



存储区域控制器 **5.x**

Contents

关于 StorageZones Controller	3
体系结构概述	5
系统要求	12
安装	16
为存储区域控制器配置 Citrix ADC	17
手动配置 Citrix ADC	24
为专用数据存储创建网络共享	28
安装 SSL 证书	30
准备好您的服务器存储 ShareFile 数据	30
安装 StorageZones Controller 并创建存储区域	39
验证您的 StorageZones Controller 设置	48
更改用户帐户的默认区域	49
指定存储区域的代理服务器	50
配置域控制器以信任存储区域控制器进行委派	50
为 Web 应用程序预览、缩略图和仅限查看共享配置存储区域控制器	52
配置多租户存储区域	57
升级	59
管理存储区域控制器	61
将辅助存储区域控制器加入到存储区域	62
更改主 StorageZones Controller 的地址或密码	62
降级和提升 StorageZones Controller	63
禁用、删除或重新部署存储区域控制器	64
将文件传输到新网络共享	65

备份主存储区域控制器配置	66
恢复主 StorageZones Controller 配置	68
替换主 StorageZones Controller	71
准备存储区域控制器以进行文件恢复	72
从您的 ShareFile 数据备份中恢复文件和文件夹	78
协调 ShareFile 云与存储区域	80
Windows Server 2012R2 ShareFile 存储区域迁移指南	80
配置上传文件的防病毒扫描	82
迁移 ShareFile 数据	86
连接器收藏夹	88
管理 ShareFile 数据的存储区域	88
创建和管理 StorageZone 连接器	90
数据丢失防护	97
监视	103
参考：存储区域控制器配置文件	111

关于 **StorageZones Controller**

June 30, 2023

存储区域控制器通过为您的 ShareFile ile 帐户提供私有数据存储来 ShareFile ile 软件即服务 (SaaS) 云存储。

有关存储区域控制器的更多信息，例如组件、数据存储等，请参阅 [存储区域控制器 5.x](#)。

请参阅[新增功能](#)，了解此功能和 Citrix Content Collaboration 中的最新增强功能。

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

提示：

Citrix 建议用户启用 [Alert Settings](#)（警报设置）并定期查看 [Security Bulletins](#)（安全公告）。

已修复的问题

已修复存储区域控制器 **5.11.24** 中的问题

安全修复：此版本包含安全性和可靠性的修复程序。

已修复存储区域控制器 **5.11.23** 中的问题

安全修复：此版本包含安全性和可靠性的修复程序。

已修复存储区域控制器 **5.11.22** 中的问题

安全修复：此版本包含安全性和可靠性的修复程序。

已修复存储区域控制器 **5.11.21** 中的问题

安全修复：此版本包含安全性和可靠性的修复程序。

已修复存储区域控制器 **5.11.18** 中的问题

安全修复：此版本包含安全性和可靠性的修复程序。

已修复存储区域控制器 **5.11.17** 中的问题

安全修复：此版本包含安全性和可靠性的修复程序。

存储区域 **Controller 5.11** 中的已修复问题

此版本解决了许多可提高整体性能和稳定性的问题。

已修复存储区域控制器 **5.10** 中的问题

此版本解决了多个有助于改进整体性能和稳定性的问题。

已修复存储区域控制器 **5.9** 中的问题

此版本包含用于提高可靠性和性能的修补程序。

已修复存储区域控制器 **5.8** 中的问题

此版本包含一个修复程序，用于改进签出文件的错误消息，以及针对 SharePoint 中新发布的托管路径的修复。

已修复存储区域控制器 **5.7** 中的问题

此版本包含修复程序，用于解决将文件上传到存储区域和本地连接器时出现的重定向问题。

已修复存储区域控制器 **5.6** 中的问题

WOPI 修复：包括更改以解决尝试编辑 Office 文件后续时出现的问题。

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的错误消息的更改。

已修复存储区域控制器 **5.5** 中的问题

此版本包含用于提高可靠性和性能的修补程序。

已修复存储区域控制器 **5.4.2** 中的问题

SharePoint 连接器修复：在特定情况下，移动 SharePoint 连接器上存在的文件可能会失败。此版本确保 SharePoint 连接器上存在的移动文件按预期工作。

安全修复：此版本包含安全性和可靠性的修复程序。

已修复存储区域控制器 **5.4.1** 中的问题

安全修复：此版本包含安全性和可靠性的修复程序。

其他支持：已添加对 Workspace 环境的 *cloud/cloudburrito* 帐户的支持。

存储区域 **Controller 5.3.1** 中已修复的问题

此版本包含用于提高可靠性和性能的修补程序。

存储区域 **Controller 5.3.1** 中已修复的问题

WOPI 修复：WOPI 访问令牌可能因盗窃公用加密密钥而被欺骗。此版本确保密钥不会在存储区域控制器之间共享。

安全修复程序：此版本包含安全性、性能和可靠性的修复程序。

已知问题

存储区域控制器 **5.10** 中的已知问题

在此版本中没有发现新问题。

存储区域控制器 **5.9** 中的已知问题

在此版本中没有发现新问题。

存储区域控制器 **5.8** 中的已知问题

在此版本中没有发现新问题。

存储区域控制器 **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

November 9, 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。高可用性部署将显示带有和不带 DMZ 代理（如 Citrix ADC）的情况。

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送数据，请配置存储区域连接器。

StorageZones Controller 概念验证部署

小心：

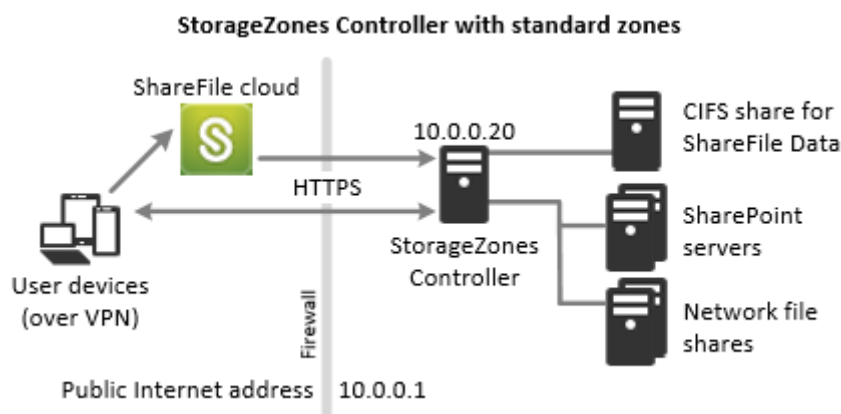
概念验证部署仅用于评估目的，不应用于关键数据存储。

概念验证部署使用单个 StorageZones Controller。本节中讨论的示例部署启用了 ShareFile 数据的存储区域和存储区域连接器。

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。要做到这一点，Controller 必须具有可公开访问的互联网地址和 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。

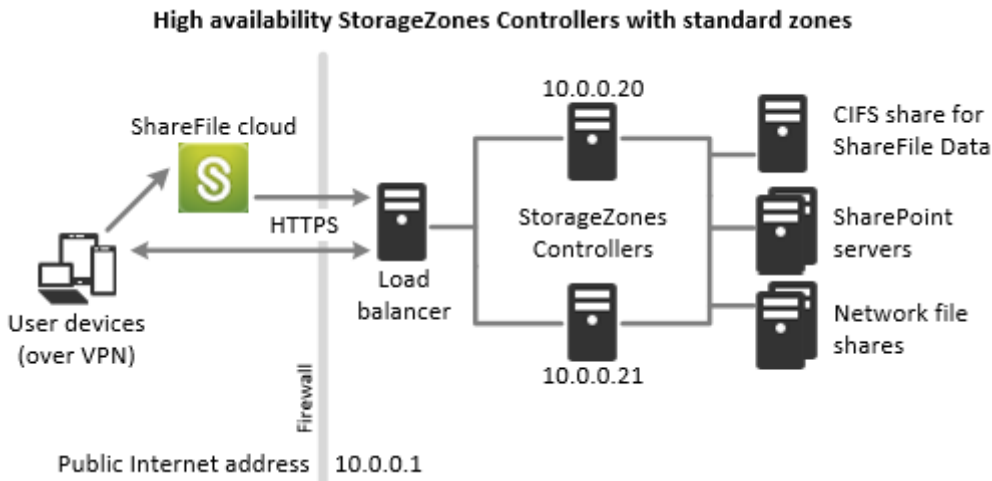
StorageZones Controller 高可用性部署

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。当您安装其他控制器时，您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。要做到这一点，每个 Controller 都必须具有可公开访问的互联网地址和 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相关联。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，Internet 和安全网络之间有一个防火墙。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。

您可以使用命名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	目标位置
1. 用户登录请求	客户端	company.sharefile.com:443
1. (可选) 重定向至 “SAML IdP 登录” 诊所诊所	客户端	SAML 身份提供程序 URL
1. 文件/文件夹和下载请求	客户端	company.sharefile.com:443
1. 文件下载	客户端	storage-location.sharefile.com:443

标准存储区 下表介绍了用户登录到 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	目标位置
1. 用户登录请求	客户端	company.sharefile.com
1. (可选) 如果使用 ADFS，请重定向至 SAML IdP 登录	客户端	SAML 身份提供程序 URL
1. 文件/文件夹和下载请求	客户端	company.sharefile.com
1. 文件下载授权	company.sharefile.com	szc.company.com
1. 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。

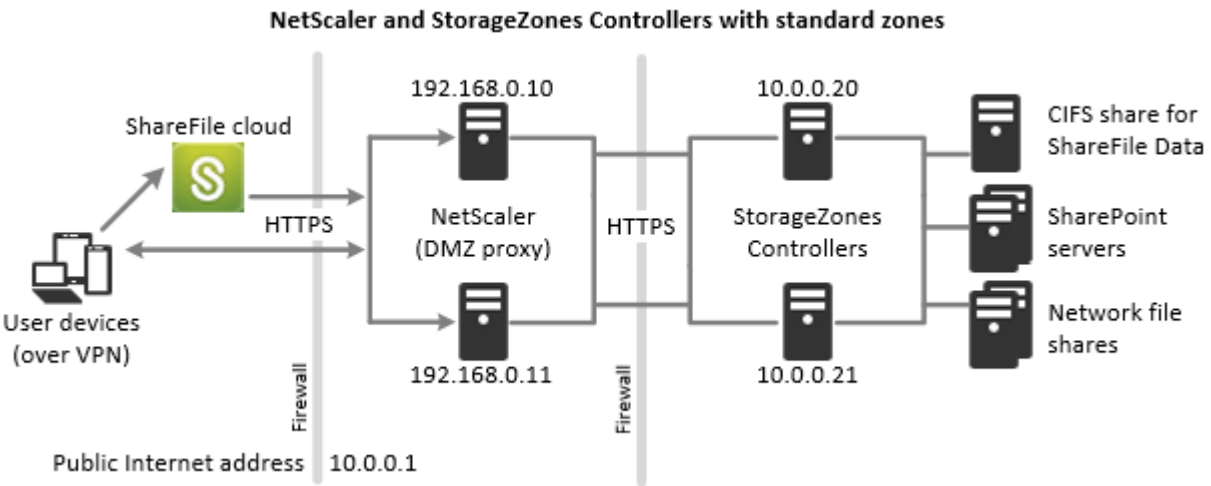
- 使用实时状态指示器向 StorageZones Controller 发出负载均衡请求。

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

- 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 SSL，以便与 ShareFile 云进行通信。

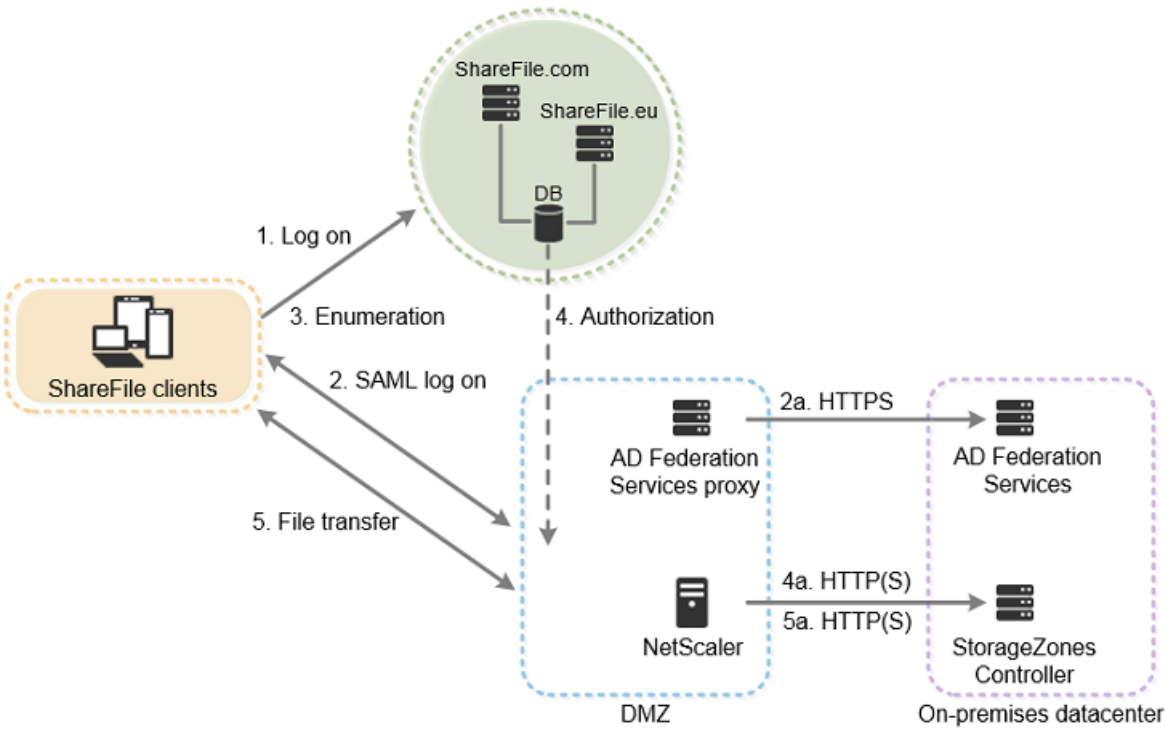


在这种情况下，两个防火墙位于互联网和安全网络之间。StorageZones Controller 驻留在内部网络中。与 ShareFile 的用户连接必须遍历第一个防火墙，并使用端口 443 上的 SSL 协议建立此连接。若要支持此连接，您必须在防火墙上打开端口 443，并在 DMZ 代理服务器的 IIS 服务上安装公用 SSL 证书（如果它们终止用户连接）。

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 之后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。

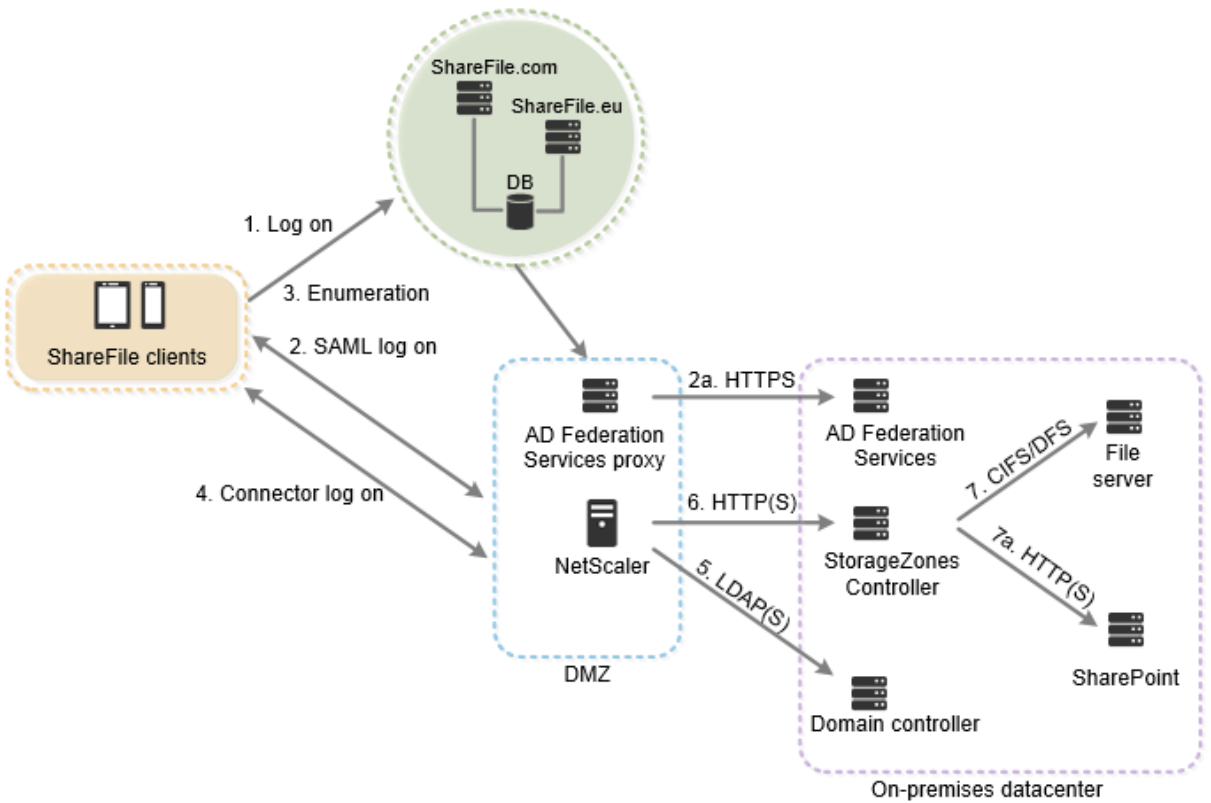
身份验证流量由 ADFS 代理服务器在 DMZ 中处理，该服务器与受信任网络上的 ADFS 服务器进行通信。文件活动是通过 DMZ 中的 Citrix ADC 访问的，该 ADC 将终止 SSL，对用户请求进行身份验证，然后代表身份验证的用户访问受信任网络中的 StorageZones Controller。使用互联网 FQDN 公司网站访问 ShareFile 的 Citrix ADC 外部地址。



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

下图和表格扩展了上一场景，显示了 StorageZone 连接器的网络连接。此方案包括在 DMZ 中使用 NetScaler 终止

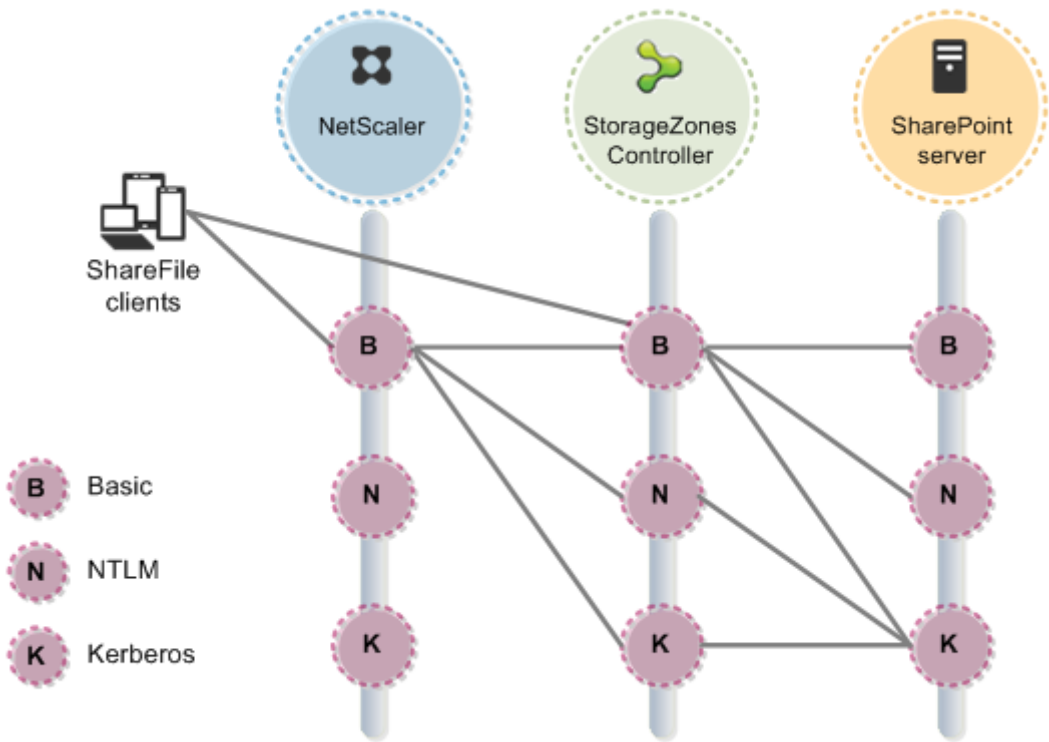
SSL 并对连接器访问执行用户身份验证。



步骤	源	目标位置	协议
1. 用户登录请求	客户端	company . sharefile.com	HTTPS
1. (可选) 重定向至 “SAML IdP 登录” 诊所诊所	客户端	SAML 身份提供程序 URL	HTTPS
2a. ADFS 登录	ADFS 代理	ADFS 服务器	HTTPS
1. 顶级连接器枚举	客户端	company . sharefile.com	HTTPS
1. 用户登录到 StorageZones Controller 服务器	客户端	szc.company.com (外部地址)	HTTPS
1. 用户身份验证	Citrix ADC IP (NSIP)	AD 域 Controller	LDAP
1. 文件/文件夹枚举和 上载/下载请求	Citrix ADC IP (NSIP)	StorageZones Controller	HTTP

步骤	源	目标位置	协议
1. 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

下图汇总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

November 20, 2023

重要：

Microsoft 将于 2023 年 10 月 10 日终止对 Windows Server 2012R2 的支持。务必在支持终止日期之前将服务器迁移到较新的版本。

存储区域控制器

- 具有 2 个 CPU 和 4 GB RAM 的专用物理机或虚拟机
- Windows Server 2012 R2（数据中心、标准版或基础版）
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

对于标准存储区域：

- 使用可公开解析的 Internet 主机名（不是 IP 地址）。
- 为与 ShareFile 的通信启用 SSL。
 - 存储区域控制器上的 SSL 证书必须受到用户设备和 ShareFile Web 服务器的信任。如果您直接在 IIS 中使用 SSL，请参阅 <http://support.microsoft.com/kb/298805>，了解有关配置 SSL 的信息。
- 允许端口 443 上的入站 TCP 请求通过您的防火墙。
- 允许通过防火墙向端口 443 上的 ShareFile 控制平面发出出站 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** 数据存储区域的服务器运行状况检查：

- 在本地主机上打开端口 80。

对于高可用性生产环境：

- 至少两台安装了存储区域控制器的服务器。
- 如果您没有使用 DMZ 代理服务器，请在 IIS 服务上安装 SSL 证书。

有关受支持证书的信息，请参阅以上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，例如 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 代理服务器和存储区域控制器之间的通信是安全的，则可以使用 HTTP。但是，建议将 HTTPS 作为最佳实践。如果您使用 HTTPS，则可以在存储区域控制器上使用私有（企业）证书，前提是该证书受到 DMZ 代理信任。DMZ 代理公开的外部地址必须使用商业上可信的证书。有关受支持证书的信息，请参阅以上标准区域的证书要求。

其他要求

注意：

ShareFile 不正式支持，也不建议使用 DFS 复制。众所周知，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该区域未处于活动状态的单独备份解决方案。

- 存储区域控制器安装程序需要管理权限。
- 要远程管理存储区域控制器，请使用远程协议（例如 RDP 或 Citrix ICA）连接到服务器，然后打开存储区域控制器控制台。

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

- 存储区域控制器可与任何符合 ICAP 的 DLP 解决方案集成，包括：
 - 赛门铁克数据丢失防护
 - McAfee DLP Prevent
 - Websense TRITON AP-DATA
 - RSA 数据丢失防护

ShareFile 数据的存储区域

ShareFile 数据的存储区域是您在存储区域控制器上启用的一项可选功能。

要求：

- ShareFile Enterprise 帐户，启用了存储区域功能
- 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

如果您计划将 ShareFile 文件存储在支持的第三方存储系统中，则 CIFS 共享用于临时文件（加密密钥、队列文件）和临时存储缓存。

- Web 服务器 (IIS) 角色和 ASP.NET 4.x。有关更多信息，请参阅 [为服务器准备 ShareFile 数据](#)。

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

SharePoint 的存储区域连接器

SharePoint 的存储区域连接器是您在存储区域控制器上启用的一项可选功能。

要求：

- 启用存储区域功能的 ShareFile Enterprise 帐户或 Citrix Endpoint Management。
- 仅支持 **Microsoft SharePoint Server 2010** 及更高版本。
- 存储区域控制器服务器必须是域成员，与 SharePoint 服务器位于同一林中。
- Web 服务器 (IIS) 角色和 ASP.NET 4.x。有关更多信息，请参阅 [为服务器准备 ShareFile 数据](#)。
- SharePoint 政策：
 - 在 SharePoint 2013 中，Web 应用程序的默认最大上传文件大小为 250 MB，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传大小。SharePoint 的上传文件大小限制为 2 GB。
 - ShareFile 客户端总是尝试签入文件的主要版本（发布）。但是，SharePoint 策略决定了文件是作为主要版本还是次要版本签入。
 - SharePoint 仅限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：有关存储区域连接器的用户设备支持的最新信息，请参阅 [ShareFile 知识库](#)。

用于 SharePoint 验证的存储区域连接器

对用户进行身份验证后，存储区域控制器服务器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 的存储区域连接器在 SharePoint 服务器上支持以下身份验证方法。

- 基本

要求您将 `<add key="CacheCredentials"value="1">` 添加到 `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`。

- 谈判 (克贝罗斯)
- Windows 质询/响应 (NTLM)

ShareFile 移动客户端使用基于 HTTPS 的基本身份验证对存储区域控制器或 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：[将域控制器配置为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)。有关更多信息，请参阅 <http://support.microsoft.com/kb/832769> 中的“为 Web 部件的委托配置信任”。

对于使用 Citrix ADC 的部署，可以终止 Citrix ADC 的基本身份验证，然后对存储区域控制器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存储区域控制器上启用的一项可选功能。

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。有关更多信息，请参阅 [为服务器准备 ShareFile 数据](#)。
- 用户设备：有关存储区域连接器的用户设备支持的最新信息，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，存储区域控制器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，并对文件服务器提出的身份验证挑战做出响应。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 (克贝罗斯)
- Windows 质询/响应 (NTLM)

要在存储区域控制器上使用 Kerberos 或 NTLM 身份验证：[将域控制器配置为信任存储区域控制器进行委派](#)。

对于使用 Citrix ADC 进行部署：要在 Citrix ADC 配置为基本身份验证时为用户提供单点登录体验，请将连接器配置为协商 (Kerberos) 和 NTLM 身份验证。

PowerShell 脚本和命令

存储区域控制器的安装包括多个 PowerShell 脚本和命令，位于 `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\` 中。

- 在 32 位 (x86) 版本的 PowerShell 中运行脚本。
- 为了获得最佳效果，请升级到 [Windows Management Framework](#) 中包含的 PowerShell 4.0 或更高版本。

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

安装

April 23, 2021

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. [准备好您的服务器存储 ShareFile 数据](#)

需要对 ShareFile 数据的存储区域和存储区域连接器进行 IIS 和 ASP.NET 安装。

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，[点击此处](#)。

有关将 ShareFile Enterprise 配置为使用 Microsoft Azure 存储区域的演示，[点击此处](#)。

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

February 14, 2022

NetScaler（版本 10.1 build 120.1316.e 及更高版本）包含一个向导，提示您输入有关存储区域控制器环境的基本信息。然后它会生成一个配置：

- 跨存储区域控制器负载均衡流量
- 为存储区域连接器提供用户身份验证
- 验证 ShareFile 上传和下载的 URI 签名
- 在 Citrix ADC 设备上终止 SSL 连接

下图显示了由配置创建的以下 Citrix ADC 组件：

- **Citrix ADC 内容交换虚拟服务器**—将用户从 ShareFile 和存储区域连接器获取数据的请求发送到相应的 Citrix ADC 负载均衡虚拟服务器。
- **Citrix ADC 负载均衡虚拟服务器**—对存储区域控制器的流量进行负载均衡，还可以处理以下操作：
 - 对于来自私有数据存储的数据请求，负载均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，负载均衡虚拟服务器可以执行用户身份验证。它会在 Citrix ADC 停止用户请求，对用户进行身份验证，然后执行用户单点登录到存储区域控制器。

注意：

通过 Citrix ADC 对存储区域连接器进行身份验证是可选的。由于已知问题，如果在 Citrix ADC 中启用了身份验证，则 WebApp 中的存储区域连接器在 Chrome、Chromium、Safari 和 Edge 浏览器中将无法正常工作。它与其他浏览器和桌面/移动客户端兼容。

从存储区域控制器 4.0 开始，管理员可以将到存储区域控制器的入站连接限制为 TLS v1.2。如果对存储区域控制器的入站流量禁用了早于 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。[单击此处了解更多信息和配置说明。](#)

注意：

要在 10.1 版本 120.1316.e 之前设置 NetScaler 版本，请参阅[手动配置 Citrix ADC](#)。

适用于 ShareFile 的 Citrix ADC 向导的设置无法处理将 Citrix Endpoint Management 用作 ShareFile 的 SAML 身份提供程序所需的配置。有关更多信息，[请单击此处](#)。

必备条件

- 有效的 Citrix ADC 配置
- 安全证书：如果在 Citrix ADC 中尚不可用，则使用向导可以在内容交换虚拟服务器上安装安全证书。
- 有关 Active Directory 配置的信息（适用于 **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
- 有权与 Active Directory 通信的管理员帐户的帐户名和密码

为存储区域控制器配置 **Citrix ADC**

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

1. 登录到 Citrix ADC 设备，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. 提供向导中要求的信息。

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	此选项已启用，表示您将使用 Citrix ADC 连接用于 ShareFile Data 的存储区域。
用于网络文件共享/SharePoint 的存储区域连接器	如果使用连接器并且要在 Citrix ADC 上执行用户身份验证，请选中该复选框。
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，系统将提示您上传证书和私钥。对于标准区域，证书必须是公开信任的，而不是自签名的。
存储区域控制器 IP 地址	一个或多个存储区域控制器服务器的内部 IP 地址。这些 IP 地址将存储区域控制器服务器定义为 Citrix ADC 内的实体。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，请为每个存储区域控制器服务器输入一个内部 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 与存储区域控制器进行通信的端口和协议。

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 选项卡并选择服务器。
超时	Citrix ADC 等待来自 LDAP 服务器的响应的最大秒数。默认值为 3 秒。最小值为 1 秒。
单点登录域	Active Directory 域名。
基本 DN（用户的位置）	存储用户的 LDAP 基本唯一判别名 (DN)。使用以下常规格式指定 DN：CN=Users,dc=domain,dc=Net
管理员绑定 DN 和密码	有权与 Active Directory 通信的管理员帐户。
登录名	一个 LDAP 属性，由 Citrix ADC 用来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，它允许用户使用其用户名登录。要求用户输入其电子邮件地址才能登录，请将此字段更改为 UserPrincipalName。

配置 Citrix ADC 以通过 Web 访问连接器

要支持对存储区域连接器的 Web 访问，必须在完成 Citrix ADC for ShareFile 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。

如以下步骤所述，您将配置其他虚拟服务器，以允许客户端对 HTTP OPTIONS 动词进行匿名访问。OPTIONS 请求在没有经过身份验证且没有 HTTPS 标注的情况下传递到存储区域控制器来验证签名。CORS 预检检查会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/>。

- 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 (/proxyService)。

完成适用于 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) 单击直至创建虚拟服务器。
- 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，请执行以下操作：在“负载平衡虚拟服务器”屏幕中，在“服务”对面，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 Traffic Management（流量管理）> Content Switching（内容交换）> Policies（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，然后构建此表达式。选择 HTTP。选择“要求”。选择“方法”。选择均衡器（字符串），然后键入选项。该表达式应如下所示：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的部分，然后单击 2 内容交换策略。
- d) 单击 **Add Binding**（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低的数量。
值最低的策略的优先级最高，因此首先处理。

4. 更新用于存储区域连接器 (_SF_CIF_SP_CSPOL) 的流量的策略：

- a) 导航到 **Traffic Management**（流量管理）> **Content Switching**（内容交换）> **Policies**（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：

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

完整的策略表达式应如下所示：

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

5. 更新用于 ShareFile Data (_SF_SZ_CSPOL) 存储区域的流量的策略：

- 导航到 **Traffic Management**（流量管理）> **Content Switching**（内容交换）> **Policies**（策略）。
- 选择 **_SF_SZ_CSPOL** 策略。
- 将以下内容添加到策略表达式中：

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

完整的策略表达式应如下所示：

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

将 **Citrix ADC** 配置为仅供查看共享

要支持仅查看共享，用户必须能够访问你的 Microsoft Office Web 应用服务器 (OWA)。如果您的 OWA 服务器可以通过自己的地址从外部访问，则存储区域控制器不需要额外的 Citrix ADC 配置。

如果要使用 Citrix ADC 内容交换策略将存储区域控制器和 Office Web App Server 合并到单个外部地址上，则必须在完成 Citrix ADC for ShareFile 向导后执行其他 Citrix ADC 配置。需要配置 Citrix ADC，以确保流量正确路由到外部可访问的 OWA 服务器。

配置以下 Citrix ADC 规则后，管理员可以重复使用其存储区域控制器区域的现有外部地址，而无需为 OWA 创建额外的外部地址。

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

1. 创建额外的负载均衡服务。

- 导航到流量管理 > 负载均衡 > 服务。
- 单击添加。
- 输入所需信息以创建与您的 OWA 服务器相对应的服务。单击确定。

2. 创建额外的负载均衡虚拟服务器：

- 导航到流量管理 > 负载均衡 > 虚拟服务器。
- 单击添加。
- 指定以下值：

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

- 单击直至创建虚拟服务器。
- 要将虚拟服务器绑定到您在上一步中创建的 OWA 服务，请单击 负载均衡虚拟服务绑定 > 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您的 OWA 服务器的新策略。

- 导航到 **Traffic Management**（流量管理）> **Content Switching**（内容交换）> **Policies**（策略）。
- 选择添加。
- 为策略命名。
- 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. 在负载均衡虚拟机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。
- 单击负载均衡虚拟服务器，然后选择内容交换策略。
- 更改策略的优先级，使（示例）“_SF_OWA” 策略的优先级排在第三位。

优先级	策略名称
90	SF_ZK_OPTIONS
95	_SF_CIF_SP_SPOL
99	_SF_OWA

优先级	策略名称
100	_SF_SZ_CSPOL

- 单击关闭。单击“完成”

为存储区域控制器服务创建监视器

默认情况下，Citrix ADC ping 存储区域控制器服务器以确定其是否处于联机状态。但是，即使控制器处于联机状态，它也可能无法向 ShareFile 网站发送心跳消息。在这种情况下，Citrix ADC 将向存储区域控制器发送流量，尽管它不与 ShareFile 进行通信。

要验证存储区域控制器与 ShareFile 的出站连接，您可以创建一个监视器来检查 heartbeat.aspx 并将其绑定到每个存储区域控制器的 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 是对应于存储区域控制器的 Citrix ADC 服务。该服务名称是由 Citrix ADC for ShareFile 向导自动创建的。服务名称包括控制器的 IP 地址，例如 sf_svc IP-address。

如果服务正在监听端口 443，则需要-secure 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**，查看向导创建的负载平衡虚拟服务器的状态。

通过 Citrix ADC 查看 ShareFile 请求的吞吐量

吞吐量统计信息可以在 仪表板 菜单中找到。

手动配置 Citrix ADC

January 4, 2023

从版本 10.1 build 120.1316 开始，NetScaler 包含一个向导，用于配置存储区域控制器数据和连接器所需的设置。

本节中的步骤描述了存储区域控制器所需的 **Citrix ADC** 设置。所有链接均适用于 NetScaler 10.1 文档。类似的主题也适用于更高版本的 Citrix ADC。

检查所有传入邮件上是否有有效的 **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，输入任何存储区域控制器的虚拟服务器 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，选择返回布尔类型。
- h) 在从响应中提取数据的表达式中，输入：


```
HTTP.RES.STATUS.EQ(200).NOT
```
- i) 单击创建。

2. 按照前面的步骤配置名为 `sf_callout_y` 的 HTTP 标注。除了表达式之外，使用相同的设置：

- 在 URL 干表达式中，输入：

```
1  "/validate.ashx?RequestURI=" + HTTP.REQ.URL.HTTP_URL_SAFE.
    B64ENCODE + "&h="
```

3. 配置响应程序策略：

- a) 在“配置响应程序策略”对话框中：对于“操作”，选择“删除”。
- b) 输入表达式：

```
1  http.REQ.URL.CONTAINS("&h=") && http.req.url.contains("/
    crossdomain.xml").not && http.req.url.contains("/validate.
    ashx?requi").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?requi").not && SYS.HTTP_CALLOUT(sf_callout_y)
```

有关详细信息，请参阅[响应程序](#)。

4. 将响应程序策略绑定到[负载均衡器虚拟服务器](#)并配置 [基于 SSL 会话的持久性](#)。

实现负载均衡

1. [配置基于令牌的负载均衡](#)。

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

在高可用性部署中, 存储区域控制器需要基于令牌的负载平衡。循环负载平衡会导致间歇性下载或上载失败, 因为客户端的上载或下载请求可能会被定向到存储区域控制器, 而不是收到来自 ShareFile.com 的授权请求的存储区域控制器。

2. 将 Citrix ADC 配置为终止 SSL 连接。

有关信息, 请参阅 [配置 SSL 卸载](#)。

为连接器配置内容切换和身份验证

1. 要启用内容切换, 请参阅 [启用内容切换](#)。

2. 为用户从本地存储区域请求 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。这些步骤使用名称为 Data_Requests。

b) 输入表达式:

```
1 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交换策略。

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 Connector_Requests 的名称。

b) 输入表达式:

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

一定要将“StorageZonesControllerFQDN”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 (内容交换)”对话框中, 为 Data_Requests 策略指定 ShareFile 数据的存储区域的负载平衡器虚拟服务器。

此负载平衡器虚拟服务器是在步骤 4 中绑定响应程序策略的服务器, 用于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_Requests 策略，为存储区域连接器指定负载均衡器虚拟服务器。

6. 为存储区域控制器配置身份验证虚拟服务器：

尽管对 Citrix ADC 的身份验证是可选的，但这是推荐的最佳做法。

- a) 在导航窗格中，展开负载均衡，为存储区域连接器选择负载均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（负载均衡）”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”，选择 **COOKIEINSERT**。
- f) 对于超时（分钟），输入 **240**。

建议使用 240 分钟的超时值。使用大于 10 分钟的最小值。

有关更多信息，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”对话框创建和配置身份验证服务器。

在 SSO 名称属性中，输入 **userPrincipalName**。

有关其他设置的更多信息，请参阅[身份验证策略](#)。

8. 为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，然后选择在上一步中配置的身份验证服务器。
- b) 输入表达式：

```
ns_true
```

有关更多信息，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 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，输入存储区域控制器的域名。
- e) 为前三个项目分别选中“覆盖全局”复选框。

有关更多信息，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
```

有关更多信息, 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, 然后对于协议, 选择 **SSL**。
- c) 选中“验证用户”复选框。
- d) 在“身份验证策略”下, 单击“主策略”, 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。

有关更多信息, 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

November 9, 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存储缓存。有关存储缓存的更多信息, 请参阅 [自定义存储缓存操作](#)。

存储区域控制器使用 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。您可以使用命名用户帐户而不是网络服务帐户来访问共享。使用网络服务帐户运行 IIS 应用程序池和 Citrix ShareFile 服务。

1. 如果要使用命名用户帐户而不是网络服务帐户来访问共享, 请在 Active Directory 中创建一个命名用户帐户。我们将指定的用户帐户称为 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对包含 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. 连接到将托管网络共享的服务器, 并为您的 ShareFile 私有数据创建一个文件夹。
3. 右键单击文件夹, 然后选择“与特定人员共享...”
4. 添加将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，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。这将使某些类型存储阵列的每个区域的最大文件数从不到 50 万增加到 1,000 万或更多。如果需要额外容量，可以更改默认设置。

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，划分的存储布局有 256 个顶级文件夹，每个文件夹包含 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数限制为 256。

使用相同的公式（16 到 N 的幂），您可以为您的网站确定适当的值。例如，`PathSelectionParams=3,4,4,4` 将顶级文件夹的数量限制为 4096（16 的 3 次幂）。第二个值将顶级文件夹的子文件夹的数量限制为 65536（16 的功率为 4）。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。文件删除服务将从树底部开始删除空文件夹，直到它到达非空文件夹。

但是, 某些升级路径可能不会更新您的设置。升级后, 验证以下项是否显示在 `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config` 中:

```
<add key="DeleteEmptyFoldersAfterFileDeletion" value="1" />
```

如果您需要添加密钥, 请在完成后重新启动文件删除服务。

安装 **SSL** 证书

November 9, 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。

准备好您的服务器存储 **ShareFile** 数据

November 20, 2023

对于 ShareFile 数据的存储区域和存储区域连接器, 本节中描述的 Web 服务器 (IIS) 角色和 ASP.NET 设置是必需的。这些说明基于 Windows Server 2012, 但对更高版本也有效。

更新 **Microsoft .NET** 版本

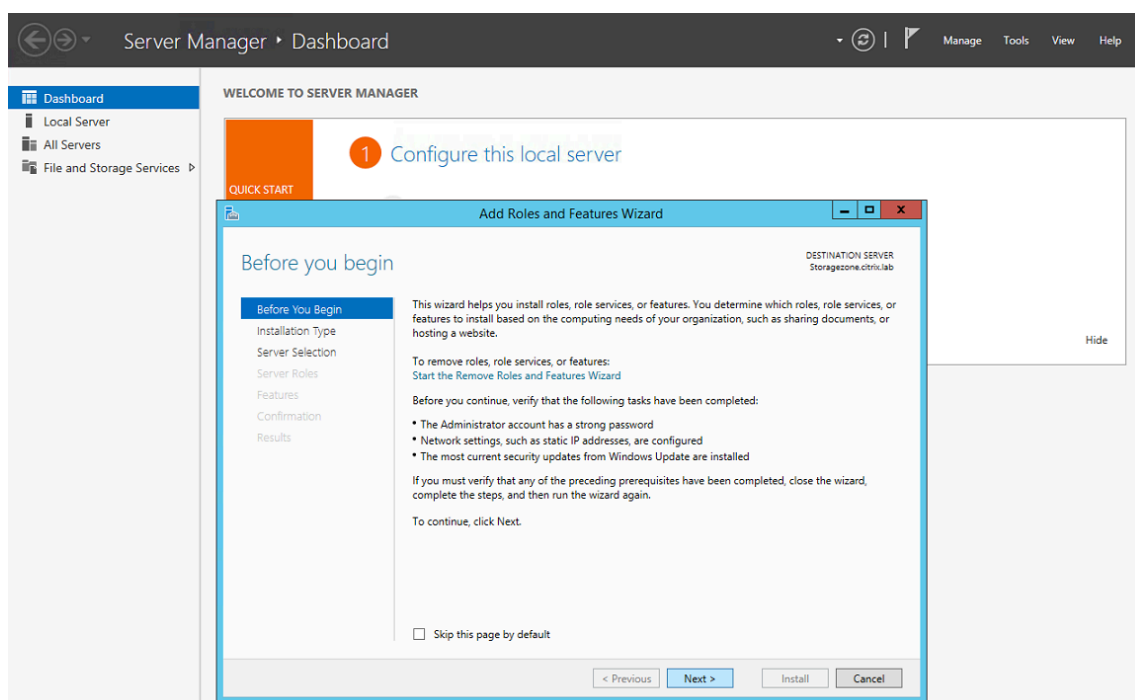
在继续安装存储区域控制器之前, 请确保您使用的是适当版本的 Microsoft .NET Framework。

- 存储区域控制器 **5.x** 需要 **.NET 4.8** 或更高版本。 [单击此处下载.NET 4.8](#)

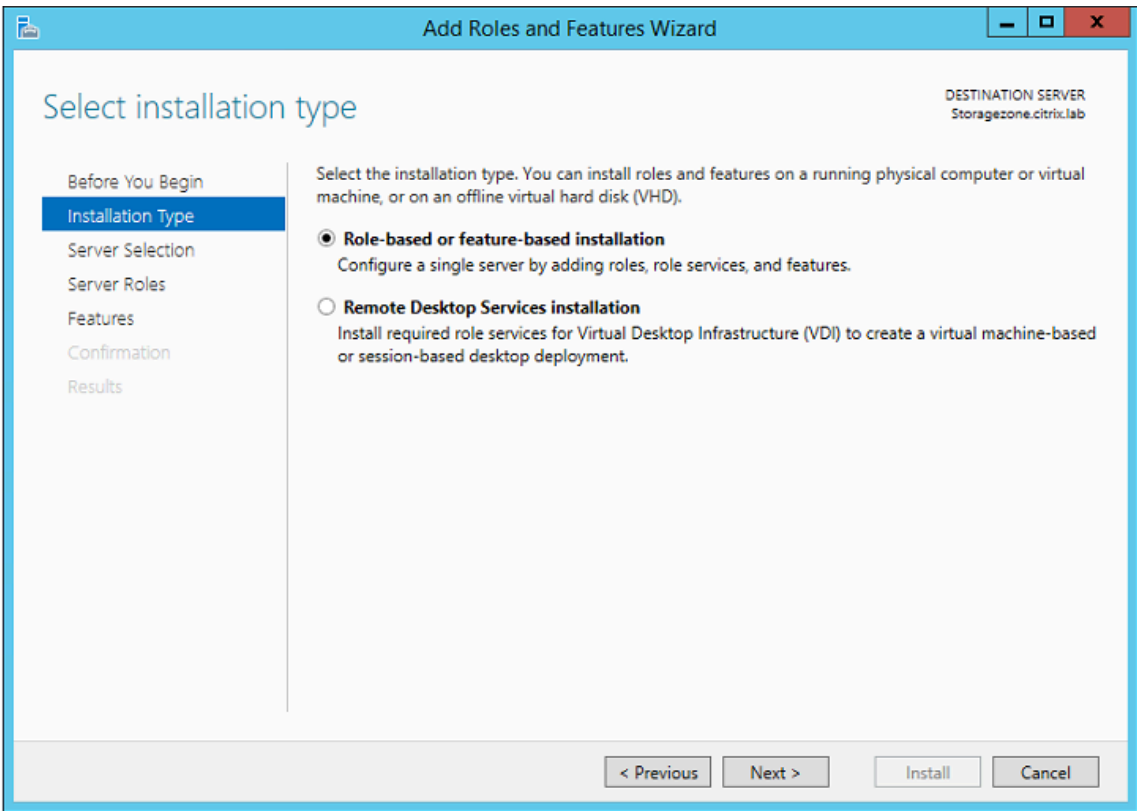
ShareFile 建议在使用 ShareFile 应用程序时使用最新版本的 Microsoft .NET。

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

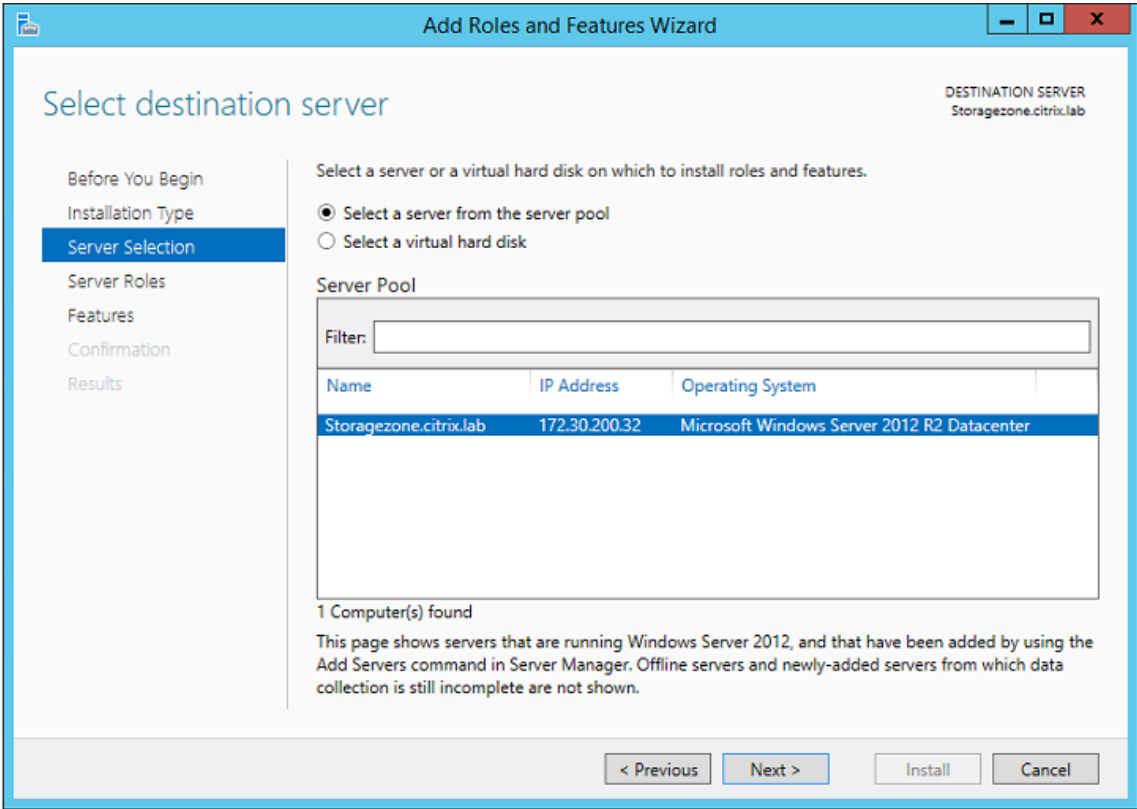
1. 在安装存储区域控制器的服务器上，使用具有本地管理员权限的帐户登录。
2. 打开 Server Manager 控制台控制台，然后单击“管理”>“添加角色和功能”以打开“添加角色和功能向导”。
3. 在“添加角色和功能向导”中，单击“下一步”。



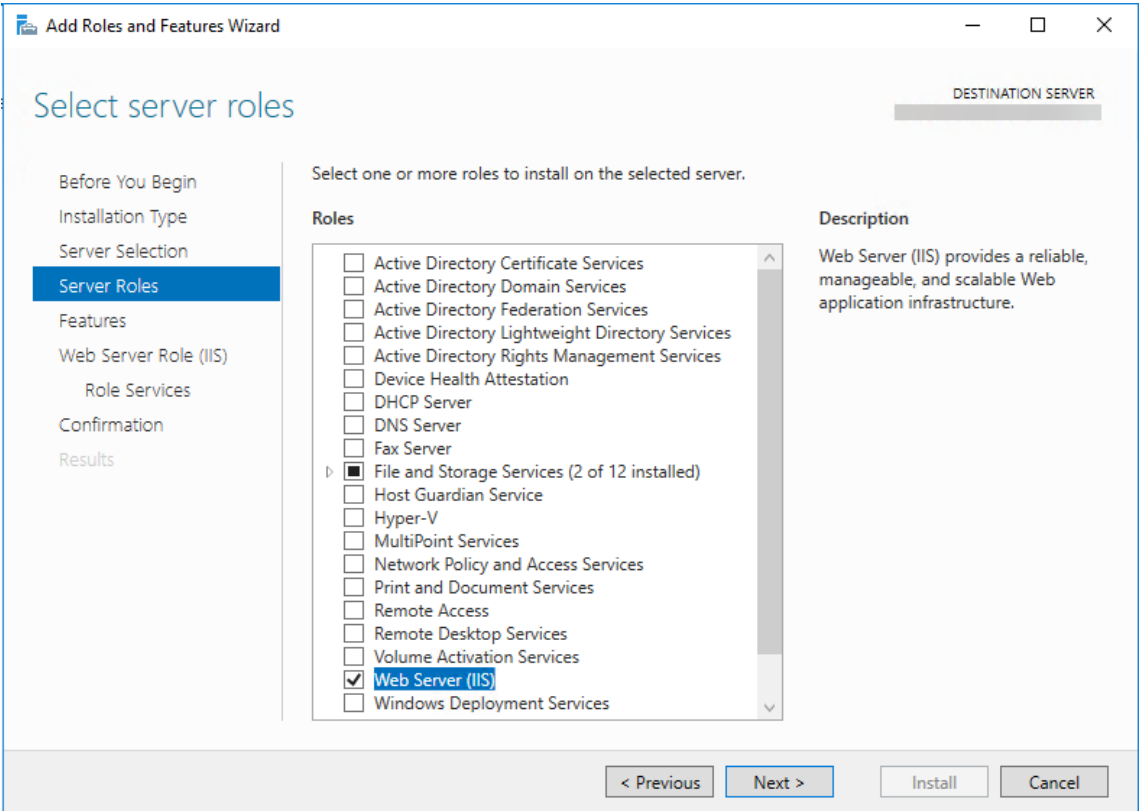
4. 在“选择安装类型”页面上，单击“基于角色或基于功能的安装”，然后单击“下一步”。



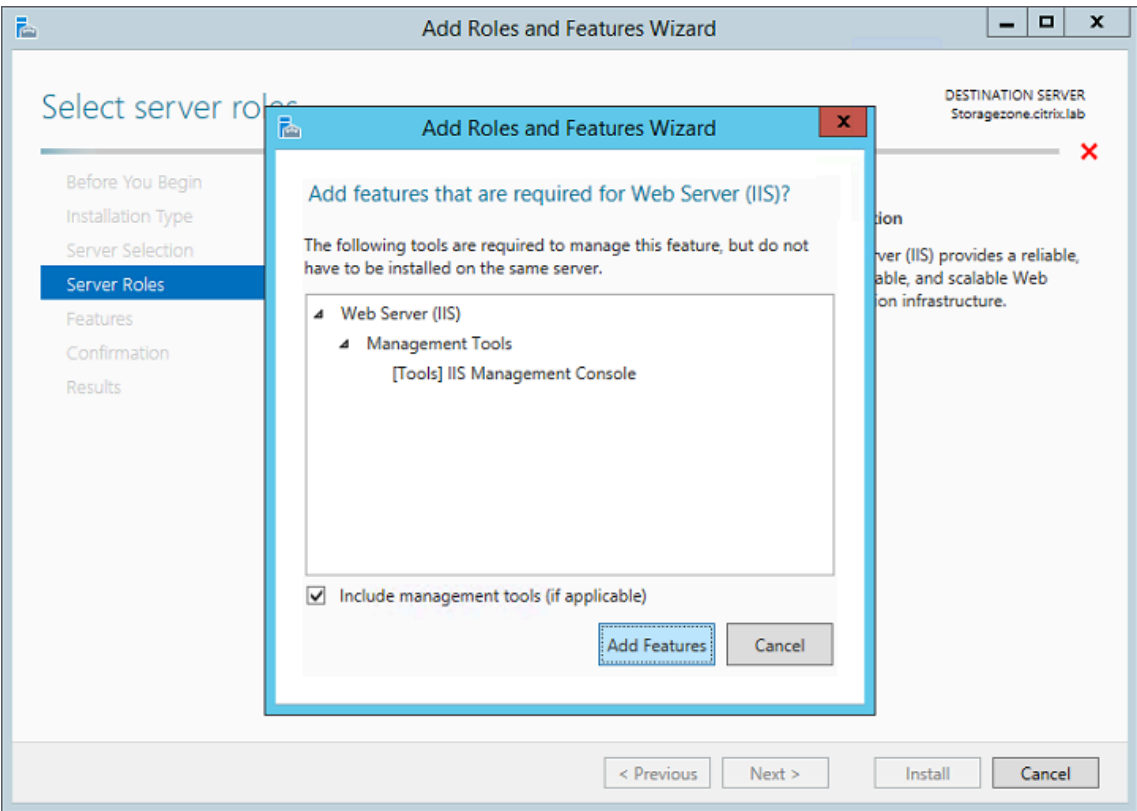
5. 在“选择目标服务器”页面上，从服务器池中选择您的服务器，然后单击“下一步”。



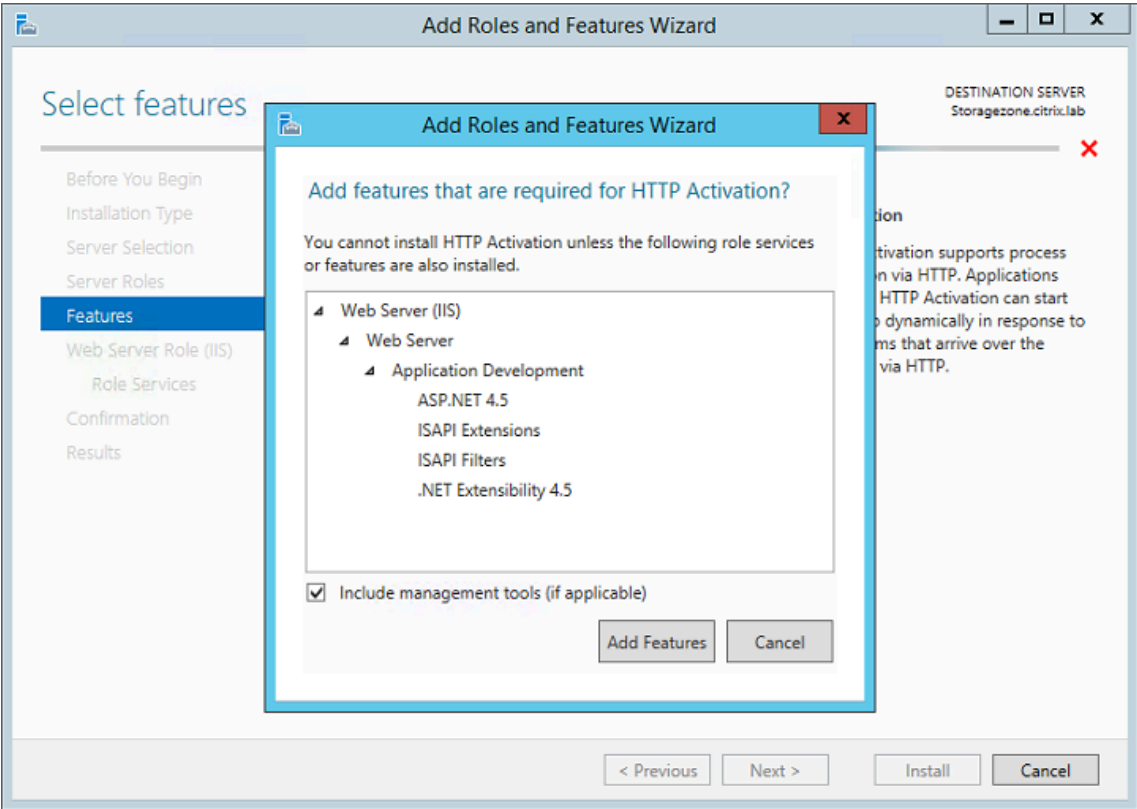
6. 在“选择服务器角色”页面上，选中 Web 服务器 (IIS) 复选框，然后单击“下一步”。



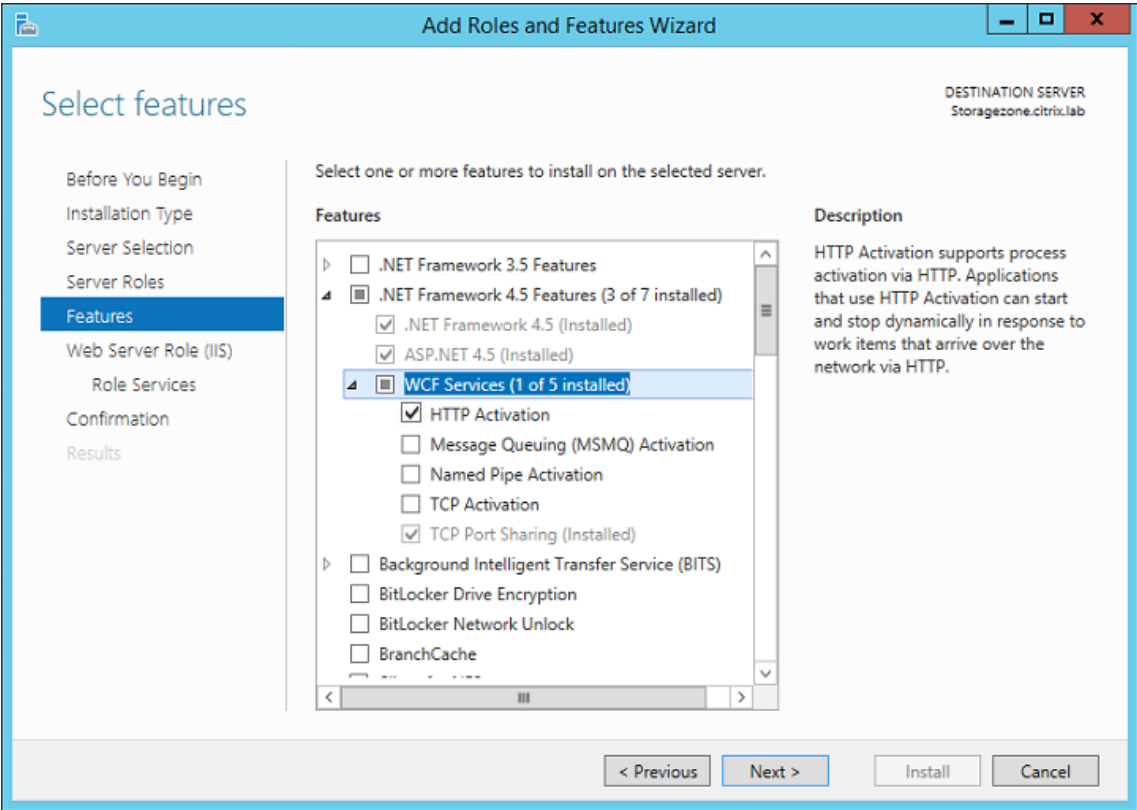
7. 单击“添加功能”添加 IIS 所需的功能。



8. 单击“添加功能”。将出现“选择功能”页面。

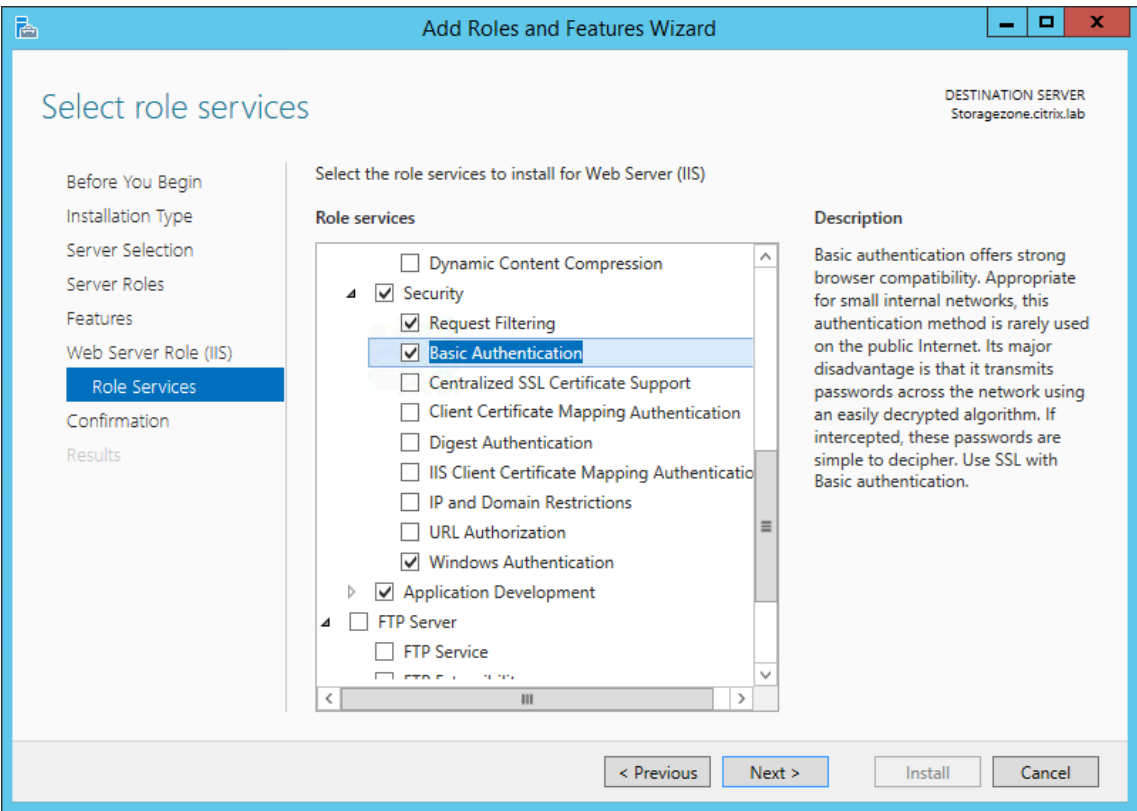


9. 选择以下屏幕中显示的所需设置，然后单击“下一步”。



10. 在 Web 服务器角色 (IIS) 页面上，单击“下一步”。

11. 在“选择角色服务”页面上，选中“基本身份验证”和“Windows 身份验证”复选框，然后单击“下一步”。

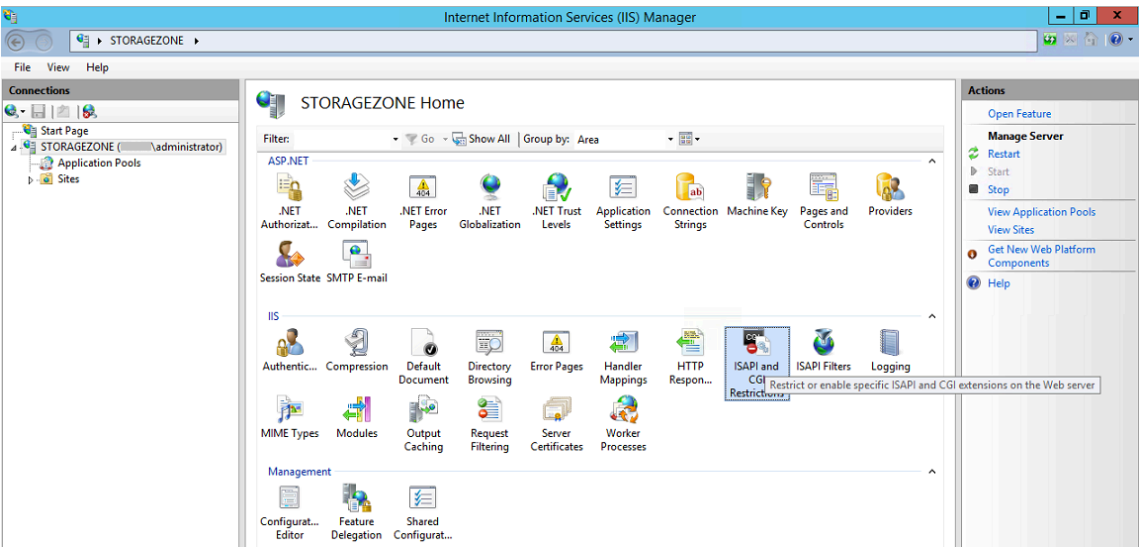


- 12. 在“确认安装选择”页面上，单击“安装”。
- 13. 安装完成后，单击“关闭”，然后重新启动服务器。

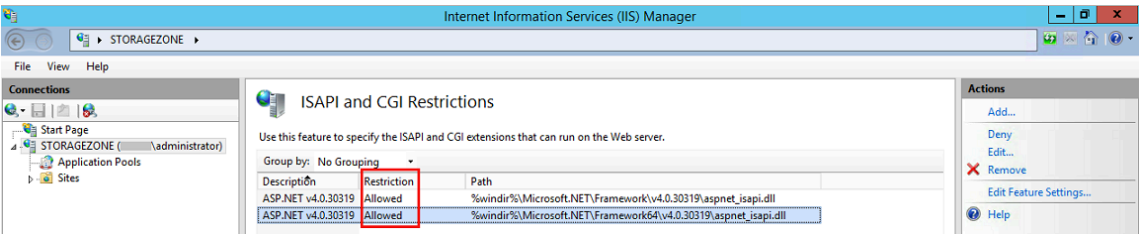
配置 IIS

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

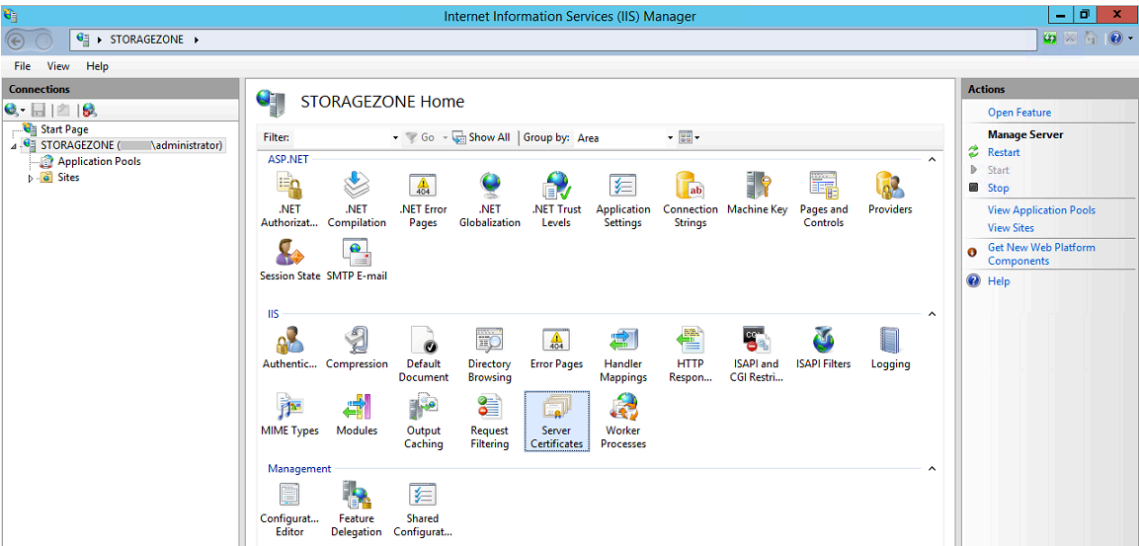
- 1. 打开 IIS 管理器控制台，单击存储区域控制器服务器节点，然后双击 ISAPI 和 CGI 限制。



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共证书：在 IIS Manager 控制台中，单击存储区域控制器服务器节点，然后双击“服务器证书”。

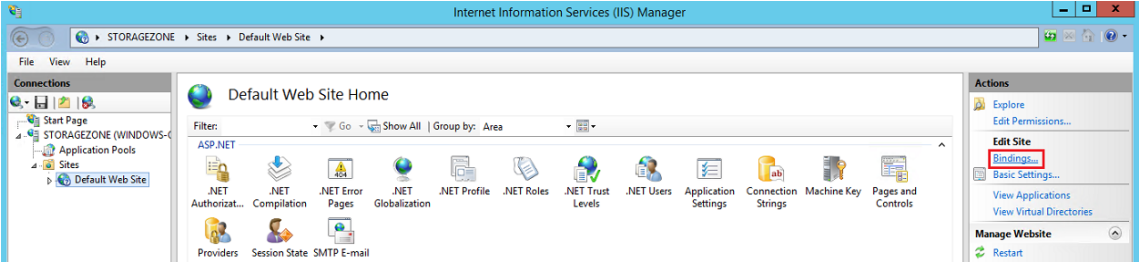


如果没有与公共证书颁发机构关联的证书，请先在服务器上安装证书，然后再继续。有关更多信息，请参阅 [安装 SSL 证书](#)。

注意：

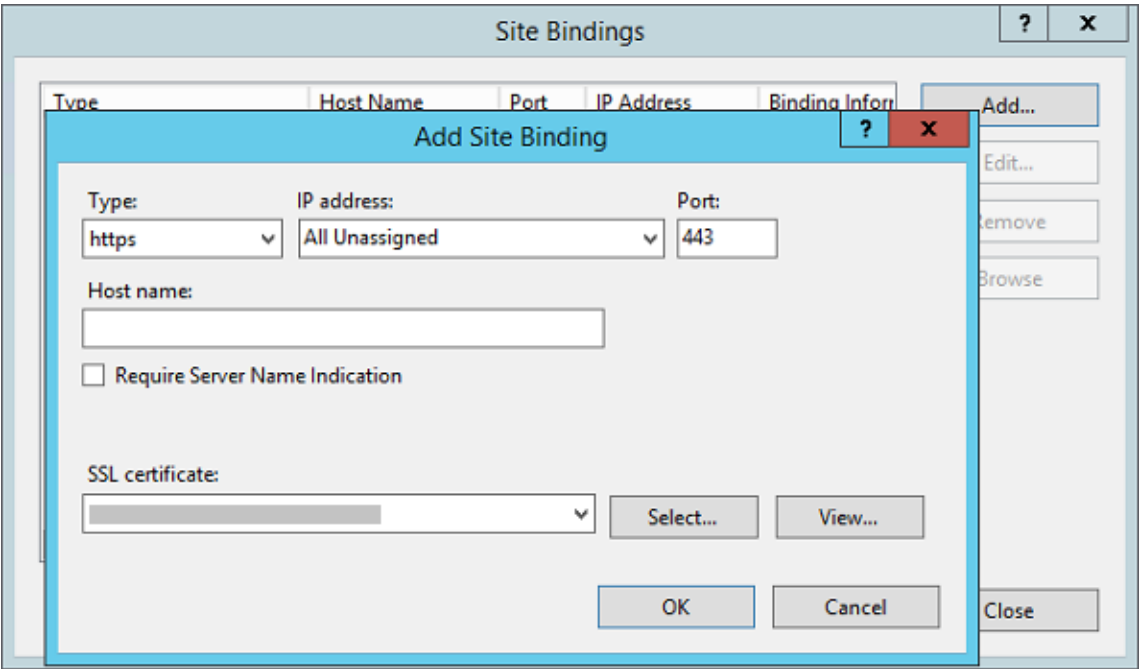
如果您使用的是带有存储区域控制器的 Citrix Gateway 或类似设备，则可以使用域服务器证书。标准区域的所有互联网流量都必须使用公共证书进行处理。

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”，按如下方式配置站点绑定：

- 类型是 https。
- IP 地址全部未分配。
- 端口为 443。
- SSL 证书是您安装的证书。



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，则会出现 IIS 徽标。

HTTPS 显示一条关于证书与 URL 标头中的本地主机名不匹配的消息。这是预料之中的，您可以放心地继续访问该网站。

7. 如果您要在虚拟机上安装存储区域控制器，请拍摄虚拟机的快照。

注意：

存储区域控制器使用 CORS，需要启用 **OPTIONS** http verb。请检查 IIS 请求筛选功能，确保 **OPTIONS** 动词未被禁用。

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

February 14, 2022

重要：

在开始安装 [系统要求](#) 之前，请验证您的环境是否满足。

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，用于允许用户访问 SharePoint 站点上的文档或指定的网络文件共享。

以下步骤介绍如何安装存储区域 Controller、为 IIS 默认网站配置身份验证、创建区域以及启用功能。

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：

安装存储区 Controller 会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 Controller 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 的编号。

- 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。
 - 在此键下创建一个新的 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样式的容器访问 (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: **true**
 - 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	出现在 ShareFile 管理员控制台中的名称。
主区域 Controller	默认值为 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，而不会出现 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。这应该是一个友好名称，而不是 FQDN。此名称将显示在 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”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。

- 选择一个存储库。

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以下附加注册表项：

- 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\storage zone\CloudStorageUploaderConfig`。
- 在此键下创建一个新的 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样式的容器访问（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：**true**
- 重新启动 StorageZones Controller 应用程序池 (StorageCenterAppPool)。

15. 要启用存储区域连接器：

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）。

- 选中要使用的每种连接器类型对应的复选框：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，请参阅本节中的[配置存储区域连接器](#)。
- 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 数据选项卡可以配置专用网络共享或受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，您必须创建一个新区域。
网络共享位置	您将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 <code>\\server\share</code> 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。如果配置页面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	网络共享位置的 UNC 路径的凭据。要使用命名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	仅当要对存储在文件共享中的文件内容进行加密时，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经受到第三方工具的保护，我们建议您不要加密共享上的文件。此设置与元数据无关。标准区域的元数据未加密。尽管此额外的安全性是在需要时提供最大安全性的选项，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（包括重复数据删除工具）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对存储进行加密。

选项	说明
密码	用于保护文件加密密钥的短语。密码短语必须包含六个以上的字符。请确保将密码短语和加密密钥存档到一个安全的位置。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。仅为 ShareFile 数据的存储区域保留此存储位置。网络服务帐户（或 Citrix ShareFile 管理服务配置为以运行身份的帐户）必须具有对此存储位置的完全访问权限。
共享缓存登录和共享缓存密码	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，您必须创建一个新区域。

选项	说明
帐户名称	Azure 存储帐户的名称。这些名称总是小写。
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”菜单包含指定帐户的所有可用容器之前，您无法继续配置。
容器名称	选择要用于此存储区域中的所有 StorageZones Controller 的 Azure 容器。在验证 Azure 访问密钥之前，此列表为空。

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	单击按钮以验证 Amazon S3 私有访问密钥。在验证完成并且存储桶名称菜单包含指定账户的所有可用存储桶之前，您无法继续配置。
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。在您的 Amazon S3 私有访问密钥验证之前，此列表将为空。

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	选中该复选框可通过安全连接连接到 SMTP 服务器。
用户名和密码	本地 SMTP 服务器的用户名和密码。
身份验证模式	默认身份验证模式使用最安全的方法从存储区域 Controller 连接到 SMTP 服务器。

选项	说明
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

通过 **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

您的 Google Cloud Platform 存储中的访问密钥 ID。

私有访问密钥

来自您的 Google Cloud Platform 存储的秘密。

验证

单击按钮以验证 Google Cloud Platform 的私有访问密钥。在验证完成并且 存储桶名称列表 包含指定账户的所有可用存储桶 之前，您无法继续配置。

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。在您的 Google Cloud Platform 秘密访问密钥验证之前，此列表将为空。

配置存储区域连接器

存储区域连接器允许用户访问 SharePoint 站点上的文档或指定的网络文件共享。您不必为 ShareFile 数据启用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到存储区域连接器的内部绑定连接。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。对于“拒绝路径”，该值无效。
- 如果允许的路径和拒绝路径相互冲突，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-Home 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-Home-Directory 值。

– %UserDomain%

重定向到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。

- 对于连接到根级 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 网站集的连接器：

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 file.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 SharePoint 2013 年 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

默认情况下，IIS/ASP.NET 会在 HTTP 响应中公开服务器标头。此标头可能对攻击者有用。标头会公开发送服务器类型，在某些情况下，还会显示版本号。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。

有关我们应在文档中提供的具体步骤，请参阅以下文章：<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

验证您的 **StorageZones Controller** 设置

November 9, 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. 验证心跳状态是否具有绿色复选标记。

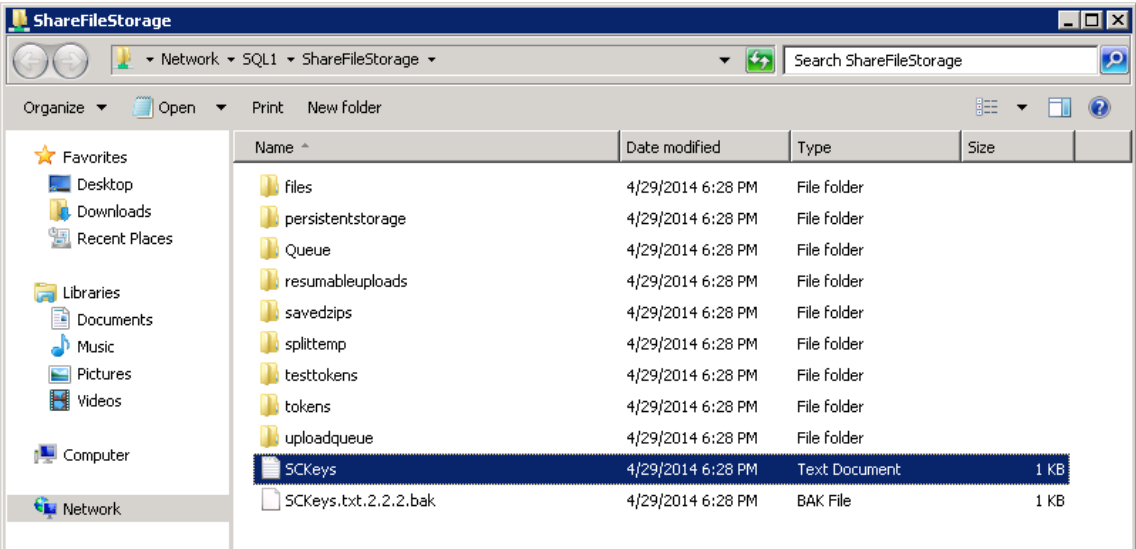
红色图标表示 ShareFile.com 未接收检测信号消息。在这种情况下，请验证从 StorageZones Controller 到 www.ShareFile.com 的网络连接，并验证从外部 PC 到 StorageZones Controller 的 URL 的网络连接。对于标准区域，StorageZones Controller 必须能够在端口 443 上使用有效的可信公共 SSL 证书访问。

升级后，从文件清理服务的 ShareFile 连接状态可能会临时显示一个红色图标。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，状态将返回为绿色图标。

3. 检查您的私有区域的连接：导航到您的私有区域的外部 URL（格式为 <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，请在内容交换和负载平衡虚拟服务器上查找数据的点击情况。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 sckey.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 sckey.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. 测试文件上传：登录 ShareFile Web 界面，创建分配给您刚刚配置的区域共享文件夹，将文件上传到该文件夹，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

April 23, 2021

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，请在用户置备期间选择存储位置。有关详细信息，请参阅 [基于 ShareFile 策略的管理](#) 文章中的 存储位置。

- 要更改单个用户的默认区域，请打开 ShareFile 管理员控制台，然后转到 管理用户。

指定存储区域的代理服务器

April 23, 2021

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。如果您使用的是 StorageZones Controller 2.2 到 2.2.2，则必须为每个辅助服务器手动向 Web.config 添加一个旁路列表，如[网站配置](#)中所述。

1. 在 StorageZones Controller 控制台 (<http://localhost/configservice/login.aspx>) 中，单击 网络选项卡。

注意：

如果您使用的是存储区域控制器 5.11.17，则更改任何代理都需要身份验证。出现提示时，输入您的账户的电子邮件地址、密码和完整账户 URL FQDN 子域，例如 subdomain.sharefile.com 或 subdomain.sharefile.eu。单击登录。

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. 选择一种身份验证模式，然后指定用于 ShareFile 代理访问的 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

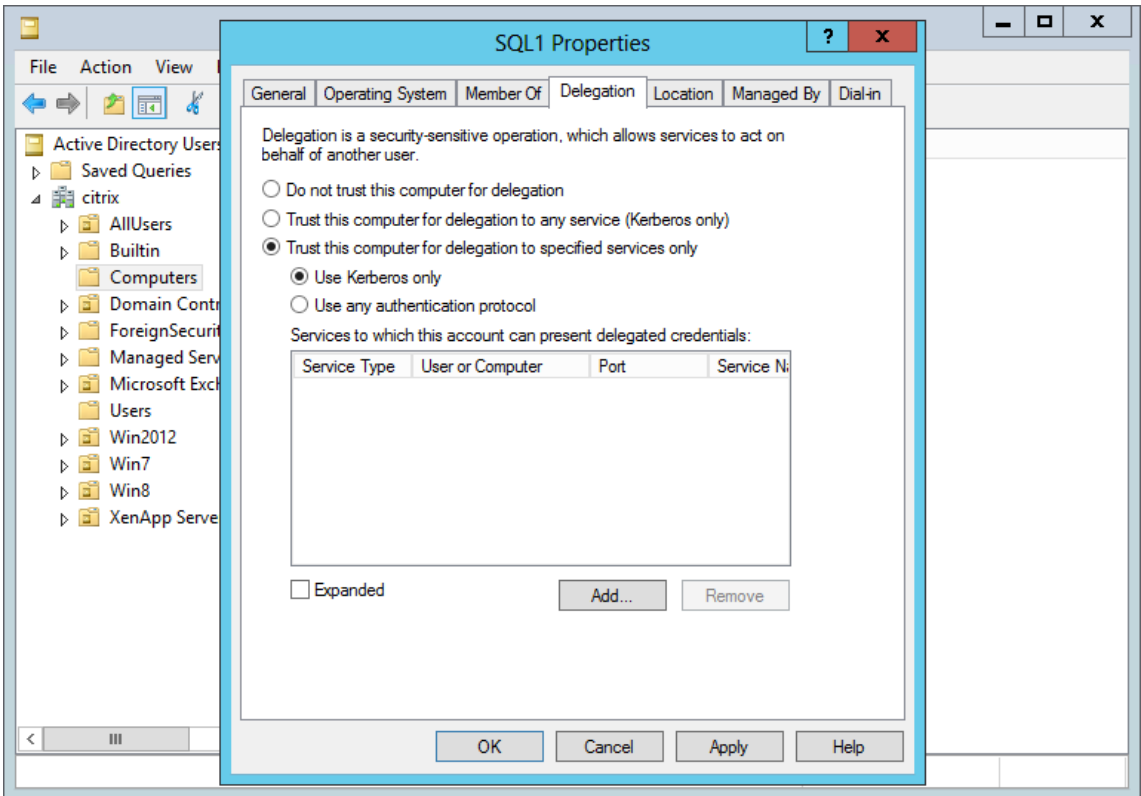
April 23, 2021

注意：

本节仅适用于存储区域连接器。

若要支持网络共享或 SharePoint 站点上的 NTLM 或 Kerberos 身份验证，请按如下方式配置域 Controller。

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”。

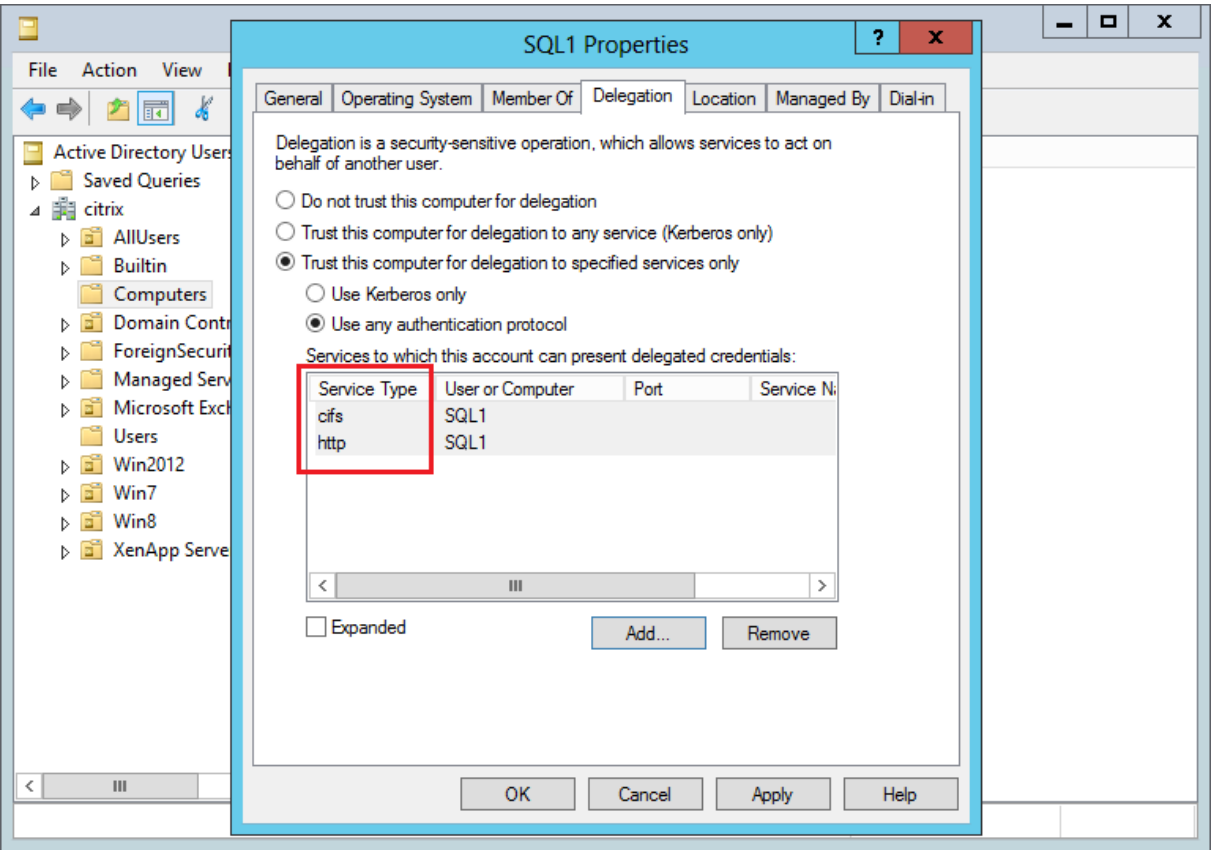


5. 对于 NTLM：

- 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** 应用程序预览、缩略图和仅限查看共享配置存储区域控制器

November 20, 2023

本地文件预览由您的本地 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，预览将由 Citrix 管理或 Microsoft 管理的 OWA 服务器呈现。

重要说明：

白名单要求：

* [.sf-api.com](https://sf-api.com) 必须允许您的 Office Online Server 访问才能在版本 5.0 或更高版本的存储区域上正常进行预览和编辑。

要求

本地文件预览支持的文件类型

- doc、.docm、.docx、.dot、.dotm、.dotx、.odt

- .ods、.xls、.xlsb、.xlsm、.xlsx
- .odp、.pot、.potm、.potx、.pps、.ppsm、.ppsx、.pptm、.pptm、.pptx
- .pdf
- 图像文件（bmp、gif、jpg、jpeg、png、tif、tiff、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 服务器应该能够访问 https://*.sf-api.com 和 https://*.sharefile.com（或.eu）
- SZC 服务器应该能够到达 OOS 服务器 <https://\<Customer OOS / OWA Endpoint\>/hosting/discovery>（例如，<https://oos.sharefileexample.com/hosting/discovery>）

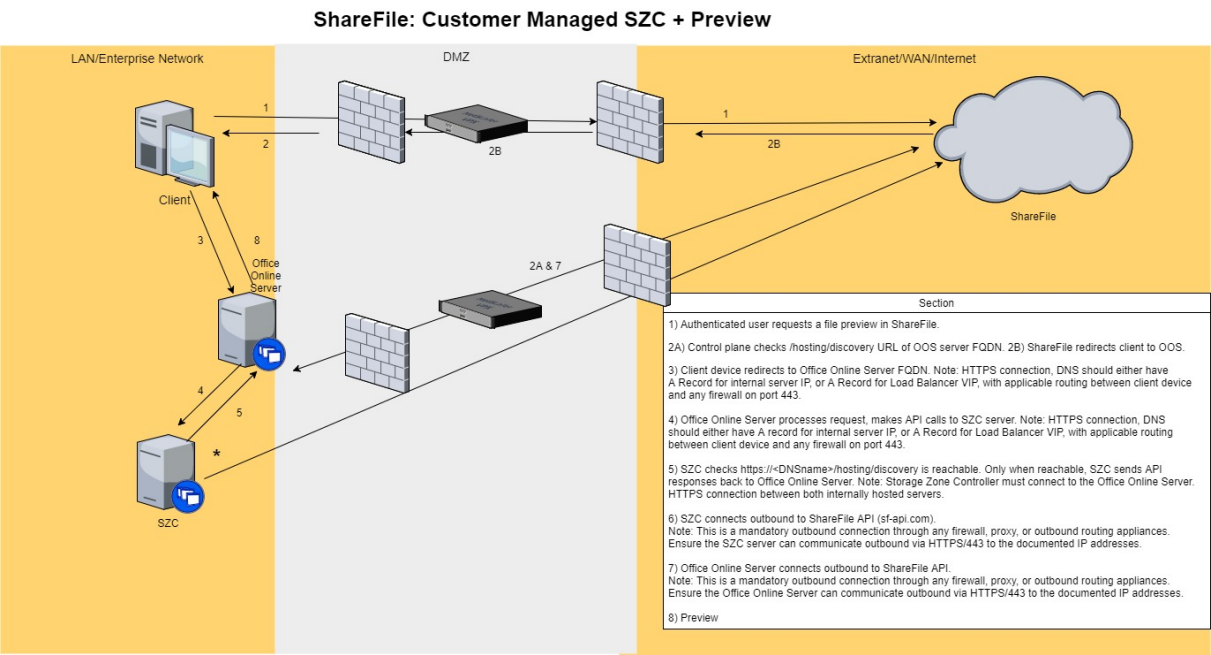
要编辑本地文件，必须在您的 ShareFile 帐户上启用[文件版本控制](#)。

在 ShareFile Web 应用程序高级偏好设置菜单中开启 Microsoft Office 在线编辑的设置不会影响编辑本地文件的功能。该特定开关不会控制您编辑本地文件的能力，但将适用于编辑存储在公共云中的任何文件。启用本地文件的编辑完全由存储区域控制器管理员按照下述步骤进行控制。

Microsoft 服务器兼容性

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

架构图和网络图



1. 经过身份验证的用户请求在 ShareFile 中预览文件。
2. ShareFile 使用 Office Online Server FQDN 向客户设备发出重定向消息
3. 客户端设备重定向到 Office Online Server FQDN。

注意：

HTTPS 连接，DNS 应该有内部服务器 IP 的 A 记录，或者负载均衡器 VIP 的 A 记录，并在端口 443 上提供客户端设备和任何防火墙之间的适用路由。

4. Office Online Server 处理请求，向存储区域控制器服务器发出 API 调用。

注意：

HTTPS 连接、DNS 应具有内部服务器 IP 的 A 记录或负载均衡器 VIP 的 A 记录，并在端口 443 上提供客户端设备和任何防火墙之间的适用路由。

5. 可以访问存储区域控制器检查 <https://<DNSName>/hosting/discovery>。只有在可以访问时，SZC 才会将 API 响应发回 Office Online Server。

注意：

存储区域控制器必须连接到 Office Online Server。两台内部托管服务器之间的 HTTPS 连接。

6. 存储区域控制器出站连接到 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的强制性出站连接。确保存储区域控制器服务器可以通过 HTTPS/443 向上面记录的 IP 地址进行出站通信。

7. Office Online Server 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的强制性出站连接。确保 Office Online Server 可以通过 HTTPS/443 向上面记录的 IP 地址进行出站通信。

8. 进行预览。

要让存储区域控制器将文件字节串流到 OOS，而不是 OOS 调用 ShareFile 控制平面来下载内容：我们需要更新存储区域控制器上其中一个配置文件中的密钥。

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

该配置文件有一个注册表项 **downloadFileFromSC**，当前设置为 **false**。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，说没有从控制平面到 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 控制平面仍会与 OOS 建立出站连接。

与另一种方法相比，使用一种方法有优点还是缺点？

在这种方法中，OOS 不会直接下载文件内容。存储区域控制器将文件字节下载并流式传输到 OOS。因此，它将增加存储区域控制器服务器的负载。

下载和流式传输文件字节是一项资源密集型任务。根据用户数量以及预览和编辑操作的数量，存储区域控制器服务器上的负载会增加。

启用本地预览和编辑

要支持浏览器内文档和图像预览、缩略图、存储在客户管理的存储区域中的数据的数据的仅限查看共享以及本地文件编辑，请按以下方式配置存储区域控制器：

1. 在存储区域控制控制台中，单击 **ShareFile** 数据选项卡。
2. 在“本地网络共享配置”部分中，启用“配置办公室 **Web** 应用程序预览”。
3. 输入您的 Microsoft Office Web 应用程序 (OWA) 服务器的外部 URL。
 - 用户必须通过订阅 Microsoft Office MSDN 下载和配置 OWA 服务器软件。

4. 选择“启用 **Office Online** 编辑”（如果需要）
5. 确认 OWA URL 可以从外部访问。
6. 验证您的 Office Online Server 是否可以与 ***.sf-api.com** 通信。
7. 在存储区域控制器控制台中，单击“监视”选项卡。
8. 确认 **OWA** 服务器连接 有绿色复选标记。

注意：

编辑本地 文件需要为 **ShareFile** 帐户启用文件版本控制。如果为该帐户禁用了文件版本控制，则本地编辑将无法运行。

重要说明：

配置时钟同步：

- 验证存储区域 Controller 上的时间是否已与时间.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 URL** 或禁用预览：

- 上述任一操作都要求为每个主控制器和辅助控制器重新启动 IIS 服务。

限制

- 移动应用程序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。

有关如何将 Citrix ADC 配置为仅限查看共享的信息，请参阅 [为存储区域控制器配置 Citrix ADC]。(/en-us/storage-zones-controller/5-0/install/configure-netscaler.html)

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。如果成功加载此页面，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

如果您在响应中收到警告或错误消息，请检查您的配置设置中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 服务器应该能够访问 https://*.sf-api.com 和 https://*.sharefile.com（或.eu）
- SZC 服务器应该能够到达 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

November 9, 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。

如果您是具有 ShareFile 预配的合作伙​​伴帐户的 CSP，则可以在域上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执行以下操作：

- 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，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。
- 更快地接纳新客户，并降低为每个客户帐户创建单独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。要应用云解决方案提供商计划，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，管理员用户可以是您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相关联。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 的编号。

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 [安装 StorageZones Controller 并创建存储区域](#) 中的步骤 10。

登录您希望在其中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。

现在，您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](#)。

当您请求租户帐户时，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，此合作伙伴管理员用户将作为管理员用户自动在该帐户上置备，并且能够登录和管理租户帐户。由于一个帐户中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。

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

在 Citrix 预配置请求的帐户后，您将收到一封电子邮件。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权限的激活链接。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。预配到租户帐户的任何新用户都将使用指定为用户文件默认位置的多租户区域。

使用 Office 联机服务器预览 Office 文件和 PDF

此功能受支持的 Office 联机服务器环境的支持。[点击这里了解设置信息](#)。

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 30, 2023

将存储区域控制器 **5.10** 或更高版本升级到最新版本

注意：

ShareFile 建议在更新和备份存储区域服务器配置之前拍摄服务器快照。要了解如何备份存储区域配置，请参阅 [备份主存储区域控制器配置](#)

有关升级存储区域控制器的问题，请参阅 [ShareFile 存储区域控制器升级故障排除](#)。

使用以下步骤升级存储区域控制器 5.10。

1. 从 [Citrix 下载页面](#) 下载最新版本的存储区域控制器软件。

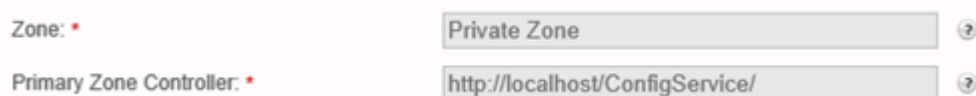
注意：

在升级和服务器重新启动期间，存储区域控制器不可用。为避免数据丢失，我们建议与用户安排一个维护时段。让他们知道升级期间该区域无法进行文件传输。

2. 在安装了存储区域控制器的 Windows 服务器上安装 MSI 文件。如果您有多台服务器，则应先将更新安装在主服务器上，然后安装在其他服务器上。有两种方法可以识别哪个服务器是主服务器：

- a) 从“配置”页面识别主存储区域控制器：

- 在控制器服务器上，从“开始”菜单导航到 <http://localhost/configservice/login.aspx> 或启动配置工具。需要“创建和管理区域”的权限才能访问配置。
- 在“数据”选项卡上，选中“主区域控制器”字段。该字段将主区域控制器的服务器主机名列为 <http://server/ConfigService>。



The screenshot shows a configuration interface with two fields. The first field is labeled 'Zone: *' and has a dropdown menu with 'Private Zone' selected. The second field is labeled 'Primary Zone Controller: *' and has a text input containing 'http://localhost/ConfigService/'. Both fields have a question mark icon to their right.

请注意，<http://localhost/ConfigService> 中的 localhost 表示此服务器是主区域控制器。

- b) 从注册表中识别主存储区域控制器：

- 在控制器服务器上，打开注册表编辑器 (regedit.exe)。
- 找到注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter
- 验证注册表项值 `isPrimaryConfigServer` 是否为 true。

3. 在主存储区域控制器上开始升级：

- a) 运行 StorageCenter.msi 启动 ShareFile 存储区域控制器安装向导。
- b) 响应提示。安装完成后，向导会显示消息“Citrix ShareFile 存储区域控制器安装向导已完成”。
- c) 重新启动服务器。

4. 在每个辅助存储区域控制器上（如果需要）：

- a) 运行 StorageCenter.msi 启动 ShareFile 存储区域控制器安装向导。
- b) 回应提示，然后选择“完成”。
- c) 重新启动服务器。

5. 在所有存储区域控制器上，重新启动所有区域成员的 IIS 服务器。

- a) 启动 CMD 提示符并以管理员身份运行。
- b) 键入 `iisreset` 然后按 **Enter** 键。如果成功，则提示符指示“Internet 服务已成功重新启动”。

c) 升级后，验证主存储区域控制器上的注册表设置是否正确。

6. 升级安装后，选择在任何区域成员上启动存储区域配置页面以登录并修改任何配置设置。

- 要随时返回存储区域控制器控制台，请打开 <http://localhost/configservice/login.aspx>。单击“完成”或返回存储区域控制器控制台后，将打开“登录”页面。

注意：

请记住，要登录存储区域控制器配置页面，您需要使用应用程序特定的密码。如果您需要创建新的应用程序专用密码，请参阅以下支持文章：[生成应用程序专用密码](#)。

- 要更改任何显示的信息，请选择 修改，进行更改，然后选择 保存。

注意：

在维护窗口结束之前，验证向每个存储区域控制器的数据传输是否正常。

管理存储区域控制器

February 14, 2022

安装主存储区域控制器和任何辅助存储区域控制器后，请使用以下过程来管理控制器并为灾难恢复做好准备。

要打开存储区域控制器控制台，请转到“开始”菜单 <http://localhost/configservice/login.aspx> 或从“开始”菜单启动配置工具。

管理存储区域控制器

- [将辅助存储区域控制器加入存储区域](#)
- [更改主 StorageZones Controller 的地址或密码](#)
- [降级和提升存储区域控制器](#)
- [禁用、删除或重新部署存储区域控制器](#)
- [将文件传输到新的网络共享](#)
- [备份主存储区域控制器配置](#)
- [恢复主 StorageZones Controller 配置](#)
- [更换主存储区域控制器](#)
- [准备存储区域控制器以进行文件恢复](#)
- [从您的 ShareFile 数据备份中恢复文件和文件夹](#)
- [将 ShareFile 云与存储区域协调一致](#)
- [配置上传文件的防病毒扫描](#)
- [迁移 ShareFile 数据](#)
- [连接器收藏夹](#)

将辅助存储区域控制器加入到存储区域

November 9, 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。然后打开 <http://localhost/configservice/login.aspx>，然后登录。
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，请将其输入到浏览器的地址字段中。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

February 14, 2022

注意：

只有帐户管理员才能更改地址或密码。

为主存储区域控制器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存储区域控制器的外部地址。

1. 在主存储区域控制器服务器上，打开 配置页面 或导航到：<http://localhost/configservice/login.aspx>。
2. 使用 ShareFile 管理员凭据登录到配置页面。
3. 在数据选项卡上，选择 修改。
4. 指定新的 外部地址 或 本地地址，然后选择 保存更改。
5. 对所有区域成员重复步骤。
6. 重新启动所有区域成员的 IIS 服务器。

更改主存储区域控制器的密码短语

注意：

更改存储区域控制器的密码短语需要当前的密码短语。

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。请确保将密码短语和加密密钥存档到一个安全的位置。

密码与您的帐户密码不同，如果丢失，则无法恢复。如果丢失了密码，则无法重新安装存储区域、将其他存储区域控制器加入存储区域，也无法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：登录其他每个成员的存储区域配置页面，并在出现提示时输入密码。
您必须为区域中的每个存储区域控制器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

November 9, 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提升为主服务器。

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 isPrimaryConfigServer 设置为 false。
- c) 使用表单 <https://IpAddress> 或 <https://hostname/ConfigService/> 将 PrimaryConfigServiceUrl 设置为将成为新的主存储区域控制器的服务器的 URL。
- 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 isPrimaryConfigServer 设置为 true。
- c) 将 PrimaryConfigServiceUrl 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) 使用表单 <https://IpAddress> 或 <https://hostname/ConfigService/> 将 PrimaryConfigServiceUrl 设置为将成为新的主存储区域控制器的服务器的 URL。
- c) 重新启动所有区域成员的 IIS 服务器。

禁用、删除或重新部署存储区域控制器

March 15, 2023

禁用存储区域控制器

注意：

如果每个存储区域控制器具有不同的外部地址，请使用此步骤。如果您对所有存储区域控制器使用相同的外部地

址，请从 Citrix ADC 接口禁用控制器。

在使服务器离线进行维护之前，请禁用存储区域控制器。

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，然后单击存储区域控制器主机名。
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。

删除存储区域控制器

删除存储区域控制器不会删除数据或 SCKeys.txt。如果您要删除主存储区域控制器，请在继续操作之前将其降级。

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，然后单击存储区域控制器主机名。
3. 单击删除。
4. 重新启动所有区域成员的 IIS 服务器。

重新部署存储区域控制器

重新部署存储区域控制器时不会丢失任何信息。

1. 从服务器上卸载存储区域。
2. 在 ShareFile Web 界面中，单击“管理员” > “存储区域”，然后选择您的区域。请勿删除该区域。
3. 选择存储区域控制器并将其删除。
4. 安装存储区域。暂时不要注册。
5. 运行存储区域控制器配置向导，将存储区域控制器加入区域并完成注册。
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

November 9, 2020

在为私有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。
- 在将任何数据传输到新共享之前，禁用新上传的存储区域控制器。在 Web 应用程序中，导航到“管理员设置” > “存储区域”。选择区域名称。在“存储中心”下，选择每个主机服务器。要终止到每个主机服务器的流量，请取消选择“服务器设置”下的“启用”选项。

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。作为最佳做法，切勿指定带有文件数据的位置的路径。仅为 ShareFile 数据的存储区域保留此存储位置。

4. 如果新网络共享位置的 UNC 路径的凭据与前一个不同，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。

备份主存储区域控制器配置

June 30, 2023

存储区域控制器安装在本地站点上，您负责对其进行备份。要完全保护您的部署，您应该拍摄存储区域控制器服务器的快照，备份配置，并 [准备存储区域控制器以进行文件恢复](#)。

请务必按照本主题中的说明备份配置。例如，如果您没有备份，但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 [存储区域控制器系统要求](#) 中的 PowerShell 脚本和命令。

存储区域控制器安装程序包括一个 PowerShell 模块，其中包含备份和还原主存储区域控制器配置设置的命令。您的备份包括区域、ShareFile Data 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的配置信息。

备份和还原命令要求您在与存储区域控制器相同的用户上下文中运行 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 <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec> 下载。

注意：

这些步骤不适用于辅助存储区域控制器。要恢复辅助存储区域控制器，请在服务器上重新安装存储区域控制器，然后将服务器加入主存储区域控制器。

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

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

例如，“远程签名”、“不受限制”或“绕过”策略允许您运行未签名的脚本。

b) 要更改你的 PowerShell 执行策略，请执行以下操作：`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
```

- 如果为存储区域控制器应用程序池使用指定用户：

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

将打开一个 PowerShell 窗口。

3. 在 PowerShell 提示符下，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，都需要导入模块。

4. 在 PowerShell 提示符下，运行 Get-SfConfig 命令并完成以下提示：

- **PrimaryZoneController** - 示例输入：
 - 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 问题无法连接到服务器名称，请连接到远程服务器：`http[s]://10.40.37.5/ConfigService/`
- 密码短语-为存储区域控制器指定的密码。

- 文件路径-示例 `c:\szc-backup.bak`

命令参数：

参数	说明	示例
“server”	主存储区域控制器服务器名称或 IP 地址。它可以是“示例”下所示的以下任何一种形式，并且必须包含尾部斜杠。	连接到本地服务器： <code>http://localhost/ConfigService/</code> ；连接到远程服务器： <code>http[s]://myservername.domain.com/ConfigService/</code> ；如果 DNS 问题阻止连接到服务器名称，则连接到远程服务器： <code>http[s]://10.40.37.5/ConfigService/</code>
“passphrase”	为存储区域控制器指定的密码短语。	“MyPassphrase”
“fullpath”	保存备份文件的位置。	“c:\szc-backup.bak”

Get-SfConfig 命令创建备份文件。

要恢复主存储区域控制器配置，请参阅 [恢复主存储区域控制器配置](#)。

恢复主 **StorageZones Controller** 配置

February 14, 2022

重要：

- 请确保在此过程中使用 PowerShell 4.0。有关 PowerShell 要求的更多信息，请参阅 [存储区域控制器系统要求](#) 中的 PowerShell 脚本和命令。
- 有关在整个系统范围内实施 TLS 的详细信息，请参阅 Microsoft 关于 [如何在客户端上启用 TLS 1.2](#) 的文章。

当主存储区域控制器被删除或出现故障时，存储区域控制器为灾难恢复提供以下选项：

- 如果辅助存储区域控制器可用，请将辅助控制器升级为主控制器。
- 如果辅助存储区域控制器不可用，并且您备份了主存储区域控制器配置（如 [备份主存储区域控制器配置](#) 中所述），请从备份文件中恢复主存储区域控制器。

- 如果您没有主存储区域控制器配置的备份，并且所有存储区域控制器都被意外删除或无法使用，则只能进行部分恢复。您可以恢复 ShareFile Data 的区域和存储区域配置，但不能恢复存储区域连接器。

从备份文件恢复主存储区域控制器

注意：

这些步骤仅适用于主存储区域控制器。要恢复辅助存储区域控制器，请在服务器上重新安装存储区域控制器，然后将服务器加入主存储区域控制器。

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

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

例如，“远程签名”、“不受限制”或“绕过”策略允许您运行未签名的脚本。

- b) 要更改你的 PowerShell 执行策略，请执行以下操作：`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：

从下载 PsExec.exe <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>，然后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：

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

- 如果为存储区域控制器应用程序池使用指定用户：

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

将打开一个 PowerShell 窗口。

3. 在 PowerShell 提示符下，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，都需要导入模块。

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：

- server 是主存储区域控制器服务器名称或 IP 地址。它可以是以下任何一种形式，并且必须包含尾部斜杠。

```
http://localhost/ConfigService/  
servername/ 或者 serverip/ （如果你使用 HTTP）  
http[s]://servername.domain.com/ConfigService/  
http[s]://serverip/ConfigService/
```

- 密码短语是为存储区域控制器指定的密码。
- fullpath 是备份文件的位置和名称。例如，c:\szc-backup.bak。

在没有备份文件的情况下恢复主存储区域控制器

如果没有备份文件，则可以恢复 ShareFile Data 的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
```

- 如果为存储区域控制器应用程序池使用指定用户：

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

将打开一个 PowerShell 窗口。

2. 在 PowerShell 提示符下，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，都需要导入模块。

3. 在 PowerShell 提示符下，运行 join-sfConfig 命令：

重要：

join-sfConfig 命令目前不支持 Azure 或 Amazon S3 存储。如果需要使用此命令，请联系 ShareFile 支持人员。

```
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：

- zoneID 可以通过以下方式获得：

- a) 在 ShareFile Web 界面中，依次单击“管理员”>“存储区域”，右键单击站点名称，然后选择“属性”。

显示的地址以如下所示的区域 ID 结尾：`zae4fb8c-8520-478f-8f87-aa589a8fd181`

。

- b) 将该 ID 复制并粘贴到 Join-SfConfig 命令中。

- StorageCenterID 可以通过以下方式获取：

- a) 在 ShareFile Web 界面中，依次单击管理员 > 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 Join-SfConfig 命令中。

- 只有在为区域启用了 ShareFile Data 的存储区域时，才需要 StorageZoneLocation。
- 仅当为该区域启用了 ShareFile Data 的存储区域并且您的存储位置需要身份验证时，才需要 StorageUsername 和 StoragePassword。
- 只有当 ShareFile 数据的存储区域存储在 Windows Azure 存储容器中时，才需要 AzureAccessName、AzureAccessKey 和 AzureContainerName。

4. 要恢复存储区域连接器，请使用存储区域控制器控制台 (<http://localhost/configservice/login.aspx>) 启用和配置连接器。

替换主 StorageZones Controller

November 9, 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。以下步骤可确保您的配置设置和所有数据都被传输。

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. 将备份的配置导入到新 Controller 上。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](#)。

准备存储区域控制器以进行文件恢复

September 11, 2023

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 到 7 天运行一次。

如何为文件恢复做准备取决于数据的存储位置：

- 支持的第三方存储系统 - 如果您使用带有存储区域控制器的第三方存储系统，则您的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中恢复文件。45 天后无法从 ShareFile 回收站中恢复文件。恢复期过后，文件将从区域中删除，从而从冗余的第三方存储中删除。如果恢复时间不足，请考虑以下解决方案之一：
 - 要防止 StorageZone Controller 文件清理服务从您的本地存储位置清除实际文件，请更改 `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config` 中“周期”设置的值。有关更多信息，请参阅 [自定义存储缓存操作](#)。请记住，延长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—如果您使用本地维护的共享进行私有数据存储，则您负责备份本地存储区域控制器的本地文件存储和注册表条目。ShareFile 存档在 ShareFile 云中存放了 3 年的相应文件元数据。

重要：为防止数据丢失，拍摄存储区域控制器服务器的快照、[备份其配置](#)并备份本地文件存储至关重要。

按照本主题所述为文件恢复准备存储区域控制器后，可以使用 ShareFile 管理员控制台执行以下操作：

- 浏览您的存储区域以查找特定日期和时间的 ShareFile Data 记录，然后标记要恢复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永久存储位置。

有关更多信息，请参阅 [从 ShareFile Data 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 云上的元数据与本地存储进行协调。ShareFile 协调功能会从 ShareFile 云中永久删除在指定日期和时间不再位于存储区域的文件的元数据。

有关更多信息，请参阅 [将 ShareFile 云与存储区域协调起来](#)

必备条件

- 具有 2 个 CPU 和 4 GB RAM 的专用物理机或虚拟机
- Windows Server 2012 R2（数据中心、标准版或基础版）
- Windows Server 2016
- Windows Server 2019
- Windows PowerShell（32 位和 64 位版本）必须支持 .NET 4 运行时程序集。有关更多信息，请参阅[存储区域控制器系统要求](#)中的“PowerShell 脚本和命令”。
- PsExec.exe - PsExec 允许您使用网络服务帐户启动 PowerShell。您也可以使用 PsExec 来安排恢复任务。从下载 PsExec.exe <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>，然后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，用于灾难恢复。

文件名	说明
DoRecovery.ps1	由 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。
recovery.log	存储恢复过程输出的日志文件。
recoveryerror.log	存储恢复过程中的错误的日志文件。
LitJson.dll	一个 .Net 库，用于处理与 JSON（JavaScript 对象表示法）字符串之间的转换。

设置备份文件夹

在备份服务器上，创建用于备份 persistentstorage 文件夹的文件夹。

ShareFile Data 文件备份的存储区域应遵循与存储区域控制器永久存储相同的布局。

如果您的备份位置与存储区域控制器永久存储的布局不同，则必须在恢复过程中执行其他步骤，将文件从备份位置复制到在 Recovery PowerShell 脚本中指定的位置。

存储布局

备份布局

```
1  \\PrimaryStorageIP
2  \StorageLocation
3  \persistentstorage
4  \sf-us-1
5  \a024f83e-b147-437e-9f28-e7d03634af42
6  \fi3d85dc_1d6c_49b0_8faa_1f36ef3d83b5
7  \fi7d5cbb_93c8_43f0_a664_74f27e72bc83
8  \fi47cd7e_64c4_47be_beb7_1207c93c1270
9
10 \\BackupStorageIP
11 \BackupLocation
12 \persistentstorage
13 \sf-us-1
14 \a024f83e-b147-437e-9f28-e7d03634af42
15 \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** 到 **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存储区域控制器安装文件夹。

1. 在存储区域控制器上，以管理员身份运行 PowerShell。
2. 此过程中使用的 PowerShell 脚本未签名，因此您可能需要更改 PowerShell 执行策略。
 - a) 确定您的 PowerShell 执行策略是否允许你运行本地未签名的脚本：PS C:\>Get-ExecutionPolicy
例如，“远程签名”、“不受限制”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：PS C:\>Set-ExecutionPolicy RemoteSigned
3. 要验证 PowerShell 的 CLRVersion 是否正确，请键入：

\$psversiontable

CLRVersion 的值必须为 4.0 或更高才能让 PowerShell 在脚本中加载 .NET 程序集。如果不是，请按如下方式在 Windows PowerShell 32 位和 64 位版本中对其进行更改：

- a) 以管理员身份运行记事本。
- b) 创建包含以下内容的文件。

```
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 \$psversiontable 以验证 CLRVersion 是否正确。

4. 关闭 PowerShell 窗口然后使用 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\powershell.exe

- c) 单击“同意”接受 PsExec.exe 许可协议。

5. 导航到存储区域控制器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：New-SCQueue -name recovery -operation recovery

该命令的输出包括创建的队列的名称。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：

\\server\(\您的主存储位置)\Queue。您会看到 Queue 文件夹，比如 92736b5d-1cff-4760-92c8-d8b04dc92cb2。

8. 如下一节所述，根据您的位置自定义恢复 PowerShell 脚本。

为您所在的位置自定义 **PowerShell** 恢复脚本

DoRecovery.ps1 PowerShell 脚本由任务调度程序执行，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. 在存储区域控制器上，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\YourBackupLocation"
- b. 将 \$storageRoot 参数设置为指向存储区域控制器永久存储的 UNC 路径。例如：\$storageRoot = "\\10.10.10.10\StorageLocation\persistentstorage"

测试恢复过程

1. 创建测试文件并将其上载到 ShareFile。
2. 一小时左右后，验证文件是否出现在永久存储中（在 \$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. 从永久存储中删除该文件。

此步骤重新创建 ShareFile 在删除文件 45 天后将执行的操作。

5. 在 ShareFile 管理员工具中，转到 管理员 > 存储区域，单击该区域，然后单击“恢复文件”。
6. 单击“恢复日期”文本框并选择文件删除之前和上载后的日期和时间。

此时将显示指定日期和时间的存储区域的文件列表。

7. 选中文件对应的复选框。
8. 选择要包含还原文件的文件夹，然后单击 还原。

该文件将添加到恢复队列中，并准备好恢复。成功恢复文件后，屏幕将更改为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：

```
1  ``
2  PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
   \WindowsPowerShell\v1.0\powershell
3  ``
```

- c. 在 PowerShell 窗口中，导航至：

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

- d. 运行恢复脚本：

```
.\DoRecovery.ps1
```

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

10. 从 ShareFile 网站下载恢复的文件。

相关的 PowerShell 命令

以下 PowerShell 命令支持灾难恢复。

- **Get-RecoveryPendingFileIDs**

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：

Get-Help Get-RecoveryPendingFileIDs -full

- **Set-RecoveryQueueItemsStatus**

为恢复队列中的所有或指定项目设置状态。这会覆盖队列中现有的恢复状态。对于语法和参数，请使用以下命令：

Get-Help Set-RecoveryQueueItemsStatus -full

创建和安排恢复任务

如果需要定时恢复任务，请按照以下步骤操作。

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. 为任务键入一个有意义的名称。
 - 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，即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. 对于“开始任务”，选择“按计划”，然后指定时间表。
5. 要创建动作，请在操作选项卡上单击新建。
 - a. 在“操作”中，选择“启动程序”并指定该程序的完整路径。例如：`C:\Windows\System32\cmd.exe`。
 - b. 对于“添加参数”，请键入：`/c "c:\windows\syswow64\WindowsPowerShell\v1.0\PowerShell.exe -File .\DoRecovery.ps1" >> .\recovery.log 2>>.\recoveryerror.log`
 - c. 对于开始位置，指定存储区域控制器安装位置中的“灾难恢复”文件夹。例如：`c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

删除服务默认期限

从 StorageZone Controller 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之前的所有设置。要修改默认时段，请在 `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc` 上编辑 `FileDeleteService.exe.config`

```
<!--No. of days to keep data blob in active storage after deletion-->
```

```
<add key="Period"value="45"/>
```

修改升级后的删除服务默认期限

在某些升级场景中，“FileDeleteService.exe.config”中的 DeletePeriod 值将设置为空。设置为 null 时，“删除期限”将默认为 45 天，即从 ShareFile 中删除的文件从物理存储中删除之前的默认天数。

要修改存储区域控制器上的 DeletePeriod，请在以下位置编辑 FileDeleteService.exe.config 文件：[C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config](#)

全新安装存储区域控制器后，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 FileDeleteService.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

November 9, 2020

通过 ShareFile 管理员控制台，您可以浏览存储区域中的特定日期和时间的 ShareFile 数据记录，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，将文件从备份恢复到存储位置。

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 Controller 系统要求](#)。

必备条件

- 完成中所述的设置和测试 [准备用于文件恢复的 StorageZones Controller](#)。安装程序包括有关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的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. 选择要包含已恢复文件的文件夹，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. 如果您的备份位置与存储区域永久存储不遵循相同的布局，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、未签名的脚本。在 PowerShell 窗口中执行以下操作：

`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) 要更改您的 PowerShell 执行策略：`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：

```
1 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：

```
1 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：

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

c) 在 PowerShell 窗口中，导航至：

`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永久存储位置。刷新控制台后，旋转图标从 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，文件恢复是立即进行的，并且 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。

协调 **ShareFile** 云与存储区域

November 9, 2020

导致本地存储中数据丢失的问题（如磁盘故障）会导致本地存储和存储在 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，以便在指定日期和时间不再在存储区域中的文件的元数据从 ShareFile 云中永久删除。

小心：

仅当本地文件存储中存在不可恢复的数据丢失时，才执行协调。协调会从 ShareFile 云中永久删除截至指定日期和时间在本地文件存储中找不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。

Windows Server 2012R2 ShareFile 存储区域迁移指南

November 20, 2023

重要：

Microsoft 将于 2023 年 10 月 10 日终止对 Windows Server 2012R2 的支持。务必在支持终止日期之前将服务器迁移到较新的版本。

本文提供了有关如何将 ShareFile 存储区域服务器从 Windows Server 2012R2 迁移到新版本的指导。

要迁移到较新版本的 Windows Server，必须向新服务器添加辅助存储区域控制器，然后将其升级为主控制器。

系统要求

存储区域控制器服务器支持以下版本：

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

说明

注意：

以下步骤不包括迁移 ShareFile 数据存储库。如果您将 ShareFile 数据存储库与计划迁移的存储区域控制器位于同一台服务器上，或者在运行 Windows Server 2012R2 的文件服务器上有要迁移的存储区域数据存储库，请参阅[将文件传输到新的网络共享](#)以了解更多信息。

步骤 1 - 为 **ShareFile** 存储区域控制器准备新服务器

使用[为 ShareFile 数据准备服务器](#)中提供的步骤准备新服务器。

步骤 2 - 在新服务器上安装存储区域控制器并将其添加为辅助服务器

为 ShareFile 准备好新服务器后，需要将其作为辅助服务器添加到存储区域。有关更多信息，请参阅[将二级存储区域控制器加入存储区域](#)。

步骤 3 - 将新服务器升级为主服务器，将旧服务器降级为辅助服务器

将新服务器添加为辅助服务器后，下一步是将其升级为主服务器。还必须将较旧的服务器降级为辅助服务器。有关此步骤的更多信息，请参阅[降级和升级存储区域控制器](#)。

注意：

ShareFile 建议您自行测试新存储区域服务器的功能，不要使用较旧的服务器作为辅助服务器。您可以通过暂时禁用旧服务器来实现此目的。有关更多信息，请参阅[禁用存储区域控制器](#)。

步骤 4（可选）- 添加其他辅助服务器

如有必要，对于每增加一台辅助服务器，请返回[步骤 2 - 在新服务器上安装存储区域控制器并将其添加为辅助服务器](#)。

步骤 5（可选）- 更新 **NetScaler** 服务组成员

如果您有 NetScaler，请确保将新的存储区域服务器添加到 ShareFile 服务组中。有关详细信息，请参阅[使用配置实用程序向服务组添加成员](#)。

第 6 步 - 从 **ShareFile** 管理门户中删除旧的存储区域控制器服务器

成功迁移存储区域服务器后，可以从 ShareFile 管理门户中删除较旧的服务器。有关更多信息，请参阅[删除存储区域控制器](#)。

配置上传文件的防病毒扫描

July 1, 2022

重要：

由于更新了 StorageZones 4.2 中的应用程序代码，一些客户必须将运行该工具的权限级别从本地管理员更新为系统网络服务。未能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 必须使用 pSExec 作为网络服务运行
- 更新日志文件位置

使用 **PSExec** 将 **SFAntivirus** 作为网络服务运行：

要更新到 SZ 4.2 或更高版本且现有计划任务链接到 SFantiVirus 的客户端，需要将运行该工具的用户级别从本地管理员更改为系统网络服务。

要获得网络服务权限，请使用 psexec 在与存储区域控制器相同的用户上下文中启动 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

管理员还必须通过编辑 log4net.config 条目来更改日志文件位置（如果他们登录到默认 SZC 日志目录之外的目录），方法是修改以下行：

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

存储区域控制器安装包括多个支持防病毒扫描的文件。默认情况下，这些文件安装在 C:\inetpub\wwwroot\Citrix\StorageCenter\T

自定义配置文件并使用 Windows 任务计划程序安排扫描（如以下步骤中所述）后，每个文件上传请求都会导致存储区域控制器将文件排队以进行防病毒扫描。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 开始，可以配置防病毒日志文件的位置。要修改日志位置，请在 C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus 处编辑 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 ICAP 协议用于已编码为 ICAP 的 RFC 标准的防病毒扫描平台。有关配置 ICAP AV 的信息可以在本文的下方找到。

注意：

在您的区域中配置防病毒后，将扫描所有新上载的项目。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. 要在存储区域控制器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 复制到其他服务器。
 - b) 在存储区域控制器上,打开 C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config 并将 QueueSDKRestricted 设置为 0: `<add key="QueueSDKRestricted" value="0" />`
2. 在运行病毒扫描的服务器上，使用存储区域控制器配置的值编辑 SFAntiVirus.exe.config：
 - a) 对于 CommandFile：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 CommandOptions 和返回代码：配置文件中提供的命令行设置就是一个示例。为您的防病毒软件和环境提供适当的设置。
 - c) 对于 ScanFileTimeout：扫描较大的文件可能需要更长时间。根据存储中预期的文件大小调整此设置。否则，这可能会增加大文件未被扫描的风险。
3. 在命令行窗口中，运行以下命令以设置病毒扫描：`SFAntiVirus.exe -register SFusername SFpassword`

使用 ICAP 进行防病毒扫描，而不是使用命令行工具

存储区域控制器 5.3 及更高版本支持将 ICAP 协议用于已编码为 ICAP 的 RFC 标准的防病毒扫描平台。如果需要，客户仍然可以使用 CLI 方法。自存储区域控制器 5.0.1 及更高版本起，租户区域支持此功能。

要在存储区域控制器上启用 ICAP AV 扫描程序，请导航到存储区域控制器配置页面。

选中“启用防病毒集成”复选框，然后在 **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

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) 为任务提供一个有意义的名称。
 - b) 在“安全 选项”下，单击“更改用户或组”，然后指定一个 Windows 用户来运行任务。用户必须具有存储位置的完全访问权限。
 - c) 无论用户是否登录，都选择“运行”。清除“不存储密码”复选框。
 - d) 选择 以最高权限运行。
 - e) 从“配置对象”菜单中，选择将运行任务的服务器的操作系统。
3. 要创建触发器：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“起始位置”，指定 SFAntiVirus.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，则以下规则适用”，选择“不启动新实例”。

AV 命令行集成到扫描服务中

必备条件

- 在安装或升级存储区域控制器 5.2 之前，请确保停止或删除现有的命令行 AV（如果它是作为计划任务或 cron 运行的）。
- 在主机上安装 .NET 4.6.2（或更高版本）。

本地存储区域控制器中的扫描服务包括对使用命令行 AV 工具的支持，例如赛门铁克命令行 AV Scan。此外，扫描服务还提供包含 ICAP 支持的防病毒产品的扫描。

要启用此功能，请在 AntiVirus/OnPrem/AVScanService/AVScanService/appSettings.config 中添加以下配置键和值

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

命令行工具特定配置

存储区域控制器 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。

配置密钥值将在下面进行解释，并附带示例值。

- 将此点设置为命令行应用程序。

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

- 查看命令行应用程序的文档，了解它支持哪些选项或开关，然后将其添加到此位置。

```
"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）的注意事项

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。在 5.2 版中，应用于 ICAP 扫描服务的关于排除的扩展名和最大文件大小（以字节为单位）的设置同样适用于 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"/>
```

新安装的存储区域控制器 5.2 将这些设置重命名为以下设置。重命名的设置反映了这样一个事实，即它们既适用于基于 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。尽管可以手动重命名，但除了 ICAP 之外，同样的设置也适用于 AV 命令行。

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

迁移 **ShareFile** 数据

August 8, 2023

有多种方法可以将 ShareFile 数据从一个本地区域迁移到另一个本地区域。

- 通过 Web 门户或用户管理工具进行迁移
- 通过 PowerShell 脚本迁移
- 通过 ZoneFix 工具进行迁移

必备条件

- 确保可以从目标区域访问源区域，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该地址。如果连接成功，则会显示 ShareFile 徽标。

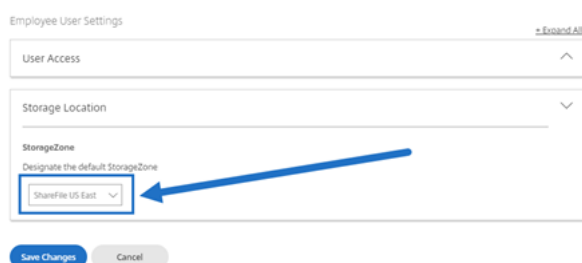
通过 **Web** 门户或用户管理工具进行迁移

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

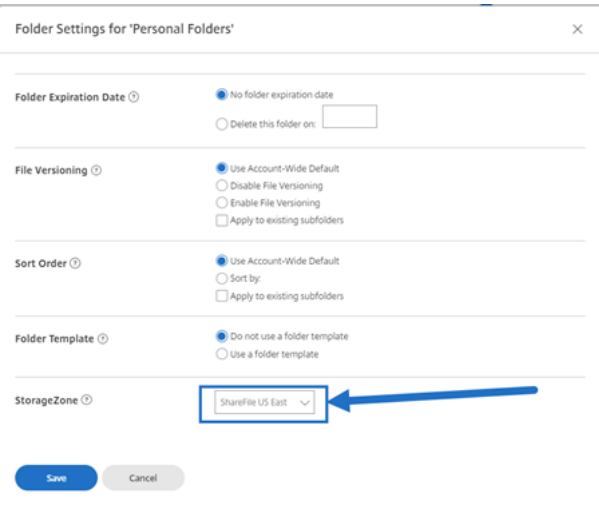
重要：

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

迁移特定用户的数据 - 导航到“人员”，然后找到“员工”用户。单击该用户可查看其个人资料页面。在“存储位置”下，选择一个新区域（如果已安装并配置了新区域）。



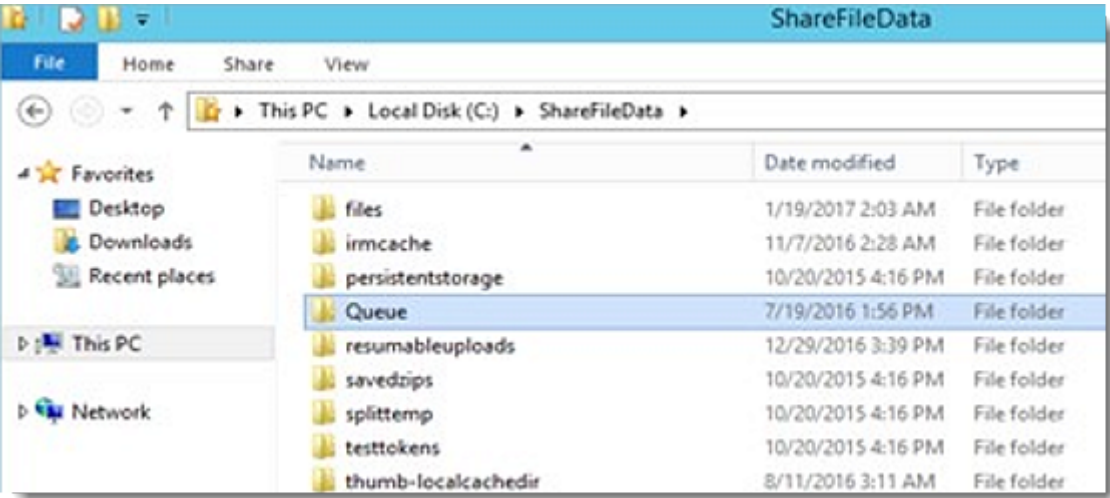
迁移特定文件夹的数据 - 导航到该文件夹并访问文件夹名称右侧的“更多选项”菜单。单击“高级文件夹设置”。使用菜单选择一个新区域。



迁移过程

首先，排队等待迁移的文件在原始区域的 存储位置 内的 队列 文件夹中创建一个占位符文件。

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



通过 PowerShell 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，然后将这些文件夹上传到新区域。

要求 -运行和安装开发工具包需要 PowerShell 4+ 和 .NET 4.x+。PowerShell 5.x 可以作为 Windows Management Framework 5.1 的一部分 [在此处](#) 下载。

通过区域修复工具迁移

区域修复工具是一种命令行工具。该工具由存储区域开发人员编写，利用 ShareFile API 来定位要迁移到特定区域的文件夹 ID。

为了获得最佳性能，建议对大小小于 2 GB 的文件夹使用此方法。

连接器收藏夹

February 14, 2022

从存储区域控制器 5.0 开始，用户可以在 ShareFile WebApp 中的 网络共享、**SharePoint** 和 **Documentum** 连接器 下将连接器文件夹设为收藏夹。有关详细信息，请参阅此 Citrix 支持知识中心 [文章](#)。

ShareFile Mobile 支持将连接器文件夹添加到收藏夹中。

管理 **ShareFile** 数据的存储区域

November 20, 2023

您可以将 ShareFile 数据存储区域与或代替 ShareFile 托管的云一起使用。

注意：

如果要删除主存储区域控制器，请将其降级，然后再继续。有关更多信息，请参阅[降级和升级存储区域控制器](#)。

在区域之间移动主文件夹和文件框

使用以下步骤在区域之间移动主文件夹和文件盒。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。

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. 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。
4. 单击创建文件夹。
5. 照常配置文件夹。创建文件夹时，您可以选择是使用 ShareFile 托管的云存储还是使用本地存储区域。

重命名或删除存储区域

重要说明：

在删除存储区域之前，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，并且您无法撤消该操作。

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**。

限制

在以下情况下，无法重命名/删除存储区域控制器：

- **ShareFile** 数据迁移正在进行中 - 在尝试删除存储区域之前完成数据迁移。
- **ShareFile** 数据存在于区域中 - 在尝试删除存储区域之前，先迁移或删除所有现有数据。

自定义存储缓存操作

ShareFile 用户请求由存储区域控制器管理。这包括：文件上载、下载和删除。然后，存储区域控制器与连接的存储器通信。例如，如果连接的存储是受支持的第三方存储系统，并且 ShareFile 用户上传了文件，则 ShareFile 客户端会将该文件发送到永久存储缓存。然后，存储区域控制器会将文件上载到第三方存储系统。

存储区域控制器使用 `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config` 中的可配置设置来管理持久性存储缓存。本讨论中介绍了特定于受支持的第三方存储系统的设置。

对于上载的文件：

- 存储区域控制器将上载的文件放置在永久存储缓存（PersistentStorage 文件夹）中。
- 以下设置控制删除服务操作的时间：
 - `MinDeletionAge` 指定从上次访问文件到可以删除文件之间的最小时间间隔。默认为 1 天。最小设置为 8 小时。
 - `OffPeakTimeOfDayStart` 和 `OffPeakTimeOfDayEnd` 指定文件删除的开始和停止时间。默认为凌晨 2 点和凌晨 4 点
 - `ProducerTimerInterval` 和 `DeleteTimerInterval` 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，请联系支持人员。
- 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。删除服务会在项目创建 24 小时后将其删除。
- 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对应的 blob。

- 默认情况下，删除服务每 10 秒 (`CheckSizeThresholdTimer`) 确定存储缓存是否已超过 10 GB 的磁盘阈值 (`DiskSpaceDropoutThresholdGB`)。如果超过阈值，则删除服务会删除过去一小时内未访问过的文件 (`CacheCleanupFileThresholdPeriodUnexpected`)。删除服务是正常调度的结果（而不是因为磁盘大小达到阈值）。如果 blob 位于支持的第三方存储中，则该服务会删除过去 24 小时内未访问过的文件 (`CacheCleanupFileThresholdPeriodNormal`)。如果 blob 不在第三方存储中，则该文件将保留在存储缓存中。

对于下载的文件：

- 当存储区域控制器收到下载请求时，它会从永久存储缓存中下载文件（如果该文件存在）。如果文件不在该缓存中，控制器会将该文件从第三方存储系统下载到永久存储缓存中。删除服务会删除过去 24 小时内未访问过的文件 (`CacheCleanupFileThresholdPeriodNormal`)。

对于已删除的文件：

- 删除服务从 `ShareFile` 应用程序获取 45 天前（周期）删除的文件列表。
- 然后，删除服务会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。

删除服务默认期限

删除服务计时器设置为 45 天。45 天的默认期限将覆盖之前的任何设置。

注意：

如果将删除期配置为少于 45 天，请联系支持人员以减少项目在回收站中显示的天数，从而使两个时间范围相等。

1. 要修改默认时段，请在 `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc` 位置编辑 `FileDeleteService.exe.config`

- `<!--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

April 23, 2021

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）

有权查看连接资源的用户可以从 ShareFile Web 界面和 ShareFile 客户端浏览连接的 SharePoint 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。要启用连接器浏览，请与 ShareFile 支持部门联系。

还提供了其他设置，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文档或文件夹同步。

连接器必须具有唯一的显示名称。用户被阻止使用帐户上其他位置当前正在使用的连接器名称。

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

- 如果您使用的是 ShareFile 数据存储区域，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. 如果您使用的是 ShareFile 数据的存储区域，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，或者必须与其具有信任关系。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”，请按以下表单指定 SharePoint 根级站点、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（但不包括站点集）和文档库。ShareFile 从用户隐藏 SharePoint 系统文件夹。

- 到 SharePoint 网站集的连接示例：<https://sharepoint.company.com/site/SiteCollection>

通过与网站集的连接，用户可以访问该集中的所有子网站。

- 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 SharePoint 2013 年 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 https://example.com/%UserDomain%_%UserName%/Documents）的站点级连接器。

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

连接到 SharePoint 个人站点时，使用变量 %URLusername% 自动解析选择的特殊字符。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](https://sharepoint.acme.com/personal/rip%20van%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，因此它在具有小屏幕的移动设备上显示良好。

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. 要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”。

此步骤仅确定用户是否可见连接器。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 及更高版本的移动客户端支持元数据标记。

注意：

仅用于 `en-us`。

为网络文件共享创建存储区域连接器

必备条件

- 如果您使用的是 ShareFile 数据存储区域，请创建要用于连接器的区域。
- 为了使网络共享连接器能够与最新版本的 Chrome、Edge 和 Firefox 浏览器配合使用，请为您的环境应用最新的 .NET 更新。有关详细信息，请参阅[.NET 框架中支持 Samesite 的知情库文章](#)。将其应用于所有存储区域连接器。考虑到最新版本的浏览器，允许为 Cookie 设置 Samesite 属性，这是必要的。
- 如果使用版本 5.10.1 或更低版本，请在所有存储区域连接器的 `C:\inetpub\wwwroot\Citrix\StorageCenter\cifs\Web.config` 文件的 `<system.web>` 标签内添加 `<httpCookies sameSite="None"requireSSL="true"/>`。考虑到最新版本的浏览器，允许为 Cookie 设置 Samesite 属性，这是必要的。

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. 如果您使用的是 ShareFile 数据的存储区域，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个域中，或者必须与其具有信任关系。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。

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-Home 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-Home-Directory 值。

- %UserDomain%

重定向到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：请勿创建到 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。

该名称用于标识用户的文件共享。名称应该很简短，因此它在具有小屏幕的移动设备上显示良好。

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. 要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”。

此步骤仅确定用户是否可见连接器。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。

启用网络文件共享的文件签入和签出

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“启用签入和签出网络文件共享”复选框。
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。此服务帐户需要对网络共享位置中存在的所有文件和文件夹具有读写访问权限。

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 内容服务器区分大小写，因此，在身份验证过程中输入的用户名应与区分大小写的凭据相匹配，除非 Documentum 内容服务器上禁用了区分大小写。

必备条件

1. 存储区域 Controller 5.3 或更高版本
2. 由 ShareFile 客户支持部门启用的文档 ECM 设置。
3. Documentum 休息服务必须部署在您的 Documentum 服务器上。[单击此处获取有关 Documentum 休息服务的更多信息。](#)
4. 如果使用 Citrix ADC，则需要进行某些配置更改。这些更改将在本文下面进一步详细介绍。

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它。

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

WebApp

- 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 内容服务器区分大小写，因此，在身份验证过程中输入的用户名应与区分大小写的凭据相匹配，除非 Documentum 内容服务器上禁用了区分大小写。

用于文档连接器的 Citrix ADC 配置

如果将 Citrix ADC 与您的环境结合使用，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。

连接器验证

管理员用户现在可以使用以下设置指定在执行 CIFS 或 SP 身份验证的 AD 查找时使用哪个域 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，则使用第二个 DC，依此类选择。

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。

如果新的应用程序设置不存在，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 30, 2023

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

您可以使用支持 ICAP（一种用于内联内容扫描的标准网络协议）的第三方 DLP 安全套件扫描上传到存储区域的文档。然后，根据 DLP 扫描的结果以及您对控制访问的严格程度的偏好，调整共享和访问权限。

支持的 DLP 系统

存储区域控制器使用 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，如果您预计负载会很大，则可能需要专用 ICAP 服务器来处理 ShareFile 数据。

符合 iCAP 标准的常见的 DLP 解决方案包括：

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

由于 ShareFile 使用您现有的 DLP 安全套件，因此您可以维护用于数据检查和安全警报的单点策略管理。如果您已经使用上述解决方案之一来扫描传出的电子邮件附件或网络流量中的敏感数据，则可以将 ShareFile 存储区域控制器指向同一台服务器。对于这些现有的 DLP 系统，如果底层 DLP 系统本身支持 ICAPS，我们还支持安全 ICAP (ICAPS)。

启用 DLP

要为 ShareFile 和存储区域控制器启用 DLP，请执行以下三个操作：

1. 在您的 ShareFile 帐户上启用 DLP 功能。
2. 在存储区域控制器服务器上启用 DLP。
3. 为每个文件分类配置允许的操作。

以下各节将详细描述这些操作。

在您的 **ShareFile** 帐户上启用 DLP 功能

要请求或确认您的 ShareFile 子域已启用 DLP，请向 [Citrix 支持部门](#) 发送请求。

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。为您的帐户启用 DLP 后，您可以继续在存储区域控制器服务器上启用 DLP。

在存储区域控制器服务器上启用 **DLP**

使用以下步骤在存储区域控制器部署上配置 DLP 设置：

1. 安装或升级到存储区域控制器 5.3 或更高版本。
2. 在存储区域控制器控制台 http://*localhost*/configservice/login.aspx 中，单击 **ShareFile** 数据 选项卡。如果该区域存在，请单击“修改”。
3. 选中“启用 **DLP** 集成”复选框，然后在 ICAP REQMOD URL 字段中键入您的 DLP 服务器的 **ICAP** 地址。地址格式为：

```
1 icap://<\*name or IP address of your DLP server\*>:<\*port\*>/
   reqmod
2
3 OR
4
5 \*icaps://<name or IP address of your DLP server\>:<port\>/
   reqmod\*
6
7 The default ICAP port is 1344 (non-secure DLP) and the default
   ICAPS port is 11344 (secure DLP).
8
9 For example, if your DLP server is dlp-server.example.com, type
   the following into the ICAP REQMOD URL field:
```

```
10
11 icap://\*dlp-server.example.com\*:1344/reqmod
12
13 OR
14
15 \*icaps://dlp-server.example.com:11344/reqmod\*
```

4. 单击“保存”或“注册”。

启用 DLP 后，通过检查“监控”选项卡上的 **DLP ICAP** 服务器状态条目来确认 DLP 服务器可以访问

根据 **DLP** 扫描结果控制访问权限

在帐户和存储区域控制器上启用 DLP 后，将扫描上传到启用 DLP 的存储区域的每个文件的每个版本以查找敏感内容。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 分类限制了文件的常规权限和共享控制。共享文档时，即使 DLP 设置允许用户匿名共享，用户仍然可以选择阻止匿名访问。但是，如果用户尝试以违反 DLP 设置的方式共享文件，ShareFile 会阻止他们这样做。

数据分类为：

- 已扫描：正常—由 DLP 系统扫描并通过“确定”的文件。
- 已扫描：已拒绝—已由 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 的分类适用于存储在 Citrix 管理的存储区域或其他未启用 DLP 的存储区域中的所有文档。该分类还适用于在配置 DLP 之前上传的启用 DLP 的存储区域中的文件。该分类还适用于由于外部 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 服务器以应阻止或删除内容的消息作为响应，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：正常”。

对于每种数据分类，您可以设置不同的访问和共享限制。对于这三个类别中的每一个类别，ShareFile 管理员选择允许的操作：

- 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“管理员”>“高级首选项”>“允许客户端共享文件”下启用。
- 匿名用户可以下载该文件

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，启用数据分类的共享权限时，还必须授予至少一类用户下载权限。

在 **ShareFile** 中配置 **DLP** 设置

- 1. 在 ShareFile 网页界面中，单击“管理员” > “数据丢失防护”。
- 2. 将“根据文件内容限制对文件的访问权限”选项更改为“是”。
- 3. 为每种数据分类配置允许的操作。

重要：
ShareFile On-Demand Sync 工具需要下载权限才能正常运行。如果您的部署包括 ShareFile On-Demand Sync，则允许员工下载所有内容分类。

当存储区域控制器向 DLP 系统发送文件时，它包含指示文件所有者的元数据。该文件还包括文件在 ShareFile 中所在的文件夹路径。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，请编辑存储区域控制器上的设置文件，网址为 [wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config](#)。下表描述了与 DLP 相关的每项设置。

设置	说明	默认值
scan-interval	DLP 服务检查 DLP 队列中是否有新文件并将它们发送到 DLP ICAP 服务器进行处理的频率。	30 秒
icap-response-timeout	存储区域控制器在将 ICAP 服务器标记为不可用之前等待 ICAP 响应的时间。	30 秒
icap-exclude-extensions	以逗号分隔的扩展名列表，可从 DLP 扫描中排除。DLP 服务器不处理名称以这些扩展名之一结尾的文件，而是将文件标记为“已扫描：确定”。示例值：“exe、jpg、bin、mov”	无
icap-max-file-size-bytes	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，所有文件大小都已发送。配置为非零值时，DLP 服务器不会处理大于配置大小的文件，但会标记为“已扫描：确定”。	31457280 (30 MB)

设置	说明	默认值
x-queue-items-to-process	每次扫描间隔迭代要扫描的最大队列项目数。降低此值可减轻向 StorageZone 添加大量文件时对 DLP 服务器的影响。	512
max-queue-processing-threads	用于消耗 DLP 扫描队列的最大并发处理器线程数。根据允许与 ICAP 服务器同时连接的最大数量设置此值。应在合理的范围内，以避免阻塞使用同一 ICAP 服务器的其他网络服务。	4
lcap-reqmod-http-request-verb	默认情况下，网络调用是使用 PUT 动词进行的。如果需要，您可以将此设置更改为 POST。	PUT

DLPExistingFiles 工具

ShareFile 存储区域控制器提供通过 ICAP 将存储中心与数据丢失防护 (DLP) 提供商集成的选项。

但是，ICAP 服务只能处理仅由新创建的文件填充的队列。这意味着服务不会扫描启用 ICAP 之前区域中存在的文件。此工具有助于将这些文件排队进行扫描，也可以将扫描的文件排入队列以进行重新扫描。

顾名思义，该工具仅适用于 DLP ICAP 服务。

要求

该工具是 PowerShell 脚本，因此需要 PowerShell 才能运行。还需要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

对于已安装的存储区域控制器，可以在 <storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1 位置找到该工具。默认情况下，存储区域控制器的安装位置为 C:\inetpub\wwwroot\Citrix\StorageCenter。

运行该工具之前的注意事项

根据以下情况，该工具可能需要为单个操作运行多次。

- 为队列大小限制规定的限制。

- 符合给定标准的项目数量。除非队列大小限制设置为零或更小，否则这种考虑是正确的。在这种情况下，该工具假设队列目录中的最大大小为 200,000 个项目。

例如，如果使用该工具对未扫描的项目进行排队，则队列大小限制设置为 500 个项目。当未扫描的项目超过 500 个时，该工具会在队列中填满 500 个项目后停止。为了追踪它在哪里停止，该工具会存储上次检索到的项目的创建日期。该工具将日期存储在 `<storage zones controller installation location>\SC` 的临时文件中，名为 `DLPExistingFiles-enddate.temp`。

每次运行之前，该工具都会查找此文件。如果文件存在，则该工具会使用其中的创建日期作为下一批文件的标记。该工具不会在完成特定操作后删除临时文件。相反，在特定操作的所有批处理完成后，区域管理员可以删除该文件。由于这种情况，完成完整操作后，应在执行其他操作之前手动删除临时文件（如果存在）。

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"
```

这会打开 PowerShell 作为网络服务运行。要验证它是否确实以网络服务形式运行，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。

```
1 <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**（必选）：此选项用于指定要排队扫描的文件类型。子选项：
 - **Unscanned**：未扫描的文件。例如，未扫描的 DLP 时代之前的文件。
 - **ScannedOK**：已扫描的已标记为干净的文件。
 - **ScannedRejected**：已标记为不干净的扫描文件。
 - **Scanned**：所有扫描的文件。
- **-queueLimit**（可选）：此选项用于指定工具停止之前队列中允许的项目数量。
- **-date**（可选）：排队等待扫描的项目的最大创建日期。例如，如果将日期指定为“10/30/2017 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等候扫描。

示例：

在所有示例中，请通过 **PsExec** 将 **PowerShell** 作为网络服务打开。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入队列，请运行以下命令。

```
1 <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。

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

要将在 2017 年 10 月 30 日上午 11:30 之前创建的所有具有以下特征的扫描项目排入队列：标记为干净，在队列限制为 200 的区域中，运行以下命令。

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

监视

February 14, 2022

存储区域控制器和 ShareFile 管理员界面包含多种资源，可帮助您监视存储区域控制器的活动并解决问题：

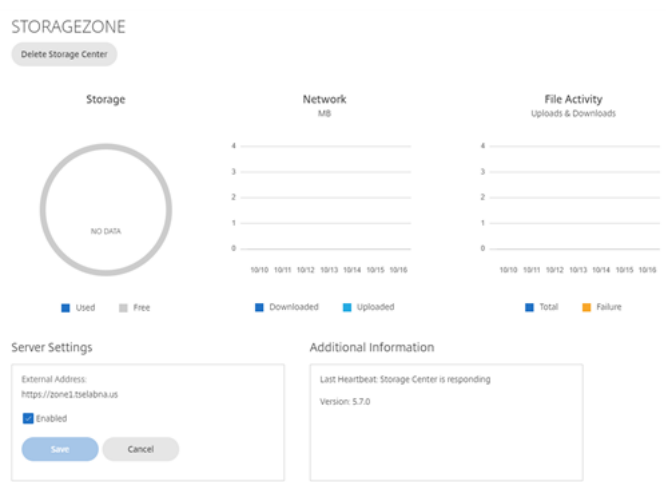
- 常规组件状态—存储区域控制器控制台上的“监视”选项卡提供组件状态以帮助您开始故障排除过程。为诸如访问权限、服务状态和检测信号状态之类的项目提供状态，这表示存储区域控制器与 ShareFile 控制平面的出站连接。

存储区域控制器每 5 分钟向 ShareFile Web 应用程序发送一次更新。如果 ShareFile Web 应用程序在 10 分钟内未收到更新，它会将存储区域控制器标记为脱机。

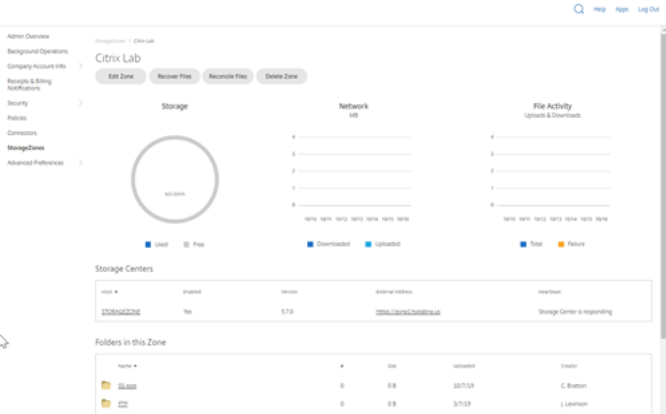
对于监控选项卡上显示为红色的项目，请查看日志文件以获取详细信息。

Monitoring（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，或者客户端是否能够访问该区域。

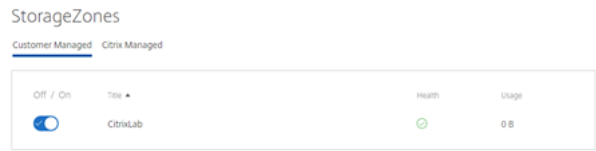
- 存储区域控制器服务器信息—有关服务器的存储使用情况、网络使用情况和文件活动的信息：在 ShareFile 界面中，登录到您的 ShareFile Enterprise 帐户，转到 管理员 > **StorageZones**，单击存储区域，然后单击存储区域控制器主机名。



- 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：在 ShareFile 界面中，登录您的 ShareFile Enterprise 帐户，转到 管理员 > **StorageZones**，然后单击区域名称。



- 存储区域控制器运行状况状态—要确定 ShareFile.com 是否正在接收来自加入该区域的存储区域控制器的检测信号消息，请查看运行状况：在 ShareFile 界面中，登录到您的 ShareFile Enterprise 帐户，转到 管理员 > **StorageZones** 中，验证“运行状况”列是否有绿色复选标记，然后单击站点名称以验证 Heartbeat 消息是否指示存储区域控制器正在响应。



- 日志文件—日志文件提供有关存储区域控制器配置及其组件的详细信息，如下节所述。

日志文件

默认情况下，存储区域控制器的以下日志文件位于 `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	存储区域控制器配置操作，包括修改现有存储区域配置、创建新的存储区域以及将新的存储区域控制器加入现有的主存储区域控制器
sc-%date%.txt	标准区域的 ShareFile 数据上传和下载活动
cifs-%date%.txt	用于网络文件共享上传和下载活动的存储区域连接器
sharepoint-%date%.txt	用于 SharePoint 上传和下载活动的存储区域连接器
cloudstorageuploader-%date%.txt	云存储上传器服务（到受支持的第三方存储系统）
copy-%date%.txt	ShareFile 复制服务
删除-%date%.txt	ShareFile 清理服务，用于永久存储缓存
s3uploader-%date%.txt	ShareFile 管理服务。包括心跳状态消息

扩展日志记录可用于以下每个组件，在需要提供详细信息以支持时非常有用。

组件	appSettingsRelease.config
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
SharePoint 的存储区域连接器	C:\inetpub\wwwroot\Citrix\StorageCenter\sp

启用扩展日志记录

以下步骤为所有存储区域控制器组件和服务启用扩展日志记录：

1. 在存储区域控制器服务器上，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。

要为特定组件启用扩展日志记录，请编辑其 appSettingsRelease.config 文件：将的值 `<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存储区域控制器。IIS 日志显示所有传入的请求。存储区域控制器的 IIS 日志位于 c:\inetpub\logs\LogFiles\W3SVC1。

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
配置存储区域控制器时出现“HTTP 错误 404-找不到文件或目录”	该消息通常源于 IIS 或的问题 ASP.NET 。确保在 Windows 安装中启用了 IIS 角色，并且在 IIS 上启用了 ASP.NET 功能。
在存储区域控制器上浏览 localhost 时出现“HTTP 错误 404.2 —未找到” 尝试上传后出现“HTTP 错误 413-请求实体太大”	该消息表明的 ISAPI 和 CGI 限制 ASP.NET 未设置为允许。 在尝试向存储区域上传失败后，该消息可能会出现在网络跟踪中，也可能是由 IIS 中的客户端证书设置引起的。要变通解决此问题，请在存储区域控制器服务器上打开 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。
配置存储区域控制器时发生 IIS 错误	IIS 错误 ASP.NET 通常表示未完全配置。在 IIS 管理器中的 ISAPI 和 CGI 限制下，确认所有 ASP.NET 商品的限制设置为允许。验证 ASP.NET 是否已在 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 ，请参阅下表后面的命令行。如果您仍然遇到问题，请查看您的 IIS 和 ASP.NET 设置。
配置存储区域控制器时出现“无法保存存储中心绑定”	该消息指示 IIS 帐户池用户存在权限问题。默认情况下，应用程序池在网络服务用户帐户下运行。默认情况下，存储区域控制器使用网络服务帐户。如果使用指定用户帐户而不是 Network Service 帐户，则指定用户帐户必须对用于私有数据存储的网络共享具有完全访问权限。
在配置区域时出现“访问被拒绝”	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 日志中包含 <code>system.net.WebException: 远程服务器返回错误: (403) 禁止</code> 。此问题可能是由于代理服务器阻止了出站请求所致。验证您的防火墙是否满足存储区域控制器系统要求中指定的要求
登录到存储区域控制器时出现“无法连接到远程服务器”	该消息通常表示存在代理问题。请确保您的代理设置已配置。如果代理设置正确，请验证是否可以存储区域控制器登录到您的 ShareFile 帐户。验证您是否具有管理员级别的权限来配置存储区域控制器，并且外部防火墙上的端口 443 处于打开状态。

问题	说明和解决办法
在为 ShareFile Data 启用和配置存储区域后，网络共享上名为 ShareFileStorage 的文件夹不包含 SCKeys.txt	存储区域控制器会在安装过程中创建 SCKeys.txt，除非用于安装存储区域控制器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存储区域控制器。
创建区域后，文件上传到共享文件夹失败	此问题表示您的内部 DNS 存在问题。您必须具有存储区域控制器 FQDN 的内部和外部 DNS 记录。
在 监控 选项卡上，检测信号状态为红色	红色图标表示存储区域控制器无法将检测信号消息发送到 ShareFile 网站。检查其他组件的图标是否为红色。如果是，请参阅日志以获取更多信息。如果 s3uploader 日志显示发送检测信号失败，则存储区域控制器服务器可能无法联系 ShareFile 网站，除非它通过代理服务器。要为存储区域控制器指定代理服务器，请打开控制器控制台并转到网络选项卡。如果存储区域控制器服务器无法使用网络服务用户访问 ShareFile 网站，则要么允许网络服务用户访问 ShareFile 网站，要么设置具有对代理服务器的出站访问权限的 Windows 用户帐户。

问题	说明和解决办法
ShareFile 管理员界面中未显示存储区域	<p>此问题可能表示外部地址或防火墙有问题。首先在存储区域控制器控制台中验证外部地址不包括端口。如果是这样，请移除端口，然后重新启动控制器。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。存储区域控制器需要该设置。验证 Windows 防火墙是否允许端口 443 上的出站流量用于以下进程：<code>C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe</code>、<code>C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCopySvc\FileCopyService.exe</code>、<code>C:\inetpub\wwwroot\Citrix\StorageCenter\s3uploader\S3UploaderService.exe</code>、<code>C:\inetpub\wwwroot\Citrix\StorageCenter\CloudStorageUploaderSvc\CloudStorageUploaderService.exe</code>、<code>C:\inetpub\wwwroot\Citrix\StorageCenter\SCProxyEmailSvc\ProxyEmailService.exe</code></p>

问题	说明和解决办法
存储区域控制器不会将数据上传到 ShareFile	<p>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、存储区域控制器和 ShareFile 客户端到达 Citrix ADC。当您上传文件并且虚拟服务器显示点击量增加时，流量将通过 Citrix ADC。验证 Citrix ADC 连接每个点的流量：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，通过在负载平衡虚拟服务器中解除对 ShareFile 数据的响应程序策略的绑定来测试 ShareFile 数据的上传。（响应程序策略会丢弃未由 ShareFile 控制平面签名的传入流量。在 Web 浏览器中，键入存储区域控制器的外部 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 成功测试了存储区域连接器的可访问性，则即使后端服务器已关闭，系统也会提示您输入凭据。或者，如果您以用户身份登录，则会收到 API 响应。https://szc-address/cifs/v3/Items/ByPath?path=\\path、https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server。API 响应采用以下格式：{ “Name” :” connectorName” , “FileName” :” FileName” , “CreationDate” :” date” , “ProgenyEditDate” :” date” , “IsHidden” :false, “Path” :” “, “StreamID” :” id” , “odata.metadata” :” https://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 设置可能导致设备连接问题。您必须具有外部 DNS 记录，并且可能还需要外部存储区域 FQDN 的内部 DNS 记录。如果您仅在使用特定设备时遇到问题，请测试该设备。</p>

问题	说明和解决办法
升级存储区域控制器后，文件清理服务中的 ShareFile 连接状态为红色图标	如果 Windows 在存储区域控制器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，状态将返回为绿色图标。
创建连接器时出现“路径超过最大长度 (1024)”	如果为存储区域控制器配置的外部地址指向 ShareFile 网站而不是存储区域控制器服务器 FQDN，则会出现此消息。
删除旧的存储区域控制器后，配置新的存储区域控制器时，会出现“名称无效”。	如果与旧存储区域控制器相关的实体仍然存在，则会出现该消息。要解决此问题：卸载新的存储区域控制器。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。 安装并配置新的存储区域控制器。如果问题仍然存在，请联系您的支持代表。当存储区域服务器无法通过 DNS 或本地 hosts 文件解析存储区域 FQDN 时，会出现此消息。

手动注册 **ASP.NET**

```
1 cd /d C:\Windows\Microsoft.NET\Framework\v4.0.30319
2 iisreset /stop
3 aspnet_regiis -i
4 iisreset /start
5 %systemroot%\system32\inetsrv\appcmd set config /section:
  isapiCgiRestriction
6 /[path='%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll'].
  allowed:True
7 %systemroot%\system32\inetsrv\appcmd set config /section:
  isapiCgiRestriction
8 /[path='%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll'
  ].allowed:True
```

ShareFile 客户端和 **Web** 应用程序疑难解答

如果移动设备无法连接到连接器，请验证连接性。上表涵盖了许多连接问题。确保存储区域控制器处于联机状态。将文件上传到区域。如果上载有效，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进行连接。检查 SharePoint 服务器或文件服务器是否可用。

如果在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。如果这些选项未列在“安全”下，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 用户是否有权访问共享。在 Server Manager 中，转到共享和存储管理，然后根据需要进行添加用户或更改用户权限。
- Citrix ADC 身份验证、授权和审核组访问存在问题。

如果在连接到 SharePoint 站点时出现“HTTP 错误 403 — 禁止”，则 SharePoint 服务器可能已配置为进行基本身份验证，但存储区域控制器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`。

如果移动应用程序尝试访问连接器时出现“HTTP 错误 503-服务不可用”，则说明连接器正在发送响应，但无法处理 HTTP 请求。如果内容交换策略、负载均衡 VIP 或响应程序策略在 Citrix ADC 上配置错误或绑定不正确，则会发生这种情况。要解决此问题，请查看 ShareFile 的 Citrix ADC 配置并更正配置。

参考：存储区域控制器配置文件

December 6, 2022

此参考概述了存储区域控制器配置文件：

- 使用微软 Azure 上的 ShareFile 数据配置存储区域控制器
- AppSettingsRelease.config
- FileDeleteService.exe.config
- SFAntiVirus.exe.config
- 网站配置

存储区域控制器安装程序创建这些文件。您在存储区域控制器控制台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。此参考列出了这些设置，并提供了指向相关信息的链接。

微软 **Azure** 存储上的 **ShareFile** 数据

客户管理的存储区域支持在你的 Microsoft Azure 帐户中本地托管 Citrix ShareFile 数据。使用兼容的第三方存储可帮助 IT 部门为其组织构建经济高效且定制的解此解决方案将 ShareFile 与微软 Azure 的二进制大对象 (Blob) 存储集成在一起。此存储是一种云服务，用于存储大量非结构化数据，可以使用 HTTP 或 HTTPS 从任何地方访问这些数据。

使用微软 **Azure** 上的 **ShareFile** 数据配置存储区域控制器

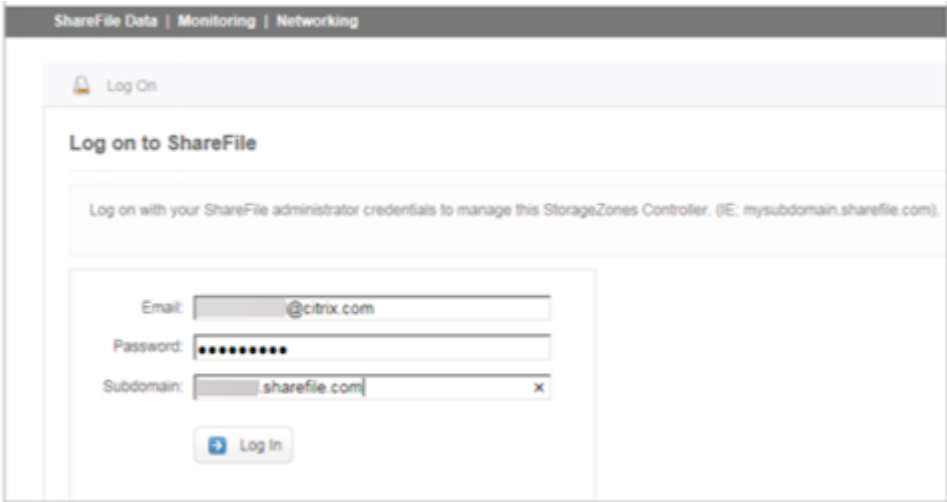
在 Microsoft Azure 上使用 ShareFile Data 创建存储区域之前，请查看系统要求和安装步骤：

- 为存储缓存创建网络共享。有关更多信息，请参阅 [为私有数据存储创建网络共享](#)。

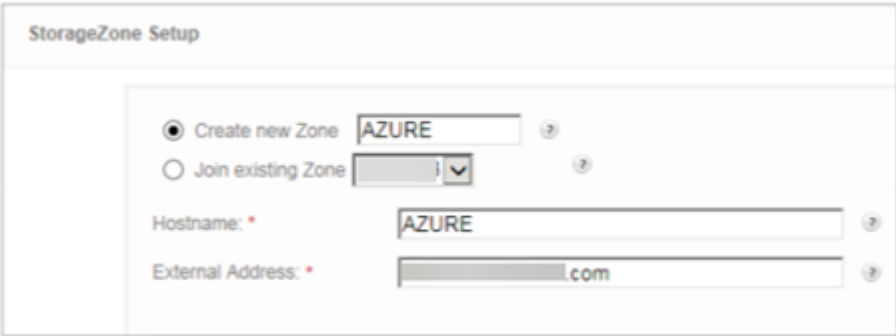
- 安装必要的 SSL 证书。有关更多信息，请参阅 [安装 SSL 证书](#)。
- 准备服务器以安装存储区域。有关更多信息，请参阅 [为服务器准备 ShareFile 数据](#)。

安装存储区域控制器软件后，转到 **Citrix ShareFile** 存储区域控制器，然后选择 配置页面。

1. 使用分配的管理员帐户登录 ShareFile。



2. 选择 创建新区域 选项，然后为新区域输入唯一名称。
3. 输入 主机名，通常将使用服务器的计算机名称。
4. 输入此区域的外部地址。这是此服务器或负载均衡器的公开可解析 FQDN 地址。



5. 选中 为 **ShareFile** 数据启用 **StorageZone** 复选框。
6. 从存储库下拉菜单中选择 **Windows Azure** 存储容器。
7. 输入在必备条件安装期间创建的共享缓存位置，请参阅[为私有数据存储创建网络共享](#)。输入有权访问共享缓存文件夹的用户名和密码。

☒ Enable StorageZones for ShareFile Data ?

Storage Repository: Windows Azure storage container ▼

Shared Cache Configuration

Shared Cache Location: * \\azure. AzureCache ?

Shared Cache Username: ?

Shared Cache Password: ?

☐ Enable Encryption ?

- 8. 输入 存储帐户名称 和 访问密钥。此信息来自你的微软 Azure 帐户。
- 9. 选择 验证。
- 10. 验证后，你将看到 Azure 可用的容器。从容器 名称下拉菜单中选择适当的容器。

Windows Azure Configuration

Storage Account Name: * ?

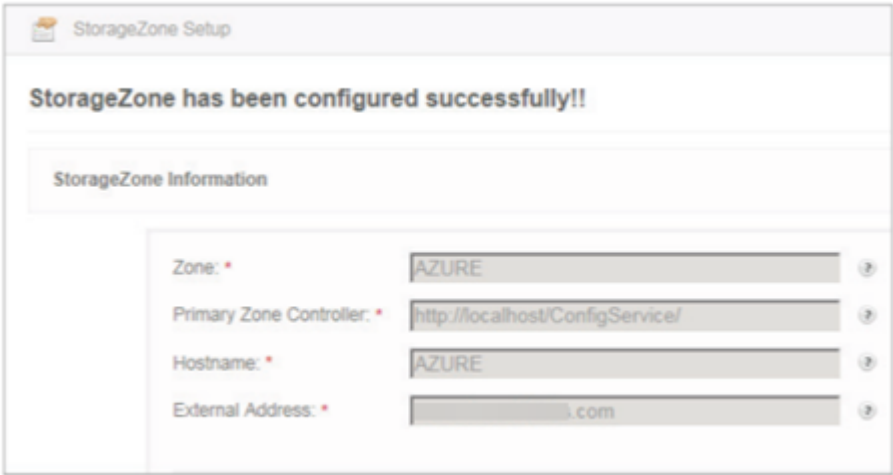
Access Key: * ? Validate

Validation successful.

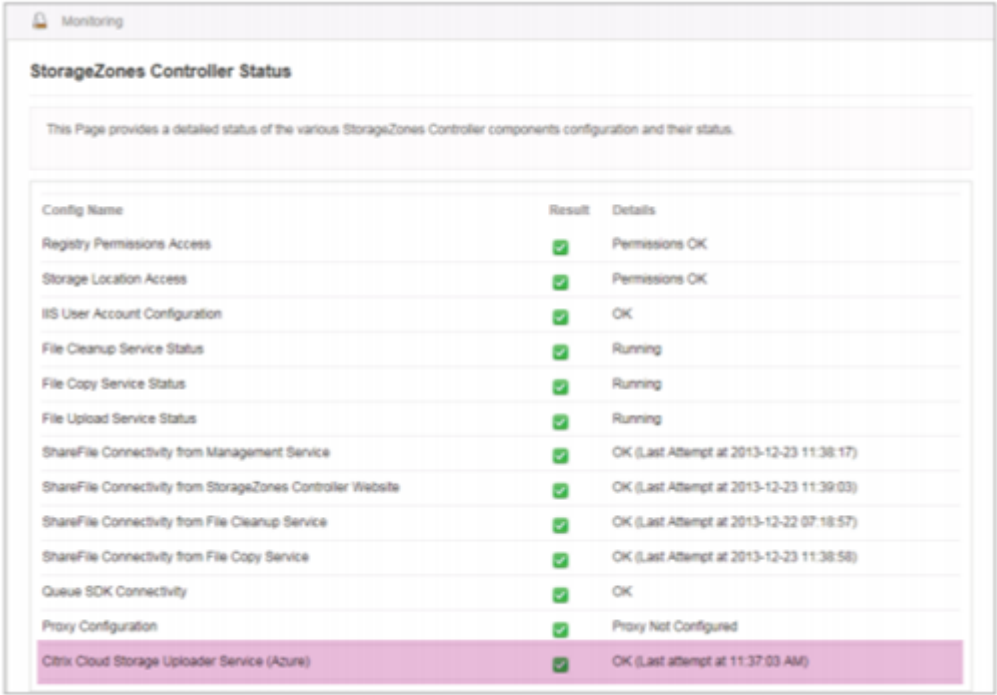
Container Name: azure-private ▼ ?

- 11. 在页面底部，输入密码短语，然后重新输入以进行验证。
- 12. 选择注册。

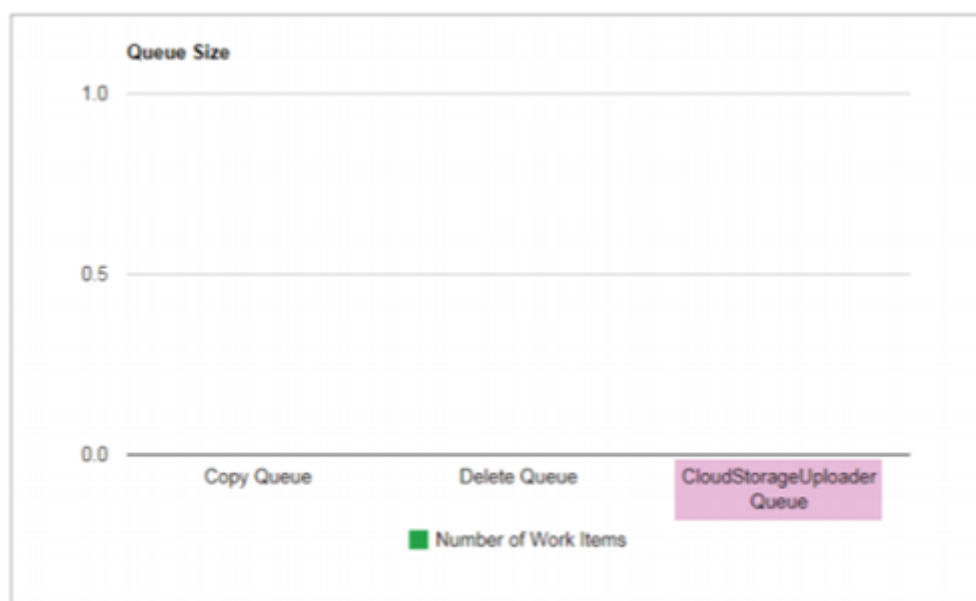
完成后，将显示以下消息：StorageZone 已成功配置！



13. 选择监控选项卡并验证 StorageZones Controller 状态。Citrix Cloud 存储上传服务 (Azure) 监控 Azure 的后台上传服务。



CloudStorageUploader 队列 监控 Azure 上传队列文件夹。



AppSettingsRelease.config

AppSettingsRelease.config 文件包含在存储区域控制器安装路径 (C:\inetpub\wwwroot\Citrix\) 中的以下文件夹中：

- StorageCenter
定义存储区域控制器的全局设置。
- StorageCenter\cifs
为网络文件共享的存储区域连接器定义设置。
- StorageCenter\sp
定义 SharePoint 的存储区域连接器的设置。

在编辑 AppSettingsRelease.config 文件之前，请验证您在正确的位置工作。

FileDeleteService.exe.config

FileDeleteService.exe.config 提供存储区域控制器用来管理永久存储缓存的控件。此配置文件位于：C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc

有关更多信息，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存储区域控制器配置、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](#)

有关更多信息，请参阅 [配置上传文件的防病毒扫描](#)。

网站配置

通常，[C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config](#) 包含通常不应更改的控件。但是，如果您将较旧的存储区域控制器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 至 2.2.2**：如果一个区域有多个 StorageZones Controller 并且所有 HTTP 流量都使用代理服务器，则必须为每台辅助服务器向 Web.Config 添加绕过列表。

注意：从版本 2.2.3 起，旁路设置包含在存储区域控制器控制台的“网络”页面中。

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

```
1 <system.net>
2   <defaultProxy enabled="true">
3     <proxy proxyaddress="http://192.0.2.0:3128" />
4   </defaultProxy>
5 </system.net>
6 </configuration>
```

2. 向该部分添加旁路列表，如下所示：

```
1 <system.net>
2   <defaultProxy enabled="true">
3     <proxy proxyaddress="http://192.0.2.0:3128" />
4     <bypasslist>
5       <add address="primaryServer" />
6     </bypasslist>
7   </defaultProxy>
8 </system.net>
9 </configuration>
```

primaryServe 要么是 IP 地址，要么是主机名 (servername.subdomain.com)。

如果您稍后更改了主存储区域控制器 IP 地址或主机名，则必须在 ConfigService\Web.config 中为每台辅助服务器更新该信息。

3. 重新启动所有区域成员的 IIS 服务器。



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).