StorageZones Controller 5.x

Machine translated content

Disclaimer

本内容的正式版本为英文版。部分 Citrix 文档内容采用了机器翻译，仅供您参考。Citrix 无法控制机器翻译的内容，这些内容可能包含错误、不准确或不合适的语言。对于从英文原文翻译成任何其他语言的内容的准确性、可靠性、适用性或正确性，或者您的 Citrix 产品或服务沿用了任何机器翻译的内容，我们均不作任何明示或暗示的保证，并且适用的最终用户许可协议或服务条款或者与 Citrix 签订的任何其他协议（产品或服务与已进行机器翻译的任何文档保持一致）下的任何保证均不适用。对于因使用机器翻译的内容而引起的任何损害或问题，Citrix 不承担任何责任。

Contents

关于 **StorageZones Controller**

October 13, 2020

StorageZones Controller 通过向 ShareFile 帐户提供私有数据存储（称为 ShareFile 数据的存储区域）来扩展 ShareFile 软件即服务 (SaaS) 云存储。

有关 StorageZones Controller（如组件、数据存储等）的详细信息，请参阅存储区域 Controller 5.x。

有 新增功能 关此和 Citrix Content Collaboration 中的最新增强功能，请参阅。

要下载最新版本，请参阅 https://www.citrix.com/downloads/sharefile/。登录到您的 Citrix 帐户以访问所有应用程序下载。

已修复的问题

存储区域 **Controller 5.10** 中修复的问题

此版本解决了多个有助于改进整体性能和稳定性的问题。

存储区域 **Controller 5.9** 中修复的问题

此版本包含提高可靠性和性能的修复程序。

存储区域 **Controller 5.8** 中修复的问题

此版本包含一个修复程序，以改进已签出文件的错误消息以及 SharePoint 中新发布的托管路径的修复程序。

存储区域 **Controller 5.7** 中修复的问题

此版本包含解决文件上传到存储区域和本地连接器的重定向问题的修复程序。

存储区域 **Controller 5.6** 中修复的问题

WOPI 修复：包括更改以解决尝试随后编辑 Office 文件时出现的问题。

SharePoint 连接器修复：此版本包括在创建 SharePoint 连接器上已存在的文件夹时显示有效错误消息的更改。

存储区域 **Controller 5.5** 中的修复问题

此版本包含提高可靠性和性能的修复程序。

存储区域 **Controller 5.4.2** 中修复的问题

SharePoint 连接器修复：移动存在于 SharePoint 连接器上的文件可能会失败的特定方案。此版本可确保 SharePoint 连接器上存在的移动文件按预期工作。

安全修补程序：此版本包含安全性和可靠性的修补程序。

存储区域 **Controller 5.4.1** 中修复的问题

安全修补程序：此版本包含安全性和可靠性的修补程序。

附加支持：为 Workspace 环境添加了对 云/ 云卷饼帐户的支持。

存储区域 **Controller 5.3.1** 中修复的问题

此版本包含提高可靠性和性能的修复程序。

存储区域 **Controller 5.3.1** 中修复的问题

WOPI 修复： WOPI 访问令牌可能被盗窃公共加密密钥欺骗。此版本确保了密钥不在 StorageZones Controller 之间共享。

安全修补程序：此版本包含安全性、性能和可靠性的修补程序。

已知问题

存储区域 **Controller 5.10** 中的已知问题

在此版本中没有发现新问题。

存储区域 **Controller 5.9** 中的已知问题

在此版本中没有发现新问题。

存储区域 **Controller 5.8** 中的已知问题

在此版本中没有发现新问题。

存储区域 **Controller 5.7** 中的已知问题

在此版本中没有发现新问题。

体系结构概述

June 15, 2020

本节概述了为概念验证评估或高可用性生产环境部署 StorageZones Controller 的情况。使用和不使用 DMZ 代理（如 Citrix ADC）进行高可用性部署。

要评估具有多个 StorageZones Controller 的部署，请遵循高可用性部署的准则。

每个部署方案都需要一个 ShareFile Enterprise 帐户。默认情况下，ShareFile 将数据存储在安全的 ShareFile 管理的云中。要使用专用数据存储（本地网络共享或受支持的第三方存储系统），请为 ShareFile Data 配置存储区域。

要从网络文件共享或 SharePoint 文档库安全地向用户传递数据，请配置存储区域连接器。

StorageZones Controller 概念验证部署

> 小心：
>
> 概念验证部署仅用于评估目的，不应用于关键数据存储。

概念验证部署使用单个 StorageZones Controller。本节中讨论的示例部署既启用了 ShareFile Data 的存储区域，也启用了存储区域连接器。

要评估单个 StorageZones Controller，您可以选择将数据存储在 StorageZones Controller 硬盘驱动器上的文件夹（如 C:\ZoneFiles）中，而不是单独的网络共享上。所有其他系统要求都适用于评估部署。

标准存储区域的概念验证部署

为标准区域配置的 StorageZones Controller 必须接受来自 ShareFile 云的绑定连接。为此，Controller 必须具有可公开访问的互联网地址和启用 SSL 以便与 ShareFile 云进行通信。下图显示了用户设备、ShareFile 云和 StorageZones Controller 之间的流量。

在这种情况下，一个防火墙站在 Internet 和安全网络之间。StorageZones Controller 驻留在防火墙内以控制访问。与 ShareFile 的用户连接必须遍历防火墙，并使用端口 443 上的 SSL 协议来建立此连接。若要支持此连接，您必须在防火墙上打开端口 443，并在 StorageZones Controller 的 IIS 服务上安装公有 SSL 证书。

StorageZones Controller 高可用性部署

对于具有高可用性的 ShareFile 生产部署，建议的最佳做法是至少安装两个 StorageZones Controller。安装第一个 Controller 时，将创建一个存储区域。安装其他控制器时，将它们加入到同一区域。属于同一区域的 StorageZones Controller 必须为存储使用相同的文件共享。

在高可用性部署中，辅助服务器是独立的、功能齐全的 StorageZones Controller。存储区域控制子系统随机选择一个 StorageZones Controller 进行操作。如果主服务器脱机，您可以轻松地将从属服务器升级为主服务器。您还可以将服务器从主服务器降级为辅助服务器。

标准区域的高可用性部署

为标准存储区域配置的 StorageZones Controller 必须接受来自 ShareFile 云的绑定连接。为此，每个 Controller 必须具有可公开访问的互联网地址和启用 SSL，以便与 ShareFile 云进行通信。您可以配置多个外部公有地址，每个地址都与不同的存储区域控制器关联。下图显示了标准存储区域的高可用性部署。

与上述概念验证部署方案类似，一个防火墙位于 Internet 和安全网络之间。StorageZones Controller 驻留在防火墙内以控制访问。与 ShareFile 的用户连接必须遍历防火墙，并使用端口 443 上的 SSL 协议来建立此连接。要支持此连接，必须在防火墙上打开端口 443，并在所有 StorageZones Controller 的 IIS 服务上安装公有 SSL 证书。

共享存储配置

属于同一存储区域的 StorageZones Controller 必须为存储使用相同的文件共享。StorageZones Controller 使用 IIS 帐户池用户访问共享。默认情况下，应用程序池在具有低级别用户权限的网络服务用户帐户下运行。默认情况下，StorageZones Controller 使用网络服务帐户。

您可以使用指定用户帐户而不是网络服务帐户来访问共享。要使用指定用户帐户，请在存储区域控制台“配置”页中指定用户名和密码。使用网络服务帐户运行 IIS 应用程序池和 Citrix ShareFile 服务。

网络连接

网络连接因区域类型而异 — Citrix 管理或标准。

Citrix 管理的区域

下表介绍了当用户登录到 ShareFile，然后从 Citrix 管理的区域下载文档时发生的网络连接。所有连接都使用 HTTPS。

步骤	源	目标
1. 用户登录请求	客户端	company.sharefile.com:443
2. （可选）重定向至“SAML IdP 登录”诊所诊所	客户端	SAML 身份提供商 URL
3. 文件/文件夹枚举和下载请求	客户端	company.sharefile.com:443
4. 文件下载	客户端	storage-location.sharefile.com:443

标准存储区域

下表介绍了当用户登录到 ShareFile，然后从标准存储区域下载文档时发生的网络连接。所有连接都使用 HTTPS。

步骤	源	目标
1. 用户登录请求	客户端	company.sharefile.com
2. （可选）如果使用 ADFS，请重定向至 SAML IdP 登录	客户端	SAML 身份提供商 URL
3. 文件/文件夹枚举和下载请求	客户端	company.sharefile.com
4. 文件下载授权	company.sharefile.com	szc.company.com
5. 文件下载	客户端	szc.company.com

StorageZones Controller DMZ 代理部署

非军事区域 (DMZ) 为内部网络提供了额外的安全层。DMZ 代理（如 Citrix ADC VPX）是一个可选组件，用于：

- 确保对 StorageZones Controller 的所有请求都源自 ShareFile 云，以便只有批准的流量到达 StorageZones Controller.

  StorageZones Controller 具有验证操作，用于检查所有传入消息的有效 URI 签名。DMZ 组件负责在转发邮件之前验证签名。

- 使用实时状态指示器向 StorageZones Controller 发出负载平衡请求。

  如果操作都可以访问相同的文件，则可以对 StorageZones Controller 进行负载平衡。

- 从 StorageZones Controller 卸载 SSL。
- 确保在通过 DMZ 之前对 SharePoint 或网络驱动器上的文件请求进行身份验证。

Citrix ADC 和 StorageZones Controller 部署

标准存储区域的部署

为标准区域配置的 StorageZones Controller 必须接受来自 ShareFile 云的绑定连接。为此，Citrix ADC 必须具有可公开访问的互联网地址和启用 SSL 以便与 ShareFile 云进行通信。

在这种情况下，两个防火墙站在互联网和安全网络之间。StorageZones Controller 驻留在内部网络中。与 ShareFile 的用户连接必须遍历第一个防火墙，并使用端口 443 上的 SSL 协议来建立此连接。要支持此连接，您必须在防火墙上打开端口 443，并在 DMZ 代理服务器的 IIS 服务上安装公共 SSL 证书（如果它们终止用户连接）。

标准区域的网络连接

下图和表格描述了当用户登录到 ShareFile，然后从部署在 Citrix ADC 后面的标准区域下载文档时发生的网络连接。在这种情况下，帐户使用 Active Directory 联合身份验证服务 (ADFS) 进行 SAML 登录。

在 DMZ 中，身份验证通信由 ADFS 代理服务器处理，该服务器与受信任网络上的 ADFS 服务器通信。文件活动是通过 DMZ 中的 Citrix ADC 访问的，该 ADC 将终止 SSL，对用户请求进行身份验证，然后代表身份验证的用户访问受信任网络中的 StorageZones Controller。ShareFile 的 Citrix ADC 外部地址可以使用互联网 FQDN 公司网站访问。

步骤	源	目标	协议
1. 用户登录请求	客户端	company.sharefile.com	HTTPS
2. （可选）重定向至“SAML IdP 登录”诊所诊所	客户端	SAML 身份提供商 URL	HTTPS
2a. ADFS 登录	ADFS 代理	ADFS 服务器	HTTPS
3. 文件/文件夹枚举和下载请求	客户端	company.sharefile.com	HTTPS
4. 文件下载授权	ShareFile	szc.company.com（外部地址）	HTTP (S)
4a. 文件下载授权	Citrix ADC IP（NSIP）	StorageZones Controller	HTTPS
5. 文件下载	客户端	szc.company.com（外部地址）	HTTPS
5a. 文件下载	Citrix ADC IP（NSIP）	StorageZones Controller	HTTP (S)

下图和表格扩展了上一方案，以显示 StorageZone 连接器的网络连接。此方案包括在 DMZ 中使用 NetScaler 终止 SSL 并对连接器访问执行用户身份验证。

步骤	源	目标	协议
1. 用户登录请求	客户端	company.sharefile.com	HTTPS
2. （可选）重定向至“SAML IdP 登录”诊所诊所	客户端	SAML 身份提供商 URL	HTTPS
2a. ADFS 登录	ADFS 代理	ADFS 服务器	HTTPS
3. 顶级连接器枚举	客户端	company.sharefile.com	HTTPS

步骤	源	目标	协议
4. 用户登录到 StorageZones Controller 服务器	客户端	`szc.company.com`（外部地址）	HTTPS
5. 用户身份验证	Citrix ADC IP（NSIP）	AD 域 Controller	地方政务处理
6. 文件/文件夹枚举和上载/下载请求	Citrix ADC IP（NSIP）	StorageZones Controller	HTTP (S)
7. 网络共享枚举和上载/下载	存储区域控制器	文件服务器	CIFS 或 DFS
7a. SharePoint 枚举和上载/下载	存储区域控制器	SharePoint	HTTP (S)

下图总结了基于用户是否进行身份验证的受支持的身份验证类型组合。

系统要求

June 15, 2020

存储区域控制器

- 具有 2 个 CPU 和 4 GB 内存的专用物理机或虚拟机
- Windows 服务器 2012 R2（数据中心、标准或基础）
- Windows Server 2016

对于标准存储区域：

- 使用可公开解析的互联网主机名（不是 IP 地址）。
- 为与 ShareFile 的通信启用 SSL。
  - StorageZones Controller 上的 SSL 证书必须受到用户设备和 ShareFile Web 服务器的信任。如果直接将 SSL 与 IIS 结合使用，请参阅 http://support.microsoft.com/kb/298805 以了解有关配置 SSL 的信息。
- 允许通过防火墙在端口 443 上的入站 TCP 请求。
- 允许通过防火墙到端口 443 上的 ShareFile 控制平面的出站 TCP 请求。
  - 单击此处查看 IP 范围和域的详细列表。

对于仅用于 **ShareFile** 数据的存储区域的服务器运行状况检查：

- 打开本地主机上的端口 80。

对于高可用性生产环境：

- 至少安装了两个 StorageZones Controller 的服务器。
- 如果不使用 DMZ 代理服务器，请在 IIS 服务上安装 SSL 证书。

  有关支持的证书的信息，请参阅上述标准区域的证书要求。

对于 **DMZ** 代理部署：

- 一个或多个 DMZ 代理服务器，如 Citrix ADC VPX 实例。
- 对于终止客户端连接并使用 HTTP 的 DMZ 代理服务器，请在代理服务器上安装 SSL 证书。

  如果 DMZ 代理服务器和 StorageZones Controller 之间的通信是安全的，则可以使用 HTTP。但是，建议将 HTTPS 作为最佳做法。如果使用 HTTPS，则可以在 StorageZones Controller 上使用私有（企业）证书（如果 DMZ 代理信任）。DMZ 代理公开的外部地址必须使用商业信任的证书。有关支持的证书的信息，请参阅上述标准区域的证书要求。

其他要求

- StorageZones Controller 安装程序需要管理权限。
- 对于 StorageZones Controller 的远程管理，请使用远程协议（如 RDP 或 Citrix ICA）连接到服务器，然后打开 StorageZones Controller 控制台。

支持的第三方存储系统

- Amazon Simple Storage Service（Amazon S3）
- Microsoft Azure

支持的数据丢失防护解决方案

- StorageZones Controller 与任何符合 ICAP 标准的 DLP 解决方案集成，包括：
  - 赛门铁克数据丢失防护
  - McAfee DLP 防止
  - Websense TRITON AP-DATA
  - RSA 数据丢失防护

ShareFile 数据的存储区域

ShareFile Data 的存储区域是您在 StorageZones Controller 上启用的可选功能。

要求：

- 已启用存储区域功能的 ShareFile Enterprise 帐户
- 包含创建和管理区域权限的 ShareFile 用户帐户

- 用于私有数据存储的 CIFS 共享

如果计划将 ShareFile 文件存储在受支持的第三方存储系统中，CIFS 共享将用于临时文件（加密密钥、排队文件），并用作临时存储缓存。

- Web 服务器 (IIS) 角色和 ASP.NET 4.x。有关详细信息，请参阅为 ShareFile 数据准备服务器。

注意：从 FTP 客户端访问 ShareFile 帐户与 ShareFile 数据的存储区域不兼容。

用于 **SharePoint** 的存储区域连接器

SharePoint 的存储区域连接器是您在 StorageZones Controller 上启用的可选功能。

要求:

- ShareFile Enterprise 帐户（启用了存储区域功能）或 Citrix Endpoint Management。
- 仅支持 **Microsoft SharePoint Server 2010** 及更新版本。
- StorageZones Controller 服务器必须是域成员，位于与 SharePoint 服务器相同的林中。
- Web 服务器 (IIS) 角色和 ASP.NET 4.x。有关详细信息，请参阅为 ShareFile 数据准备服务器。
- SharePoint 策略：
  - 在 SharePoint 2013 年中的 Web 应用程序的默认最大上载文件大小为 250 MB，并且在 SharePoint 2010 中为 50 MB。要更改默认值：在 SharePoint 管理中心中，转到 Web 应用程序常规设置页面并更改最大上载大小。SharePoint 的上载文件大小限制为 2 GB。
  - ShareFile 客户端始终尝试签入文件的主要版本（发布）。但是，SharePoint 策略确定文件是作为主要版本还是次要版本签入。
  - SharePoint 仅查看权限不允许用户下载文件。要从 ShareFile 客户端读取文件，SharePoint 用户必须具有读取权限。
- 用户设备：有关用户设备支持存储区域连接器的最新信息，请参阅 ShareFile 知识库。

用于 **SharePoint** 身份验证的存储区域连接器

对用户进行身份验证后，StorageZones Controller 服务器将代表经过身份验证的用户与 SharePoint 服务器建立连接，并响应 SharePoint 服务器提出的身份验证挑战。SharePoint 的存储区域连接器支持 SharePoint 服务器上的以下身份验证方法。

- 基本

  要求您添加 `<add key=”CacheCredentials”value=”1”\>` 到 `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.

- 谈判 (克尔贝罗斯)
- Windows 质询/响应 (NTLM)

ShareFile 移动客户端使用 HTTPS 的基本身份验证来对 StorageZones Controller 或 DMZ 代理进行身份验证。SharePoint 的单点登录受 SharePoint 服务器上设置的身份验证要求的约束。要在 SharePoint 服务器上使用 Kerberos 或 NTLM 身份验证，请执行以下操作：配置域控制器以信任存储区域控制器进行委派。

如果您的 SharePoint 服务器配置为 Kerberos 身份验证：为 SharePoint 服务器应用程序池的指定用户服务帐户配置服务主体名称 (SPN)。有关详细信息，请参阅中的 “为 Web 部件委派配置信任”http://support.microsoft.com/kb/832769。

对于使用 Citrix ADC 进行部署，可以终止 Citrix ADC 的基本身份验证，然后对 StorageZones Controller 执行其他类型的身份验证。

网络文件共享的存储区域连接器

网络文件共享的存储区域连接器是您在 StorageZones Controller 上启用的可选功能。

要求:

- ShareFile Enterprise 或 Citrix Endpoint Management 帐户。
- 存储区域连接器服务器必须是域成员，与网络文件服务器位于同一林中。
- Web 服务器 (IIS) 角色和 ASP.NET 4.x。有关详细信息，请参阅为 ShareFile 数据准备服务器。
- 用户设备：有关用户设备支持存储区域连接器的最新信息，请参阅 ShareFile 知识库。

用于网络文件共享身份验证的连接器

对用户进行身份验证后，StorageZones Controller 服务器代表经过身份验证的用户与网络文件服务器建立连接，并响应文件服务器提出的身份验证挑战。网络文件共享的存储区域连接器支持文件服务器上的以下身份验证方法。

- 谈判 (克尔贝罗斯)
- Windows 质询/响应 (NTLM)

若要在 StorageZones Controller 上使用 Kerberos 或 NTLM 身份验证：配置域控制器以信任存储区域控制器进行委派。

对于使用 Citrix ADC 的部署：要在将 Citrix ADC 配置为基本身份验证时为用户提供单点登录体验，请为协商 (Kerberos) 和 NTLM 身份验证配置连接器。

PowerShell 脚本和命令

StorageZones Controller 安装包括位于中的多个 PowerShell 脚本和命令`C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\`。

- 在 32 位 (x86) 版本的 PowerShell 中运行脚本。
- 要获得最佳效果，请升级到随附的 PowerShell 4.0 Windows Management Framework 4.0。

  由于.NET Framework 4 的兼容性问题，PowerShell 2.0 会导致重大问题。

安装

June 15, 2020

按照显示的顺序完成以下任务，以安装和设置 StorageZones Controller、ShareFile Data 的存储区域和存储区域连接器。

1. 为存储区域控制器配置 Citrix ADC

   您可以使用 Citrix ADC 作为 StorageZones Controller 的 DMZ 代理。

2. 为专用数据存储创建网络共享

   ShareFile 数据的存储区域需要您的私有数据的网络共享，即使您将 ShareFile 文件存储在受支持的第三方存储系统中也是如此。

3. 安装 SSL 证书

   托管标准区域的存储区域控制器需要 SSL 证书。

4. 为 ShareFile 数据准备服务器

   对于 ShareFile 数据的存储区域和存储区域连接器，IIS 和 ASP.NET 设置是必需的。

5. 安装 StorageZones Controller 并创建存储区域

6. 验证您的 StorageZones Controller 设置

7. 更改用户帐户的默认区域

   默认情况下，现有和新置备的用户帐户使用 ShareFile 管理的云存储作为默认区域。

8. 指定存储区域的代理服务器

   存储区域控制器控制台允许您为存储区域控制器指定代理服务器。还可以使用其他方法指定代理服务器。

9. 配置域控制器以信任存储区域控制器进行委派

   配置域控制器以在网络共享或 SharePoint 站点上支持 NTLM 或 Kerberos 身份验证。

10. 将辅助存储区域控制器加入到存储区域

    要配置存储区域以实现高可用性，请至少将两个存储区域控制器连接到该存储区域。

有关使用 Microsoft Azure 存储配置 StorageZones Controller 的演示，单击此处。

有关将 ShareFile Enterprise 配置为使用 Microsoft Azure 存储区域的演示，请 单击此处。

其他设置说明

- 配置多租户存储区域
- 为 Web 应用程序预览、缩略图和仅查看共享配置 StorageZones Controller

为存储区域控制器配置 **Citrix ADC**

June 15, 2020

NetScaler 版本 10.1 版本生成 120.1316.e 及更高版本包含一个向导，提示您输入有关 StorageZones Controller 环境的基本信息。然后它生成一个配置：

- 跨存储区域控制器平衡流量的负载
- 为存储区域连接器提供用户身份验证
- 验证 ShareFile 上载和下载的 URI 签名
- 终止 Citrix ADC 设备上的 SSL 连接

图中显示了由配置创建的这些 Citrix ADC 组件：

- **Citrix ADC** 内容交换虚拟服务器 — 将用户对数据的请求从 ShareFile 和存储区域连接器发送到相应的 Citrix ADC 负载平衡虚拟服务器。
- **Citrix ADC** 负载平衡虚拟服务器 — 对 StorageZones Controller 的流量进行负载平衡，并处理以下事项：
  - 对于来自私有数据存储的数据请求，负载平衡虚拟服务器会执行哈希验证，以确保传入请求中存在有效的 URI 签名。
  - 对于来自存储区域连接器的数据请求，负载平衡虚拟服务器会执行用户身份验证。它会停止 Citrix ADC 上的用户请求，对用户进行身份验证，然后对用户执行单点登录到 StorageZones Controller。

  尽管 Citrix ADC 的身份验证是可选的，但建议采用最佳做法。

自 StorageZones Controller 4.0 起，管理员可以将与 StorageZones Controller 的入站连接限制为 TLS v1.2。如果针对向 StorageZones Controller 的入站流量禁用早于 TLS v1.2 的协议，则与存储区域交互的所有客户端软件组件也必须支持 TLS v1.2。单击此处获取更多信息和配置说明。

> 注意：
>
> 若要设置 10.1 版本 120.1316.e 之前版本的 NetScaler 版本，请参阅手动配置 Citrix ADC。

针对 ShareFile 的 Citrix ADC 向导的设置不会处理将 Citrix Endpoint Management 用作 ShareFile 的 SAML 身份提供程序所需的配置。有关详细信息，请参阅单击此处。

必备条件

- 正常工作的 Citrix ADC 配置
- 安全证书：如果 Citrix ADC 中尚未提供安全证书，则通过向导可以在内容交换虚拟服务器上安装一个证书。
- 有关 **Active Directory** 配置的信息（用于 **ShareFile** 的 **Citrix ADC** 向导必须使用 **Citrix NetScaler** 企业版许可证完成）：
  - Active Directory 服务器的 IP 地址和端口
  - Active Directory 域名

- 存储用户的 LDAP 基本 DN
- 具有与 Active Directory 通信权限的管理员帐户的帐户名和密码

为 **StorageZones Controller** 配置 **Citrix ADC**

以下步骤介绍了如何使用用于 ShareFile 的 Citrix ADC 向导。

1. 登录到 Citrix ADC 装置，然后在“配置”选项卡上导航到“流量管理”。
2. 在 Citrix ShareFile 下，单击“为 ShareFile 设置 Citrix ADC”。

   您还可以按如下方式访问该向导：在“移动性”下，单击“配置 **Endpoint Management”**、**“ShareFile”** 和 **“Citrix Gateway**”。
3. 提供向导中请求的信息。

选项	说明
名称	内容交换虚拟服务器的显示名称。
IP 地址	用于内容交换虚拟服务器的外部（公共或 DMZ）IP 地址。如果使用 DMZ IP 地址，则必须定义从外部防火墙地址到此 DMZ IP 地址的网络地址转换 (NAT) 映射。
ShareFile 数据	此选项处于启用状态，表示您将对 ShareFile 数据的存储区域使用 Citrix ADC 连接。
网络文件共享/共享点的存储区域连接器	如果使用连接器并希望在 Citrix ADC 上执行用户身份验证，请选中此复选框。
证书	为内容交换虚拟服务器选择证书或安装证书。如果您选择安装证书，系统将提示您上载证书和私钥。对于标准区域或具有外部主机名的受限区域，证书必须是公开信任的，而不是自签名。
StorageZones Controller IP 地址	一个或多个 StorageZones Controller 服务器的内部 IP 地址。这些 IP 地址将 StorageZones Controller 服务器定义为 Citrix ADC 内部的实体。如果已将服务器添加到 Citrix ADC，请单击从现有添加并选择服务器。要使用 Citrix ADC 进行负载平衡，请为每个 StorageZones Controller 服务器输入内部 IP 地址。要仅将 Citrix ADC 用于 SSL 和身份验证，请仅输入一个 IP 地址。
端口和协议	用于从 Citrix ADC 到 StorageZones Controller 的通信的端口和协议。

选项	说明
身份验证、授权和审核（Citrix ADC AAA）虚拟服务器 IP 地址	Citrix ADC AAA 虚拟服务器未使用的内部 IP 地址。Citrix ADC 创建此虚拟服务器供其自己使用。服务器不需要外部访问。
LDAP 服务器 IP 地址和端口	Active Directory 服务器的 IP 地址和端口。如果已将 LDAP 服务器添加到 Citrix ADC，请单击“选择 LDAP”选项卡并选择该服务器。
超时	Citrix ADC 等待 LDAP 服务器响应的最大秒数。默认为 3 秒。最小值为 1 秒。
单点登录域	Active Directory 域名。
基本 DN（用户位置）	存储用户的 LDAP 基本判别名 (DN)。使用常规形式指定 DN：CN=Users,dc=domain, dc=Net
管理员绑定 DN 和密码	具有与 Active Directory 通信权限的管理员帐户。
登录名称	一个 LDAP 属性，Citrix ADC 用于确定用户是使用其用户名还是电子邮件地址登录。默认为 SamAccountName，该名称允许用户使用其用户名登录。要要求用户输入其电子邮件地址以登录，请将此字段更改为用户主名称。

为受限区域或对连接器的 **Web** 访问配置 **Citrix ADC**

要支持受限区域或对存储区域连接器的 Web 访问，必须在完成针对 ShareFile 的 Citrix ADC 向导后执行其他 Citrix ADC 配置。

- 创建和配置第三个 Citrix ADC 负载平衡虚拟服务器，用于确保 ShareFile 客户端仅在登录到受信任的 ShareFile 域时才发送凭据。

  StorageZones Controller 使用跨源资源共享 (CORS) 标准为向受限区域的请求以及从 ShareFile Web 界面到存储区域连接器的请求提供必要的安全性。CORS 使用 HTTP 标头允许客户端和服务器相互了解足够的情况，以确定请求或响应是否应该成功。

  如以下步骤所述，您将配置额外的虚拟服务器，以允许客户端对 HTTP OPTIONS 动词进行匿名访问。OPTIONS 请求将传递到 StorageZones Controller，而不经过身份验证，也不使用 HTTPS 标注来验证签名。CORS 预检检查在发送凭据之前验证域信任。

  执行配置不需要了解 CORS。但是，有关 CORS 的更多信息，请参阅 http://enable-cors.org/。

  使用 Internet 资源管理器对受限区域中的连接器进行 Web 访问需要配置 Internet 资源管理器。

- 要支持对存储区域连接器的 Web 访问，请向用于到 /cifs 和 /sp 的流量的内容交换策略添加路径 (/Proxy Service)。

完成针对 ShareFile 的 Citrix ADC 向导后，在 Citrix ADC 中执行以下步骤。

1. 创建第三个负载平衡虚拟服务器：
   a) 导航到 流量管理 **>** 负载平衡 **>** 虚拟服务器。
   b) 单击 “添加”。
   c) 指定以下值：

选项	值
名称	策略名称，例如 SF_ZONE_OPTIONS
协议	SSL
IP 地址类型	不可寻址

   d) 单击以创建虚拟服务器。
   e) 要将与向导创建的负载平衡虚拟服务器相同的服务绑定到该服务器：在负载平衡虚拟服务器屏幕中的 “服务” 中，单击 >，然后单击 “保存”。
   f) 向虚拟服务器添加证书。
2. 为刚刚添加的虚拟服务器创建策略：
   a) 导航到流量管理 > 内容切换 > 策略。
   b) 在详细信息窗格中，单击添加，然后指定名称、目标 LB 虚拟服务器和表达式值。单击 表达式编辑器，然后生成此表达式。选择 **HTTP**。选择 **REQ**。选择 方法。选择均衡器（字符串）并键入选项。该表述应改为：`HTTP.REQ.METHOD.EQ("OPTIONS")`
   c) 单击完成。
   d) 单击创建。
3. 将刚创建的策略绑定到新的负载平衡虚拟服务器：
   a) 导航到 流量管理 **>** 内容切换 **>** 虚拟服务器。
   b) 在列表中，单击虚拟服务器，然后单击 编辑。
   c) 导航到内容交换策略绑定部分，然后单击 2 个内容交换策略。
   d) 单击添加绑定。
   e) 选择新的内容策略，然后选择目标负载平衡虚拟服务器。
   f) 单击 **Bind**（绑定）。
   g) 单击 编辑绑定并更新 优先级。更改新策略的优先级，使其具有三个策略中最少的数量。
   具有最低值的策略具有最高优先级，因此首先处理。
4. 更新用于到存储区域连接器的流量的策略 (_SF_CIF_SP_CSPOL)：
   a) 导航到 流量管理 **>** 内容切换 **>** 策略。
   b) 选择 _SF_CIF_SP_CSPOL 策略。
   c) 将以下内容添加到策略表达式中：

```
|| HTTP.REQ.URL.CONTAINS("/ProxyService/")
```


完整的策略表达式应如下所示：

```
HTTP.REQ.URL.CONTAINS("/cifs/") || HTTP.REQ.URL.CONTAINS("/sp/
    ") ||
HTTP.REQ.URL.CONTAINS("/ProxyService/")
```

5. 更新用于向 ShareFile 数据 (_SF_SZ_CSPOL) 存储区域的流量的策略：
   a) 导航到 流量管理 **>** 内容切换 **>** 策略。
   b) 选择 **_SF_SZ_CSPOL** 策略。
   c) 将以下内容添加到策略表达式中：

```
&& HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT
```

完整的策略表达式应如下所示：

```
HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("
    /sp/ ").NOT
&& HTTP.REQ.URL.CONTAINS("/ProxyService/").NOT
```

为仅查看共享配置 **Citrix ADC**

若要支持仅查看共享，用户必须能够访问您的 Microsoft Office Web 应用服务器 (OWA)。如果 OWA 服务器可通过其自己的地址进行外部访问，则不需要为 StorageZones Controller 进行额外的 Citrix ADC 配置。

如果要使用 Citrix ADC 内容交换策略将 StorageZones Controller 和 Office Web 应用程序服务器合并到单个外部地址，则必须在完成 ShareFile 的 Citrix ADC 向导后执行其他 Citrix ADC 配置。需要 Citrix ADC 配置，以确保流量被正确路由到外部可访问的 OWA 服务器。

配置了以下 Citrix ADC 规则后，管理员可以重复使用其 StorageZones Controller 区域的现有外部地址，从而无需为 OWA 创建额外的外部地址。

要创建和配置其他 Citrix ADC 负载平衡虚拟服务器，请执行以下操作：

1. 创建额外的负载平衡服务。
   - 导航到 流量管理 **>** 负载平衡 **>** 服务。
   - 单击添加。
   - 输入创建与 OWA 服务器对应的服务所需的信息。单击确定。
2. 创建额外的负载平衡虚拟服务器：
   - 导航到 流量管理 **>** 负载平衡 **>** 虚拟服务器。
   - 单击添加。
   - 指定以下值：

选项	值
名称	策略名称，如 SF_OWA_vServer
协议	SSL
IP 地址类型	不可寻址

- 单击以创建虚拟服务器。
- 要将虚拟服务器绑定到上一步中创建的 OWA 服务，请单击 负载平衡虚拟服务绑定 **>** 选择服务。单击您在上一步中创建的服务旁边的复选框。
- 单击 **Select**（选择）。
- 单击 **Bind**（绑定）。

3. 创建用于将流量路由到 OWA 服务器的新策略。
   - 导航到 流量管理 **>** 内容切换 **>** 策略。
   - 选择添加。
   - 命名策略。
   - 添加以下表达式：
     - HTTP.REQ.URL.CONTAINS(“/hosting/discovery”)
       || HTTP.REQ.URL.CONTAINS(“/x/”)
       || HTTP.REQ.URL.CONTAINS(“/wv/”)
       || HTTP.REQ.URL.CONTAINS(“/p/”)
       完整的策略表达式应如下所示：
       HTTP.REQ.URL.CONTAINS(“/hosting/discovery”)
       || HTTP.REQ.URL.CONTAINS(“/x/”)
       || HTTP.REQ.URL.CONTAINS(“/wv/”)
       || HTTP.REQ.URL.CONTAINS(“/p/”)
4. 在负载平衡虚拟中更新新策略的优先级
   - 导航到 流量管理 **>** 内容切换 **>** 虚拟服务器。
   - 单击负载平衡虚拟服务器，然后选择内容交换策略。
   - 更改策略的优先级，以便（示例）“_SF_OWA” 策略的优先级位于第三位。

优先级	策略名称
90	SF_ZK_OPTIONS
95	_SF_CIF_SP_SPOL
99	_SF_OWA
100	_SF_SZ_CSPOL

- 单击关闭。单击 “完成”

为 **StorageZones Controller** 服务创建监视器

默认情况下，Citrix ADC 会对 StorageZones Controller 服务器进行 ping 处理，以确定它是否处于联机状态。但是，即使 Controller 处于联机状态，它可能无法向 ShareFile 网站发送检测信号消息。在这种情况下，Citrix ADC 将向 StorageZones Controller 发送流量，尽管它不与 ShareFile 通信。

要验证 StorageZones Controller 与 ShareFile 的出站连接，您可以创建一个监视器来检查心脏.aspx 并将其绑定到每个 StorageZones Controller 的 Citrix ADC 服务。

```
1     add lb monitor SZC_Heartbeat HTTP-ECV -send "GET /heartbeat.aspx" -
          recv "\*\*\*ONLINE\*\*\*"  -secure YES
2 bind service StorageZone_Svc -monitorName SZC_Heartbeat
```

StorageZone_Svc 是对应于 StorageZones Controller 的 Citrix ADC 服务。该服务名由 Citrix ADC 针对 ShareFile 向导自动创建。服务名称包括 Controller 的 IP 地址，例如 _SF_SVC_ip-address。

-如果服务正在侦听端口 443，则需要 “是”。

验证 **Citrix ADC** 配置

完成向导后，转到 “流量管理**”>“**负载平衡**”>“**虚拟服务器” 以查看由向导创建的负载平衡虚拟服务器的状态。

查看通过 **Citrix ADC ShareFile** 请求的吞吐量

吞吐量统计信息可以在 控制板菜单中找到。

手动配置 **Citrix ADC**

June 15, 2020

从版本 10.1 版本 120.1316 开始，Citrix ADC 包含一个向导，用于配置 StorageZones Controller 数据和连接器所需的设置。

本节中的步骤介绍 StorageZones Controller 所需的 Citrix ADC 设置。所有链接都适用于 NetScaler 10.1 文档。类似的主题适用于更高版本的 Citrix ADC。

检查所有传入邮件上的有效 **URI** 签名

1. 创建一个名为 sf_callout 的 HTTP 标注：
    a) 在配置 HTTP 标注对话框中，单击虚拟服务器或 IP 地址，然后指定地址。
    b) 在请求发送到服务器下，单击 基于属性，然后单击 配置请求属性。

c) 选择 获取方法。

d) 在“主机表达式”中，输入任何 StorageZones Controller 的虚拟服务器 IP 地址或主机 IP 地址。

e) 在 URL 干表达式中，输入：

```
1 ”/validate.ashx?RequestURI=” + HTTP.REQ.URL.BEFORE_STR(”&h”).
    HTTP_URL_SAFE.B64ENCODE + ”&h=”+ HTTP.REQ.URL.QUERY.VALUE(”
    h”)
```

f) 单 击“确定”，然后返回“配置 HTTP 标注”对话框。

g) 在“服务器响应”下，选择“布尔”的返回类型。

h) 在表达式中，要从响应中提取数据，请输入：

```
HTTP.RES.STATUS.EQ(200).NOT
```

i) 单击创建。

有关详细信息，请参阅 HTTP 标注。

2. 按照上述步骤配置名为 sf_callout_y 的 HTTP 标注。除表达式外，使用相同的设置：

   - 在 URL 干表达式中，输入：

   ```
   ”/validate.ashx?RequestURI=”+ HTTP.REQ.URL.HTTP\\_URL\\_SAFE.
   B64ENCODE + ”\\&h=”
   ```

3. 配置响应者策略：

   a) 在配置响应程序策略对话框中：对于操作，选择删除。

   b) 在表达式中，输入：

   ```
   1 http.REQ.URL.CONTAINS(”&h=”) && http.req.url.contains(”/
       crossdomain.xml”).not && http.req.url.contains(”/validate.
       ashx?requri”).not && SYS.HTTP_CALLOUT(sf_callout) || http.
       REQ.URL.CONTAINS(”&h=”).NOT && http.req.url.contains(”/
       crossdomain.xml”).not && http.req.url.contains(”/validate.
       ashx?requri”).not && SYS.HTTP_CALLOUT(sf_callout_y)
   ```

   有关详细信息，请参阅响应方。

4. 将响应程序策略绑定到负载平衡器虚拟服务器 并进行配置 基于 SSL 会话的持久性。

要负载平衡

1. 配置基于令牌的负载平衡。

   使用规则表达式： “http.REQ.URL.QUERY.VALUE(”uploadid”)”

   高可用性部署中的 StorageZones Controller 需要基于令牌的负载平衡。循环负载平衡将导致间歇性下载或上载失败，因为客户端上载或下载请求可能会被定向到 StorageZones Controller，而不是从 ShareFile.com 接收授权请求的控制器。

2. 将 Citrix ADC 配置为终止 SSL 连接。

   有关信息，请参阅 配置 SSL 卸载 及其子主题。

配置连接器的内容切换和身份验证

1. 启用内容切换，如中所述 启用内容切换。
2. 为来自本地存储区域的用户请求 ShareFile 数据创建内容切换策略：
   a) 在“配置内容交换策略”对话框中：输入内容交换策略的名称。这些步骤使用名称“数据请求”。
   b) 输入表达式：

   ```
   HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerHostName")&& HTTP
   .REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("/sp/").
   NOT
   ```

   c) 单击确定。

   有关详细信息，请参阅内容交换。
3. 为用户请求从存储区域连接器访问的数据创建内容切换策略。
   a) 在“配置内容交换策略”对话框中：指定内容交换策略的名称。这些步骤使用名称“连接器请求”。
   b) 输入表达式：

   ```
   HTTP.REQ.HOSTNAME.CONTAINS("StorageZonesControllerFQDN")&& (HTTP.
   REQ.URL.CONTAINS("/cifs/")|| HTTP.REQ.URL.CONTAINS("/sp/"))
   ```

   请务必将“存储区域 Controller FQDN”替换为控制器的 FQDN。
   c) 单击确定。
4. 创建内容交换虚拟服务器。
5. 设置内容交换策略目标：
   - 在配置虚拟服务器（内容切换）对话框中：对于 Data_Reques 策略，为 ShareFile 数据的存储区域指定负载均衡器虚拟服务器。

     此负载均衡器虚拟服务器是您在步骤 4 中将响应程序策略绑定到该服务器的服务器，检查所有传入消息上的有效 URI 签名并进行负载平衡。
   - 对于 Connector_Request 策略，指定存储区域连接器的负载均衡器虚拟服务器。
6. 为存储区域连接器配置身份验证虚拟服务器：

   尽管 Citrix ADC 的身份验证是可选的，但建议采用最佳做法。
   a) 在导航窗格中，展开负载平衡，为存储区域连接器选择负载平衡器虚拟服务器的名称，然后单击打开。
   b) 在配置虚拟服务器（负载平衡）对话框中，单击 高级选项卡，然后展开 身份验证设置。

c) 选中基于 401 的身份验证的复选框，然后选择身份验证虚拟服务器。

d) 单击方 法和持久性选项卡。

e) 对于持久性，请选择 **COOKIEINSERT**。

f) 对于超时（分钟），请输入 **240**。

建议使用 240 分钟的超时值。最小值应大于 10 分钟。

有关详细信息，请参阅配置身份验证虚拟服务器。

7. 使用“配置身份验证服务器”对话框可以创建和配置身份验证服务器。

在 SSO 名称属性中，输入 用户主名称。

有关其他设置的详细信息，请参阅 身份验证策略。

8. 为刚刚创建的身份验证服务器配置身份验证策略：

a) 在配置身份验证策略对话框中：输入策略的名称，然后选择上一步中配置的身份验证服务器。

b) 输入表达式：

```
ns_true
```

有关详细信息，请参阅配置身份验证策略。

9. 为单点登录配置会话配置文件：

a) 在配置会话配置文件对话框中，输入配置文件的名称。
b) 选中单点登录到 Web 应用程序的复选框。
c) 对于凭据索引，选择 主要。
d) 在单点登录域中，输入 StorageZones Controller 的域名。
e) 为前面三个项目中的每个项目选中“覆盖全局”复选框。

有关详细信息，请参阅会话配置文件。

10. 为单点登录配置会话策略：

a) 在“配置会话策略”对话框中，输入策略的名称。

b) 对于 请求配置文件，选择在上一步中配置的会话配置文件的名称。

c) 输入表达式：

```
ns_true
```

有关详细信息，请参阅会话策略。

11. 创建身份验证虚拟服务器：

a) 在配置虚拟服务器（身份验证）对话框中，输入服务器的名称和 IP 地址。
b) 单击 身份验证选项卡，对于 协议，选择 **SSL**。
c) 选中对用户进行身份验证的复选框。

d) 在“身份验证策略”下，单击“主”，然后选择您在步骤 7 中配置的身份验证策略。
e) 单击 策略选项卡，单击 会话，然后选择您在步骤 9 中配置的会话策略。

有关详细信息，请参阅配置身份验证虚拟服务器。

为专用数据存储创建网络共享

June 15, 2020

ShareFile 数据的存储区域需要您的私有数据的网络共享。如果将多个 StorageZones Controller 配置为一个区域内的高可用性和负载均衡，则所有控制器都会访问相同的共享位置以获取私有数据。

即使您将 ShareFile 文件存储在受支持的第三方存储系统中，StorageZones Controller 也需要用于加密密钥、排队文件、其他临时项的网络共享，以及用于将文件上载到该存储系统或从该存储系统下载的存储缓存。有关存储缓存的详细信息，请参阅 自定义存储缓存操作。

StorageZones Controller 使用 IIS 帐户池用户访问网络共享。默认情况下，应用程序池在具有低级别用户权限的网络服务用户帐户下运行。StorageZones Controller 默认使用网络服务帐户。您可以使用指定用户帐户而不是网络服务帐户来访问共享。但是，您应该使用网络服务帐户运行 IIS 应用程序池和 Citrix ShareFile 服务。

1. 如果要使用指定用户帐户而不是网络服务帐户来访问共享，请在 Active Directory 中创建一个指定用户帐户。我们将该指定用户帐户称为 ShareFile 服务帐户。
   注意：配置 StorageZones Controller 时，您将指定网络共享用户名和网络共享密码，它们是用于访问共享的帐户（ShareFile 服务帐户或网络服务帐户）的凭据。

   为了提高安全性，管理员需要拒绝所有其他用户访问包含 ShareFile 存储库的特定文件夹的权限，并仅授予正在配置的存储位置用户的访问权限。
2. 连接到将承载网络共享的服务器，并为您的 ShareFile 专用数据创建文件夹。
3. 右键单击文件夹，然后选择与特定人员共享...
4. 添加用于访问共享的帐户（网络服务帐户或 ShareFile 服务帐户），并将权限级别更改为读/写。
5. 单击“共享”，然后单击“完成”。
6. 右键单击该文件夹，然后选择“属性”。
7. 在安全选项卡上，验证将用于访问共享的帐户（网络服务帐户或 ShareFile 服务帐户）是否具有完全访问权限。

增加每个区域的文件数

默认情况下，将存储区域 Controller 配置为使用 CIFS 共享将文件存储在文件夹层次结构中，而不是单个文件夹中。

您可以配置 StorageZones Controller 来划分持久存储布局。这将某些类型的存储阵列的每个区域的最大文件数从 50 万增加到 1000 万或更多。如果需要额外的容量，可以更改默认值。

若要启用 **StorageZones Controller** 将文件存储在多个文件夹中

> 小心：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。
>
> 注意：
>
> 如果 StorageZones Controller 已升级，请检查注册表项 `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone\PathSelection is set to 1. If it is set to 0, update it to 1` 的值。

完成注册表编辑后，重新启动 StorageZones Controller 上的 IIS。

增加文件夹的最大数量

默认情况下，分割的存储布局有 256 个顶级文件夹，每个文件夹都包含 256 个文件夹。该配置在主 StorageZones Controller 注册表项中表示`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone:PathSelectionParams=2,2`。

第一个值将顶级文件夹的数量限制为 “16 的 2 次方” 或 256。第二个值还将顶级文件夹的子文件夹的数量限制为 256。

使用相同的公式（16 到 N 的幂），您可以为您的站点确定适当的值。例如，路径选择参数 = 3,4,4,4 将顶级文件夹的数量限制为 4096（16 为 3 的幂）。第二个值将顶级文件夹的子文件夹的数量限制为 65536（16 到 4 的幂）。第三个值将二级文件夹的子文件夹的数量限制为 65536，依此类推。

如果完成注册表的编辑，则在主存储区域和辅助 StorageZones Controller 上重新启动 IIS。

删除空文件夹

当 StorageZones Controller 将文件存储在多个文件夹中时，文件删除可能会导致文件夹空。默认情况下，StorageZones Controller 删除空文件夹。文件删除服务将删除空文件夹，从树底部开始，直到到达非空文件夹为止。

但是，某些升级路径可能无法更新您的设置。升级后，验证中是否显示以下密钥 `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`:

```
<add key=”DeleteEmptyFoldersAfterFileDeletion”  value= “1” />
```

如果需要添加密钥，请在完成后重新启动文件删除服务。

安装 **SSL** 证书

June 15, 2020

如果不使用通配符证书，则必须为 StorageZones Controller 服务器创建证书签名请求 (CSR)，并将请求提交给证书颁发机构 (CA)。有关帮助，请参阅 CA 的文档。

请按照以下步骤安装证书。

1. 在 StorageZones Controller 服务器上，打开 MMC，然后选择 “文件”>“添加/删除管理单元”。
2. 选择证书，然后单击 添加。
3. 选择 “计算机帐户”，单击 “下一步”，单击 “完成”，然后单击 “确定”。
4. 在 MMC 控制台中，展开 “证书”>“个人”。
5. 右键单击 “证书”，选择 “所有任务”>“导入”，然后单击 “下一步”。
6. 单击 浏览，然后从文件扩展名菜单中选择 个人信息交换。
7. 浏览到证书位置，然后单击 打开。
8. 单击 下一步，输入与您的私钥关联的 密码，单击 下一步两次，然后单击 完成。
9. 出现消息 “导入成功” 后，单击 “确定”。

对于公用证书，请确保其颁发的域解析为 StorageZones Controller 的本地 IP 地址。为此，请更新 StorageZones Controller 上的主机文件，以将与证书关联的域映射到 StorageZones Controller IP 地址。如果两个地址无法解析，用户将无法从 StorageZones Controller 上载文件。

为 **ShareFile** 数据准备服务器

June 15, 2020

对于 ShareFile 数据的存储区域和存储区域连接器，必须使用本节中介绍的 Web 服务器 (IIS) 角色和 ASP.NET 设置。这些说明基于 Windows Server 2012。StorageZones Controller 的旧文档 中提供了有关 Windows Server 2008 的说明。

更新 **Microsoft .NET** 版本

继续安装 StorageZones Controller 之前，请确保您使用的是适当版本的 Microsoft .NET Framework。

- 存储区域 **Controller 5.x** 需要**.NET 4.8** 或更高版本。点击此处下载.NET 4.8

ShareFile 建议在使用 ShareFile 应用程序时使用最新版本的 Microsoft .NET。

启用 **Web** 服务器 **(IIS)** 角色和 **ASP.NET** 角色服务

1. 在安装存储区域 Controller 的服务器上，使用具有本地管理员权限的帐户登录。
2. 打开服务器管理器控制台仪表板，然后单击 管理 **>** 添加角色和功能以打开添加角色和功能向导。
3. 在添加角色和功能向导中，单击 下一步。
4. 在 “选择安装类型” 页上，单击 “基于角色或基于功能的安装”，然后单击 “下一步”。

5. 在“选择目标服务器”页上，从服务器池中选择您的服务器，然后单击“下一步”。
6. 在“选择服务器角色”页上，选中 Web 服务器 (IIS) 复选框和 Windows 服务器更新服务复选框，然后单击 下一步。
7. 单击“添加功能”以添加 IIS 所需的功能。
8. 单击“添加功能”。此时将显示“选择功能”页面。
9. 选择以下屏幕中显示的所需设置，然后单击“下一步”。
10. 在 Web 服务器角色 (IIS) 页上，单击 下一步。
11. 在“选择角色服务”页上，选中“基本身份验证”和“Windows 身份验证”复选框，然后单击“下一步”。
12. 在“确认安装选择”页上，单击“安装”。
13. 安装完成后，单击“关闭”，然后重新启动服务器。

配置 **IIS**

启用 Web 服务器 (IIS) 角色和 ASP.NET 角色服务后，配置 IIS。

1. 打开 IIS 管理器控制台，单击 StorageZones Controller 服务器节点，然后双击 ISAPI 和 CGI 限制。
2. 将每个 ASP.NET 条目设置为允许。
3. 验证服务器上是否安装了域服务器或公用证书：在 IIS 管理器控制台中，单击 StorageZones Controller 服务器节点，然后双击服务器证书。

   如果没有与公共证书颁发机构关联的证书，请在服务器上安装证书，然后继续操作。有关详细信息，请参阅安装 SSL 证书。

   > 注意：
   >
   > 如果您使用的是 Citrix Gateway 或类似设备与 StorageZones Controller，则可以使用域服务器证书。标准区域的所有互联网流量必须使用公共证书进行处理。

4. 在 IIS 管理器控制台中，单击 默认网站，然后单击 绑定。
5. 单击添加并按如下方式配置站点绑定：
   - 类型是 https。
   - IP 地址为“全部未分配”。
   - 港口是 443。
   - SSL 证书是您已安装的证书。
6. 要测试 Web 服务器连接，请导航到 `http://localhost/` 和 `https://localhost/`。如果连接成功，则会显示 IIS 徽标。

   HTTPS 在 URL 标头中显示有关证书与本地主机名称不匹配的消息。这是预期的，你可以安全地继续访问网站。
7. 如果要在 VM 上安装 StorageZones Controller，请拍摄虚拟机的快照。

安装 **StorageZones Controller** 并创建存储区域

June 15, 2020

> 重要：
>
> 在开始安装 系统要求 之前，验证您的环境是否符合。

安装 StorageZones Controller 时，您可以创建区域并配置主 StorageZones Controller 或 将辅助 StorageZones Controller 连接到区域。

配置主 StorageZones Controller 时，您可以启用以下任一功能或两项功能：

- ShareFile Data 的存储区域，用于指定专用数据存储，可以是专用网络共享或受支持的第三方存储系统。
- 存储区域连接器，允许用户访问 SharePoint 站点或指定网络文件共享上的文档。

以下步骤介绍如何安装 StorageZones Controller、配置 IIS 默认网站的身份验证、创建区域和启用功能。

1. 下载并安装存储区域控制器软件：
   - 从 ShareFile 下载页面中http://www.citrix.com/downloads/sharefile.html，登录并下载最新的 StorageZones Controller 安装程序。

   > 注意：
   >
   > 安装 StorageZones Controller 将服务器上的默认网站更改为 Controller 的安装路径。

   应在默认网站上启用匿名身份验证。
2. 在要安装存储区域控制器的服务器上，运行 StorageCenter.msi。
   - 将启动 ShareFile StorageZones Controller 安装向导。
   - 对于多租户，请运行以下命令：***msiexec /i StorageCenter_5.0.1.msi MULTITENANT=1***

   > 注意：
   >
   > 在前面的命令中，您可能需要更新版本号（示例中为 5.0.1）以匹配您尝试安装的 msi 号。

   - 响应提示。安装完成后，清除 启动 **StorageZones Controller** 配置页面的复选框，然后单击 完成。
3. 重新启动 StorageZones Controller。
4. 要测试安装是否成功，请导航到 `http://localhost/`。如果安装成功，会显示 ShareFile 徽标。
5. 如果没有显示 ShareFile 徽标，请清除浏览器缓存，然后重试。

   > 重要：
   >
   > 如果您打算克隆存储区域控制器，请先捕获磁盘映像，然后再继续配置存储区域控制器。

6. 要在 ShareFile 中使用 S3 兼容的存储提供程序，请在创建或配置存储区域之前执行以下步骤。
   - 打开 Windows 注册表编辑器（运行 **> regedit.exe**）。

- 找到注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter。
- 在此项下创建一个新的 REG_SZ 值：
  - 值名称：**S3EndpointAddress**
  - 值类型：**REG_SZ**
  - 值数据：输入与您的 S3 兼容存储端点对应的 HTTPS URL。
- 如果存储提供程序仅支持路径式容器访问（请参阅 http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html），请在此项下创建另一个值。
  - 值名称：**S3ForcePathStyle**
  - 值类型：**REG_SZ**
  - 值数据：真
- 重新启动 StorageZones Controller 应用程序池 (StorageCenterAppPool)。
- 从 S3 兼容的存储系统中收集以下信息：
  - 用于 ShareFile 数据访问密钥 ID 的 S3 存储桶的名称
  - 访问密钥 ID
  - 私有访问密钥

7. 继续执行以下步骤以创建新的存储区域。选择 Amazon S3 作为永久存储位置。StorageZones Controller 使用您输入的自定义端点地址，而不是实际的 Amazon S3 服务。配置 S3 详细信息时，请选择您之前创建的存储桶名称。
8. 导航到 StorageZones Controller 控制台。
9. 从“开始”屏幕 `http://localhost/configservice/login.aspx` 或菜单中打开或启动配置工具。有关在 Windows 8 中使用“开始”屏幕快捷方式的信息，请参阅 管理 StorageZones Controller。
10. 在 **StorageZones Controller** 登录页上，输入您的帐户的电子 邮件地址、密码和完整帐户 **URL FQDN** 子域 `subdomain.sharefile.com`，如 `subdomain.sharefile.eu` 或。单击登录。
11. 要设置主 StorageZones Controller，请单击“创建新区域”并提供区域信息：

选项	说明
区域	显示在 ShareFile 管理员控制台中的名称。

选项	说明
主区域 Controller	默认为 `http://localhost/ConfigService`。如果您使用 SSL，请将 HTTP 更改为 https。请记住，ShareFile 仅支持标准区域的有效、受信任的公共 SSL 证书。如果配置辅助存储区域主机时遇到问题，请确保您可以在该服务器上的本地浏览器中解析 ConfigService URL，但没有 SSL 错误。localhost 将解析为服务器 IP 地址。您可以改为指定服务器名称（例如 `https://servername.subdomain.com/ConfigService`）。服务器名称必须由辅助 StorageZones Controller 服务器解析。
主机名	StorageZones Controller 的唯一标识符。ShareFile 建议您使用服务器主机名作为标识符。这应该是一个友好的名称，而不是 FQDN。此名称显示在 ShareFile 管理员控制台中。
外部地址	此 StorageZones Controller 的 FQDN。如果此 StorageZones Controller 将用于标准区域，则必须从 Internet 访问该 URL。如果您使用的是负载均衡器，请输入其地址。当您提交页面时，ShareFile 会验证该地址。

12. 要指定专用数据存储，请执行以下操作。

    - 选中为 **ShareFile** 数据启用存储区域的复选框。
    - 要配置标准区域，请清除该复选框。

    > 注意：
    >
    > 配置 StorageZones Controller 后，无法更改其区域类型。

    StorageZones Controller 使用服务帐户凭据连接到受信任的 Active Directory 域服务器进行电子邮件地址查找。

    - 选择存储库。

13. 如果您不想启用存储区域连接器，请单击“注册”以将 StorageZones Controller 注册到 ShareFile，然后继续执行步骤 14。
14. 如果您使用的是 S3 兼容存储，请在存储区域注册后创建这些附加注册表项：

    - 打开 Windows 注册表编辑器（运行 **> regedit.exe**）。

- 查找注 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\storage zone\CloudStorageUploaderConfig` 册表项。
- 在此项下创建一个新的 REG_SZ 值：
  - 值名称：**S3EndpointAddress**
  - 值类型：**REG_SZ**
  - 值数据：输入与您的 S3 兼容存储端点对应的 HTTPS URL。
- 如果存储提供程序仅支持路径式容器访问（请参阅 http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html），请在此项下创建另一个值。
  - 值名称：**S3ForcePathStyle**
  - 值类型：**REG_SZ**
  - 值数据：真
- 重新启动 StorageZones Controller 应用程序池 (StorageCenterAppPool)。

15. 要启用存储区域连接器，请执行以下操作：

    启用连接器将创建 IIS 应用程序 “cifs”（用于网络文件共享的连接器）和 “sp”（用于 SharePoint 的连接器）。

    - 选中要使用的每个连接器类型的复选框：为网络文件共享启用存储区域连接器和为 SharePoint 启用存储区域连接器。有关连接器设置的信息 配置存储区域连接器，请参阅本节中的。
    - 单击 “注册”。将显示您的 StorageZones Controller 信息。
    - 如果为存储区域连接器指定了 “允许路径” 或 “拒绝路径”，请重新启动 IIS 服务器。

16. 要配置辅助 StorageZones Controller，请参阅管理 StorageZones Controller。

> 重要：
>
> StorageZones Controller 安装在您的本地站点上，您负责备份它。为了保护您的部署，您应该拍摄 StorageZones Controller 服务器的快照 备份 StorageZones Controller 配置 和 准备用于灾难恢复的 StorageZones Controller。

为 **ShareFile** 数据配置存储区域

> 注意：
>
> ShareFile 数据的存储区域适用于 Citrix Endpoint Management Enterprise Edition，而不适用于其他 Citrix Endpoint Management 版本。

创建存储区域时，您可以从 StorageZones Controller 向导或从 StorageZones Controller 控制台为 ShareFile Data 配置存储区域。使用 ShareFile 数据选项卡配置专用网络共享或支持的第三方存储系统的设置。

网络共享设置

选项	说明
存储库	选择“本地网络共享”。创建区域后，无法更改存储库选项。例如，要从本地网络共享切换到第三方存储，必须创建新区域。
网络共享位置	用于私有数据存储和数据（如加密密钥、排队文件和其他临时项目）的网络共享的 UNC 路径。在表单 `\\server\share` 中指定路径。属于同一存储区域的 StorageZones Controller 必须为存储使用相同的文件共享。注意：StorageZones Controller 将使用专有存储格式覆盖此路径中的任何数据。切勿指定具有文件数据的位置的路径。仅为 ShareFile Data 保留此存储区域的存储位置。StorageZones Controller 使用配置页面上提供的网络共享用户名/密码访问网络共享。如果配置页上没有提供网络共享用户名/密码，则默认情况下将使用网络服务帐户。网络服务帐户必须具有对此存储位置的完全访问权限。默认情况下，StorageZones Controller 还将使用网络服务帐户的 StorageCenterAppPool。请务必注意，唯一支持的配置是使用网络服务帐户。
网络共享用户名和网络共享密码	网络共享位置 UNC 路径的凭据。要使用指定用户帐户而不是网络服务帐户访问共享，请指定这些凭据。您可以继续使用网络服务帐户运行 IIS 应用程序池和 Citrix ShareFile 服务。
启用加密	仅当您想要加密存储在文件共享上的文件内容时，才选中此复选框。在企业环境中，网络共享位于您的网络内，并且已通过第三方工具进行保护，我们建议您不要对共享上的文件进行加密。此设置与元数据无关。标准区域的元数据不加密。尽管在需要时提供这种额外的安全性可作为最高安全性的选项，但加密共享上的文件将使第三方工具（如防病毒扫描程序和文件管理器工具（包括重复数据消除工具）无法读取磁盘。ShareFile 使用文件加密密钥来确认下载请求的有效性并加密存储。

选项	说明
密码	用于保护文件加密密钥的短语。确保将密码短语和加密密钥存档在安全位置。您必须为区域中的每个 StorageZones Controller 使用相同的密码短语。密码短语与您的帐户密码不同，如果丢失，则无法恢复。如果丢失密码，则无法重新安装存储区域、将其他 StorageZones Controller 加入到存储区域，或者在服务器出现故障时恢复存储区域。注意：加密密钥显示在共享存储路径的根目录中。丢失加密密钥文件 Sckeys.txt 会立即中断对所有存储区域文件的访问。请务必将加密密钥文件作为正常数据中心过程的一部分进行备份。

共享缓存配置设置

选项	说明
共享缓存位置	包含存储缓存和数据（如加密密钥、排队文件和其他临时项目）的网络共享路径。在表单 `\\server\share` 中指定路径。属于同一存储区域的 StorageZones Controller 必须为存储使用相同的文件共享。注意：StorageZones Controller 将使用专有存储格式覆盖此路径中的任何数据。切勿指定具有文件数据的位置的路径。将此存储位置保留为仅供 ShareFile 数据使用的存储区域。网络服务帐户（或 Citrix ShareFile 管理服务配置为运行的帐户）必须具有对此存储位置的完全访问权限。
共享高速缓存登录和共享高速缓存密码	共享缓存位置的 UNC 路径的凭据。
启用加密	选中此复选框可对存储在共享缓存中的文件进行加密。

Windows Azure 存储容器设置

选项	说明
存储库	选择 Azure 存储容器。创建区域后，无法更改存储库选项。例如，要从本地网络共享切换到基于 Azure 的存储，必须创建一个新的区域。

选项	说明
帐户名称	Azure 存储帐户的名称。这些名称始终是小写的。
访问密钥	Azure 存储的主访问密钥或辅助访问密钥。从 Windows Azure 管理门户的“管理访问密钥”屏幕复制密钥。
验证	单击按钮以验证 Azure 访问密钥。在验证完成并且“容器名称”菜单包括指定帐户的所有可用容器之前，您无法继续进行配置。
容器名称	选择要用于此存储区域中的所有 StorageZones Controller 的 Azure 容器。此列表为空，直到您的 Azure 访问密钥经过验证。

Amazon S3 存储桶设置

选项	说明
存储库	选择 Amazon S3 存储桶。创建区域后，无法更改存储库选项。例如，要从本地网络共享切换到 Amazon S3 存储，您必须创建一个新区域。
访问密钥 ID	您的 Amazon S3 存储的访问密钥 ID。
私有访问密钥	您的 Amazon S3 存储的私有访问密钥。
验证	单击该按钮以验证 Amazon S3 私有访问密钥。在验证完成后，您无法继续进行配置，并且“存储桶名称”菜单包含指定帐户的所有可用存储桶。
存储桶名称	选择要用于此存储区域中的所有 StorageZones Controller 的 Amazon S3 存储桶。此列表为空，直到您的 Amazon S3 私有访问密钥经过验证。

SMTP 设置

选项	说明
SMTP 服务器地址和 SMTP 端口号	您的本地 SMTP 服务器主机名和端口。
使用 SSL	选中通过安全连接连接连接到 SMTP 服务器的复选框。
用户名和密码	本地 SMTP 服务器的用户名和密码。

选项	说明
身份验证模式	默认身份验证模式使用最安全的方法从 StorageZones Controller 连接到 SMTP 服务器。
发件人地址	显示在“发件人”字段中的电子邮件地址。

Google Cloud 平台

从 **Google Cloud Platform >** 设置 **>** 互操作性生成访问密钥和密钥。

在运行存储区域配置之前，请将 **S3EndpointAddress** 注册表值设置为 `https://storage.googleapis.com`，然后重新启动 IIS。

选项 1

说明

存储库

选择 **Amazon S3** 存储桶。创建区域后，无法更改 存储库选项。例如，要从本地网络共享切换到 Amazon S3 存储，您必须创建一个新区域。

访问密钥 ID

来自 Google Cloud Platform 存储的访问密钥 ID。

私有访问密钥

从您的 Google Cloud Platform 存储的秘密.

验证

单击该按钮以验证 Google Cloud Platform 秘密访问密钥。在验证完成后，您无法继续进行配置，并且“存储桶名称”列表包含指定帐户的所有可用存储桶。

存储桶名称

选择要用于此存储区域中的所有 StorageZones Controller 的正确存储桶。此列表为空，直到您的 Google Cloud Platform 秘密访问密钥经过验证。

配置存储区域连接器

存储区域连接器允许用户访问 SharePoint 站点或指定网络文件共享上的文档。您不必启用 ShareFile 数据的存储区域即可使用存储区域连接器。

> 注意：
>
> ShareFile 数据的存储区域和存储区域连接器功能可以共享一个区域。但是，StorageZones Controller 保持

> 两种数据类型的数据和访问规则分开。

使用 StorageZones Controller 向导或从 StorageZones Controller 控制台创建区域时，可以配置存储区域连接器。

要控制对特定网络文件共享或 SharePoint 文档库的访问，请指定允许路径或拒绝路径的列表。保存更改后，重新启动 IIS 服务器。

首先根据允许的路径检查存储区域连接器的绑定连接。如果允许连接，则会根据被拒绝的路径检查路径。例如，要提供对其所有子文件夹的访问权限，请指定允许的路径 `\\myserver\teamshare`。`\\myserver\teamshare`

- 默认情况下允许所有连接，并由“允许的路径”值指示。该值对于被拒绝的路径无效。
- 如果允许的路径和拒绝的路径相互冲突，则强制执行最严格的路径。
- 条目以逗号分隔。
- 对于连接到网络文件共享的连接器，请指定允许的 UNC 路径。

  使用 FQDN 的示例：`\\fileserver.acme.com\shared`

  您可以在 UNC 路径中使用以下变量：

  - %UserName%

    重定向到用户的主目录。示例路径：`\\myserver\homedirs\\%UserName%`

  - %HomeDrive%

    重定向到“Active Directory”属性主目录中定义的用户的主文件夹路径。示例路径：`%HomeDrive%`

  - %TSHomeDrive%

    重定向到用户的终端服务主目录，如 Active Directory 属性 MS-TS-主目录中定义的。当用户从终端服务器或 Citrix XenApp 服务器登录到 Windows 时，将使用该位置。示例路径：%TSHomeDrive%

    在 Active Directory 用户和计算机管理单元中，编辑用户对象时，可以在远程桌面服务配置文件选项卡上访问 MS-TS-主目录值。

  - %UserDomain%

    重定向至经过身份验证的用户的 NetBIOS 域名。例如，如果经过身份验证的用户登录名是“abc\johnd”，则变量将替换为“abc”。示例路径：`\\myserver%UserDomain%_%UserName%`

  变量不区分大小写。

- 对于指向根级 SharePoint 站点的连接器，请指定根级路径。

  示例：`https://sharepoint.company.com`

- 对于连接到 SharePoint 站点集合的连接器：

  示例：`https://sharepoint.company.com/site/SiteCollection`

- 对于连接到 SharePoint 2010 文档库的连接器，请指定 URL（不包括路径终止符，如文件.aspx 或/窗体）。

  示例:

  - https://mycompany.com/sharepoint/
  - https://mycompany.com/sharepoint/sales-team/Shared Documents/
  - https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx

  默认的 SharePoint 2013 URL（启用最小下载策略时）的格式为：https://sharepoint.company.com/_layouts/15/start.aspx\##/Shared%20Documents/。

删除服务器标头的安全建议

IIS/ASP.NET 默认情况下公开 HTTP 响应中的服务器标头。此标题可能会对攻击者有用。标头会显示发送服务器类型，在某些情况下会显示版本号。此标头对于生产站点不是必需的，可以禁用。

遗憾的是，StorageZones Controller 安装程序无法自动删除此标头。但是，我们可以在我们的 StorageZones Controller 文档/安装指南中向客户提供删除此标题的建议。

请参阅以下文章，了解我们应该在我们的文档中提供的具体步骤：https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

验证您的 **StorageZones Controller** 设置

June 15, 2020

验证 StorageZones Controller 是否已注册 ShareFile，然后在继续之前检查其他配置问题。

1. 在 StorageZones Controller 控制台中，单击 监控选项卡。
2. 验证检测信号状态是否有绿色复选标记。

   红色图标表示 ShareFile.com 未接收检测信号消息。在这种情况下，请验证从 StorageZones Controller 到 www.ShareFile.com 的网络连接，并验证从外部 PC 到 StorageZones Controller 的 URL 的网络连接。对于标准区域，StorageZones Controller 必须能够在端口 443 上使用有效的可信公共 SSL 证书访问。

   升级后，从文件清理服务的 ShareFile 连接状态可能会暂时显示红色图标。如果 Windows 在 StorageZones Controller 建立网络连接之前启动该服务，则会发生这种情况。Controller 服务器返回网络后，状态将返回绿色图标。

3. 检查您的私有区域的连接性：导航到您的私有区域的外部 URL（以形式 https://server.subdomain.com）。

   如果允许互联网流量传入和传出 StorageZones Controller，您将看到 ShareFile 徽标。如果 StorageZones Controller 配置不正确，您可能会看到 IIS 徽标或 Citrix ADC 登录屏幕。确保允许通过端口 443 进行入站和出

站 HTTPS 流量。如果您的外部 URL 指向 Citrix ADC，请查找数据的内容交换和负载平衡虚拟服务器上的点击。有关详细信息，请参阅中的 “StorageZones Controller 不将数据上载到 ShareFile”安装和配置疑难解答。

4. 验证为私有数据存储创建的网络共享是否具有文件夹结构和由 StorageZones Controller 创建的几个文件，包括 sckeys.txt，这些文件必须位于共享存储的根文件夹中。

   Skeys.txt 是在安装 StorageZones Controller 时创建的，前提是没有凭据或访问权限问题。如果 sckeys.txt 不存在，请验证文件共享上的访问控制列表，然后重新安装 StorageZones Controller。

5. 从 ShareFile 界面检查存储区域连接器的状态：

   a) 登录到您的 ShareFile Enterprise 帐户，导航到管理 **>** 存储区域，并验证 “运行状况” 列包含绿色复选标记。

   b) 单击站点名称并验证检测信号消息是否指示 StorageZones Controller 正在响应。

6. 测试文件上载：登录 ShareFile Web 界面，创建分配给您刚刚配置的区域的共享文件夹，将文件上载到该文件夹，然后验证该文件是否显示在该文件夹中。

更改用户帐户的默认区域

June 15, 2020

默认情况下，现有和新置备的用户帐户使用 ShareFile 管理的云存储作为默认区域。更改默认区域，如下所示：

- 要为从 AD 置备的用户帐户指定默认区域，请打开用户管理工具，然后单击选项图标。
- 要为根级别文件夹选择区域，请打开 ShareFile 管理员控制台，然后转到管理用户。（需要超级用户组中的成员资格。）
- 要更改单个用户的默认区域，请打开 ShareFile 管理员控制台并转到管理用户。（需要超级用户组中的成员资格。）您还可以在 “管理用户” 页面上创建和管理区域权限。

指定存储区域的代理服务器

June 15, 2020

存储区域控制器控制台允许您为存储区域控制器指定代理服务器。还可以使用其他方法指定代理服务器。

主存储区域和辅助 StorageZones Controller 使用 HTTP 相互通信。如果所有 HTTP 流量都配置为通过不支持连接到内部服务器的出站代理服务器，则必须将主 StorageZones Controller 配置为绕过代理服务器，以便其能够相互通信，如以下步骤所述。

> 重要：
>
> 旁路列表设置仅为最新的 StorageZones Controller 版本显示。如果使用的是 StorageZones Controller 2.2

> 到 2.2.2，则必须为每个辅助服务器手动添加一个绕过列表，如中所述 网络配置。

1. 在 StorageZones Controller 控制台 (`http://localhost/configservice/login.aspx`) 中，单击 网络选项卡。
2. 选中“启用代理”复选框，然后输入代理服务器地址和端口。
3. 选择身份验证模式并指定为 ShareFile 代理访问指定的 Windows 帐户。
4. 如果站点代理所有出站 HTTP 流量，并且一个区域具有多个 StorageZones Controller，请配置绕过设置：
   - 如果所有 StorageZones Controller 流量都位于同一子网上，请选中 旁路代理... 复选框，以便控制器可以相互通信。
   - 如果 StorageZones Controller 位于不同的子网上，请在绕过地址中输入主 StorageZones Controller 主机名或 IP 地址。
5. 重新启动所有区域成员的 IIS 服务器。

配置域控制器以信任存储区域控制器进行委派

June 15, 2020

> 注意：
>
> 本节仅适用于存储区域连接器。

要支持网络共享或 SharePoint 站点上的 NTLM 或 Kerberos 身份验证，请配置域 Controller，如下所示。

1. 在存储区域域的域 Controller 上，单击 开始 **>** 管理工具 **> Active Directory** 用户和计算机。
2. 展开域，然后展开“计算机”文件夹。
3. 在右窗格中，右键单击 StorageZones Controller 名称，选择 属性，然后单击委 派选项卡。
4. 对于 Kerberos，选择“信任此计算机以仅委派给指定服务”。
5. 对于 NTLM：
   a) 选择“信任此计算机仅委派给指定的服务”和“使用任何身份验证协议”。单击确定。
   b) 单击添加按钮。在 添加服务对话框中，单击 用户或计算机，然后浏览到或键入网络共享或 SharePoint 服务器的主机名。单击确定。

      如果您有多个文件服务器或 SharePoint 服务器，请为每个服务器添加一个服务。
   c) 在“可用服务”列表中，选择使用的服务：CIFS（用于网络文件共享的连接器）和 HTTP（用于 SharePoint 的连接器）。单击确定。

为 **Web App** 预览、缩略图和仅查看共享配置 **StorageZones Controller**

June 15, 2020

本地文件预览由本地 Microsoft Office Web 应用程序 (OWA) 服务器呈现。预览存储在 Citrix 管理的存储区域中的文件时，将由 Citrix 托管的或 Microsoft 托管的 OWA 服务器呈现预览。

> 重要：
>
> 白名单要求：
>
> `*.sf-api.com` 必须可由 Office 联机服务器访问，以便进行预览和编辑才能在版本 5.0 或更高版本的存储区域上正常运行。

要求

本地文件预览支持的文件类型

- 文档、.docm、.docx、.dot、.dotm、.dotx、.odt
- .ods、.xl、.xlsb、.xlsx、.xlsx
- 点点点
- .pdf
- 图像文件（bmp，gif，jpg，jpeg，png，TIF，TIFF）

本地文件编辑支持的文件类型

- .docm、.docx、.odt
- .ods、.xlsb、.xlsm、.xlsx
- .odp、.ppsx、.pptx

支持的环境

- 标准区域
- 多租户区域
- Web 应用程序

白名单/网络注意事项

- OOS 服务器应该能够访问 `https://\*.sf-api.com`（或.eu）
- SZC 服务器应该能够达到 `https://\*.sf-api.com` 和 `https://\*.sharefile.com`（或.eu）
- SZC 服务器应该能够访问 OOS 服务器 `https://\<Customer OOS / OWA Endpoint\>/hosting/discovery`（例如，`https://oos.sharefileexample.com/hosting/discovery`）

要编辑本地文件，文件版本控制 必须在您的 ShareFile 帐户上启用。

在 ShareFile Web 应用程序高级首选项菜单中打开 Microsoft Office 在线编辑的设置不会影响编辑本地文件的能力。该特定切换不会控制您编辑本地文件的能力，但将应用于编辑存储在公有云中的任何文件。启用预备文件的编辑完全由 StorageZones Controller Admin 使用以下步骤进行控制。

Microsoft 服务器兼容性

- **Microsoft Server 2016**：同时支持编辑和预览文件功能。编辑也可以禁用。
- **Microsoft Server 2013**：仅支持预览文件的功能。

体系结构和网络示意图

1. 经过身份验证的用户请求在 ShareFile 中进行文件预览。
2. ShareFile 发出重定向到客户端设备与 Office Online Server FQDN
3. 客户端设备重定向到 Office Online Server FQDN。注意：HTTPS 连接，DNS 应具有内部服务器 IP 记录或负载均衡器 VIP 记录，并在客户端设备和端口 443 上的任何防火墙之间进行适用路由。
4. Office 在线服务器处理请求，使 API 调用 StorageZones Controller 服务器。注意：HTTPS 连接、DNS 应具有内部服务器 IP 记录或负载均衡器 VIP 记录，并在客户端设备和端口 443 上的任何防火墙之间进行适用路由。
5. StorageZones Controller 检查`https://\<DNSname\>/hosting/discovery` 是可访问的。仅当可到达时，SZC 将 API 响应发送回 Office 在线服务器。注意：StorageZones Controller 必须连接到 Office 联机服务器。两个内部托管服务器之间的 HTTPS 连接。
6. StorageZones Controller 将出站连接到 ShareFile API (sf-api.com)。注意：这是通过任何防火墙、代理或出站路由设备进行的强制出站连接。确保 StorageZones Controller 服务器可以通过 HTTPS/443 到上述记录的 IP 地址进行出站通信。
7. Office Online Server 将出站连接到 ShareFile API。注意：这是通过任何防火墙、代理或出站路由设备进行的强制出站连接。确保 Office Online Server 可以通过 HTTPS/443 到上述记录的 IP 地址进行出站通信。
8. 进行预览。

要让 StorageZones Controller 将文件字节流到 OOS，而不是调用 ShareFile 控制平面来下载内容：我们需要更新 StorageZones Controller 上的配置文件之一的密钥。

C:\inetpub\wwwroot\Citrix\StorageCenter\WopiServer\AppSettingsReleaseOnPrem.config 需要更新。

这个配置文件有一个密钥 下载文件，目前是 错误的。将密钥更改为 **true** 并重新启动 IIS。

这样做会更新配置。OOS 也不再调用 ShareFile 控制平面来下载文件内容。

使用此选项时，声明不会有从控制平面到 OOS 的入站流量是否正确?

如果使用上述选项，OOS 将不再与 ShareFile 控制平面建立出站连接。

但是，无论是否使用上述选项，ShareFile 控制平面仍然与 OOS 建立出站连接。

使用一种方法与另一种方法是否有优点或缺点?

在这种方法中，OOS 不直接下载文件内容。StorageZones Controller 下载并将文件字节流式传输到 OOS。因此，它将增加在 StorageZones Controller 服务器上的负载。

下载和流式处理文件字节是一项资源密集型任务。根据用户数量和预览和编辑操作的数量，StorageZones Controller 服务器上的负载增加。

启用本地预览和编辑

要支持浏览器内的文档和图像预览、缩略图、仅查看共享客户管理的存储区域中存储的数据以及本地文件编辑，请按照以下方式配置 StorageZones Controller：

1. 在 StorageZones Controller 控制台中，单击 **ShareFile** 数据选项卡。
2. 在“本 地网络共享配置”部分，启用“配 置 **Office Web** 应用程序预览”。
3. 输入您的微软 Office Web 应用程序 (OWA) 服务器的外部 URL。
    - 用户必须通过其 Microsoft Office MSDN 订阅下载和配置 OWA 服务器软件。
4. 选择 启用 **Office** 联机编辑（如果需要）
5. 验证 OWA URL 是否可从外部访问。
6. 验证您的 Office 联机服务器是否可以与通信 `*.sf-api.com`。
7. 在 StorageZones Controller 控制台中，单击 监控选项卡。
8. 验证 **OWA** 服务器连接是否有绿色复选标记。

> 注意：
>
> 需要 文件版本控制 为 ShareFile 帐户启用编辑本地文件。如果帐户禁用了“文件版本控制”，则本地编辑将不起作用。

重要：

配置时钟同步：

- 验证存储区域 Controller 上的时间是否与 time.windows .com 或其他 NTP 服务器同步。有关配置时钟同步的信息，请单击此处。

修改 **OWA URAL** 或禁用预览：

- 上述任一操作都要求为每个主 Controller 和辅助控制器重新启动 IIS 服务。

限制

- 移动应用不支持浏览器内编辑。
- 连接器不支持浏览器内预览。

VDR 帐户不支持 WOPI 预览。

有关如何为仅查看共享配置 Citrix ADC 的信息，请参阅 为 StorageZones Controller 配置 Citrix ADC。

对 **OWA** 和 **OOS** 问题进行故障排除

如果您在预览或编辑本地文件时遇到问题，以下步骤将有助于识别和纠正特定问题。

要对配置进行故障排除，请首先登录 OWA 或 OOS 计算机。

1. 验证 Office WebApps 或 OfficeOnline Windows 服务是否在 services.msc 中运行。
2. 在新浏览器中，打开 `http://localhost/hosting/discovery` 页面。如果此页面成功加载，则应返回 XML 响应。
3. 以管理员身份运行 PowerShell 并执行以下命令：

```
Get-OfficeWebAppsFarm
```

如果在响应中收到警告或错误消息，请检查配置设置是否存在任何错误或错误。

网络注意事项：

- OOS 服务器应该能够访问 **`https://*.sf-api.com`** （或**.eu**）
- SZC 服务器应该能够达到 **`https://*.sf-api.com`** 和 **`https://*.sharefile.com`** （或**.eu**）
- SZC 服务器应该能够访问 OOS 服务器 **`https://<CustomerOOS/OWAEndpoint\>/hosting/discovery`**。例如 `https://oos.sharefileexample.com/hosting/discovery`。

配置多租户存储区域

June 15, 2020

多租户存储区域是 ShareFile StorageZones Controller 功能，使 Citrix 服务提供程序 (CSP) 能够创建和管理由所有租户共享的单个存储区域。

如果您是由 ShareFile 预配的合作伙伴帐户的 CSP，则可以在您的域中托管一个支持无限数量租户的多租户标准存储区域。使用多租户区域可以：

- 为每个租户提供一个唯一的 ShareFile 帐户，并利用所有出色的 ShareFile 功能，例如自定义品牌、文件保留首选项和安全设置。
- 为所有租户维护单个存储库。
- 更快地加入新客户，并降低为每个客户帐户创建单独的存储区域的成本和管理复杂性。

创建合作伙伴帐户

您必须拥有合作伙伴帐户，才能注册多租户存储区域。

要创建合作伙伴帐户，您必须注册 CSP 计划，并向您的首选经销商订购一个库存 SKU，使您有权提供 ShareFile 作为服务。要应用于云解决方案提供商程序，请转到 https://www.citrix.com/partner-programs/service-provider.html。

如果您已经注册为 CSP，并且已为库存 SKU 的 CSP 订购了相应的 ShareFile，则已为您创建合作伙伴帐户。如果您无法找到此新的合作伙伴帐户，请联系 ShareFile Account Services acctsvcs@sharefile.com。

当您开始在 CSP ShareFile 产品下配置客户帐户时，我们建议您在合作伙伴帐户上创建一个通用服务帐户管理员用户。通过这种方式，管理员用户可以成为所有客户帐户的官方合作伙伴管理员。确保此服务帐户管理员用户已打开“管理租户”权限。因此，我们鼓励合作伙伴在填写 CSP 客户帐户请求表之前立即创建合作伙伴管理员（在步骤 4 中）。

安装和设置多租户存储区域

- 创建新的多租户存储区域并将其与您的合作伙伴帐户关联。有关详细信息，请参阅 安装 StorageZones Controller 并创建存储区域。
- 在多租户模式下安装 StorageZones Controller。请确保在上一步中提到的安装文章中运行以下指定的命令提示符。

```
msiexec /i StorageCenter\\_5.0.1.msi MULTITENANT=1
```

> 注意：
>
> 在前面的命令中，您可能需要更新版本号（示例中为 5.0.1）以匹配您尝试安装的 msi 号。

配置新的存储区域并将其与您的合作伙伴帐户关联

有关详细信息，请参阅中的步骤 10 安装 StorageZones Controller 并创建存储区域。

登录您想要注册新区域的合作伙伴帐户。

> 重要：
>
> 此帐户必须具有以下 ShareFile 权限：管理租户以及创建和管理区域。

您现在可以登录到您的合作伙伴帐户并查看新的多租户存储区域。单击“管理员设置”>“存储区域”>“合作伙伴管理”选项卡。

请求多租户区域的租户帐户

要请求租户帐户，请填写 CSP 客户帐户请求表。

请求租户帐户时，还必须指定合作伙伴管理员用户。此合作伙伴管理员必须是您的合作伙伴帐户上的管理员用户，并启用了“管理租户”权限。创建租户帐户后，该合作伙伴管理员用户将自动作为管理员用户在该帐户上置备，并能够登录和管理租户帐户。由于一个帐户上不能有两个用户具有相同的电子邮件地址，因此表单上指定的合作伙伴管理员电子邮件不能与同一表单上的客户管理员相同。

要确保最快的周转，请确保提供正确的组织 ID 和要用作租户帐户的存储区域的多租户区域名称。

Citrix 配置请求的帐户后，您将收到一封电子邮件。该电子邮件将包含有关租户子域的详细信息以及用于设置访问的激活链接。ShareFile 将向您和您客户的管理用户发送单独的电子邮件。

然后，您的客户可以开始使用 ShareFile。为租户帐户置备的任何新用户都将使用您指定的多租户区域作为用户文件的默认位置。

使用 **Office** 联机服务器预览 **Office** 文件和 **PDF**

支持的 Office 联机服务器环境支持此功能。点击此处查看设置信息。

连接器共享

多租户区域支持此功能。

管理租户

在合作伙伴帐户中，有一个租户管理控制板位于“管理 设置**”>“**高级首选项”下。此集中式控制板允许您查看与合作伙伴帐户关联的所有租户的状态。控制板包括每个租户的许可证消耗量、默认存储区域、存储消耗量和帐户状态（付费或试用）。

> 注意：
>
> 控制板仅适用于您的合作伙伴帐户中已启用“管理租户”用户权限的用户。

多租户限制

多租户存储区域不支持 ShareFile 信息权限管理功能 (IRM)。

故障排除

无法创建区域：禁止

注册存储区域后，如果收到以下错误：“无法创建区域：禁止”，请检查您的用户权限是否包含“管理租户”权限。

升级

June 15, 2020

> 警告
>
> 如果使用的是 StorageZones Controller 2.x，则必须首先升级到版本 3.0.1。要从 2.x 升级到 3.0.1，请联系对援助的支持。升级到版本 3.0.1 后，您可以升级到最新版本。

如果安装了此版本：	执行此操作：
StorageZone 连接器 1.0	无法升级存 StorageZone 域连接器 1.0；卸载存 StorageZone 域连接器 1.0 并安装最新的 StorageZones Controller
存储中心 1.0	将存储中心 1.0 升级到存储中心 1.1。然后，验证存储中心 1.1 的配置是否正确且工作正常，然后再继续。然后将存储中心 1.1 升级到存 StorageZones Controller 2.0 更新 1。然后将 StorageZones Controller 2.0 更新 1 升级到 StorageZones Controller 3.0.1。最后，升级到最新的 StorageZones Controller。
存储中心 1.1	将存储中心 1.1 升级到存 StorageZones Controller 2.0 更新 1。在继续之前，请验证存储中心 2.0 更新 1 的配置是否正确并正常工作。然后将 StorageZones Controller 2.0 更新 1 升级到 StorageZones Controller 3.0.1。最后，升级到最新的 StorageZones Controller。
StorageZones Controller 2.x	将存 StorageZones Controller 2.x 升级到存 StorageZones Controller 3.0.1，然后升级到最新的 StorageZones Controller。
StorageZones Controller 3 测试版计划	StorageZones Controller 3 是测试版程序软件，必须是存储区的新安装。否则，您可以升级到最新的 StorageZones Controller。
StorageZones Controller 3.x	升级到最新的 StorageZones Controller
StorageZones Controller 4.x	升级到最新的 StorageZones Controller

将 **StorageZones Controller 3.0.1** 或更高版本升级到最新版本

StorageZones Controller 3.0.1、3.x 和 4.x 可以直接升级，如以下步骤所述。

1. 要获取最新版本，请联系 对援助的支持。

   > 注意：
   >
   > 安装 StorageZones Controller 会将服务器上的默认网站更改为 Controller 的安装路径。

2. 在要升级主 StorageZones Controller 的服务器上：
   - 运行 StorageCenter.msi 以启动 ShareFile StorageZones Controller 安装向导。
   - 响应提示。安装完成后，向导将显示消息 “已完成 Citrix ShareFile StorageZones Controller 安装向导”。

- 单击完成。StorageZones Controller 控制台将打开。

> 重要：
>
> 如果您计划克隆 StorageZones Controller，请勿继续配置。捕获磁盘映像，然后配置每个 StorageZones Controller。

- 要随时返回到 StorageZones Controller 控制台，请从“开始”菜单打开`http://localhost/configservice/login.aspx` 或启动配置工具。单击 完成或返回到 StorageZones Controller 控制台后，“登录”页打开。
- 若要更改任何显示的信息，请单击“修改”，进行更改，然后单击“保存”。

3. 验证主 StorageZones Controller 上的注册表设置：

   并非所有的升级路径添加注册表设置必须增加每个区域的文件数。要启用该功能，请验证设置是否包含在注册表中。有关详细信息，请参阅 增加每个区域的文件数。

4. 在每个辅助 StorageZones Controller 上：
   - 运行 StorageCenter.msi 以启动 ShareFile StorageZones Controller 安装向导。
   - 响应提示，然后单击“完成”。StorageZones Controller 控制台登录页打开。
   - 登录。若要更改任何显示的信息，请单击“修改”，进行更改，然后单击“保存”。
5. 重新启动所有区域成员的 IIS 服务器。

将 **StorageZones Controller 2.x** 升级到 **StorageZones Controller 3.0.1**

这些步骤升级由先前版本的 StorageZones Controller 创建的标准区域。

1. 备份主 StorageZones Controller，如中所述 备份主 StorageZones Controller 配置。
2. 从中的 ShareFile 下载页面 http://www.citrix.com/downloads/sharefile.html，登录并下载最新的 StorageZones Controller 3 安装程序。

   > 注意：
   >
   > 安装 StorageZones Controller 会将服务器上的默认网站更改为 Controller 的安装路径。

3. 在要升级主 StorageZones Controller 的服务器上：
   - 运行 StorageCenter.msi 以启动 ShareFile StorageZones Controller 安装向导。
   - 响应提示。安装完成后，向导将显示消息“已完成 Citrix ShareFile StorageZones Controller 安装向导”。
   - 单击完成。将打开“StorageZones Controller”控制台。

> 重要：
>
> 如果计划克隆 StorageZones Controller，请不要继续配置。捕获磁盘映像，然后配置每个 StorageZones Controller。

- 要随时返回到 StorageZones Controller 控制台，请从“开始”菜单打开`http://localhost/configservice/login.aspx` 或启动配置工具。单击完成或返回到 StorageZones Controller 控制台后，将打开“登录”页。
- 若要更改任何显示的信息，请单击“修改”，进行更改，然后单击“保存”。

4. 验证主 StorageZones Controller 上的注册表设置：

   并非所有的升级路径都会添加增加每个区域的文件数所需的注册表设置。要启用该功能，请验证设置是否包含在注册表中。有关详细信息，请参阅 增加每个区域的文件数。

5. 在每个辅助 StorageZones Controller 上：
   - 运行 StorageCenter.msi 以启动 ShareFile StorageZones Controller 安装向导。
   - 响应提示，然后单击“完成”。此时将打开“StorageZones Controller”控制台“登录”页。
   - 登录。若要更改任何显示的信息，请单击“修改”，进行更改，然后单击“保存”。
6. 重新启动所有区域成员的 IIS 服务器。
7. 若要升级到 StorageZones Controller 3.4，请参阅本文前面的文章中的 **StorageZones Controller 3.1** 或 **3.0.1** 升级到 StorageZones Controller 3.4。

> 重要：
>
> 如果要从 2.2.3 之前的版本升级到 StorageZones Controller 3.0.1，并且以前自定义了“生产者计时器”或“删除计时器”设置，请与 ShareFile 支持联系，以获取有关配置“生产者计时器间隔”和“删除计时器间隔”设置的帮助。

管理 **StorageZones Controller**

June 15, 2020

安装主 StorageZones Controller 和任何辅助 StorageZones Controller 后，请使用以下过程来管理控制器并准备让其进行灾难恢复。

要打开 StorageZones Controller 控制台，请转到`http://localhost/configservice/login.aspx` 或从“开始”菜单启动配置工具。

管理 **StorageZones Controller**

- 将辅助存储区域控制器加入到存储区域

将辅助存储区域控制器加入到存储区域

June 15, 2020

要配置存储区域以实现高可用性，请至少将两个存储区域控制器连接到该存储区域。要做到这一点，您必须：

1. 安装主 StorageZones Controller 并创建区域（如中所述安装 StorageZones Controller 并创建存储区域）。
2. 在第二台服务器上安装 StorageZones Controller，并将该 Controller 加入到同一个区域。

属于同一区域的 **StorageZones Controller** 必须为存储使用相同的文件共享。

在高可用性部署中，辅助服务器是独立的、功能齐全的 StorageZones Controller。存储区域控制子系统随机选择 StorageZones Controller 来处理操作请求，包括上载、下载、复制和删除操作。

如果主服务器脱机，您可以轻松地将从属服务器升级为主服务器。您还可以将服务器从主服务器降级为辅助服务器。

1. 在服务器上打开 Web 浏览器作为辅助 StorageZones Controller。然后打 `http://localhost/configservice/login.aspx`开并登录。
2. 单击“加入现有区域”，然后选择存储区域。
3. 输入请求的信息，然后单击 注册。

   对于主区域 Controller，您只能输入主机名或 IP 地址，ShareFile 将填写完整的 URL。要测试 URL，请将其输入浏览器的地址字段。如果 URL 正确，则会显示一个 ShareFile 横幅页面。对于标准区域：如果 URL 不正确且您指定了 https，请验证您使用的是有效的受信任公共 SSL 证书。
4. 如果要为主 StorageZones Controller 使用代理服务器，请指定辅助 Controller 的代理服务器，如中所述指定存储区域的代理服务器。

5. 重新启动所有区域成员的 IIS 服务器。

   辅助 StorageZones Controller 在启动期间继承主 Controller 的配置。

更改主 **StorageZones Controller** 的地址或密码

June 15, 2020

为主 **StorageZones Controller** 指定不同的外部或本地地址

您可以使用此过程或其他服务器管理工具更改主 StorageZones Controller 的外部地址。

1. 在 ShareFile Web 界面中，单击 管理，然后单击 存储区域。
2. 单击区域名称，然后单击主 StorageZones Controller 主机名。
3. 指定新的 外部地址或 本地地址，然后单击 保存更改。
4. 重新启动所有区域成员的 IIS 服务器。

更改主 **StorageZones Controller** 的密码

1. 打开存储区域配置页面：`http://localhost/configservice/login.aspx`。
2. 单击 **Modify**（修改）。
3. 指定用于保护文件加密密钥的密码短语。确保将密码短语和加密密钥存档在安全位置。

   密码短语与您的帐户密码不同，如果丢失，则无法恢复。如果丢失密码，则无法重新安装存储区域、将其他 StorageZones Controller 加入到存储区域，或者在服务器出现故障时恢复存储区域。

   > 注意：
   >
   > 加密密钥显示在共享存储路径的根目录中。丢失加密密钥文件会立即中断对所有存储区域文件的访问。

4. 如果更改了主服务器上的密码短语：登录到每个其他成员的存储区域配置页面，并在出现提示时输入密码短语。

   您必须为区域中的每个 StorageZones Controller 使用相同的密码短语。

5. 重新启动所有区域成员的 IIS 服务器。

降级和提升 **StorageZones Controller**

June 15, 2020

在高可用性部署中，辅助服务器是独立的、功能齐全的 StorageZones Controller。要维护或替换主 StorageZones Controller，请先将其降级，然后提升辅助 Controller。如果主服务器脱机，则可以将从属服务器升级为主服务器。

> 小心：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

1. 要降级主 StorageZones Controller，请执行以下操作：
   a) 找到注册表项：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) 将“主配置服务器”设置为“假”。
   c) 使用表单`https://IPaddress` 或将主要配置服务器 URL 设置为将成为新的主 StorageZones Controller 的服务器的 URL`https://hostname/ConfigService/`。
   d) 重新启动所有区域成员的 IIS 服务器。
2. 要提升辅助 StorageZones Controller，请执行以下操作：
   a) 找到注册表项：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) 将主配置服务器设置为 true。
   c) 将主配置服务 URL 设置为 `http://localhost/ConfigService/`。
   d) 重新启动所有区域成员的 IIS 服务器。
3. 修改所有其他辅助 StorageZones Controller：
   a) 找到注册表项：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) 使用窗体`https://IPaddress` 或将主要配置服务器 URL 设置为将成为新的主 StorageZones Controller 的服务器的 URL`https://hostname/ConfigService/`。
   c) 重新启动所有区域成员的 IIS 服务器。

禁用、删除或重新部署 **StorageZones Controller**

June 15, 2020

禁用 **StorageZones Controller**

> 注意：
>
> 如果每个 StorageZones Controller 具有不同的外部地址，请使用此过程。如果对所有 StorageZones Controller 使用相同的外部地址，则从 Citrix ADC 接口禁用控制器。

在使服务器脱机进行维护之前，禁用 StorageZones Controller。

1. 在 ShareFile Web 界面中，单击 管理，然后单击 存储区域。
2. 单击区域名称，然后单击 StorageZones Controller 主机名。
3. 清除已启用的复选框，然后单击 保存更改。
4. 重新启动所有区域成员的 IIS 服务器。

删除 **StorageZones Controller**

删除 StorageZones Controller 不会删除数据或 sckeys.txt。如果要删除主 StorageZones Controller，请先将其降级，然后再继续操作。

1. 在 ShareFile Web 界面中，单击 管理，然后单击 存储区域。
2. 单击区域名称，然后单击 StorageZones Controller 主机名。
3. 单击删除。
4. 重新启动所有区域成员的 IIS 服务器。

重新部署 **StorageZones Controller**

重新部署 StorageZones Controller 时，不会丢失任何信息。

1. 从服务器卸载存储区域。
2. 在 ShareFile Web 界面中，单击 “管理**”>“**存储区域”，然后选择您的区域。不要删除区域。
3. 选择 StorageZones Controller 并将其删除。
4. 安装存储区域。不要注册它。
5. 运行 StorageZones Controller 配置向导，将 StorageZones Controller 加入到区域并完成注册。
6. 重新启动所有区域成员的 IIS 服务器。

将文件传输到新网络共享

June 15, 2020

在为专用数据存储设置新的网络共享之前：

要求

- 属于同一存储区域的 StorageZones Controller 必须为存储使用相同的文件共享。
- StorageZones Controller 使用 IIS 帐户池用户访问共享。默认情况下，应用程序池在具有低级别用户权限的网络服务用户帐户下运行。默认情况下，StorageZones Controller 使用网络服务帐户。
- 网络服务帐户必须具有对此存储位置的 完全访问权限。

1. 打开存储区域配置页面：`http://localhost/configservice/login.aspx`。
2. 单击 **Modify**（修改）。
3. 在“存储位置”中，在窗体中输入您的网络共享的 UNC 路径，`\\server\share` 然后单击“保存”。

   > 小心：
   >
   > StorageZones Controller 使用专有存储格式覆盖此路径中的任何数据。最佳做法是，切勿指定具有文件数据的位置的路径。将此存储位置保留为仅供 ShareFile 数据使用的存储区域。

4. 如果新网络共享位置 UNC 路径的凭据不同于前一个凭据，请指定存储登录和存储密码。
5. 重新启动所有区域成员的 IIS 服务器。
6. 登录到所有区域成员的配置页面。
7. 将整个目录结构（包括 Sckeys.txt）复制到新服务器。

备份主 StorageZones Controller 配置

June 15, 2020

StorageZones Controller 安装在您的本地站点上，您负责备份它。要完全保护您的部署，您应该拍摄 StorageZones Controller 服务器的快照，备份您的配置和准备用于文件恢复的 StorageZones Controller。

如本主题所述，备份配置至关重要。例如，如果您没有备份并且有人意外删除了某个区域，则无法恢复该区域中的文件夹和文件。

> 重要：
>
> 请确保在此过程中使用 PowerShell 4.0。有关 PowerShell 要求的详细信息，请参阅中的 PowerShell 脚本和命令 存储区域 Controller 系统要求。

StorageZones Controller 安装程序包括 PowerShell 模块，其中包含备份和还原主 StorageZones Controller 配置设置的命令。您的备份将包括区域的配置信息、ShareFile 数据的存储区域、SharePoint 的存储区域连接器和网络文件共享的存储区域连接器。

备份和还原命令要求您在与 StorageZones Controller 相同的用户上下文下运行 32 位版本的 PowerShell。要设置用户上下文，请使用工具 PSExec。该工具可从中下载 http://technet.microsoft.com/en-us/sysinternals/bb897553。

> 注意：
>
> 这些步骤不适用于辅助 StorageZones Controller。若要恢复辅助 StorageZones Controller，请在服务器上重新安装 StorageZones Controller，然后将服务器加入到主 StorageZones Controller 器。

1. 此过程中使用的 PowerShell 脚本是未签名的，因此您可能需要更改 PowerShell 执行策略。

a) 确定 PowerShell 执行策略是否允许您运行本地未签名脚本：PS C:\>Get-ExecutionPolicy

例如，“远程签名”、“无限制”或“绕过”策略允许您运行未签名的脚本。

b) 要更改 PowerShell 执行策略，请执行以下操作：PS C:\>Set-ExecutionPolicy RemoteSigned

2. 设置此 PowerShell 会话的用户上下文。在命令窗口中，运行以下命令之一。

- 如果使用默认网络服务帐户：

```
PsExec.exe -i -u ”NT AUTHORITY\NetworkService”C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell
```

- 如果为 StorageZones Controller 应用程序池使用命名用户：

```
PsExec.exe -i -u ”domain\username”C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell
```

此时将打开“PowerShell”窗口。

3. 在 PowerShell 提示符中，导入模块 ConfigBR.dll：Import-Module ”C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll”

每次打开新的 PowerShell 窗口时，都必须导入该模块。

4. 在 PowerShell 提示符下，运行以下命令：Get-SfConfig -PrimaryZoneController ”server”-Passphrase ”passphrase”-FilePath ”fullpath”

例如：

```
Get-SfConfig -PrimaryZoneController ”`https://myserver.domain.com/ConfigService/`” -Passphrase ”mypassphrase” -FilePath ”c:\szc-backup.bak”
```

命令参数：

参数	说明	示例
“服务器”	主 StorageZones Controller 服务器名称或 IP 地址。它可以采用示例下显示的任何以下形式，并且必须包含尾随斜杠。	连接到本地服务器：`http://localhost/ConfigService/`；连接到远程服务器：`http[s]://myservername.domain.com/ConfigService/`；如果 DNS 问题阻止连接到服务器名称，则连接到远程服务器：`http[s]://10.40.37.5/ConfigService/`
“密码短语”	为 StorageZones Controller 指定的密码。	“我的密码短语”
“完整路径”	保存备份文件的位置。	“c:\szc-备份.bak”

使用 Get-SF 配置命令创建备份文件。

要还原主 StorageZones Controller 配置，请参阅恢复主 StorageZones Controller 配置。

恢复主 **StorageZones Controller** 配置

June 15, 2020

当主 StorageZones Controller 被删除或变得不可用时，StorageZones Controller 为灾难恢复提供了以下选项：

- 如果辅助 StorageZones Controller 可用，请将辅助 Controller 提升为主控制器。
- 如果辅助 StorageZones Controller 不可用，并且您备份了主 StorageZones Controller 配置（如中所述备份主 StorageZones Controller 配置），请从备份文件。
- 如果您没有主 StorageZones Controller 配置的备份，并且所有 StorageZones Controller 都被意外删除或变得无法使用，则只能进行部分恢复。您可以为 ShareFile Data 恢复区域和存储区域配置，但不能恢复存储区域连接器。

> 重要：
>
> 请确保在此过程中使用 PowerShell 4.0。有关 PowerShell 要求的详细信息，请参阅中的 PowerShell 脚本和命令
> 存储区域 Controller 系统要求。

从备份文件恢复主 **StorageZones Controller**

> 注意：
>
> 这些步骤仅适用于主 StorageZones Controller。若要恢复辅助 StorageZones Controller，请在服务器上重新安装 StorageZones Controller，然后将服务器加入到主 StorageZones Controller。

1. 此过程中使用的 PowerShell 脚本是未签名的，因此您可能需要更改 PowerShell 执行策略。
   a) 确定 PowerShell 执行策略是否允许您运行本地未签名脚本：PS `C:\>Get-ExecutionPolicy`
   例如，“远程签名”、“无限制”或“绕过”策略允许您运行未签名的脚本。
   b) 要更改 PowerShell 执行策略，请执行以下操作：PS `C:\>Set-ExecutionPolicy RemoteSigned`
2. 设置此 PowerShell 会话的用户上下文。在命令窗口中，运行以下命令之一。

   > 注意：
   >
   > 从 http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx 下载 PsExec.exe 并按照该页面上的安装说明进行操作。

   - 如果使用默认网络服务帐户：

   ```
   PsExec.exe -i -u ”NT AUTHORITY\NetworkService” C:\Windows\
      SysWOW64\WindowsPowerShell\v1.0\powershell
   ```

   - 如果为 StorageZones Controller 应用程序池使用命名用户：

   ```
   PsExec.exe -i -u ”domain\username” C:\Windows\SysWOW64\
      WindowsPowerShell\v1.0\powershell
   ```

   此时将打开“PowerShell”窗口。
3. 从 PowerShell 提示符中，导入模块配置.dll：`Import-Module ”C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll”`
   每次打开新的 PowerShell 窗口时，都必须导入该模块。
4. 在 PowerShell 提示符下，运行以下 `Set-SfConfig` 命令：`Set-SfConfig -PrimaryZoneController ”server”-Passphrase ”passphrase”-FilePath ”fullpath”`
   其中，
   - 服务器是主 StorageZones Controller 服务器名称或 IP 地址。它可以采用以下任何形式，并且必须包含尾随斜杠。
     `http://localhost/ConfigService/`

servername/ 或 serverip/ （如果您使用 HTTP）

```
http[s]://servername.domain.com/ConfigService/
```

```
http[s]://serverip/ConfigService/
```

- 密码是为 StorageZones Controller 指定的密码。
- 完整路径是备份文件的位置和名称。例如 c:\szc-backup.bak。

恢复没有备份文件的主 **StorageZones Controller**

如果没有备份文件，则可以为 ShareFile Data 恢复区域和存储区域配置，但不能恢复存储区域连接器。

1. 设置此 PowerShell 会话的用户上下文。在命令窗口中，运行以下命令之一。
   - 如果使用默认网络服务帐户：

     ```
     PsExec.exe -i -u "NT AUTHORITY\NetworkService"C:\Windows\SysWOW64\
     WindowsPowerShell\v1.0\powershell
     ```

   - 如果将指定用户用于 StorageZones Controller 应用程序池：

     ```
     PsExec.exe -i -u "domain\username"C:\Windows\SysWOW64\WindowsPowerShell
     \v1.0\powershell
     ```

   此时将打开 “PowerShell” 窗口。
2. 从 PowerShell 提示符中，导入模块配置.dll：`Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

   每次打开新的 PowerShell 窗口时，都必须导入该模块。
3. 在 PowerShell 提示符下，运行连接到 SF 配置命令：

   > 重要：
   >
   > 连接 SF 配置命令当前不支持 Azure 或 Amazon S3 存储。如果需要使用此命令，请与 ShareFile 支持部门联系。

```
1 Join-SfConfig -ShareFileUserName "ShareFileUserName" -
    ShareFilePassword "ShareFilePassword" -subdomain "subdomain.
    sharefile.com" -ZoneId "ZoneId" -SCID "StorageCenterId" -
    Passphrase "passphrase" [-StorageZoneLocation "
    StorageZoneLocation"] [-StorageUsername "StorageUserName"] [-
    Storagepass "StoragePassword"] [-AzureAccountName "
    StorageAccount"] [-AzureSecretKey "PrimaryOrSecondaryAccessKey"
    ] [-AzureContainerName "Container"] [-S3AccessKey "S3AccessKey"
    ] [-S3SecretKey "S3SecretKey"] [-S3ContainerName "
```



```
S3ContainerName”] [-S3EndpointAddress ”S3EndpointAddress”] [-
S3ForcePathStyle]
```

其中，

- 可以通过以下方式获取区 ID：
  a) 在 ShareFile Web 界面中，单击 “管理”>“存储区域”，右键单击站点名称，然后选择 “属性”。
  显示的地址以区域 ID 结尾，如下所示：zae4fb8c-8520-478f-8f87-aa589a8fd181。
  b) 将该 ID 复制并粘贴到连接 SF 配置命令中。
- StorageCenterId 可以通过以下方式获得：
  a) 在 ShareFile Web 界面中，单击 “管理”>“存储区域”，单击站点名称，右键单击主机名，然后选择 “属性”。
  显示的地址以如下所示的存储 ID 结尾：scd344cf-8043-4ce2-974b-8f9cd83e2978。
  b) 将该 ID 复制并粘贴到连接 SF 配置命令中。
- 存储区域仅当为该区域启用了 ShareFile 数据的存储区域时才需要定位。
- 仅当为该区域启用了 ShareFile 数据的存储区域并且您的存储位置需要身份验证时，才需要存储用户名和存储密码。
- 仅当 ShareFile 数据的存储区域存储在 Windows Azure 存储容器中时，才需要使用 Azure 帐户名称、Azure 访问密钥和 Azure 容器名称。

4. 要恢复存储区域连接器，请使用 StorageZones Controller 控制台 (http://localhost/configservice/login.aspx) 启用和配置连接器。

替换主 StorageZones Controller

June 15, 2020

若要将主 StorageZones Controller 替换为位于不同位置（如不同域）的控制器，请使用备份和还原过程。以下步骤确保传输配置设置和所有数据。

1. 为现有 StorageZones Controller 配置创建备份文件。请参阅 备份主 StorageZones Controller 配置。
2. 在新的网络位置安装 StorageZones Controller，但不要配置。
3. 将备份的配置导入新 Controller。请参阅 恢复主 StorageZones Controller 配置。
4. 将数据复制到新的网络共享，登录到新 StorageZones Controller 的配置控制台，然后输入新的存储路径信息。请参阅 将文件传输到新网络共享。
5. 在新的 StorageZones Controller 配置控制台中，更新 Controller 的外部 URL。请参阅 更改主 StorageZones Controller 的地址或密码。

准备用于文件恢复的 **StorageZones Controller**

June 15, 2020

> 警告：
>
> ShareFile 恢复功能不会自动备份您的永久存储位置。您负责选择备份实用程序并每 1 至 7 天运行一次。

如何准备文件恢复取决于数据的存储位置：

- 受支持的第三方存储系统 — 如果您使用带有 StorageZones Controller 的第三方存储系统，则第三方存储是冗余的，不需要本地备份。但是，请注意，删除文件的 ShareFile 用户可以在短时间内从回收站恢复该文件。45 天后无法从 ShareFile 回收站恢复文件。恢复期后，文件将从区域中删除，因此从冗余的第三方存储中删除。如果恢复时间不够，请考虑以下解决方案之一：
  - 增加文件保留在 ShareFile 回收站中的时间量。要执行此操作，请更改 C:\inetpub\wwwroot\Citrix\StorageCenter\S 中的周期设置的值有关详细信息，请参阅自定义存储缓存操作。请记住，增加保留时间也会增加所需的第三方存储量。
  - 每七天创建一次本地备份 StorageZone 文件，并为备份确定适当的保留策略。
- 本地存储 — 如果将本地维护的共享用于私有数据存储，则负责备份本地 StorageZones Controller 本地文件存储和注册表项。ShareFile 存档 ShareFile 云中驻留的相应文件元数据 3 年。
  重要提示：为了防止数据丢失，您必须拍摄 StorageZones Controller 服务器的快照
  备份其配置，并备份本地文件存储。

如本主题所述，准备用于文件恢复的 StorageZones Controller 后，您可以使用 ShareFile 管理员控制台执行以下操作：

- 浏览特定日期和时间的 ShareFile Data 记录的存储区域，然后标记要还原的任何文件和文件夹。ShareFile 将标记的项目添加到恢复队列中。然后运行恢复脚本，将文件从备份还原到持久存储位置。

  有关详细信息，请参阅从您的 ShareFile 数据备份中恢复文件和文件夹。

- 当您无法从本地存储中恢复数据时，将存储在 ShareFile 云中的元数据与本地存储协调起来。ShareFile 协调功能从 ShareFile 云中永久删除指定日期和时间不再位于存储区域中的文件的元数据。

  有关详细信息，请参阅 将 ShareFile 云与存储区域协调

必备条件

- Windows Server 2012 R2 或 Windows Server 2008 R2
- Windows PowerShell（32 位和 64 位版本）必须支持.NET 4 运行时程序集。有关详细信息，请参阅中的“PowerShell 脚本和命令”存储区域 Controller 系统要求。
- PsExec.exe - PsExec 允许您使用网络服务帐户启动 PowerShell。您还可以使用 PsExec 计划恢复任务。从 http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx 下载 PsExec.exe 并按照该页面上的安装说明进行操作。

用于灾难恢复的文件摘要

以下文件位于 C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery 中，用于灾难恢复。

文件名	说明
DoRecovery.ps1	Windows 任务计划程序执行的 PowerShell 脚本来处理恢复过程。此文件存储文件备份和存储位置。
Recovery.psm1	处理恢复队列操作的 PowerShell 模块。
恢复。日志	存储恢复进程输出的日志文件。
恢复错误。日志	存储恢复过程中错误的日志文件。
利日森.dll	一个.NET 库，用于处理来自 JSON（JavaScript 对象表示法）字符串的转换。

设置备份文件夹

在备份服务器上，创建要备份持久存储文件夹的文件夹。

ShareFile Data 文件备份的存储区域应遵循与 StorageZones Controller 永久存储相同的布局。

如果备份位置不遵循与 StorageZones Controller 持久存储相同的布局，则必须在恢复过程中执行额外步骤，将文件从备份位置复制到您在恢复 PowerShell 脚本中指定的位置。

存储布局

备份布局

```
\\\PrimaryStorageIP
  \StorageLocation
   \persistentstorage
    \sf-us-1
     \a024f83e-b147-437e-9f28-e7d03634af42
      \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
       \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
        \fi47cd7e_64c4_47be_beb7_1207c93c1270

\\\BackupStorageIP
 \BackupLocation
  \persistentstorage
   \sf-us-1
    \a024f83e-b147-437e-9f28-e7d03634af42
     \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
```



```
16          \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
17           \fi47cd7e_64c4_47be_beb7_1207c93c1270
```

> 重要：
>
> ShareFile 恢复功能不会自动备份您的永久存储位置。您负责选择备份实用程序并每 **1** 至 **7** 天运行一次。

创建灾难恢复队列

此一次性设置是必需的。以下命令示例使用默认 StorageZones Controller 安装文件夹。

1. 在 StorageZones Controller 上，以管理员身份运行 PowerShell。
2. 此过程中使用的 PowerShell 脚本是未签名的，因此您可能需要更改 PowerShell 执行策略。
   a) 确定您的 PowerShell 执行策略是否允许您运行本地的未签名脚本：PS C:\ > 获取执行策略

   例如，“远程签名”、“无限制” 或 “绕过” 策略允许您运行未签名的脚本。

   b) 要更改您的 PowerShell 执行策略，请执行 PS C:\>Set-ExecutionPolicy RemoteSigned
3. 要验证 PowerShell 的版本是否正确，请键入：

   $PSE 版本表

   ClrVersion 的值必须为 4.0 或更高，才能使 PowerShell 能够在脚本中加载.NET 程序集。如果不是，请更改 Windows PowerShell 的 32 位版本和 64 位版本，如下所示：

   a) 以管理员身份运行记事本。

   b) 创建具有以下内容的文件。

```
1       <?xml version=”1.0”?>
2       <configuration>
3           <startup useLegacyV2RuntimeActivationPolicy=”true”>
4               <supportedRuntime version=”v4.0.30319”/>
5               <supportedRuntime version=”v2.0.50727”/>
6           </startup>
7       </configuration>
```

   c) 选择 “文件”>“另存为”，将文件命名为 powershell.exe.config，然后将其保存到以下位置：

   C:\Windows\System32\WindowsPowerShell\v1.0

   C:\Windows\SysWOW64\WindowsPowerShell\v1.0

   d) 关闭 PowerShell 窗口，以管理员身份打开一个新窗口，然后键入 $ psversion 表以验证 CLrVersion 是否正确。

4. 关闭 PowerShell 窗口并使用 PsExec.exe 启动 PowerShell，如下所示：

   a) 以管理员身份打开命令提示符窗口。

   b) 导航到 PsExec.exe 的位置并输入：

   PsExec.exe -i -u “NT AUTHORITY\NetworkService” C:\Windows\SysWOW64\WindowsPowerShell\v1.0\p

   c) 单击同意接受 PsExec.exe 许可协议。

5. 导航到 StorageZones Controller 安装文件夹中的灾难恢复工具文件夹：

   cd ‘C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery’

6. 导入 Recovery.psm1 模块：

   Import-Module .\Recovery.psm1

7. 要创建恢复队列，请输入：新建 SCQue-名称恢复-操作恢复

   该命令的输出包括所创建的队列的名称。例如：Queue 92736b5d-1cff-4760-92c8-d8b04dc92cb2 created

   要查看新文件夹，请打开文件浏览器并导航到：

   \\ 服务器\（您的主存储位置）\ 队列。您将看到“队列”文件夹，例如 92736b5d-1cff-4760-92c8-d8b04dc92cb2。

8. 为您的位置自定义恢复 PowerShell 脚本，如下一节所述。

为您的位置自定义恢复 **PowerShell** 脚本

任务计划程序执行 DoRecovery.ps1 PowerShell 脚本以处理恢复过程。此文件包括必须为站点指定的文件备份和存储位置。

1. 在 StorageZones Controller 上，导航到恢复 PowerShell 脚本：

   C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery\DoRecovery.ps1

2. 按如下方式编辑脚本：

   a. 将 $backupRoot 参数设置为指向备份位置的 UNC 路径。例如：$backupRoot = “\\10.10.10.11\(*Your*BackupLocation)

   b. 将 $storageRoot 参数设置为指向 StorageZones Controller 持久存储的 UNC 路径。例如：$storageRoot = “\\10.10.10.10\StorageLocation\persistentstorage”

测试恢复过程

1. 创建一个测试文件并将其上载到 ShareFile。
2. 一个小时左右后，验证该文件是否显示在持久存储中（在为 $backupRoot 指定的路径中）。
3. 从 ShareFile 中删除文件：在 ShareFile 管理员工具中，单击 回收站，选择该文件，然后单击 永久删除。

4. 从永久存储中删除文件。

   此步骤将重新创建 ShareFile 将在文件被删除 45 天后执行的操作。

5. 在 ShareFile 管理员工具中，转到 管理 **>** 存储区域，单击该区域，然后单击 恢复文件。

6. 在“恢复日期”文本框中单击，然后选择文件被删除之前和上载之后的日期和时间。

   此时将显示指定日期和时间存储区域的文件列表。

7. 选中该文件的复选框。

8. 选择要包含还原文件的文件夹，然后单击 还原。

   该文件将添加到备份队列中，并准备好恢复。成功恢复文件后，屏幕会更改以显示现在包含已恢复文件的文件夹。

9. 要恢复文件，请执行以下操作：

   a. 以管理员身份打开命令提示符窗口。

   b. 导航到 PsExec.exe 的位置，然后键入：

   ```
   ```
   PsExec.exe -i -u ”NT AUTHORITY\NetworkService” C:\Windows\SysWOW64
       \WindowsPowerShell\v1.0\powershell
   ```
   ```

   c. 在 PowerShell 窗口中，导航到：

   CD `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

   d. 运行恢复脚本：

   `.\DoRecovery.ps1`

   PowerShell 窗口将包含消息“已恢复项目”。文件将添加到永久存储位置。

10. 从 ShareFile 网站下载还原的文件。

相关的 **PowerShell** 命令

以下 PowerShell 命令支持灾难恢复。

- 恢复等待中的文件 **ID**

  获取恢复所需的文件 ID 列表。对于语法和参数，请使用以下命令：

  获取帮助获取恢复等待文件-已满

- **Set-RecoveryQueueItemsStatus**

为恢复队列中的所有项目或指定项目设置状态。这将覆盖队列中的现有恢复状态。对于语法和参数，请使用以下命令：

Get-Help Set-RecoveryQueueItemsStatus -full

创建和计划恢复任务的步骤

如果需要计划恢复任务，请执行以下步骤。

1. 启动 Windows 任务计划程序，然后在“操作”窗格中单击“创建任务”。
2. 在 常规选项卡上：

   a. 键入任务的有意义的名称。

   b. 在“安全选项”下，单击“更改用户或组”，然后指定要运行任务的用户（网络服务或对存储位置具有写入权限的指定用户）。

   c. 从“配置为”菜单中，选择要运行任务的服务器的操作系统。
3. 要创建触发器，请在“触发器”选项卡上单击“新建”。
4. 在“开始任务”中，选择“按计划”，然后指定计划。
5. 要创建操作，请在“操作”选项卡上单击“新建”。

   a. 对于“操作”，选择“启动程序”并指定程序的完整路径。例如：`C:\Windows\System32\cmd.exe`。

   b. 对于“添加参数”，键入：`/c "c:\windows\syswow64\WindowsPowerShell\v1.0\PowerShell.exe -File .\DoRecovery.ps1" >> .\recovery.log 2>>.\recoveryerror.log`

   c. 对于“开始”，请在 StorageZones Controller 安装位置中指定灾难恢复文件夹。例如：`c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

删除服务默认期间

从 StorageZone 控制器 4.0 开始，删除服务计时器将设置为 45 天。45 天的默认期限将覆盖以前的任何设置。要修改默认期间，请编辑 C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc 下的 FileDeleteService.exe.config。

```
<!--No. of days to keep data blob in active storage after deletion-->
<add key="Period"value="45"/>
```

修改升级后删除服务默认期间

在某些升级方案中，DeletePeriod 值将设置为空在“FileDeleteService.exe.config”。如果设置为空，则“删除期间”将默认为 45 天，从物理存储中删除已从 ShareFile 中删除的文件之前的默认天数。

要修改 StorageZones Controller 上的删除周期，请在以下位置编辑 FileDeleteService.exe.config 文件：`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

在对 StorageZones Controller 进行干净安装后，删除服务将每 8 小时运行一次，以清理临时文件和文件夹。要修改计时器，请在以下位置编辑文件删除。Exe.config 文件：`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

从您的 **ShareFile** 数据备份中恢复文件和文件夹

June 15, 2020

通过 ShareFile 管理员控制台，您可以浏览特定日期和时间的 ShareFile Data 记录的存储区域，并标记要还原的任何文件和文件夹。ShareFile 将标记的项目添加到恢复队列中。然后，您可以运行提供的脚本，将文件从备份还原到存储位置。

> 重要：
>
> 请确保在此过程中使用 PowerShell 4.0。有关 PowerShell 要求的详细信息，请参阅中的 PowerShell 脚本和命令
> 存储区域 Controller 系统要求。

必备条件

- 完成中介绍的设置和测试 准备用于文件恢复的 StorageZones Controller。安装程序包括创建文件夹以包含已恢复文件的说明。

1. 在 ShareFile Web 界面中，单击 管理，然后单击 存储区域。
2. 单击区域名称，然后单击 恢复文件。
3. 单击“恢复日期”文本框，然后选择日期和时间。

   此时将显示指定日期和时间存储区域的文件列表。
4. 选中要还原的每个文件的复选框，然后单击还原。
5. 选择要包含还原文件的文件夹，然后单击还原。

   文件夹列表显示一个旋转图标，指示恢复正在进行中。
6. 如果备份位置不遵循与存储区域永久性存储相同的布局，请将文件从备份位置复制到编辑 DoRecovery.ps1 时指定的位置。
7. DoRecovery.ps1 PowerShell 脚本是未签名的，因此您可能需要更改此过程的 PowerShell 执行策略。

a) 确定 PowerShell 执行策略是否允许您运行本地未签名脚本。在 PowerShell 窗口中：`Get-ExecutionPolicy`

例如，“远程签名”、“无限制”或“绕过”策略允许您运行未签名的脚本。

b) 要更改 PowerShell 执行策略，请执行以下操作：`Set-ExecutionPolicy RemoteSigned`

8. 设置此 PowerShell 会话的用户上下文。在命令窗口中，运行以下命令之一。

- 如果使用默认网络服务帐户：

```
PsExec.exe -i -u ”NT AUTHORITY\NetworkService” C:\Windows\
    SysWOW64\WindowsPowerShell\v1.0\powershell
```

- 如果为 StorageZones Controller 应用程序池使用命名用户：

```
PsExec.exe -i -u ”domain\username” C:\Windows\SysWOW64\
    WindowsPowerShell\v1.0\powershell
```

此时将打开“PowerShell”窗口。

9. 恢复文件：

a) 以管理员身份打开命令提示符窗口。

b) 导航到 PsExec.exe 的位置并输入：

```
PsExec.exe -i -u ”NT AUTHORITY\NetworkService” C:\Windows\
    SysWOW64\WindowsPowerShell\v1.0\powershell
```

c) 在 PowerShell 窗口中，导航到：

CD `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

d) 运行恢复脚本：

`.\DoRecovery.ps1`

PowerShell 窗口将包含消息“已恢复项目”。恢复的文件将从备份复制到持久存储位置。刷新控制台后，旋转图标会从 ShareFile Web 界面中消失成功恢复的文件。

如果从 ShareFile Web 应用程序中删除的文件尚未被 StorageZones Controller 删除服务删除，则该文件仍处于持久存储位置。在这种情况下，文件恢复是立即恢复的，并且在 ShareFile Web 界面中不会出现旋转图标。

如果无法恢复文件，请参阅灾难恢复文件夹中提供的帮助文件。

将 **ShareFile** 云与存储区域协调

June 15, 2020

导致本地存储中数据丢失的问题（如磁盘故障）会导致本地存储与存储在 ShareFile 云中的元数据之间的状态不一致。您可以自动协调这些差异，以便从 ShareFile 云中永久删除指定日期和时间不再在存储区域中的文件的元数据。

> 小心：
>
> 仅当本地文件存储中存在无法恢复的数据丢失时，才执行协调。协调会从 ShareFile 云中永久清除截至指定日期和时间未在本地文件存储中找到的任何文件的元数据。

1. 单击 管理，然后单击 存储区域。
2. 单击区域名称，然后单击 协调文件。
3. 单击“协调日期”文本框，然后选择日期和时间。
4. 单击 协调。此时将显示确认对话框。

配置上载文件的防病毒扫描

June 15, 2020

> 重要：
>
> 由于存储区域 4.2 中的应用程序代码更新，某些客户必须将工具运行的权限级别从本地管理员更新为系统网络服务。无法更新权限将导致防病毒扫描无法启动。

要求/摘要

- 使用 StorageZones Controller 4.2 或更高版本的用户
- SFAntivirus 必须作为使用 PsExec 的网络服务运行
- 更新日志文件位置

使用 **PsExec** 以网络服务的形式运行 **SFAntivirus**：

更新到 SZ 4.2 或更高版本的客户端，使用链接到 SFAntivirus 的现有计划任务，需要将工具运行的用户级别从本地管理员更改为系统网络服务。

若要获取网络服务权限，请使用 PSExec 在与 StorageZones Controller 相同的用户上下文下启动 PowerShell (x86)，并使用以下命令获取网络服务权限：

```
PsExec.exe -i -u ”NT AUTHORITY\\NetworkService”C:\\Windows\\SysWOW64\\
WindowsPowerShell\\v1.0\\powershell
```


更新日志文件位置

如果管理员正在登录到默认 SZC 日志目录之外的目录，则还必须通过修改 log4net.config 条目来更改日志文件位置：

```
\<file value=”..\\..\\SC\\logs\\avscantool-”/\>
```

StorageZones Controller 安装包括多个支持防病毒扫描的文件。这些文件默认安装在 C:\inetpub\wwwroot\Citrix\StorageCen 中

在您自定义配置文件并使用 Windows 任务计划程序安排扫描（如以下步骤所述）后，每个文件上载请求都会导致 StorageZones Controller 将文件排队进行防病毒扫描。如果报告了扫描文件的问题，“文件夹”视图将包含该文件的警告图标。如果用户尝试下载该文件，则会显示一条警告消息。

从 StorageZones Controller 4.0 起，可以配置防病毒日志文件位置。要修改日志位置，请编辑 C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus 下的 SFAntivirus.exe.config 文件

防病毒扫描不会删除该文件。

StorageZones Controller 4.2 或更高版本支持将已编码为 ICAP RFC 标准的防病毒扫描平台使用 ICAP 协议。有关配置 ICAP AV 的信息可以在本文中进一步找到。

必备条件

- 如果您将在 StorageZones Controller 上运行病毒扫描 (SFAntivirus.exe)，请确保在 Controller 上禁用加密：在存储区域控制台配置页上，验证是否清除了启用加密复选框。

> 注意：
>
> 在您的区域上配置防病毒软件后，会扫描任何新上载的项目。防病毒配置不可追溯。配置它不会扫描区域中已存在的文件和项目。

为您的位置准备配置

1. 若要在 StorageZones Controller 以外的服务器上运行病毒扫描，请执行以下操作：
   a) 将文件夹 C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus 复制到另一台服务器。
   b) 在 StorageZones Controller 上，打开 C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.conf 并将队列设置为 0：`<add key=”QueueSDKRestricted”value=”0”/>`
2. 在运行病毒扫描的服务器上，使用 StorageZones Controller 配置的值编辑 SFAntiVirus.exe.config：
   a) 对于命令文件：指定防病毒软件的完整路径。该软件必须与 ShareFile 防病毒文件夹位于同一台服务器上。
   b) 对于命令选项和返回代码：配置文件中提供的命令行设置为示例。为您的防病毒软件和环境提供适当的设置。
   c) 对于扫描文件超时：较大的文件可能需要更长的时间才能扫描。根据存储中预期的文件大小调整此设置。否则，这可能会增加大型文件未被扫描的风险。

3. 在命令行窗口中，运行以下命令来设置病毒扫描：`SFAntiVirus.exe -register SFusername SFpassword`

使用 **ICAP** 进行 **AV** 扫描，而不是命令行工具

StorageZones Controller 4.2 或更高版本支持将 ICAP 协议与已编码为 ICAP 的 RFC 标准的防病毒扫描平台一起使用。如果客户需要，仍可以使用 CLI 方法。自 SZ 5.0.1 或更高版本起，租户区域支持此功能。

要在 StorageZones Controller 上启用 ICAP AV 扫描仪，请导航到 StorageZones Controller 配置页面。

选中“启用防病毒集成”复选框，并在“**ICAP RESPMOD URL**”字段中输入防病毒服务器的地址。这是 ICAP 响应修改服务的 URL：`ICAP://SERVER/RESPMOD`。

单击 测试连通性以确认您的设置。

创建和计划病毒扫描任务的步骤

> 注意：
>
> 只有在使用命令行工具时，才需要为病毒扫描创建计划任务。使用 ICAP 时不需要这样做。

1. 启动 Windows 任务计划程序，然后在“操作”窗格中单击“创建任务”。
2. 在 常规选项卡上：
   a) 为任务提供有意义的名称。
   b) 在安全选项下，单击“更改用户或组”，然后指定要运行任务的 Windows 用户。用户必须对存储位置具有完全访问权限。
   c) 无论用户是否登录，选择运行。保持清除“不存储密码”复选框。
   d) 选择“以最高权限运行”。
   e) 从“配置为”菜单中，选择要运行任务的服务器的操作系统。
3. 创建触发器：在“触发 器”选项卡上，单击“新建”。然后，对于“开始任务”，选择“按计划”并指定计划。
4. 要创建操作：在“操作”选项卡上，单击“新建”。
   a) 对于“操作”，选择“启动程序”并指定程序的完整路径。例如：

      ```
      C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus\\SFAntiVirus.exe
      ```

   b) 对于“开始于”，请指定 SfantiVir.exe 的位置：`C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus`
5. 在“设置”选项卡上，对于“如果任务已在运行，则适用以下规则”，选择“不启动新实例”。

将 **AV** 命令行集成到扫描服务

必备条件

- 在安装或升级 StorageZones Controller 5.2 之前，请确保停止或删除现有命令行 AV，如果它作为计划任务或 cron 运行。
- 在主机上安装.NET 4.6.2（或更高版本）。

本地 StorageZones Controller 中的扫描服务包括对使用命令行 AV 工具（如赛门铁克命令行 AV 扫描）的支持。此外，扫描服务还使用支持 ICAP 的防病毒产品提供扫描。

若要启用此功能，请在防病毒/Onprem/AVscan 服务/AVscan 服务/应用程序设置中添加以下配置密钥和值。配置

```
<add key=”use-command-line-av”value=”true”/>
```

命令行工具特定配置

StorageZones Controller 5.2 的升级或新安装包括一个新的配置文件：

`AntiVirus/OnPrem/AVScanService/AVScanService/avCommandLineSettings.json`

此文件处理 AV 命令行的必要设置。

下面对配置键值进行了说明，其中包含了示例值。

- 将此点设置为您的命令行应用程序。

  ```
  ”command-file”: ”c:\\\\\vscan\\\\\scan.exe”
  ```

- 查看命令行应用程序的文档，了解它支持的选项或开关，然后将它们添加到此位置。

  ```
  ”command-options”: ”/ALL /ANALYZE /MIME /NOMEM /NORENAME /SECURE ”,
  ```

- 包括指示干净扫描的输出值。

  ```
  ”scanner-codes-for-clean-file”: ”0, 19”,
  ```

- 包括指示受感染文件的输出值。

  ```
  ”scanner-codes-for-infected-file”: ”12, 13”,
  ```

- 包括指示未扫描文件的输出值。

  ```
  ”scanner-codes-for-notscanned-file”: ”2, 6, 8, 15, 20, 21, 102”
  ```

关于强制执行最大文件大小（不包括扩展名）的注

在 5.2 版之前，您无法在命令行 AV 上强制执行扩展名排除或最大文件大小强制执行。您只能在 ICAP 扫描服务上执行此操作。对于 5.2 版本，应用于 ICAP 扫描服务的相同设置有关排除的扩展名和最大文件大小（以字节为单位）适用于 AV 命令行服务。

这些设置被命名为：


```
<add key="icap-exclude-extensions"value=""/>
```

```
<add key="icap-max-file-size-bytes"value="0"/>
```

StorageZones Controller 5.2 的新安装将这些设置重命名为以下内容。重命名的设置反映了这些设置既适用于基于 ICAP 的 AV，也适用于命令行 AV。

```
<add key="exclude-extensions"value=""/>
```

```
<add key="max-file-size-bytes"value="0"/>
```

升级时，不会重命名这些设置。虽然手动重命名可以起作用，但除了 ICAP 之外，AV 命令行也可以使用相同的设置。

```
<add key="icap-exclude-extensions"value=""/>
```

```
<add key="icap-max-file-size-bytes"value="0"/>
```

迁移 **ShareFile** 数据

June 15, 2020

有多种方法可以将 ShareFile 数据从一个本地区迁移到另一个本地区。

- 通过 Web 门户或用户管理工具进行迁移
- 通过 PowerShell 脚本进行迁移
- 通过区内修复工具迁移

必备条件

- 确保源区域可以从目标区域访问，并取消阻止到源存储中心的出站连接。
- 要测试区域之间的连接，请通过在目标区域的浏览器中导航到源区域的外部地址来访问源区域的外部地址。如果连接成功，则会显示 ShareFile 徽标。

通过 **Web** 门户或用户管理工具进行迁移

在 ShareFile Web 应用程序中，您可以为单个用户或特定用户启动区域之间的数据迁移。

> 重要：
>
> 保存以下更改会立即触发异步迁移操作，将现有文件上载到新区域。在此迁移期间上载到文件夹的新文件将进入新区域。

迁移特定用户的数据 -导航至“人员”，然后找到“员 工”用户。单击用户可查看其个人资料页面。在“存储位置”下，选择一个新的区域（如果已安装和配置了一个区域）。

迁移特定文件夹的数据 -导航到文件夹并访问文件夹名称右侧的“更多选项”菜单。单击“高级文件夹设置”。使用菜单选择一个新区域。

迁移过程

首先，排队等待迁移的文件会在原始区域的“存储位置”内的“队列”文件夹中创建占位符文件。

成功处理占位符文件后，迁移的文件将从原始区域中删除并添加 `persistentstorage` 到新区域中。`persistentstorage`

通过 **PowerShell** 进行迁移

ShareFile PowerShell SDK 允许用户从其原始区域位置下载大型文件夹结构，并将这些文件夹上载到新区域。

要求 -需要 PowerShell 4+ 和.NET 4.x+ 才能运行和安装软件开发工具包。可以下载 PowerShell 5 此处。

通过区域修复工具迁移

区域修复工具是一个命令行工具。该工具由存储区域开发人员编写，利用 ShareFile API 将目标文件夹 ID 迁移到特定区域。

为了获得最佳性能，建议对于大小小于 2 GB 的文件夹使用此方法。

使用 **StorageZones Controller** 配置启用 **FIPS 140-2** 模式

June 15, 2020

在为 ShareFile 应用以下配置之前，请验证是否在 Windows 服务器上启用了 FIPS 模式。对此，请执行以下操作：

1. 启动注册表编辑器（注册表编辑器）。
2. 浏览到路径：`HKEY_LOCAL_MACHINE\SOFTWARE\PowerShell\Server\16`
3. 检查注册表值 **UseFIPSCompliantAPI**。
4. 如果值数据 (DWORD) 为 **1**，则启用 FIPS 兼容模式。

如果 未启用 FIPS 兼容模式，请使用以下命令启用 FIPS 兼容模式：

1. 以 Windows 系统管理员身份登录到 Windows。
2. 单击 开始，单击 控制面板，然后单击 管理工具。

   > 注意：
   >
   > 您可能需要切换到大图标进行下一步。

3. 单击 本地安全策略。此时将显示“本地安全设置”窗口。
4. 在导航窗格中，单击 本地策略，然后单击 安全选项。
5. 在右侧窗格中，双击 系统加密：使用 **FIPS** 兼容算法进行加密、哈希和签名。

> 注意：
>
> 启用上述设置可能会影响计算机上的所有应用程序。

6. 在出现的对话框中，单击 启用、单击 应用，然后单 击确定。
7. 关闭“本 地安全设置”窗口。

有关详细信息，请参阅Microsoft 支持文章。

默认情况下，StorageZones Controller 可能会使用不符合 FIPS 140-2 标准的加密模块。安装 StorageZones Controller 后和运行 ConfigService 之前：客户必须添加以下代码示例才能在其 Controller 中打开 FIPS 140-2 合规性。

```
<appSettings>

<add key=”fipsOnly” value=”1” />

</appSettings>
```

将前面的代码示例添加为 <configuration> 元素的子代码添加到以下文件的末尾：

C:\Windows\Microsoft.NET\Framework\v4.0.x\Config\machine.config

接下来，重置 IIS 并重新启动所有 ShareFile 服务。或者，重新启动计算机。

> 注意：
>
> 不支持信息资源管理 (IRM)。

连接器收藏夹

June 15, 2020

从 StorageZones Controller 5.0 开始，用户可以将连接器文件夹作为收藏夹在 ShareFile WebApp 中的网络共享、**SharePoint** 和 **Documentum** 连接器下。有关详细信息，请参阅此 Citrix 支持知识中心 一文。

ShareFile 移动设备支持将连接器文件夹添加到收藏夹。另请注意，不支持在受限区域上创建连接器文件夹的收藏夹。

管理 **ShareFile** 数据的存储区域

June 15, 2020

您可以将存储区域用于 ShareFile 数据，也可以替代 ShareFile 管理的云。

在区域之间移动主文件夹和文件盒

使用以下步骤可将主文件夹和文件盒从 ShareFile 管理的云存储移动到专用区域或专用区域之间。或者，使用 ShareFile 用户管理工具在区域之间迁移用户。

1. 单击“主页”，然后导航到该文件夹。
2. 在右侧导航窗格中，单击 编辑文件夹选项。
3. 从存储区域菜单中，选择一个区域，然后单击 保存。
4. 重新启动所有区域成员的 IIS 服务器。

在存储区域中创建文件夹

1. 单击“主页”，然后单击“文件夹”。
2. 在 文件夹选项卡上，单击 添加文件夹。
3. 照常指定文件夹信息，对于存储站点，选择要存储此文件夹及其内容的存储区域。单击创建文件夹。
4. 像往常一样配置文件夹。创建文件夹时，可以选择是使用 ShareFile 管理的云存储还是使用本地存储区域。
5. 重新启动所有区域成员的 IIS 服务器。

重命名或删除存储区域

> 重要：
>
> 删除存储区域之前，请对其进行备份。删除区域会擦除该区域中的所有文件和文件夹，您无法撤消此操作。

1. 单击 管理，然后单击 存储区域。
2. 单击区域名称。
   - 重命名区域：单击 编辑区域，键入新名称，然后单击 保存更改。
   - 删除区域：单击区域名称，然后单击 删除区域。
3. 重新启动所有区域成员的 IIS 服务器。

自定义存储缓存操作

ShareFile 用户对文件上载、下载和删除的请求由 StorageZones Controller 处理，然后该控制器与连接的存储进行通信。例如，如果连接的存储是受支持的第三方存储系统，并且 ShareFile 用户上载文件，则 ShareFile 客户端将该文件发送到持久存储缓存。StorageZones Controller 然后将文件上载到第三方存储系统。

StorageZones Controller 使用中的可配置设置管理持久存储缓存`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`。本讨论中将介绍特定于受支持的第三方存储系统的设置。

对于上载的文件：

- StorageZones Controller 将上载的文件放置在持久存储缓存（永久存储文件夹）中。
- 以下设置控制删除服务操作的时间：

  - MinDeletionage 指定上次访问文件到可以删除文件之间的最短时间间隔。默认为 1 天。最少设置为 8 小时。
  - 离开时间日期开始和离开峰值时间日期结束指定文件删除的开始和停止时间。默认为上午 2 点和凌晨 4 点。
  - 生产者计时器间隔和删除计时器间隔控制删除服务操作的频率。如果默认值（1 天）不适合您的站点，请联系支持部门。
- 删除服务还管理包含临时项目（如加密密钥和排队文件）的文件夹。删除服务将在创建这些项目 24 小时后删除它们。
- 仅适用于受支持的第三方存储系统：
  - 删除服务确定存储缓存中的文件在受支持的第三方存储中是否具有相应的 Blob。
  - 默认情况下，删除服务每 10 秒（检查大小计时器）确定存储缓存是否超过 10 GB 的磁盘阈值（磁盘空间丢弃阈值 GB）。如果超过阈值，则删除服务将删除在过去一小时内未访问的文件 (CacheCleanupFileThreasholdPeriodUnExpected)。当删除服务由于正常计划（而不是因为磁盘大小达到阈值）运行时，如果 Blob 位于受支持的第三方存储中，则该服务将删除过去 24 小时内未访问过的文件（高速保存文件正常）。如果 Blob 不在第三方存储中，则该文件将保留在存储缓存中。

对于已下载的文件：

- 当 StorageZones Controller 收到下载请求时，它会从持久存储缓存中下载该文件（如果该文件存在）。如果文件不在该缓存中，则 Controller 将文件从第三方存储系统下载到持久存储缓存中。删除服务将删除过去 24 小时内未访问过的文件（高速缓存文件保存期正常）。

对于已删除的文件：

- 删除服务从 ShareFile 应用程序获取 45 天前（期间）删除的文件列表。
- 然后，删除服务将从存储位置删除相应的文件或从第三方存储中删除相应的对象。

删除服务默认期间

从 StorageZones Controller 4.0 开始，删除服务计时器设置为 45 天。45 天的默认期间将覆盖以前的任何设置。

1. 要修改默认期间，请编辑文件删除。例如 `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`
   - `<!--No. of days to keep data blob in active storage after deletion -->`
   - `<add key="Period"value="45"/>`

创建和管理 **StorageZone** 连接器

June 15, 2020

存储区域连接器提供对文档和文件夹的访问权限：

- SharePoint 网站、网站集和文档库

- 网络文件共享
- 文档连接器（需要 SZC 4.1 或更高版本）

有权查看已连接资源的用户可以从 SharePoint Web 界面和 SharePoint 客户端浏览连接的 ShareFile 站点、SharePoint 库和网络文件共享。

默认情况下，ShareFile Web 界面禁用连接器浏览。若要启用连接器浏览，请与 ShareFile 支持联系。

还有其他设置，允许用户指定要用于 Active Directory 查找的域 Controller。请参阅本文的身份验证部分。 此设置需要 SZ 4.1 或更高版本。

连接器系统要求

存储区域连接器不支持跨设备共享或文件夹同步。

连接器必须具有唯一的显示名称。用户被阻止使用当前在帐户上其他位置使用的连接器名称。

创建存储区域连接器的权限

要创建和管理连接器，您的管理员或员工用户 必须具有以下权限：

- 创建和管理连接器
- 创建根级别文件夹

为 **SharePoint** 创建存储区域连接器

必备条件

- 如果要为 ShareFile 数据使用存储区域，请创建要用于连接器的区域。

以下步骤介绍了如何从 ShareFile Web 界面创建存储区域连接器。ShareFile 用户还可以通过键入 SharePoint 站点的 URL 从受支持的设备创建连接器。

1. 以管理员身份使用 “创建和管理连接器” 权限登录到您的 ShareFile 帐户。
2. 导航到 “管理设置”**>**“连接器”。
3. 对于 SharePoint 连接器类型，单击 “添加”。
4. 如果要为 ShareFile 数据使用存储区域，请为连接器选择一个区域。

   连接器的区域必须与 SharePoint 服务器位于同一个域中，或者必须与该服务器具有信任关系。如果您在多个域中有 SharePoint 服务器，并且无法在域之间配置信任，请为每个域创建一个 StorageZones Controller。
5. 对于站点，请使用以下形式指定 SharePoint 根级别站点、网站集或文档库的 URL。
   - 到 SharePoint 根级站点的连接示例：`https://sharepoint.company.com`

     通过与根级站点的连接，用户可以访问根级别下的所有站点（但不能访问站点集合）和文档库。ShareFile 隐藏用户的 SharePoint 系统文件夹。

- 到 SharePoint 站点集合的示例连接：`https://sharepoint.company.com/site/SiteCollection`

  通过与站点集合的连接，用户可以访问该集合中的所有子站点。

- 连接到 SharePoint 2010 文档库的示例：
  - `https://mycompany.com/sharepoint/`
  - `https://mycompany.com/sharepoint/sales-team/Shared Documents/`
  - `https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx`

- 连接到 SharePoint 2013 文档库的示例：

  默认的 SharePoint 2013 URL（启用最小下载策略时）的格式为：`https://sharepoint.company.com/\\_layouts/15/start.aspx\##/Shared%20Documents/`。

- 重定向到经过身份验证的用户的 NetBIOS 名称的连接示例：

  使用变量%UserDomain% 将经过身份验证的用户的登录名替换为该用户的 NetBIOS 名称。新变量使您能够创建到 URL（如）的站点级连接器 `https://example.com/%UserDomain%\\_%UserName%/Documents`。

- 连接到“我的网站”或 OneDrive for Business 时的示例连接：

  使用变量%URLusername% 可在连接到 SharePoint 个人站点时自动解析选定的特殊字符。此变量用%20 替换空格，并用下划线替换句点。使用%URLusername% 变量需要 SZ v3.4.1。

  如果用户的“域\ 用户名”是“acme\ rip.van winkle”，则

  `https://sharepoint.acme.com/personal/%URLusername%`
  将被解析为：
  `https://sharepoint.acme.com/personal/rip van%20winkle`

6. 键入连接器的用户友好名称。

   该名称用于向用户标识 SharePoint 站点。名称应该很简短，所以它显示在具有小屏幕的移动设备上。

7. 单击“添加连接器”。此时将显示“查看/编辑文件夹访问”对话框。
8. 使连接器对其他人可见：在查看/编辑文件夹访问中，添加用户和通讯组，然后单击 保存更改。

   此步骤仅确定连接器是否对用户可见。存储区域连接器从 **SharePoint** 服务器继承访问权限。

启用 **SharePoint** 元数据标记

配置 StorageZones Controller 时，请确保已启用 SharePoint 连接器。

SharePoint 2013 和更高版本的移动客户端支持元数据标记。

> 注意：
>
> 仅限于美国。

为网络文件共享创建存储区域连接器

必备条件

- 如果要为 ShareFile 数据使用存储区域，请创建要用于连接器的区域。

以下步骤介绍了如何从 ShareFile Web 界面创建连接器。ShareFile 用户还可以通过键入文件共享的路径从受支持的设备创建连接器。

1. 以具有“创建和管理连接器”权限的管理员身份登录到您的 ShareFile 帐户。
2. 导航到“管理设置”>“连接器”。
3. 单击“网络共享”连接器类型的 添加。
4. 如果要为 ShareFile 数据使用存储区域，请为连接器选择一个区域。

   连接器的区域必须与文件共享位于同一域中，或者必须与它具有信任关系。如果您在多个域中有文件共享，并且无法在域之间配置信任，请为每个域创建一个 StorageZones Controller。
5. 对于“路径”，键入 UNC 路径。

   具有 FQDN 的示例：\\ 文件服务器.acme.com\ 共享

   您可以在 UNC 路径中使用以下变量：

   - %UserName%

     重定向到用户的主目录。示例路径：\\myserver\homedirs\%UserName%
   - %HomeDrive%

     重定向到“Active Directory”属性主目录中定义的用户的主文件夹路径。示例路径：%HomeDrive%
   - %TSHomeDrive%

     重定向到用户的终端服务主目录，如 Active Directory 属性 MS-TS-主目录中定义的。当用户从终端服务器或 Citrix XenApp 服务器登录到 Windows 时，将使用该位置。示例路径：%TSHomeDrive%

     在 Active Directory 用户和计算机管理单元中，编辑用户对象时，可以在远程桌面服务配置文件选项卡上访问 MS-TS-主目录值。
   - %UserDomain%

     重定向至经过身份验证的用户的 NetBIOS 域名。例如，如果经过身份验证的用户登录名是“abc\johnd”，则变量将替换为“abc”。示例路径：\\myserver\%UserDomain%_%UserName%

   变量不区分大小写。

重要提示：请勿创建指向 ShareFile 数据存储位置的连接器。根据用户权限，这样做可以使用户删除所有 ShareFile 数据。

6. 键入连接器的用户友好名称。

   该名称用于标识给用户的文件共享。名称应该很简短，所以它显示在具有小屏幕的移动设备上。

7. 单击“添加连接器”。此时将显示“查看/编辑文件夹访问”对话框。

8. 使连接器对其他人可见：在查看/编辑文件夹访问中，添加用户和通讯组，然后单击保存更改。

   此步骤仅确定连接器是否对用户可见。存储区域连接器从网络共享继承访问权限。读/写访问权限由网络共享的安全设置决定，并且也受 **ShareFile** 计划的影响。

为网络文件共享启用文件签入和签出

必备条件

必须配置 StorageZones Controller 版本 5.8 和网络文件共享连接器。

步骤

1. 登录到存储中心。此时将显示配置页面。
2. 单击配置页面上的 修改。
3. 选中复选 框启用网络文件共享的签入和签出。
4. 键入用户和网络共享所在的域的名称。
5. 键入服务帐户的用户名和密码。此服务帐户必须具有对网络共享位置中存在的所有文件和文件夹的读写访问权限。

为 **Documentum** 创建存储区域连接器

> 注意：
>
> Documentum 连接器设置仅支持基本身份验证。Documentum Content Server 区分大小写，因此在身份验证期间输入的用户名应与区分大小写的凭据匹配，除非 Documentum 内容服务器上禁用区分大小写。

必备条件

1. StorageZones Controller 4.1 或更高版本
2. 由 ShareFile 客户支持启用的 Documentum ECM 设置。
3. 必须在您的 Documentum 服务器上部署 Documentum 静止服务。单击此处获取有关 Documentum 休息服务的其他信息。
4. 如果使用 Citrix ADC，则需要进行某些配置更改。这些更改将在本文中进一步详细介绍。

ShareFile 客户支持启用此功能后，请导航到您的 StorageZones Controller 并找到存储区域连接器菜单。单击“启用对现有企业内容管理 (ECM) 数据源的访问”复选框。保存所做的更改。

接下来，登录 ShareFile Web 应用程序并导航到 “管理员设置”>“连接器”。

单击 Documentum 连接器类型旁边的添加按钮。

指定 EMC 服务器的路径并输入连接器的名称。继续。

接下来，授予用户对 Documentum 连接器的访问权限。

创建连接器后，您可以从 Web 和移动应用程序访问该连接器。

支持的操作

移动（iOS/Android/通用 Windows 平台）：

- 浏览
- 文件上载/下载
- 文件和文件夹创建/删除
- 脱机编辑

Web 应用程序

- 连接器创建
- 浏览
- 文件上载/下载
- 文件夹创建/删除

不支持

- 共享存储在 Documentum 连接器中的文件
- 路径白名单/黑名单

> 注意：
>
> Documentum Content Server 区分大小写，因此在身份验证期间输入的用户名应与区分大小写的凭据匹配，除非 Documentum 内容服务器上禁用区分大小写。

针对 **Documentum** 连接器的 **Citrix ADC** 配置

如果在您的环境中使用 Citrix ADC，请对您的 Citrix ADC 配置进行以下更改：

1. Append the following to the _SF_CIFS_SP policy under Content Switching > Policies:

   ```
   HTTP.REQ.URL.CONTAINS("/cifs/")|| HTTP.REQ.URL.CONTAINS("/sp/")|| HTTP.REQ.URL.CONTAINS("/documentum/")|| HTTP.REQ.URL.CONTAINS("/ProxyService/")
   ```


2. 将以下内容附加到 “内容切换”>“策略” 下的 _SF_SZ_CSPOL 策略：

```
HTTP.REQ.URL.CONTAINS(”/cifs/”).NOT && HTTP.REQ.URL.CONTAINS(”/sp/”)
.NOT && HTTP.REQ.URL.CONTAINS(”/ProxyService/”).NOT && HTTP.REQ.URL.
CONTAINS(”/documentum/”).NOT
```

更改连接器名称

连接器名称用于标识 SharePoint 站点或网络文件共享给用户。

1. 以管理员身份登录到您的 ShareFile 帐户，然后单击连接器选项卡。
2. 在 “标题” 列中，单击连接器名称。
3. 键入连接器的用户友好名称，然后单击 “保存”。

删除连接器

删除连接器不会从 SharePoint 或网络文件共享中删除数据。

1. 以管理员身份登录到您的 ShareFile 帐户，然后单击连接器选项卡。
2. 选中连接器的复选框，单击 删除，然后单 击确定。

连接器身份验证

管理员用户现在可以使用以下设置指定在对 CIFS 或 SP 身份验证执行 AD 查找时要使用哪个域 Controller。

```
<add key=”Domaincontrollers”value=”DC01,dc02.domain.com,123.456.789.1”/>
```

上面的 “Value=” 可以设置为单个 DC 或多个 DC，由主机名、FQDN 或 IP 地址标识。多个 DC 应用逗号或分号分隔。

如果指定了多个 DC，则将针对第一个 DC 执行查找。如果发生错误，则会使用第二个 DC，依此类举。

上述属性可以添加到，以`C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config` 便它将被所有 StorageZones Controller IIS 应用程序（包括 CIFS、SP 和 ProxyService）继承。

如果不存在新的应用程序设置，则自动选择 DC 的默认行为将继续。

从网络共享/**SharePoint** 连接器获取直接链接

用户现在可以从网络共享/SharePoint 连接器 “获取直接链接”，同时使用适用于 iOS 或 Android 的最新版本的 ShareFile。

如果管理员想要禁用此功能，他们可以通过添加：

```
<add key=”disable-direct-link”value=”1”/>
```

以上内容可以添加到 `C:\inetpub\wwwroot\Citrix\StorageCenter\sps\AppSettingsRelease.config`。

基本身份验证和本地化用户名

基本身份验证不支持非 ASCII 字符。如果使用本地化的用户名，建议用户使用 NTLM 和协商。

数据丢失防护

June 15, 2020

ShareFile 中的数据丢失防护 (DLP) 功能允许您根据文件中找到的内容限制访问和共享。

您可以使用支持 ICAP 的任何第三方 DLP 安全套件扫描上载到存储区域的文档，这是一种用于内联内容扫描的标准网络协议。然后，您可以根据 DLP 扫描的结果以及您希望控制访问的严格程度来调整共享和访问权限。

支持的 **DLP** 系统

StorageZones Controller 使用 ICAP 协议与第三方 DLP 解决方案进行交互。将 ShareFile 与现有 DLP 解决方案一起使用不需要更改现有策略或服务器。但是，如果您期望负载很大，您可能希望专门指定 ICAP 服务器来处理 ShareFile 数据。

常用的符合 ICAP 标准的 DLP 解决方案包括：

- 赛门铁克数据丢失防护
- McAfee DLP 防止
- Websense TRITON AP-DATA
- RSA 数据丢失防护

由于 ShareFile 使用现有的 DLP 安全套件，因此您可以为数据检查和安全警报维护单点策略管理。如果您已经使用上述解决方案之一扫描传出电子邮件附件或 Web 流量中的敏感数据，则可以将 ShareFile StorageZones Controller 指向同一服务器。对于这些现有的 DLP 系统，如果底层 DLP 系统本身支持 ICAPS，我们也支持安全的 ICAP (ICAPS)。

启用 **DLP**

若要为 ShareFile 和 StorageZones Controller 启用 DLP，请执行以下三个操作：

1. 在您的 ShareFile 帐户上启用 DLP 功能。
2. 在 StorageZones Controller 服务器上启用 DLP。
3. 为每个文件分类配置允许的操作。

以下各节将详细介绍这些操作。

在您的 **ShareFile** 帐户上启用 **DLP** 功能

要请求或确认您的 ShareFile 子域已为 DLP 启用，请向发送请求 Citrix 支持。

对于某些帐户，启用 DLP 可能还需要为 ShareFile 网站启用更新的用户体验。为 DLP 启用帐户后，您可以继续在 StorageZones Controller 服务器上启用 DLP。

在 **StorageZones Controller** 服务器上启用 **DLP**

使用以下步骤在 StorageZones Controller 部署上配置 DLP 设置：

1. 安装或升级到 StorageZones Controller 3.2 或更高版本。
2. 在 StorageZones Controller 控制台中http://*localhost*/configservice/login.aspx，单击 **ShareFile** 数据选项卡。如果区域存在，请单击“修改”。
3. 选中启用 **DLP** 集成复选框，然后在 **ICAP REQMOD URL** 字段中键入 DLP 服务器的 ICAP 地址。地址格式为：

```
icap://<\*name or IP address of your DLP server\*>:<\*port\*>/
    reqmod

OR

\*icaps://<name or IP address of your DLP server>:<port>/reqmod\*

The default ICAP port is 1344 (non-secure DLP) and the default
    ICAPS port is 11344 (secure DLP).

For example, if your DLP server is dlp-server.example.com, type
    the following into the ICAP REQMOD URL field:

icap://\*dlp-server.example.com\*:1344/reqmod

OR

\*icaps://dlp-server.example.com:11344/reqmod\*
```

4. 单击 保存或 注册。

启用 DLP 后，通过检查监视选项卡上的 **DLP ICAP** 服务器状态条目，确认 DLP 服务器是否可以访问。

根据 **DLP** 扫描结果控制访问

在帐户和 StorageZones Controller 上启用 DLP 后，上载到启用 DLP 的存储区域的每个文件的每个版本都将被扫描以查找敏感内容。扫描结果作为数据分类存储在 ShareFile 数据库中。

DLP 设置根据文件的 DLP 分类限制文件可用的正常权限和共享控制。共享文档时，用户仍然可以选择阻止匿名访问，即使 DLP 设置允许他们匿名共享文档。但是，如果用户尝试以违反 DLP 设置的方式共享文件，则 ShareFile 会阻止他们这样做。

数据分类如下：

- 已扫描：确定 — DLP 系统扫描并通过确定的文件。
- 已扫描：已拒绝 — DLP 系统扫描并发现包含敏感数据的文件。
- 未扫描 — 尚未扫描的文件。

“未扫描” 分类适用于存储在 Citrix 管理的存储区域或未启用 DLP 的其他存储区域中的所有文档。此分类还适用于在配置 DLP 之前上载的已启用 DLP 的存储区域中的文件。此分类也适用于因外部 DLP 系统不可用或响应速度慢而等待扫描的文件。

每个项目的分类由 ICAP 服务器响应规则确定。如果 DLP ICAP 服务器响应时显示应阻止或删除内容的消息，则该文件将被标记为已 扫描：已拒绝。否则，文件将标记为已 扫描：确定。

对于每个数据分类，您可以设置不同的访问和共享限制。对于三个类别中的每个类别，ShareFile 管理员选择允许哪些操作：

- 员工可以下载或共享文件。
- 第三方客户端用户可以下载或共享文件。默认情况下，客户端共享处于禁用状态，但可以在管理 **>** 高级首选项 **>** 允许客户端共享文件下启用。
- 匿名用户可以下载文件

当用户共享文件时，只有具有下载权限的用户才能接收该文件。因此，当您为数据分类启用共享权限时，还必须至少授予一类用户下载权限。

在 **ShareFile** 中配置 **DLP** 设置

1. 在 ShareFile Web 界面中，单击 管理 **>** 数据丢失防护。
2. 将 “根据文件 内容限制对文件的访问” 选项更改为 “是**”**。
3. 为每个数据分类配置允许的操作。

> 重要：
>
> SShareFile On-Demand Sync 工具需要下载权限才能正常操作。如果您的部署包括 ShareFile On-Demand Sync，则为所有内容分类启用员工下载。

当 StorageZones Controller 向 DLP 系统发送文件时，它包含指示文件所有者的元数据。该文件还包括文件驻留在 ShareFile 中的文件夹路径。此信息允许 DLP 服务器管理员查看特定于 ShareFile 的有关包含敏感内容的文件的详细信息。

DLP 的高级设置

要调整 DLP 扫描过程，请编辑 StorageZones Controller 上找到的设置文件`wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`。下表介绍了与 DLP 相关的每个设置。

设置	说明	默认值
扫描间隔	DLP 服务检查 DLP 队列中的新文件并将其发送到 DLP ICAP 服务器进行处理的频率。	30 秒
icap-response-timeout	在将 ICAP 服务器标记为不可用之前，StorageZones Controller 等待 ICAP 响应的时间。	30 秒
icap-exclude-extensions	要从 DLP 扫描中排除的扩展名的逗号分隔列表。DLP 服务器不处理名称以其中一个扩展名结尾的文件，但将文件标记为 “已扫描: 确定”。示例值：“exe,jpg,bin,mov”	无
icap-max-file-size-bytes	要发送到 DLP 服务器进行处理的文件的最大大小（以字节为单位）。值为 0 表示没有最大值，并且发送所有文件大小。使用非零值配置时，DLP 服务器不会处理大于配置大小的文件，但标记为已扫描: 确定。	31457280 (30 MB)
x 队列项目到流程	每次扫描间隔迭代要扫描的排队项目的最大数量。减小此值可减轻将大量文件添加到 StorageZone 域时对 DLP 服务器的影响。	512
最大队列处理线程	用于耗尽 DLP 扫描队列的最大并发处理器线程数。根据允许到您的 ICAP 服务器的最大同时连接数设置此值。为了避免阻止使用同一 ICAP 服务器的其他网络服务，应该在合理的限制范围内。	4
Icap-reqmod-http-request-verb	默认情况下，使用 PUT 动词进行网络调用。如果需要，您可以将此设置更改为开机自检。	PUT

DLPExistingFiles 工具

ShareFile StorageZones Controller 提供了通过 ICAP 将存储中心与数据丢失防护 (DLP) 提供程序集成的选项。

但是，ICAP 服务只能通过新创建的文件填充的队列工作。这意味着服务不会扫描启用 ICAP 之前区域中存在的文件。此

工具可帮助对这些文件进行排队以进行扫描，还可以对扫描的文件进行排队以进行重新扫描。

正如名称所述，该工具当前仅适用于 DLP ICAP 服务。

要求

该工具是一个 PowerShell 脚本，因此需要 PowerShell 才能运行。PsExec 或类似的工具，因为脚本需要作为网络服务运行才能访问网络共享位置。

位置

对于已安装的 StorageZones Controller，该工具可以在中找到<storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1。默认情况下，StorageZones Controller 安装位置C:\inetpub\wwwroot\Citrix\StorageCenter。

运行工具之前的注意事项

该工具可能需要为单个操作运行多次，具体取决于以下情况。

- 为队列大小限制提供的限制。
- 给定条件的项目数。除非将队列大小限制设置为零或更小，否则此考虑为真。在这种情况下，该工具假定队列目录中最大大小为 200,000 个项目。

例如，如果使用该工具将未扫描的项目排队，则队列大小限制设置为 500 个项目。如果有超过 500 个未扫描的项目，工具会在队列中填满 500 个项目后停止。为了跟踪停止的位置，该工具会存储最后一次检索项的创建日期。该工具将日期存储在 <storage zones controller installation location>\SC 的临时文件中，名称为 DLPExistingFiles-enddate.temp。

在每次运行之前，该工具都会查找此文件。如果文件存在，则该工具将使用其中的创建日期作为下一批文件的标记。完成某个操作时，该工具不会删除临时文件。相反，在完成特定操作的所有批处理后，区域管理员可以删除该文件。由于这种情况，当完成完整操作时，临时文件（如果存在）应手动删除，然后再执行其他不同的操作。

使用 **PsExec** 运行该工具

打开命令窗口并使用以下命令运行 PsExec。

```
1 PsExec.exe -i -u ”nt authority\network service”
2
3 ”C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe”
```

这将打开作为网络服务运行的 PowerShell。要验证它确实作为网络服务运行，请运行 **whoami** 并检查结果。

PowerShell 打开后，直接在那里运行该工具以执行任何必要的任务。


```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 <options>
```

命令行选项

以下选项可用于运行该工具：

- **-runscan**（必需）：此选项用于指定要排队进行扫描的文件类型。子选项：
  - 未扫描：未扫描的文件。例如，未扫描的 DLP 之前的时代文件。
  - 扫描：已标记为“干净”的扫描文件。
  - 扫描已注射：已标记为未清除的扫描文件。
  - 已扫描：所有扫描的文件。
- **-queueLit**（可选）：此选项用于指定在工具停止之前队列中允许的项目数。
- **-date**（可选）：要排队等待扫描的项目的最大创建日期。例如，如果日期被指定为“10/30/2017 年 11:30 AM”，则只有那些在此日期/时间之前创建的文件才会排队进行扫描。

示例：

对于所有示例，请通过 PsExec 打开 PowerShell 作为网络服务。有关说明，请参阅本文前面的步骤。

要将区域中未扫描的项目排队，请运行以下命令。

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Unscanned
```

要将队列限制为 100 的区域内的所有扫描项目排队，请运行以下命令。

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan Scanned -queueLimit 100
```

要对 2017 年 10 月 30 日上午 11:30 之前创建的具有以下特征的所有扫描项进行排队，请执行以下操作：在队列限制为 200 的区域中标记为“干净”时，运行以下命令。

```
<storage zones controller installation location>\Tools\DLPExistingFiles
    \DLPExistingFiles.ps1 -runscan ScannedOK -queueLimit 200 -date ”
    10/30/2017 11:30 AM”
```


监视

June 15, 2020

StorageZones Controller 和 ShareFile 管理员界面包括几个资源，以帮助您监视 StorageZones Controller 活动并解决问题：

- 常规组件状态 — StorageZones Controller 控制台上的“监控”选项卡提供组件状态，以帮助您启动故障排除过程。为访问权限、服务状态和检测信号状态等项提供状态，这表示 StorageZones Controller 与 ShareFile 控制平面的出站连接。

  StorageZones Controller 每 5 分钟向 ShareFile Web 应用程序发送一次更新。如果 ShareFile Web 应用程序未在 10 分钟内收到更新，它将 StorageZones Controller 标记为脱机。

  对于“监视”选项卡上显示为红色的项，请查看日志文件以获取详细信息。

  “监视”选项卡不指示存储区域在连接方面是否正常工作。这包括 ShareFile 控制平面是否可以访问外部存储区域 URL 或客户端是否能够访问该区域。

- **StorageZones Controller** 服务器信息 — 有关服务器的存储使用情况、网络使用情况和文件活动的信息：从 ShareFile 界面登录到您的 ShareFile Enterprise 帐户，转到管理 **>** 存储区域，单击“存储区域”，然后单击 StorageZones Controller 主机名。
- 区域信息 — 有关区域的存储使用情况、网络使用情况和文件活动的信息：从 ShareFile 界面登录到您的 ShareFile Enterprise 帐户，转到管理 **>** 存储，然后单击区域名称。
- **StorageZones Controller** 运行状况 - 要确定 ShareFile.com 是否从加入到该区域的 StorageZones Controller 接收检测信号消息，请查看运行状况状态：从 ShareFile 界面，登录到您的 ShareFile Enterprise 帐户，转到管理 **> StorageZone**，验证运行状况列具有绿色复选标记，然后单击站点名称以验证检测信号消息是否指示 StorageZones Controller 正在响应。
- 日志文件 — 日志文件提供有关 StorageZones Controller 配置及其组件的详细信息，如下一节所述。

日志文件

默认情况下，StorageZones Controller 的以下日志文件位于中`C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs`：

日志文件名	包含以下内容的日志记录信息：
cfgsrv-%date%.txt	StorageZones Controller 配置操作，包括修改现有存储区域配置、创建新存储区域以及将新 StorageZones Controller 加入现有主 StorageZones Controller
sc-%date%.txt	标准区域的 ShareFile 数据上载和下载活动

日志文件名	包含以下内容的日志记录信息：
CIFS-%date%.txt	用于网络文件共享上载和下载活动的存储区连接器
sharepoint-%date%.txt	用于 SharePoint 上载和下载活动的存储区连接器
cloudstorageuploader-%date%.txt	云存储上载服务（至受支持的第三方存储系统）
copy-%date%.txt	ShareFile 复制服务
delete–%date%.txt	ShareFile 清理服务，用于持久存储缓存
s3uploader–%date%.txt	ShareFile 管理服务。包括检测信号状态消息

扩展日志记录可用于以下每个组件，并且在需要提供详细信息以支持时非常有用。

组件	应用程序的位置设置发布。配置
ShareFile 数据	C:\inetpub\wwwroot\Citrix\StorageCenter
网络文件共享的存储区域连接器	C:\inetpub\wwwroot\Citrix\StorageCenter\cifs
用于 SharePoint 的存储区域连接器	C:\inetpub\wwwroot\Citrix\StorageCenter\sp

启用扩展日志记录

以下步骤为所有 StorageZones Controller 组件和服务启用扩展日志记录：

1. 在 StorageZones Controller 服务器上，打开 IIS。
2. 导航到默认网站，然后打开应用程序设置。
3. 将启用扩展日志记录的值从 0 更改为 1。
4. 重新启动 Citrix ShareFile 管理服务。
5. 解决此问题后，我们建议您清除扩展日志记录以减少日志记录量。

要启用特定组件的扩展日志记录，请编辑其应用程序设置释放.config 文件：将值 <add key=”enable-extended-logging”value=”0”/> 从 0 更改为 1。

您还可以检查 IIS 日志以确定流量是否到达 StorageZones Controller。IIS 日志显示所有传入的请求。StorageZones Controller 的 IIS 日志在 c:\inetpub\logs\LogFiles\W3SVC1. 中

要启用扩展 IIS 日志记录，请参阅 http://support.microsoft.com/kb/313437。

安装和配置疑难解答

问题	说明和解决办法
StorageZones Controller 配置期间出现“HTTP 错误 404-找不到文件或目录”	该消息通常是由 IIS 或的问题导致的 ASP.NET。确保在 Windows 安装上启用了 IIS 角色，并且在 IIS 上启用了该 ASP.NET 功能。
在 StorageZones Controller 上浏览本地主机时出现“HTTP 错误 404.2-未找到”	该消息指示的 ISAPI 和 CGI 限制未 ASP.NET 设置为“允许”。
尝试上载后出现“HTTP 错误 413-请求实体太大”	在尝试向存储区域上传失败后，该消息可能会显示在网络跟踪上，并且可能来自 IIS 中的客户端证书设置。若要变通解决此问题，请在 StorageZones Controller 服务器上打开 IIS。导航到默认网站，然后打开 SSL 设置。对于客户端证书，选择忽略。重新启动 Citrix ShareFile 管理服务。
StorageZones Controller 配置过程中发生 IIS 错误	IIS 错误通常表示 ASP.NET 未完全配置。在 IIS 管理器的 ISAPI 和 CGI 限制下验证所有 ASP.NET 商品的“限制”设置为“允许”。验证 ASP.NET 是否在 IIS 中注册：在 IIS 管理器中的应用程序池下，验证是否存在 ASP.NET 列表。要手动注册 ASP.NET，请参阅此表后面的命令行。如果您仍然遇到问题，请查看您的 IIS 和 ASP.NET 设置。
StorageZones Controller 配置期间出现“保存存储中心绑定失败”	该消息指示 IIS 帐户池用户上存在权限问题。默认情况下，应用程序池在网络服务用户帐户下运行。StorageZones Controller 默认使用网络服务帐户。如果您使用指定用户帐户而不是网络服务帐户，则指定用户帐户必须具有对用于专用数据存储的网络共享的完全访问权限。
在区域配置过程中出现“拒绝访问”	如果您登录的 ShareFile 帐户没有创建和管理区域的权限，则会出现此消息。使用 ShareFile 管理员控制台设置该权限。
出站请求被阻止	当出站请求被阻止时，cfgsrv 日志包括 System.net.webException：远程服务器返回错误：(403) 禁止。此问题可能是由于代理服务器阻止出站请求造成的。验证您的防火墙是否满足 StorageZones Controller 系统要求中指定的要求

问题	说明和解决办法
登录到 StorageZones Controller 时出现“无法连接到远程服务器”	该消息通常表示代理问题。请确保您的代理设置已配置。如果代理设置正确，请确认您可以从 StorageZones Controller 登录到 ShareFile 帐户。验证您是否具有管理员级别的权限来配置 StorageZones Controller，以及端口 443 在外部防火墙上打开。
您的网络共享上名为“ShareFileStorage”的文件夹不包括 sckeys.txt 后启用和配置 StorageZones for ShareFile Data	StorageZones Controller 在安装过程中创建 sckeys.txt，除非您用于安装 StorageZones Controller 的帐户不在访问控制列表中。更新访问控制列表并重新安装 StorageZones Controller。
创建区域后，文件上载到共享文件夹失败	此问题表示您的内部 DNS 存在问题。您必须具有 StorageZones Controller FQDN 的内部和外部 DNS 记录。
在“监视”选项卡上，检测信号状态为红色	红色图标表示 StorageZones Controller 无法向 ShareFile 网站发送检测信号消息。检查其他组件的图标是否为红色。如果是这样，请参阅日志了解更多信息。如果 s3uploader 日志显示未能发送检测信号，则 StorageZones Controller 服务器可能无法与 ShareFile 网站联系，除非它通过代理服务器。若要为 StorageZones Controller 指定代理服务器，请打开 Controller 控制台并转到“网络”选项卡。如果 StorageZones Controller 服务器无法使用网络服务用户访问 ShareFile 网站，则允许网络服务用户访问 ShareFile 网站或设置具有代理服务器出站访问权限的 Windows 用户帐户。

问题	说明和解决办法
存储区域不显示在 ShareFile 管理员界面中	此问题可能表示外部地址或防火墙存在问题。首先在 StorageZones Controller 控制台中验证外部地址不包括端口。如果是，请删除端口，然后重新启动 Controller。如果外部地址不包括端口，请确保 Windows 防火墙配置正确。默认情况下，Windows 防火墙设置允许端口 443 上的 ShareFile 服务的出站流量。存储区域 Controller 需要该设置。验证 Windows 防火墙是否允许在端口 443 上执行以下进程的出站流量：C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCopySvc\Fil :\inetpub\wwwroot\Citrix\StorageCenter\s3uploader\S3UploaderService.exe“、、C:\inetpub\wwwroot\Citrix\StorageCenter\CloudStorageUploaderSvc\CloudStorageUploaderService.exe、C:\inetpub\wwwroot\Citrix\StorageCenter\SCProxyEmailSvc\ProxyEmailService.exe

问题	说明和解决办法
StorageZones Controller 不会将数据上载到 ShareFile	在 Citrix ADC 控制台中，右键单击负载平衡虚拟服务器以获取统计信息，以验证流量是否从 ShareFile 控制平面、StorageZones Controller 和 ShareFile 客户端到达 Citrix ADC。当您上载文件并且虚拟服务器显示点击量增加时，流量将通过 Citrix ADC 传递。验证 Citrix ADC 连接的每个点的流量：内容交换虚拟服务器、连接器和 ShareFile 数据的负载平衡虚拟服务器、绑定到两个虚拟服务器之一的 HTTP 标注、绑定到 ShareFile 数据虚拟服务器的响应程序策略、连接器虚拟服务器绑定到 Citrix ADC AAA。然后，通过在 ShareFile 数据的负载平衡虚拟服务器中解除响应程序策略的绑定来测试上载的 ShareFile 数据。（响应程序策略删除未由 ShareFile 控制平面签名的传入流量。在 Web 浏览器中，键入 StorageZones Controller 的外部 FQDN。如果存在连接，则会显示 ShareFile 徽标。在 Web 浏览器中，键入连接器的 URL。如果以下 URL 成功测试存储区域连接器的可访问性，则系统将提示您输入凭据，即使后端服务器已关闭。或者，如果您以用户身份登录，则会得到 API 响应。`https://szc-address/cifs/v3/Items/ByPath?path=\\path`，`https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server`。API 响应的格式如下：{“Name”:”connectorName”,“FileName”:”FileName”,“CreationD`://szc-address/cifs/v3/$metadata##`Items/ShareFile.Api.Models.Folder@Element”,“Id”:”id”}.其他示例：`https://szc-address/cifs/v3/getItems(itemID)`、`https://szc-address/sp/v3/getItems(itemID)`。对于 iOS：`https://szc-address/cifs/v3/Items/(connector-folder-ID)?$select=Name,FileName,CreationDate,ProgenyEditDate...`。从外部网络测试设备。DNS 设置可能会导致设备连接问题。您必须具有外部 DNS 记录，并且您可能还需要外部存储区域 FQDN 的内部 DNS 记录。如果仅使用特定设备时遇到问题，请测试该设备。

问题	说明和解决办法
从文件清理服务的 ShareFile 连接状态是一个红色图标升级 StorageZones Controller 后	如果 Windows 在 StorageZones Controller 建立网络连接之前启动文件清理服务，则会出现红色图标。Controller 服务器返回网络后，状态将返回绿色图标。
连接器创建过程中出现 “路径超过最大长度 (1024)”	如果为 StorageZones Controller 配置的外部地址指向 ShareFile 网站而不是 StorageZones Controller 服务器 FQDN，则会发生此消息。
删除旧的 StorageZones Controller 后配置新的 StorageZones Controller 时，会显示 “无效名称”。	如果与旧 StorageZones Controller 相关的实体仍然存在，则可能会发生此消息。要解决此问题：卸载新的 StorageZones Controller。删除共享网络文件夹。删除文件夹 c:\inetpub\wwwroot\Citrix. 打开注册表编辑器并删除注册表项 **HKEY_LOCAL_MACHINE/Software/Wow6432Note/Citrix**。安装和配置新的 StorageZones Controller。如果问题仍然存在，请与您的支持代表联系。当存储区域服务器无法通过 DNS 或本地主机文件解析存储区域 FQDN 时，会出现此消息。

手动注册 **ASP.NET**

```
cd /d C:\Windows\Microsoft.NET\Framework\v4.0.30319
iisreset /stop
aspnet_regiis -i
iisreset /start
%systemroot%\system32\inetsrv\appcmd set config /section:
    isapiCgiRestriction
/[path='%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll'].
    allowed:True
%systemroot%\system32\inetsrv\appcmd set config /section:
    isapiCgiRestriction
/[path='%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll'
    ].allowed:True
```

疑难解答 **ShareFile** 客户端和 **Web** 应用程序

如果移动设备无法连接到连接器，请验证连接性。上表介绍了许多连接问题。确保 StorageZones Controller 处于联机状态。将文件上载到区域。如果上载工作正常，则问题特定于连接器。尝试使用蜂窝网络和公司网络从移动设备连接。检查 SharePoint 服务器或文件服务器是否可用。

如果尝试访问连接器时出现“HTTP 错误 401 — 未经授权”，则可能是以下任何问题，可能会阻止用户从 ShareFile 客户端或 ShareFile Web 应用程序访问连接器：

- IIS 配置不正确：验证 Web 服务 (IIS) 角色是否启用了基本身份验证和 Windows 身份验证。如果这些选项未在“安全性”下列出，请使用服务器管理器安装它们，然后重新启动 IIS。
- 用户权限不正确：验证 AD 用户是否具有对共享的访问权限。从服务器管理器中，转到“共享和存储管理”，然后根据需要添加用户或更改用户权限。
- Citrix ADC 身份验证、授权和审核组访问的问题。有关故障排除信息，请参阅 <CTX126589。

如果连接到 SharePoint 站点时出现“HTTP 错误 403-禁止”，则 SharePoint 服务器可能配置为基本身份验证，但 StorageZones Controller 可能未配置为缓存凭据。要解决此问题，请添加 `<add key=”CacheCredentials”value=”1”/>` 到 `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`。

如果移动应用尝试访问连接器时出现“HTTP 错误 503-服务不可用”，则连接器正在发送响应，但无法处理 HTTP 请求。如果在 Citrix ADC 上配置不正确或绑定了内容交换策略、负载平衡 VIP 或响应程序策略，则会发生这种情况。要解决此问题，请检查 ShareFile 的 Citrix ADC 配置并更正配置。

限制 **StorageZone**

June 15, 2020

受限制的存储区域用于保护敏感数据。只有员工才能访问受限制的存储。

受限区域不支持第三方用户身份验证。

> 注意：
>
> 受限存储区域为“维护结束”。此生命周期策略在中详细介绍 生命周期里程碑定义。不支持创建新的受限存储区域。使用受限存储区域的现有客户将收到有关未来任何产品里程碑的进一步通信。

受限区要素

区域身份验证：除了登录 ShareFile 之外，用户还必须单独向 StorageZones Controller 进行身份验证，以访问存储在受限区域中的文档。目录查找可确保登录到 ShareFile 的用户与对区域进行身份验证的用户相同。此额外的身份验证要求限制了共享。文档只能与有权访问 StorageZones Controller 且可以使用企业凭据进行身份验证的其他人共享。在受限区域中，文件不能匿名共享。必须向用户授予查看文件的权限，并且必须始终登录才能接收共享文件。

元数据加密：有关区域中文件和文件夹的所有信息都使用密钥加密，然后再发送到 ShareFile。因此，组织外部的任何人都不能看到受限区域中的文件夹或文件名。只有通过企业身份验证对 StorageZones Controller 才能访问加密密钥、解密文件和元数据。

StorageZones Controller 的内部地址：对于受限区域，授权在 StorageZones Controller 和 ShareFile 客户端之间进行，而不是在 StorageZones Controller 和 ShareFile 云之间进行。因此，托管受限区域的 StorageZones

Controller 不需要外部地址或外部 SSL 证书。当 StorageZones Controller 配置为仅内部地址时，用户必须连接到公司网络或 VPN 才能访问受限区域中的文档。

来自邮件服务器的电子邮件通知：当用户收到有关受限区域中共享文件和文件夹的电子邮件通知时，电子邮件将从内部邮件服务器而不是 ShareFile 服务器发送。

标准区域和限制区域之间的差异

属性	标准区域	受限区域
存储区域服务器可以通过以下方式进行管理：	Citrix 或者你	你
用户身份验证由...	ShareFile.com 或 ShareFile.eu	ShareFile.com 或 ShareFile.eu 的组合加上本地 StorageZones Controller
文件可以与... 共享	员工和第三方用户（即拥有电子邮件地址的任何人）	员工或其他拥有域帐户的用户
存储在 ShareFile 控制平面中的文件和文件夹元数据是...	以明文形式存储，对某些 Citrix 员工可见	使用您的私钥加密，Citrix 不可用
电子邮件通知使用...	ShareFile 邮件服务器或 SMTP 服务器	您的 SMTP 服务器
区域的外部地址是...	必填	不需要

标准和受限制的存储区域

您可以将存储区域指定为标准区域或限制区域。

- 标准存储区域专用于存储非敏感数据，员工可以在此区域中与非员工共享数据。
- 受限制的存储区域可保护敏感数据：只有员工才能访问该区域中存储的数据。

下表总结了标准区域和限制区域之间的差异。

属性	标准区域	受限区域
存储区域服务器可以通过以下方式进行管理：	Citrix 或者你	你
用户身份验证由...	ShareFile.com 或 ShareFile.eu	ShareFile.com 或 ShareFile.eu 的组合加上本地 StorageZones Controller
文件可以与... 共享	员工和第三方用户（即拥有电子邮件地址的任何人）	员工或其他拥有域帐户的用户

属性	标准区域	受限区域
存储在 ShareFile 控制平面中的文件和文件夹元数据是...	以明文形式存储，对某些 Citrix 员工可见	使用您的私钥加密，Citrix 不可用
电子邮件通知使用...	ShareFile 邮件服务器或 SMTP 服务器	您的 SMTP 服务器
区域的外部地址是...	必填	不需要

在 Citrix 管理的区域中，ShareFile 云执行除员工身份验证之外的所有操作，此操作由 StorageZones Controller 处理。

在标准区域中，将在云中处理网站维护和更新、客户端和应用程序更新、文件元数据、上载和下载授权、电子邮件通知 (SMTP)、第三方用户身份验证和文件夹权限。员工身份验证、文件存储和加密由 Controller 处理。

在受限区域中，网站维护和更新、客户端和应用程序更新以及文件夹权限在云中进行处理。员工身份验证、文件存储和加密、文件元数据、上载和下载授权以及电子邮件通知 (SMTP) 由 Controller 处理。受限区域不支持第三方用户身份验证。

ShareFile 支持在域中混合使用标准区域和受限区域。您可以创建多个受限区域，其中每个区域都有自己的唯一身份验证要求。例如，如果不应允许域 A 中的用户与域 B 中的用户共享文件，请为每个域安装单独的受限区域。

本节的其余部分介绍 ShareFile 管理区域、标准区域和受限区域中的工作流程。

针对受限存储区域的概念验证部署

为受限区域配置的 StorageZones Controller 不需要接受来自 ShareFile 云的内绑定连接：您可以使用内部地址对其进行配置。下图显示了用户设备、ShareFile 云和 StorageZones Controller 之间的流量。

在这种情况下，一个防火墙站在 Internet 和安全网络之间。StorageZones Controller 驻留在防火墙内以控制访问。与 ShareFile 的用户连接必须遍历防火墙，并使用端口 443 上的 SSL 协议来建立此连接。若要支持此连接，您必须在防火墙上打开端口 443，并在 StorageZones Controller 的 IIS 服务上安装 SSL 证书（可以是私有的）。

对于受限区域，StorageZones Controller 从本地 SMTP 服务器（而不是从 ShareFile）发送电子邮件通知。

针对受限区域的高可用性部署

为受限区域配置的 StorageZones Controller 不需要接受来自 ShareFile 云的绑定连接：您可以使用内部地址配置每个控制器。下图显示了受限区域的高可用性部署。

在这种情况下，一个防火墙站在 Internet 和安全网络之间。StorageZones Controller 驻留在防火墙内以控制访问。与 ShareFile 的用户连接必须遍历防火墙，并使用端口 443 上的 SSL 协议来建立此连接。若要支持此连接，您必须在防火墙上打开端口 443，并在 StorageZones Controller 的 IIS 服务上安装 SSL 证书（可以是私有的）。

对于受限区域，StorageZones Controller 从本地 SMTP 服务器（而不是从 ShareFile）发送电子邮件通知。

受限区域

下表介绍了当用户登录到 ShareFile 然后从受限区域下载文档时发生的网络连接。所有连接都使用 HTTPS。

步骤	源	目标
1. 用户登录请求	客户端	company.sharefile.com
2. 如果使用 ADFS，请重定向至“SAML IdP 登录”	客户端	SAML 身份提供商 URL
3. 文件/文件夹枚举和下载请求	客户端	szc.company.com
4. 文件下载授权并获取加密元数据	szc.company.com	company.sharefile.com
5. 文件下载	客户端	szc.company.com

针对受限存储区域的部署

下图显示了受限区域的高可用性部署。

对于受限区域，StorageZones Controller 从本地 SMTP 服务器（而不是从 ShareFile）发送电子邮件通知。

受限区域的网络连接

下图和表描述了用户登录 ShareFile 然后将文档上载到限制区域时发生的网络连接。在这种情况下，帐户使用 Active Directory 联合身份验证服务 (ADFS) 进行 SAML 登录。身份验证通信由 ADFS 代理服务器处理，该服务器与受信任网络上的 ADFS 服务器通信。

步骤	源	目标	协议
1. ShareFile 客户端或浏览器打开连接	客户端	company.sharefile.com 或 company.sharefile.eu	HTTPS
2. （可选）重定向至“SAML IdP 登录”诊所诊所	客户端	SAML 身份提供商 URL	HTTPS
3. ShareFile 将用户重定向到 StorageZones Controller	客户端	company.sharefile.com 或 company.sharefile.eu	HTTPS

步骤	源	目标	协议
4. 客户端将 Windows 凭据提交到 StorageZones Controller	客户端	存储区域控制器	HTTPS
5. StorageZones Controller 验证凭据并授予客户端访问权限	存储区域控制器	域 Controller	Kerberos
6. 客户端将文件上载到 StorageZones Controller	客户端	存储区域控制器	HTTPS
7. 文件被写入受限区域的存储库	存储区域控制器	本地存储	CIFS
8. StorageZones Controller 加密文件元数据并将其发送到 ShareFile	存储区域控制器	`company.sharefile.com` 或 `company.sharefile.eu`	HTTPS

对于受限制的存储区域：

- 使用内部或外部主机名。
- 为与 ShareFile 的通信启用 SSL。

  如果使用内部主机名，则可以使用私有证书。证书必须受到用户设备的信任。

  如果使用外部主机名，则 StorageZones Controller 上的 SSL 证书必须受到用户设备和 ShareFile Web 服务器的信任。
- 提供从 StorageZones Controller 到以下服务总线 URI 之一的出站 HTTP 访问：
  - ShareFile.com 帐户：`sf-zk-email-use.servicebus.windows.net`
  - ShareFile.eu 帐户：`sf-zk-email-euw.servicebus.windows.net`

  请务必与您的网络团队安排网络依赖关系。

客户端对受限存储区域的要求

ShareFile Web 应用程序支持来自以下 Web 浏览器的受限存储区域：

- Internet Explorer 11

  要启用从 ShareFile Web 应用程序访问受限区域中的文件夹和连接器，请执行以下操作：

1. 打开 Internet 浏览器，转到 Internet 选项，单击 安全选项卡，然后单击 受信任的站点。
2. 单击 站点，然后添加您的子域和外部 StorageZones Controller 地址。
3. 单击 “关闭”，然后单击 “自定义级别”。
4. 对于 “杂项”>“跨域访问数据源”，请选择 “启用”。
5. 对于 “用户身份验证”>“登录”，选择 “提示输入用户名和密码”。

- Chrome
- Firefox
- Safari
- Secure Web

要支持受限制的存储区域，ShareFile 客户端必须升级到以下版本或更高版本：

- ShareFile Sync for Windows 3.1
- ShareFile Outlook 插件 3.2.2
- ShareFile for iOS 3.3
- Android 3.4 的 ShareFile
- ShareFile 的 Windows Phone 2.3.10

截至本文发布日期，不支持这些 ShareFile 客户端和工具与受限制的存储区域一起使用：

注意：有关 ShareFile 客户端功能的最新信息，请参阅
ShareFile 支持 站点或与您的 ShareFile 支持代表联系。

- 域外使用 ShareFile Desktop Sync for Windows 3.1 和 ShareFile Outlook 插件

  客户端必须位于与 StorageZones Controller 服务器位于同一 Active Directory 林中的加入域的 Windows 桌面上。客户端可以使用 NTLM 或 Kerberos 对受限区域进行静默身份验证。

- On-Demand Sync for Windows
- Sync for Mac
- ShareFile Enterprise Sync Manager
- Secure Mail for iOS
- ShareFile Desktop 小组件
- ShareFile 为黑莓
- ShareFile 移动网站

不支持以下备用帐户访问方法与受限存储区一起使用：

- FTP
- PowerShell
- ShareFile 命令行界面 (SFCLI)
- HTTPS API (V1)

- WebDav
- SMTP

> 重要
>
> ShareFile 不正式支持，并且不建议使用 **DFS** 复制。已知它会导致较大文件的锁定失败。如果必须使用 DFS 复制，请在非高峰时段使用单独的备份解决方案，当区域未处于主动使用中。

升级受限存储区域

将 StorageZones Controller 升级到最新版本时，该 Controller 将继续使用标准区域。不能将标准区域升级到限制区域。

要将标准区域替换为受限区域，您必须安装新的 StorageZones Controller 并配置受限区域。

要支持受限区域或对连接器的 Web 访问，必须在完成向导后执行其他 Citrix ADC 配置。配置确保 ShareFile 客户端仅在登录到受信任的 ShareFile 域时才发送凭据。要支持对连接器的 Web 访问，还可以向用于传输到 /cifs 和 /sp 的流量的内容切换策略添加路径 (/Proxy Service)。

其他限制区域信息

对受限存储区域的支持会影响 ShareFile 服务的所有方面。由于支持元数据加密和区域身份验证所需的协议更改，因此在受限存储区域中处理文档时不支持某些 **ShareFile** 客户端和功能。

目录

客户端和工具

Sync for Windows	3.1 及以上
适用于 Microsoft Outlook 的插件	3.2.2 及以上
On-Demand Sync for Windows	不支持
Drive Mapper	3.01.171.0 及更高版本

ShareFile for iOS	3.3 — 仅限 MDX
Android 的 ShareFile	3.4 及以上
ShareFile 的 Windows Phone 8	2.3.10 及以上
Sync for Mac	不支持
ShareFile Desktop	不支持
XenMobile WorxMail for iOS	不支持
XenMobile WorxMail for Android	支持
打印到 ShareFile	不支持
移动网站	不支持
其他帐户访问方法	
PowerShell	不支持
SFCLI	不支持
REST API(V3)	支持
HTTPS APT(V1)	不支持
RSZ 测试覆盖范围	不支持
FTP	不支持
将文件通过电子邮件发送到文件夹	不支持
.NET 开发工具包	支持

浏览器

Windows	互联网浏览器 11, 火狐浏览器 (最新版本), 铬 (最新版本)
macOS	Safari 浏览器（最新版本），火狐（最新版本），铬（最新版本）
iOS	野生动物园，Secure Web
Android	Secure Web

功能

最终用户操作：使用文件：

浏览和下载文件	支持
上载文件（上载器类型）	HTML5：支持；Flash：不支持；Java：不支持；标准 HTML 表单：不支持
回收站	支持
批量下载和删除	支持
文件盒	视图：支持；删除：支持；上载：支持；下载：不支持；从文件盒发送：不支持
文件预览（缩略图）	不支持
在 Web 浏览器中查看文档	不支持
文件重新上载	不支持
每个文件多个版本	不支持
搜索	搜索结果中未包含的受限区商品
将文件夹标记为收藏夹	不支持
复制或移动文件	不支持
编辑文件夹选项：文件夹过期日期、文件保留策略	支持
共享文件夹冒泡	不支持

最终用户操作：共享和协作：

发送文件：需要上传，使用 ShareFile 发送电子邮件，给我一个链接，我可以复制，要求用户登录，限制下载次数	支持
接收和下载共享文件	支持
在受限存储区域中创建共享文件夹	支持
将用户添加到文件夹：控制上载和下载的权限	支持
请求文件	支持
请求启用“需要 ShareFile 登录”的文件	不支持

电子邮件通知	支持
收件箱：发送给我的文件	支持
收件箱：已发送邮件	查看、过期、重新发送、编辑：支持
查看活动日志	支持
获取签名（通过 RightSignature）	不支持

行政操作：

在受限区域中创建用户	支持
将用户迁移到其他区域	不支持
报告：访问审核、使用情况报告、消息报告、带宽报告、存储报告	HTML 查看器：支持；Excel /CSV/PDF 查看器：显示加密元数据
区域管理	
监视存储使用情况	支持
监控带宽使用情况	支持
监视文件活动	支持
恢复文件	不支持
协调文件	不支持
删除区域	支持
高可用性	支持

Sync for Windows

最低版本-3.1

从加入域的客户端进行身份验证-NTLM 或 Kerberos	支持
从非域客户端进行身份验证-用户提示输入密码	支持
在受限区域中同步“我的文件和文件夹”	支持

从受限区域同步共享文件夹	支持
上载、下载、同步	支持
On-demand Sync for XenApp and XenDesktop 环境	不支持
查看收藏夹文件夹	不适用于受限制的存储区域文件夹
右键单击 > 复制链接	支持
右键单击 > 电子邮件文件	支持

移动应用程序

请参阅下面特定于应用程序的表格：

iOS-最低版本 **3.3**

浏览和下载文件	支持
脱机查看内容	支持
创建文件夹	支持
创建或编辑文件	支持
上载照片或视频	支持
使用用户名/密码进行验证	支持
使用 Worx 微型 VPN 进行单点登录	支持
共享：复制链接	支持
分享：通过电子邮件共享	不支持
添加或编辑文件夹注释	不支持
创建注释或编辑现有注释	不支持
将用户添加到文件夹或编辑现有文件夹权限	不支持
标记/取消将文件夹标记为收藏夹	不支持
请求文件	不支持
缩略图预览	不支持

多项删除	不支持
使文件夹脱机可用	除了根级别“与我共享”文件夹外，支持
共享文件夹	除了根级别“与我共享”文件夹外，支持
在受限存储区域中创建连接器	不支持

Android-最低版本 **3.4**

浏览和下载文件	支持
脱机查看内容	支持
发送文件	支持
创建文件夹	支持
创建或编辑文件	支持
上载文件	支持
使用用户名/密码进行验证	支持
使用 Worx 微型 VPN 进行单点登录	支持
请求文件	不支持
创建备忘录	不支持
上载后覆盖现有文件	不支持

Outlook 插件

从加入域的客户端进行身份验证-NTLM 或 Kerberos	支持
从非域客户端进行身份验证-用户提示输入密码	支持
浏览并从 ShareFile 中选择文件	支持
在启用“要求收件人登录”的情况下浏览和选择 ShareFile 中的文件	不支持
将附件转换为 ShareFile 链接	支持

将附件转换为已启用“要求收件人登录”的 ShareFile 链接	不支持
请求文件	支持
请求启用“要求收件人登录”的文件	不支持

参考：**StorageZones Controller** 配置文件

June 15, 2020

此参考概述了 StorageZones Controller 配置文件：

- 应用程序设置发布。配置
- 文件删除。例如配置
- SFAntiVirus.exe.config
- 网络配置

StorageZones Controller 安装程序创建这些文件。您在 StorageZones Controller 控制台中所做的更改将保存到文件中。

要使用或配置某些功能，必须在配置文件中手动添加或更新某些设置。此参考文献列出了这些设置，并提供指向相关信息的链接。

应用程序设置发布。配置

应用程序设置释放.config 文件包含在 StorageZones Controller 安装路径 (C:\inetpub\wwwroot\Citrix\) 中的以下文件夹中：

- StorageCenter

  定义 StorageZones Controller 的全局设置。

- StorageCenter\cifs

  定义网络文件共享的存储区域连接器的设置。

- StorageCenter\sp

  定义 SharePoint 的存储区域连接器的设置。

在编辑应用程序设置发布.config 文件之前，请验证您在正确的位置工作。

文件删除。例如配置

FileDeleteService.Exe.config 提供了 StorageZones Controller 用于管理持久性存储缓存的控件。此配置文件位于：`C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`

有关详细信息，请参阅自定义存储缓存操作。

SFAntiVirus.exe.config

SFAntiVirus.exe.config 为扫描仪软件提供有关您的 StorageZones Controller 配置、扫描仪软件的位置和各种命令选项的信息。此配置文件位于：`C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`

有关详细信息，请参阅配置上载文件的防病毒扫描。

网络配置

通常，`C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` 包含通常不应更改的控件。但是，如果将旧 StorageZones Controller 与代理服务器一起使用，则需要对其进行更新。

仅适用于 **StorageZones Controller 2.2** 到 **2.2.2**：如果一个区域具有多个 StorageZones Controller，并且所有 HTTP 流量都使用代理服务器，则必须为每个辅助服务器添加一个绕过列表。

注意：自版本 2.2.3 起，绕过设置包含在 StorageZones Controller 控制台的网络页面中。

1. 在文本编辑器中打开文件并找到该 `<system.net>` 部分。以下是配置代理服务器后该部分的示例：

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
    </defaultProxy>
  </system.net>
</configuration>
```

2. 向该部分添加一个旁路列表，如下所示：

```
<system.net>
    <defaultProxy enabled="true">
      <proxy proxyaddress="http://192.0.2.0:3128" />
      <bypasslist>
        <add address="primaryServer" />
      </bypasslist>
    </defaultProxy>
  </system.net>
```



```
</configuration>
```

主服务器是 IP 地址或主机名（服务器名称.sub 域.com）。

如果稍后更改主 StorageZones Controller IP 地址或主机名，则必须更新每个辅助服务器的 ConfigService\Web.config 中的信息。

3. 重新启动所有区域成员的 IIS 服务器。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States