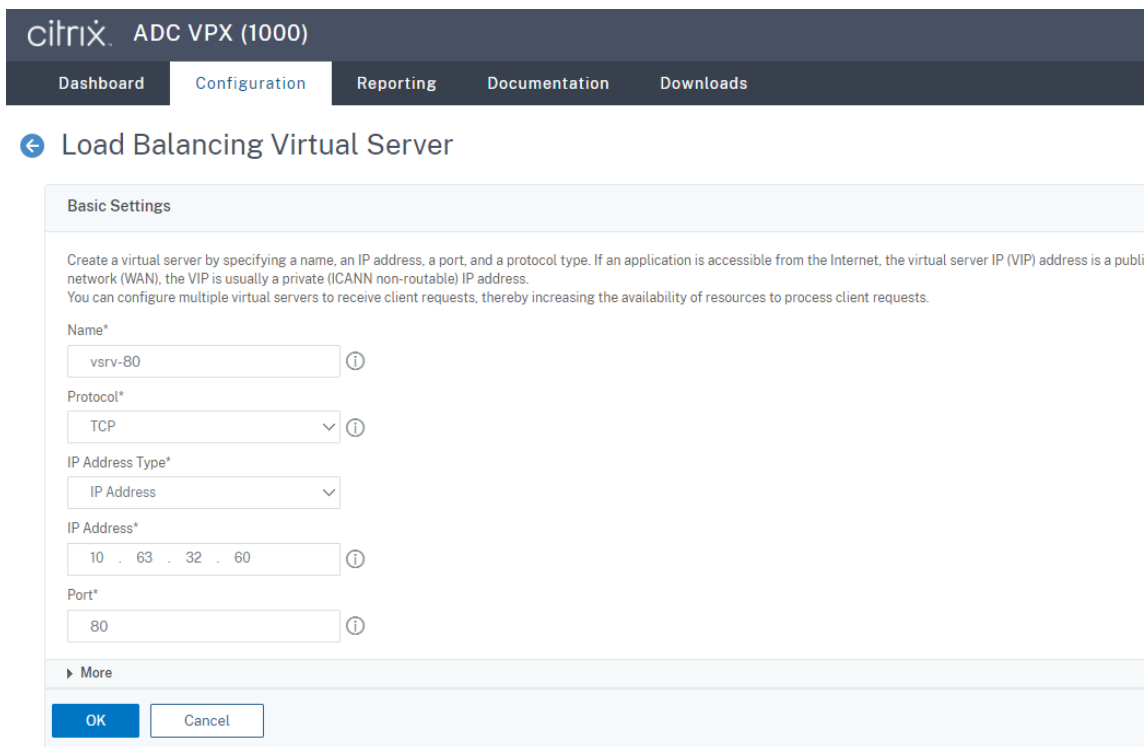
Pour obtenir un exemple, consultez la capture d'écran suivante.



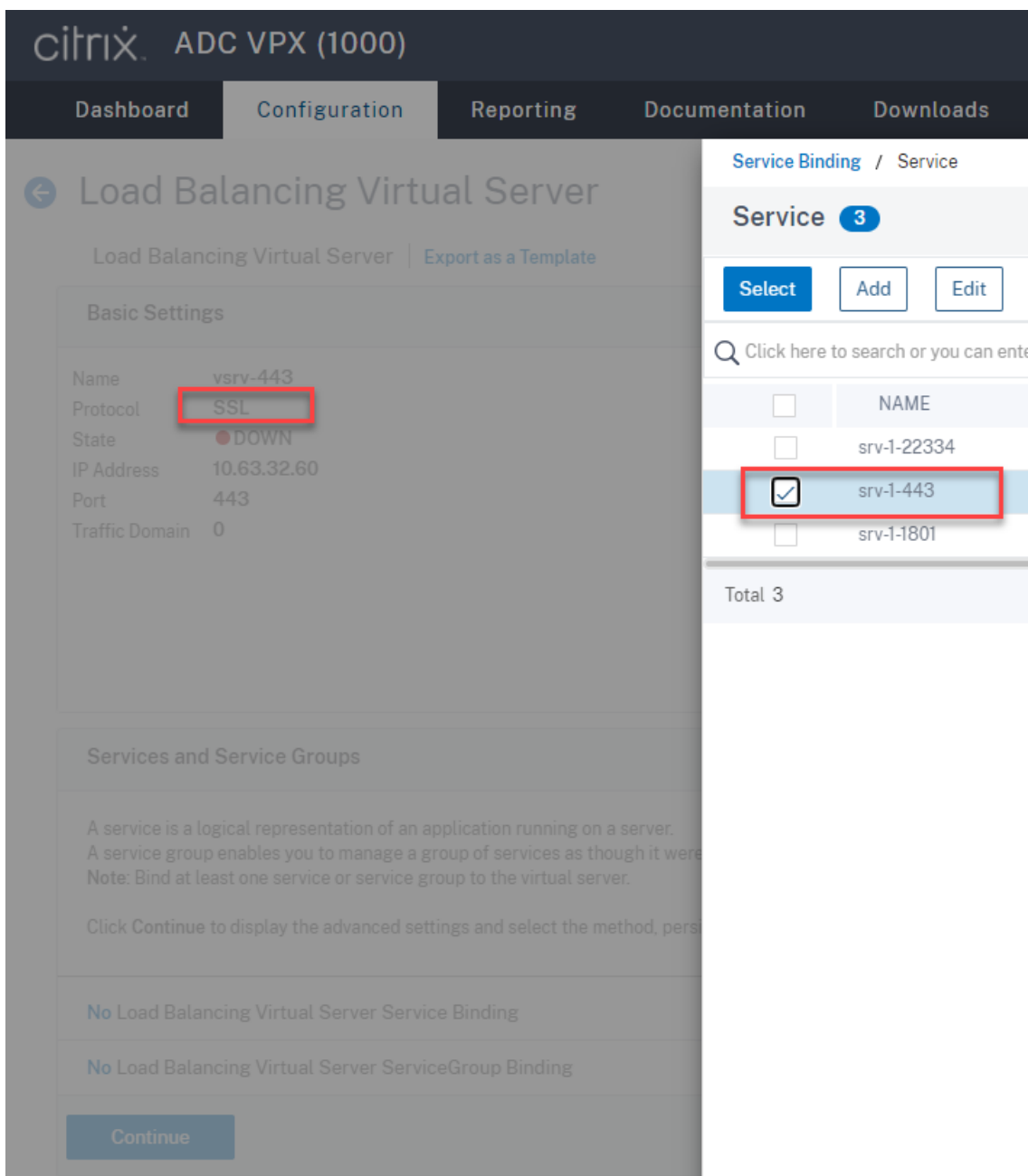
Accédez à **Traffic Management -> Load Balancing -> Virtual Servers** et cliquez sur **Add**.



Ajoutez chaque serveur virtuel avec l'adresse VIP Citrix ADC. Tapez un nom de serveur, sélectionnez **TCP** ou **SSL**, puis sélectionnez le numéro de port approprié comme décrit précédemment.



Liez chaque serveur virtuel au **service d'équilibrage de charge** du même port. Par exemple :



Conseil :

Le **service d'équilibrage de charge** associé au port 22334 est requis uniquement lorsque vous utilisez le serveur WebSocket version 1.0.

Choisissez une méthode d'équilibrage de charge.

Method

Method is a load balancing algorithm that the Citrix ADC uses to s

Load Balancing Method*

LEASTBANDWIDTH ⓘ

New Service Startup Request Rate

0

Backup LB Method*

ROUNDROBIN

New Service Request unit*

PER_SECOND

Increment Interval

Configurez la persistance sur chaque serveur virtuel. Nous vous recommandons de sélectionner **SOURCEIP** comme type de persistance. Pour de plus amples informations, consultez la section [Paramètres de persistance](#).

Persistence

Configure persistence to route all connections from the same user if the persistence type fails.

Select Persistence Type*

SOURCEIP
 RULE
 OTHERS
 (i)

Time-out (mins)*

IPv4 Netmask

IPv6 Mask Length

OK

(Requis uniquement lorsque vous utilisez le serveur WebSocket version 1.0) Ajoutez un profil HTTP pour le serveur virtuel d'équilibrage de charge associé au port 22334.

Profiles
×

A profile is a collection of settings that can be applied to a NetScaler entity, such as a virtual server or service. You can apply the same profile to multiple entities of the same type.

<p>Net Profile <input style="width: 90%; border: 1px solid #ccc;" type="text" value=""/> + / ✎</p> <p>TCP Profile <input style="width: 90%; border: 1px solid #ccc;" type="text" value=""/> + / ✎</p> <p>LB Profile <input style="width: 90%; border: 1px solid #ccc;" type="text" value=""/> + / ✎</p>	<p>HTTP Profile <input style="width: 90%; border: 1px solid #ccc;" type="text" value="websocket_SSL"/> + / ✎ / ?</p> <p>DB Profile <input style="width: 90%; border: 1px solid #ccc;" type="text" value=""/> + / ✎</p> <p>DNS Profile Name <input style="width: 90%; border: 1px solid #ccc;" type="text" value=""/> + / ✎</p>
--	---

OK

10. Installez un certificat SAN (Subject Alternative Name) dans Citrix ADC.

Obtenez un certificat SAN au format PEM auprès d'une autorité de certification (CA) de confiance. Extrayez et téléchargez les fichiers de certificat et de clé privée dans Citrix ADC en accédant à **Traffic Management > SSL > Server Certificate Wizard**.

Pour plus d'informations, consultez la section [Certificats SSL](#).

4 Install Certificate

Certificate-Key Pair Name*

Certificate File Name*
 ?

Key File Name*
 ?

Password*
 ?

Notify When Expires

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period

11. Liez un certificat SAN à chaque serveur virtuel d'équilibrage de charge SSL.

Accédez à **Traffic Management > Load Balancing > Virtual Servers**, sélectionnez un serveur virtuel d'équilibrage de charge SSL, puis cliquez sur **Server Certificate**.

The screenshot shows the Citrix ADC VPX (1000) configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The main heading is 'Load Balancing Virtual Server' with a back arrow. Below the heading, there is a breadcrumb 'Load Balancing Virtual Server | Export as a Template'.

The 'Basic Settings' section contains the following information:

Name	vsrv-443
Protocol	SSL
State	● DOWN
IP Address	10.63.32.60
Port	443
Traffic Domain	0

The 'Services and Service Groups' section shows:

- 1 Load Balancing Virtual Server Service Binding
- No Load Balancing Virtual Server ServiceGroup Binding

The 'Certificate' section shows:

- No Server Certificate (highlighted with a red box)
- No CA Certificate

A 'Continue' button is located at the bottom of the configuration panel.

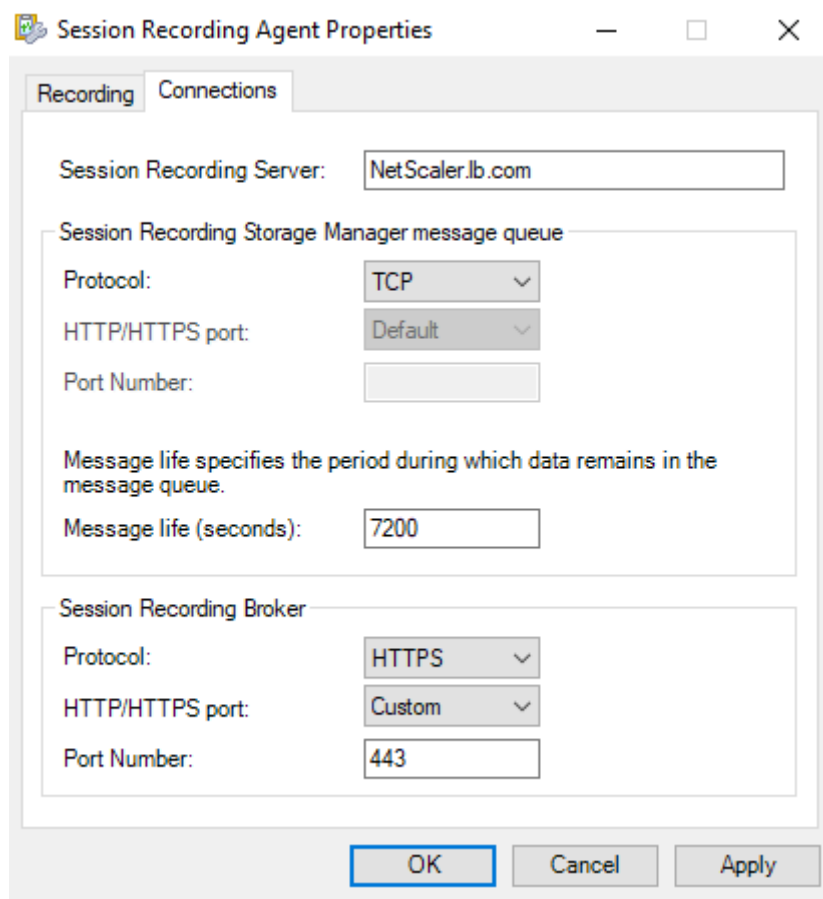
Ajoutez le certificat SAN mentionné précédemment et cliquez sur **Bind**.

Étape 4 – Configurer un agent d'enregistrement de session existant pour prendre en charge l'équilibrage de charge

1. Connectez-vous à l'agent d'enregistrement de session à l'aide d'un compte d'administrateur de domaine.
2. Ouvrez **Propriétés de l'agent d'enregistrement de session**.

3. Effectuez cette étape si vous utilisez Microsoft Message Queuing (MSMQ) sur TCP.

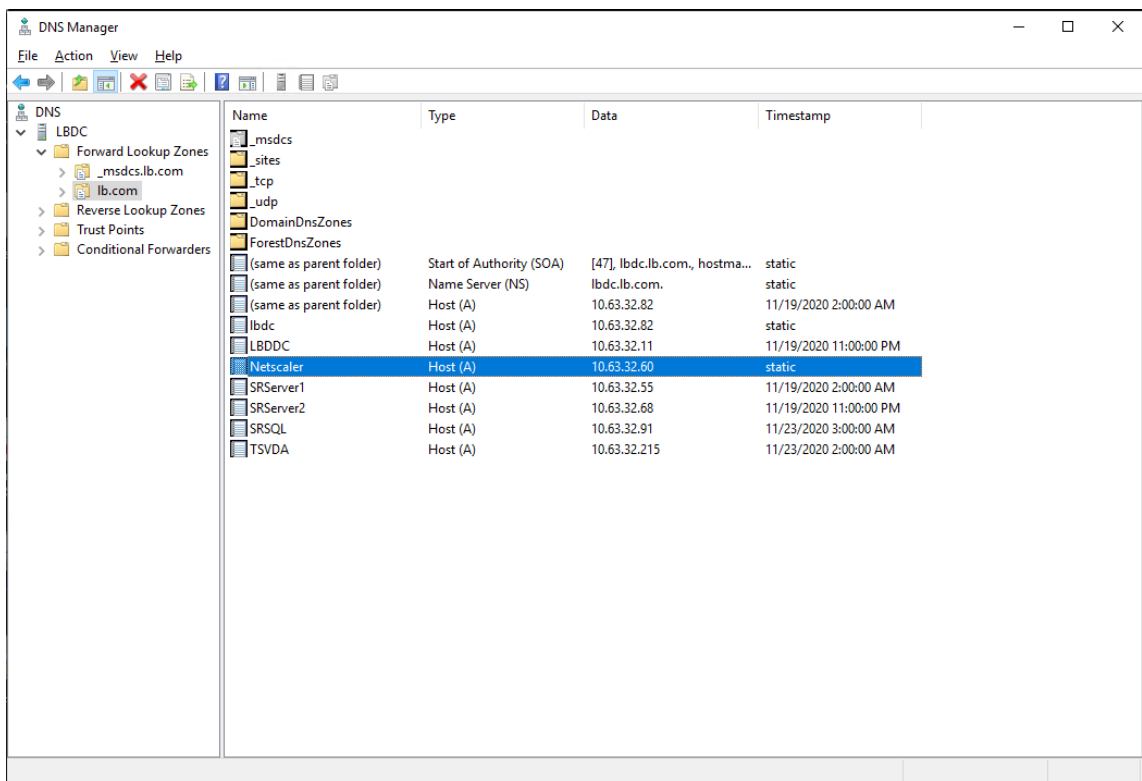
Tapez le nom de domaine complet de votre adresse VIP Citrix ADC dans la zone **Serveur d'enregistrement de session**.



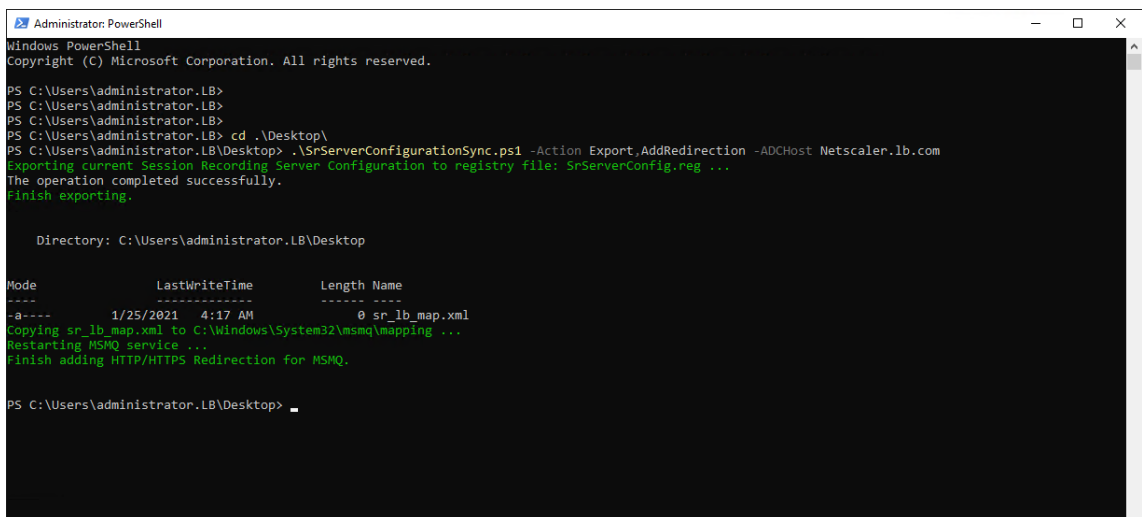
Sur chaque serveur d'enregistrement de session, ajoutez et définissez la valeur DWORD `IgnoreOSNameValidation` sur 1 sous `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters`. Pour plus d'informations, consultez l'article [CTX248554](#) du centre de connaissances.

4. Effectuez cette étape si vous utilisez MSMQ sur HTTP ou HTTPS.

(Ignorer si cette étape a été effectuée.) Créez un enregistrement hôte pour l'adresse VIP Citrix ADC sur le contrôleur de domaine.

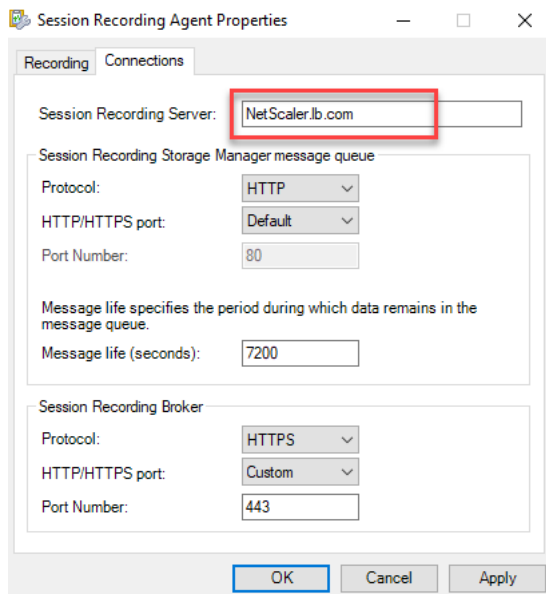


Sur chaque serveur d'enregistrement de session, exécutez la commande powershell.exe -file SrServerConfigurationSync.ps1 -Action AddRedirection - ADCHost <ADCHost> pour ajouter des redirections de Citrix ADC vers l'hôte local. <ADCHost> est le nom de domaine complet de l'adresse VIP Citrix ADC. Un fichier de redirection, par exemple, sr_lb_map.xml, est généré sous C:\Windows\System32\msmq\Mapping.



Remarque : accédez au dossier où SrServerConfigurationSync.ps1 réside lorsque vous exécutez PowerShell.exe.

Tapez le nom de domaine complet de votre adresse VIP Citrix ADC dans la zone **Serveur d'enregistrement de session**. Par exemple :



Étape 5 – Configurer un lecteur d'enregistrement de session existant pour prendre en charge l'équilibrage de charge

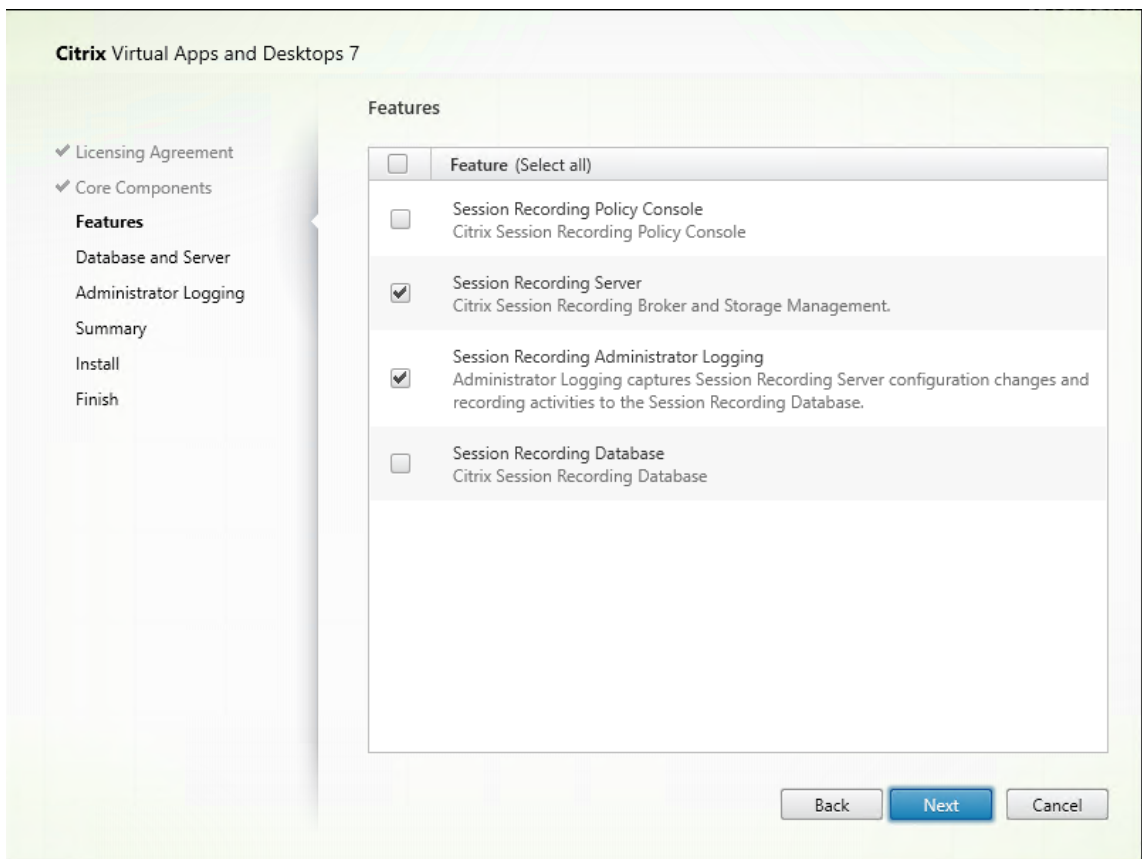
Sur chaque machine sur laquelle vous avez installé le composant Lecteur d'enregistrement de session, ajoutez l'adresse VIP Citrix ADC ou son nom de domaine complet en tant que serveur d'enregistrement de session connecté.

Étape 6 – Vérifier si l'équilibrage de charge fonctionne pour le serveur d'enregistrement de session existant configuré

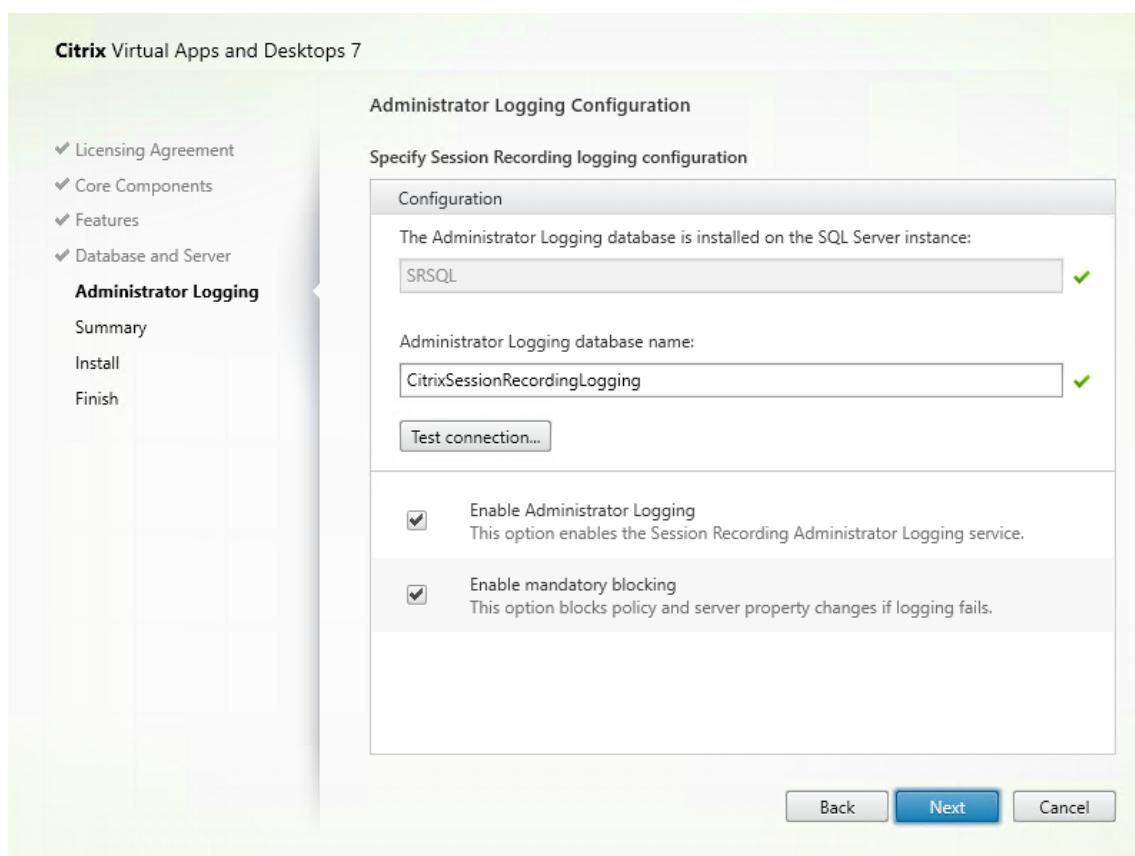
1. Lancez une session virtuelle Citrix.
2. Vérifiez si la session peut être enregistrée.
3. Vérifiez si le lecteur Web et le lecteur d'enregistrement de session peuvent lire le fichier d'enregistrement.

Étape 7 – Ajouter d'autres serveurs d'enregistrement de session

1. Préparez une machine dans le même domaine et installez uniquement les modules Serveur d'enregistrement de session et Journalisation de l'Administrateur d'enregistrement de session sur la machine.

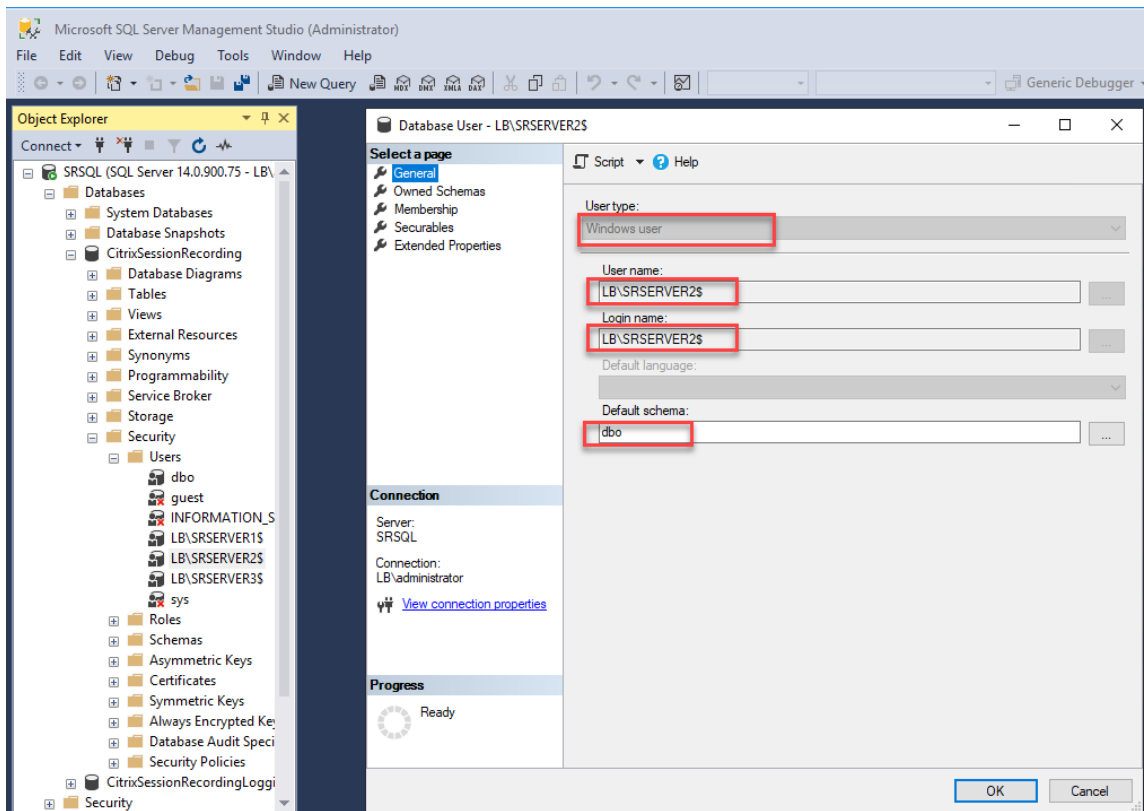


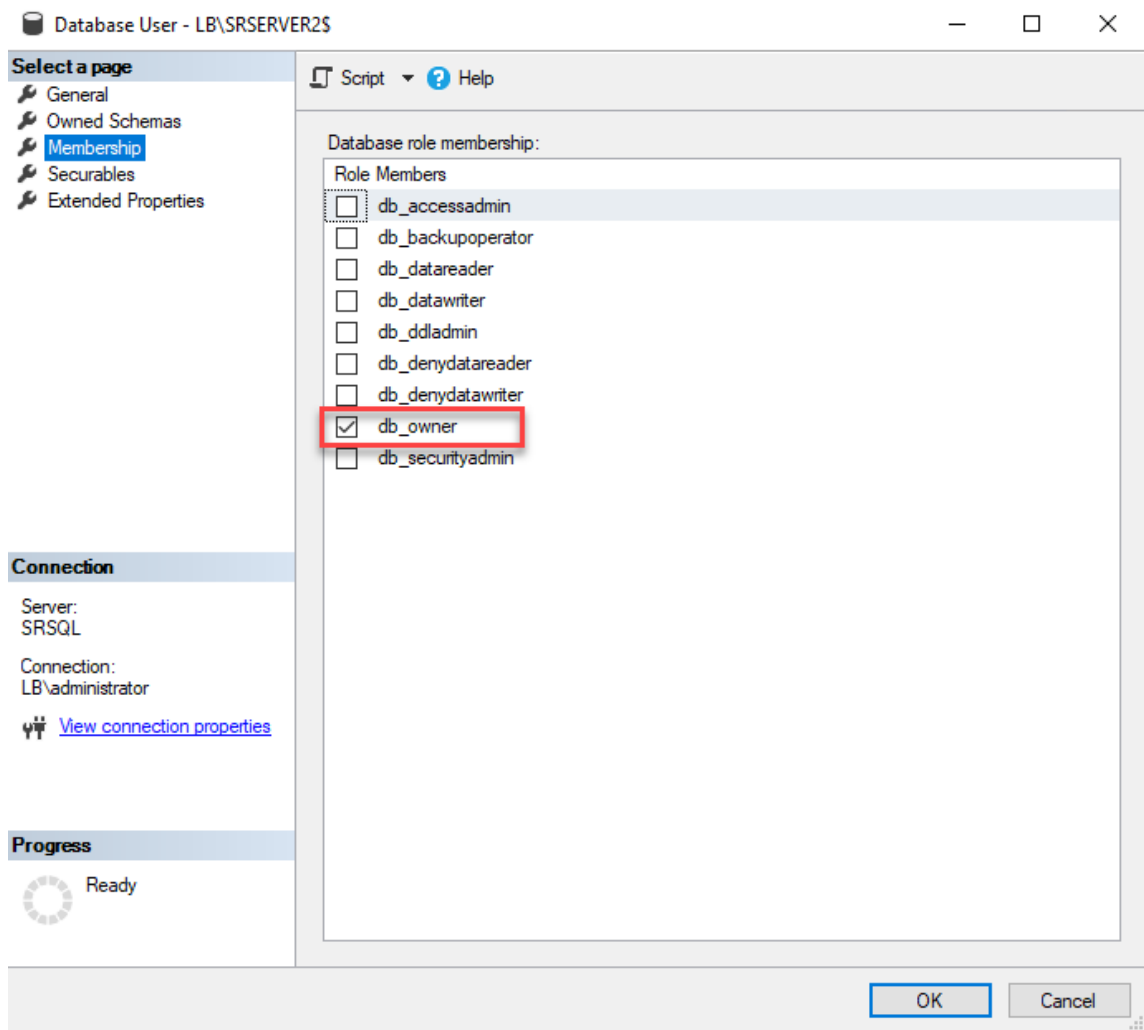
2. Utilisez les mêmes noms de base de données que le serveur d'enregistrement de session existant. Par exemple :



3. Désactivez le pare-feu réseau sur la machine.
4. Sur le serveur SQL sur lequel vous avez installé la base de données d'enregistrement de session, ajoutez tous les comptes de machine Serveur d'enregistrement de session à la base de données d'enregistrement de session partagée et accordez-leur l'autorisation `db_owner`. Par exemple :

Enregistrement de session 2210





5. Accordez l'autorisation de lecture/écriture des dossiers de stockage et de restauration d'enregistrement (par exemple `SessionRecordingsRestored` et `SessionRecording`) au compte de machine du nouveau serveur d'enregistrement de session, par exemple `LB\SRServer2$`. Le signe dollar \$ est requis.
6. Répétez l'Étape 3 pour ajouter des **services d'équilibrage de charge** pour le nouveau serveur d'enregistrement de session et modifier les serveurs virtuels existants pour ajouter des liaisons aux services d'équilibrage de charge. Il n'est pas nécessaire d'ajouter d'autres serveurs virtuels. Par exemple :

citrix ADC VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Search in Menu

- System >
- AppExpert >
- Traffic Management** >
 - Load Balancing >
 - Virtual Servers
 - Services
 - Service Groups
 - Monitors
 - Metric Tables
 - ☆ Servers
 - Persistence Groups
 - Radius Nodes !

Traffic Management / Load Balancing / Servers

Servers 2

Add Edit Delete Rename Select Action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE	IPADDRESS / DOMAIN
<input type="checkbox"/>	srv-1	● ENABLED	10.63.32.55
<input type="checkbox"/>	srv-2	● ENABLED	10.63.32.74
Total 2			

citrix ADC VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Search in Menu

- System >
- AppExpert >
- Traffic Management** >
 - Load Balancing >
 - Virtual Servers
 - ☆ Services
 - Service Groups
 - Monitors
 - Metric Tables
 - Servers
 - Persistence Groups
 - Radius Nodes !
 - Priority Load Balancing ! >
 - Content Switching ! >
 - Cache Redirection ! >
 - DNS >
 - GSLB ! >
 - SSL >
 - Subscriber >
 - Service Chaining >
 - User >

Traffic Management / Load Balancing / Services / Services

Services

Services 8 Auto Detected Services 0 Internal Services 6

Add Edit Delete Rename Statistics No action

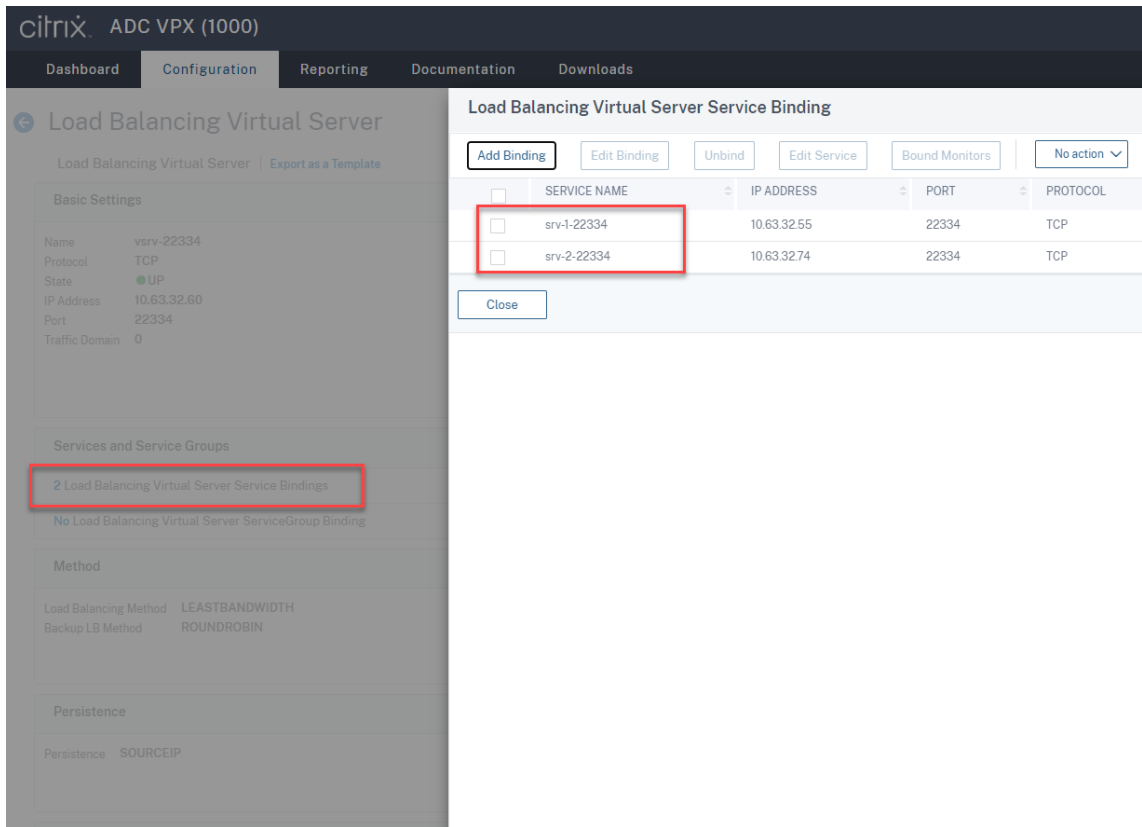
Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	SERVER STATE	IP ADDRESS/DOMAIN NAME	PORT	PROTOCOL
<input type="checkbox"/>	srv-1-80	● UP	10.63.32.55	80	TCP
<input type="checkbox"/>	srv-1-443	● UP	10.63.32.55	443	TCP
<input type="checkbox"/>	srv-1-1801	● UP	10.63.32.55	1801	TCP
<input type="checkbox"/>	srv-1-22334	● UP	10.63.32.55	22334	TCP
<input type="checkbox"/>	srv-2-443	● UP	10.63.32.74	443	TCP
<input type="checkbox"/>	srv-2-80	● UP	10.63.32.74	80	TCP
<input type="checkbox"/>	srv-2-1801	● UP	10.63.32.74	1801	TCP
<input type="checkbox"/>	srv-2-22334	● UP	10.63.32.74	22334	TCP
Total 8					

The screenshot shows the Citrix ADC VPX (1000) management interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The left sidebar contains a search menu and a tree view of configuration categories. The main content area is titled 'Virtual Servers' and shows a list of four virtual servers. The 'Edit' button is highlighted with a red box. The table below shows the details of the virtual servers.

<input type="checkbox"/>	NAME	STATE	EFFECTIVE STATE	IP ADDRESS
<input type="checkbox"/>	vsrv-80	● UP	● UP	10.63.32.60
<input type="checkbox"/>	vsrv-1801	● UP	● UP	10.63.32.60
<input type="checkbox"/>	vsrv-443	● UP	● UP	10.63.32.60
<input checked="" type="checkbox"/>	vsrv-22334	● UP	● UP	10.63.32.60

Total 4



7. Copiez le fichier de configuration de la console d'autorisation d'enregistrement de session `SessionRecordingAzManStore.xml` du serveur d'enregistrement de session existant vers le nouveau serveur d'enregistrement de session. Le dossier réside dans `<Session Recording Server installation path>\App_Data`.
8. Pour utiliser MSMQ sur HTTP ou HTTPS pour le nouveau serveur d'enregistrement de session, procédez comme suit pour importer les paramètres de registre du serveur d'enregistrement de session en cours de fonctionnement.

Sur le serveur d'enregistrement de session existant, par exemple `SrServer1`, exécutez la commande `powershell.exe -file SrServerConfigurationSync.ps1 -Action Export -ADCHost <ADCHost >`, où `<ADCHost>` est le nom de domaine complet de l'adresse VIP Citrix ADC. Un fichier de registre exporté, `SrServerConfig.reg`, est généré.

Copiez le fichier `SrServerConfig.reg` sur le nouveau serveur d'enregistrement de session et exécutez la commande `powershell.exe -file SrServerConfigurationSync.ps1 -Action Import,AddRedirection -ADCHost <ADCHost>`. La valeur **EnableLB** est ajoutée à la clé de registre du nouveau serveur d'enregistrement de session sous `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` et un fichier `sr_lb_map.xml` est ajouté sous `C:\Windows\System32\msmq\Mapping`.

9. Répétez la procédure pour ajouter un autre serveur d'enregistrement de session.

Dépanner

- Les sessions ne sont pas enregistrées lorsque vous utilisez un enregistrement CNAME ou un enregistrement ALIAS pour un serveur d'enregistrement de session. Pour plus d'informations, consultez l'article [CTX248554](#) du centre de connaissances.
- Les fichiers d'enregistrement peuvent être stockés localement mais ne peuvent pas être stockés dans un chemin UNC (Universal Naming Convention). Pour résoudre ce problème, définissez le mode de démarrage du service Gestionnaire de stockage d'enregistrement de session Citrix sur **Automatique (Démarrage différé)**.

Déployer et équilibrer la charge de l'enregistrement de session sur Azure

February 20, 2024

Conditions préalables

- Vous disposez déjà de Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) dans Azure.
- Vous disposez d'un compte Azure.

Étape 1 : télécharger le programme d'installation Citrix Virtual Apps and Desktops dans Azure

Remarque :

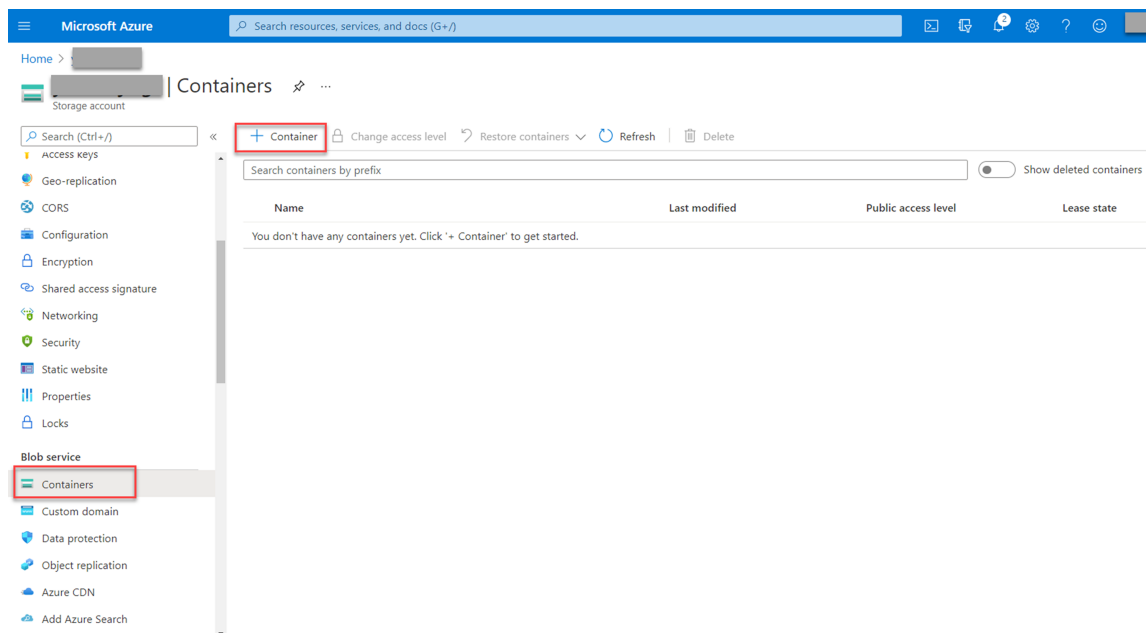
Ignorez l'étape 1 si vous utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de Citrix Virtual Apps and Desktops et télécharger le fichier ISO du produit vers une VM dans Azure.

1. Dans le [portail Azure](#), créez un compte de stockage **general-purpose v2** et acceptez le niveau de performance par défaut, **Standard**.

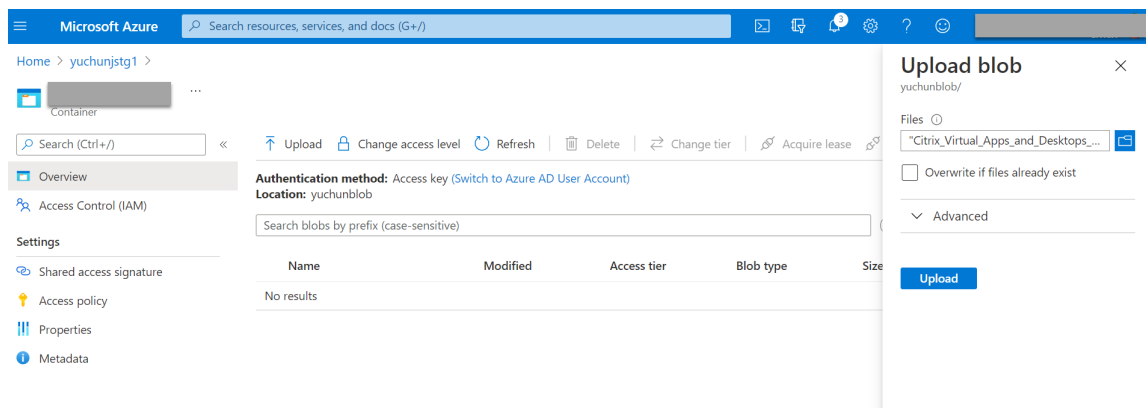
Tout accès au stockage Azure passe par un compte de stockage.

The screenshot shows the 'Create storage account' page in the Microsoft Azure portal. The page is titled 'Create storage account' and includes a breadcrumb trail: 'Home > Storage accounts >'. Below the title, there is a brief description of Azure Storage and a link to 'Learn more about Azure storage accounts'. The page is divided into two main sections: 'Project details' and 'Instance details'. In the 'Project details' section, there are dropdown menus for 'Subscription' (set to 'cse-dev-03-ca') and 'Resource group'. In the 'Instance details' section, there are fields for 'Storage account name', 'Location' (set to '(US) East US'), 'Performance' (with 'Standard' selected and 'Premium' unselected), 'Account kind' (set to 'StorageV2 (general purpose v2)'), and 'Replication' (set to 'Read-access geo-redundant storage (RA-GRS)'). A red rectangular box highlights the 'Performance' and 'Account kind' fields. At the bottom of the form, there are three buttons: 'Review + create', '< Previous', and 'Next: Networking >'. The browser's address bar shows 'portal.azure.com/#create/Microsoft.StorageAccount'.

2. Accédez à votre nouveau compte de stockage et sélectionnez **Conteneurs** dans la section **Service BLOB** pour créer un conteneur.



3. Téléchargez le programme d'installation Citrix Virtual Apps and Desktops dans le conteneur.



Étape 2 : créer une instance gérée SQL dans le portail Azure

Pour de plus amples informations, consultez la section [Créer une instance gérée SQL Azure](#).

Étape 3 : créer des machines virtuelles (VM) Azure

Choisissez **Windows Server 2019 Datacenter –Gen1** pour l'image et **Standard_D4as_v4 –4 vcpus, 16GiB memory** pour la taille. Pour de plus amples informations, consultez la section [Créer une machine virtuelle Windows dans le portail Azure](#).

portal.azure.com/#create/Microsoft.VirtualMachine

Microsoft Azure Search resources, services, and docs (G+/)

All services > Virtual machines >

Create a virtual machine

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ cse-dev-03-ca

Resource group * ⓘ (New) Resource group
[Create new](#)

Instance details

Virtual machine name * ⓘ

Region * ⓘ (US) East US

Availability options ⓘ No infrastructure redundancy required

Image * ⓘ Windows Server 2019 Datacenter - Gen1
[See all images](#)

Azure Spot instance ⓘ

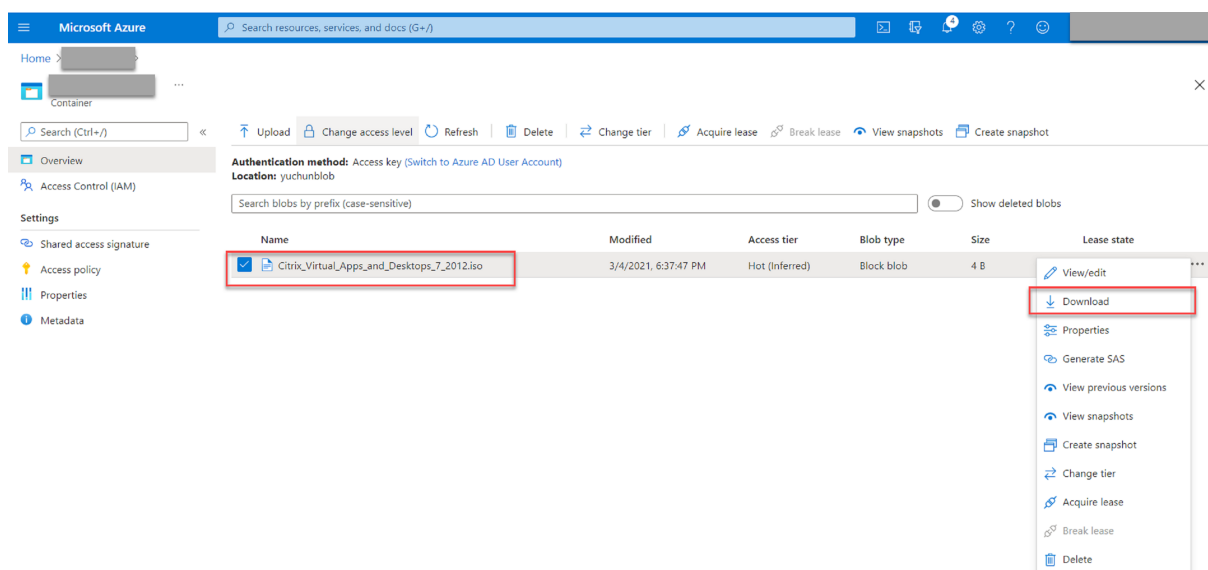
Size * ⓘ Standard_D4s_v3 - 4 vcpus, 16 GiB memory (\$83.22/month)
[See all sizes](#)

Administrator account

Username * ⓘ

[Review + create](#) < Previous Next : Disks >

Étape 4 : accéder au Bureau à distance et télécharger le programme d'installation Citrix Virtual Apps and Desktops sur les VM Azure



Étape 5 : exécuter le programme d'installation pour installer les composants d'enregistrement de session sur les VM Azure

Pour de plus amples informations, consultez la section [Installer les composants de l'administration de l'enregistrement de session](#).

Étape 6 : configurer un partage de fichiers Azure pour stocker des enregistrements

Pour créer un partage de fichiers Azure pour stocker des enregistrements, procédez comme suit :

1. Dans le [portail Azure](#), créez un compte de stockage, puis créez un partage de fichiers Azure.

Pour obtenir un guide de démarrage rapide, consultez la section [Créer et gérer des partages de fichiers Azure avec le portail Azure](#). Le tableau suivant vous recommande de prendre en considération ces configurations.

Taille du fichier d'enregistrement Mo/heure	Nombre de sessions enregistrées par jour	Type de partage de fichiers	Quota de partage de fichiers (To)	Nombre de serveur d'enregistrement de session	Taille du serveur d'enregistrement de session
< 6,37	< 1 000	Disque standard HDD (StorageV2)	2	1	Standard D4as_v4
< 6,37	1 000–2 000	SSD Premium	3	1	Standard D4as_v4
< 6,37	2 000–3 000	SSD Premium	5	1	Standard D4as_v4
< 6,37	3 000–4 000	SSD Premium	6	1	Standard D4as_v4
Environ 10	< 1 000	Disque standard HDD (StorageV2)	3	1	Standard D4as_v4
Environ 10	1 000–2 500	SSD Premium	6	1	Standard D4as_v4
Environ 10	2 500–4 000	SSD Premium	10	2	Standard D4as_v4

Le quota de partage de fichiers est calculé en fonction de huit heures par jour, de 23 jours ouvrables par mois et d'une période de conservation d'un mois pour chaque fichier d'enregistrement.

2. Ajoutez les informations d'identification du partage de fichiers Azure à l'hôte sur lequel vous avez installé le serveur d'enregistrement de session.

- a) Démarrez une invite de commandes en tant qu'administrateur et remplacez le lecteur dans le dossier **<chemin d'installation du serveur d'enregistrement de session>\Bin**.

Par défaut, le serveur d'enregistrement de session est installé dans `C:\Program Files\Citrix\SessionRecording\Server`.

- b) Exécutez la commande **SsRecUtils.exe -AddAzureFiles <storageAccountName> <file-ShareName> <accesskey>**

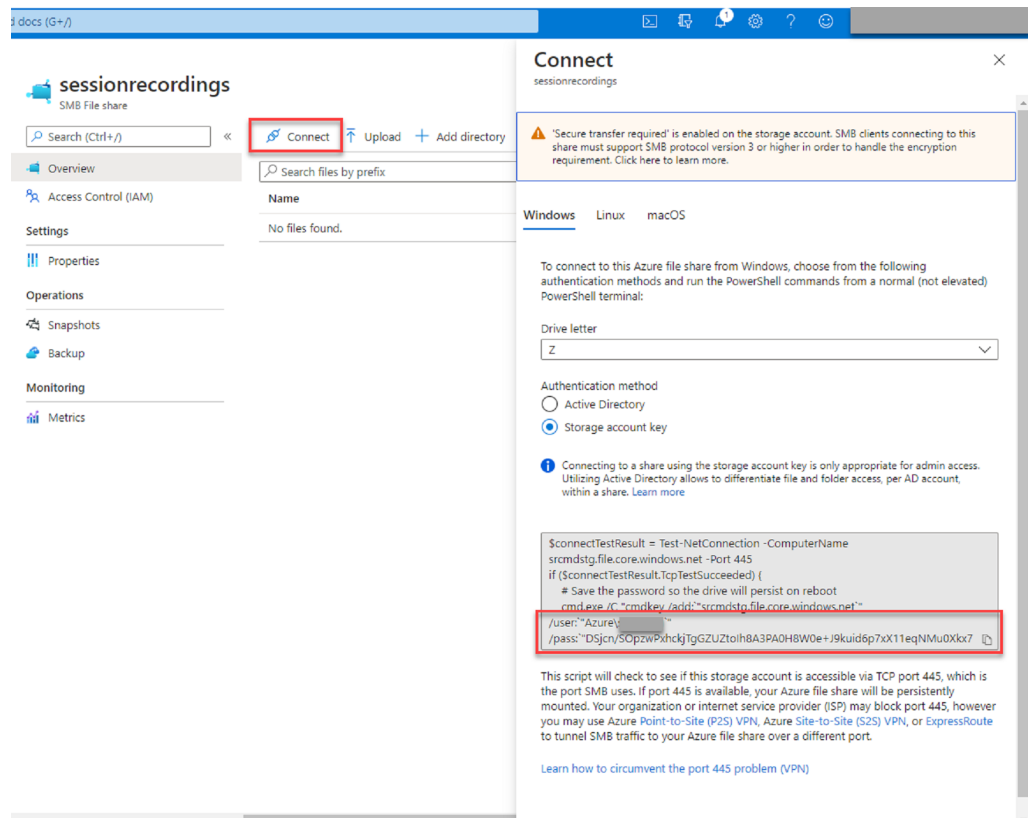
Où,

- **<storageaccountname>** est le nom de votre compte de stockage dans Azure.
- **<filesharename>** est le nom du partage de fichiers contenu dans votre compte de stockage.

- **<accesskey>** est votre clé de compte de stockage qui peut être utilisée pour accéder au partage de fichiers.

Il existe deux façons d'obtenir votre clé de compte de stockage :

- Vous pouvez obtenir votre clé de compte de stockage à partir de la chaîne de connexion qui apparaît lorsque vous cliquez sur le bouton **Connecter** sur votre page de partage de fichiers.

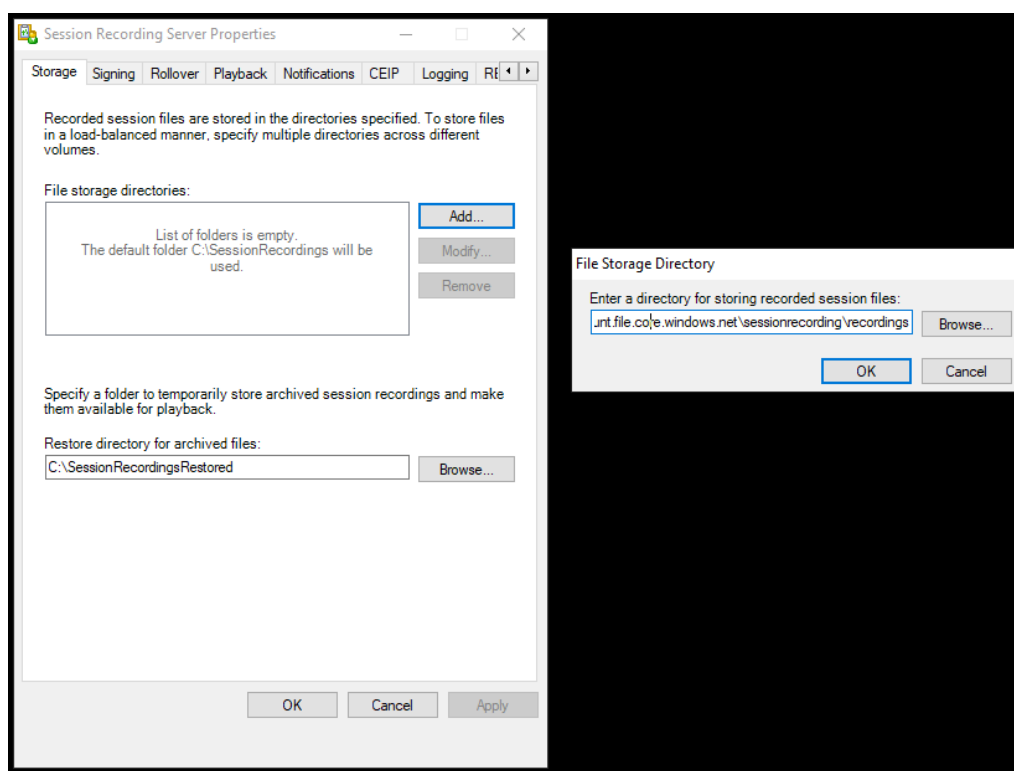


- Vous pouvez également obtenir votre clé de compte de stockage en cliquant sur **Clés d'accès** dans le panneau de navigation de gauche de la page de votre compte de stockage.

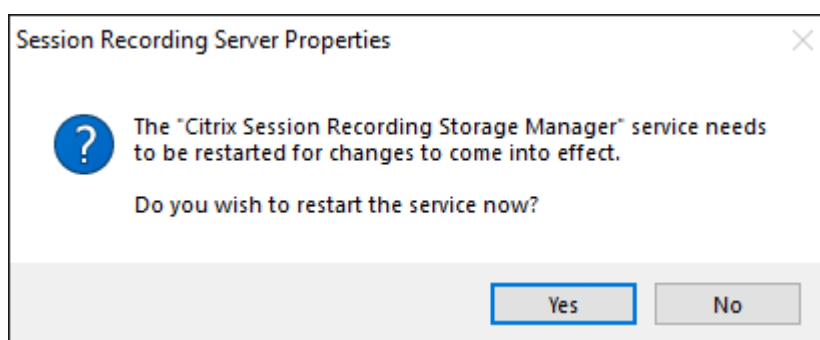
The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and the text 'Microsoft Azure'. Below this, the breadcrumb navigation shows 'Home > srcmd > [Storage account]'. The main heading is 'Access keys'. A search bar is present below the heading. On the left, a navigation menu lists various options, with 'Access keys' highlighted in a red box. The main content area contains instructions on using access keys and a 'Hide keys' button. Two keys are listed: 'key1' and 'key2', each with a refresh icon, a key value, and a connection string.

- c) Montez le partage de fichiers Azure sur l'hôte sur lequel vous avez installé le serveur d'enregistrement de session.
- Ouvrez **Propriétés du serveur d'enregistrement de session**.
 - Cliquez sur **Ajouter** sur l'onglet **Stockage**.
 - Entrez le chemin UNC au format `\\<storageaccountname>.file.core.windows.net\<filessharename>`

Spécifiez un sous-dossier sous le partage de fichiers pour stocker vos fichiers d'enregistrement. Le serveur d'enregistrement de session crée automatiquement le sous-dossier.



- iv. Cliquez sur **OK** dans la boîte de dialogue **Répertoire de stockage des fichiers**.
- v. Cliquez sur **Appliquer** dans la fenêtre **Propriétés du serveur d'enregistrement de session**.
- vi. Cliquez sur **OK** une fois que l'option **Appliquer** devient grisée.
- vii. Cliquez sur **Oui** lorsque vous êtes invité à redémarrer le service Gestionnaire de stockage d'enregistrement de session.



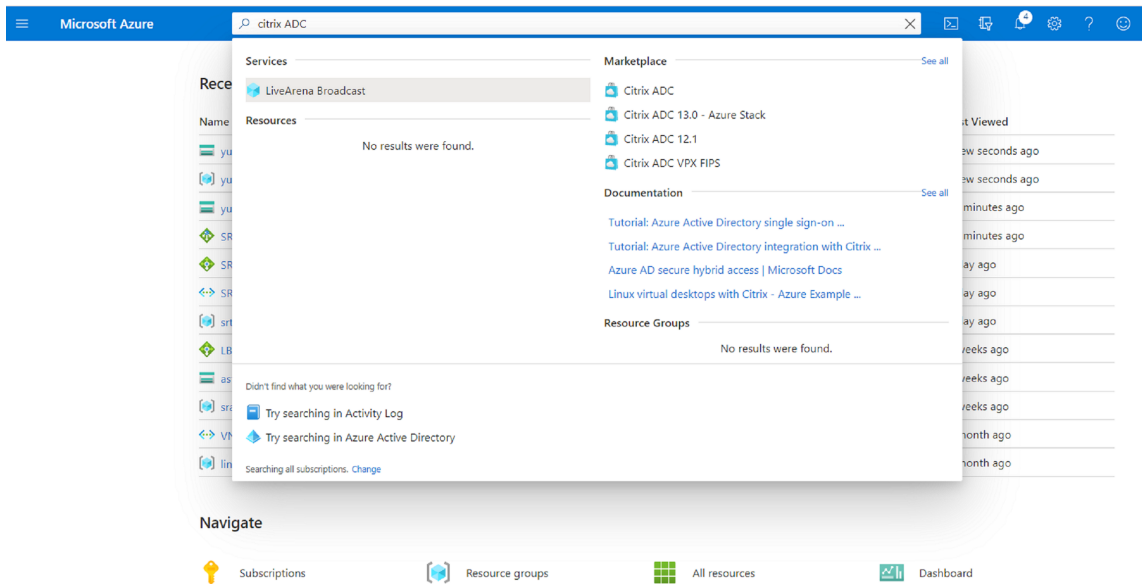
Étape 7 : ajouter un équilibreur de charge

S'il existe plusieurs serveurs d'enregistrement de session, nous vous recommandons d'ajouter un équilibreur de charge. Azure offre de nombreuses options pour équilibrer la charge des demandes

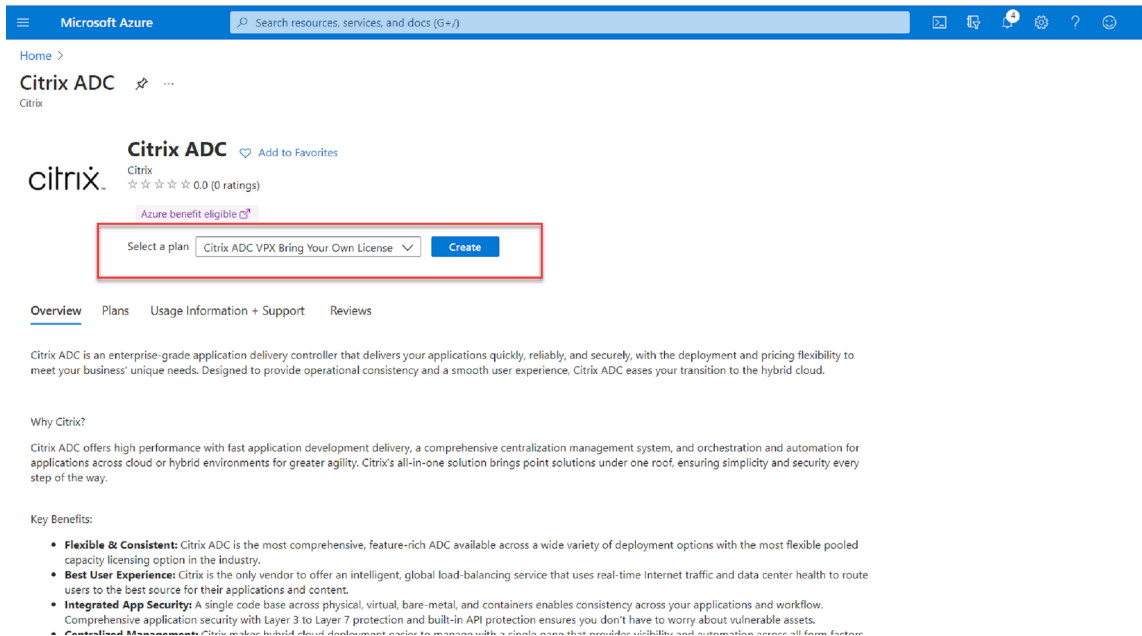
de trafic. Cette section vous guide tout au long du processus de création de Citrix ADC, Azure Load Balancer et Azure Application Gateway dans Azure.

Option 1 : créer une instance Citrix ADC VPX dans Azure

1. Dans le [portail Azure](#), tapez Citrix ADC dans la zone de recherche.

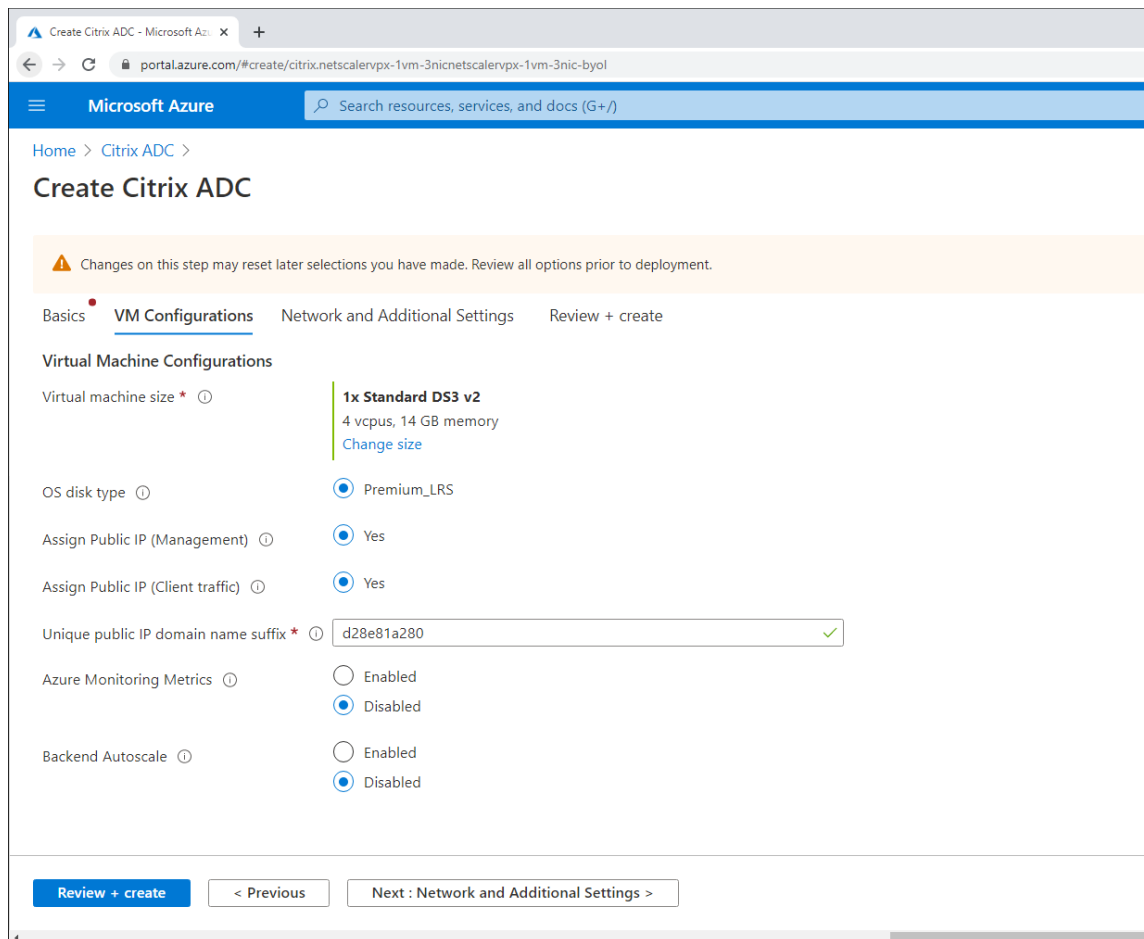


2. Choisissez le plan **Citrix ADC VPX –BYOL (utilisez votre propre licence)**, puis cliquez sur **Créer**.



3. Sélectionnez ou créez un groupe de ressources et définissez les autres paramètres dans l'onglet **Options de base**.

4. Définissez les configurations des machines virtuelles.



5. Vérifiez et modifiez les paramètres réseau si nécessaire. Choisissez **ssh (22)**, **http (80)**, **https (443)** pour les ports entrants publics.

Un réseau virtuel est automatiquement créé. Si un environnement d'enregistrement de session est déjà installé, vous pouvez utiliser ses paramètres de réseau virtuel et de sous-réseau serveur.

Microsoft Azure Search resources, services, and docs (G+)

Home > Citrix ADC >

Create Citrix ADC

Configure virtual networks

Virtual network * ⓘ (new) citrix-adc-vpx-virtual-network ▼
[Create new](#)

Management Subnet * ⓘ (new) 01-management-subnet (10.128.0/24) ▼

Client Subnet * ⓘ (new) 11-client-subnet (10.129.0/24) ▼

Server Subnet * ⓘ (new) 12-server-subnet (10.130.0/24) ▼

Public IP (Management)

Management Public IP (NSIP) * ⓘ (new) citrix-adc-vpx-nsip ▼
[Create new](#)

Management Domain Name ⓘ citrix-adc-vpx-nsip-23f12ee6b2 ✓
.eastus.cloudapp.azure.com

Public IP (Clientside)

Clientside Public IP (VIP) * ⓘ (new) citrix-adc-vpx-vip ▼
[Create new](#)

Clientside Domain Name ⓘ citrix-adc-vpx-vip-23f12ee6b2 ✓
.eastus.cloudapp.azure.com

Public Inbound Ports (Management only)

Ports open for Management public IP ⓘ None
 ssh (22)
 ssh (22), http (80), https (443)

Review + create < Previous Next : Review + create >


The screenshot shows the 'Create Citrix ADC' wizard in the Microsoft Azure portal, specifically the 'Network and Additional Settings' step. The breadcrumb navigation is 'Home > Citrix ADC >'. The main title is 'Create Citrix ADC'. Below the title, there are four tabs: 'Basics', 'VM Configurations', 'Network and Additional Settings' (which is active and underlined), and 'Review + create'. The 'Boot diagnostics' section has a 'Diagnostic storage account' dropdown menu with the value '(new) citrixadcpxe42b4be259' and a 'Create New' link below it. The 'Network Settings' section is titled 'Configure virtual networks' and contains four dropdown menus: 'Virtual network' with '(new) citrix-adc-vpx-virtual-network' and a 'Create new' link; 'Management Subnet' with '(new) 01-management-subnet (10.1.32.0/24)'; 'Client Subnet' with '(new) 11-client-subnet (10.1.33.0/24)'; and 'Server Subnet' with '(new) 12-server-subnet (10.1.34.0/24)'. The 'Accelerated Networking' section has three radio button options, all of which are selected to 'On': 'Accelerated Networking (Management Interface)', 'Accelerated Networking (Client Interface)', and 'Accelerated Networking (Server Interface)'. The 'Public IP (Management)' section has a 'Management Public IP (NSIP)' dropdown menu with the value '(new) citrix-adc-vpx-nsip' and a 'Create new' link below it. At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Review + create >'.

6. Cliquez sur **Suivant : Vérifier + créer** pour créer l'instance Citrix ADC VPX et attendez la fin du déploiement.

Microsoft Azure Search resources, services, and documentation

Home > Citrix ADC >

Create Citrix ADC

 Validation Passed

Basics VM Configurations Network and Additional Settings Review + create

PRODUCT DETAILS

Citrix ADC
by Citrix
[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics

Subscription	cse-dev-03-ca
Resource group	srcmdtest
Region	East US
Citrix ADC Release Version	13.0
License Subscription	Bring Your Own License
Virtual Machine name	citrix-adc-vpx
Username	nsroot
Password	*****

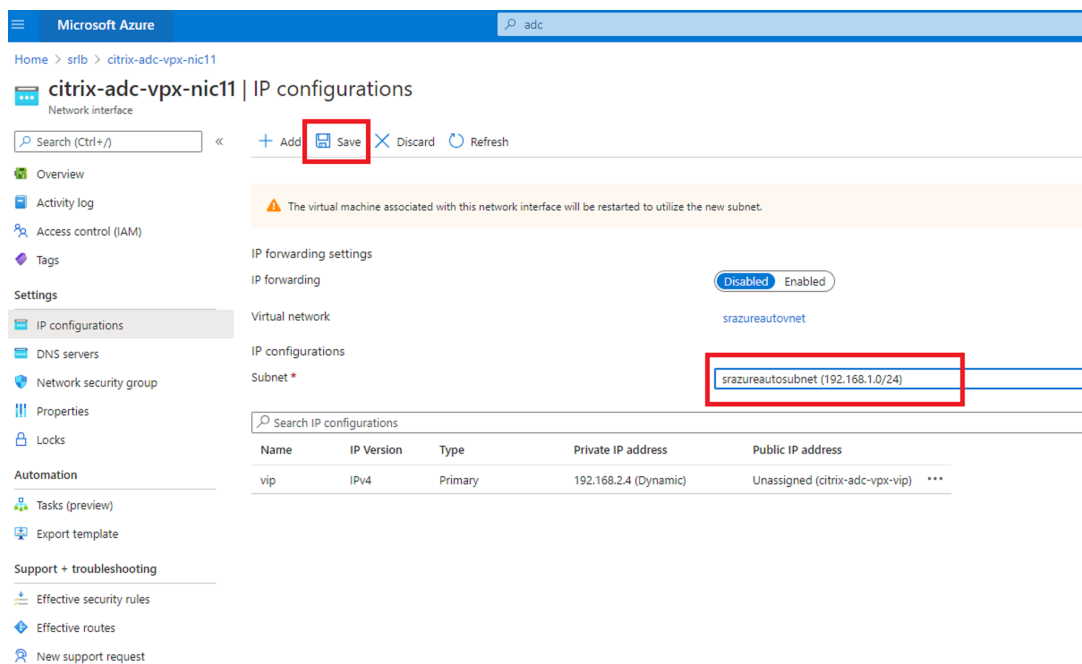
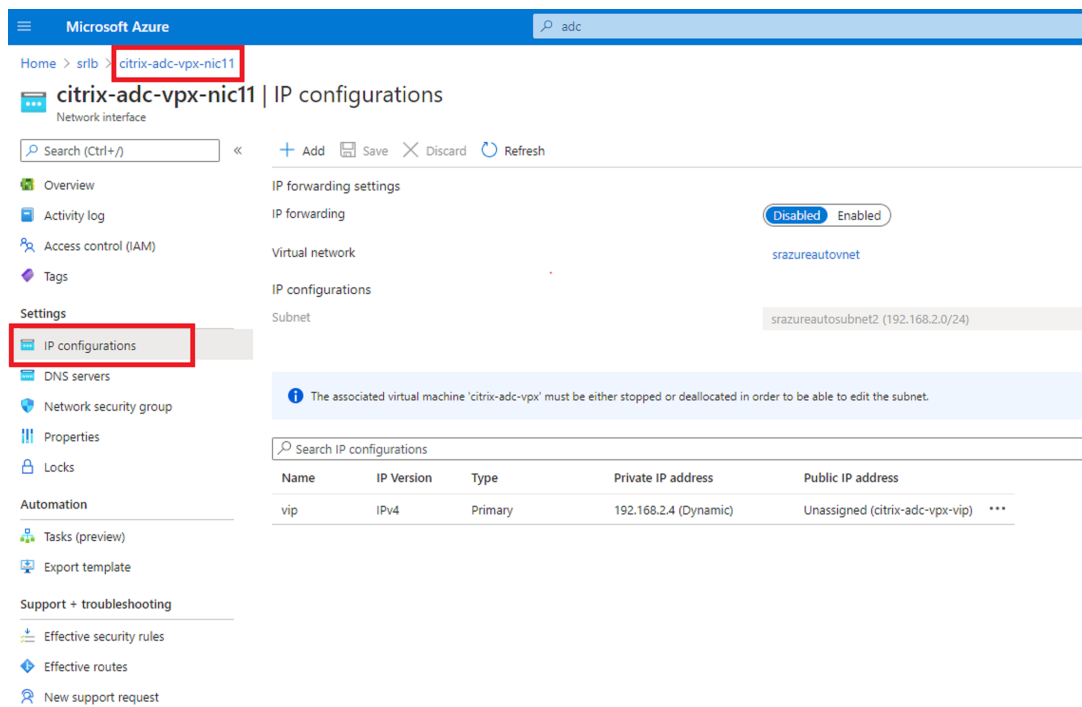
VM Configurations

[Create](#) [< Previous](#) [Next](#) [Download a template for automation](#)

7. Définissez l'adresse IP du sous-réseau (SNIP) et l'adresse VIP Citrix ADC sur le même sous-réseau.

L'adresse SNIP et l'adresse VIP doivent se trouver sur le même sous-réseau. Dans cet exemple, nous définissons l'adresse VIP sur le sous-réseau de l'adresse SNIP.

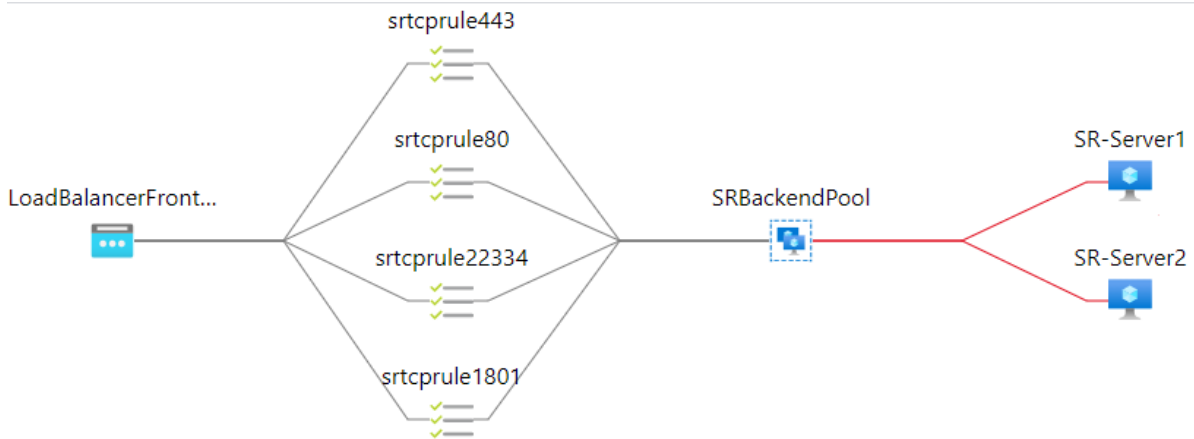
- Arrêtez la machine virtuelle **citrix-adc-vpx**.
- Modifiez le sous-réseau de l'adresse VIP.



c) Démarrez la machine virtuelle **citrix-adc-vpx**.

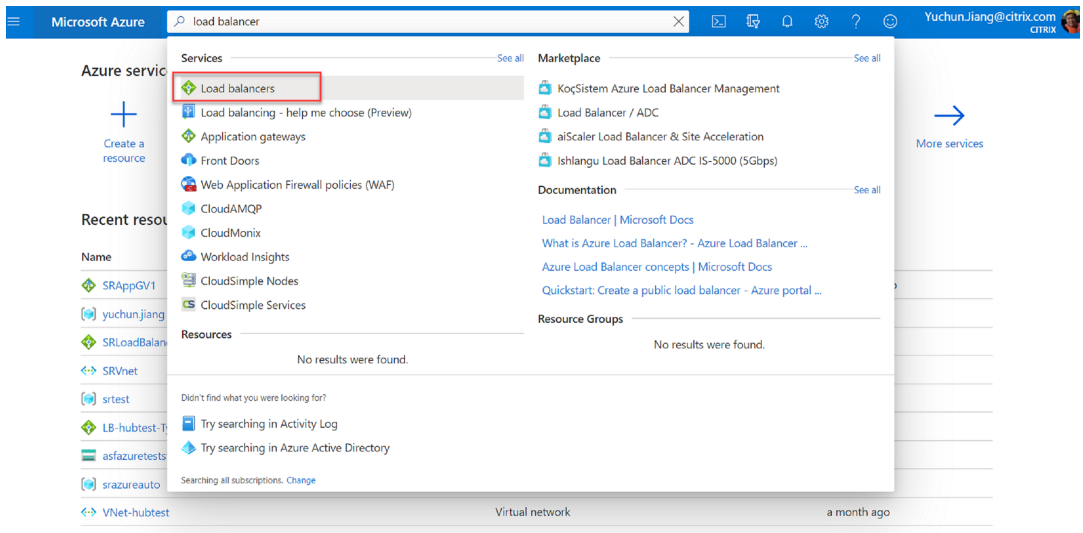
Option 2 : créer un équilibreur de charge Azure

Azure Load Balancer est un service TCP pass-through. Le diagramme suivant montre l'équilibrage de charge via TCP passthrough.



1. Créez un équilibreur de charge Azure.

a) Effectuez une recherche dans le portail Azure et sélectionnez **Équilibrages de charge** dans **Marketplace**.



Sur l'onglet **Options de base** de la page **Créer un équilibreur de charge**, configurez les paramètres comme décrit dans le tableau suivant :

Paramètre	Valeur
Abonnement	Sélectionnez votre abonnement.
Groupe de ressources	Par exemple, sélectionnez le groupe srlbtest créé précédemment.
Nom	Entrez SRLoadBalance .
Région	Sélectionner (États-Unis) Est des États-Unis .
Type	Sélectionner Interne .

Paramètre	Valeur
SKU	Sélectionner Standard
Réseau virtuel	Par exemple, sélectionnez le réseau srazureautovnet créé précédemment
Sous-réseau	Par exemple, sélectionnez le sous-réseau srazureautosubnet créé précédemment.
Affectation d'adresses IP	Sélectionnez Dynamique .
Zone de disponibilité	Sélectionner Redondant dans une zone .

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Create load balancer

is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription * cse-dev-03-ca

Resource group * srlbtest [Create new](#)

Instance details

Name * SRLoadBalance

Region * (US) East US

Type * Internal Public

SKU * Basic Standard

Configure virtual network.

Virtual network * srazureautovnet

Subnet * srazureautosubnet (192.168.1.0/24) [Manage subnet configuration](#)

IP address assignment * Static Dynamic

Availability zone * Zone-redundant

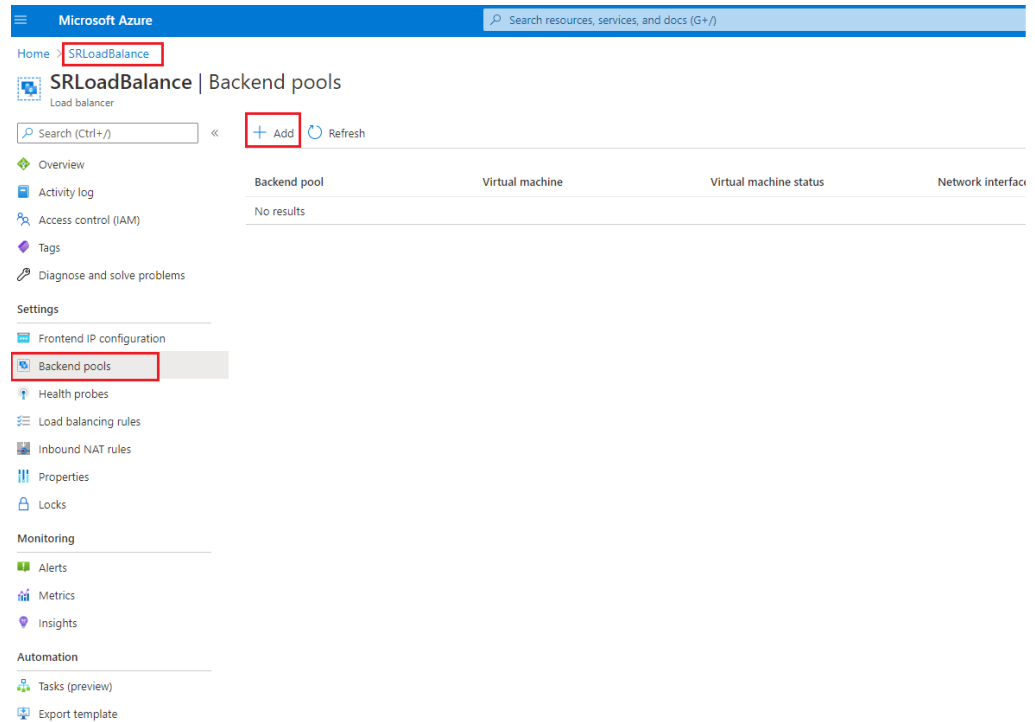
[Review + create](#) < Previous Next : Tags > [Download a template for automation](#)

b) Ajoutez des ressources d'équilibrage de charge, y compris un pool principal, des sondes

d'intégrité et des règles d'équilibrage de charge.

- Ajoutez un pool principal.

Sélectionnez l'équilibreur de charge que vous avez créé dans la liste des ressources et cliquez sur **Pools principaux** dans le panneau de navigation de gauche. Cliquez sur **Ajouter** pour ajouter un pool principal.



Donnez un nom au nouveau pool principal, puis cliquez sur **Ajouter**.

Microsoft Azure

Home > SRLoadBalance >

Add backend pool

SRLoadBalance

Name *

Virtual network

IP version IPv4 IPv6

Virtual machines

You can only attach virtual machines in eastus that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

[+ Add](#) [X Remove](#)

Virtual machine ↑↓	IP Configuration ↑↓	Availability set ↑↓
No virtual machines selected		

Virtual machine scale sets

Virtual Machine Scale Sets must be in same location as Load Balancer. Only IP configurations that have the same SKU (Basic/Standard) as the Load Balancer can be selected. All of the IP configurations have to be in the same Virtual Network.

i No virtual machine scale set is found in eastus that matches the above criteria

[Add](#)

- Ajoutez des sondes d'intégrité.
Sélectionnez l'équilibreur de charge que vous avez créé dans la liste des ressources, puis cliquez sur **Sondes d'intégrité** dans le panneau de navigation de gauche.

Enregistrement de session 2210

The screenshot shows the Microsoft Azure portal interface for a Load balancer named SRLoadBalance. The left-hand navigation pane is visible, with the 'Health probes' option highlighted. In the main content area, there is a search bar and a table of health probes. The table currently shows 'No results.' A red box highlights the '+ Add' button next to the search bar, and another red box highlights the 'Health probes' menu item in the left sidebar.

Cliquez sur **Ajouter** pour ajouter des sondes d'intégrité sur les ports 80, 22334, 1801 et 443.

The screenshot shows the same Microsoft Azure portal interface, but now the table of health probes is populated with four entries. The table has columns for Name, Protocol, Port, and Used By. The 'Add' and 'Refresh' buttons are visible above the table. The 'Health probes' menu item in the left sidebar is also highlighted.

Name	Protocol	Port	Used By
SRHealthProbe1801	TCP	1801	SRTCPRule1801
SRHealthProbe22334	TCP	22334	SRTCPRule22334
SRHealthProbe443	TCP	443	SRTCPRule443
SRHealthProbe80	TCP	80	SRTCPRule80

Par exemple, utilisez les paramètres suivants pour créer une sonde d'intégrité sur le port 80.

Paramètre

Valeur

Nom

Entrez **SRHealthProbe80**.

Protocole

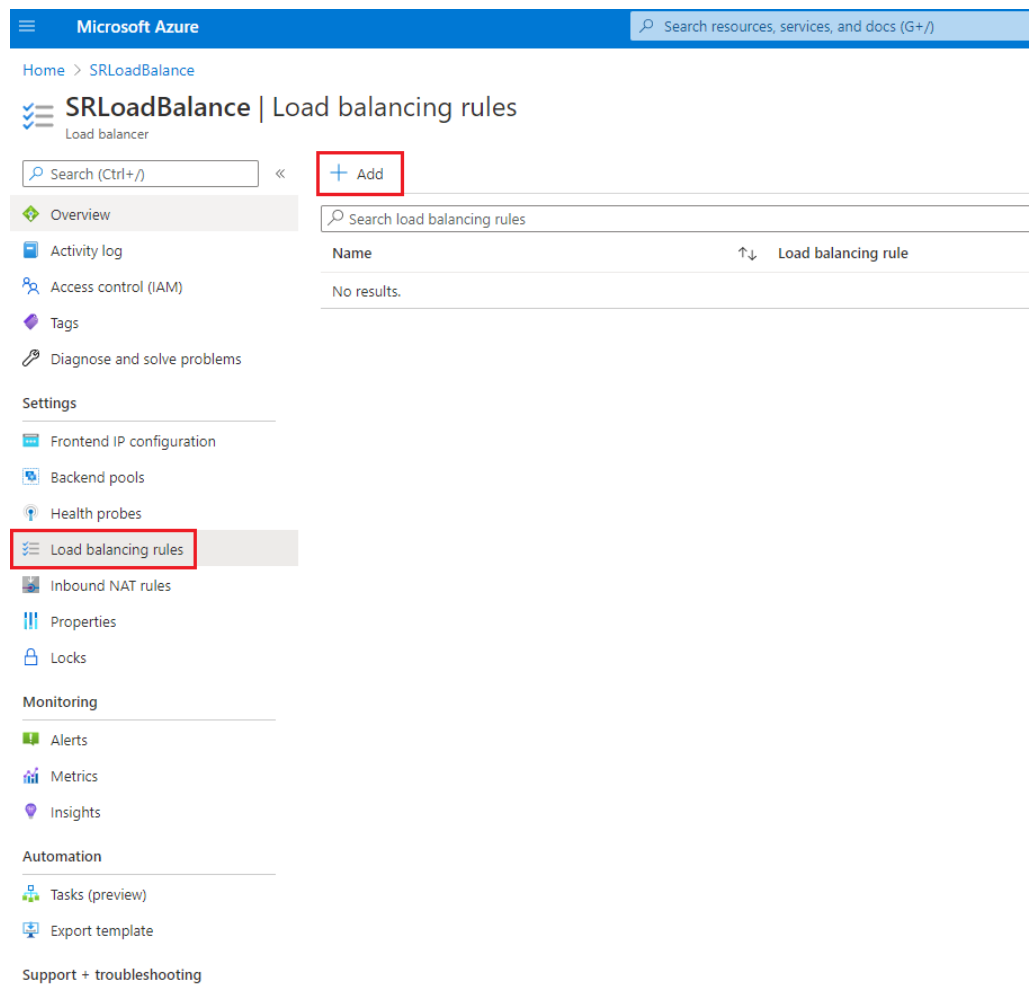
Sélectionnez **TCP**.

Paramètre	Valeur
Port	Entrez 80 .
Intervalle	5
Seuil de défaillance sur le plan de l'intégrité	Sélectionnez 2 pour le seuil de défaillance sur le plan de l'intégrité ou le nombre d'échecs de sonde consécutifs devant se produire avant qu'une machine virtuelle soit considérée comme défaillante sur le plan de l'intégrité.

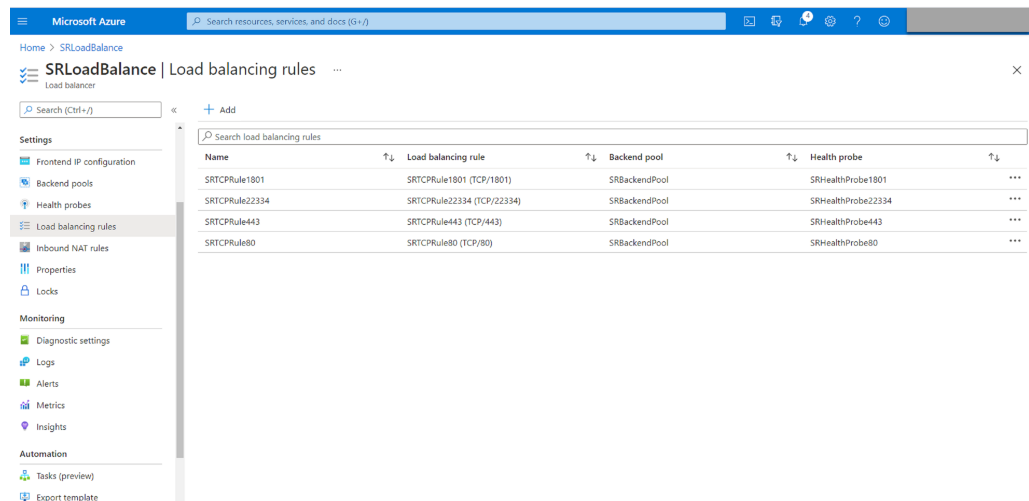
The screenshot shows the configuration page for an SRHealthProbe resource in the Microsoft Azure portal. The breadcrumb navigation is 'Home > SRLoadBalance > SRHealthProbe'. Below the resource name, there are 'Save', 'Discard', and 'Delete' buttons. The configuration fields are as follows:

- Name ***: SRHealthProbe80
- Protocol ⓘ**: TCP
- Port * ⓘ**: 80
- Interval * ⓘ**: 5 seconds
- Unhealthy threshold * ⓘ**: 2 consecutive failures
- Used by ⓘ**: Not used

- Ajoutez une règle d'équilibrage de charge.
Sélectionnez l'équilibreur de charge que vous avez créé dans la liste des ressources, puis cliquez sur **Règles d'équilibrage de charge** dans le panneau de navigation de gauche. Cliquez sur **Ajouter** pour ajouter une règle d'équilibrage de charge.



Cliquez sur **Ajouter** pour ajouter des règles d'équilibrage de charge associées aux ports 80, 22334, 1801 et 443.



Par exemple, utilisez les paramètres suivants pour créer une règle d'équilibrage de charge associée au port 80.

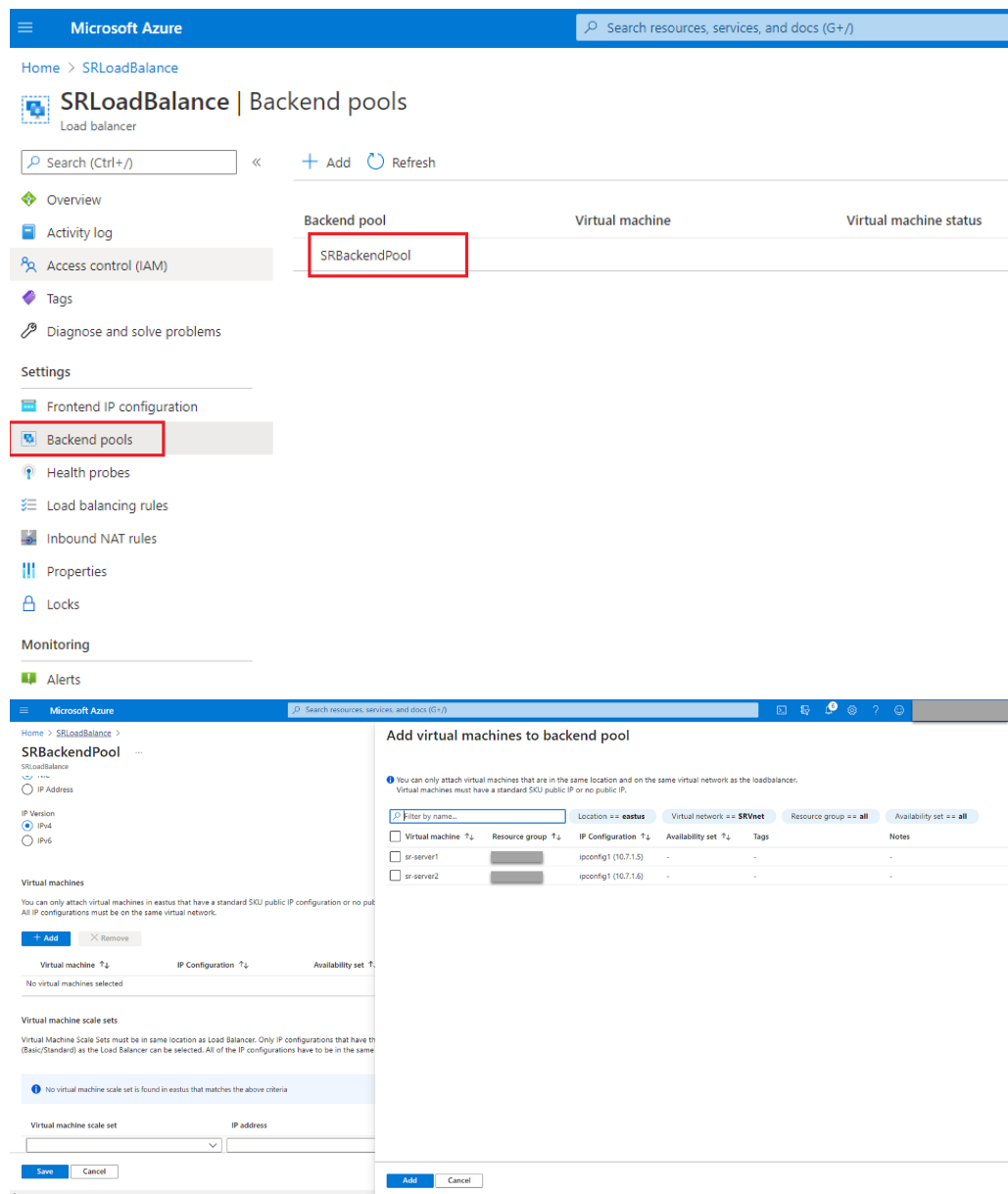
Paramètre	Valeur
Nom	Entrez un nom, par exemple, SRTCPRule80 .
Version IP	Sélectionner IPv4 .
Adresse IP frontale	Sélectionnez LoadBalancerFrontEnd .
Protocole	Sélectionnez TCP .
Port	Entrez 80 .
Port principal	Entrez 80 .
Pool principal	Sélectionnez SRBackendPool .
Sonde d'intégrité	Sélectionnez SRHealthProbe80 .
Persistance de session	Sélectionnez IP du client .
Délai d'inactivité (minutes)	Acceptez le paramètre par défaut.
Réinitialisation TCP	Sélectionnez Activé .
Traduction d'adresses réseau sources sortantes (SNAT)	Sélectionnez (Recommandé) Utiliser des règles de trafic sortant pour fournir aux membres du pool principal l'accès à Internet .

The screenshot shows the 'Add load balancing rule' configuration page in the Microsoft Azure portal. The page is titled 'Add load balancing rule' and is for a resource named 'SRLoadBalance'. The configuration fields are as follows:

- Name ***: SRTCPRule80
- IP Version ***: IPv4 (selected), IPv6
- Frontend IP address ***: 192.168.1.23 (LoadBalancerFrontEnd)
- HA Ports**:
- Protocol**: TCP (selected), UDP
- Port ***: 80
- Backend port ***: 80
- Backend pool**: SRBackendPool
- Health probe**: SRHealthProbe80 (TCP:80)
- Session persistence**: Client IP
- Idle timeout (minutes)**: 4
- TCP reset**: Enabled (selected), Disabled
- Floating IP**: (empty)

An 'OK' button is located at the bottom of the form.

- Ajoutez les machines virtuelles Azure sur lesquelles le serveur d'enregistrement de session est installé au pool principal.



c) Testez l'équilibreur de charge Azure.

Si vous ne pouvez pas ajouter un serveur au pool principal et que le message d'erreur suivant s'affiche **NetworkInterfaceAndLoadBalancerAreInDifferentAvailabilitySets**, dissociez l'adresse IP publique de l'interface réseau du serveur.

Microsoft Azure

Home > srlbtest > SR-Server1-ip > sr-server172 >

ipconfig1

sr-server172

Save Discard

Public IP address settings

Public IP address

Disassociate Associate

Public IP address *

SR-Server1-ip (20.62.236.36)

Create new

Private IP address settings

Virtual network/subnet

srazureautovnet/srazureautosubnet

Assignment

Dynamic Static

IP address

192.168.1.19

Option 3 : créer une passerelle d'application Azure Application Gateway

Conseil :

Application Gateway V2 ne prend pas en charge les demandes de routage via un proxy compatible NTLM.

1. Créez une passerelle d'application Azure Application Gateway.

Configurez les paramètres suivants lorsque vous créez une passerelle d'application.

- Sur l'onglet **Option de base**, définissez **Niveau** sur **Standard**.
- Sur l'onglet **Serveurs frontaux**, définissez **Type d'adresse IP frontale** sur **Privé**. La nouvelle passerelle d'application est utilisée comme équilibreur de charge interne.

2. Ajoutez un pool principal.

[Home](#) > [SRAppGV1](#) >

Edit backend pool

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name

AGbackendpool

Add backend pool without targets

Yes

No

Backend targets

2 items

Target type	Target	
IP address or FQDN	192.168.1.13	...
IP address or FQDN	192.168.1.18	...
IP address or FQDN	<input type="text"/>	

Associated rule

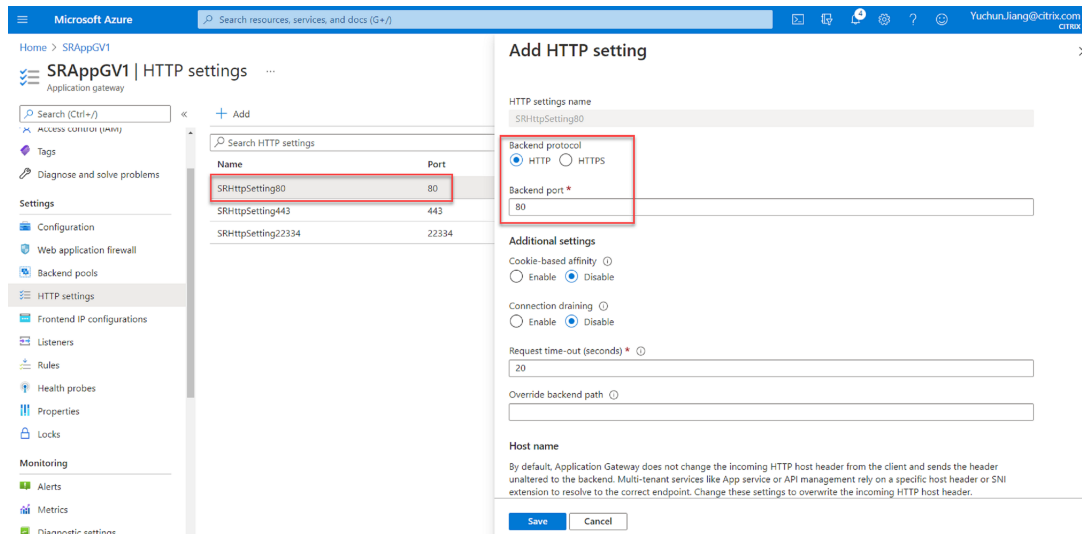
[SRHttpRule80](#)

[SRHttpRule443](#)

3. Créez des paramètres HTTP.

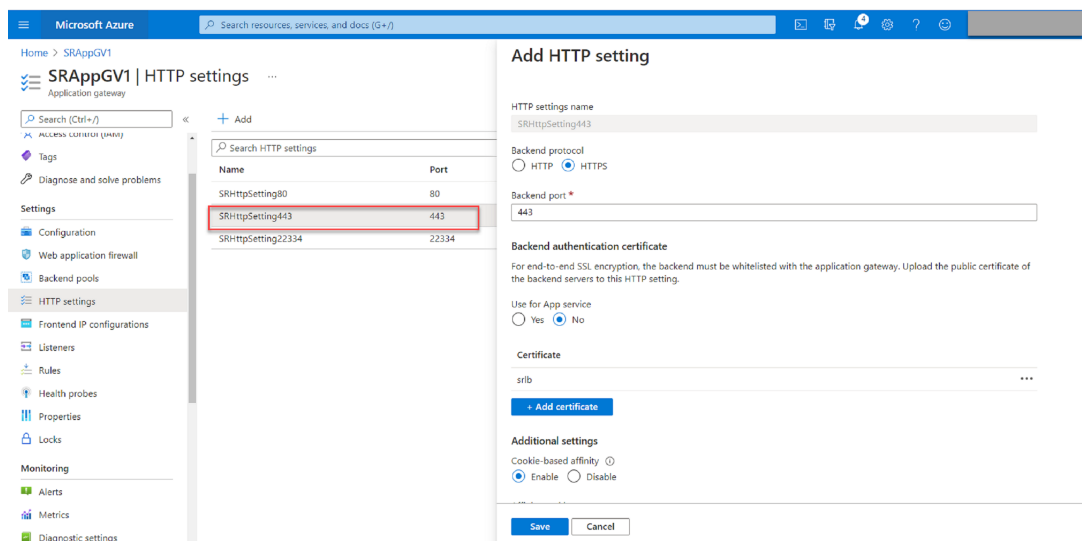
Azure Application Gateway prend en charge HTTP et HTTPS pour le routage des demandes vers les serveurs principaux. Créez des paramètres HTTP pour les ports 80, 443 et 22334.

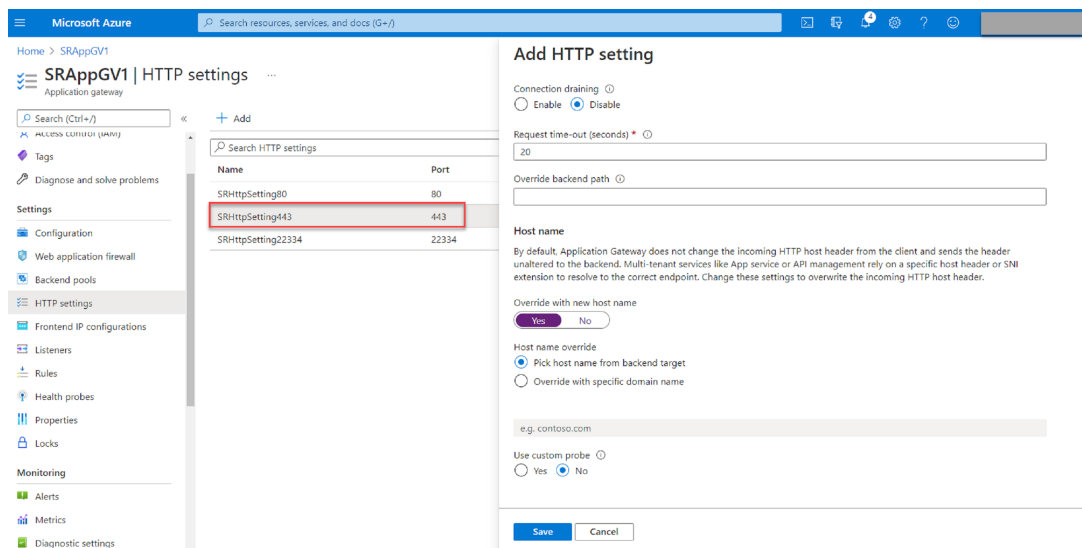
- HTTP sur le port 80



- HTTP sur le port 443

Un certificat d'authentification est requis pour autoriser les serveurs principaux à accéder à Application Gateway V1. Le certificat d'authentification est la clé publique des certificats de serveur principal au format X.509 (.CER) codé en base 64. Pour plus d'informations sur l'exportation de la clé publique à partir de votre certificat TLS/SSL, consultez [Exporter le certificat d'authentification \(pour le SKU v1\)](#).



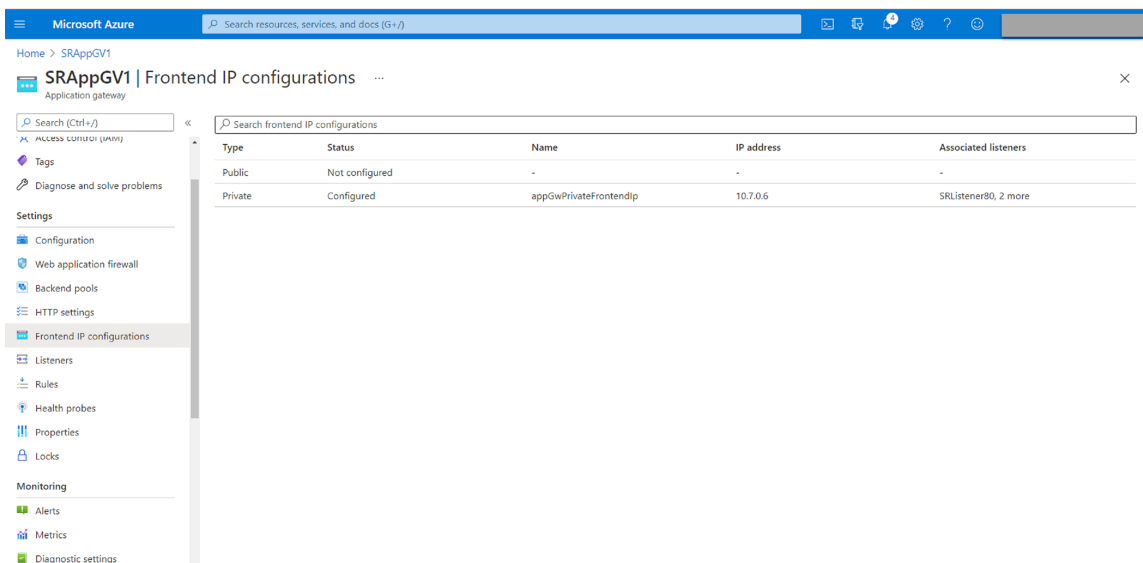


- HTTP ou HTTPS sur le port 22334

Si WebSocket utilise HTTP, utilisez le même paramètre que le port 80.

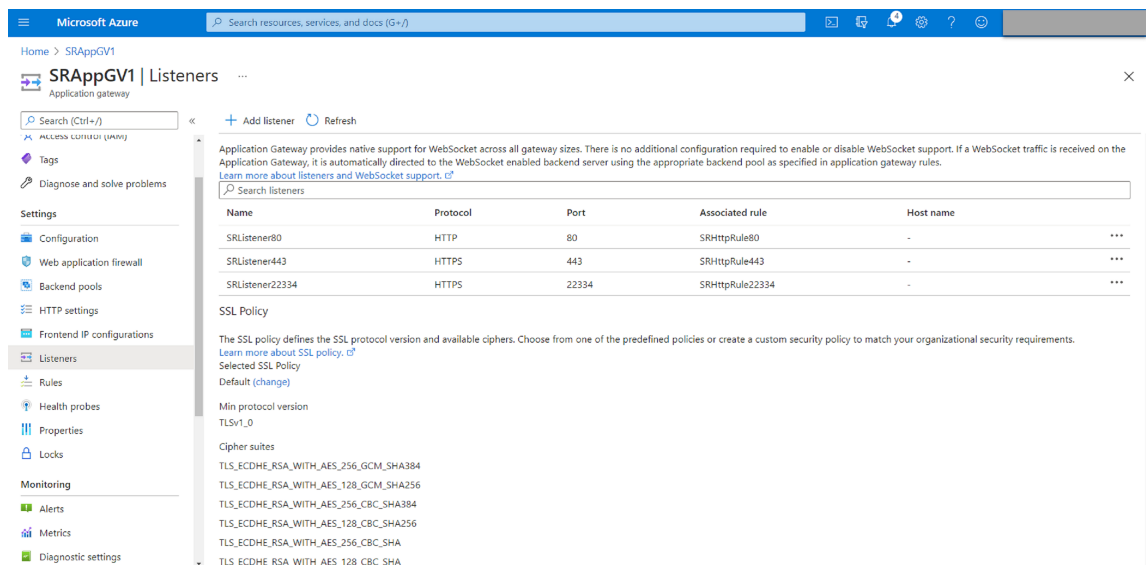
Si WebSocket utilise HTTPS, utilisez le même paramètre que le port 443.

4. Ajoutez une adresse IP frontale.

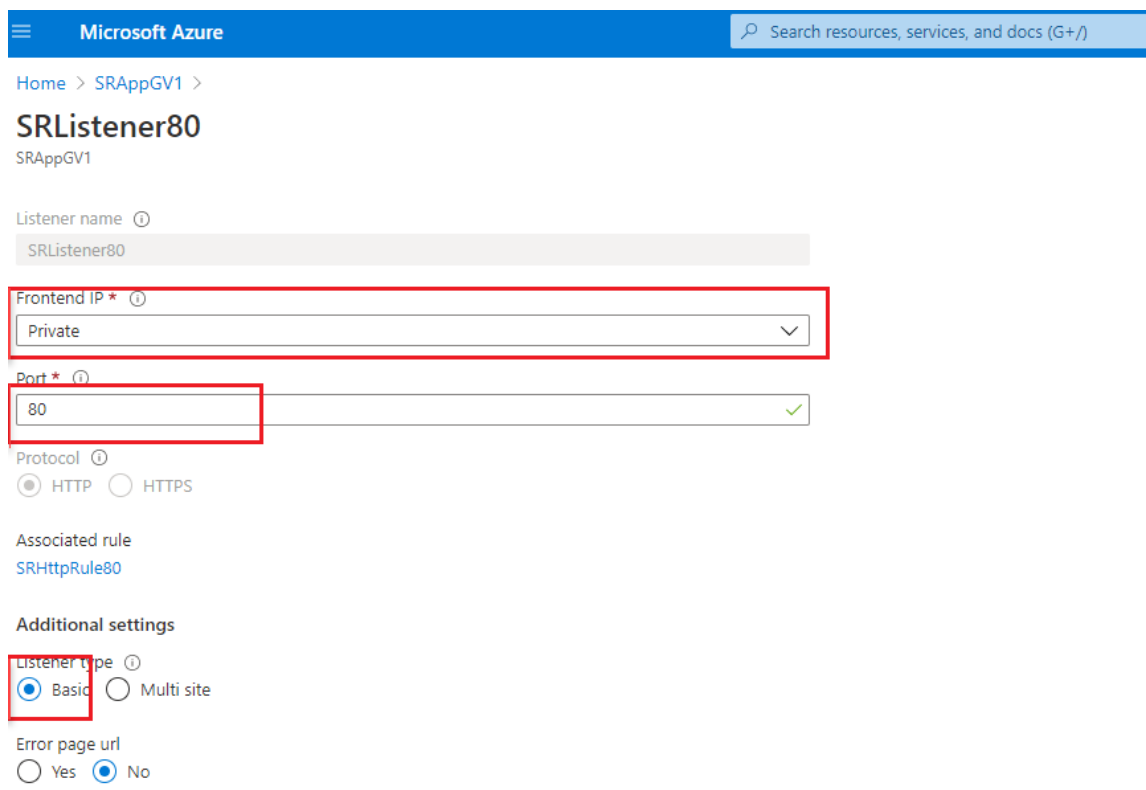


5. Ajoutez des écouteurs.

Ajoutez des écouteurs sur les ports 80, 443 et 22334, par exemple :



- Écouteur sur le port 80



- Écouteur sur le port 443

Créez un certificat auto-signé et téléchargez le certificat dans le [portail Azure](#) lorsque vous créez l'écouteur HTTPS. Pour de plus amples informations, consultez la section [Certificats pris en charge pour un arrêt TLS](#) et [Créer un certificat auto-signé](#).

[Home](#) > [SRAppGV1](#) >

SRListener443

SRAppGV1

Listener name ⓘ

SRListener443

Frontend IP * ⓘ

Private

Port * ⓘ

443

Protocol ⓘ

HTTP HTTPS

Choose a certificate

Create new Select existing

Certificate *

lbdc

Renew or edit selected certificate

Associated rule

[SRHttpRule443](#)

Additional settings

Listener type ⓘ

Basic Multi site

Error page url

Yes No

- Écouteur sur le port 22334

Si WebSocket utilise HTTP, utilisez le même paramètre que le port 80. Si WebSocket utilise HTTPS, utilisez le même paramètre que le port 443. L'exemple suivant montre le paramètre d'un écouteur HTTPS sur le port 22334.

Microsoft Azure

Home > SRAppGV1 >

SRListener22334

SRAppGV1

Listener name ⓘ
SRListener22334

Frontend IP * ⓘ
Private

Port * ⓘ
22334

Protocol ⓘ
 HTTP HTTPS

Choose a certificate
 Create new Select existing

Certificate *
lbdc

Renew or edit selected certificate

Associated rule
[SRHttpRule22334](#)

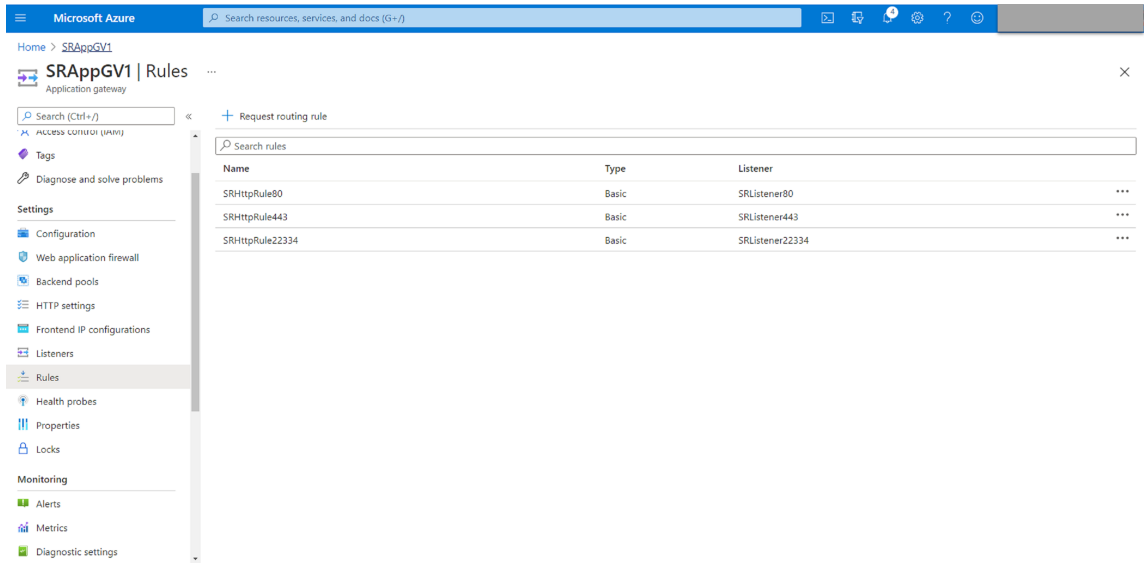
Additional settings

Listener type ⓘ
 Basic Multi site

Error page url
 Yes No

6. Créez des règles de routage des demandes.

Créez des règles pour les ports 80, 443 et 22334, par exemple :



- Règle de routage pour le port 80

SRHttpRule80

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name: SRHttpRule80

*** Listener** * Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener *: SRListener80

SRHttpRule80

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name: SRHttpRule80

* Listener * *** Backend targets**

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type: Backend pool Redirection

Backend target *: AGbackendpool

HTTP settings *: SRHttpSetting80

- Règle de routage pour le port 443

SRHttpRule443

SRApplGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

*** Listener** *** Backend targets**

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener *

SRHttpRule443

SRApplGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

*** Listener** *** Backend targets**

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type Backend pool Redirection

Backend target *

HTTP settings *

- Règle de routage pour le port 22334

SRHttpRule22334

SRApplGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

*** Listener** *** Backend targets**

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener *

SRHttpRule22334

SRApGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

* Listener * Backend targets

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type Backend pool Redirection

Backend target * ⓘ

HTTP settings * ⓘ

7. Ajoutez les machines virtuelles Azure sur lesquelles le serveur d'enregistrement de session est installé au pool principal.
8. Configurez les serveurs d'enregistrement de session conformément à l'article du Centre de connaissances [CTX230015](#).

Dépanner

December 21, 2022

Les informations de dépannage contenues dans ce chapitre contiennent des solutions à certains problèmes éventuels que vous pourriez rencontrer pendant ou après l'installation des composants de l'enregistrement de session.

Avertissement :

Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Échec de l'installation des composants du serveur

December 21, 2022

L'installation des composants du serveur d'enregistrement de session échoue avec les codes d'erreur 2503 et 2502.

Résolution : vérifiez la liste de contrôle d'accès (ACL) du dossier C:\windows\Temp pour vous assurer que Utilisateurs et groupes locaux ont un accès en écriture à ce dossier. Si ce n'est pas le cas, ajoutez manuellement les autorisations en écriture.

Le test de la connexion à la base de données échoue lors de l'installation

December 21, 2022

Lorsque vous installez la base de données d'enregistrement de session ou le serveur d'enregistrement de session, le test de la connexion échoue avec le message d'erreur **Échec du test de la connexion à la base de données. Corrigez le nom de l'instance de base de données**, et ce, même si le nom de l'instance de base de données est correct.

Dans ce cas, assurez-vous que l'utilisateur actuel dispose de l'autorisation de rôle SQL Server public pour éviter l'échec pour cause d'autorisation insuffisante.

L'agent ne peut pas se connecter au serveur

February 20, 2024

Lorsque l'agent d'enregistrement de session ne peut pas se connecter au serveur d'enregistrement de session, le message d'événement **Détection d'exception pendant l'envoi du message d'interrogation au broker d'enregistrement de session** est journalisé, suivi du texte d'exception. Le texte d'exception donne les raisons de l'échec de la connexion. Ces raisons sont les suivantes :

- **La connexion sous-jacente a été fermée. Impossible d'établir une relation de confiance pour le canal sécurisé TLS.** Cette exception signifie que le serveur d'enregistrement de session utilise un certificat signé par une autorité de certification (CA) que le serveur hébergeant l'agent d'enregistrement de session n'a pas approuvé ou que le serveur hébergeant l'agent d'enregistrement de session n'a pas de certificat d'autorité de certification. Le certificat peut aussi avoir expiré ou peut avoir été révoqué.

Solution : installez un certificat d'autorité de certification correct sur le serveur hébergeant l'agent d'enregistrement de session. Utilisez une autorité de certification de confiance.

- **Le serveur distant a renvoyé une erreur :** (403) interdit. Cette erreur HTTPS standard se produit lorsque vous tentez de vous connecter à l'aide de HTTP, qui est un protocole non sécurisé.

La machine hébergeant le serveur d'enregistrement de session rejette la connexion car elle n'accepte que les connexions sécurisées.

Solution : utilisez les **propriétés de l'agent d'enregistrement de session** pour modifier le protocole de l'agent d'enregistrement de session vers **HTTPS**.

- **Le broker d'enregistrement de session a renvoyé une erreur inconnue lors de l'évaluation d'une requête de stratégie d'enregistrements. Code d'erreur 5 (accès refusé). Veuillez consulter le journal des événements sur le serveur d'enregistrement de session pour plus de détails.** Cette erreur se produit lorsque les sessions démarrent et qu'une requête pour une évaluation de stratégie d'enregistrement est faite. L'erreur est le résultat de la suppression du groupe Utilisateurs authentifiés (membre par défaut) du rôle Requête de stratégie de la console d'autorisation d'enregistrement de session.

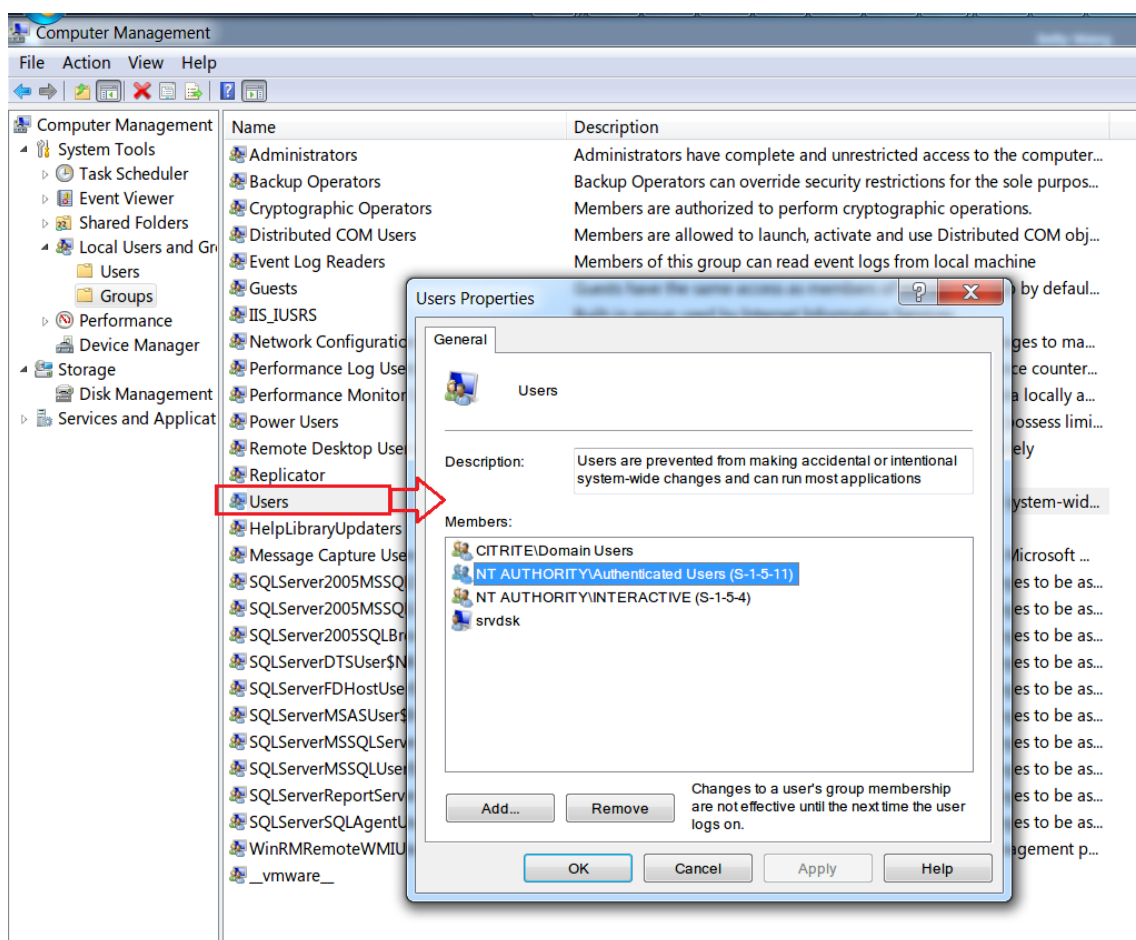
Solution : ajoutez à nouveau le groupe Utilisateurs authentifiés à ce rôle ou ajoutez chaque serveur hébergeant chaque agent d'enregistrement de session au rôle PolicyQuery.

- **La connexion sous-jacente a été fermée. Une connexion qui devait être maintenue active a été fermée par le serveur.** Cette erreur signifie que le serveur d'enregistrement de session est en panne, ou qu'il est indisponible pour accepter les requêtes. IIS est peut-être déconnecté ou a redémarré, ou le serveur entier peut être déconnecté.

Solution : vérifiez que le serveur d'enregistrement de session est démarré et connecté au réseau. Assurez-vous que le service IIS est en cours d'exécution sur le serveur.

- **Le serveur distant a renvoyé une erreur : 401 (non autorisé).** Cette erreur se traduit des manières suivantes :
 - Au démarrage du service Agent d'enregistrement de session, une erreur décrivant l'erreur 401 est enregistrée dans le journal des événements.
 - La requête de stratégie échoue sur l'Agent d'enregistrement de session.
 - Les enregistrements de session ne sont pas capturés sur l'Agent d'enregistrement de session.

Solution : assurez-vous que le groupe **NT AUTHORITY\Authenticated Users** est membre du groupe **Users** local sur l'Agent d'enregistrement de session.



Le serveur ne peut pas se connecter à la base de données

December 21, 2022

Lorsque le serveur d'enregistrement de session ne peut pas se connecter à la base de données d'enregistrement de session, il est possible qu'un message similaire aux suivants s'affiche :

Source de l'événement :

Une erreur liée au réseau ou à une instance spécifique s'est produite lors de l'établissement d'une connexion à SQL Server. Ce message s'affiche dans le journal d'événements d'applications avec l'ID 2047. Vous pouvez trouver le journal des événements dans l'Observateur d'événements sur le serveur d'enregistrement de session.

Description Gestionnaire de stockage d'enregistrement de session Citrix : Détection d'exception pendant l'établissement de connexion à la base de données. Cette erreur s'affiche dans le journal des événements d'applications de l'observateur d'événements du serveur d'enregistrement

de session.

Impossible de se connecter au serveur d'enregistrement de session. Assurez-vous que le serveur d'enregistrement de session fonctionne. Ce message d'erreur apparaît lorsque vous lancez la console de stratégie d'enregistrement de session.

Résolution :

- Vous avez installé Microsoft SQL Server sur un serveur autonome et n'avez pas réussi à configurer les services ou les paramètres appropriés pour l'enregistrement de session. Sur le serveur, le protocole TCP/IP doit être activé et le service SQL Server doit fonctionner. Veuillez consulter la documentation Microsoft pour des informations sur l'activation de ces paramètres.
- Lors de l'installation de l'enregistrement de session (option Administration), des informations incorrectes ont été fournies pour le serveur et la base de données. Désinstallez la base de données d'enregistrement de session et réinstallez-la, en fournissant les informations correctes.
- Le serveur de la base de données d'enregistrement de session est en panne. Vérifiez que le serveur est connecté.
- La machine hébergeant le serveur d'enregistrement de session ou celle hébergeant le serveur de la base de données d'enregistrement de session ne peut pas résoudre le nom de domaine complet ou le nom NetBIOS de l'autre. Utilisez la commande ping pour vérifier que les noms peuvent être résolus.
- Vérifiez la configuration du pare-feu sur la base de données d'enregistrement de session pour vous assurer que les connexions du serveur SQL Server sont autorisées. Pour plus d'informations, veuillez consulter l'article Microsoft sur <https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?redirectedfrom=MSDN&view=sql-server-ver15>.

La connexion a échoué pour l'utilisateur 'NT_AUTHORITY\ANONYMOUS LOGON'. Ce message d'erreur signifie que les services sont journalisés incorrectement en tant que .\administrator.

Résolution : redémarrez les services en tant qu'utilisateur système local et redémarrez les services SQL.

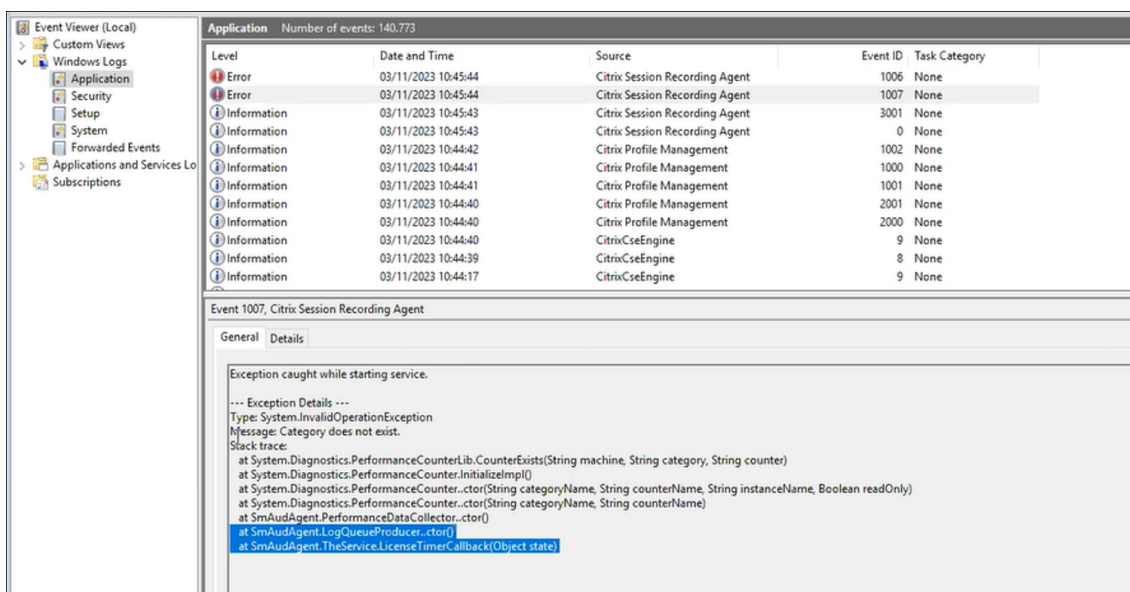
Échec de l'enregistrement des sessions

February 20, 2024

Si l'enregistrement de vos sessions échoue, vérifiez le journal d'événements d'application dans l'observateur d'événements de l'agent d'enregistrement de session et du serveur d'enregistrement de session. Cela peut vous fournir des informations de diagnostic importantes.

Si les sessions ne sont pas enregistrées, les causes possibles sont les suivantes :

- **Connectivité des composants et certificats.** Si les composants d'enregistrement de session ne peuvent pas communiquer entre eux, l'enregistrement de la session peut échouer. Pour résoudre les problèmes d'enregistrement, vérifiez que tous les composants sont configurés correctement de manière à pointer vers les machines correctes et que tous les certificats sont valides et installés correctement.
- **Environnements de domaine non Active Directory.** L'enregistrement de session est conçu pour être exécuté dans un environnement de domaine Microsoft Active Directory. Si vous n'évoluez pas dans un environnement Active Directory, vous pouvez avoir des difficultés d'enregistrement. Veillez à ce que tous les composants d'enregistrement de session sont exécutés sur des machines membres d'un domaine Active Directory.
- **Le partage de session entre en conflit avec la stratégie active.** L'enregistrement de session fait correspondre la stratégie active à la première application publiée qu'un utilisateur ouvre. Toute application suivante ouverte au cours de la même session continue d'observer la stratégie en vigueur pour la première application. Pour empêcher le partage de session d'entrer en conflit avec la stratégie active, publiez les applications en conflit sur des VDA avec OS multi-session distincts.
- **L'enregistrement n'est pas activé.** Par défaut, l'installation de l'agent d'enregistrement de session sur un VDA pour OS multi-session permet d'activer la fonction d'enregistrement sur le VDA. L'enregistrement n'aura pas lieu tant qu'une stratégie d'enregistrement active n'a pas été configurée pour le permettre.
- **La stratégie d'enregistrement active n'autorise pas l'enregistrement.** Une session peut être enregistrée uniquement lorsqu'elle répond aux règles de la stratégie d'enregistrement active.
- **Les services d'enregistrement de session ne sont pas exécutés.** Pour que les sessions soient enregistrées, le service de l'agent d'enregistrement de session doit être exécuté sur un VDA avec OS multi-session et le service Gestionnaire de stockage d'enregistrement de session doit s'exécuter sur la machine hébergeant le serveur d'enregistrement de session.
- **MSMQ n'est pas configuré.** Si MSMQ n'est pas configuré correctement sur le serveur exécutant l'agent d'enregistrement de session et sur la machine hébergeant le serveur d'enregistrement de session, des problèmes d'enregistrement peuvent se produire.
- **Les compteurs de performance Windows sont manquants, désactivés ou endommagés pour l'agent d'enregistrement de session.** Les erreurs suivantes peuvent s'afficher dans le journal d'application de l'agent d'enregistrement de session :



Pour résoudre le problème, reconstruisez tous les compteurs de performance en procédant comme suit :

1. Ouvrez l'invite de commande (CMD) en tant qu'administrateur.
2. Accédez à Windows\System32 en tapant `cd c:\windows\system32\`.
3. Tapez `lodctr /R`, puis appuyez sur **Entrée**. La commande `lodctr /R` reconstruit les compteurs de performance.
4. Une fois la commande `lodctr /R` exécutée, certains compteurs reconstruits peuvent être désactivés. Pour vérifier l'état du compteur, exécutez la commande `lodctr /Q`. Si vous constatez qu'un compteur est désactivé, vous pouvez l'activer en exécutant la commande `lodctr /E: [counter name]`.

Impossible d'afficher la lecture de session active

December 21, 2022

Si vous rencontrez des difficultés lors de l'affichage d'enregistrements avec le lecteur d'enregistrement de session, le message d'erreur suivant peut s'afficher :

Échec du téléchargement du fichier de la session enregistrée. La lecture de session active n'est pas autorisée. Le serveur est configuré de manière à interdire cette fonctionnalité. Cette erreur indique que le serveur est configuré pour interdire l'action.

Résolution : dans **Propriétés du serveur d'enregistrement de session**, choisissez l'onglet **Lecture** et cochez la case **Autoriser la lecture d'une session active**.

Les enregistrements sont endommagés ou incomplets

December 21, 2022

- Lorsque vous affichez des enregistrements endommagés ou incomplets dans le lecteur, des avertissements peuvent également s'afficher dans les journaux d'événements de l'agent d'enregistrement de session.

Source de l'événement : Gestionnaire de stockage d'enregistrement de session Citrix

Description : perte de données lors de l'enregistrement du fichier **<nom du fichier icl>**

Le problème se produit généralement lorsque MCS ou PVS est utilisé pour créer les VDA avec une image principale configurée et que Microsoft Message Queuing (MSMQ) est installé. Dans ce cas, les VDA ont les mêmes **QMID** pour MSMQ.

Pour résoudre ce problème, créez un **QMID** unique pour chaque VDA. Pour de plus amples informations, consultez la section [Installer, mettre à niveau et désinstaller](#).

- Le lecteur d'enregistrement de session peut signaler une erreur interne avec ce message : **«Le fichier lu indique qu'une erreur système interne (code d'erreur : 9) s'est produite pendant l'enregistrement d'origine. Le fichier peut toujours être lu jusqu'au niveau où l'erreur d'enregistrement s'est produite.»** lors de la lecture d'un nouveau fichier d'enregistrement.

Le problème se produit en raison de la taille insuffisante du tampon sur l'agent d'enregistrement de session lorsque des sessions graphiques intensives sont enregistrées.

Pour contourner le problème, modifiez les données de la valeur **HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMB** et définissez-les sur un niveau plus élevé dans l'agent d'enregistrement de session, puis redémarrez la machine.

Vérifier les connexions des composants

December 21, 2022

Pendant l'installation de l'enregistrement de session, il se peut que les composants ne se connectent pas à d'autres. Tous les composants communiquent avec le serveur d'enregistrement de session (broker). Par défaut, le broker (un composant IIS) est sécurisé à l'aide du certificat du site Web IIS par défaut. Si un composant ne peut pas se connecter au serveur d'enregistrement de session, il est possible que les tentatives de connexion des autres composants échouent également.

L'agent d'enregistrement de session et le serveur d'enregistrement de session (gestionnaire de stockage et broker) journalisent les erreurs de connexion dans le journal des événements des applications.

Vous pouvez afficher le journal dans l'Observateur d'événements de la machine hébergeant le serveur d'enregistrement de session. La console de stratégie d'enregistrement de session et le lecteur d'enregistrement de session affichent des messages d'erreur de connexion à l'écran lorsque les connexions échouent.

Vérifier que l'agent d'enregistrement de session est connecté

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. À partir du menu **Démarrer**, choisissez **Propriétés de l'Agent d'enregistrement de session**.
3. Dans la boîte de dialogue **Propriétés de l'agent d'enregistrement de session**, cliquez sur l'onglet **Connexions**.
4. Vérifiez que le nom de domaine complet correct est entré dans le champ **Serveur d'enregistrement de session**.
5. Vérifiez que le serveur choisi pour la valeur Serveur d'enregistrement de session peut être contacté par votre VDA pour OS multi-session.

Pour plus d'informations, voir [L'agent ne peut pas se connecter au serveur](#).

Remarque :

Recherchez des erreurs et des avertissements dans le journal des événements de l'application.

Vérifier que le serveur d'enregistrement de session est connecté

Attention :

L'utilisation de l'Éditeur du Registre peut entraîner de sérieux problèmes et nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques.

1. Ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session.
2. Ouvrez l'Éditeur de Registre.
3. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.
4. Vérifiez que la valeur **SmAudDatabaseInstance** réfère correctement à la base de données d'enregistrement de session que vous avez installée sur votre instance SQL Server.

Pour plus d'informations, voir [Le serveur ne peut pas se connecter à la base de données](#).

Vérifier que la base de données d'enregistrement de session est connectée

1. À l'aide d'un outil de gestion SQL, ouvrez votre instance SQL contenant la base de données d'enregistrement de session que vous avez installée.

2. Ouvrez les autorisations de sécurité de la base de données d'enregistrement de session.
3. Vérifiez que le compte d'ordinateur d'enregistrement de session a accès à la base de données. Par exemple, si la machine hébergeant le serveur d'enregistrement de session a pour nom **Ss-RecSrv** dans le domaine MIS, le compte d'ordinateur de votre base de données doit être configuré ainsi : **MIS\SsRecSrv\$**. Cette valeur est configurée au cours de l'installation de la base de données d'enregistrement de session.

Tester la connectivité IIS

Vous pouvez tester les connexions au site IIS du serveur d'enregistrement de session avec un navigateur Web pour accéder à la page Web du broker d'enregistrement de session. Il peut vous aider à déterminer si les problèmes de communication éventuels entre les composants de l'enregistrement de session proviennent d'une mauvaise configuration de protocole, de problèmes de certification ou de problèmes au niveau du broker d'enregistrement de session.

Pour vérifier la connectivité IIS avec l'agent d'enregistrement de session :

1. Ouvrez une session sur le serveur sur lequel l'agent d'enregistrement de session est installé.
2. Lancez un navigateur Web et entrez l'adresse suivante :
 - Pour HTTPS : <https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl>, où `servername` correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
 - Pour HTTP : <http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl>, où `servername` correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à vous authentifier par NT LAN Manager (NTLM), connectez-vous avec un compte d'administrateur de domaine.

Pour vérifier la connectivité IIS avec le lecteur d'enregistrement de session :

1. Ouvrez une session sur le poste de travail sur lequel le lecteur d'enregistrement de session est installé.
2. Lancez un navigateur Web et entrez l'adresse suivante :
 - Pour HTTPS : <https://servername/SessionRecordingBroker/Player.rem?wsdl>, où `servername` correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
 - Pour HTTP : <http://servername/SessionRecordingBroker/Player.rem?wsdl>, où `servername` correspond au nom de la machine hébergeant le serveur d'enregistrement de session.

3. Si vous êtes invité à vous authentifier par NT LAN Manager (NTLM), connectez-vous avec un compte d'administrateur de domaine.

Pour vérifier la connectivité IIS avec la console de stratégie d'enregistrement de session :

1. Ouvrez une session sur le serveur sur lequel la console de stratégie d'enregistrement de session est installée.
2. Lancez un navigateur Web et entrez l'adresse suivante :
 - Pour HTTPS: `https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, où `servername` correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
 - Pour HTTP: `http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, où `servername` correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
3. Si vous êtes invité à vous authentifier par NT LAN Manager (NTLM), connectez-vous avec un compte d'administrateur de domaine.

Si votre navigateur affiche un document au format XML, cela permet de vérifier que la console de stratégie d'enregistrement de session est connectée au serveur d'enregistrement de session à l'aide du protocole configuré.

Dépanner les problèmes de certificat

Si le protocole de communication que vous utilisez est HTTPS, la machine hébergeant le serveur d'enregistrement de session doit être configurée avec un certificat de serveur. Toutes les connexions de composant au serveur d'enregistrement de session doivent posséder un certificat racine d'autorité de certification (CA). Sans cela, les tentatives de connexion entre les différents composants échoueront.

Vous pouvez tester vos certificats en accédant à la page Web du broker d'enregistrement de session, de la même manière que vous le feriez pour tester la connectivité IIS. Si vous pouvez accéder à la page XML de chaque composant, cela signifie que les certificats sont configurés correctement.

Voici quelques situations courantes pour lesquelles les émissions de certificats perturbent les connexions :

- **Certificats non valides ou manquants.** Si le serveur exécutant l'agent d'enregistrement de session n'a pas de certificat racine pouvant faire confiance au certificat de serveur, et qu'il ne peut pas faire confiance et se connecter au serveur d'enregistrement de session sur le protocole HTTPS, la connexion échoue. Vérifiez que tous les composants font confiance au certificat du serveur d'enregistrement de session.

- **Nom incohérent.** Si le certificat de serveur attribué à la machine hébergeant le serveur d'enregistrement de session est créé avec un nom de domaine complet (FQDN), tous les composants se connectant doivent utiliser le nom de domaine complet lors de la connexion au serveur d'enregistrement de session. Si un nom NetBIOS est utilisé, configurez les composants avec un nom NetBIOS pour le serveur d'enregistrement de session.
- **Certificats expirés.** Si un certificat de serveur est expiré, la connectivité au serveur d'enregistrement de session via le protocole HTTPS échoue. Veuillez vérifier que le certificat de serveur attribué à la machine hébergeant le serveur d'enregistrement de session est valide et qu'il n'est pas arrivé à expiration. Si le même certificat est utilisé pour la signature numérique des enregistrements de session, le journal des événements du serveur d'enregistrement de session produira des messages d'erreur indiquant que le certificat a expiré ou des messages d'avertissement lorsqu'il arrive à expiration.

Échec de la recherche d'enregistrements à l'aide du lecteur

December 21, 2022

Si vous rencontrez des difficultés lors de la recherche d'enregistrements avec le lecteur d'enregistrement de session, les messages d'erreur suivants peuvent s'afficher :

- **Échec de la recherche des fichiers de session enregistrée. Le nom de serveur distant n'a pas pu être résolu : nomserveur. nomserveur.** **nomserveur** est le nom du serveur auquel le lecteur d'enregistrement de session tente de se connecter. Le lecteur d'enregistrement de session ne peut pas contacter le serveur d'enregistrement de session. Il existe deux raisons possibles : un nom de serveur tapé incorrectement ou le DNS ne peut pas résoudre le nom du serveur.

Résolution : dans la barre de menu du lecteur, choisissez **Outils > Options > Connexions** et vérifiez que le nom du serveur dans la liste **Serveurs d'enregistrement de session** est correct. S'il est correct, exécutez la commande ping dans une invite de commande afin de vérifier s'il est possible de résoudre le nom. Lorsque le serveur d'enregistrement de session est en panne ou hors ligne, le message d'erreur d'échec de recherche des fichiers de session enregistrés est **Impossible de contacter le serveur distant**.

- **Impossible de contacter le serveur distant.** Cette erreur se produit lorsque le serveur d'enregistrement de session est en panne ou déconnecté.

Résolution : vérifiez que le serveur d'enregistrement de session est connecté.

- **Accès refusé.** Une erreur d'accès refusé se produit si l'utilisateur n'a pas obtenu d'autorisation de recherche et de téléchargement de fichiers de session enregistrée.

Résolution : attribuez le rôle Lecteur à l'utilisateur à l'aide de la console d'autorisation d'enregistrement de session.

- **Accès refusé lorsque le rôle Lecteur est attribué.** Cette erreur se produit lorsque vous installez le lecteur d'enregistrement de session sur la même machine que le serveur d'enregistrement de session, et que vous avez activé la fonction UAC. Lorsque vous attribuez au groupe d'utilisateurs Administrateurs du domaine ou Administrateurs le rôle Lecteur, un utilisateur administrateur non intégré dans ce groupe peut échouer à la vérification basée sur le rôle.

Résolutions :

- Exécuter le lecteur d'enregistrement de session en tant qu'administrateur.
 - Attribuer à des utilisateurs spécifiques le rôle Lecteur plutôt qu'à l'ensemble du groupe.
 - Installer le lecteur d'enregistrement de session sur une machine distincte de celle du serveur d'enregistrement de session.
- **Échec de la recherche des fichiers de session enregistrée. La connexion sous-jacente a été fermée. Impossible d'établir une relation de confiance pour le canal sécurisé TLS.** L'erreur se produit lorsque le serveur d'enregistrement de session utilise un certificat signé par une autorité de certification auquel la machine cliente ne fait pas confiance ou pour lequel elle n'a pas de certificat d'autorité de certification.

Résolution : installez le certificat CA correct ou de confiance sur la station de travail sur laquelle le lecteur d'enregistrement de session est installé.

- **Le serveur distant a renvoyé une erreur :** (403) interdit. Il s'agit d'une erreur HTTPS standard qui se produit lorsque vous tentez de vous connecter en utilisant HTTP (protocole non sécurisé). Le serveur rejette la connexion parce qu'il est configuré par défaut pour n'accepter que les connexions sécurisées.

Résolution : Dans la barre de menu du **lecteur d'enregistrement de session**, choisissez **Outils > Options > Connexions**. Sélectionnez le serveur dans la liste **Serveurs d'enregistrement de session**, puis cliquez sur **Modifier**. Changez le protocole de **HTTP** à **HTTPS**.

Résolution des problèmes MSMQ

Si un message de notification s'affiche mais que l'utilisateur ne peut pas trouver les enregistrements après avoir effectué une recherche dans le lecteur d'enregistrement de session, il y a un problème avec MSMQ. Vérifiez que la file d'attente est connectée au serveur d'enregistrement de session (Gestionnaire de stockage). Utilisez un navigateur Web pour tester les connexions afin d'identifier des erreurs de connexion éventuelles (si vous utilisez HTTP ou HTTPS pour votre protocole de communication MSMQ).

Pour vérifier que la file d'attente est connectée :

1. Ouvrez une session sur le serveur hébergeant l'agent d'enregistrement de session et affichez les files d'attente sortantes.
2. Vérifiez que la file d'attente de la machine hébergeant le serveur d'enregistrement de session indique un état connecté.
 - Si l'état indiqué est **En attente de connexion**, que la file d'attente contient des messages et que le protocole est HTTP ou HTTPS (selon le protocole sélectionné dans l'onglet **Connexions** de la boîte de dialogue **Propriétés de dialogue de l'agent d'enregistrement de session**), effectuez les opérations de l'étape 3.
 - Si l'état indique **connecté** et qu'aucun message ne se trouve dans la file d'attente, il peut y avoir un problème sur le serveur hébergeant le serveur d'enregistrement de session. Ignorez l'étape 3 et effectuez l'étape 4.
3. Si la file d'attente contient des messages, ouvrez un navigateur Web et entrez l'adresse suivante :
 - Pour HTTPS : [https://servername/msmq/private\\$/CitrixSmAudData](https://servername/msmq/private$/CitrixSmAudData), où **servername** correspond au nom de la machine hébergeant le serveur d'enregistrement de session.
 - Pour HTTP : [http://servername/msmq/private\\$/CitrixSmAudData](http://servername/msmq/private$/CitrixSmAudData), où **servername** correspond au nom de la machine hébergeant le serveur d'enregistrement de session.

Si la page renvoie une erreur telle que **Le serveur n'accepte que les connexions sécurisées**, changez le protocole MSMQ figurant dans la liste **Propriétés de l'agent d'enregistrement de session** pour HTTPS. Si la page fait état d'un problème avec le certificat de sécurité du site Web, il se peut qu'il y ait un problème avec une relation d'approbation pour le canal sécurisé TLS. Dans ce cas, installez le certificat CA correct, ou utilisez une CA de confiance.

4. Si la file d'attente ne contient pas de message, ouvrez une session sur la machine hébergeant le serveur d'enregistrement de session et affichez les files d'attente privées. Sélectionnez **citrixs-mauidata**. Si la file d'attente contient des messages (colonne Nombre de messages), vérifiez que le service StorageManager de l'enregistrement de session a démarré. S'il ne l'est pas, redémarrez le service.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).