Controlador de zonas de almacenamiento 5.x

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Acerca del controlador de zonas de almacenamiento

May 28, 2024

El controlador de zonas de almacenamiento amplía el almacenamiento en la nube de ShareFile Software as a Service (SaaS) al proporcionar a su cuenta de ShareFile almacenamiento de datos privado.

Para obtener más información sobre el controlador de zonas de almacenamiento, como los componentes, el almacenamiento de datos y más, consulte Storage zones controller 5.x.

Consulta Novedades para conocer las mejoras más recientes en esto y en ShareFile.

Para descargar la versión más reciente del controlador ShareFile Storagezone, consulte https://dl.sharefile.com/sto controller. Inicia sesión en tu cuenta de ShareFile para acceder a todas las descargas de aplicaciones.

> **SUGERENCIA:**
>
> ShareFile recomienda que los usuarios habiliten las alertas de detección de amenazas.

Problemas resueltos

Problemas solucionados en el controlador de zonas de almacenamiento 5.11.25

Esta versión aborda varios problemas que mejoran el rendimiento y la estabilidad generales.

Problemas solucionados en el controlador de zonas de almacenamiento 5.11.24

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

Problemas solucionados en el controlador de zonas de almacenamiento 5.11.23

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

Problemas solucionados en el controlador de zonas de almacenamiento 5.11.22

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

Problemas solucionados en el controlador de zonas de almacenamiento 5.11.21

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas solucionados en el controlador de zonas de almacenamiento 5.11.18

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

Problemas solucionados en el controlador de zonas de almacenamiento 5.11.17

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

Problemas solucionados en el controlador de zonas de almacenamiento 5.11

Esta versión aborda una serie de problemas que mejoran el rendimiento y la estabilidad generales.

Problemas solucionados en el controlador de zonas de almacenamiento 5.10

En esta versión, se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento generales.

Problemas solucionados en el controlador de zonas de almacenamiento 5.9

Esta versión contiene correcciones para mejorar la fiabilidad y el rendimiento.

Problemas solucionados en el controlador de zonas de almacenamiento 5.8

Esta versión contiene una corrección para mejorar los mensajes de error para los archivos desprotegidos y una corrección para las rutas administradas recientemente publicadas en SharePoint.

Problemas solucionados en el controlador de zonas de almacenamiento 5.7

Esta versión contiene correcciones para solucionar un problema de redireccionamiento en las cargas de archivos a la zona de almacenamiento y a los conectores locales.

Problemas solucionados en el controlador de zonas de almacenamiento 5.6

Solución de WOPI: incluye cambios para resolver los problemas que aparecen al intentar editar archivos de Office en ocasiones posteriores.

Corrección de SharePoint Connector: esta versión incluye cambios para mostrar mensajes de error válidos al crear carpetas que ya existen en SharePoint Connector.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas solucionados en el controlador de zonas de almacenamiento 5.5

Esta versión contiene correcciones para mejorar la fiabilidad y el rendimiento.

Problemas solucionados en el controlador de zonas de almacenamiento 5.4.2

Solución de SharePoint Connector: mover archivos que están presentes en el conector de SharePoint puede fallar en escenarios específicos. Esta versión garantiza que mover los archivos que están presentes en SharePoint Connector funcione como se esperaba.

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

Problemas solucionados en el controlador de zonas de almacenamiento 5.4.1

Correcciones de seguridad: esta versión contiene correcciones de seguridad y confiabilidad.

Compatibilidad adicional: Se agregó compatibilidad para cuentas de *cloud/*cloudburrito para el entorno de Workspace.

Problemas solucionados en el controlador de zonas de almacenamiento 5.3.1

Esta versión contiene correcciones para mejorar la fiabilidad y el rendimiento.

Problemas solucionados en el controlador de zonas de almacenamiento 5.3.1

Solución de WOPI: los tokens de acceso de WOPI podían ser falsificados mediante el robo de la clave criptográfica pública. Esta versión garantizó que la clave no se compartiera entre los controladores de zonas de almacenamiento.

Correcciones de seguridad: esta versión contiene correcciones de seguridad, rendimiento y confiabilidad.

Problemas conocidos

Problemas conocidos en el controlador de zonas de almacenamiento 5.10

No se han observado nuevos problemas en esta versión.

Problemas conocidos en el controlador de zonas de almacenamiento 5.9

No se han observado nuevos problemas en esta versión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas conocidos en el controlador de zonas de almacenamiento 5.8

No se han observado nuevos problemas en esta versión.

Problemas conocidos en el controlador de zonas de almacenamiento 5.7

No se han observado nuevos problemas en esta versión.

Descripción de la arquitectura

July 25, 2024

En esta sección se proporciona una descripción general de la implementación del controlador de zonas de almancenamiento para evaluaciones de prueba de concepto o entornos de producción de alta disponibilidad. La implementación de alta disponibilidad se muestra con y sin un proxy DMZ, como Citrix ADC.

Para evaluar una implementación con varios controladores de zonas de almacenamiento, siga las directrices para una implementación de alta disponibilidad.

Cada uno de los escenarios de implementación requiere una cuenta de ShareFile Enterprise. De forma predeterminada, ShareFile almacena los datos en la nube segura gestionada de ShareFile. Para usar el almacenamiento de datos privado, ya sea un recurso compartido de red local o un sistema de almacenamiento de terceros compatible, configure las zonas de almacenamiento para ShareFile Data.

Para entregar datos de forma segura a los usuarios desde recursos compartidos de archivos de red o bibliotecas de documentos de SharePoint, configure los conectores de zonas de almacenamiento.

Implementación de prueba de concepto del controlador de zonas de almacenamiento

> **Precaución:**
>
> Una implementación de prueba de concepto está pensada únicamente para fines de evaluación y no debe usarse para el almacenamiento de datos críticos.

Una implementación de prueba de concepto utiliza un único controlador de zonas de almacenamiento. El ejemplo de implementación que se describe en esta sección tiene habilitadas tanto las zonas de almacenamiento para ShareFile Data como los conectores de zonas de almacenamiento.

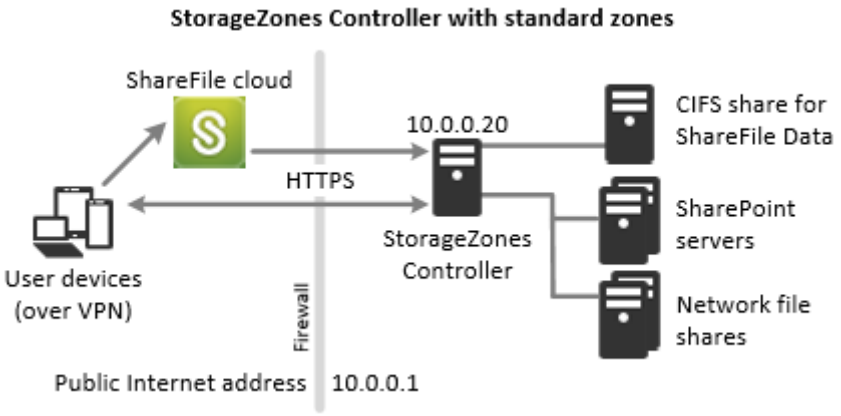
Para evaluar un único controlador de zonas de almacenamiento, si lo desea, puede almacenar los datos en una carpeta (como C:\ZoneFiles) del disco duro del controlador de zonas de almacenamiento

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

en lugar de en un recurso compartido de red independiente. Todos los demás requisitos del sistema se aplican a una implementación de evaluación.

Implementación de prueba de concepto para zonas de almacenamiento estándar

Un controlador de zonas de almacenamiento configurado para zonas estándar debe aceptar conexiones entrantes desde la nube de ShareFile. Para ello, el controlador debe tener una dirección de Internet de acceso público y SSL habilitado para las comunicaciones con la nube de ShareFile. La siguiente ilustración indica el flujo de tráfico entre los dispositivos de los usuarios, la nube de ShareFile y el controlador de zonas de almacenamiento.



En este caso, un firewall se interpone entre Internet y la red segura. El controlador de zonas de almacenamiento reside dentro del firewall para controlar el acceso. Las conexiones de usuario a ShareFile deben atravesar el firewall y utilizar el protocolo SSL en el puerto 443 para establecer esta conexión. Para admitir esta conectividad, debe abrir el puerto 443 del firewall e instalar un certificado SSL público en el servicio IIS del StorageZones Controller.

Implementación de alta disponibilidad del controlador de zonas de almacenamiento

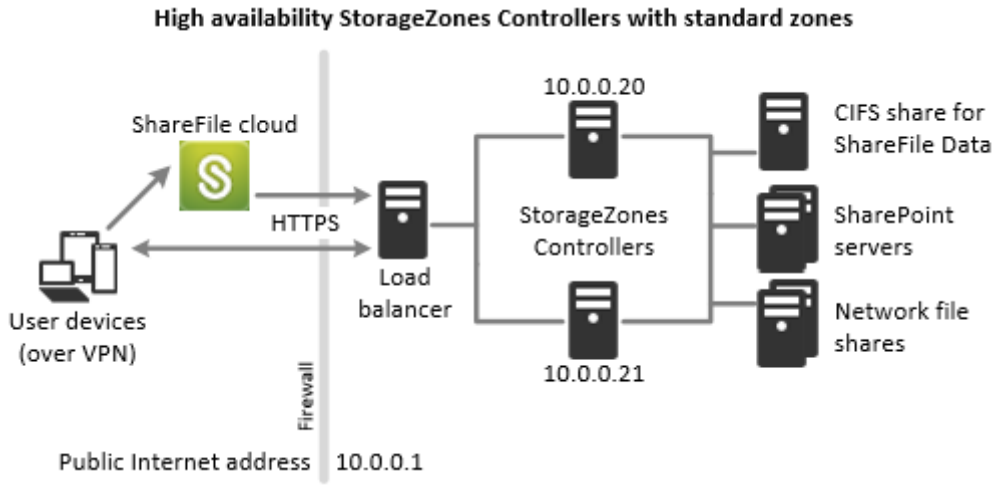
Para una implementación de producción de ShareFile con alta disponibilidad, la práctica recomendada es instalar al menos dos controladores de zonas de almacenamiento. Al instalar el primer controlador, se crea una zona de almacenamiento. Cuando instala los demás controladores, los une a la misma zona. Los controladores de zonas de almacenamiento que pertenecen a la misma zona deben usar el mismo recurso compartido de archivos para el almacenamiento.

En una implementación de alta disponibilidad, los servidores secundarios son controladores de zonas de almacenamiento independientes y en pleno funcionamiento. El subsistema de control de zonas de almacenamiento elige aleatoriamente un controlador de zonas de almacenamiento para las operaciones. Si el servidor principal se desconecta, puede ascender fácilmente un servidor secundario a primario. También puede degradar un servidor de primario a secundario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Implementación de alta disponibilidad para zonas estándar

Los controladores de zonas de almacenamiento configurados para zonas de almacenamiento estándar deben aceptar conexiones entrantes desde la nube de ShareFile. Para ello, cada controlador debe tener una dirección de Internet de acceso público y SSL habilitado para las comunicaciones con la nube de ShareFile. Puede configurar varias direcciones públicas externas, cada una asociada a un controlador de zonas de almacenamiento diferente. La siguiente figura muestra una implementación de alta disponibilidad para zonas de almacenamiento estándar.



Al igual que en el escenario de implementación de la prueba de concepto anterior, un firewall se interpone entre Internet y la red segura. Los controladores de zonas de almacenamiento residen dentro del firewall para controlar el acceso. Las conexiones de usuario a ShareFile deben atravesar el firewall y utilizar el protocolo SSL en el puerto 443 para establecer esta conexión. Para admitir esta conectividad, debe abrir el puerto 443 en el firewall e instalar un certificado SSL público en el servicio IIS de todos los controladores de zonas de almacenamiento.

Configuración de almacenamiento compartido

Los controladores de zonas de almacenamiento que pertenecen a la misma zona de almacenamiento deben usar el mismo recurso compartido de archivos para el almacenamiento. Los controladores de zonas de almacenamiento acceden al recurso compartido mediante el usuario del grupo de cuentas de IIS. De forma predeterminada, los grupos de aplicaciones operan bajo la cuenta de usuario del Servicio de red, que tiene derechos de usuario de bajo nivel. Un controlador de zonas de almacenamiento usa la cuenta de servicio de red de forma predeterminada.

Puede utilizar una cuenta de usuario con nombre en lugar de la cuenta Servicio de red para acceder al recurso compartido. Para usar una cuenta de usuario nominal, especifique el nombre de usuario y la contraseña en la página de configuración de la consola StorageZones. Ejecute el grupo de aplicaciones de IIS y los servicios de ShareFile con la cuenta de servicio de red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conexiones de red

Las conexiones de red varían según el tipo de zona: administrada por ShareFile o estándar.

Zonas administradas por ShareFile En la tabla siguiente se describen las conexiones de red que se producen cuando un usuario inicia sesión en ShareFile y, a continuación, descarga un documento de una zona administrada por ShareFile. Todas las conexiones utilizan HTTPS.

Paso	Origen	Destino
1. Solicitud de inicio de sesión de usuario	Cliente	`company.sharefile.com:443`
2. (Opcional) Redirigir al inicio de sesión del IdP de SAML	Cliente	URL del proveedor de identidades SAML
3. Enumeración de archivos/carpetas y solicitud de descarga	Cliente	`company.sharefile.com:443`
4. Descarga de archivos	Cliente	`storage-location.sharefile.com:443`

Zonas de almacenamiento estándar En la tabla siguiente se describen las conexiones de red que se producen cuando un usuario inicia sesión en ShareFile y, a continuación, descarga un documento de una zona de almacenamiento estándar. Todas las conexiones utilizan HTTPS.

Paso	Origen	Destino
1. Solicitud de inicio de sesión de usuario	Cliente	`company.sharefile.com`
2. (Opcional) Si usa ADFS, redirija al inicio de sesión del IdP de SAML	Cliente	URL del proveedor de identidades SAML
3. Enumeración de archivos/carpetas y solicitud de descarga	Cliente	`company.sharefile.com`
4. Autorización de descarga de archivos	`company.sharefile.com`	`szc.company.com`
5. Descarga de archivos	Cliente	`szc.company.com`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Implementación del proxy DMZ del controlador de zonas de almacenamiento

Una zona desmilitarizada (DMZ) proporciona una capa adicional de seguridad para la red interna. Un proxy DMZ, como Citrix ADC VPX, es un componente opcional que se utiliza para:

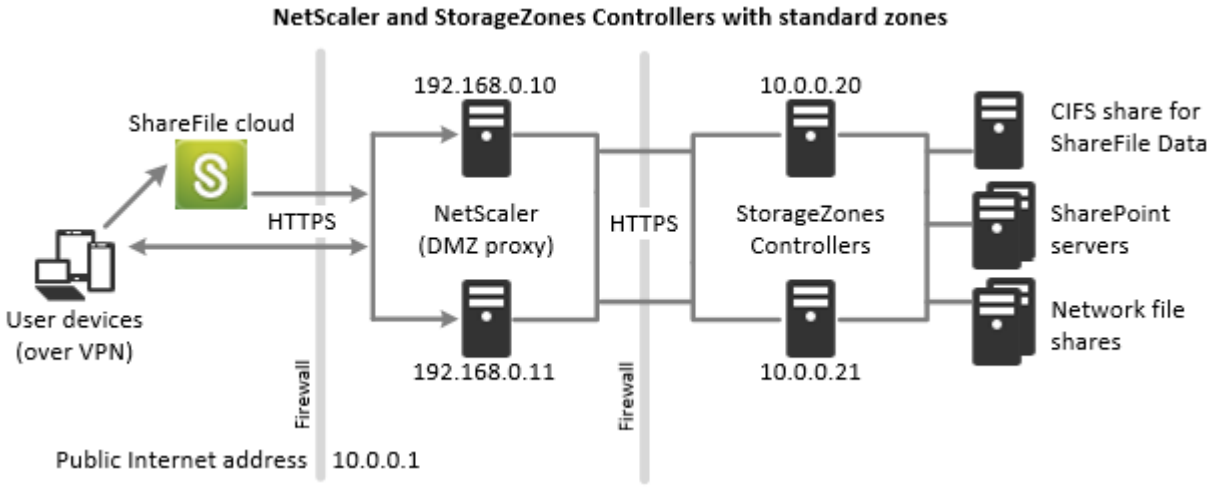
- Asegúrese de que todas las solicitudes a un controlador de zonas de almacenamiento se originen en la nube de ShareFile, de modo que solo el tráfico aprobado llegue a los controladores de zonas de almacenamiento.

  El controlador de zonas de almacenamiento tiene una operación de validación que comprueba si hay firmas de URI válidas para todos los mensajes entrantes. El componente DMZ es responsable de validar las firmas antes de reenviar los mensajes.
- Equilibre la carga de las solicitudes a los controladores de zonas de almacenamiento mediante indicadores de estado en tiempo real.

  La carga de las operaciones se puede equilibrar en los controladores de zonas de almacenamiento si todos pueden acceder a los mismos archivos.
- Descargue el SSL de los controladores de zonas de almacenamiento.
- Asegúrese de que las solicitudes de archivos en SharePoint o en unidades de red estén autenticadas antes de pasar por la DMZ.

Implementación de Citrix ADC y controlador de zonas de almacenamiento

Implementación para zonas de almacenamiento estándar Los controladores de zonas de almacenamiento configurados para zonas estándar deben aceptar conexiones entrantes desde la nube de ShareFile. Para ello, el Citrix ADC debe tener una dirección de Internet de acceso público y SSL habilitado para las comunicaciones con la nube ShareFile.



En este escenario, dos firewalls se interponen entre Internet y la red segura. Los controladores de zonas de almacenamiento residen en la red interna. Las conexiones de usuario a ShareFile deben

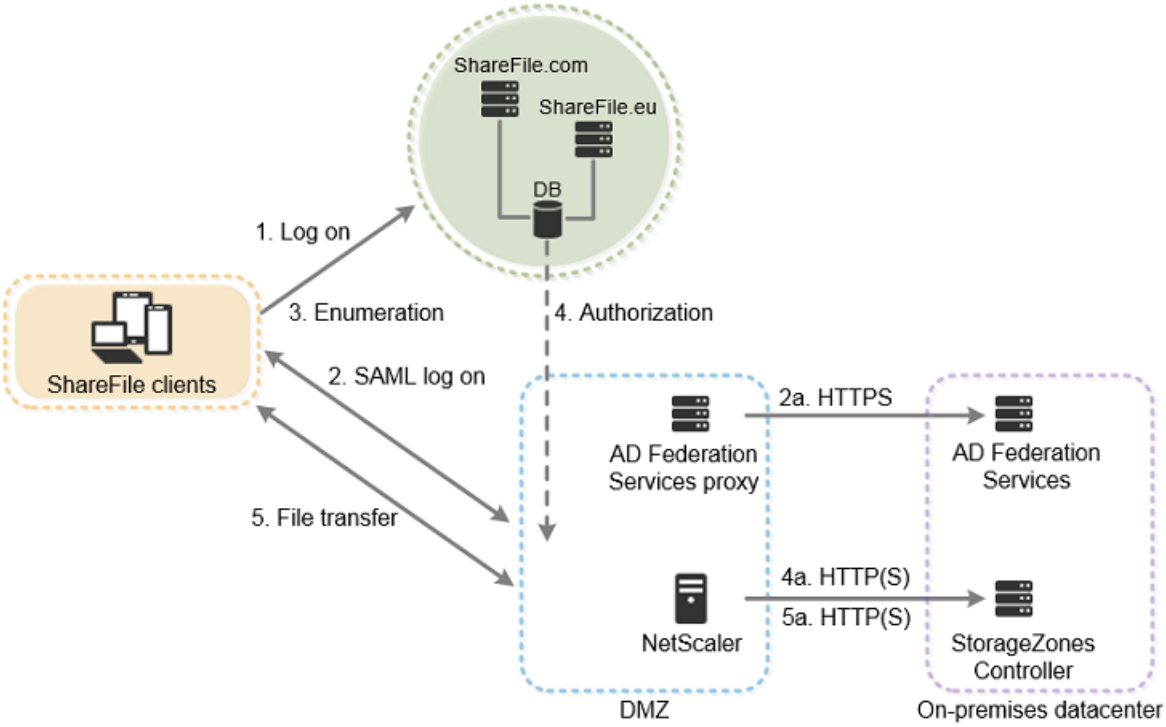
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

atravesar el primer firewall y usar el protocolo SSL en el puerto 443 para establecer esta conexión. Para admitir esta conectividad, debe abrir el puerto 443 del firewall e instalar un certificado SSL público en el servicio IIS de los servidores proxy DMZ (si terminan la conexión del usuario).

Conexiones de red para zonas estándar

En el diagrama y la tabla siguientes se describen las conexiones de red que se producen cuando un usuario inicia sesión en ShareFile y, a continuación, descarga un documento desde una zona estándar implementada detrás de Citrix ADC. En este caso, la cuenta utiliza Servicios de federación de Active Directory (ADFS) para el inicio de sesión de SAML.

El tráfico de autenticación se gestiona en la DMZ mediante un servidor proxy ADFS que se comunica con un servidor ADFS de la red de confianza. Se accede a la actividad de los archivos a través de Citrix ADC en la DMZ, que termina el SSL, autentica las solicitudes de los usuarios y, a continuación, accede al controlador de zonas de almacenamiento de la red de confianza en nombre de los usuarios autenticados. Se accede a la dirección externa de Citrix ADC para ShareFile mediante el FQDN de Internet szc.company.com.



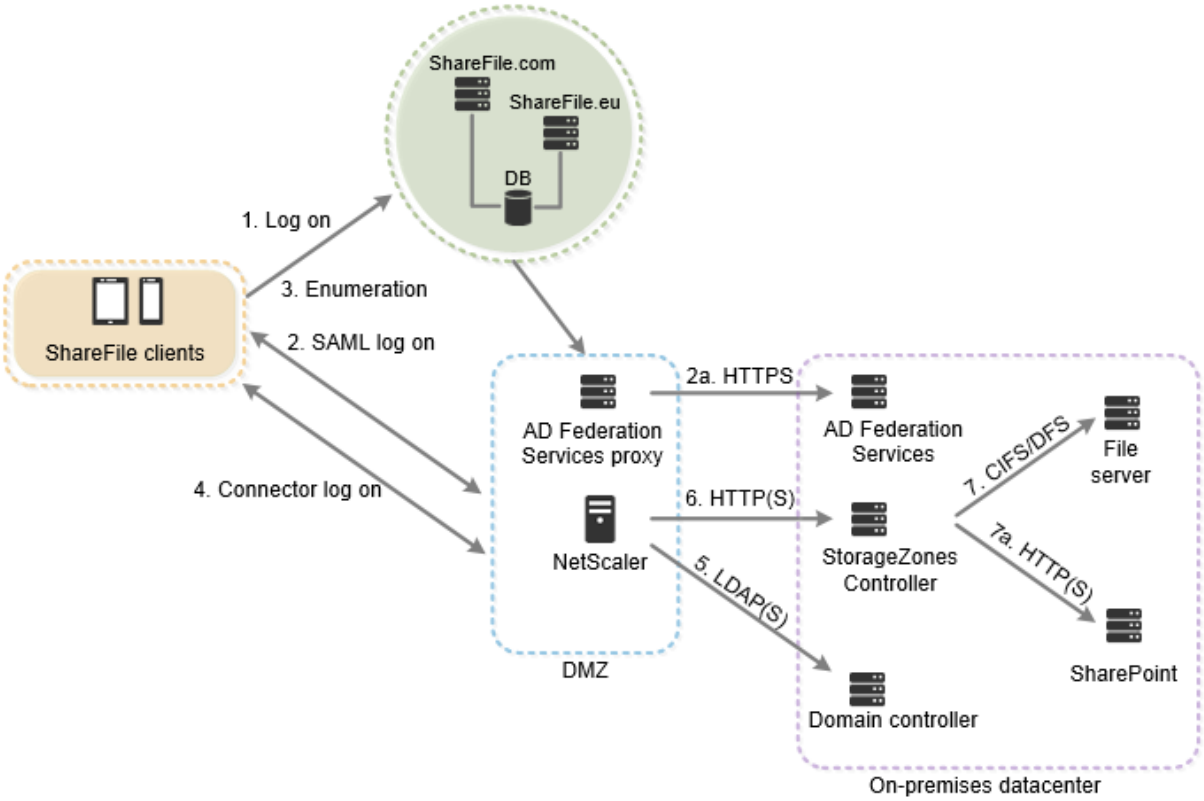
Paso	Origen	Destino	Protocolo
1. Solicitud de inicio de sesión de usuario	Cliente	`company.sharefile.com`	HTTPS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paso	Origen	Destino	Protocolo
2. (Opcional) Redirigir al inicio de sesión del IdP de SAML	Cliente	URL del proveedor de identidades SAML	HTTPS
2a. Inicio de sesión en ADFS	Proxy ADFS	Servidor ADFS	HTTPS
3. Enumeración de archivos/carpetas y solicitud de descarga	Cliente	company.sharefile.com	HTTPS
4. Autorización de descarga de archivos	ShareFile	szc.company.com (dirección externa)	HTTP (S)
4a. Autorización de descarga de archivos	IP de NetScaler ADC (NSIP)	controlador de zonas de almacenamiento	HTTPS
5. Descarga de archivos	Cliente	szc.company.com (dirección externa)	HTTPS
5a. Descarga de archivos	IP de NetScaler ADC (NSIP)	controlador de zonas de almacenamiento	HTTP (S)

El siguiente diagrama y tabla amplían el escenario anterior para mostrar las conexiones de red de los StorageZone Connectors. Este escenario incluye el uso de NetScaler en la DMZ para terminar el SSL y realizar la autenticación de usuario para el acceso a los conectores.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

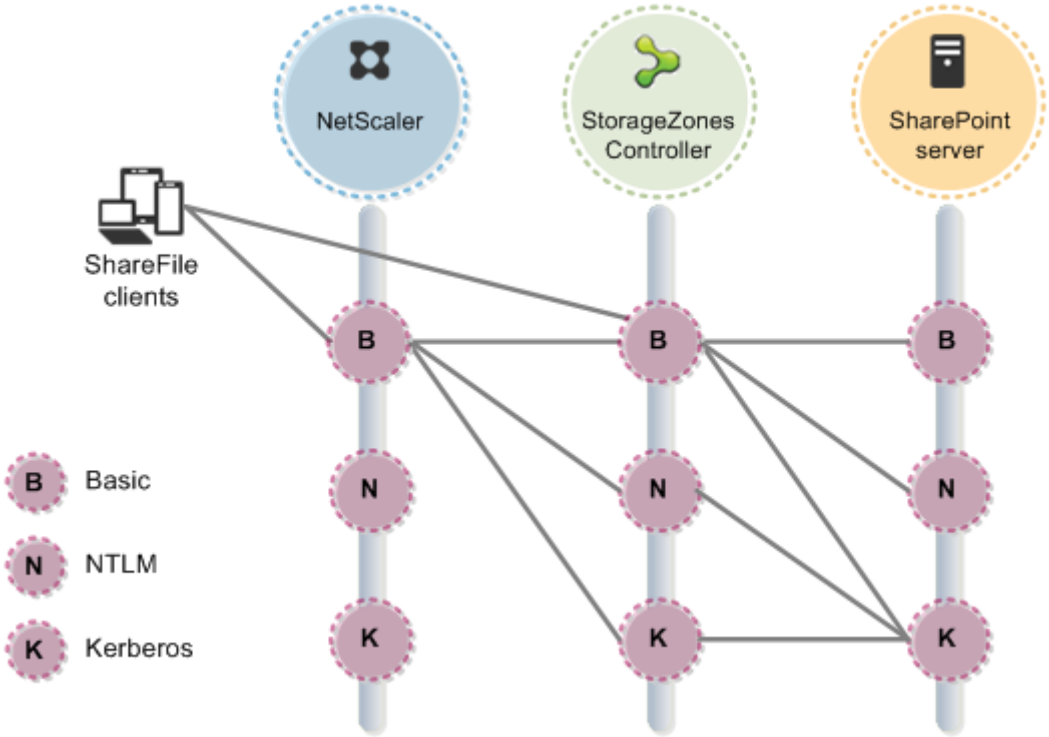


Paso	Origen	Destino	Protocolo
1. Solicitud de inicio de sesión de usuario	Cliente	company.sharefile.com	HTTPS
2. (Opcional) Redirigir al inicio de sesión del IdP de SAML	Cliente	URL del proveedor de identidades SAML	HTTPS
2a. Inicio de sesión en ADFS	Proxy ADFS	Servidor ADFS	HTTPS
3. Enumeración de conectores de nivel superior	Cliente	company.sharefile.com	HTTPS
4. Inicio de sesión del usuario en el servidor del controlador de zonas de almacenamiento	Cliente	szc.company.com (dirección externa)	HTTPS
5. Autenticación de usuarios	IP de NetScaler ADC (NSIP)	Controlador de dominio de AD	LDAP(S)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paso	Origen	Destino	Protocolo
6. Enumeración de archivos/carpetas y solicitudes de carga/descarga	IP de NetScaler ADC (NSIP)	controlador de zonas de almacenamiento	HTTP (S)
7. Enumeración y carga/descarga de recursos compartidos de red	Controlador de zonas de almacenamiento	Servidor de archivos	CIFS o DFS
7a. Enumeración y carga/descarga de SharePoint	Controlador de zonas de almacenamiento	SharePoint	HTTP (S)

El siguiente diagrama resume las combinaciones de tipos de autenticación admitidas en función de si el usuario se autentica.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos del sistema

November 16, 2023

> **Importante:**
>
> Microsoft finalizará el soporte para Windows Server 2012R2 el 10 de octubre de 2023. Es importante migrar el servidor a una versión más reciente antes de la fecha de finalización del soporte.

Controlador de zonas de almacenamiento

- Una máquina física o virtual dedicada con 2 CPU y 4 GB de RAM
- Windows Server 2012 R2 (centro de datos, estándar o Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Para zonas de almacenamiento estándar:

- Utilice un nombre de host de Internet que pueda resolverse públicamente (no una dirección IP).
- Habilite SSL para las comunicaciones con ShareFile.
  - Los dispositivos de usuario y los servidores web de ShareFile deben confiar en el certificado SSL del controlador de zonas de almacenamiento. Si usa SSL directamente con IIS, consulte http://support.microsoft.com/kb/298805 para obtener información sobre la configuración de SSL.
- Permita las solicitudes TCP entrantes en el puerto 443 a través de su firewall.
- Permita que las solicitudes TCP salientes lleguen al plano de control de ShareFile en el puerto 443 a través de su firewall.
  - Haga clic aquí para obtener una lista detallada de los rangos de IP y los dominios.

Para la comprobación del estado del servidor, utilizada solo para las zonas de almacenamiento de datos de ShareFile:

- Abra el puerto 80 en el servidor local.

Para un entorno de producción de alta disponibilidad:

- Un mínimo de dos servidores con el controlador de zonas de almacenamiento instalado.
- Si no utiliza servidores proxy de la DMZ, instale un certificado SSL en el servicio IIS.

  Para obtener información acerca de los certificados admitidos, consulte los requisitos de certificado para las zonas estándar anteriores.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para la implementación de un proxy en la DMZ:

- Uno o más servidores proxy de DMZ, como instancias de Citrix ADC VPX.
- Para un servidor proxy DMZ que termina la conexión del cliente y utiliza HTTP, instale un certificado SSL en el servidor proxy.

  Si las comunicaciones entre el servidor proxy de la DMZ y el controlador de zonas de almacenamiento son seguras, puede utilizar HTTP. Sin embargo, se recomienda usar HTTPS como práctica recomendada. Si usa HTTPS, puede usar un certificado privado (empresarial) en el controlador de zonas de almacenamiento si el proxy de la DMZ confía en él. La dirección externa expuesta por el proxy de la DMZ debe utilizar un certificado de confianza comercial. Para obtener información acerca de los certificados admitidos, consulte los requisitos de certificado para las zonas estándar anteriores.

Otros requisitos

> **Nota:**
>
> ShareFile no admite oficialmente ni recomienda utilizar la replicación de DFS. Se sabe que causa errores de bloqueo para archivos más grandes. Si se debe usar la replicación DFS, use soluciones de reserva separadas durante las horas de menor actividad cuando la zona no esté en uso activo.

- El instalador del controlador de zonas de almacenamiento requiere privilegios de administrador.
- Para la administración remota del controlador de zonas de almacenamiento, utilice un protocolo remoto, como RDP o Citrix ICA, para conectarse al servidor y, a continuación, abrir la consola del controlador de zonas de almacenamiento.

Sistemas de almacenamiento de terceros compatibles

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

Soluciones de prevención de pérdida de datos compatibles

- El controlador de zonas de almacenamiento se integra con cualquier solución DLP compatible con ICAP, que incluye:
  - Prevención de pérdida de datos de Symantec
  - McAfee DLP Prevent
  - Websense TRITON AP-DATA
  - Prevención de pérdida de datos de RSA

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Zonas de almacenamiento para datos de ShareFile

Las zonas de almacenamiento de datos de ShareFile son una función opcional que se habilita en un controlador de zonas de almacenamiento.

Requisitos:

- Cuenta ShareFile Enterprise, con la función de zona de almacenamiento habilitada
- Una cuenta de usuario de ShareFile que incluye permisos para crear y administrar zonas
- Un recurso compartido de CIFS para almacenamiento privado de datos

Si tiene previsto almacenar archivos de ShareFile en un sistema de almacenamiento de terceros compatible, el recurso compartido de CIFS se utiliza para archivos temporales (claves de cifrado, archivos en cola) y como caché de almacenamiento temporal.

- El rol Servidor web (IIS) y ASP.NET 4.x. Para obtener más información, consulte Preparar el servidor para los datos de ShareFile.

Nota: El acceso a una cuenta de ShareFile desde un cliente FTP no es compatible con las zonas de almacenamiento de datos de ShareFile.

Conector de zona de almacenamiento para SharePoint

El conector de zonas de almacenamiento para SharePoint es una función opcional que se habilita en un controlador de zonas de almacenamiento.

Requisitos:

- Cuenta ShareFile Enterprise, con la función de zona de almacenamiento habilitada, o Citrix Endpoint Management.
- Solo se admiten **Microsoft SharePoint Server 2010 y versiones posteriores**.
- El servidor del controlador de zonas de almacenamiento debe ser miembro del dominio y estar en el mismo bosque que el servidor de SharePoint.
- El rol Servidor web (IIS) y ASP.NET 4.x. Para obtener más información, consulte Preparar el servidor para los datos de ShareFile.
- Directivas de SharePoint:
  - El tamaño máximo predeterminado del archivo de carga para una aplicación web en SharePoint 2013 es de 250 MB y en SharePoint 2010 es de 50 MB. Para cambiar el valor predeterminado: en la Administración central de SharePoint, vaya a la página de configuración general de la aplicación web y cambie el tamaño máximo de carga. El límite de tamaño del archivo de carga para SharePoint es de 2 GB.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Los clientes de ShareFile siempre intentan archivar una versión principal (publicación) de un archivo. Sin embargo, las directivas de SharePoint determinan si un archivo se registra como una versión principal o secundaria.
  - El permiso SharePoint View-Only no permite a los usuarios descargar archivos. Para leer un archivo de un cliente de ShareFile, un usuario de SharePoint debe tener permiso de lectura.

- Dispositivos de usuario: para obtener la información más reciente sobre la compatibilidad de los dispositivos de usuario con los conectores de zonas de almacenamiento, consulte la base de conocimientos de ShareFile.

Conector de zona de almacenamiento para la autenticación de SharePoint

Tras autenticar al usuario, el servidor del controlador de zonas de almacenamiento establece conexiones con el servidor de SharePoint en nombre del usuario autenticado y responde a los desafíos de autenticación presentados por el servidor de SharePoint. El conector de zona de almacenamiento para SharePoint admite los siguientes métodos de autenticación en el servidor de SharePoint.

- Básica

  Requiere que agregue `<add key="CacheCredentials"value="1"\>` a `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.

- Negociar (Kerberos)
- Desafío/Respuesta de Windows (NTLM)

Los clientes móviles de ShareFile utilizan la autenticación básica a través de HTTPS para autenticarse en el controlador de zonas de almacenamiento o en el proxy de la DMZ. El inicio de sesión único en SharePoint se rige por los requisitos de autenticación establecidos en el servidor de SharePoint. Para utilizar la autenticación Kerberos o NTLM en el servidor de SharePoint: configure el controlador de dominio para que confíe en el controlador de zonas de almacenamiento para la delegación.

Si el servidor de SharePoint está configurado para la autenticación Kerberos: configure un nombre principal de servicio (SPN) para las cuentas de servicio de usuario nombradas del grupo de aplicaciones del servidor de SharePoint. Para obtener más información, consulte “Configurar la confianza para la delegación de elementos web”en http://support.microsoft.com/kb/832769.

Para las implementaciones con Citrix ADC, es posible finalizar la autenticación básica en Citrix ADC y, a continuación, realizar otros tipos de autenticación en el controlador de zonas de almacenamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Conector de zona de almacenamiento para archivos compartidos de red

El conector de zonas de almacenamiento para recursos compartidos de archivos en red es una función opcional que se habilita en un controlador de zonas de almacenamiento.

Requisitos:

- Cuenta de ShareFile Enterprise o Citrix Endpoint Management.
- El servidor del conector de la zona de almacenamiento debe ser miembro del dominio y estar en el mismo bosque que los servidores de archivos de la red.
- El rol Servidor web (IIS) y ASP.NET 4.x. Para obtener más información, consulte Preparar el servidor para los datos de ShareFile.
- Dispositivos de usuario: para obtener la información más reciente sobre la compatibilidad de los dispositivos de usuario con los conectores de zonas de almacenamiento, consulte la base de conocimientos de ShareFile.

Conector para autenticación de archivos compartidos en red

Tras autenticar al usuario, el servidor del controlador de zonas de almacenamiento establece conexiones con el servidor de archivos de red en nombre del usuario autenticado y responde a los desafíos de autenticación presentados por el servidor de archivos. El conector de zona de almacenamiento para recursos compartidos de archivos en red admite los siguientes métodos de autenticación en el servidor de archivos.

- Negociar (Kerberos)
- Desafío/Respuesta de Windows (NTLM)

Para utilizar la autenticación Kerberos o NTLM en el controlador de zonas de almacenamiento: configure el controlador de dominio para que confíe en el controlador de zonas de almacenamiento para ladelegación.

Para implementaciones con Citrix ADC: para ofrecer a los usuarios una experiencia de inicio de sesión único cuando Citrix ADC esté configurado para la autenticación básica, configure el conector para la autenticación Negotiate (Kerberos) y NTLM.

Scripts y comandos de PowerShell

La instalación del controlador de zonas de almacenamiento incluye varios scripts y comandos de PowerShell, que se encuentran en `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\`.

- Ejecute los scripts en la versión de 32 bits (x86) de PowerShell.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para obtener los mejores resultados, actualice a PowerShell 4.0 o posterior, incluido en Windows Management Framework.

  PowerShell 2.0 causa problemas significativos debido a problemas de compatibilidad con .NET Framework 4.

Instalación

October 13, 2020

Complete las siguientes tareas, en el orden que se presenta, para instalar y configurar el controlador de zonas de almacenamiento, las zonas de almacenamiento para datos de ShareFile y los conectores de zonas de almacenamiento.

1. Configurar Citrix ADC para los controladores de zonas de almacenamiento

   Puede usar Citrix ADC como proxy DMZ para controlador de zonas de almacenamiento.

2. Crear un recurso compartido de red para el almacenamiento de datos privados

   Las zonas de almacenamiento para ShareFile Data requieren un recurso compartido de red para los datos privados, incluso si almacena archivos ShareFile en un sistema de almacenamiento de terceros compatible.

3. Instalar un certificado SSL

   Un controlador de zonas de almacenamiento que hospeda zonas estándar requiere un certificado SSL.

4. Preparar el servidor para los datos de ShareFile

   La instalación de IIS y ASP.NET es necesaria para las zonas de almacenamiento para los datos de ShareFile y para los StorageZone Connectors.

5. Instalar el controlador de zonas de almacenamiento y crear una zona de almacenamiento

6. Verificar la configuración del controlador de zonas de almacenamiento

7. Cambiar la zona predeterminada para las cuentas de usuario

   De forma predeterminada, las cuentas de usuario existentes y recién aprovisionadas utilizan el almacenamiento en la nube administrado por ShareFile como zona predeterminada.

8. Especificar un servidor proxy para las zonas de almacenamiento

   La consola de controlador de zonas de almacenamiento permite especificar un servidor proxy para controlador de zonas de almacenamiento. También puede especificar un servidor proxy mediante otros métodos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. Configurar el controlador de dominio de modo que confíe en el controlador de zonas de almacenamiento para la delegación

   Configure el controlador de dominio para admitir la autenticación NTLM o Kerberos en recursos compartidos de red o sitios de SharePoint.

10. Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento

    Para configurar una zona de almacenamiento para alta disponibilidad, conecte al menos dos controladores de zonas de almacenamiento.

Para una demostración de la configuración del controlador de zonas de almacenamiento con Microsoft Azure Storage,haga clic aquí.

Para obtener una demostración de cómo configurar ShareFile Enterprise para usar una zona de almacenamiento de Microsoft Azure, haga clic aquí.

Instrucciones de configuración adicionales

- Configurar zonas de almacenamiento multiarrendatario
- Configurar el controlador de zonas de almacenamiento para vistas previas de aplicaciones web, miniaturas y uso compartido solo de vista

Configurar Citrix ADC para los controladores de zonas de almacenamiento

February 9, 2022

NetScaler, versión 10.1 build 120.1316.e y posteriores, incluye un asistente que le pide información básica sobre el entorno del controlador de zonas de almacenamiento. A continuación, genera una configuración que:

- Equilibra la carga del tráfico entre los controladores de zonas de almacenamiento
- Proporciona autenticación de usuarios para conectores de zonas de almacenamiento
- Valida las firmas URI para cargas y descargas de ShareFile
- Termina las conexiones SSL en el dispositivo Citrix ADC

El diagrama muestra estos componentes de Citrix ADC creados por la configuración:

- **Servidor virtual de conmutación de contenido Citrix ADC:** envía solicitudes de datos de los usuarios desde ShareFile y desde los conectores de zona de almacenamiento al servidor virtual de equilibrio de carga de Citrix ADC apropiado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Servidor virtual de equilibrio de carga Citrix ADC:** la carga equilibra el tráfico de los controladores de zonas de almacenamiento y también gestiona lo siguiente:
  - Para las solicitudes de datos de su almacenamiento de datos privado, un servidor virtual de equilibrio de carga realiza la validación de hash para garantizar que las firmas URI válidas estén presentes en las solicitudes entrantes.
  - Para las solicitudes de datos de los conectores de zonas de almacenamiento, un servidor virtual de equilibrio de carga puede realizar la autenticación del usuario. Detiene una solicitud de usuario en Citrix ADC, autentica al usuario y, a continuación, realiza el inicio de sesión único del usuario en el controlador de zonas de almacenamiento.

> **Nota:**
>
> La autenticación en los conectores de zonas de almacenamiento a través de Citrix ADC es opcional. Debido a un problema conocido, si la autenticación está habilitada en Citrix ADC, los conectores de zona de almacenamiento de WebApp no funcionan en los exploradores Chrome, Chromium, Safari y Edge. Es compatible con otros exploradores y clientes de escritorio/móviles.

A partir del controlador de zonas de almacenamiento 4.0, los administradores pueden limitar las conexiones entrantes a los controladores de zonas de almacenamiento a TLS v1.2. Si los protocolos anteriores a TLS v1.2 están inhabilitados para el tráfico entrante al controlador de la zona de almacenamiento, todos los componentes del software cliente que interactúan con la zona de almacenamiento también deben admitir TLS v1.2. Haga clic aquí para obtener información adicional e instrucciones de configuración.

> **Nota:**
>
> Para configurar versiones de NetScaler anteriores a 10.1 compilación 120.1316.e, consulte Configurar Citrix ADC manualmente.

La configuración del asistente Citrix ADC para ShareFile no controla la configuración requerida para usar Citrix Endpoint Management como proveedor de identidad SAML para ShareFile. Para obtener más información, haga clic aquí.

Requisitos previos

- Una configuración de Citrix ADC que funcione
- Certificado de seguridad: si uno aún no está disponible en Citrix ADC, el asistente le permite instalar uno en el servidor virtual de conmutación de contenido.
- Información sobre la configuración de Active Directory (**el asistente Citrix ADC para ShareFile debe completarse con la licencia de Citrix NetScaler Enterprise Edition**):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Dirección IP y puerto del servidor de Active Directory
- Nombre de dominio de Active Directory
- DN base LDAP donde se almacenan los usuarios
- Nombre de cuenta y contraseña de una cuenta de administrador que tiene permisos para comunicarse con Active Directory

Configurar Citrix ADC para controladores de zonas de almacenamiento

En los siguientes pasos se describe cómo utilizar el asistente Citrix ADC para ShareFile.

1. Inicie sesión en el dispositivo Citrix ADC y, en la ficha Configuración, vaya a Administración del tráfico.
2. En Citrix ShareFile, haga clic en Configurar Citrix ADC para ShareFile.

   También puede acceder al asistente de la siguiente manera: En Movilidad, haga clic en **Configurar Endpoint Management, ShareFile y Citrix Gateway**.
3. Proporcione la información solicitada en el asistente.

Opción	Descripción
Nombre	Nombre para mostrar del servidor virtual de conmutación de contenido.
Dirección IP	La dirección IP externa (pública o DMZ) que se utilizará para el servidor virtual de conmutación de contenido. Si usa una dirección IP DMZ, debe definir una asignación de traducción de direcciones de red (NAT) desde su dirección de firewall externo a esta dirección IP DMZ.
Datos de ShareFile	Esta opción está habilitada, lo que indica que utilizará la conexión Citrix ADC para las zonas de almacenamiento de datos de ShareFile.
conectores de zona de almacenamiento para recursos compartidos de archivos de red/SharePoint	Si usa conectores y quiere realizar la autenticación de usuarios en Citrix ADC, seleccione la casilla de verificación.
Certificado	Elija un certificado o instale uno para el servidor virtual de conmutación de contenido. Si elige instalar un certificado, se le pedirá que cargue el certificado y la clave privada. Para las zonas estándar, los certificados deben ser de confianza pública y no autofirmados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
dirección IP del controlador de zonas de almacenamiento	Las direcciones IP internas de uno o más servidores de controladores de zonas de almacenamiento. Estas direcciones IP definen los servidores del controlador de zonas de almacenamiento como entidades dentro de Citrix ADC. Si ya agregó los servidores a Citrix ADC, haga clic en Agregar de existente y seleccione los servidores. Para usar Citrix ADC para el equilibrio de carga, introduzca una dirección IP interna para cada servidor del controlador de zonas de almacenamiento. Para usar Citrix ADC solo para SSL y autenticación, introduzca solo una dirección IP.
Puerto y protocolo	El puerto y el protocolo utilizados para la comunicación desde Citrix ADC a los controladores de zonas de almacenamiento.
La dirección IP del servidor virtual de autenticación, autorización y auditoría (Citrix ADC AAA)	Una dirección IP interna no utilizada para el servidor virtual AAA de Citrix ADC. Citrix ADC crea este servidor virtual para su propio uso. El servidor no requiere acceso externo.
Dirección IP y puerto del servidor LDAP	La dirección IP y el puerto del servidor de Active Directory. Si ya agregó un servidor LDAP a Citrix ADC, haga clic en la ficha Elegir LDAP y elija el servidor.
Se acabó el tiempo	El número máximo de segundos que Citrix ADC espera una respuesta del servidor LDAP. El valor predeterminado es 3 segundos. El valor mínimo es de 1 segundo.
Dominio de inicio de sesión único	El nombre de dominio de Active Directory.
DN base (ubicación de los usuarios)	Nombre distintivo (DN) base de LDAP en el que se almacenan los usuarios. Especifique el DN con el formato general: CN=Users, dc=domain, DC=net
DN y contraseña de enlace de administrador	Una cuenta de administrador que tiene permisos para comunicarse con Active Directory.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
Nombre de inicio de sesión	Atributo LDAP, utilizado por Citrix ADC para determinar si los usuarios inician sesión con su nombre de usuario o dirección de correo electrónico. El valor predeterminado es sAMAccountName, que permite a los usuarios iniciar sesión con sus nombres de usuario. Para solicitar a los usuarios que introduzcan su dirección de correo electrónico para iniciar sesión, cambie este campo a userPrincipalName.

Configurar Citrix ADC para el acceso web a los conectores

Para admitir el acceso web a los conectores de zonas de almacenamiento, debe realizar una configuración adicional de Citrix ADC después de completar el asistente de Citrix ADC para ShareFile.

- Cree y configure un tercer servidor virtual de equilibrio de carga de Citrix ADC, que se utiliza para garantizar que los clientes de ShareFile envíen credenciales solo cuando inicien sesión en un dominio de ShareFile de confianza.

  Como se describe en los pasos siguientes, configurará el servidor virtual adicional para permitir el acceso anónimo de los clientes para el verbo HTTP OPTIONS. La solicitud OPTIONS pasa al controlador de zonas de almacenamiento sin autenticarse y sin llamadas HTTPS para validar la firma. La comprobación previa de CORS valida la confianza del dominio antes de enviar las credenciales.

  No es necesario comprender CORS para realizar la configuración. Sin embargo, para obtener más información sobre CORS, consulte http://enable-cors.org/.

- Para admitir el acceso web a los conectores de zonas de almacenamiento, agregue una ruta (/ProxyService) a la directiva de conmutación de contenido utilizada para el tráfico a /cifs y /sp.

Realice los siguientes pasos en Citrix ADC después de completar el asistente de Citrix ADC para ShareFile.

1. Cree un tercer servidor virtual de equilibrio de carga:

   a) Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.

   b) Haga clic en Agregar.

   c) Especifique los valores siguientes:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Valor
Nombre	Un nombre de directiva, como SF_ZONE_OPTIONS
Protocolo	SSL
Tipo de dirección IP	No direccionable

d) Haga clic en para crear el servidor virtual.

e) Para vincular los mismos servicios que los servidores virtuales de equilibrio de carga creados por el asistente: En la pantalla Servidor virtual de equilibrio de carga, en Servicio, haga clic en > y, a continuación, en Guardar.

f) Agregue un certificado al servidor virtual.

2. Cree una directiva para el servidor virtual que acaba de agregar:

   a) Vaya a Administración del tráfico > Cambio de contenido > Directivas.

   b) En el panel de detalles, haga clic en Agregar y, a continuación, especifique los valores Nombre, Servidor virtual LB de destino y Expresión. Haga clic en **Editor de expresiones** y, después, cree esta expresión. Selecciona **HTTP**. Seleccione **REQ**. Seleccione **MÉTODO**. Seleccione EQ (cadena) y escriba OPTIONS. La expresión debe ser la siguiente: `HTTP.REQ.METHOD.EQ("OPTIONS")`

   c) Haga clic en **Listo**.

   d) Haga clic en **Crear**.

3. Enlace la directiva que acaba de crear al nuevo servidor virtual de equilibrio de carga:

   a) Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**.

   b) En la lista, haga clic en el servidor virtual y haga clic en **Modificar**.

   c) Vaya a la sección Vinculación de directivas de conmutación de contenido y haga clic en 2 directivas de conmutación de contenido.

   d) Haga clic en **Agregar enlace**.

   e) Seleccione la nueva directiva de contenido y seleccione el servidor virtual de equilibrio de carga de destino.

   f) Haga clic en **Bind**.

   g) Haga clic en **Modificar enlace** y actualice la **prioridad**. Cambie la prioridad de la nueva directiva para que tenga el número más bajo de las tres directivas.

   La directiva con el valor más bajo tiene la prioridad más alta y, por lo tanto, se maneja primero.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Actualice la directiva utilizada para el tráfico a los conectores de zonas de almacenamiento (_SF_CIF_SP_CSPOL):

   a) Vaya a **Administración del tráfico > Cambio de contenido > Directivas**.

   b) Seleccione la directiva _SF_CIF_SP_CSPOL.

   c) Agregue lo siguiente a la expresión de directiva:

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

   La expresión de directiva completa debe ser la siguiente:

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

5. Actualice la directiva utilizada para el tráfico a las zonas de almacenamiento de datos de ShareFile (_SF_SZ_CSPOL):

   a) Vaya a **Administración del tráfico > Cambio de contenido > Directivas**.

   b) Seleccione la directiva **_SF_SZ_CSPOL**.

   c) Agregue lo siguiente a la expresión de directiva:

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

   La expresión de directiva completa debe ser la siguiente:

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

Configurar Citrix ADC para compartir de solo lectura

Para admitir el uso compartido de solo lectura, los usuarios deben poder acceder a Microsoft Office Web Apps Server (OWA). Si su servidor OWA es accesible externamente en su propia dirección, no se debe requerir ninguna configuración adicional de Citrix ADC para el controlador de zonas de almacenamiento.

Si quiere combinar el controlador de zonas de almacenamiento y Office Web App Server en una sola dirección externa mediante directivas de conmutación de contenido de Citrix ADC, debe realizar una configuración adicional de Citrix ADC después de completar el asistente de Citrix ADC para ShareFile. La configuración de Citrix ADC es necesaria para garantizar que el tráfico se enrute correctamente a su servidor OWA de acceso externo.

Una vez configuradas las siguientes reglas de Citrix ADC, los administradores pueden reutilizar la dirección externa existente de su zona de controlador de zonas de almacenamiento, lo que elimina la necesidad de crear una dirección externa adicional para OWA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para crear y configurar un servidor virtual de equilibrio de carga Citrix ADC adicional:

1. Crea un servicio de equilibrio de carga adicional.
   - Vaya a **Administración de Tráfico > Equilibrio de carga > Servicios**.
   - Haga clic en **Agregar**.
   - Introduzca la información requerida para crear un servicio que corresponda a sus servidores de OWA. Haga clic en **Aceptar**.
2. Cree un servidor virtual de equilibrio de carga adicional:
   - Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
   - Haga clic en **Agregar**.
   - Especifique los valores siguientes:

Opción	Valor
Nombre	Un nombre de directiva, como SF_OWA_vServer
Protocolo	SSL
Tipo de dirección IP	No direccionable

   - Haga clic en para crear el servidor virtual.
   - Para vincular el servidor virtual al servicio OWA que creó en el paso anterior, haga clic en **Enlace de servicio virtual de equilibrio de carga > Seleccionar servicio**. Haga clic en la casilla de verificación junto al servicio que creó en el paso anterior.
   - Haga clic en **Seleccionar**.
   - Haga clic en **Bind**.
3. Cree una nueva directiva para enrutar el tráfico a su servidor OWA.
   - Vaya a **Administración del tráfico > Cambio de contenido > Directivas**.
   - Seleccione **Agregar**.
   - Nombra la directiva.
   - Agregue la siguiente expresión:
     - HTTP.REQ.URL.CONTAINS(“/hosting/discovery”)
       || HTTP.REQ.URL.CONTAINS(“/x/”)
       || HTTP.REQ.URL.CONTAINS(“/wv/”)
       || HTTP.REQ.URL.CONTAINS(“/p/”)
       La expresión de directiva completa debe ser la siguiente:
       HTTP.REQ.URL.CONTAINS(“/hosting/discovery”)
       || HTTP.REQ.URL.CONTAINS(”/x/”)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

|| HTTP.REQ.URL.CONTAINS("/wv/")
|| HTTP.REQ.URL.CONTAINS("/p/")

4. Actualizar la prioridad de la nueva directiva en el entorno virtual de equilibrio de carga
   - Vaya a **Administración del tráfico > Cambio de contenido > Servidores virtuales**.
   - Haga clic en el servidor virtual de equilibrio de carga y seleccione Directivas de conmutación de contenido.
   - Cambie la prioridad de las directivas para que la directiva (Ejemplo) "_SF_OWA"sea la tercera en prioridad.

Prioridad	Nombre de la directiva
90	SF_ZK_OPTIONS
95	_SF_CIF_SP_SPOL
99	_SF_OWA
100	_SF_SZ_CSPOL

   - Haga clic en **Cerrar**. Haga clic en **Listo**.

Crear un monitor para el servicio de controlador de zonas de almacenamiento

De forma predeterminada, Citrix ADC hace ping al servidor del controlador de zonas de almacenamiento para determinar si está en línea. Sin embargo, incluso si el controlador está en línea, es posible que no pueda enviar mensajes de latido al sitio web de ShareFile. En ese caso, Citrix ADC enviará tráfico al controlador de zonas de almacenamiento aunque no se comunique con ShareFile.

Para verificar la conectividad saliente del controlador de zonas de almacenamiento a ShareFile, puede crear un monitor que compruebe heartbeat.aspx y lo vincule al servicio Citrix ADC para cada controlador de zonas de almacenamiento.

```
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 es el servicio Citrix ADC que corresponde a un controlador de zonas de almacenamiento. El asistente Citrix ADC para ShareFile crea automáticamente ese nombre de servicio. El nombre del servicio incluye la dirección IP del controlador, como SF_SVC_ip-address.

-secure YES se requiere si el servicio escucha en el puerto 443.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comprobar la configuración de Citrix ADC

Después de completar el asistente, vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales** para ver el estado de los servidores virtuales de equilibrio de carga creados por el asistente.

Ver el rendimiento de las solicitudes de ShareFile a través de Citrix ADC

Las estadísticas de rendimiento se pueden encontrar en el menú **Panel** de control.

Configurar Citrix ADC manualmente

April 20, 2023

A partir de la versión 10.1, versión 120.1316, NetScaler incluye un asistente que configura los ajustes necesarios para los datos y conectores del controlador de zonas de almacenamiento.

Los pasos de esta sección describen la configuración de **Citrix ADC** necesaria para el controlador de zonas de almacenamiento. Todos los enlaces son para la documentación de NetScaler 10.1. Hay temas similares disponibles para las versiones posteriores de Citrix ADC.

Para comprobar si hay firmas de URI válidas en todos los mensajes entrantes

1. Cree una llamada HTTP denominada sf_callout:
   a) En el cuadro de diálogo Configurar llamada HTTP, haga clic en **Servidor virtual o Dirección IP** y especifique la dirección.
   b) En Solicitud de envío al servidor, haga clic en **Basado en atributos** y, a continuación, en **Configurar atributos de solicitud**.
   c) Seleccione **Get Method**.
   d) En Expresión del host, introduzca la dirección IP del servidor virtual o la dirección IP del host de cualquiera de los controladores de zonas de almacenamiento.
   e) En la Expresión del vástago URL, escriba:

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

   f) Haga clic en **Aceptar** y, a continuación, vuelva al cuadro de diálogo Configurar llamada HTTP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

g) En Respuesta del servidor, elija un tipo de retorno Booleano.

h) En la Expresión para extraer datos de la respuesta, introduzca:

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

i) Haga clic en **Crear**.

2. Siga los pasos anteriores para configurar una llamada HTTP denominada sf_callout_y. Utilice la misma configuración excepto para la expresión:

   - En la Expresión del vástago URL, escriba:

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

3. Configurar una directiva de respuesta:

   a) En el cuadro de diálogo Configurar directiva de respondedor: Para Acción, elija Soltar.

   b) Introduzca la expresión:

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

   Para obtener más información, consulte Respondedor.

4. Vincule la directiva de respuesta al servidor virtual del equilibrador de cargas y configure la persistencia basada en sesiones SSL.

Para equilibrar la carga

1. Configure el equilibrio de carga basado en tokens.

   Utilice la expresión de la regla: “`http.REQ.URL.QUERY.VALUE("uploadid")`”

   El equilibrio de carga basado en tokens es necesario para los controladores de zonas de almacenamiento en una implementación de alta disponibilidad. El equilibrio de carga por turnos produce errores de carga o descarga intermitentes, ya que la solicitud de un cliente de carga o descarga puede dirigirse a un controlador de zona de almacenamiento distinto del que recibió la solicitud de autorización de ShareFile.com.

2. Configure Citrix ADC para terminar las conexiones SSL.

   Para obtener más información, consulte Configurar la descarga de SSL.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para configurar la conmutación y la autenticación de contenido para Connectors

1. Para habilitar el cambio de contenido, consulte Habilitar el cambio de contenido.
2. Cree una directiva de cambio de contenido para las solicitudes de los usuarios de datos de ShareFile desde sus zonas de almacenamiento locales:

   a) En el cuadro de diálogo Configurar la directiva de cambio de contenido, introduzca un nombre para la directiva de cambio de contenido. En estos pasos se utiliza el nombre Data_Requests.

   b) Introduzca la expresión:

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

   c) Haga clic en **Aceptar**.

   Para obtener más información, consulte Cambio de contenido.

3. Cree una directiva de cambio de contenido para las solicitudes de los usuarios de datos a los que se accede desde los conectores de zonas de almacenamiento.

   a) En el cuadro de diálogo Configurar la directiva de cambio de contenido, especifique un nombre para la directiva de cambio de contenido. En estos pasos se utiliza el nombre Connector_Solicitudes.

   b) Introduzca la expresión:

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

   Asegúrese de reemplazar “StorageZonesControllerFQDN”por el FQDN de su controlador.

   c) Haga clic en **Aceptar**.

4. Cree un servidor virtual de conmutación de contenido.
5. Establezca los destinos de directiva de conmutación de contenido:

   - En el cuadro de diálogo Configurar servidor virtual (cambio de contenido), para la directiva Data_Requests, especifique el servidor virtual del equilibrador de carga para las zonas de almacenamiento de datos de ShareFile.

     Este servidor virtual de equilibrador de carga es el que vincula la directiva de respuesta en el paso 4 para comprobar si hay firmas de URI válidas en todos los mensajes entrantes y para equilibrar la carga.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para la directiva Connector_Requests, especifique el servidor virtual del equilibrador de cargas para los conectores de zonas de almacenamiento.

6. Configure el servidor virtual de autenticación para la controladora de zonas de almacenamiento:

   Aunque la autenticación en Citrix ADC es opcional, es una práctica recomendada.

   a) En el panel de navegación, expanda Equilibrio de carga, seleccione el nombre del servidor virtual del equilibrador de cargas para los conectores de zonas de almacenamiento y, a continuación, haga clic en Abrir.

   b) En el cuadro de diálogo Configurar servidor virtual (equilibrio de carga), haga clic en la ficha Avanzado y, a continuación, expanda los parámetros de autenticación.

   c) Marque la casilla de la autenticación basada en 401 y, a continuación, elija el servidor virtual de autenticación.

   d) Haga clic en la ficha **Método y persistencia**.

   e) Para Persistencia, elija **COOKIEINSERT**.

   f) Para Tiempo de espera (min), escriba **240**.

      Se recomienda un valor de tiempo de espera de 240 minutos. Utilice un valor mínimo superior a 10 minutos.

      Para obtener más información, consulte Configuración del servidor virtual de autenticación.

7. Utilice el cuadro de diálogo Configurar servidor de autenticación para crear y configurar un servidor de autenticación.

   En Atributo de nombre de SSO, escriba **UserPrincipalName**.

   Para obtener más información sobre otras configuraciones, consulte Directivas de autenticación.

8. Configure una directiva de autenticación para el servidor de autenticación:

   a) En el cuadro de diálogo Configurar directiva de autenticación: Escriba un nombre para la directiva y, a continuación, seleccione el servidor de autenticación configurado en el paso anterior.

   b) Introduzca la expresión:

      ```
      ns_true
      ```

   Para obtener más información, consulte Configurar una directiva de autenticación.

9. Configure un perfil de sesión para Single Sign-On:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) En el cuadro de diálogo Configurar perfil de sesión, introduzca un nombre para el perfil.
b) Marque la casilla de Single Sign-On en las aplicaciones web.
c) Para el índice de credenciales, seleccione **PRINCIPAL**.
d) En el dominio de Single Sign-On, introduzca el nombre de dominio de su controlador de zonas de almacenamiento.
e) Marque las casillas **Supeditar global** para cada uno de los tres elementos anteriores.

Para obtener más información, consulte Perfiles de sesión.

10. Configure una directiva de sesión para Single Sign-On:

    a) En el cuadro de diálogo Configurar directiva de sesión, introduzca un nombre para la directiva.

    b) En Perfil de solicitud, seleccione el nombre del perfil de sesión configurado en el paso anterior.

    c) Introduzca la expresión:

    ```
    ns_true
    ```

    Para obtener más información, consulte Directivas de sesión.

11. Cree un servidor virtual de autenticación:

    a) En el cuadro de diálogo Configurar servidor virtual (autenticación), introduzca un nombre y la dirección IP del servidor.
    b) Haga clic en la ficha Autenticación y, en Protocolo, seleccione **SSL**.
    c) Marque la casilla de Autenticar usuarios.
    d) En Directivas de autenticación, haga clic en **Principal** y, a continuación, elija la directiva de autenticación que configuró en el paso 7.
    e) Haga clic en la ficha Directivas, haga clic en **Sesión** y, a continuación, elija la directiva de sesión que configuró en el paso 9.

    Para obtener más información, consulte Configuración del servidor virtual de autenticación.

Crear un recurso compartido de red para el almacenamiento de datos privados

October 13, 2020

Las zonas de almacenamiento de datos de ShareFile requieren un recurso compartido de red para sus datos privados. Cuando se configuran varios controladores de zonas de almacenamiento para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

alta disponibilidad y equilibrio de carga dentro de una zona, todos los controladores acceden a la misma ubicación compartida para los datos privados.

Incluso si almacena archivos ShareFile en un sistema de almacenamiento de terceros compatible, el controlador de zonas de almacenamiento requiere un recurso compartido de red para claves de cifrado, archivos en cola, otros elementos temporales y una caché de almacenamiento para cargas de archivos o descargas desde ese sistema de almacenamiento. Para obtener más información acerca de la caché de almacenamiento, consulte Personalizar operaciones de caché de almacenamiento.

Los controladores de zonas de almacenamiento acceden a un recurso compartido de red mediante el usuario del grupo de cuentas de IIS. De forma predeterminada, los grupos de aplicaciones operan bajo la cuenta de usuario del Servicio de red, que tiene derechos de usuario de bajo nivel. El controlador de zonas de almacenamiento utiliza la cuenta de servicio de red de forma predeterminada. Puede utilizar una cuenta de usuario con nombre en lugar de la cuenta Servicio de red para acceder al recurso compartido. Utilice la cuenta Servicio de red para ejecutar el grupo de aplicaciones de IIS y Citrix ShareFile Services.

1. Si quiere utilizar una cuenta de usuario con nombre en lugar de la cuenta Servicio de red para tener acceso al recurso compartido, cree una cuenta de usuario con nombre en Active Directory. Nos referiremos a esa cuenta de usuario con nombre como la cuenta de servicio ShareFile.
   Nota: Al configurar el controlador de zonas de almacenamiento, especificará el nombre de usuario del recurso compartido de red y la contraseña del recurso compartido de red, que son las credenciales de la cuenta que utilizará para acceder al recurso compartido, ya sea la cuenta del servicio ShareFile o la cuenta del servicio de red.

   Para mejorar la seguridad, el administrador deberá denegar permisos a todos los demás usuarios a la carpeta concreta que contiene el repositorio de almacenamiento de ShareFile y dar acceso solo al usuario de ubicación de almacenamiento que se está configurando.

2. Conéctese al servidor que alojará el recurso compartido de red y cree una carpeta para sus datos privados de ShareFile.
3. Haga clic con el botón derecho en la carpeta y elija Compartir con personas específicas…
4. Agregue la cuenta que utilizará para acceder al recurso compartido (cuenta de servicio de red o cuenta de servicio ShareFile) y cambie el nivel de permiso a Lectura/Escritura.
5. Haga clic en Compartir y haga clic en Listo.
6. Haga clic con el botón derecho en la carpeta y elija Propiedades
7. En la ficha Seguridad, compruebe que la cuenta que va a utilizar para acceder al recurso compartido (cuenta de servicio de red o cuenta de servicio de ShareFile) tiene permisos de acceso total.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aumentar el número de archivos por zona

De forma predeterminada, un controlador de zonas de almacenamiento está configurado para utilizar un recurso compartido CIFS para almacenar archivos en una jerarquía de carpetas en lugar de una sola carpeta.

Puede configurar el controlador de zonas de almacenamiento para dividir el diseño de almacenamiento persistente. Esto aumenta el número máximo de archivos por zona para algunos tipos de arreglos de discos de almacenamiento de información de menos de medio millón a diez millones o más. Si necesita capacidad adicional, puede cambiar el valor predeterminado.

Para habilitar el controlador de zonas de almacenamiento para almacenar archivos en varias carpetas

> **Precaución:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.
>
> **Nota:**
>
> Si se ha actualizado el controlador de zonas de almacenamiento, compruebe si el valor de la clave del Registro `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone\PathSelection is set to 1. If it is set to 0, update it to 1`.

Reinicie IIS en los controlador de zonas de almacenamiento cuando haya terminado de modificar el Registro.

Para aumentar el número máximo de carpetas

De forma predeterminada, el diseño de almacenamiento dividido tiene 256 carpetas de nivel superior, cada una de las cuales contiene 256 carpetas. Esa configuración se representa en la clave de registro del controlador de zonas de almacenamiento principal`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\storagezone: PathSelectionParams=2,2`.

El primer valor restringe el número de carpetas de nivel superior a “16 a la potencia de 2”o 256. El segundo valor también limita el número de carpetas secundarias de las carpetas de nivel superior a 256.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mediante esa misma fórmula (16 a la potencia de N) puede determinar los valores apropiados para su sitio. Por ejemplo, PathSelectionParams=3,4,4,4 restringe el número de carpetas de nivel superior a 4096 (16 a la potencia de 3). El segundo valor limita el número de carpetas secundarias de las carpetas de nivel superior a 65536 (16 a la potencia de 4). El tercer valor limita el número de carpetas secundarias de las carpetas de segundo nivel a 65536, y así sucesivamente.

Reinicie IIS en los controlador de zonas de almacenamiento primario y secundario si ha terminado de modificar el registro.

Para quitar carpetas vacías

Cuando el controlador de zonas de almacenamiento almacena archivos en varias carpetas, la eliminación de archivos puede dar lugar a carpetas vacías. De forma predeterminada, el controlador de zonas de almacenamiento elimina carpetas vacías. El servicio de eliminación de archivos eliminará carpetas vacías, comenzando en la parte inferior del árbol y continuando hasta que llegue a una carpeta no vacía.

Sin embargo, es posible que algunas rutas de actualización no actualicen la configuración. Después de una actualización, compruebe que aparece la siguiente clave en `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`:

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

Si necesita agregar la clave, reinicie el servicio de eliminación de archivos cuando haya terminado.

Instalar un certificado SSL

October 13, 2020

Si no utiliza un certificado comodín, debe crear una solicitud de firma de certificado (CSR) para el servidor del controlador de zonas de almacenamiento y enviar la solicitud a una entidad emisora de certificados (CA). Para obtener ayuda, consulte la documentación de su CA.

Siga estos pasos para instalar un certificado.

1. En el servidor del controlador de zonas de almacenamiento, abra MMC y, a continuación, elija **Archivo > Agregar o quitar complemento**.
2. Seleccione Certificados y haga clic en **Agregar**.
3. Seleccione Cuenta de equipo, haga clic en **Siguiente**, en **Finalizar** y, a continuación, haga clic en **Aceptar**.
4. En la consola de MMC, expanda **Certificados > Personal**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Haga clic con el botón secundario en **Certificados**, seleccione **Todas las tareas > Importar** y, a continuación, haga clic en **Siguiente**.
6. Haga clic en **Examinar** y, a continuación, en el menú de extensión de nombre de archivo, elija **Intercambio de información personal**
7. Vaya a la ubicación del certificado y, a continuación, haga clic en **Abrir**.
8. Haga clic en **Siguiente**, escriba la **contraseña** asociada a su clave privada, haga clic en **Siguiente** dos veces y, a continuación, haga clic en **Finalizar**.
9. Cuando aparezca el mensaje **Importar correctamente**, haga clic en **Aceptar**.

Para un certificado público, asegúrese de que el dominio al que se emite se resuelve en la dirección IP local del controlador de zonas de almacenamiento. Para ello, actualice el archivo hosts en el controlador de zonas de almacenamiento para asignar el dominio asociado con el certificado a la dirección IP del controlador de zonas de almacenamiento. Si las dos direcciones no se resuelven, los usuarios no podrán cargar archivos desde el controlador de zonas de almacenamiento.

Preparar el servidor para los datos de ShareFile

November 16, 2023

El rol de servidor web (IIS) y la configuración de ASP.NET que se describen en esta sección son necesarios para las zonas de almacenamiento de datos de ShareFile y para los conectores de zonas de almacenamiento. Estas instrucciones se basan en Windows Server 2012, pero también son válidas para versiones posteriores.

Actualizar la versión de Microsoft .NET

Antes de continuar con la instalación del controlador de zonas de almacenamiento, asegúrese de utilizar la versión adecuada de Microsoft .NET Framework.

- **El controlador de zonas de almacenamiento 5.x requiere .NET 4.8 o posterior**. Haga clic aquí para descargar .NET 4.8

ShareFile recomienda utilizar la versión más reciente de Microsoft .NET cuando se utilicen las aplicaciones de ShareFile.

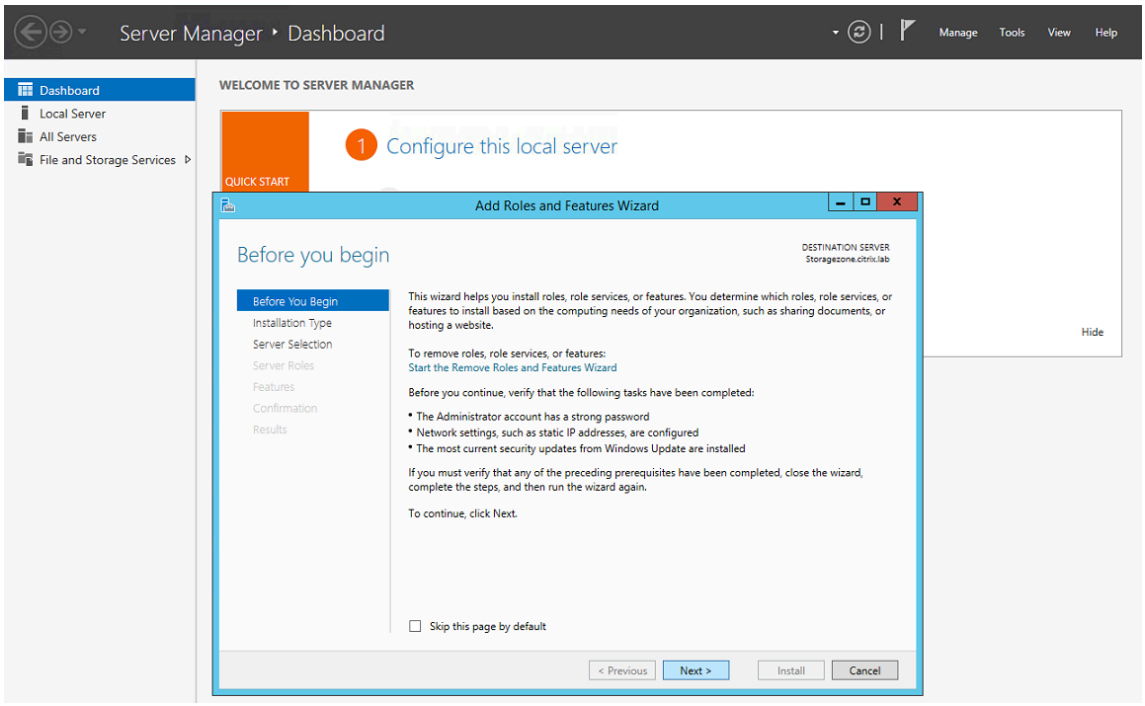
Para habilitar el rol de servidor web (IIS) y el servicio de roles de ASP.NET

1. En el servidor donde instale el controlador de zonas de almacenamiento, inicie sesión con una cuenta que tenga privilegios de administrador local.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

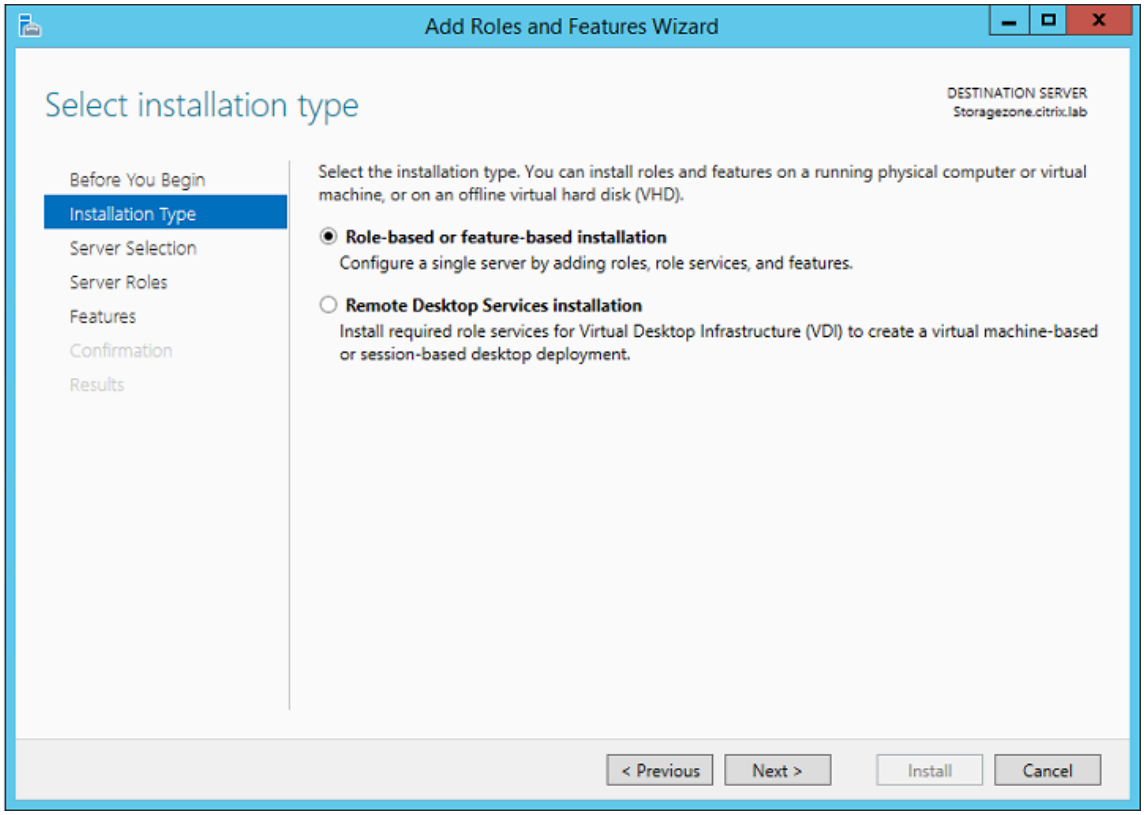
2. Abra el panel de control de la consola de Server Manager y, a continuación, haga clic en **Administrar > Agregar funciones y** funciones para abrir el asistente para agregar funciones y funciones.

3. En el Asistente para agregar funciones y funciones, haga clic en **Siguiente**.



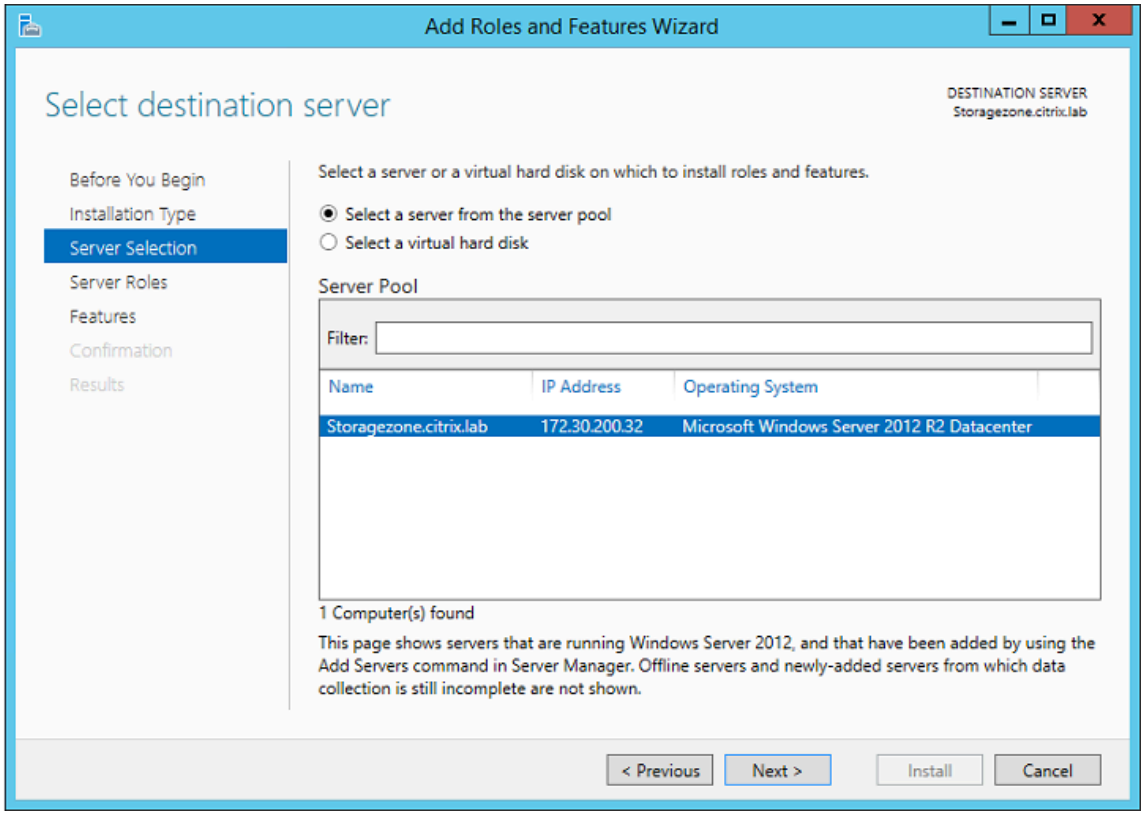
4. En la página Seleccione el tipo de instalación, haga clic en Instalación basada en funciones o funciones y, a continuación, en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



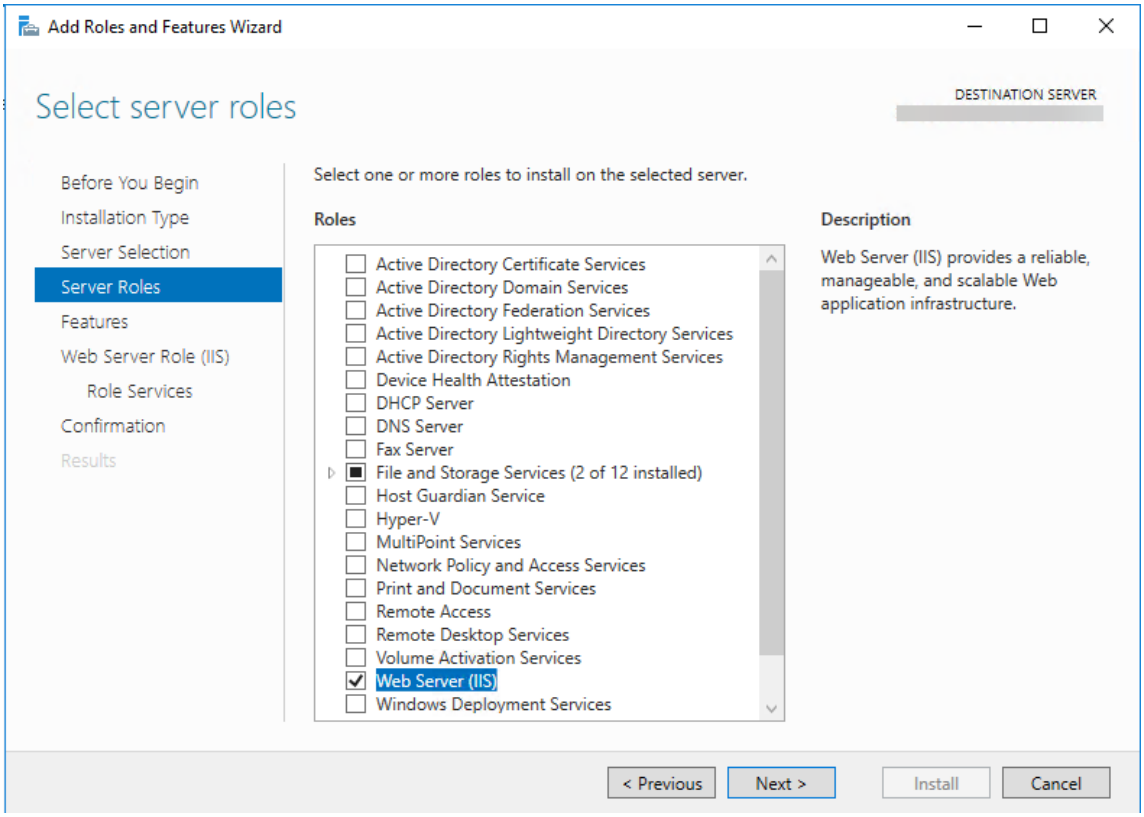
5. En la página Seleccione el servidor de destino, elija su servidor del grupo de servidores y, a continuación, haga clic en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

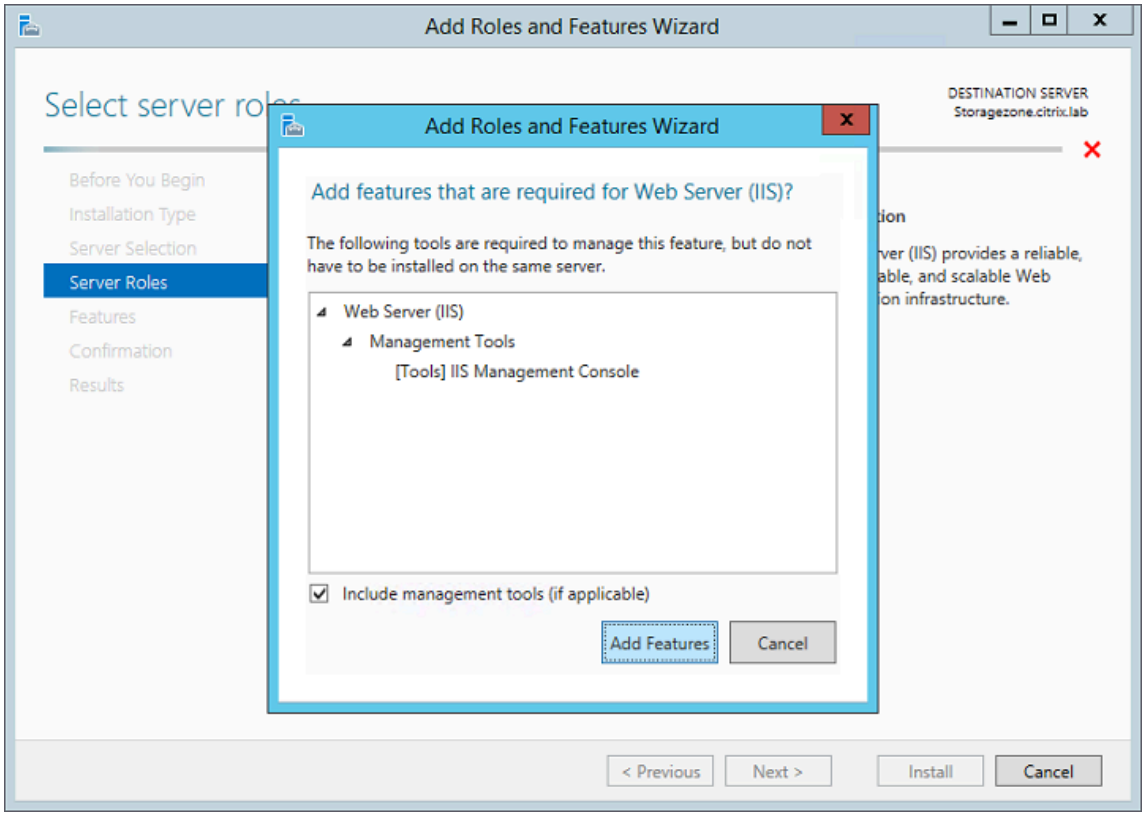


6. En la página Seleccionar funciones de servidor, active la casilla de verificación Servidor web (IIS) y, a continuación, haga clic en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

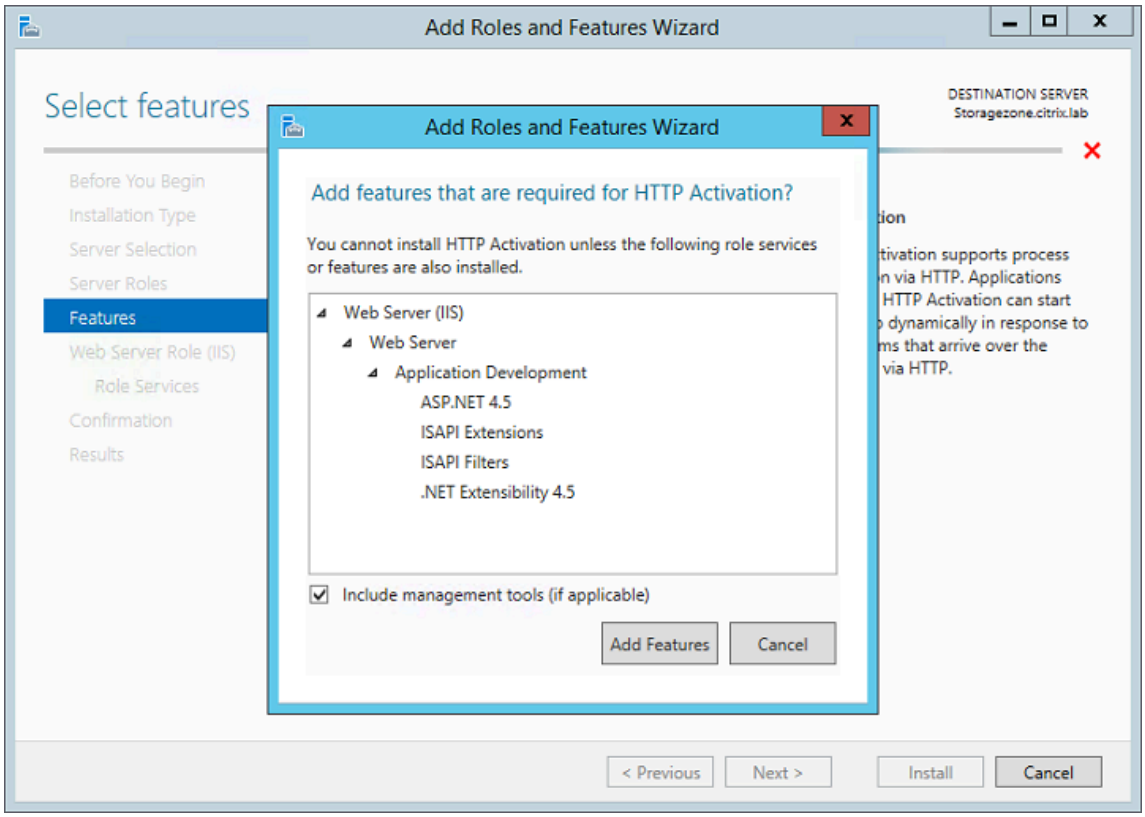


7. Haga clic en **Agregar funciones** para agregar las funciones necesarias para IIS.



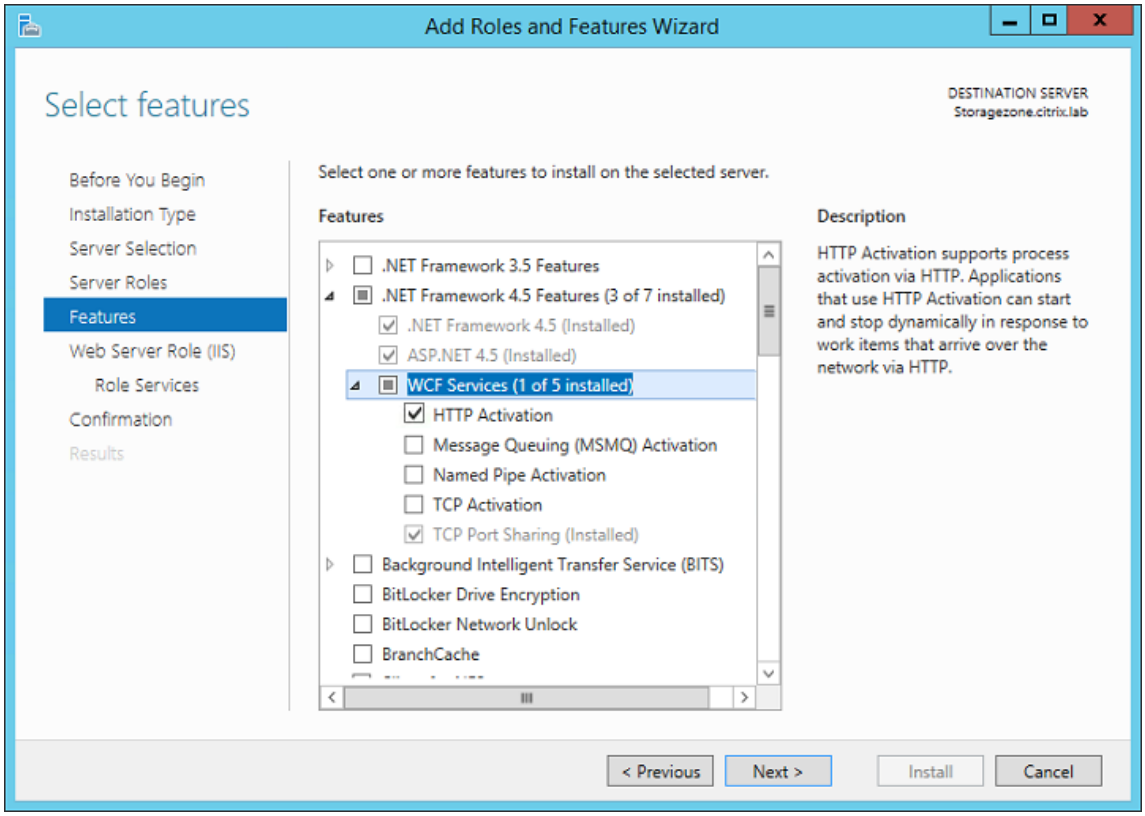
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Haga clic en **Agregar funciones**. Aparece la página Seleccionar funciones.



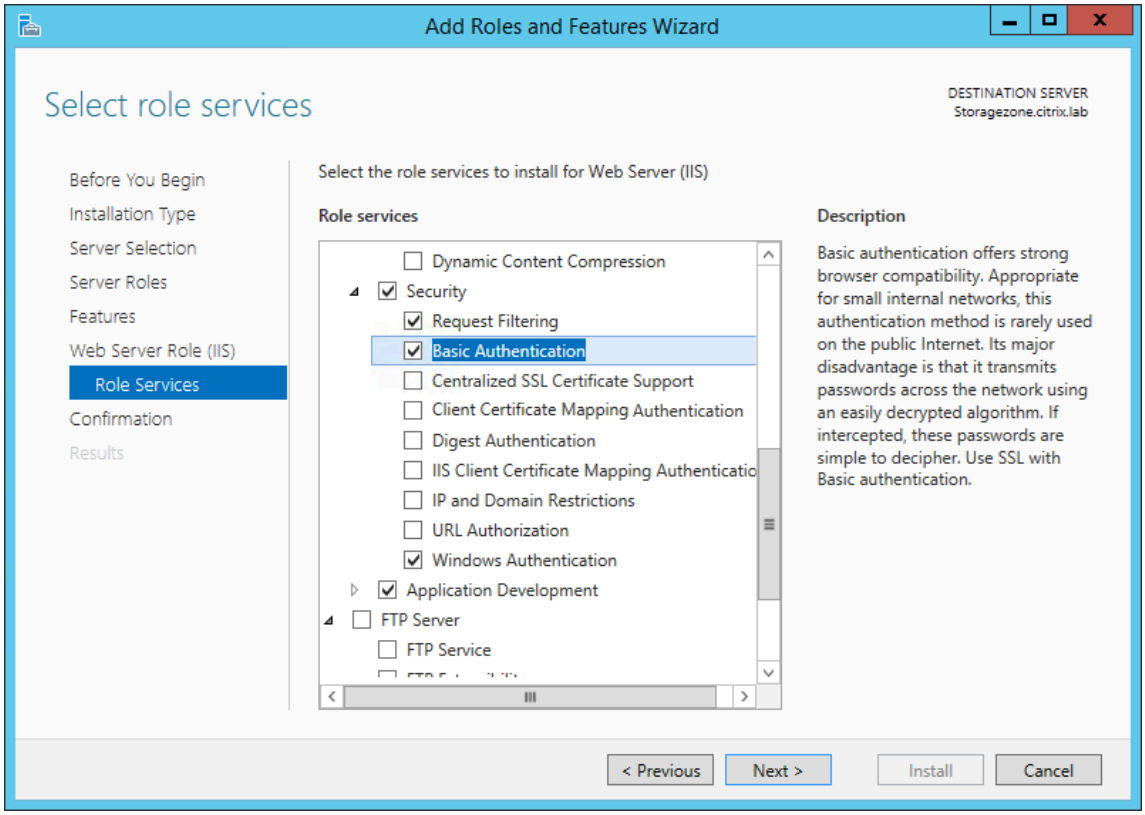
9. Seleccione los ajustes necesarios que se muestran en la siguiente pantalla y, a continuación, haga clic en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. En la página Función de servidor web (IIS), haga clic en **Siguiente**.
11. En la página Seleccione servicios de rol, active las casillas Autenticación básica y Autenticación de Windows y, a continuación, haga clic en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



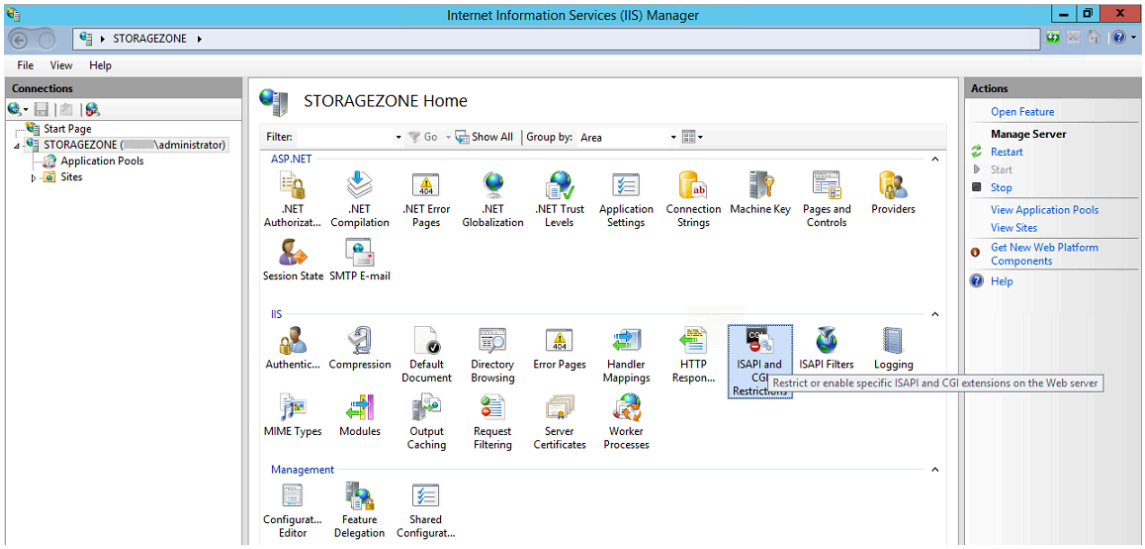
12. En la página Confirmar las selecciones de instalación, haga clic en **Instalar**.
13. Cuando finalice la instalación, haga clic en **Cerrar** y, a continuación, reinicie el servidor.

Para configurar IIS

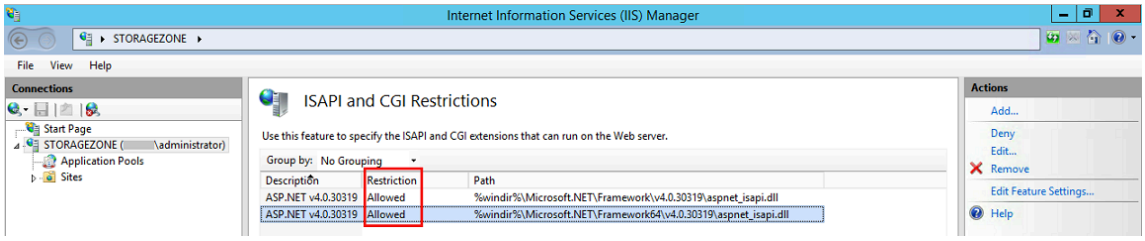
Después de habilitar el rol de servidor web (IIS) y el servicio de roles de ASP.NET, configure IIS.

1. Abra la consola de IIS Manager, haga clic en el nodo servidor del controlador de zona de almacenamiento y, a continuación, haga doble clic en Restricciones de ISAPI y CGI.

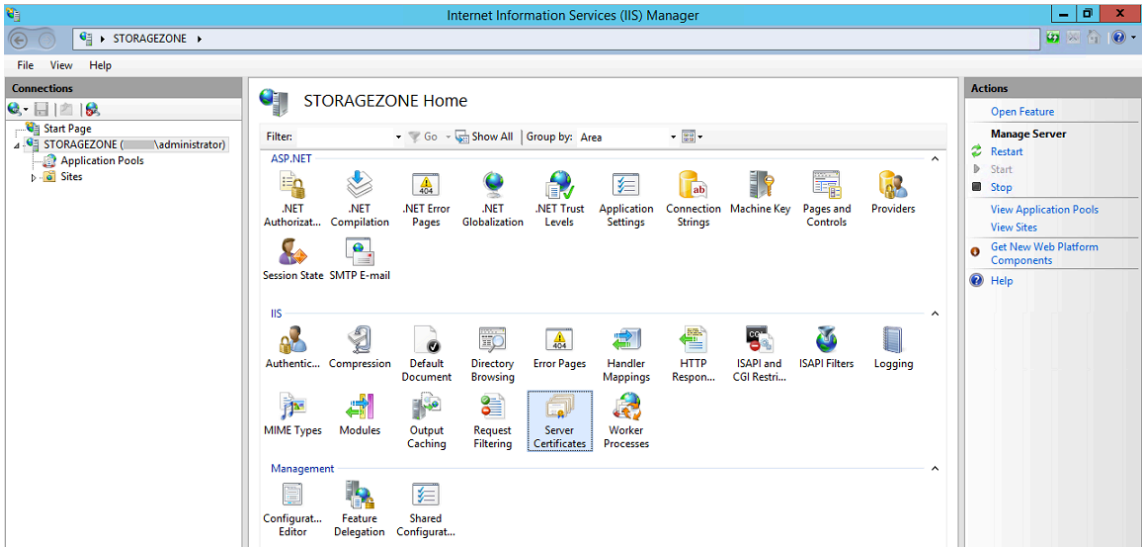
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Defina cada entrada de ASP.NET como Permitida.



3. Compruebe que haya un servidor de dominio o un certificado público en el servidor: en la consola de IIS Manager, haga clic en el nodo del servidor del controlador de zona de almacenamiento y, a continuación, haga doble clic en Certificados de servidor.

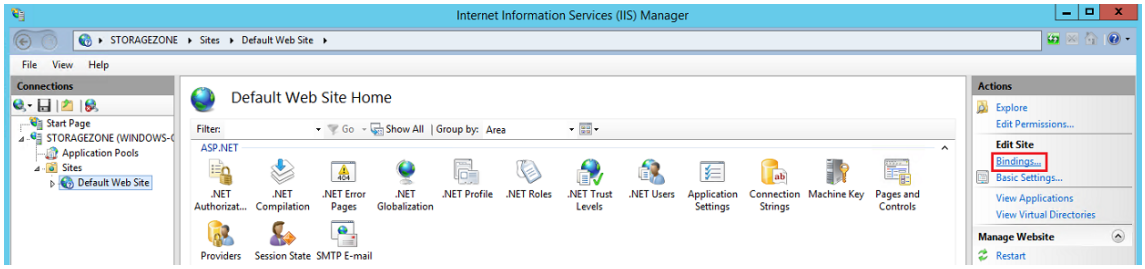


Si no hay ningún certificado asociado a una entidad de certificación pública, instale un certificado en el servidor antes de continuar. Para obtener más información, consulte Instalar un certificado SSL.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

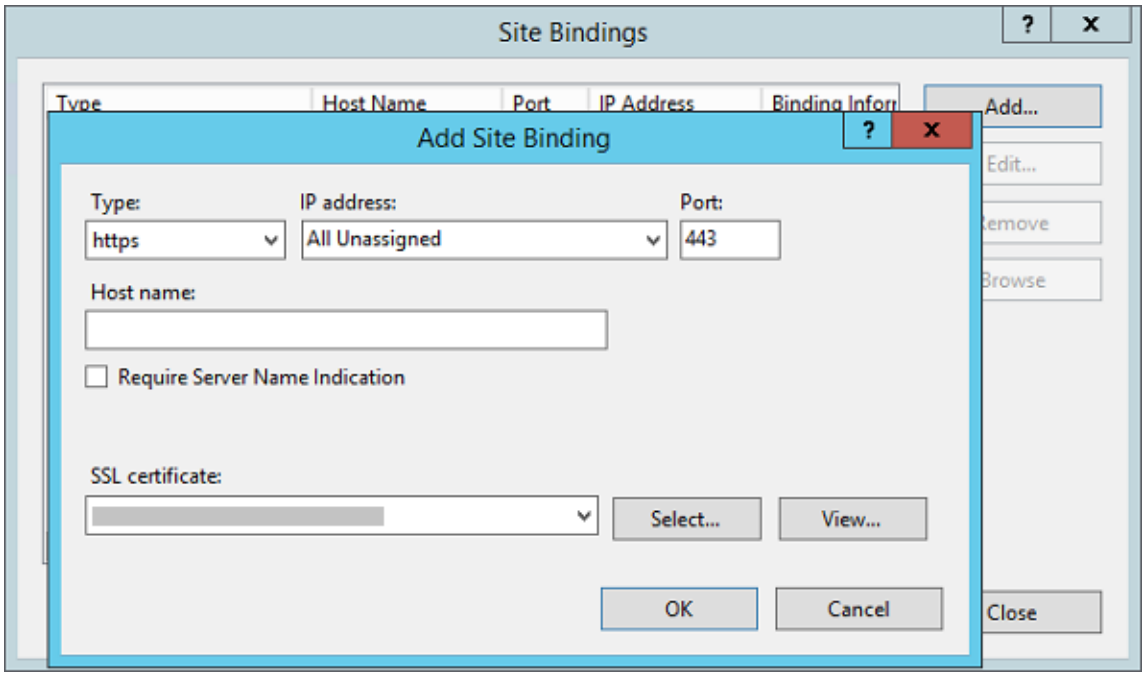
> **Nota:**
>
> Si utiliza un dispositivo Citrix Gateway o similar con controlador de zonas de almacenamiento, puede utilizar un certificado de servidor de dominio. Todo el tráfico de Internet de las zonas estándar debe gestionarse mediante un certificado público.

4. En la consola de IIS Manager, haga clic en **Sitio web predeterminado** y, a continuación, en **Enlaces.**



5. Haga clic en Agregar y configure el enlace del sitio de la siguiente manera:

   - El tipo es https.
   - La dirección IP no está asignada.
   - El puerto es 443.
   - El certificado SSL es su certificado instalado.



6. Para probar la conexión del servidor web, vaya a `http://localhost/` y a `https://localhost/`. Si la conexión se realiza correctamente, aparece el logotipo de IIS.

   HTTPS muestra un mensaje en el que se indica que el certificado no coincide con el nombre del

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

host local en el encabezado de la URL. Esto es lo esperado y puede continuar con seguridad en el sitio web.

7. Si va a instalar el controlador de zonas de almacenamiento en una máquina virtual, tome una instantánea de la máquina virtual.

> **NOTA:**
>
> El controlador de zonas de almacenamiento usa CORS y requiere que se habilite el verbo http **OPTIONS**. Compruebe la función de filtrado de solicitudes de IIS para asegurarse de que el verbo **OPTIONS** no esté inhabilitado.

Instalar el controlador de zonas de almacenamiento y crear una zona de almacenamiento

March 16, 2024

> **Importante:**
>
> - Verifique que su entorno cumpla con los requisitos del sistema antes de iniciar la instalación.
> - El controlador de zonas de almacenamiento ShareFile usa contraseñas específicas de la aplicación. Para obtener más información, consulte Crear una contraseña específica de la aplicación.

Al instalar un controlador de zonas de almacenamiento, puede crear una zona y configurar un controlador de zonas de almacenamiento principal o
unir los controladores de zonas de almacenamiento secundarios a una zona.

Al configurar un controlador de zonas de almacenamiento principal, puede habilitar una de estas funciones o ambas:

- Zonas de almacenamiento para ShareFile Data, para especificar el almacenamiento privado de datos, ya sea un recurso compartido de red privada o un sistema de almacenamiento de terceros compatible.
- Conectores de zonas de almacenamiento, para dar a los usuarios acceso a los documentos de los sitios de SharePoint o a los recursos compartidos de archivos de red específicos.

En los pasos siguientes se describe cómo instalar el StorageZones Controller, configurar la autenticación para el sitio web predeterminado de IIS, crear una zona y habilitar las funciones.

1. Descargue e instale el software del controlador de zonas de almacenamiento:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Desde la página de descarga de ShareFile en https://dl.sharefile.com/storagezone-controller, inicie sesión y descargue el instalador más reciente de StorageZones Controller.

> **Nota:**
>
> La instalación del controlador de zonas de almacenamiento cambia el sitio web predeterminado del servidor por la ruta de instalación del controlador.

La autenticación anónima debe estar habilitada en el sitio web predeterminado.

2. En el servidor en el que desea instalar el StorageZones Controller, ejecute StorageCenter.msi.
   - Se inicia el asistente de configuración del controlador de zonas de almacenamiento de ShareFile.
   - Para la tenencia múltiple, ejecute el siguiente comando: ***msiexec /i StorageCenter_5.0.1.msi***MULTITENANT=1

> **Nota:**
>
> En el comando anterior, es posible que necesite actualizar el número de versión (5.0.1 en el ejemplo) para que coincida con el número de msi que está intentando instalar.

   - Responda a las indicaciones. Cuando finalice la instalación, desactive la casilla de verificación **Iniciar la página de configuración del controlador de zonas de almacenamiento** y, a continuación, haga clic en **Finalizar**.
3. Reinicie el StorageZones Controller.
4. Para comprobar que la instalación se ha realizado correctamente, navegue hasta `http://localhost/`. Si la instalación se realizó correctamente, aparecerá el logotipo de ShareFile.
5. Si no aparece el logotipo de ShareFile, borre la memoria caché del explorador Web y vuelva a intentarlo.

> **Importante:**
>
> Si va a clonar el controlador de zonas de almacenamiento, capture la imagen de disco antes de continuar con la configuración del controlador.

6. Para usar un proveedor de almacenamiento compatible con S3 con ShareFile, lleve a cabo los siguientes pasos antes de crear o configurar una zona de almacenamiento.
   - Abra el Editor del Registro de Windows (**Ejecutar > regedit.exe**).
   - Busque la clave de registro HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ Citrix\ StorageCenter.
   - Cree un nuevo valor REG_SZ bajo esta clave:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Nombre del valor: **S3EndpointAddress**
  - Tipo de valor: **REG_SZ**
  - Datos de valor: introduzca la URL HTTPS que corresponde a su punto final de almacenamiento compatible con S3.

- Si el proveedor de almacenamiento solo admite el acceso a contenedores tipo ruta (consulte http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html), cree otro valor con esta clave.

  - Nombre del valor: **S3ForcePathStyle**
  - Tipo de valor: **REG_SZ**
  - Datos de valor: **verdaderos**

- Reinicie el grupo de aplicaciones del controlador de zonas de almacenamiento (StorageCenterAppPool).

- Recopile la siguiente información de su sistema de almacenamiento compatible con S3:

  - El nombre de un bucket de S3 que se va a usar como ID de clave de ShareFile DataAccess
  - ID de clave de acceso
  - Clave de acceso secreta

7. Continúe con los pasos siguientes para crear una nueva zona de almacenamiento. Elija Amazon S3 como ubicación de almacenamiento persistente. El controlador de zonas de almacenamiento utiliza la dirección de punto final personalizada que ha introducido en lugar del servicio Amazon S3 real. Al configurar los detalles de S3, elija el nombre del bucket que creó anteriormente.

8. Navegue hasta la consola del controlador StorageZones.

9. Abra `http://localhost/configservice/login.aspx` o inicie la herramienta de configuración desde la pantalla o el menú Inicio. Para obtener información sobre el uso del acceso directo a la pantalla de inicio en Windows 8, consulte Administrar controladores de zonas de almacenamiento.

10. En la **página de inicio de sesión del controlador de zonas de almacenamiento**, introduzca la **dirección de correo electrónico**, la **contraseña** y el **subdominio FQDN de la URL completa de la cuenta**, como `subdomain.sharefile.com` o `subdomain.sharefile.eu`. Haga clic en **Iniciar sesión**.

11. Para configurar el controlador de zonas de almacenamiento principal, haga clic en **Crear nueva zona** e introduzca la información de la zona:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
Zona	Nombre que aparece en la consola de administración de ShareFile.
Controlador de zona principal	El valor predeterminado es `http://localhost/ConfigService`. Si usas SSL, cambia HTTP a https. Tenga en cuenta que ShareFile solo admite certificados SSL públicos válidos y confiables para las zonas estándar. Si tiene problemas para configurar un host de zona de almacenamiento secundario, asegúrese de poder resolver la URL de ConfigService en un navegador local de ese servidor, sin errores de SSL. localhost resuelve en la dirección IP del servidor. En su lugar, puede especificar un nombre de servidor (por ejemplo `https://servername.subdomain.com/ConfigService`). El nombre del servidor debe poder resolverlo un servidor StorageZones Controller secundario.
Nombre de host	Un identificador único para su controlador de zonas de almacenamiento. ShareFile recomienda usar el nombre de host del servidor como identificador. Debe ser un nombre descriptivo y no el FQDN. Este nombre aparece en la consola de administrador de ShareFile.
Dirección externa	El FQDN de este controlador de zonas de almacenamiento. Si este controlador de zonas de almacenamiento se va a utilizar para zonas estándar, se debe poder acceder a la URL desde Internet. Si utilizas un balanceador de cargas, introduce su dirección. Al enviar la página, ShareFile valida la dirección.

12. Para especificar el almacenamiento privado de datos, haga lo siguiente.
    - Seleccione la casilla de verificación **Habilitar zonas de almacenamiento para ShareFile Data**.
    - Para configurar una zona estándar, desactive la casilla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Después de configurar un StorageZones Controller, no puede cambiar su tipo de zona.

El StorageZones Controller usa las credenciales de la cuenta de servicio para conectarse al servidor de dominio Active Directory de confianza para buscar direcciones de correo electrónico.

- Elija un repositorio de almacenamiento.

13. Si no desea habilitar los conectores de zonas de almacenamiento, haga clic en **Registrar para registrar** StorageZones Controller con ShareFile y, a continuación, continúe con el paso 14.
14. Si utiliza un almacenamiento compatible con S3, cree estas entradas de registro adicionales después de que se registre la zona de almacenamiento:
    - Abra el Editor del Registro de Windows (**Ejecutar > regedit.exe**).
    - Busque la clave del Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\storage zone\CloudStorageUploaderConfig`.
    - Cree un nuevo valor REG_SZ bajo esta clave:
        - Nombre del valor: **S3EndpointAddress**
        - Tipo de valor: **REG_SZ**
        - Datos de valor: introduzca la URL HTTPS que corresponde a su punto final de almacenamiento compatible con S3.
    - Si el proveedor de almacenamiento solo admite el acceso a contenedores tipo ruta (consulte http://docs.aws.amazon.com/AmazonS3/latest/dev/VirtualHosting.html), cree otro valor con esta clave.
        - Nombre del valor: **S3ForcePathStyle**
        - Tipo de valor: **REG_SZ**
        - Datos de valor: **verdaderos**
    - Reinicie el grupo de aplicaciones del controlador de zonas de almacenamiento (StorageCenterAppPool).
15. Para habilitar los conectores de zonas de almacenamiento:

    Al habilitar los conectores, se crean las aplicaciones de IIS «cifs» (conector para recursos compartidos de archivos de red) y «sp» (conector para SharePoint).

    - Seleccione la casilla de verificación de cada tipo de conector que desee usar: Habilitar el conector de zona de almacenamiento para recursos compartidos de archivos de red y Habilitar el conector de zona de almacenamiento para SharePoint. Para obtener información sobre la configuración de los conectores, consulte Configurar conectores de zonas de almacenamiento, en esta sección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Haga clic en **Registrar**. Aparece la información del controlador de zonas de almacenamiento.
- Si especificó **rutas permitidas o rutas denegadas para los** conectores de zonas de almacenamiento, reinicie el servidor IIS.

16. Para configurar los controladores de zonas de almacenamiento secundarios, consulte Administrar los controladores de zonas de almacenamiento.

> **Importante:**
>
> Se instala un controlador de zonas de almacenamiento en su sitio local y usted es responsable de realizar una copia de seguridad. Para proteger su implementación, debe tomar una instantánea del servidor de StorageZones Controller, hacer una copia de seguridad de la configuración de StorageZones Controllery preparar StorageZones Controller para la recuperación ante desastres.

Configurar zonas de almacenamiento para ShareFile Data

> **Nota:**
>
> Las zonas de almacenamiento para ShareFile Data están disponibles para Citrix Endpoint Management Enterprise Edition y no están disponibles para otras ediciones de Citrix Endpoint Management.

Puede configurar zonas de almacenamiento para ShareFile Data desde el asistente del controlador de zonas de almacenamiento al crear una zona de almacenamiento o desde la consola del controlador de zonas de almacenamiento. Utilice la pestaña ShareFile Data para configurar los ajustes de los recursos compartidos de redes privadas o los sistemas de almacenamiento de terceros compatibles.

Configuración de redes compartidas

Opción	Descripción
repositorio de almacenamiento	Elige Compartir red local. Después de crear la zona, no puede cambiar la opción Repositorio de almacenamiento. Por ejemplo, para cambiar de un recurso compartido de red local a un almacenamiento de terceros, debe crear una nueva zona.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
Ubicación de red compartida	La ruta UNC al recurso compartido de red que utilizará para el almacenamiento de datos privados y para datos como claves de cifrado, archivos en cola y otros elementos temporales. Especifique la ruta en el formulario `\\server\share`. Los controladores de zonas de almacenamiento que pertenezcan a la misma zona de almacenamiento deben utilizar el mismo recurso compartido de archivos para el almacenamiento. Precaución: el controlador de zonas de almacenamiento sobrescribirá cualquier dato de esta ruta con un formato de almacenamiento propietario. Nunca especifique una ruta de acceso a una ubicación con datos de archivo. Reserve esta ubicación de almacenamiento para las zonas de almacenamiento únicamente para los datos de ShareFile. Los controladores de zonas de almacenamiento acceden al recurso compartido de red mediante el nombre de usuario y la contraseña de Network Share que se proporcionan en la página de configuración. Si no se proporciona ningún nombre de usuario o contraseña de Network Share en la página de configuración, la cuenta de Network Service se utilizará de forma predeterminada. La cuenta del servicio de red debe tener acceso total a esta ubicación de almacenamiento. El controlador de zonas de almacenamiento también utilizará la cuenta de servicio de red de forma predeterminada para StorageCenterAppPool. Es importante tener en cuenta que la única configuración admitida es usar la cuenta de servicio de red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
Nombre de usuario de Network Share y contraseña de Network Share	Las credenciales de la ruta UNC de la ubicación de su red compartida. Para usar una cuenta de usuario nominal en lugar de la cuenta del Servicio de red para acceder al recurso compartido, especifique esas credenciales. Puede seguir ejecutando el grupo de aplicaciones de IIS y los servicios de ShareFile mediante la cuenta de servicio de red.
Habilitar cifrado	Seleccione la casilla de verificación solo si desea cifrar el contenido de los archivos almacenados en el recurso compartido de archivos. En un entorno empresarial en el que el recurso compartido de red se encuentra dentro de la red y ya está protegido por herramientas de terceros, se recomienda no cifrar los archivos del recurso compartido. Esta configuración no está relacionada con los metadatos. Los metadatos no están cifrados para las zonas estándar. Aunque esta seguridad adicional se ofrece como una opción para la máxima seguridad cuando sea necesario, el cifrado de archivos en el recurso compartido hará que el disco sea ilegible por herramientas de terceros, como escáneres antivirus y herramientas de filer, incluidas las herramientas de deduplicación de datos. ShareFile utiliza una clave de cifrado de archivos para confirmar la validez de las solicitudes de descarga y cifrar el almacenamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
Frase secreta	Frase utilizada para proteger la clave de cifrado de archivos. La contraseña debe contener más de seis caracteres. Asegúrese de archivar la frase de contraseña y la clave de cifrado en una ubicación segura. Debe usar la misma frase de contraseña para cada controlador de zonas de almacenamiento de una zona. La frase de contraseña no es la misma que la contraseña de su cuenta y no se puede recuperar si se pierde. Si pierde la frase de contraseña, no puede reinstalar zonas de almacenamiento, unir controladores de zonas de almacenamiento adicionales a la zona de almacenamiento ni recuperar la zona de almacenamiento si el servidor falla. Nota: La clave de cifrado aparece en la raíz de la ruta de almacenamiento compartido. La pérdida del archivo de clave de cifrado, SCKeys.txt, interrumpe inmediatamente el acceso a todos los archivos de la zona de almacenamiento. Asegúrese de hacer una copia de seguridad del archivo de clave de cifrado como parte de los procedimientos normales de su centro de datos.

Opciones de configuración de caché compartida

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
Ubicación de caché compartida	la ruta a un recurso compartido de red que contendrá la memoria caché de almacenamiento y los datos, como las claves de cifrado, los archivos en cola y otros elementos temporales. Especifique la ruta en el formulario `\\server\share`. Los controladores de zonas de almacenamiento que pertenezcan a la misma zona de almacenamiento deben utilizar el mismo recurso compartido de archivos para el almacenamiento. Precaución: el controlador de zonas de almacenamiento sobrescribirá cualquier dato de esta ruta con un formato de almacenamiento propietario. Nunca especifique una ruta de acceso a una ubicación con datos de archivo. Reserve esta ubicación de almacenamiento solo para zonas de almacenamiento de datos de ShareFile. La cuenta del servicio de red (o la cuenta con la que está configurado el servicio de administración de ShareFile) debe tener acceso total a esta ubicación de almacenamiento.
Inicio de sesión en caché compartida y contraseña de caché compartida	Las credenciales de la ruta UNC de su ubicación de caché compartida.
Habilitar cifrado	Seleccione la casilla de verificación para cifrar los archivos almacenados en la memoria caché compartida.

Configuración del contenedor de almacenamiento de Windows Azure

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
repositorio de almacenamiento	Elija el contenedor de almacenamiento de Azure. Después de crear la zona, no puede cambiar la opción Repositorio de almacenamiento. Por ejemplo, para cambiar de un recurso compartido de red local a un almacenamiento basado en Azure, debe crear una nueva zona.
Nombre de cuenta	El nombre de su cuenta de almacenamiento de Azure. Estos nombres siempre están en minúsculas.
Clave de acceso	La clave de acceso principal o secundaria de su almacenamiento de Azure. Copie la clave de la pantalla Administrar claves de acceso del Portal de administración de Windows Azure.
Validar	Haga clic en el botón para validar la clave de acceso de Azure. No puede continuar con la configuración hasta que se complete la validación y el menú Nombre del contenedor incluya todos los contenedores disponibles para la cuenta especificada.
Nombre del contenedor	Seleccione el contenedor de Azure que se usará para todos los controladores de zonas de almacenamiento de esta zona de almacenamiento. Esta lista estará vacía hasta que se valide la clave de acceso de Azure.

Configuración del depósito de almacenamiento de Amazon S3

Opción	Descripción
repositorio de almacenamiento	Elija el depósito de almacenamiento de Amazon S3. Después de crear la zona, no puede cambiar la opción Repositorio de almacenamiento. Por ejemplo, para cambiar de un recurso compartido de red local al almacenamiento de Amazon S3, debe crear una nueva zona.
ID de clave de acceso	El ID de la clave de acceso de su almacenamiento de Amazon S3.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opción	Descripción
Clave de acceso secreta	La clave de acceso secreta para su almacenamiento en Amazon S3.
Validar	Haga clic en el botón para validar la clave de acceso secreta de Amazon S3. No puede continuar con la configuración hasta que se complete la validación y el menú Nombre del depósito incluya todos los depósitos disponibles para la cuenta especificada.
Nombre del depósito	Seleccione el bucket de Amazon S3 para usarlo en todos los controladores de zonas de almacenamiento de esta zona de almacenamiento. Esta lista estará vacía hasta que se valide la clave de acceso secreta de Amazon S3.

Configuración de SMTP

Opción	Descripción
Dirección del servidor SMTP y número de puerto SMTP	El nombre de host y el puerto del servidor SMTP local.
Usa SSL	Seleccione la casilla para conectarse al servidor SMTP a través de una conexión segura.
Nombre de usuario y contraseña	El nombre de usuario y la contraseña del servidor SMTP local.
Modo de autenticación	El modo de autenticación predeterminado utiliza el método más seguro disponible para conectarse desde el StorageZones Controller al servidor SMTP.
Dirección del remitente	La dirección de correo electrónico que aparece en el campo De.

Plataforma Google Cloud

Genera una clave de acceso y un secreto desde **Google Cloud Platform > Configuración > Interoperabilidad**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Antes de ejecutar StorageZones Configuration, defina el valor de registro de **S3EndpointAddress** en `https://storage.googleapis.com` y, a continuación, reinicie IIS.

Opción 1

Descripción

Repositorio de almacenamiento

Elija el depósito de **almacenamiento de Amazon S3**. Después de crear la zona, no puede cambiar la opción **Repositorio de almacenamiento**. Por ejemplo, para cambiar de un recurso compartido de red local al almacenamiento de Amazon S3, debe crear una nueva zona.

ID de clave de acceso

El ID de la clave de acceso de tu almacenamiento de Google Cloud Platform.

Clave de acceso secreta

El secreto de tu almacenamiento en Google Cloud Platform.

Validar

Haz clic en el botón para validar la clave de acceso secreta de Google Cloud Platform. No puede continuar con la configuración hasta que se complete la validación y la lista de **nombres de bucket** incluya todos los buckets disponibles para la cuenta especificada.

Nombre del depósito

Seleccione el depósito correcto para usar en todos los controladores de zonas de almacenamiento de esta zona de almacenamiento. Esta lista estará vacía hasta que se valide tu clave de acceso secreta de Google Cloud Platform.

Configurar conectores de zonas de almacenamiento

Los conectores de zonas de almacenamiento permiten a los usuarios acceder a los documentos de los sitios de SharePoint o a los recursos compartidos de archivos de red específicos. No es necesario habilitar las zonas de almacenamiento para que ShareFile Data utilice conectores de zonas de almacenamiento.

> **Nota:**
>
> Las zonas de almacenamiento para ShareFile Data y las funciones de los conectores de zonas de almacenamiento pueden compartir una zona. Sin embargo, el controlador de zonas de almacenamiento mantiene separados los datos y las reglas de acceso para los dos tipos de datos.

Puede configurar los conectores de zonas de almacenamiento al crear una zona mediante el asistente del controlador de zonas de almacenamiento o desde la consola del controlador de zonas de almacenamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para controlar el acceso a determinados recursos compartidos de archivos de red o bibliotecas de documentos de SharePoint, especifique una lista de rutas permitidas o rutas denegadas. Después de guardar los cambios, reinicie el servidor IIS.

Las conexiones entrantes a los conectores de zonas de almacenamiento se comprueban primero con las rutas permitidas. Si se permite la conexión, la ruta se compara con las rutas denegadas. Por ejemplo, para proporcionar acceso a `\\myserver\teamshare` y a todas sus subcarpetas, especifique una ruta permitida de `\\myserver\teamshare`.

- Todas las conexiones están permitidas de forma predeterminada, lo que se indica con un valor de rutas permitidas. El valor no es válido para las rutas denegadas.
- Si las rutas permitidas y denegadas entran en conflicto, se aplica la ruta más restrictiva.
- Las entradas están separadas por comas.
- Para los conectores a los recursos compartidos de archivos de red, especifique las rutas UNC permitidas.

  Ejemplo con FQDN: `\\fileserver.acme.com\shared`

  Puede utilizar las siguientes variables en la ruta de acceso UNC:

  - %Nombre de usuario%

    Redirige al directorio principal de un usuario. Ruta de ejemplo: `\\myserver\homedirs\\%UserName%`

  - %HomeDrive%

    Redirige a la ruta de acceso a la carpeta principal de un usuario, tal y como se define en la propiedad de Active Directory Home-Directory. Ruta de ejemplo: `%HomeDrive%`

  - %TSHomeDrive%

    Redirige al directorio principal de Terminal Services de un usuario, tal como se define en la propiedad MS-TS-Home-Directory de Active Directory. La ubicación se usa cuando un usuario inicia sesión en Windows desde un servidor Terminal Server o un servidor Citrix XenApp. Ruta de ejemplo: %tsHomeDrive%

    En el complemento Usuarios y equipos de Active Directory, se puede acceder al valor del directorio principal de MS-TS en la pestaña Perfil de servicios de escritorio remoto al editar un objeto de usuario.

  - %Dominio de usuario%

    Redirige al nombre de dominio NetBIOS del usuario autenticado. Por ejemplo, si el nombre de inicio de sesión del usuario autenticado es «abc\johnd», la variable se sustituye por «abc». Ruta de ejemplo: `\\myserver%UserDomain%_%UserName%`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las variables no distinguen mayúsculas y minúsculas

- Para un conector a un sitio de SharePoint de nivel raíz, especifique la ruta de acceso de nivel raíz.

  Ejemplo:`https://sharepoint.company.com`

- Para un conector a una colección de sitios de SharePoint:

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

- Para los conectores a las bibliotecas de documentos de SharePoint 2010, especifique las URL (sin incluir los terminadores de rutas, como file.aspx o /Forms).

  Ejemplos:

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

  La URL predeterminada de SharePoint 2013 (cuando la estrategia de descarga mínima está habilitada) tiene el formato: `https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`.

Recomendación de seguridad para eliminar el encabezado del servidor

IIS/ASP.NET expone de forma predeterminada el encabezado del servidor en las respuestas HTTP. Este encabezado podría resultar útil para un atacante. El encabezado revela el tipo de servidor de envío y, en algunos casos, el número de versión. Este encabezado no es necesario para los sitios de producción y se puede deshabilitar.

Lamentablemente, el instalador del controlador de zonas de almacenamiento no puede eliminar este encabezado automáticamente. Sin embargo, podemos recomendar a los clientes que eliminen este encabezado en nuestra guía de documentación e instalación del controlador de zonas de almacenamiento.

Consulte el siguiente artículo para conocer los pasos específicos que debemos proporcionar en nuestra documentación: `https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/`

Verificar la configuración del controlador de zonas de almacenamiento

October 13, 2020

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Compruebe que un controlador de zonas de almacenamiento registrado con ShareFile y, a continuación, compruebe si hay otros problemas de configuración antes de continuar.

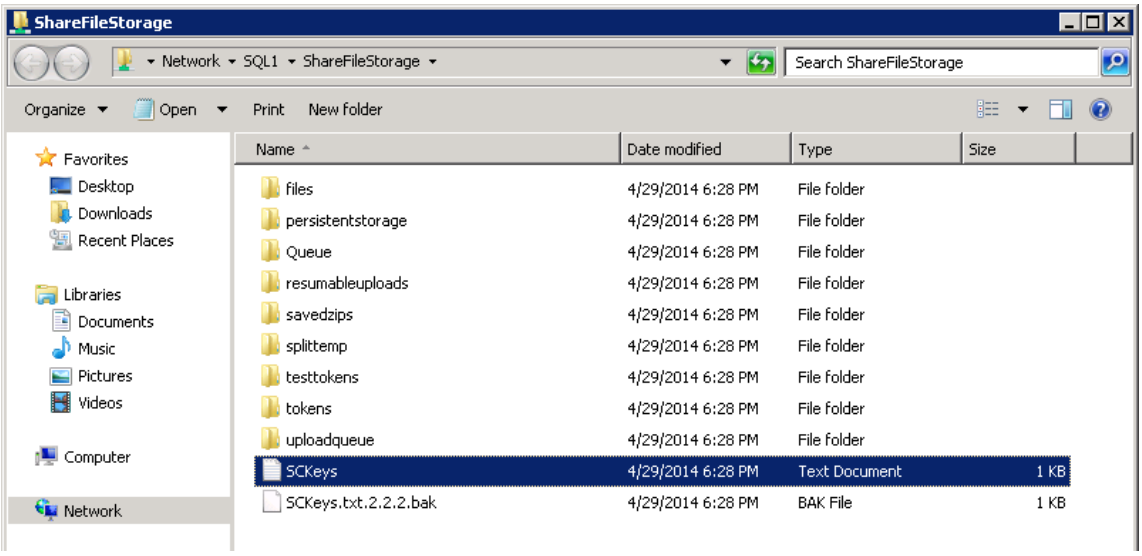
1. En la consola del controlador de zonas de almacenamiento, haga clic en la ficha **Supervisión**.
2. Compruebe que el Estado de latido tenga una marca de verificación verde.

   Un icono rojo indica que ShareFile.com no está recibiendo los mensajes de latidos. En ese caso, verifique la conectividad de red desde su controlador de zonas de almacenamiento a www.sharefile.com y desde un equipo externo a la URL de su controlador de zonas de almacenamiento. Para zonas estándar, el controlador de zonas de almacenamiento debe ser accesible en el puerto 443 con un certificado SSL público válido y de confianza.

   Después de una actualización, el estado de Conectividad ShareFile desde Servicios de limpieza de archivos podría mostrar temporalmente un icono rojo. Esto ocurre si Windows inicia ese servicio antes de que el controlador de zonas de almacenamiento establezca una conexión de red. El estado volverá a un icono verde después de que el servidor del Controller vuelva a estar en la red.
3. Comprobar la conectividad a su zona privada: Desplácese hasta la URL externa (en forma de `https://server.subdomain.com`) de su zona privada.

   Si se permite que el tráfico de Internet pase hacia y desde un controlador de zonas de almacenamiento, verá el logotipo de ShareFile. Si el controlador de zonas de almacenamiento no está configurado correctamente, es posible que vea un logotipo de IIS o una pantalla de inicio de sesión de Citrix ADC. Asegúrese de que el tráfico HTTPS entrante y saliente está permitido a través del puerto 443. Si la dirección URL externa apunta a Citrix ADC, busque aciertos en la conmutación de contenido y el servidor virtual de equilibrio de carga para los datos. Para obtener más información, consulte "El controlador de zonas de almacenamiento no carga datos a ShareFile"en Solucionar problemas de instalación y configuración.
4. Compruebe que el recurso compartido de red que ha creado para el almacenamiento privado de datos tiene una estructura de carpetas y algunos archivos creados por el controlador de zonas de almacenamiento, incluido Sckeys.txt, que debe residir en la carpeta raíz del almacenamiento compartido.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



SCKeys.txt se crea cuando se instala el controlador de zonas de almacenamiento, siempre que no haya problemas de credenciales o derechos de acceso. Si Sckeys.txt no está presente, compruebe las listas de control de acceso en el recurso compartido de archivos y, a continuación, vuelva a instalar el controlador de zonas de almacenamiento.

5. Compruebe el estado de los StorageZone Connectors desde la interfaz de ShareFile:

   a) Inicie sesión en su cuenta de ShareFile Enterprise, vaya a **Administrar > Zonas de almacenamiento** y compruebe que la columna Estado incluya una marca de verificación verde.

   b) Haga clic en el nombre del sitio y compruebe que el mensaje Heartbeat indica que el controlador de zonas de almacenamiento está respondiendo.

6. Probar una carga de archivos: Inicie sesión en la interfaz web ShareFile, cree una carpeta compartida asignada a la zona que acaba de configurar, cargue un archivo en esa carpeta y, a continuación, compruebe que el archivo aparece en la carpeta.

Cambiar la zona predeterminada para las cuentas de usuario

March 16, 2024

De forma predeterminada, las cuentas de usuario existentes y recién aprovisionadas utilizan el almacenamiento en la nube administrado por Sharefile como zona predeterminada. Cambie la zona predeterminada de la siguiente manera:

- Para especificar la zona predeterminada para las cuentas de usuario aprovisionadas desde AD, durante el aprovisionamiento de usuarios, seleccione la ubicación de almacenamiento. Para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

obtener más información, consulte **Editar opciones de reglas de usuario** en el artículo Administración basada en políticas de ShareFile.

- Para cambiar la zona predeterminada de un usuario individual, abra la consola de administrador de ShareFile y vaya a **Administrar**usuarios.

Especificar un servidor proxy para las zonas de almacenamiento

April 19, 2021

La consola de controlador de zonas de almacenamiento permite especificar un servidor proxy para controlador de zonas de almacenamiento. También puede especificar un servidor proxy mediante otros métodos.

Los controlador de zonas de almacenamiento primario y secundario se comunican entre sí mediante HTTP. Si todo el tráfico HTTP está configurado para pasar por un servidor proxy saliente que no admite conexiones de nuevo a un servidor interno, debe configurar los controlador de zonas de almacenamiento principal y secundario para omitir el servidor proxy para que puedan comunicarse entre sí, como se describe en los pasos siguientes: Sí.

> **Importante:**
>
> La configuración de la lista de omisión aparece solo para la última versión del controlador de zonas de almacenamiento. Si está utilizando controlador de zonas de almacenamiento 2.2 a 2.2.2, debe agregar manualmente una lista de omisión a Web.config para cada servidor secundario, como se describe en Web.config.

1. En la consola del controlador de zonas de almacenamiento (`http://localhost/configservice/login.aspx`), haga clic en la ficha **Redes**.

   > **Nota:**
   >
   > Si está utilizando el controlador de zonas de almacenamiento 5.11.17, cambiar cualquier proxy requiere autenticación. Cuando se le solicite, introduzca la dirección de correo electrónico, la contraseña y el subdominio FQDN de la URL de cuenta completa, como subdominio.sharefile.com o subdominio.sharefile.eu, de su cuenta. Haga clic en Iniciar sesión.

2. Active la casilla de verificación Habilitar proxy e introduzca la dirección y el puerto del servidor proxy.
3. Seleccione un modo de autenticación y especifique su cuenta de Windows designada para el acceso proxy de ShareFile.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Si el sitio proporciona proxy todo el tráfico HTTP saliente y una zona tiene varios controlador de zonas de almacenamiento, configure las opciones de omisión:
    - Si todo el tráfico del controlador de zonas de almacenamiento está en la misma subred, active la casilla de verificación **Omitir proxy…** para que los controladores puedan comunicarse entre sí.
    - Si los controlador de zonas de almacenamiento se encuentran en subredes diferentes, escriba el nombre de host del controlador de zonas de almacenamiento principal o la dirección IP en Dirección de omisión.
5. Reinicie el servidor IIS de todos los miembros de la zona.

Configurar el controlador de dominio de modo que confíe en el controlador de zonas de almacenamiento para la delegación

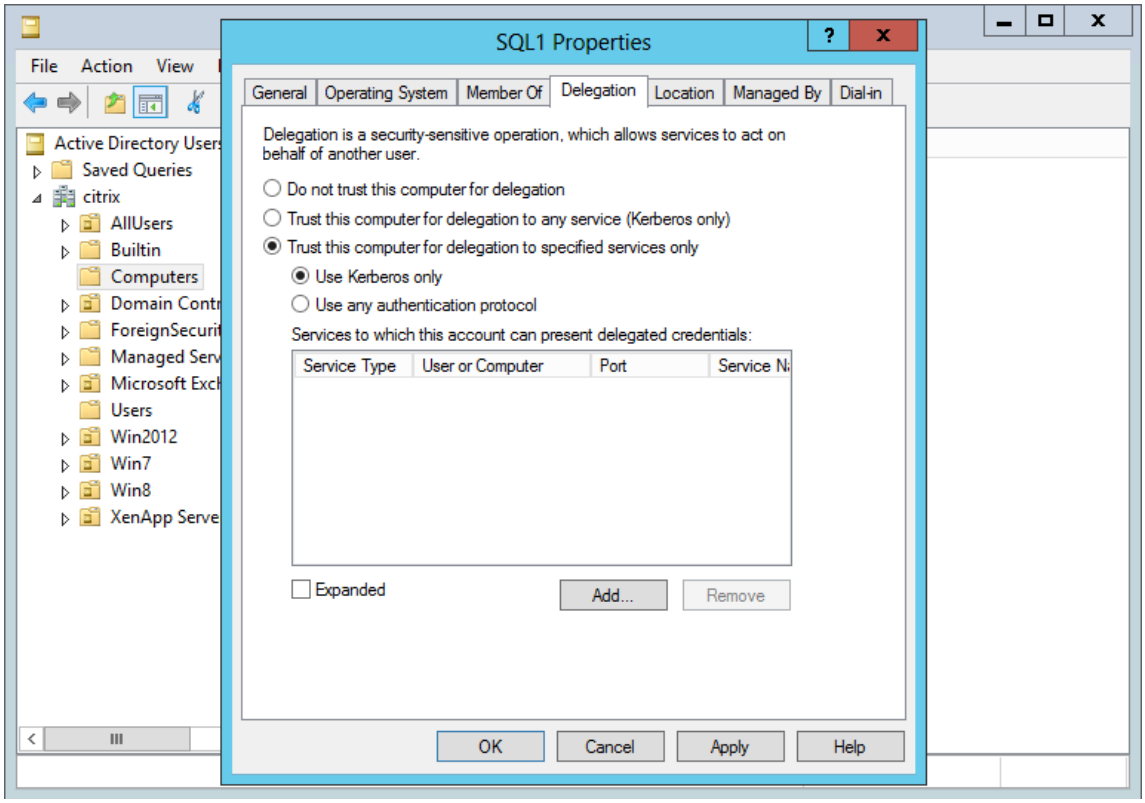
October 13, 2020

> **Nota:**
>
> Esta sección solo se aplica a los StorageZone Connectors.

Para admitir la autenticación NTLM o Kerberos en recursos compartidos de red o sitios de SharePoint, configure el Controller de dominio de la siguiente manera.

1. En el Controller de dominio del dominio de zonas de almacenamiento, haga clic en **Inicio > Herramientas administrativas > Usuarios y equipos de Active Directory**.
2. Expanda el dominio y expanda la carpeta Equipos.
3. En el panel derecho, haga clic con el botón secundario en el nombre del controlador de zonas de almacenamiento, seleccione **Propiedades** y, a continuación, haga clic en la ficha **Delegación**.
4. Para Kerberos, seleccione **Confiar en este equipo solo para la delegación a servicios especificados**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Para NTLM:

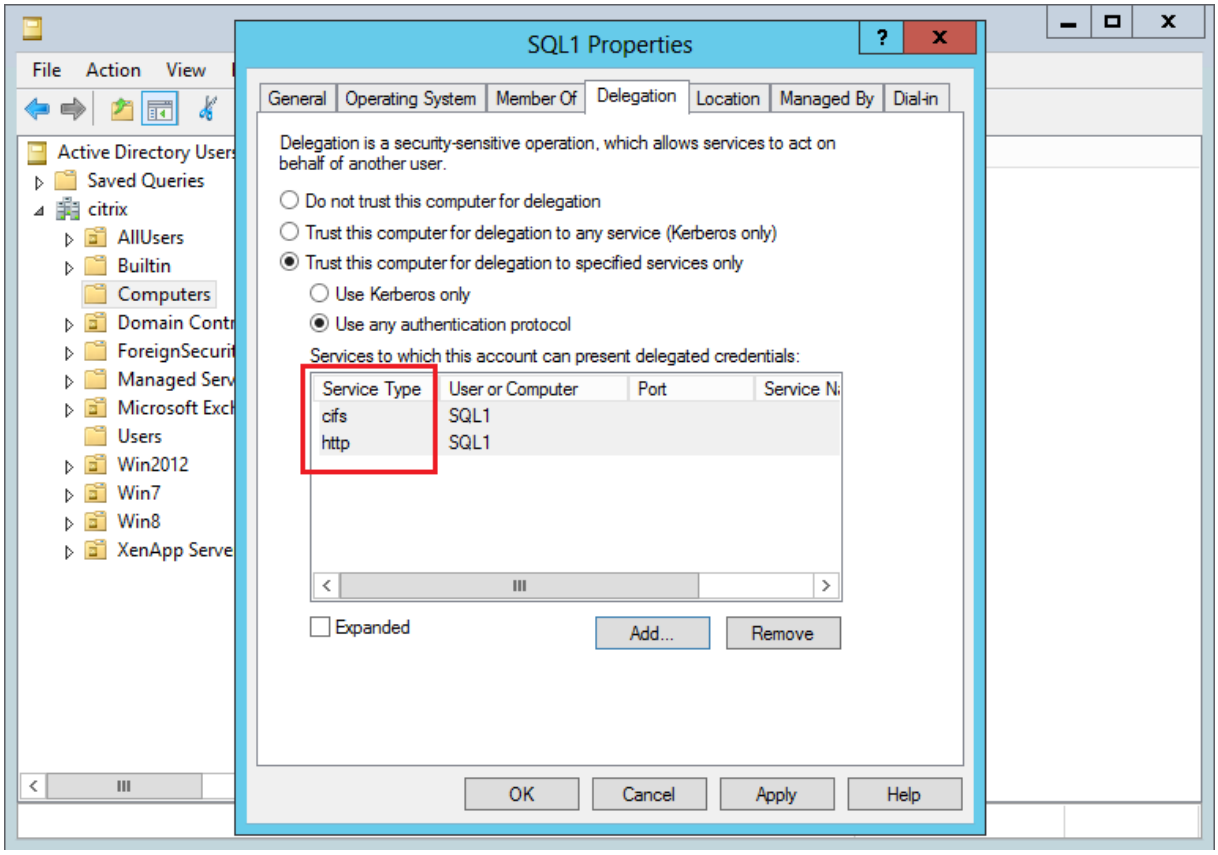
   a) Seleccione **Confiar en este equipo para la delegación solo a servicios especificados** y **Usar cualquier protocolo de autenticación**. Haga clic en **Aceptar**.

   b) Haga clic en el botón **Add**. En el cuadro de diálogo **Agregar servicios**, haga clic en **Usuarios o equipos** y, a continuación, busque o escriba el nombre de host para el recurso compartido de red o el servidor de SharePoint. Haga clic en **Aceptar**.

      Si tiene varios servidores de archivos o servidores de SharePoint, agregue un servicio para cada uno.

   c) En la lista Servicios disponibles, seleccione los servicios utilizados: CIFS (para conector para recursos compartidos de archivos de red) y HTTP (para conector para SharePoint). Haga clic en Aceptar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configure el controlador de zonas de almacenamiento para obtener vistas previas de aplicaciones web, miniaturas y uso compartido de solo lectura

March 16, 2024

Las vistas previas de archivos locales se representan en el servidor Microsoft Office Web Apps (OWA) local. Al obtener una vista previa de los archivos almacenados en una zona de almacenamiento administrada por Citrix, los servidores OWA administrados por Citrix o Microsoft renderizarán las vistas previas.

> **Importante:**
>
> **Requisitos para la inclusión en listas de permitidos**:
>
> `*.sf-api.com` debe estar accesible desde su servidor de Office Online para obtener una vista previa y editarla para que funcione correctamente en las zonas de almacenamiento versión 5.0 o posterior.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos

Tipos de archivos compatibles para la vista previa de archivos locales

- documento, .docm, .docx, .punto, .dotm, .punto, .punto, .odt
- .ods, .xls, .lsb, .xlsm, .xlsx
- .odp, .pot, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx
- .pdf
- Archivos de imagen (bmp, gif, jpg, jpeg, png, tif, tiff)

Tipos de archivos compatibles para la edición de archivos local

- .docm, .docx, .dot
- .ods, .lsb, .xlsm, .xlsx
- .odp, .ppsx, .pptx

Entornos admitidos

- Zonas estándar
- Zonas multiarrendatario
- Aplicación web

Consideraciones sobre listas de permitidos o redes

- El servidor OOS debería poder contactar con `https://\*.sf-api.com` **(o .eu)**
- El servidor SZC debería poder contactar con `https://\*.sf-api.com` y `https://\*.sharefile.com` **(o .eu)**
- El servidor SZC debería poder contactar con el servidor OOS `https://\<Customer OOS / OWA Endpoint\>/hosting/discovery` (por ejemplo, `https://oos.sharefileexample.com/hosting/discovery`)

Para modificar archivos locales, el control de versiones de archivos debe estar habilitado en su cuenta de ShareFile.

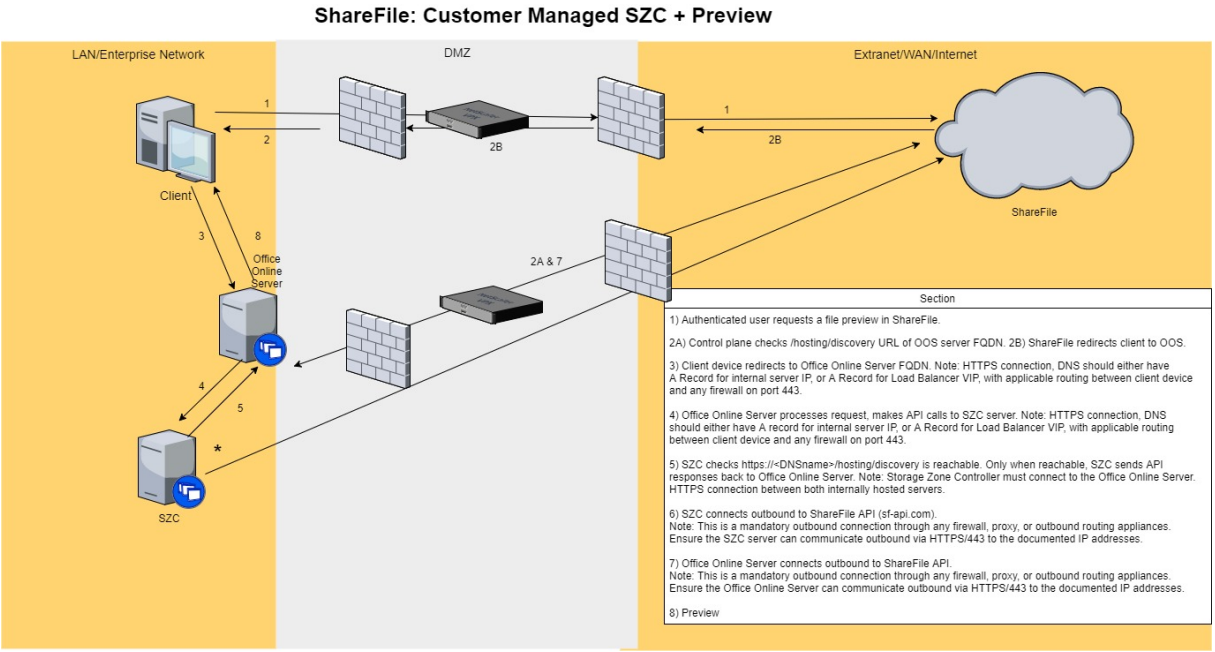
La configuración para activar la edición en línea de Microsoft Office en el menú de preferencias avanzadas de ShareFile Web App no afecta a la capacidad de modificar archivos locales. Esa opción específica **no** controlará la capacidad de modificar archivos locales, sino que se aplicará a la edición de cualquier archivo almacenado en una nube pública. La habilitación de la edición de archivos locales la controla exclusivamente el administrador del controlador de zonas de almacenamiento mediante los pasos que se describen a continuación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Compatibilidad con servidores de Microsoft

- **Microsoft Server 2016**: admite la posibilidad de modificar y previsualizar archivos. La edición también se puede desactivar.
- **Microsoft Server 2013**: solo admite la posibilidad de previsualizar archivos.

Diagrama de arquitectura y red



1. El usuario autenticado solicita una vista previa del archivo en ShareFile.
2. ShareFile emite una redirección al dispositivo cliente con el FQDN de Office Online Server
3. El dispositivo cliente redirige al FQDN de Office Online Server.

   > **Nota:**
   >
   > En la conexión HTTPS, el DNS debe tener un registro para la IP interna del servidor o un registro para el VIP de Load Balancer, con el enrutamiento aplicable entre el dispositivo cliente y cualquier firewall en el puerto 443.

4. Office Online Server procesa la solicitud y realiza llamadas a la API al servidor del controlador de zonas de almacenamiento.

   > **Nota:**
   >
   > En la conexión HTTPS, el DNS debe tener un registro para la IP interna del servidor o un registro para el VIP de Load Balancer, con el enrutamiento aplicable entre el dispositivo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> cliente y cualquier firewall en el puerto 443.

5. El controlador de zonas de almacenamiento comprueba si puede contactar con `https://\<DNSname\>/hosting/discovery` Solo cuando está disponible, SZC envía las respuestas de la API a Office Online Server.

   > **Nota:**
   >
   > El controlador de zona de almacenamiento debe conectarse al servidor de Office Online. Conexión HTTPS entre ambos servidores alojados internamente.

6. El controlador de zonas de almacenamiento conecta el correo saliente a la API de ShareFile (sf-api.com).

   > **Nota:**
   >
   > Esta es una conexión saliente obligatoria a través de cualquier firewall, proxy o dispositivo de enrutamiento saliente. Asegúrese de que el servidor del controlador de zonas de almacenamiento pueda comunicarse de forma saliente mediante HTTPS/443 con las direcciones IP documentadas anteriormente.

7. Office Online Server conecta el servidor saliente a la API de ShareFile.

   > **Nota:**
   >
   > Esta es una conexión saliente obligatoria a través de cualquier firewall, proxy o dispositivo de enrutamiento saliente. Asegúrese de que Office Online Server pueda comunicarse de forma saliente mediante HTTPS/443 con las direcciones IP documentadas anteriormente.

8. Se produce la vista previa.

Para que el controlador de zonas de almacenamiento transmita bytes de archivos a OOS en lugar de que OOS llame al plano de control de ShareFile para descargar el contenido: necesitamos actualizar una clave en uno de los archivos de configuración del controlador de zonas de almacenamiento.

Es necesario actualizar **C:\inetpub\wwwroot\Citrix\StorageCenter\WopiServer\AppSettingsReleaseOnPrem.**

Este archivo de configuración tiene una clave **downloadFileFromSC** que actualmente es **false**. Cambie la clave a **verdadera** y reinicie IIS.

Al hacerlo, se actualiza la configuración. Además, OOS ya no llama al plano de control de ShareFile para descargar el contenido del archivo.

Al usar esta opción, ¿sería correcto afirmar que no habría tráfico entrante desde el plano de control a OOS?

Si se usa la opción anterior, OOS ya no realiza conexiones salientes al plano de control de ShareFile.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sin embargo, el plano de control de ShareFile sigue realizando conexiones salientes a OOS, independientemente de si se utiliza o no la opción anterior.

¿Hay ventajas o desventajas de usar un método frente al otro?

En este enfoque, OOS no descarga el contenido del archivo directamente. El controlador de zonas de almacenamiento descarga y transmite los bytes del archivo a OOS. Por lo tanto, aumentará la carga en los servidores del controlador de zonas de almacenamiento.

Descargar y transmitir bytes de archivos es una tarea que consume muchos recursos. Según la cantidad de usuarios y la cantidad de operaciones de vista previa y edición, la carga aumenta en los servidores de StorageZones Controller.

Habilitar la vista previa y la edición locales

Para admitir la vista previa de documentos e imágenes en el navegador, las miniaturas, el uso compartido de datos almacenados en zonas de almacenamiento administradas por el cliente y la edición de archivos local, configure el controlador de zonas de almacenamiento de la siguiente manera:

1. En la consola del controlador de zonas de almacenamiento, haga clic en la **ficha ShareFile Data**.
2. En la sección **Configuración de recursos compartidos de red local**, habilite **Configurar vistas previas de aplicaciones web de oficina**.
3. Introduzca la URL externa de su servidor de Microsoft Office Web Apps (OWA).
   - Los usuarios deben descargar y configurar el software del servidor OWA mediante su suscripción a Microsoft Office MSDN.
4. Seleccione **Habilitar la edición de Office Online** (si es necesario)
5. Compruebe que la URL de OWA sea accesible externamente.
6. Compruebe que los servidores de Office Online se puedan comunicar con `*.sf-api.com`.
7. En la consola del controlador de zonas de almacenamiento, haga clic en la ficha **Supervisión**.
8. Compruebe que **OWA Server Connectivity** tenga una marca de verificación verde.

> **Nota:**
>
> La edición de archivos locales requerirá que se habilite el control de versiones de archivos en la cuenta de ShareFile. Si el control de versiones de archivos está inhabilitado para la cuenta, la edición local no funcionará.

Importante:

Configurar la sincronización del reloj:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Verifique que la hora de su controlador de zonas de almacenamiento esté sincronizada con time.windows.com u otro servidor NTP. Haga clic aquí para obtener información sobre cómo configurar la sincronización del reloj.? (Redirigido desde =MSDN)

Modificación del URAL de OWA o desactivaciónde las vistas previas:

- Cualquiera de las acciones anteriores requiere que se reinicie el servicio IIS para cada controlador principal y secundario.

Limitaciones

- Las aplicaciones móviles no admiten la edición en el navegador.
- Los conectores no admiten vistas previas en el navegador.

Las vistas previas de WOPI no son compatibles con las cuentas de VDR.

Para obtener información sobre cómo configurar su Citrix ADC para compartir solo lectura, consulte [Configurar Citrix ADC para]el controlador de zonas de almacenamiento.(/en-us/storage-zones-controller/5-0/install/configure-netscaler.html)

Solución de problemas de OWA y OOS

Si tiene problemas para obtener una vista previa o modificar archivos locales, los pasos siguientes le ayudarán a identificar y corregir problemas específicos.

Para solucionar problemas de configuración, primero inicie sesión en la máquina OWA u OOS.

1. Compruebe que los servicios Windows de Office WebApps u OfficeOnline se estén ejecutando en services.msc.
2. En un explorador web nuevo, abra la página `http://localhost/hosting/discovery`. Si esta página se carga correctamente, se devolverá una respuesta XML.
3. Ejecute PowerShell como administrador y ejecute el siguiente comando:

```
Get-OfficeWebAppsFarm
```

Si recibe un mensaje de ADVERTENCIA o ERROR en la respuesta, revise los ajustes de configuración para ver si hay errores o equivocaciones.

Consideraciones sobre la red:

- El servidor OOS debería poder contactar con `https://*.sf-api.com` **(o .eu)**
- El servidor SZC debería poder contactar con `https://*.sf-api.com` y `https://*.sharefile.com` **(o .eu)**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El servidor SZC debería poder acceder al servidor OOS. `https://<CustomerOOS/OWAEndpoint\>/hosting/discovery` Por ejemplo: `https://oos.sharefileexample.com/hosting/discovery`.

Configurar zonas de almacenamiento multiusuario

March 16, 2024

Una zona de almacenamiento multiusuario es una función del controlador de zonas de almacenamiento de ShareFile que permite a los proveedores de servicios (CSP) de Citrix crear y administrar una única zona de almacenamiento que comparten todos los inquilinos.

Si es un CSP con una cuenta de socio aprovisionada por ShareFile, puede alojar una zona de almacenamiento estándar multiusuario en su dominio que admita un número ilimitado de inquilinos. El uso de una zona multiinquilino le permite:

- Proporcione a cada inquilino una cuenta de ShareFile única y aproveche todas las excelentes funciones de ShareFile, como la personalización de la marca, las preferencias de retención de archivos y la configuración de seguridad.
- Mantenga un único repositorio de almacenamiento para todos sus inquilinos.
- Incorpore nuevos clientes con mayor rapidez y reduzca el costo y la complejidad de la administración que implica crear una zona de almacenamiento independiente para cada cuenta de cliente.

Crear una cuenta de socio

Debe tener una cuenta de socio antes de poder registrar una zona de almacenamiento multiusuario.

Para crear una cuenta de socio, debes registrarte en el programa CSP y pedir un SKU de stock a tu distribuidor preferido que te dé derecho a ofrecer ShareFile como servicio.

Si ya está registrado como CSP y ha pedido el SKU de stock de ShareFile para CSP correspondiente, ya se ha creado una cuenta de socio para usted. < acctsvcs@sharefile.com >Si no puede encontrar esta nueva cuenta de socio, póngase en contacto con los servicios de cuentas de ShareFile en.

Cuando comience a aprovisionar cuentas de clientes con su oferta CSP ShareFile, le recomendamos que cree un usuario administrador de cuentas de servicio genérico en su cuenta de socio. De esta forma, el usuario administrador puede ser el administrador asociado oficial de todas sus cuentas de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

cliente. Asegúrese de que este usuario administrador de la cuenta de servicio tenga activado el permiso Administrar inquilinos. Por eso, animamos a los socios a crear este administrador de socios ahora antes de completar el formulario de solicitud de cuenta de cliente de CSP (en el paso 4).

Instalar y configurar una zona de almacenamiento multiinquilino

- Cree una nueva zona de almacenamiento multiusuario y asóciela a su cuenta de socio. Para obtener más información, consulte Instalar el controlador de zonas de almacenamiento y crear una zona de almacenamiento.
- Instale el controlador de zona de almacenamiento en modo multiusuario. Asegúrese de ejecutar la siguiente línea de comandos especificada en el artículo de instalación mencionado en el paso anterior.

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

> **Nota:**
>
> En el comando anterior, es posible que necesite actualizar el número de versión (5.0.1 en el ejemplo) para que coincida con el número de msi que está intentando instalar.

Configure la nueva zona de almacenamiento y asóciela a su cuenta de socio

Para obtener más información, consulte el paso 10 de Instalar el controlador de zonas de almacenamiento y crear una zona de almacenamiento.

Inicie sesión en su cuenta de socio en la que desea registrar la nueva zona.

> **Importante:**
>
> Esta cuenta debe tener los siguientes permisos de ShareFile: Administrar inquilinos y Crear y administrar zonas.

Ahora puede iniciar sesión en su cuenta de socio y ver la nueva zona de almacenamiento multiusuario. Haga clic en la **pestaña Configuración del administrador > Zonas de almacenamiento > Administrado por el socio**.

Solicitar cuentas de inquilinos para la zona multiinquilino

Para solicitar cuentas de inquilino, rellene el formulario de solicitud de cuenta de cliente de CSP.

Cuando solicite una cuenta de inquilino, también debe especificar un usuario administrador asociado. Este administrador asociado debe ser un usuario administrador en su cuenta de socio con el permiso Administrar inquilinos habilitado. Cuando se crea una cuenta de inquilino, este usuario administrador

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

asociado se aprovisionará automáticamente en la cuenta como usuario administrador y podrá iniciar sesión y administrar la cuenta de inquilino. Como no puede haber dos usuarios en una cuenta con la misma dirección de correo electrónico, el correo electrónico del administrador del socio especificado en el formulario no puede ser el mismo que el del administrador del cliente en el mismo formulario.

Para garantizar la entrega más rápida, asegúrese de proporcionar el ID de organización correcto y el nombre de la zona multiusuario que desea usar como zona de almacenamiento para la cuenta del inquilino.

Recibirá un correo electrónico cuando Citrix aprovisione las cuentas solicitadas. El correo electrónico incluirá detalles sobre el subdominio del inquilino y un enlace de activación para configurar el acceso. ShareFile le enviará a usted y a los usuarios administrativos de sus clientes correos electrónicos por separado.

A continuación, sus clientes pueden empezar a usar ShareFile. Todos los usuarios nuevos aprovisionados a la cuenta de un inquilino utilizarán la zona multiinquilino que especificó como ubicación predeterminada para los archivos del usuario.

Vista previa de archivos de Office y PDF con un servidor de Office Online

Esta funcionalidad es compatible con los entornos de Office Online Server compatibles. Haga clic aquí para obtener información sobre la configuración.

Uso compartido de conectores

Esta funcionalidad es compatible con las zonas multiinquilino.

Gestiona inquilinos

Dentro de la cuenta de socio, hay un panel de administración de inquilinos ubicado en **Configuración del administrador > Preferencias avanzadas**. Este panel centralizado te permite comprobar el estado de todos los inquilinos vinculados a tu cuenta de socio. El panel incluye el consumo de licencias, la zona de almacenamiento predeterminada, el consumo de almacenamiento y el estado de la cuenta (de pago o de prueba) de cada inquilino.

> **Nota:**
>
> El panel solo está disponible para los usuarios de su cuenta de socio que tengan habilitado el permiso de usuario **Administrar inquilinos**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Limitaciones de múltiples inquilinos

La función de administración de derechos de información (IRM) de ShareFile no es compatible con las zonas de almacenamiento multiusuario.

Solución de problemas

No se pudo crear la zona: Prohibido

Al registrarse en la zona de almacenamiento, si recibe el siguiente error: «No se pudo crear la zona: prohibida», compruebe que sus permisos de usuario incluyen el permiso «Administrar inquilinos».

Actualizaciones

March 16, 2024

Actualice el controlador de zonas de almacenamiento 5.10 o posterior a la versión más reciente

> **Notas:**
>
> ShareFile recomienda tomar una instantánea del servidor antes de la actualización y hacer una copia de seguridad de la configuración del servidor de la zona de almacenamiento. Para obtener información sobre cómo hacer una copia de seguridad de la configuración de la zona de almacenamiento, consulte Hacer una copia de seguridad de la configuración de una controladora de zonas de almacenamiento principal
>
> . Si tiene problemas con la actualización de la controladora de zonas de almacenamiento, consulte Solución de problemas con las actualizaciones del controlador de zonas de almacenamiento de ShareFile.

Actualice el controlador de zonas de almacenamiento 5.10 mediante los siguientes pasos.

1. Descargue la versión más reciente del software Storage Zone Controller desde la página de descargas de ShareFile.

   > **Nota:**
   >
   > Los controladores de zona de almacenamiento no están disponibles durante la actualización y el reinicio del servidor. Para evitar la pérdida de datos, recomendamos programar un período de mantenimiento con los usuarios. Hágales saber que la zona no está

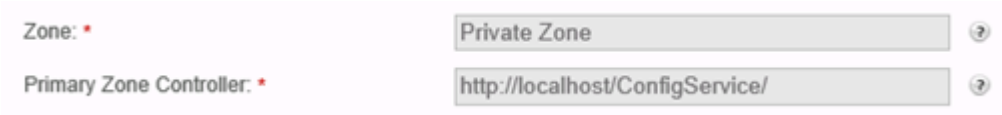
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> disponible para la transferencia de archivos durante la actualización.

2. Instale el archivo MSI en el servidor Windows que tenga instalado el controlador de zona de almacenamiento. Si tiene varios servidores, la actualización debe instalarse primero en el servidor principal y luego en los demás. Hay dos formas de identificar qué servidor es el servidor principal:

   a) Identifique el controlador de zonas de almacenamiento principal en la página **de configuración** :

      - En un servidor de controladores, vaya a `http://localhost/configservice/login.aspx` o inicie la herramienta de configuración desde el menú Inicio. Se requiere el permiso para "crear y administrar zonas"para acceder a la configuración.
      - En la ficha **Datos**, marque el campo Controlador de zona principal. El campo muestra el nombre de host del servidor del controlador de zona principal como `http://server/ConfigService`.



      Tenga en cuenta que el localhost de `http://localhost/ConfigService` indica que este servidor es el controlador de zona principal.

   b) Identifique el controlador de zonas de almacenamiento principal en el Registro:

      - En un servidor de controladores, abra el Editor del Registro (regedit.exe).
      - Busque la clave de registro: HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ Citrix\ StorageCenter
      - Verifique que el valor de la clave `isPrimaryConfigServer` sea true.

3. Inicie la actualización en el controlador de zona de almacenamiento principal:

   a) Ejecute StorageCenter.msi para iniciar el asistente de instalación del controlador de zonas de almacenamiento de ShareFile.

   b) Responda a las indicaciones. Cuando finalice la instalación, el asistente mostrará el mensaje "Asistente de configuración del controlador de zonas de almacenamiento Citrix ShareFile completado".

   c) Reinicie el servidor.

4. En cada controlador de zona de almacenamiento secundario (si es necesario):

   a) Ejecute StorageCenter.msi para iniciar el asistente de instalación del controlador de zonas de almacenamiento de ShareFile.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

   b) Responda a las instrucciones y, a continuación, seleccione **Finalizar.**

   c) Reinicie el servidor.

5. En todos los controladores de zona de almacenamiento, reinicie el servidor IIS de todos los miembros de la zona.

   a) Inicie el indicador de CMD y ejecútelo como administrador.

   b) Escriba `iisreset` y presione **Entrar**. Si se realiza correctamente, el mensaje indica "Los servicios de Internet se reiniciaron correctamente".

   c) Verifique que la configuración del registro del controlador de zonas de almacenamiento principal sea correcta después de la actualización.

6. Tras la instalación de la actualización, elija abrir la página de configuración de zonas de almacenamiento en cualquier miembro de la zona para iniciar sesión y modificar los ajustes de configuración.

   - Para volver a la consola del controlador de zonas de almacenamiento en cualquier momento, abra `http://localhost/configservice/login.aspx`. Tras hacer clic en **Finalizar** o volver a la consola del controlador de zonas de almacenamiento, se abre la página de inicio de sesión.

   > **Nota: Tenga**
   >
   > en cuenta que para iniciar sesión en la página de configuración del controlador de zona de almacenamiento, debe utilizar una contraseña específica de la aplicación. Si necesitas crear una nueva contraseña específica de la aplicación, consulta el siguiente artículo de soporte: Crear una contraseña específica de la aplicación.

   - Para cambiar la información que se muestra, seleccione **Modificar**, realice los cambios y seleccione **Guardar**.

   > **Nota:**
   >
   > Verifique que las transferencias de datos a cada controlador de zona de almacenamiento funcionen antes de finalizar el período de mantenimiento.

Administrar controladores de zonas de almacenamiento

February 9, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de instalar los controladores de zonas de almacenamiento principales y secundarios, utilice los siguientes procedimientos para administrar los controladores y prepararlos para la recuperación ante desastres.

Para abrir la consola del controlador de zonas de almacenamiento, vaya a `http://localhost/configservice/login.aspx` o inicie la herramienta de configuración desde el menú Inicio.

Administrar el controlador de zonas de almacenamiento

- Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento
- Cambiar la dirección o la frase de contraseña de un controlador de zonas de almacenamiento principal
- Rebajar y promover controladores de zonas de almacenamiento
- Inhabilitar, eliminar o volver a implementar un controlador de zonas de almacenamiento
- Transferir archivos a un nuevo recurso compartido de red
- Realizar una copia de seguridad de la configuración de un controlador de zonas de almacenamiento principal
- Recuperar una configuración de controlador de zonas de almacenamiento principal
- Reemplazar un controlador de zonas de almacenamiento principal
- Preparar el controlador de zonas de almacenamiento para la recuperación de archivos
- Recuperar archivos y carpetas de su copia de seguridad de ShareFile Data
- Reconciliar la nube de ShareFile con una zona de almacenamiento
- Configurar análisis antivirus de archivos cargados
- Migrar datos de ShareFile
- Favoritos del conector

Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento

October 13, 2020

Para configurar una zona de almacenamiento para alta disponibilidad, conecte al menos dos controladores de zonas de almacenamiento. Para hacer eso, debes:

1. Instale un controlador de zonas de almacenamiento principal y cree una zona (como se describe en Instalar un controlador de zonas de almacenamiento y crear una zona de almacenamiento).
2. Instale el controlador de zonas de almacenamiento en un segundo servidor y únelo a la misma zona.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los controlador de zonas de almacenamiento que pertenezcan a la misma zona deben utilizar el mismo recurso compartido de archivos para el almacenamiento.

En una implementación de alta disponibilidad, los servidores secundarios son controlador de zonas de almacenamiento independientes y totalmente funcionales. El subsistema de control de zonas de almacenamiento elige aleatoriamente un controlador de zonas de almacenamiento para gestionar las solicitudes de operación, incluidas las operaciones de carga, descarga, copia y eliminación.

Si el servidor principal se desconecta, puede ascender fácilmente un servidor secundario a primario. También puede degradar un servidor de primario a secundario.

1. Abra un explorador web en el servidor para que sea un controlador de zonas de almacenamiento secundario. A continuación `http://localhost/configservice/login.aspx`, abra e inicie sesión.
2. Haga clic en **Unir zona existente** y seleccione la zona de almacenamiento.
3. Introduzca la información solicitada y haga clic en **Registrar**.

   Para el Controller de zona principal, puede introducir solo el nombre de host o la dirección IP, y ShareFile rellenará la URL completa. Para probar una URL, introdúzcala en el campo de dirección del explorador. Si la dirección URL es correcta, aparecerá una página de banner de ShareFile. Para zonas estándar: Si la dirección URL es incorrecta y ha especificado https, compruebe que está utilizando certificados SSL públicos válidos y de confianza.
4. Si utiliza un servidor proxy para el controlador de zonas de almacenamiento principal, especifique el servidor proxy para el Controller secundario, como se describe en Especificar un servidor proxy para las zonas de almacenamiento.
5. Reinicie el servidor IIS de todos los miembros de la zona.

   Un controlador de zonas de almacenamiento secundario hereda la configuración del Controller principal durante el inicio.

Cambiar la dirección o la frase de contraseña de un controlador de zonas de almacenamiento principal

February 9, 2022

> **Nota:**
>
> Solo el administrador de la cuenta puede hacer cambios de dirección o frase de contraseña.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para especificar una dirección externa o local diferente para un controlador de zonas de almacenamiento principal

Puede cambiar la dirección externa de un controlador de zonas de almacenamiento principal mediante este procedimiento u otras herramientas de administración de servidores.

1. En el servidor del controlador de zona de almacenamiento principal, abra la **página de configuración** o vaya a: `http://localhost/configservice/login.aspx`.
2. Inicie sesión en la página de configuración con credenciales de administrador de ShareFile.
3. En la ficha Datos, seleccione **Modificar**.
4. Especifique la nueva **dirección externa** o **local** y, a continuación, seleccione **Guardar cambios**.
5. Repita los pasos en todos los miembros de zona.
6. Reinicie el servidor IIS de todos los miembros de la zona.

Para cambiar la frase de contraseña de un controlador de zonas de almacenamiento principal

> **Nota:**
>
> La frase de contraseña actual es necesaria para cambiar la frase de contraseña de un controlador de zonas de almacenamiento.

1. Abra la página de configuración de zonas de almacenamiento: `http://localhost/configservice/login.aspx`.
2. Haga clic en **Modificar**.
3. Especifique una frase de contraseña que se utilizará para proteger la clave de cifrado de archivos. Asegúrese de archivar la frase de contraseña y la clave de cifrado en una ubicación segura.

   La frase de contraseña no es la misma que la contraseña de su cuenta y no se puede recuperar si se pierde. Si pierde la frase de contraseña, no puede reinstalar zonas de almacenamiento, unir controladores de zonas de almacenamiento adicionales a la zona de almacenamiento ni recuperar la zona de almacenamiento si el servidor falla.

   > **Nota:**
   >
   > La clave de cifrado aparece en la raíz de la ruta de almacenamiento compartida. La pérdida del archivo de clave de cifrado interrumpe de inmediato el acceso a todos los archivos de la zona

4. Si cambió la frase de contraseña en el servidor principal: inicie sesión en la página de configuración de zonas de almacenamiento para cada uno de los demás miembros e introduzca la frase de contraseña cuando se le solicite.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Debe usar la misma frase de contraseña para cada controlador de zonas de almacenamiento de una zona.

5. Reinicie el servidor IIS de todos los miembros de la zona.

Desnivel y promoción de controlador de zonas de almacenamiento

October 13, 2020

En una implementación de alta disponibilidad, los servidores secundarios son controlador de zonas de almacenamiento independientes y totalmente funcionales. Para mantener o reemplazar una controlador de zonas de almacenamiento principal, vuelva a degradarla primero y, a continuación, promueva una controladora secundaria. Si el servidor principal se desconecta, puede ascender un servidor secundario a primario.

> **Precaución:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. Para degradar un controlador de zonas de almacenamiento principal:
   a) Busque la clave del Registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) Establezca IsPrimaryConfigServer en false.
   c) Establezca PrimaryConfigServiceURL en la dirección URL del servidor que será el nuevo controlador de zonas de almacenamiento principal, mediante el formulario `https://IPaddress` o `https://hostname/ConfigService/`.
   d) Reinicie el servidor IIS de todos los miembros de la zona.
2. Para promover un controlador de zonas de almacenamiento secundario:
   a) Busque la clave del Registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) Establezca IsPrimaryConfigServer en true.
   c) Establezca PrimaryConfigServiceURL en `http://localhost/ConfigService/`.
   d) Reinicie el servidor IIS de todos los miembros de la zona.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Modifique todos los controlador de zonas de almacenamiento secundarias adicionales:
   a) Busque la clave del Registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StorageCenter`
   b) Establezca PrimaryConfigServiceURL en la dirección URL del servidor que será el nuevo controlador de zonas de almacenamiento principal mediante el formulario `https://IPaddress` o `https://hostname/ConfigService/`.
   c) Reinicie el servidor IIS de todos los miembros de la zona.

Inhabilitar, eliminar o volver a implementar un controlador de zonas de almacenamiento

March 13, 2023

Para inhabilitar un controlador de zonas de almacenamiento

> **Nota:**
>
> Utilice este procedimiento si cada controlador de zonas de almacenamiento tiene una dirección externa diferente. Inhabilite un controlador desde la interfaz Citrix ADC si utiliza la misma dirección externa para todos los controladores de zonas de almacenamiento.

Desactive un controlador de zonas de almacenamiento antes de desconectar el servidor para realizar tareas de mantenimiento.

1. En la interfaz web de ShareFile, haga clic en **Administrador** y, a continuación, en **Zonas de almacenamiento**.
2. Haga clic en el nombre de la zona y, a continuación, en el nombre de host del controlador de zonas de almacenamiento.
3. Desactive la casilla de verificación habilitada y, a continuación, haga clic en **Guardar cambios**.
4. Reinicie el servidor IIS de todos los miembros de la zona.

Para eliminar un controlador de zonas de almacenamiento

Al eliminar un controlador de zonas de almacenamiento no se eliminan los datos ni el SCKeys.txt. Si va a eliminar un controlador de zonas de almacenamiento principal, destrúyalo antes de continuar.

1. En la interfaz web de ShareFile, haga clic en **Administrador** y, a continuación, en **Zonas de almacenamiento**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Haga clic en el nombre de la zona y, a continuación, en el nombre de host del controlador de zonas de almacenamiento.
3. Haga clic en **Eliminar**.
4. Reinicie el servidor IIS de todos los miembros de la zona.

Para volver a implementar un controlador de zonas de almacenamiento

No se pierde información al volver a implementar un controlador de zonas de almacenamiento.

1. Desinstale las zonas de almacenamiento del servidor.
2. En la interfaz web de ShareFile, haga clic en **Administración > Zonas de almacenamiento**y, a continuación, seleccione su zona. No elimines la zona.
3. Seleccione el controlador de zonas de almacenamiento y elimínelo.
4. Instale zonas de almacenamiento. No lo registre todavía.
5. Ejecute el asistente de configuración del controlador de zonas de almacenamiento para unir el controlador de zonas de almacenamiento a una zona y completar el registro.
6. Reinicie el servidor IIS de todos los miembros de la zona.

Transferir archivos a un nuevo recurso compartido de red

October 13, 2020

Antes de configurar un nuevo recurso compartido de red para el almacenamiento de datos privado:

Requisitos

- Los controlador de zonas de almacenamiento que pertenezcan a la misma zona de almacenamiento deben utilizar el mismo recurso compartido de archivos para el almacenamiento.
- Los controladores de zonas de almacenamiento acceden al recurso compartido mediante el usuario del grupo de cuentas de IIS. De forma predeterminada, los grupos de aplicaciones operan bajo la cuenta de usuario del Servicio de red, que tiene derechos de usuario de bajo nivel. Un controlador de zonas de almacenamiento utiliza la cuenta Servicio de red de forma predeterminada.
- La cuenta de Servicio de red debe tener acceso **completo** a esta ubicación de almacenamiento.
- Inhabilite los controladores de zonas de almacenamiento para las nuevas cargas antes de transferir datos al nuevo recurso compartido. En la aplicación web, vaya a **Configuración del administrador** > **StorageZones**. Seleccione el nombre de la zona. En **Centros de almacenamiento**,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

seleccione cada servidor host. Para terminar el tráfico a cada servidor host, anule la selección de la opción **Habilitado** en **Configuración del servidor**.

1. Abra la página de configuración de zonas de almacenamiento: `http://localhost/configservice/login.aspx`.
2. Haga clic en **Modificar**.
3. En **Ubicación de almacenamiento**, escriba la ruta de acceso UNC al recurso compartido de red, en el formulario `\\server\share` y, a continuación, haga clic en **Guardar**.

   > **Precaución:**
   >
   > El controlador de zonas de almacenamiento sobrescribe los datos de esta ruta con un formato de almacenamiento propietario. Como práctica recomendada, nunca especifique una ruta de acceso a una ubicación con datos de archivo. Reserve esta ubicación de almacenamiento solo para zonas de almacenamiento para ShareFile Data.

4. Si las credenciales de la ruta UNC de la nueva ubicación de recurso compartido de red difieren de las anteriores, especifique el inicio de sesión de almacenamiento y la contraseña de almacenamiento.
5. Reinicie el servidor IIS de todos los miembros de la zona.
6. Inicie sesión en la página de configuración de todos los miembros de la zona.
7. Copie toda la estructura de directorios, incluido SCkeys.txt, en el nuevo servidor.

Realizar una copia de seguridad de la configuración de un controlador de zonas de almacenamiento principal

June 29, 2023

Se instala un controlador de zonas de almacenamiento en su sitio local y usted es responsable de realizar una copia de seguridad. Para proteger completamente su implementación, debe tomar una instantánea del servidor del controlador de zonas de almacenamiento, hacer una copia de seguridad de su configuración y preparar el controlador de zonas de almacenamiento para la recuperación de archivos.

Es fundamental que haga una copia de seguridad de la configuración tal como se describe en este tema. Por ejemplo, si no tiene una copia de seguridad y alguien elimina accidentalmente una zona, no podrá recuperar las carpetas y los archivos de esa zona.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Importante:**
>
> Asegúrese de utilizar PowerShell 4.0 para este procedimiento. Para obtener más información sobre los requisitos de PowerShell, consulte Scripts y comandos de PowerShell en los requisitos del sistema del controlador de zonas de almacenamiento.

El instalador del controlador de zonas de almacenamiento incluye un módulo de PowerShell con comandos que crean una copia de seguridad y restauran la configuración de un controlador de zonas de almacenamiento principal. La copia de seguridad incluye información de configuración para zonas, zonas de almacenamiento para ShareFile Data, conector de zona de almacenamiento para SharePoint y conector de zona de almacenamiento para recursos compartidos de archivos de red.

Los comandos de copia de seguridad y restauración requieren que ejecute la versión de 32 bits de PowerShell en el mismo contexto de usuario que el controlador de zona de almacenamiento. Para establecer el contexto del usuario, use la herramienta PSExec. Esta herramienta está disponible para su descarga en https://docs.microsoft.com/en-us/sysinternals/downloads/psexec.

> **Nota:**
>
> Estos pasos no se aplican a un controlador de zonas de almacenamiento secundario. Para recuperar un controlador de zonas de almacenamiento secundario, reinstale el controlador de zona de almacenamiento en el servidor y, a continuación, únalo al controlador de zonas de almacenamiento principal.

1. El script de PowerShell que se usa en este procedimiento no está firmada, por lo que debe cambiar la directiva de ejecución de PowerShell.

   a) Determine si la directiva de ejecución de PowerShell le permite ejecutar scripts locales sin firmar: PS `C:\>Get-ExecutionPolicy`

      Por ejemplo, una directiva de RemoteSigned, Sin restricciones o Bypass permite ejecutar scripts sin firmar.

   b) Para cambiar la directiva de ejecución de PowerShell: PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. Establezca el contexto de usuario para esta sesión de PowerShell. En una ventana de comandos, ejecute uno de los siguientes comandos.

   - Si utiliza la cuenta predeterminada de servicio de red:

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

   - Si usa un usuario designado para el grupo de aplicaciones del controlador de zonas de almacenamiento:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Se abre una ventana de PowerShell.

3. En el símbolo del sistema de PowerShell, importe el módulo ConfigBR.dll: `Import-Module C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll`

   Debe importar el módulo cada vez que abra una nueva ventana de PowerShell.

4. Desde la línea de comandos de PowerShell, ejecute el comando Get-SfConfig y complete las siguientes instrucciones:

   - **PrimaryZoneController**: Entradas de ejemplo:
     - Conéctese a un servidor local: `http://localhost/ConfigService/`
     - Conéctese a un servidor remoto: `http[s]://myservername.domain.com/ConfigService/`
     - Conéctese a un servidor remoto si los problemas de DNS impiden la conexión a un nombre de servidor: `http[s]://10.40.37.5/ConfigService/`
   - Frase de contraseña: la frase de contraseña especificada para el controlador de zona de almacenamiento.
   - FilePath: ejemplo `c:\szc-backup.bak`

   Parámetros de comando:

Parámetros	Descripción	Ejemplos
“server”	El nombre del servidor o la dirección IP del controlador de zonas de almacenamiento principal. Puede tener cualquiera de las siguientes formas que se muestran en Ejemplos y debe incluir la barra inclinada final.	Conectarse a un servidor local: `http://localhost/ConfigService/`; Conectarse a un servidor remoto: `http[s]://myservername.domain.com/ConfigService/`; Conectarse a un servidor remoto si los problemas de DNS impiden la conexión a un nombre de servidor: `http[s]://10.40.37.5/ConfigService/`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetros	Descripción	Ejemplos
“passphrase”	Frase de contraseña especificada para el controlador de zona de almacenamiento.	“MyPassphrase”
“fullpath”	Una ubicación para guardar el archivo de copia de seguridad.	“c:\szc-backup.bak”

El comando **Get-SfConfig** crea el archivo de copia de seguridad.

Para restaurar la configuración de un controlador de zonas de almacenamiento principal, consulte Recuperar una configuración de controlador de zonas de almacenamiento principal.

Recuperar una configuración de controlador de zonas de almacenamiento principal

February 9, 2022

> **Importante:**
>
> - Asegúrese de utilizar PowerShell 4.0 para este procedimiento. Para obtener más información sobre los requisitos de PowerShell, consulte los scripts y comandos de PowerShell en Requisitos del sistema del controlador de zonas de almacenamiento.
> - Para obtener más información sobre la implementación de TLS en todo el sistema, consulte el artículo de Microsoft sobre Cómo habilitar TLS 1.2 en los clientes.

El controlador de zonas de almacenamiento proporciona estas opciones para la recuperación ante desastres cuando se elimina o falla un controlador de zonas de almacenamiento principal:

- Si hay disponible un controlador de zonas de almacenamiento secundario, asciende el controlador secundario a uno principal.
- Si no hay un controlador de zonas de almacenamiento secundario disponible y realizó una copia de seguridad de la configuración del controlador de zonas de almacenamiento principal (como se describe en Realizar una copia de seguridad de la configuración del controlador de zonas de almacenamiento principal), recupere el controlador de zonas de almacenamiento principal del archivo de la copia de seguridad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si no tiene una copia de seguridad de la configuración del controlador de zonas de almacenamiento principal y todos los controladores de zonas de almacenamiento se eliminan accidentalmente o quedan inutilizables, solo es posible la recuperación parcial. Puede recuperar las zonas y la configuración de las zonas de almacenamiento de datos de ShareFile, pero no de los conectores de zonas de almacenamiento.

Para recuperar un controlador de zonas de almacenamiento principal a partir de un archivo de copia de seguridad

> **Nota:**
>
> Estos pasos solo se aplican a un controlador de zonas de almacenamiento principal. Para recuperar un controlador de zonas de almacenamiento secundario, reinstale el controlador de zonas de almacenamiento en el servidor y, a continuación, una el servidor al controlador de zonas de almacenamiento principal.

1. El script de comandos de PowerShell que se usa en este procedimiento no está firmada, por lo que puede que sea necesario cambiar la directiva de ejecución de PowerShell.

   a) Determine si la directiva de ejecución de PowerShell le permite ejecutar scripts locales sin firmar: PS `C:\>Get-ExecutionPolicy`

      Por ejemplo, una directiva de RemoteSigned, Sin restricciones o Bypass permite ejecutar scripts sin firmar.

   b) Para cambiar la directiva de ejecución de PowerShell: PS `C:\>Set-ExecutionPolicy RemoteSigned`

2. Establezca el contexto de usuario para esta sesión de PowerShell. En una ventana de comandos, ejecute uno de los siguientes comandos.

   > **Nota:**
   >
   > Descargue PsExec.exe en https://docs.microsoft.com/en-us/sysinternals/downloads/psexec y siga las instrucciones de instalación de esa página.

   - Si utiliza la cuenta predeterminada de servicio de red:

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

   - Si usa un usuario designado para el grupo de aplicaciones del controlador de zonas de almacenamiento:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Se abre una ventana de PowerShell.

3. En el símbolo del sistema de PowerShell, importe el módulo ConfigBR.dll: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

   Debe importar el módulo cada vez que abra una nueva ventana de PowerShell.

4. En el símbolo del sistema de PowerShell, ejecute el comando `Set-SfConfig`: `Set-SfConfig -PrimaryZoneController "server"-Passphrase "passphrase"-FilePath "fullpath"`

   Donde:

   - server es el nombre del servidor o la dirección IP del controlador de zonas de almacenamiento principal. Puede tener cualquiera de las formas siguientes y debe incluir la barra inclinada final.

     `http://localhost/ConfigService/`

     `servername/` o `serverip/` (si usa HTTP)

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

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

   - passphrase es la especificada para el controlador de zonas de almacenamiento.
   - fullpath es la ubicación y el nombre del archivo de copia de seguridad. Por ejemplo, `c:\szc-backup.bak`.

Para recuperar un controlador de zonas de almacenamiento principal sin un archivo de copia de seguridad

Si no tiene un archivo de copia de seguridad, puede recuperar las zonas y la configuración de las zonas de almacenamiento para ShareFile Data, pero no los conectores de zonas de almacenamiento.

1. Establezca el contexto de usuario para esta sesión de PowerShell. En una ventana de comandos, ejecute uno de los siguientes comandos.

   - Si utiliza la cuenta predeterminada de servicio de red:

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

   - Si usa un usuario designado para el grupo de aplicaciones del controlador de zonas de almacenamiento:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Se abre una ventana de PowerShell.

2. En el símbolo del sistema de PowerShell, importe el módulo ConfigBR.dll: `Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfigBR\ConfigBR.dll"`

   Debe importar el módulo cada vez que abra una nueva ventana de PowerShell.

3. En el símbolo del sistema de PowerShell, ejecute el comando Join-SfConfig:

   > **Importante:**
   >
   > El comando Join-SfConfig actualmente no es compatible con el almacenamiento de Azure o Amazon S3. Contacte con la asistencia de ShareFile si necesita usar este comando.

```
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]
```

   Donde:

   - ZoneID se puede obtener de la siguiente manera:

     a) En la interfaz web de ShareFile, haga clic en **Administración > Zonas de almacenamiento**, haga clic con el botón secundario en el nombre del sitio y, a continuación, elija **Propiedades**.

        La dirección que se muestra termina con el identificador de zona que se ve así: `zae4fb8c-8520-478f-8f87-aa589a8fd181`.

     b) Copie y pegue ese ID en el comando Join-SfConfig.

   - StorageCenterId se puede obtener de la siguiente manera:

     a) En la interfaz web de ShareFile, haga clic en Admin > zonas de almacenamiento, haga clic en el nombre del sitio, haga clic con el botón secundario del mouse en el nombre de host y,

        La dirección que se muestra termina con el identificador de almacenamiento que se ve así: `scd344cf-8043-4ce2-974b-8f9cd83e2978`.

     b) Copie y pegue ese ID en el comando Join-SfConfig.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- StorageZoneLocation solo se necesita si las zonas de almacenamiento para ShareFile Data están habilitadas para la zona.
- StorageUsername y StoragePassword solo son necesarios si las zonas de almacenamiento para ShareFile Data están habilitadas para la zona y su ubicación de almacenamiento requiere autenticación.
- AzureAccountName, AzureAccessKey y AzureContainerName solo se necesitan si las zonas de almacenamiento para ShareFile Data se almacenan en un contenedor de almacenamiento de Windows Azure.

4. Para recuperar conectores de zonas de almacenamiento, use la consola del controlador de zonas de almacenamiento (`http://localhost/configservice/login.aspx`) para habilitar y configurar los conectores.

Reemplazar un controlador de zonas de almacenamiento principal

October 13, 2020

Para reemplazar un controlador de zonas de almacenamiento principal por otro que se encuentre en una ubicación diferente, como en un dominio diferente, utilice los procedimientos de copia de seguridad y restauración. Los siguientes pasos garantizan que se transfieran los valores de configuración y todos los datos.

1. Cree un archivo de copia de seguridad para la configuración del controlador de zonas de almacenamiento existente. Consulte Respaldar la configuración de un controlador de zonas de almacenamiento principal.
2. Instale, pero no configure, un controlador de zonas de almacenamiento en la nueva ubicación de red.
3. Importe la configuración de copia de seguridad en el nuevo Controller. Consulte Recuperar una configuración de controlador de zonas de almacenamiento principal.
4. Copie los datos en el nuevo recurso compartido de red, inicie sesión en la consola de configuración del nuevo controlador de zonas de almacenamiento e introduzca la nueva información de ruta de almacenamiento. Consulte Transferir archivos a un nuevo recurso compartido de red.
5. En la nueva consola de configuración del controlador de zonas de almacenamiento, actualice la URL externa del Controller. Consulte Cambiar la dirección o la frase de contraseña de un controlador de zonas de almacenamiento principal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Preparar el controlador de zonas de almacenamiento para la recuperación de archivos

September 4, 2023

> **Advertencia:**
>
> La función de recuperación de ShareFile no realiza automáticamente una copia de seguridad de la ubicación de almacenamiento persistente. Usted es responsable de elegir una utilidad de copia de seguridad y ejecutarla cada 1 a 7 días.

La forma en que se prepare para la recuperación de archivos depende del lugar donde se almacenen los datos:

- **Un sistema de almacenamiento de terceros compatible**: Si utilizas un sistema de almacenamiento de terceros con controlador de zonas de almacenamiento, el almacenamiento de terceros es redundante y no se requiere una copia de seguridad local. Sin embargo, tenga en cuenta que un usuario de ShareFile que elimine un archivo puede recuperarlo de la papelera de reciclaje durante un breve período. No se puede recuperar un archivo de la papelera de reciclaje de ShareFile después de 45 días. Tras el período de recuperación, el archivo se elimina de la zona y, por lo tanto, del almacenamiento redundante de terceros. Si ese tiempo de recuperación no es el adecuado, considere una de estas soluciones:
  - Para evitar que el servicio de limpieza de archivos de StorageZone Controller purgue el archivo real de su ubicación de almacenamiento local, cambie el valor de la configuración **Periodo** en `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\SCFileCleanSvc\\FileDeleteService.exe.config`. Para obtener más información, consulte Personalizar las operaciones de memoria caché de almacenamiento. Tenga en cuenta que aumentar el tiempo de retención también aumenta la cantidad de almacenamiento de terceros necesaria.
  - Cree una copia de seguridad local de sus archivos de StorageZone cada siete días y determine la directiva de retención adecuada para las copias de seguridad.
- **Almacenamiento local**: Si utiliza un recurso compartido mantenido localmente para el almacenamiento de datos privados, es responsable de hacer una copia de seguridad de las entradas de registro y almacenamiento de archivos locales del controlador de zonas de almacenamiento local. ShareFile archiva los metadatos del archivo correspondiente que residen en la nube de ShareFile durante 3 años.
  Importante: Para protegerse contra la pérdida de datos, es fundamental que tome una instantánea del servidor del controlador de zonas de almacenamiento, haga una copia de seguridad de su configuración y haga una copia de seguridad del almacenamiento de archivos local.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de preparar el controlador de zonas de almacenamiento para la recuperación de archivos, tal como se describe en este tema, puede utilizar la consola de administración de ShareFile para:

- Explore sus zonas de almacenamiento en busca de registros de ShareFile Data para una fecha y hora determinadas y, a continuación, etiquete los archivos y carpetas que desee restaurar. ShareFile agrega los elementos etiquetados a una cola de recuperación. A continuación, ejecuta un script de recuperación para restaurar los archivos de la copia de seguridad a la ubicación de almacenamiento persistente.

  Para obtener más información, consulte Recuperar archivos y carpetas de la copia de seguridad de ShareFile Data.

- Reconcilie los metadatos almacenados en la nube de ShareFile con su almacenamiento local cuando no pueda recuperar datos de su almacenamiento local. La función de reconciliación de ShareFile elimina permanentemente de la nube de ShareFile los metadatos de los archivos que ya no se encuentran en una zona de almacenamiento en una fecha y hora especificadas.

  Para obtener más información, consulte Reconciliar la nube de ShareFile con una zona de almacenamiento

Requisitos previos

- Una máquina física o virtual dedicada con 2 CPU y 4 GB de RAM
- Windows Server 2012 R2 (centro de datos, estándar o Essentials)
- Windows Server 2016
- Windows Server 2019
- Windows PowerShell (versiones de 32 y 64 bits) debe admitir ensamblados en tiempo de ejecución de .NET 4. Para obtener más información, consulte la sección “Scripts y comandos de PowerShell”en los requisitos del sistema del controlador de zonas de almacenamiento.
- PsExec.exe: PsExec le permite iniciar PowerShell mediante la cuenta de servicio de red. También puede usar PsExec para programar tareas de recuperación. Descargue PsExec.exe en https://docs.microsoft.com/en-us/sysinternals/downloads/psexec y siga las instrucciones de instalación de esa página.

Resumen de los archivos utilizados para la recuperación ante desastres

Los siguientes archivos, ubicados en C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery, se utilizan para la recuperación ante desastres.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre de archivo	Descripción
DoRecovery.ps1	Script de PowerShell ejecutado por el programador de tareas de Windows para gestionar el proceso de recuperación. Este archivo almacena las ubicaciones de copia de seguridad y almacenamiento de archivos.
Recovery.psm1	Módulo de PowerShell que gestiona las operaciones de la cola de recuperación.
recovery.log	Archivo de registro que almacena el resultado de un proceso de recuperación.
recoveryerror.log	Archivo de registro que almacena los errores del proceso de recuperación.
LitJson.dll	Una biblioteca.Net para gestionar las conversiones desde y hacia cadenas JSON (notación de objetos de JavaScript).

Para configurar la carpeta de respaldo

En el servidor de respaldo, cree la carpeta en la que realizará la copia de seguridad de la carpeta de almacenamiento persistente.

Las zonas de almacenamiento para la copia de seguridad de archivos de ShareFile Data deben seguir el mismo diseño que el almacenamiento persistente del controlador de zonas de almacenamiento.

Si su ubicación de respaldo no sigue el mismo diseño que el almacenamiento persistente del controlador de zonas de almacenamiento, debe realizar un paso adicional durante el proceso de recuperación para copiar los archivos de la ubicación de respaldo a la ubicación que especifique en el script de Recovery PowerShell.

Diseño de almacenamiento

Diseño de respaldo

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

\\\BackupStorageIP
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
```

> **Importante:**
>
> La función de recuperación de ShareFile no realiza automáticamente una copia de seguridad de la ubicación de almacenamiento persistente. **Usted es responsable de elegir una utilidad de copia de seguridad y ejecutarla cada 1 a 7 días.**

Para crear una cola de recuperación ante desastres

Esta configuración única es obligatoria. Los siguientes ejemplos de comandos utilizan la carpeta de instalación del controlador de zonas de almacenamiento predeterminada.

1. En el controlador de zonas de almacenamiento, ejecute PowerShell como administrador.
2. El script de PowerShell utilizado en este procedimiento no está firmado, por lo que puede que tenga que cambiar la directiva de ejecución de PowerShell.

   a) Determine si su directiva de ejecución de PowerShell le permite ejecutar scripts locales sin firmar: PS C:\ >Get-ExecutionPolicy

      Por ejemplo, una directiva de RemoteSigned, Sin restricciones o Bypass permite ejecutar scripts sin firmar.

   b) Para cambiar la directiva de ejecución de PowerShell: PS C:\ >Set-ExecutionPolicy Remote-Signed

3. Para comprobar que PowerShell tiene la versión CLR correcta, escriba:

   Tabla de versiones $ps

   El valor de CLRVersion debe ser 4.0 o superior para que PowerShell pueda cargar ensamblados de .NET en scripts. Si no es así, cámbielo para las versiones de 32 y 64 bits de Windows PowerShell de la siguiente manera:

   a) Ejecute NotePad como administrador.

   b) Crea un archivo con el siguiente contenido.

```
1      <?xml version="1.0"?>
2      <configuration>
3          <startup useLegacyV2RuntimeActivationPolicy="true">
4              <supportedRuntime version="v4.0.30319"/>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
5             <supportedRuntime version="v2.0.50727"/>
6         </startup>
7     </configuration>
```

c) Seleccione Archivo > Guardar como, asigne al archivo el nombre powershell.exe.config y guárdelo en las siguientes ubicaciones:

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

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

d) Cierre la ventana de PowerShell, abra una nueva como administrador y escriba $psversiontable para comprobar que la versión CLR es correcta.

4. Cierre la ventana de PowerShell e inicie PowerShell con PsExec.exe de la siguiente manera:

   a) Abra una ventana del símbolo del sistema como administrador.

   b) Vaya a la ubicación de PsExec.exe e introduzca:

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

   c) Haga clic en Aceptar para aceptar el contrato de licencia de PsExec.exe.

5. Navegue hasta la carpeta de herramientas de recuperación ante desastres en la carpeta de instalación del controlador de zonas de almacenamiento:

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

6. Importe el módulo Recovery.psm1:

   Módulo de importación. \ Recovery.psm1

7. Para crear la cola de recuperación, introduzca: new-SCQueue -name recovery -operation recovery

   El resultado de ese comando incluye el nombre de la cola creada. Por ejemplo: Se creó la cola 92736b5d-1cff-4760-92c8-d8b04dc92cb2

   Para ver la nueva carpeta, abre un explorador de archivos y navega hasta:

   \\ server\ (*Su* ubicación de almacenamiento principal)\ Queue. Verás la carpeta Queue, como 92736b5d-1cff-4760-92c8-d8b04dc92cb2.

8. Personalice el script de recuperación de PowerShell para su ubicación, tal como se describe en la siguiente sección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para personalizar el script de recuperación de PowerShell para su ubicación

El programador de tareas ejecuta el script DoRecovery.ps1 de PowerShell para gestionar el proceso de recuperación. Este archivo incluye las ubicaciones de copia de seguridad y almacenamiento de archivos que debe especificar para su sitio.

1. En el controlador de zonas de almacenamiento, navegue hasta el script de recuperación de PowerShell:

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

2. Modifique el guion de la siguiente manera:

   a. Configure el parámetro $backupRoot para que apunte a la ruta UNC de la ubicación de la copia de seguridad. Por ejemplo: $backupRoot = "\\10.10.10.11\(*Your*BackupLocation)\persistentstorage"

   b. Configure el parámetro $storageRoot para que apunte a la ruta UNC del almacenamiento persistente del controlador de zonas de almacenamiento. Por ejemplo: $storageRoot = "\\10.10.10.10\StorageLocation\persistentstorage"

Para probar el proceso de recuperación

1. Crea un archivo de prueba y súbelo a ShareFile.
2. Transcurrida aproximadamente una hora, compruebe que el archivo aparezca en el almacenamiento persistente (en la ruta especificada para $backupRoot).
3. Eliminar el archivo de ShareFile: en la herramienta de administración de ShareFile, haga clic en la **papelera de reciclaje**, seleccione el archivo y, a continuación, haga clic en **Eliminar permanentemente**.
4. Elimine el archivo del almacenamiento persistente.

   Este paso vuelve a crear la acción que ShareFile realizaría 45 días después de eliminar el archivo.

5. En la herramienta de administración de ShareFile, vaya a **Administración > Zonas de almacenamiento**, haga clic en la zona y, a continuación, en **Recuperar archivos**.
6. Haga clic en el cuadro de texto **Fecha de recuperación** y seleccione la fecha y la hora antes de eliminar el archivo y después de subirlo.

   Aparecerá la lista de archivos de la zona de almacenamiento en la fecha y hora especificadas.

7. Seleccione la casilla de verificación del archivo.
8. Seleccione la carpeta que contenga los archivos restaurados y, a continuación, haga clic en **Restaurar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El archivo se agrega a la cola de recuperación y está listo para restaurarse. Cuando el archivo se recupera correctamente, la pantalla cambia para mostrar la carpeta que ahora contiene el archivo recuperado.

9. Para recuperar el archivo:

   a. Abra una ventana del símbolo del sistema como administrador.

   b. Navegue hasta la ubicación de PsExec.exe y, a continuación, escriba:

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

   c. En la ventana de PowerShell, vaya a:

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

   d. Ejecute el script de recuperación:

   `.\DoRecovery.ps1`

   La ventana de PowerShell incluirá el mensaje "Elemento recuperado". El archivo se agrega a la ubicación de almacenamiento persistente.

10. Descargue el archivo restaurado del sitio web de ShareFile.

Comandos de PowerShell relacionados

Los siguientes comandos de PowerShell admiten la recuperación ante desastres.

- **Get-RecoveryPendingFileIDs**

  Obtiene la lista de identificadores de archivos necesarios para la recuperación. Para la sintaxis y los parámetros, utilice este comando:

  Get-Help Get-RecoveryPendingFileIDs -full

- **Set-RecoveryQueueItemsStatus**

  Establece el estado de todos los elementos de la cola de recuperación o de los especificados. Esto sobrescribe el estado de recuperación existente en la cola. Para la sintaxis y los parámetros, utilice este comando:

  Get-Help Set-RecoveryQueueItemsStatus -full

Para crear y programar una tarea de recuperación

En caso de que sea necesaria una tarea de recuperación programada, siga los pasos que se indican a continuación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Inicie el Programador de tareas de Windows y, en el panel **Acciones**, haga clic en **Crear tarea**.
2. En la ficha **General**:

   a. Escriba un nombre significativo para la tarea.

   b. En **Opciones de seguridad**, haga clic en **Cambiar usuario o grupo**y especifique el usuario que ejecutará la tarea, ya sea el servicio de red o un usuario nominal que tenga permisos de escritura en la ubicación de almacenamiento.

   c. En el menú **Configurar para**, seleccione el sistema operativo del servidor en el que se ejecutará la tarea.
3. Para crear un disparador, en la ficha **Desencadenadores**, haga clic en **Nuevo**.
4. En **Comenzar la tarea**, elija Según **un cronograma** y, a continuación, especifique una programación.
5. Para crear una acción, en la ficha **Acciones**, haga clic en **Nueva**.

   a. En **Acción**, elija **Iniciar un programa** y especifique la ruta completa al programa. Por ejemplo: `C:\Windows\System32\cmd.exe`.

   b. Para **Agregar argumentos,** escriba: `/c “c:\windows\syswow64\WindowsPowerShell\v1.0\PowerShell.exe -File .\DoRecovery.ps1” >> .\recovery.log 2>>.\recoveryerror.log`

   c. En **Empezar en**, especifique la carpeta Disaster Recovery en la ubicación de instalación del controlador de zonas de almacenamiento. Por ejemplo: `c:\inetpub\wwwroot\Citrix\StorageCenter\Tools\Disaster Recovery`

Eliminar el período predeterminado del servicio

A partir de StorageZone Controller 4.0, el temporizador de eliminación del servicio se configurará en 45 días. El período predeterminado de 45 días sobrescribirá cualquier configuración anterior. Para modificar el período predeterminado, modifique FileDeleteService.exe.config en C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc

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

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

Modificar el período predeterminado del servicio de eliminación después de la actualización

En algunos escenarios de actualización, el valor DeletePeriod se establecerá en nulo en “FileDeleteService.exe.config”. Si se establece en nulo, el período de eliminación se establece de forma predeter-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

minada en 45 días, el número predeterminado de días antes de que un archivo que se haya eliminado de ShareFile se elimine del almacenamiento físico.

Para modificar el DeletePeriod en el controlador de zonas de almacenamiento, modifique el archivo FileDeleteService.exe.config en la siguiente ubicación: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

Tras una instalación limpia del controlador de zonas de almacenamiento, el servicio de eliminación se ejecutará cada 8 horas para limpiar los archivos y carpetas temporales. Para modificar el temporizador, modifique el archivo FileDeleteService.exe.config en la siguiente ubicación: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`

Recuperar archivos y carpetas de su copia de seguridad de ShareFile Data

April 19, 2021

La consola de administrador de ShareFile permite examinar las zonas de almacenamiento en busca de registros de datos de ShareFile para una fecha y hora concretas y etiquetar los archivos y carpetas que desee restaurar. ShareFile agrega los elementos etiquetados a una cola de recuperación. A continuación, puede ejecutar el script proporcionado para restaurar los archivos desde una copia de seguridad a la ubicación de almacenamiento.

> **Importante:**
>
> Asegúrese de utilizar PowerShell 4.0 para este procedimiento. Para obtener más información acerca de los requisitos de PowerShell, consulte los scripts y comandos de PowerShell en
> Requisitos del sistema del controlador de zonas de almacenamiento.

Requisitos previos

- Complete la configuración y las pruebas descritas en Preparar el controlador de zonas de almacenamiento para la recuperación de archivos. El programa de instalación incluye instrucciones para crear una carpeta que contenga los archivos recuperados.

1. En la interfaz web de ShareFile, haga clic en **Administrador** y, a continuación, haga clic en **Zonas de almacenamiento**.
2. Haga clic en el nombre de la zona y haga clic en **Recuperar** archivos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Haga clic en el cuadro de texto **Fecha de recuperación** y seleccione una fecha y una hora.

   Aparecerá la lista de archivos de la zona de almacenamiento en la fecha y hora especificadas.

4. Active la casilla de verificación de cada archivo que quiere restaurar y, a continuación, haga clic en Restaurar.

5. Seleccione la carpeta para contener los archivos restaurados y, a continuación, haga clic en Restaurar.

   La lista de carpetas muestra un icono giratorio para indicar que la recuperación está en proceso.

6. Si la ubicación de copia de seguridad no sigue el mismo diseño que el almacenamiento persistente de la zona de almacenamiento, copie los archivos de la ubicación de copia de seguridad en la ubicación especificada al modificar DoRecovery.ps1.

7. El script de PowerShell DoRecovery.ps1 no está firmado, por lo que es posible que deba cambiar la directiva de ejecución de PowerShell para este procedimiento.

   a) Determine si la directiva de ejecución de PowerShell le permite ejecutar scripts locales sin firmar. En una ventana de PowerShell: `Get-ExecutionPolicy`

      Por ejemplo, una directiva de RemoteSigned, Sin restricciones o Bypass permite ejecutar scripts sin firmar.

   b) Para cambiar la directiva de ejecución de PowerShell: `Set-ExecutionPolicy RemoteSigned`

8. Establezca el contexto de usuario para esta sesión de PowerShell. En una ventana de comandos, ejecute uno de los siguientes comandos.

   - Si utiliza la cuenta predeterminada de servicio de red:

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

   - Si utiliza un usuario con nombre para el grupo de aplicaciones del controlador de zonas de almacenamiento:

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

   Se abre una ventana de PowerShell.

9. Recuperar el archivo:

   a) Abra una ventana del símbolo del sistema como administrador.

   b) Vaya a la ubicación de PsExec.exe e introduzca:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

c) En la ventana de PowerShell, vaya a:

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

d) Ejecute el script de recuperación:

`.\DoRecovery.ps1`

La ventana de PowerShell incluirá el mensaje "Elemento recuperado". Los archivos recuperados se copian de la copia de seguridad a la ubicación de almacenamiento persistente. Después de actualizar la consola, los iconos giratorios desaparecen de la interfaz web ShareFile para los archivos recuperados correctamente.

Si un archivo que se elimina de la aplicación web ShareFile aún no ha sido eliminado por el servicio de eliminación del controlador de zonas de almacenamiento, el archivo sigue estando en la ubicación de almacenamiento persistente. En ese caso, la recuperación de archivos es inmediata y un icono giratorio no aparece en la interfaz web ShareFile.

Si no puede recuperar un archivo, consulte el archivo de ayuda proporcionado en la carpeta Recuperación ante desastres.

Reconciliar la nube de ShareFile con una zona de almacenamiento

October 13, 2020

Un problema, como un error de disco, que provoca la pérdida de datos en el almacenamiento local da como resultado un estado incoherente entre el almacenamiento local y los metadatos almacenados en la nube ShareFile. Puede conciliar automáticamente esas diferencias para que los metadatos de los archivos que ya no se encuentren en la zona de almacenamiento en una fecha y hora especificadas se eliminen permanentemente de la nube de ShareFile.

> **Precaución:**
>
> Realice una conciliación solo si tiene una pérdida de datos irrecuperable en el almacenamiento de archivos local. Una conciliación borra permanentemente los metadatos de la nube ShareFile para cualquier archivo que no se encuentre en el almacenamiento de archivos local a partir de la fecha y hora que especifique.

1. Haga clic en **Administrador** y, a continuación, en **Zonas de almacenamiento**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Haga clic en el nombre de la zona y, a continuación, en **Reconciliar archivos**.
3. Haga clic en el cuadro de texto **Reconciliar fecha** y seleccione una fecha y una hora.
4. Haga clic en **Reconciliar**. Aparecerá un cuadro de diálogo de confirmación.

Guía de migración a Windows Server 2012R2 para zonas de almacenamiento de ShareFile

November 16, 2023

> **Importante:**
>
> Microsoft finalizará el soporte para Windows Server 2012R2 el 10 de octubre de 2023. Es importante migrar el servidor a una versión más reciente antes de la fecha de finalización del soporte.

Este artículo proporciona instrucciones sobre cómo migrar el servidor ShareFile Storage Zone de Windows Server 2012R2 a una versión más reciente.

Para migrar a una versión más reciente de Windows Server, debe agregar un controlador de zona de almacenamiento secundario al nuevo servidor y, a continuación, promocionarlo como controlador principal.

Requisitos del sistema

El servidor Storage Zones Controller admite las siguientes versiones:

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

Instrucciones

> **Nota:**
>
> Los siguientes pasos **NO** cubren la migración del repositorio de datos de ShareFile. Si tiene el repositorio de datos de ShareFile en el mismo servidor que el controlador de zona de almacenamiento que planea migrar o tiene un repositorio de datos de zona de almacenamiento en un servidor de archivos que ejecuta Windows Server 2012R2 para migrar, consulte Transferir archivos a un nuevo recurso compartido de red para obtener más información.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paso 1: Preparar el nuevo servidor para el ShareFile Storage Zone Controller

Prepare el nuevo servidor siguiendo los pasos que se indican en Preparar el servidor para los datos de ShareFile.

Paso 2: Instale el Storage Zone Controller en el nuevo servidor y agréguelo como secundario

Tras preparar el nuevo servidor para ShareFile, debe agregarlo a la zona de almacenamiento como servidor secundario. Consulte Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento para obtener más información.

Paso 3: Promover el nuevo servidor a Primario, degradar el antiguo servidor a Secundario

Tras agregar el nuevo servidor como secundario, el siguiente paso es promocionarlo a principal. El servidor anterior también debe degradarse a secundario. Para obtener más información sobre este paso, consulte Cómo degradar y promover los controladores de zonas de almacenamiento.

> **Nota:**
>
> ShareFile recomienda probar la funcionalidad del nuevo servidor de zona de almacenamiento por sí solo, sin utilizar el servidor anterior como secundario. Puede hacerlo inhabilitando temporalmente el servidor anterior. Para obtener más información, consulte Para inhabilitar un controlador de zona de almacenamiento

Paso 4 (opcional): Agregar servidores secundarios adicionales

Si es necesario, para cada servidor secundario adicional, vuelva al paso 2: Instalar el Storage Zone Controller en el nuevo servidor y agréguelo como secundario.

Paso 5 (opcional): Actualizar los miembros del grupo de servicio de NetScaler

Si tiene un NetScaler, asegúrese de que los nuevos servidores de zonas de almacenamiento se agreguen al grupo de servicios de ShareFile. Consulte Para agregar miembros a un grupo de servicios mediante la utilidad de configuración para obtener más información.

Paso 6: Eliminar el antiguo servidor Storage Zone Controller del portal de administración de ShareFile

Una vez que los servidores de Storage Zone se hayan migrado correctamente, los servidores más antiguos se pueden eliminar del portal de administración de ShareFile. Consulte Para eliminar un con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

trolador de zonas de almacenamiento para obtener más información.

Configurar análisis antivirus de archivos cargados

June 29, 2022

> **Importante:**
>
> Debido a las actualizaciones del código de la aplicación en StorageZones 4.2, algunos clientes deben actualizar el nivel de permisos en el que se ejecuta la herramienta desde el administrador local hasta el servicio de red del sistema. Si no se actualizan los permisos, los análisis antivirus no se iniciarán.

Requisitos/Resumen

- Usuario que utiliza StorageZones Controller 4.2 o posterior
- SFAntivirus debe ejecutarse como un servicio de red mediante PsExec
- Actualizar ubicación del archivo de registro

Ejecute SFAntivirus como un servicio de red con PsExec:

Los clientes que actualicen a SZ 4.2 o posterior con tareas programadas existentes que se vinculen a SFAntiVirus deben cambiar el nivel de usuario en el que se ejecuta la herramienta de administrador local al servicio de red del sistema.

Para obtener los derechos de servicio de red, use PsExec para iniciar PowerShell (x86) en el mismo contexto de usuario que el controlador de zonas de almacenamiento y obtenga los derechos de servicio de red mediante el siguiente comando:

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

Actualizar ubicación del archivo de registro

Los administradores también deben cambiar la ubicación del archivo de registro modificando la entrada log4net.config, si estaban iniciando sesión en un directorio fuera del directorio de registro SZC predeterminado, modificando la siguiente línea:

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

La instalación del controlador de zonas de almacenamiento incluye varios archivos que admiten análisis antivirus. Los archivos se instalan de forma predeterminada en C:\inetpub\wwwroot\Citrix\StorageCenter\Tools

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de personalizar el archivo de configuración y usar el Programador de tareas de Windows para programar los análisis, como se describe en los siguientes pasos, cada solicitud de carga de archivos hace que el controlador de zonas de almacenamiento ponga el archivo en cola para un análisis antivirus. Si se notifican problemas para un archivo analizado, la vista Carpetas incluye un icono de advertencia para el archivo. Si un usuario intenta descargar el archivo, aparece un mensaje de advertencia.

A partir de StorageZones Controller 4.0, se puede configurar la ubicación del archivo de registro del antivirus. Para modificar la ubicación del registro, modifique el archivo SFAntivirus.exe.config en C:\inetpub\wwwroot\Citrix\StorageCenter\tools\SFAntiVirus.

El análisis antivirus no elimina el archivo.

StorageZones Controller 4.2 o posterior admite el uso del protocolo ICAP con plataformas de análisis antivirus codificadas según el estándar RFC para ICAP. La información sobre la configuración de un AV ICAP se encuentra más adelante en este artículo.

> **Nota:**
>
> Después de configurar el antivirus en su zona, se analizarán todos los elementos recién subidos. La configuración del antivirus no es retroactiva. Al configurarlo, no se analizan los archivos y elementos que ya existen en la zona.

Para preparar la configuración de su ubicación

1. Para ejecutar análisis de virus en un servidor que no sea el controlador de zonas de almacenamiento:

   a) Copie la carpeta C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus en el otro servidor.

   b) En el controlador de zonas de almacenamiento, abra C:\inetpub\wwwroot\Citrix\StorageCenter\AppSe y establezca QueueSDKRestricted en 0: `<add key="QueueSDKRestricted"value="0"/>`

2. En el servidor en el que ejecuta los análisis de virus, modifique SFAntivirus.exe.config con los valores de la configuración del controlador de zonas de almacenamiento:

   a) Para CommandFile: especifique la ruta completa al software antivirus. El software debe residir en el mismo servidor que la carpeta antivirus ShareFile.

   b) Para CommandOptions y códigos de devolución: la configuración de la línea de comandos proporcionada en el archivo de configuración es un ejemplo. Proporcione la configuración adecuada para el software y el entorno antivirus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c) Para ScanFileTimeout: los archivos más grandes pueden tardar más en analizarse. Ajuste este parámetro de acuerdo con el tamaño de archivo que espera tener en su almacenamiento. **De lo contrario, esto podría aumentar el riesgo de que no se analice un archivo grande.**

3. En una ventana de línea de comandos, ejecute el siguiente comando para configurar los análisis de virus: `SFAntiVirus.exe -register SFusername SFpassword`

Usar ICAP para escaneos AV en lugar de herramientas de línea de comandos

El controlador de zonas de almacenamiento 5.3 y posteriores admiten el uso del protocolo ICAP con plataformas de análisis antivirus que se han codificado según el estándar RFC para ICAP. Los clientes pueden seguir utilizando el método CLI si lo desean. Esta función es compatible con las zonas de arrendatarios a partir de Storage Zones Controller 5.0.1 y posteriores.

Para habilitar un escáner AV ICAP en el controlador de zona de almacenamiento, vaya a la página de configuración del controlador de zonas de almacenamiento.

Seleccione la casilla **Habilitar integración antivirus** e introduzca la dirección de su servidor de antivirus en el campo **URL de ICAP RESPMOD**. Esta es la URL del servicio de modificación de respuestas ICAP: `ICAP://SERVER/RESPMOD`.

Haga clic en **Probar conectividad** para confirmar la configuración.

Para crear y programar una tarea de análisis de virus

> **Nota:**
>
> La creación de tareas programadas para análisis de virus solo es necesaria cuando se utilizan herramientas de línea de comandos. Esto no es necesario cuando se utiliza ICAP.

1. Inicie el Programador de tareas de Windows y, en el panel **Acciones**, haga clic en **Crear tarea**.
2. En la ficha **General** :

   a) Proporcione un nombre descriptivo para la tarea.

   b) En Opciones **de seguridad**, haga clic en **Cambiar usuario o grupo**y especifique un usuario de Windows para ejecutar la tarea. El usuario debe tener permiso de acceso total en la ubicación de almacenamiento.

   c) Seleccione **Ejecutar tanto si el usuario ha iniciado sesión como si no**. Deje desmarcada la casilla **No almacenar contraseña**.

   d) Selecciona **Ejecutar con los privilegios más altos**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

   e) En el **menú Configurar para**, seleccione el sistema operativo del servidor en el que se ejecutará la tarea.

3. Para crear un disparador: en la ficha **Desencadenantes**, haga clic en **Nuevo**. A continuación, para **Comenzar la tarea**, elija **Según una programación** y especifique una programación.
4. Para crear una acción: en la ficha **Acciones**, haga clic en **Nueva**.

   a) En **Acción**, elija **Iniciar** un programa y especifique la ruta completa al programa. Por ejemplo:

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

   b) Para Iniciar en, especifique la ubicación de SFAntiVirus.exe: `C:\\inetpub\\wwwroot\\Citrix\\StorageCenter\\Tools\\SFAntiVirus`

5. En la ficha **Configuración**, en **Si la tarea ya se está ejecutando**, se aplica la siguiente regla, elija **No iniciar una nueva instancia**.

Integración de línea de comandos AV en Scan Service

Requisitos previos

- Antes de instalar o actualizar el controlador de zonas de almacenamiento 5.2, asegúrese de detener o eliminar el AV de línea de comandos existente si se ejecuta como una tarea programada o como un cron.
- Instale .NET 4.6.2 (o posterior) en un equipo host.

El servicio de escaneo en el controlador de zonas de almacenamiento local incluye soporte para usar una herramienta AV de línea de comandos, como AV Scan de línea de comandos de Symantec. Además, el servicio de análisis proporciona análisis con productos antivirus compatibles con ICAP.

Para habilitar esta función, agregue esta clave y el valor de configuración en AntiVirus/OnPrem/AVScanService/AVScanService/appSettings.config

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

Configuración específica de la herramienta de línea de comandos

La actualización o la nueva instalación de Storage Zones Controller 5.2 incluye un nuevo archivo de configuración:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Este archivo gestiona los ajustes necesarios para la línea de comandos AV.

Los valores de clave de configuración se explican a continuación con valores de ejemplo incluidos.

- Establezca este punto en la aplicación de línea de comandos.

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

- Consulte la documentación de la aplicación de línea de comandos para ver qué opciones o conmutadores admite y, a continuación, agréguelos en esta ubicación.

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

- Incluya los valores de salida que indican un escaneo limpio.

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

- Incluye valores de salida que indiquen el archivo infectado.

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

- Incluya valores de salida que indiquen archivos no analizados.

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

Notas sobre la aplicación del tamaño máximo de archivo, excluidas las extensiones

Antes de la versión 5.2, no se podía imponer la exclusión de extensiones ni la aplicación del tamaño máximo de archivo en el AV de línea de comandos. Solo podía hacerlo en el servicio ICAP Scan. Con la versión 5.2, los mismos ajustes que se aplicaban al servicio de análisis ICAP con respecto a las extensiones excluidas y el tamaño máximo de archivo en bytes se aplican al servicio de línea de comandos AV.

Estos parámetros se denominaron como:

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

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

Una nueva instalación de Storage Zones Controller 5.2 cambia el nombre de estos ajustes por el siguiente. Los ajustes renombrados reflejan el hecho de que son aplicables tanto al AV basado en ICAP como al AV de línea de comandos.

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

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

En una actualización, no se cambia el nombre de estos parámetros. Aunque los cambios de nombre manuales funcionan, los mismos ajustes también funcionarían para la línea de comandos AV además de ICAP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Migrar datos de ShareFile

August 4, 2023

Hay varias formas de migrar datos de ShareFile de una zona local a otra.

- Migrar mediante Portal web o User Management Tool
- Migrar mediante PowerShell Script
- Migrar mediante la herramienta ZoneFix

Requisitos previos

- Asegúrese de que se pueda acceder a la zona de origen desde la zona de destino y desbloquee las conexiones salientes al Centro de almacenamiento de origen.
- Para probar la conexión entre zonas, acceda a la dirección externa de la zona de origen navegando hasta ella en un explorador en la zona de destino. Si la conexión se realiza correctamente, aparece el logotipo de ShareFile.

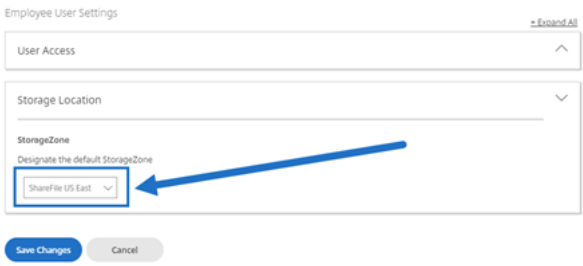
Migrar mediante Portal web o User Management Tool

En la aplicación web ShareFile, puede iniciar la migración de datos entre zonas para un usuario individual o para una carpeta específica.

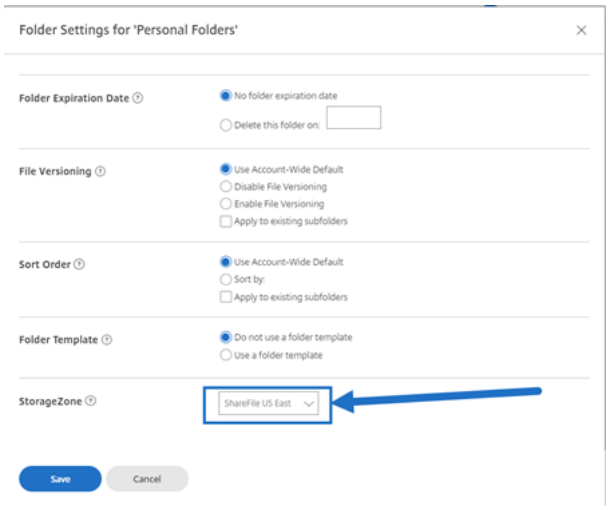
> **Importante:**
>
> Al guardar los siguientes cambios, se desencadena inmediatamente una operación de migración asíncrona para cargar los archivos existentes en la nueva zona. Los archivos nuevos cargados en la carpeta durante este período de migración pasan a la nueva zona.

Migrar datos para un usuario específico: Vaya a **Personas** y, a continuación, localice el usuario **empleado**. Haga clic en el usuario para ver su página de perfil. En **Ubicación de almacenamiento**, seleccione una nueva zona (si ya se ha instalado y configurado una).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Migrar datos para una carpeta específica: Vaya hasta la carpeta y acceda al menú **Más opciones** a la derecha del nombre de la carpeta. Haga clic en **Configuración avanzada de carpetas**. En el menú, seleccione una nueva zona.

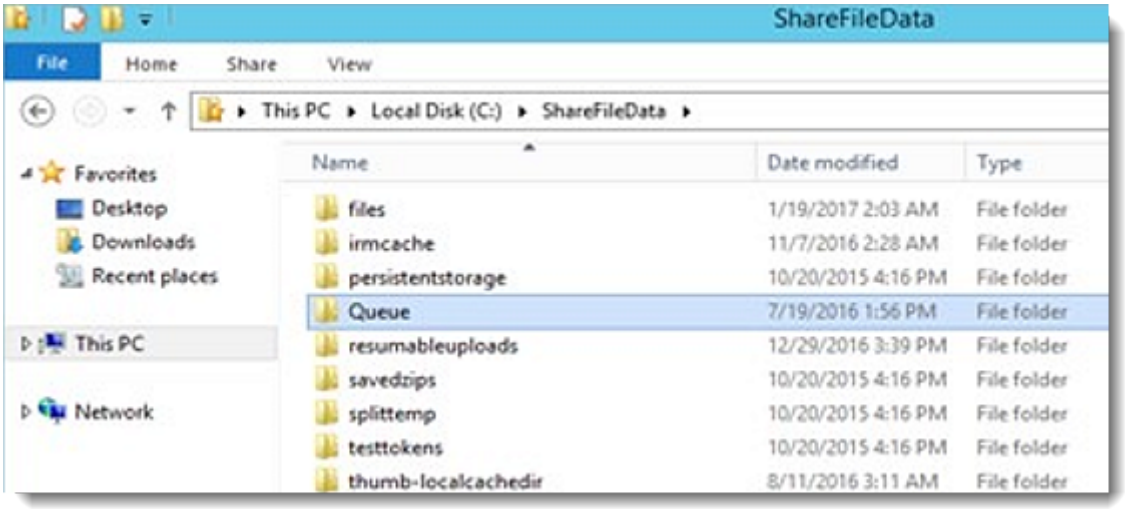


Proceso de migración

En primer lugar, los archivos en cola para la migración crean un archivo de marcador de posición en una carpeta de **cola** dentro de la **ubicación de almacenamiento** de la zona original.

Una vez que el archivo marcador de posición se procesa correctamente, el archivo migrado se elimina en el `persistentstorage` de la zona original y se agrega al `persistentstorage` de la nueva zona.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Migrar a través de PowerShell

El SDK de PowerShell de ShareFile permite a los usuarios descargar estructuras de carpetas grandes desde su ubicación de zona original y cargar esas carpetas en una nueva zona.

Requisitos: Se requieren PowerShell 4+ y .NET 4.x+ para ejecutar e instalar el SDK. PowerShell 5.x se puede descargar aquí como parte de Windows Management Framework 5.1.

Migrar mediante la herramienta Zone Fix

La herramienta Zone Fix es una herramienta de línea de comandos. Escrita por desarrolladores de zonas de almacenamiento, la herramienta aprovecha la API de ShareFile para apuntar a los ID de carpeta para la migración a una zona específica.

Para un rendimiento óptimo, se recomienda este método para carpetas de menos de 2 GB de tamaño.

Favoritos del conector

February 9, 2022

A partir del controlador de zonas de almacenamiento 5.0, los usuarios pueden convertir las carpetas de conectores en Favoritos en **Network Shares**, **SharePoint**y **Documentum Connectors** dentro de ShareFile WebApp. Para obtener más información, consulte este artículo de Citrix Support KnowledgeCenter.

ShareFile Mobile admite la adición de una carpeta de conectores a sus favoritos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Administrar zonas de almacenamiento para datos de ShareFile

November 16, 2023

Puede usar zonas de almacenamiento para ShareFile Data con o en lugar de la nube administrada por ShareFile.

> **Nota:**
>
> Si va a eliminar un controlador de zona de almacenamiento principal, vuelva a un estado anterior antes de continuar. Para obtener más información, consulte Demostración y promoción de controladores de zonas de almacenamiento.

Mover carpetas de inicio y File Boxes entre zonas

Siga los siguientes pasos para mover las carpetas de inicio y los cuadros de archivos entre zonas. También puede utilizar la ShareFile User Management Tool para migrar usuarios entre zonas.

1. Haga clic en **Inicio** y, a continuación, vaya a la carpeta.
2. En el panel de navegación derecho, haga clic en **Modificar opciones de carpeta**.
3. En el menú de zona de almacenamiento, seleccione una zona y, a continuación, haga clic en **Guardar**.

Crear una carpeta en una zona de almacenamiento

1. Haga clic en **Inicio** y luego en **Carpetas**.
2. En la ficha **Carpeta**, haga clic en **Agregar carpeta**.
3. Especifique la información de la carpeta. En **Storage Site**, seleccione la zona de almacenamiento en la que desea almacenar esta carpeta y su contenido.
4. Haga clic en **Crear carpeta**.
5. Configure la carpeta como de costumbre. Al crear una carpeta, puede elegir si quiere usar el almacenamiento en la nube administrado por ShareFile o su zona de almacenamiento local.

Cambiar el nombre o eliminar una zona de almacenamiento

> **Importante:**
>
> Antes de eliminar una zona de almacenamiento, haga una copia de seguridad. Al eliminar una zona, se borran todos los archivos y carpetas de esa zona y no se puede deshacer la operación.

1. Haga clic en **Administrador** y, a continuación, en **Zonas de almacenamiento**
2. Pulse en el nombre de la zona.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para cambiar el nombre de la zona: haga clic en **Modificar zona**, escriba un nombre nuevo y, a continuación, haga clic en **Guardar cambios**.
- Para eliminar la zona: Haga clic en el nombre de la zona y, a continuación, en **Eliminar zona**.

Limitaciones

No se puede cambiar el nombre ni eliminar los controladores de zona de almacenamiento si:

- **La migración de datos de ShareFile está en curso**: Complete la migración de datos antes de intentar eliminar la zona de almacenamiento.
- **Los datos de ShareFile existen en la zona**: Migre o elimine todos los datos existentes antes de intentar eliminar la zona de almacenamiento.

Personalizar operaciones de caché de almacenamiento

Las solicitudes de los usuarios de ShareFile se administran con el controlador de zonas de almacenamiento. Esto incluye: cargas, descargas y eliminaciones de archivos. El controlador de zonas de almacenamiento se comunica entonces con el almacenamiento conectado. Por ejemplo, si el almacenamiento conectado es un sistema de almacenamiento de terceros compatible y un usuario de ShareFile carga un archivo, el cliente de ShareFile envía el archivo a la memoria caché de almacenamiento persistente. El controlador de zonas de almacenamiento carga el archivo en el sistema de almacenamiento de terceros.

El controlador de zonas de almacenamiento administra la memoria caché de almacenamiento persistente mediante ajustes configurables en `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe.config`. En este análisis se indican las configuraciones específicas de un sistema de almacenamiento de terceros compatible.

Para los archivos cargados:

- El controlador de zonas de almacenamiento coloca los archivos cargados en una memoria caché de almacenamiento persistente (la carpeta PersistentStorage).
- La siguiente configuración controla el tiempo de las operaciones de eliminación del servicio:
  - `MinDeletionAge` especifica el intervalo de tiempo mínimo entre la última vez que se accedió a un archivo y el momento en que se puede eliminar. El valor predeterminado es de 1 día. La configuración mínima es de 8 horas.
  - `OffPeakTimeOfDayStart` y `OffPeakTimeOfDayEnd` especifican las horas de inicio y finalización de la eliminación de archivos. Los valores predeterminados son las 2 a. m. y las 4 a. m.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - `ProducerTimerInterval` y `DeleteTimerInterval` controlan la frecuencia de las operaciones del servicio de eliminación. Contacte con la asistencia si los valores predeterminados (1 día) no son apropiados para su sitio.

- Los servicios de eliminación también administran carpetas que contienen elementos temporales, como claves de cifrado y archivos en cola. El servicio de eliminación elimina esos elementos 24 horas después de su creación.
- Solo para sistemas de almacenamiento de terceros compatibles:
  - El servicio de eliminación determina si un archivo en la memoria caché de almacenamiento tiene un blob correspondiente en el almacenamiento de terceros compatible.
  - De forma predeterminada, cada 10 segundos (`CheckSizeThreasholdTimer`), el servicio de eliminación determina si la memoria caché de almacenamiento ha superado el umbral de disco de 10 GB (`DiskSpaceDropoutThresholdGB`). Si se supera el umbral, el servicio de eliminación elimina los archivos a los que no se haya accedido en la última hora (`CacheCleanupFileThreasholdPeriodUnExpected`). El servicio de eliminación se ejecuta como resultado de una programación normal (y no porque el tamaño del disco haya alcanzado el umbral). El servicio elimina los archivos a los que no se haya accedido en las últimas 24 horas (`CacheCleanupFileThresholdPeriodNormal`) si el blob se encuentra en un almacenamiento de terceros compatible. Si el blob no está en el almacenamiento de terceros, el archivo permanece en la memoria caché de almacenamiento.

Para los archivos descargados:

- Cuando el controlador de zonas de almacenamiento recibe una solicitud de descarga, descarga el archivo de la memoria caché de almacenamiento persistente si el archivo está ahí. Si el archivo no está en esa memoria caché, el controlador descarga el archivo desde el sistema de almacenamiento de terceros a la memoria caché de almacenamiento persistente. El servicio de eliminación elimina los archivos a los que no se ha accedido en las últimas 24 horas (CacheCleanupFileThresholdPeriodNormal).

Para los archivos eliminados:

- El servicio de eliminación obtiene de la aplicación ShareFile una lista de archivos que se eliminaron hace 45 días (período).
- El servicio de eliminación elimina los archivos correspondientes de la ubicación de almacenamiento o los objetos correspondientes del almacenamiento de terceros.

Eliminar período predeterminado del servicio

El temporizador de eliminación de servicio está configurado en 45 días. El período predeterminado de 45 días sobrescribe cualquier configuración anterior.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si el período de eliminación está configurado en menos de 45 días, ponte en contacto con el servicio de asistencia para reducir el número de días que se muestran los artículos en la **papelera de reciclaje** para que ambos períodos sean iguales.

1. Para modificar el período predeterminado, modifique FileDeleteService.exe.config en `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`
   - `<!--No. of days to keep data blob in active storage after deletion-->`
   - `<add key="Period"value="45"/>`

Crear y administrar conectores de zonas de almacenamiento

April 19, 2021

Los StorageZone Connectors proporcionan acceso a documentos y carpetas en:

- Sitios, colecciones de sitios y bibliotecas de documentos de SharePoint
- Recursos compartidos de red
- Conector de Documentum (requiere SZC 4.1 o posterior)

Los usuarios con permiso para ver un recurso conectado pueden examinar sitios de SharePoint conectados, bibliotecas de SharePoint y recursos compartidos de archivos de red desde la interfaz web de ShareFile y clientes ShareFile.

De forma predeterminada, la exploración de conectores está inhabilitada para la interfaz web de ShareFile. Para habilitar la exploración del conector, póngase en contacto con el soporte de ShareFile

Hay opciones adicionales disponibles que permiten a los usuarios especificar qué Controller de dominio utilizar para las búsquedas de Active Directory. Consulte la sección Autenticación de este artículo. Esta configuración requiere SZ 4.1 o posterior.

Requisitos del sistema de conectores

Los conectores de zona de almacenamiento no admiten el uso compartido de documentos ni la sincronización de carpetas entre dispositivos.

Los conectores deben tener un nombre para mostrar único. Se bloquea a los usuarios el uso de un nombre de conector que está en uso en otro lugar de la cuenta.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Permisos para crear StorageZone Connectors

Para crear y administrar conectores, el usuario Administrador o Empleado **debe tener los siguientes permisos**:

- **Crear y administrar conectores**
- **Crear carpetas en el nivel raíz**

Para crear un conector de zonas de almacenamiento para SharePoint

Requisitos previos

- Si utiliza zonas de almacenamiento para datos de ShareFile, cree la zona que se utilizará para el conector.

En los siguientes pasos se describe cómo crear un conector de zonas de almacenamiento desde la interfaz web ShareFile. Los usuarios de ShareFile también pueden crear un conector a partir de dispositivos compatibles escribiendo la dirección URL del sitio de SharePoint.

1. Inicie sesión en su cuenta de ShareFile como administrador con el permiso Crear y administrar conectores.
2. Vaya a **Configuración del administrador > Conectores**.
3. Haga clic en **Agregar** para el tipo de conector de SharePoint.
4. Si utiliza zonas de almacenamiento para los datos de ShareFile, elija una zona para el conector.

   La zona de un conector debe estar en el mismo dominio que el servidor de SharePoint o debe tener una relación de confianza con él. Si tiene servidores SharePoint en varios dominios y no puede configurar confianzas entre los dominios, cree un controlador de zonas de almacenamiento para cada dominio.
5. En Sitio, especifique la dirección URL de un sitio de nivel raíz de SharePoint, una colección de sitios o una biblioteca de documentos en los siguientes formularios.

   - Ejemplo de conexión a un sitio de nivel raíz de SharePoint: `https://sharepoint.company.com`

     Una conexión a un sitio de nivel raíz proporciona a los usuarios acceso a todos los sitios (pero no a las colecciones de sitios) y a las bibliotecas de documentos bajo el nivel raíz. ShareFile oculta las carpetas del sistema de SharePoint de los usuarios.
   - Ejemplo de conexión a una colección de sitios de SharePoint: `https://sharepoint.company.com/site/SiteCollection`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Una conexión a una colección de sitios proporciona a los usuarios acceso a todos los subsitios de esa colección.

- Ejemplo de conexión a una biblioteca de documentos de SharePoint 2010:
  - `https://mycompany.com/sharepoint/`
  - `https://mycompany.com/sharepoint/sales-team/Shared Documents/`
  - `https://mycompany.com/sharepoint/sales-team/Shared Documents/Forms/AllItems.aspx`
- Ejemplo de conexión a una biblioteca de documentos de SharePoint 2013:

  La dirección URL predeterminada de SharePoint 2013 (cuando la estrategia de descarga mínima está habilitada) tiene el siguiente formato: `https://sharepoint.company.com/\\_layouts/15/start.aspx\\#/Shared%20Documents/`.
- Ejemplo de conexión que redirige al nombre NetBIOS de un usuario autenticado:

  Utilice la variable %UserDomain% para sustituir el nombre de inicio de sesión del usuario autenticado por el nombre NetBIOS de ese usuario. La nueva variable le permite crear un conector de nivel de sitio a una dirección URL como `https://example.com/%UserDomain%\\_%UserName%/Documents`.
- Ejemplo de conexión al conectarse a "Mi sitio"o OneDrive para la Empresa:

  Utilice la variable %`URLusername`% para resolver automáticamente los caracteres especiales seleccionados al conectarse a sitios personales de SharePoint. Esta variable reemplaza espacios con %20 y puntos con guiones bajos. El uso de la %`URLusername`% variable requiere SZ v3.4.1.

  Si el "dominio\ nombre de usuario"del usuario es "acme\ rip.van winkle", entonces

  `https://sharepoint.acme.com/personal/%URLusername%`
  se resolverá para:
  `https://sharepoint.acme.com/personal/rip van%20winkle`

6. Escriba un nombre fácil de usar para el conector.

   El nombre se utiliza para identificar el sitio de SharePoint a los usuarios. El nombre debe ser breve para que se muestre bien en dispositivos móviles con pantallas pequeñas.

7. Haga clic en **Agregar conector**. Aparecerá el cuadro de diálogo **Ver/Modificar acceso a carpetas**.

8. Para que los conectores sean visibles para otros usuarios: En Ver/Modificar acceso a carpetas, agregue usuarios y grupos de distribución y, a continuación, haga clic en **Guardar cambios**.

   Este paso solo determina si un conector es visible para los usuarios. **Los StorageZone Connectors heredan permisos de acceso del servidor de SharePoint.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para habilitar el etiquetado de metadatos de SharePoint

Al configurar el controlador de zonas de almacenamiento, asegúrese de que los conectores de SharePoint están habilitados.

El etiquetado de metadatos es compatible con SharePoint 2013 y clientes móviles posteriores.

> **Nota:**
>
> `en-us` Sólo para.

Para crear un conector de zonas de almacenamiento para recursos compartidos de archivos de red

Requisitos previos

- Si utiliza zonas de almacenamiento para datos de ShareFile, cree la zona que se utilizará para el conector.
- Para que los conectores de recursos compartidos de red funcionen con las versiones más recientes de los navegadores Chrome, Edge y Firefox, aplique la última actualización.NET para su entorno. Para obtener más información, consulte Artículos de KB que admiten SameSite en .NET Framework. Aplique esto a todos los conectores de zona de almacenamiento. Esto es necesario para permitir que el atributo SameSite se establezca para las cookies teniendo en cuenta la última versión de los navegadores.
- Si utiliza la versión 5.10.1 o inferior, agregue `<httpCookies sameSite="None" requireSSL="true"/` dentro de la `<system.web>` etiqueta del archivo C:\inetpub\wwwroot\Citrix\Sto en todos los conectores de zona de almacenamiento. Esto es necesario para permitir que el atributo SameSite se establezca para las cookies teniendo en cuenta la última versión de los navegadores.

En los siguientes pasos se describe cómo crear un conector desde la interfaz Web ShareFile. Los usuarios de ShareFile también pueden crear un conector a partir de dispositivos compatibles escribiendo la ruta de acceso de un recurso compartido de archivos.

1. Inicie sesión en su cuenta de ShareFile como administrador con el permiso Crear y administrar conectores.
2. Vaya a **Configuración de administrador > Conectores**.
3. Haga clic en **Agregar** para el tipo de conector de recursos compartidos de red.
4. Si utiliza zonas de almacenamiento para los datos de ShareFile, elija una zona para el conector.

   La zona de un conector debe estar en el mismo dominio que el recurso compartido de archivos o debe tener una relación de confianza con él. Si tiene recursos compartidos de archivos en

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

varios dominios y no puede configurar confianzas entre los dominios, cree un controlador de zonas de almacenamiento para cada dominio.

5. En Ruta de acceso, escriba la ruta de acceso UNC.

   Ejemplo con FQDN: \\fileserver.acme.com\shared

   Puede utilizar las siguientes variables en la ruta de acceso UNC:

   - %UserName%

     Redirige al directorio principal de un usuario. Ruta de acceso de ejemplo: \\myserver\homedirs\%UserName%

   - %HomeDrive%

     Redirige a la ruta de acceso a la carpeta principal de un usuario, tal y como se define en la propiedad de Active Directory Home-Directory. Ruta de acceso de ejemplo: %HomeDrive%

   - %TSHomeDrive%

     Redirige al directorio principal de Servicios de Terminal Server de un usuario, como se define en la propiedad de Active Directory MS-TS-Home-Directory. La ubicación se utiliza cuando un usuario inicia sesión en Windows desde un servidor Terminal Server o un servidor Citrix XenApp. Ruta de acceso de ejemplo: %TSHomeDrive%

     En el complemento Usuarios y equipos de Active Directory, se puede acceder al valor de MS-TS-Home-Directory en la ficha Perfil de Servicios de Escritorio remoto al modificar un objeto de usuario.

   - %UserDomain%

     Redirige al nombre de dominio NetBIOS del usuario autenticado. Por ejemplo, si el nombre de inicio de sesión de usuario autenticado es “abc\johnd”, la variable se sustituye por “abc”. Ruta de acceso de ejemplo: \\myserver\%UserDomain%_%UserName%

   Las variables no distinguen mayúsculas y minúsculas

   Importante: No cree un conector a la ubicación de almacenamiento de datos de ShareFile. Dependiendo de los permisos de los usuarios, hacerlo puede permitir que los usuarios eliminen todos los datos de ShareFile.

6. Escriba un nombre fácil de usar para el conector.

   El nombre se utiliza para identificar el recurso compartido de archivos a los usuarios. El nombre debe ser breve para que se muestre bien en dispositivos móviles con pantallas pequeñas.

7. Haga clic en Agregar conector. Aparecerá el cuadro de diálogo Ver/Modificar acceso a carpetas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Para que los conectores sean visibles para otros usuarios: En Ver/Modificar acceso a carpetas, agregue usuarios y grupos de distribución y, a continuación, haga clic en Guardar cambios.

   Este paso solo determina si un conector es visible para los usuarios. **Los StorageZone Connectors heredan permisos de acceso del recurso compartido de red. Los permisos para el acceso de lectura/escritura están determinados por la configuración de seguridad del recurso compartido de red y también se ven afectados por el plan ShareFile.**

Para habilitar el registro y la retirada de archivos para recursos compartidos de archivos de red

Requisitos previos

La versión 5.8 del controlador de zonas de almacenamiento y el conector de recursos compartidos de archivos de red deben estar configurados.

Pasos

1. Inicie sesión en Storage Center. Aparecerá la página de configuración.
2. Haga clic en **Modificar** en la página de configuración.
3. Active la casilla de verificación **Habilitar registro y desproteger para recursos compartidos de archivos de red**.
4. Escriba el nombre del dominio en el que se encuentran los usuarios y los recursos compartidos de red.
5. Escriba el nombre de usuario y la contraseña de la cuenta de servicio. Se requiere que esta cuenta de servicio tenga acceso de lectura y escritura en todos los archivos y carpetas presentes en la ubicación del recurso compartido de red.

Para crear un conector de zonas de almacenamiento de información para Documentum

> **Nota:**
>
> Solo se admite la autenticación básica para la configuración del conector de Documentum. Documentum Content Server distingue entre mayúsculas y minúsculas, por lo que el nombre de usuario introducido durante la autenticación debe coincidir con las credenciales que distinguen entre mayúsculas y minúsculas, a menos que se inhabilite la distinción entre mayúsculas y minúsculas en el servidor de contenido de Documentum.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos previos

1. Controlador de zonas de almacenamiento 5.3 o posterior
2. Configuración de ECM de Documentum habilitada por el soporte al cliente de ShareFile.
3. El servicio Rest de Documentum debe implementarse en el servidor de Documentum. Haga clic aquí para obtener información adicional sobre Documentum Rest Service.
4. Si se utiliza Citrix ADC, se requieren ciertos cambios de configuración. Estos cambios se detallan más adelante en este artículo.

Una vez habilitada esta función por el servicio de atención al cliente de ShareFile, vaya a su controlador de zonas de almacenamiento y busque el menú del conector de zonas de almacenamiento. Haga clic en la casilla de verificación "Habilitar el acceso a los orígenes de datos de Enterprise Content Management (ECM) existentes". Guarde los cambios.

A continuación, inicie sesión en la aplicación web ShareFile y vaya a **Configuración de administración > Conectores.**

Haga clic en el botón **Agregar** junto al tipo de conector de Documentum.

Especifique la ruta de acceso de su servidor EMC e introduzca un nombre para su conector. Continúe.

A continuación, conceda a los usuarios acceso al conector de Documentum.

Una vez creado el conector, puede acceder a él desde las aplicaciones web y móviles.

Acciones admitidas

Móvil (iOS/Android/Plataforma universal de Windows):

- Navegación
- Cargas y descargas de archivos
- Creación/eliminación de archivos y carpetas
- Edición sin conexión

WebApp

- Creación de conectores
- Navegación
- Cargas y descargas de archivos
- Creación/eliminación de carpetas

No se admite

- Compartir archivos almacenados en un conector de Documentum

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Lista blanca/Lista negra de rutas

> **Nota:**
>
> Documentum Content Server distingue entre mayúsculas y minúsculas, por lo que el nombre de usuario introducido durante la autenticación debe coincidir con las credenciales que distinguen entre mayúsculas y minúsculas, a menos que se inhabilite la distinción entre mayúsculas y minúsculas en el servidor de contenido de Documentum.

Configuración de Citrix ADC para el conector de Documentum

Si utiliza un ADC de Citrix con su entorno, realice los siguientes cambios en la configuración de Citrix ADC:

1. Anexa lo siguiente a la directiva _SF_CIFS_SP en Conmutación de contenido > Directivas:

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

2. Agregue lo siguiente a la directiva _SF_SZ_CSPOL en Content Switching > Directivas:

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

Para cambiar el nombre de un conector

Un nombre de conector se utiliza para identificar un sitio de SharePoint o un recurso compartido de archivos de red para los usuarios.

1. Inicie sesión en su cuenta de ShareFile como administrador y, a continuación, haga clic en la ficha conectores.
2. En la columna **Título**, haga clic en el nombre del conector.
3. Escriba un nombre sencillo para el conector y, a continuación, haga clic en **Guardar**.

Para eliminar un conector

Al eliminar un conector no se quitan datos de SharePoint o de un recurso compartido de archivos de red.

1. Inicie sesión en su cuenta de ShareFile como administrador y, a continuación, haga clic en la ficha conectores.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Active la casilla de verificación del conector, haga clic en **Eliminar** y, a continuación, haga clic en **Aceptar**.

Autenticación

Los usuarios administradores ahora pueden utilizar la siguiente configuración para especificar qué Controller de dominio usar al realizar búsquedas de AD para la autenticación CIFS o SP.

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

El "Value="anterior se puede establecer en un único DC o varios DC identificados por nombre de host, FQDN o dirección IP. Varios DC deben estar separados por comas o punto y coma.

Si se especifican varios DC, la búsqueda se ejecutará contra el primer DC. Si se produce un error, se utiliza el segundo DC, y así sucesivamente.

La propiedad anterior se puede agregar a para`C:\inetpub\wwwroot\Citrix\StorageCenter\AppSettingsRelease.config` que sea heredada por todas las aplicaciones IIS del controlador de zonas de almacenamiento (incluidos CIFS, SP y ProxyService).

Si la nueva configuración de la aplicación no está presente, el comportamiento predeterminado de seleccionar automáticamente un DC continúa.

Obtener un vínculo directo desde los conectores de recursos compartidos de red o SharePoint

Los usuarios ahora pueden "Obtener un vínculo directo"desde conectores de recursos compartidos de red y SharePoint mientras utilizan la última versión de la aplicación ShareFile para iOS o Android.

Si el administrador quiere desactivar esta función, puede hacerlo agregando:

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

Lo anterior se puede agregar a `C:\inetpub\wwwroot\Citrix\StorageCenter\sps\AppSettingsRelease.config`.

Autenticación básica y nombres de usuario localizados

La autenticación básica no admite caracteres que no sean ASCII. Si utiliza nombres de usuario localizados, se sugiere que los usuarios utilicen NTLM y Negotiate.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Prevención de pérdida de datos

May 28, 2024

Las funciones de prevención de pérdida de datos (DLP) de ShareFile permiten restringir el acceso y el uso compartido en función del contenido que se encuentra en un archivo.

Puede escanear los documentos cargados en su zona de almacenamiento mediante cualquier paquete de seguridad DLP de terceros que sea compatible con ICAP, un protocolo de red estándar para el escaneo de contenido en línea. A continuación, ajusta los privilegios de acceso y uso compartido en función de los resultados del análisis de DLP y de sus preferencias en cuanto a la rigurosidad con la que quiere controlar el acceso.

Sistemas DLP compatibles

El controlador de zonas de almacenamiento utiliza el protocolo ICAP para interactuar con soluciones DLP de terceros. El uso de ShareFile con una solución de DLP existente no requiere cambios en las directivas o los servidores existentes. Sin embargo, es posible que quiera dedicar servidores ICAP para procesar los datos de ShareFile si espera que la carga sea significativa.

Las soluciones de DLP más populares que cumplen con ICAP incluyen:

- Prevención de pérdida de datos de Symantec
- McAfee DLP Prevent
- Websense TRITON AP-DATA

Como ShareFile usa su suite de seguridad DLP existente, puede mantener un único punto de administración de directivas para la inspección de datos y las alertas de seguridad. Si ya utiliza una de las soluciones anteriores para analizar los archivos adjuntos del correo electrónico saliente o el tráfico web en busca de datos confidenciales, puede dirigir el controlador de zonas de almacenamiento de ShareFile al mismo servidor. Para estos sistemas de DLP existentes, también admitimos el ICAP seguro (ICAPS) si el propio sistema DLP subyacente es compatible con ICAPS.

Habilitar DLP

Para habilitar DLP para ShareFile y el controlador de zonas de almacenamiento, realice las tres acciones siguientes:

1. Habilite las capacidades de DLP en su cuenta de ShareFile.
2. Habilite DLP en el servidor del controlador de zonas de almacenamiento.
3. Configure las acciones permitidas para cada clasificación de archivos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Estas acciones se describen en detalle en las siguientes secciones.

Habilite las capacidades de DLP en su cuenta de ShareFile

Para solicitar o confirmar que el subdominio de ShareFile está habilitado para DLP, envíe una solicitud a Citrix Support.

Para algunas cuentas, habilitar DLP también puede requerir habilitar una experiencia de usuario más reciente para el sitio web de ShareFile. Una vez que su cuenta esté habilitada para DLP, puede continuar con la habilitación de DLP en el servidor del controlador de zonas de almacenamiento.

Habilite DLP en su servidor controlador de zonas de almacenamiento

Siga los siguientes pasos para configurar los ajustes de DLP en la implementación del controlador de zonas de almacenamiento:

1. Instale o actualice el controlador de zonas de almacenamiento 5.3 o posterior.
2. En la consola del controlador de zonas de almacenamiento `http://*localhost*/configservice/login.aspx`, haga clic en la **ficha Datos de ShareFile** . Haga clic en **Modificar** si la zona existe.
3. Seleccione la casilla **Habilitar la integración de DLP** y escriba la dirección ICAP de su servidor de DLP en el campo URL de **ICAP** REQMOD. El formato de la dirección es:

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

OR

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

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

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

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

OR

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

4. Haga clic en **Guardar** o **Registrar**.

Después de habilitar la DLP, confirme que se puede acceder al servidor DLP comprobando la entrada **Estado del servidor ICAP de DLP** en la ficha **Supervisión**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Controle el acceso en función de los resultados del escaneo DLP

Una vez activado el DLP en la cuenta y el controlador de zonas de almacenamiento, se escanearán todas las versiones de todos los archivos que se carguen en la zona de almacenamiento habilitada para DLP en busca de contenido confidencial. Los resultados del análisis se almacenan en la base de datos de ShareFile como una clasificación de datos.

La configuración de DLP restringe los permisos normales y los controles de uso compartido disponibles para los archivos en función de su clasificación de DLP. Al compartir un documento, el usuario puede optar por bloquear el acceso anónimo, incluso si la configuración de DLP le permite compartirlo de forma anónima. Sin embargo, si el usuario intenta compartir un archivo de una manera que infrinja la configuración de DLP, ShareFile le impide hacerlo.

Las clasificaciones de datos son:

- **Escaneado**: Aceptar: Archivos escaneados por un sistema DLP y aprobados como correctos.
- **Escaneado: Rechazado:** Archivos que se escanearon con un sistema DLP y se descubrió que contenían datos confidenciales.
- **Sin escanear**: Archivos que no se han escaneado.

La clasificación **sin escanear** se aplica a todos los documentos almacenados en zonas de almacenamiento gestionadas por Citrix u otras zonas de almacenamiento en las que la DLP no esté habilitada. La clasificación también se aplica a los archivos de las zonas de almacenamiento habilitadas para DLP que se cargaron antes de configurar el DLP. La clasificación también se aplica a los archivos que están a la espera de ser escaneados porque el sistema DLP externo no está disponible o responde con lentitud.

La clasificación de cada elemento viene determinada por la regla de respuesta del servidor ICAP. Si el servidor ICAP de DLP responde con un mensaje en el que se indica que el contenido debe bloquearse o eliminarse, el archivo se marca como **Escaneado:**Rechazado. De lo contrario, el archivo se marca como **Escaneado: OK**.

Para cada clasificación de datos, puede establecer diferentes restricciones de acceso y uso compartido. Para cada una de las tres categorías, el administrador de ShareFile elige qué acciones permitir:

- Los empleados pueden descargar o compartir el archivo.
- Los usuarios de clientes externos pueden descargar o compartir el archivo. El uso compartido entre clientes está desactivado de forma predeterminada, pero se puede habilitar en **Administración > Preferencias avanzadas > Permitir a los clientes compartir archivos**.
- Los usuarios anónimos pueden descargar el archivo

Cuando un usuario comparte un archivo, solo los usuarios con permisos de descarga pueden recibir el archivo. Por lo tanto, al habilitar el permiso de uso compartido para una clasificación de datos, también debe conceder al menos una clase de permiso de descarga de usuarios.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para configurar los ajustes de DLP en ShareFile

1. En la interfaz web de ShareFile, haga clic en **Administración > Prevención de pérdida de datos**.
2. Cambie la opción de **Limitar el acceso a los archivos en función de su contenido** a **Sí**.
3. Configure las acciones permitidas para cada clasificación de datos.

> **Importante:**
>
> La herramienta de ShareFile On-Demand Sync requiere permisos de descarga para su funcionamiento normal. Habilite las descargas de los empleados para todas las clasificaciones de contenido si su implementación incluye la ShareFile On-Demand Sync.

Cuando el controlador de zonas de almacenamiento envía un archivo al sistema DLP, incluye metadatos que indican el propietario del archivo. El archivo también incluye la ruta de la carpeta en la que reside el archivo en ShareFile. Esta información permite al administrador del servidor DLP ver detalles específicos de ShareFile sobre los archivos que contienen contenido confidencial.

Configuración avanzada para DLP

Para ajustar el proceso de escaneo de DLP, modifique el archivo de configuración que se encuentra en el controlador de zonas de almacenamiento en `wwwroot\Citrix\StorageCenter\SCDLPScanSvc\appSettings.config`. En la siguiente tabla se describe cada configuración relacionada con DLP.

Parámetro	Descripción	Valor predeterminado
scan-interval	La frecuencia con la que el servicio de DLP comprueba si hay archivos nuevos en la cola de DLP y los envía al servidor ICAP de DLP para su procesamiento.	30 segundos
icap-response-timeout	Cuánto tiempo espera el controlador de zonas de almacenamiento a recibir una respuesta de ICAP antes de marcar el servidor ICAP como no disponible.	30 segundos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro	Descripción	Valor predeterminado
icap-exclude-extensions	Lista de extensiones separadas por comas para excluirlas del análisis de DLP. El servidor DLP no procesa los archivos con nombres que terminen en una de estas extensiones, sino que los marca como escaneados: OK. Valor de ejemplo: “exe,jpg,bin,mov”	Ninguno
icap-max-file-size-bytes	Tamaño máximo del archivo (en bytes) que se va a enviar al servidor DLP para su procesamiento. Un valor de 0 significa que no hay un máximo y que se envían todos los tamaños de archivo. Cuando se configura con un valor distinto de cero, el servidor DLP no procesa los archivos que superen el tamaño configurado, sino que se marcan como Escaneados: OK.	31457280 (30 MB)
x-queue-items-to-process	El número máximo de elementos en cola para escanear por cada iteración del intervalo de escaneo. Disminuya este valor para mitigar el impacto en su servidor de DLP cuando se agrega una gran cantidad de archivos a StorageZone.	512

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro	Descripción	Valor predeterminado
max-queue-processing-threads	Cantidad máxima de subprocesos de procesador simultáneos que se pueden utilizar para vaciar la cola de escaneado de DLP. Defina este valor en función del número máximo de conexiones simultáneas permitidas a su servidor ICAP. Debe estar dentro de límites razonables para evitar bloquear otros servicios de red que utilizan el mismo servidor ICAP.	4
Icap-reqmod-http-request-verb	De forma predeterminada, las llamadas a la red se realizan con el verbo PUT. Puede cambiar esta configuración a POST si es necesario.	PUT

Herramienta DLPExistingFiles

El controlador de zonas de almacenamiento de ShareFile ofrece opciones para integrar el centro de almacenamiento con los proveedores de prevención de pérdida de datos (DLP) a través de ICAP.

Sin embargo, los servicios ICAP funcionan mediante colas que solo se llenan con archivos recién creados. Esto significa que los servicios no analizarán los archivos que existan en una zona antes de que se habilite el ICAP. Esta herramienta ayuda a poner esos archivos en cola para su análisis y también puede poner en cola los archivos escaneados para volver a escanearlos.

Como su nombre indica, la herramienta solo funciona para el servicio ICAP de DLP.

Requisitos

La herramienta es un script de PowerShell y, por lo tanto, necesita PowerShell para ejecutarse. También se necesitaPsExec o una herramienta similar, ya que el script debe ejecutarse como servicio de red para acceder a la ubicación compartida de la red.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ubicación

Para un controlador de zonas de almacenamiento instalado, puede encontrar la herramienta en <storage zones controller installation location>\Tools\DLPExistingFiles\DLPExistingFiles.ps1. La ubicación de instalación del controlador de zonas de almacenamiento es la predeterminada C:\inetpub\wwwroot\Citrix\StorageCenter.

Consideraciones antes de ejecutar la herramienta

Es posible que la herramienta deba ejecutarse varias veces para una sola operación, según lo siguiente.

- Las limitaciones proporcionadas para el límite de tamaño de la cola.
- El número de elementos para los criterios dados. Esta consideración es cierta a menos que el límite de tamaño de la cola esté establecido en cero o menos. En ese caso, la herramienta asume un tamaño máximo de 200 000 elementos en el directorio de colas.

Por ejemplo, si la herramienta se utiliza para poner en cola elementos no escaneados, el límite de tamaño de la cola se establece en 500 elementos. Cuando hay más de 500 elementos sin escanear, la herramienta se detiene cuando se hayan llenado 500 elementos en la cola. Para saber dónde se detuvo, la herramienta almacena la fecha de creación del último elemento recuperado. La herramienta almacena la fecha en un archivo temporal en <storage zones controller installation location>\SC con el nombre DLPExistingFiles-enddate.temp.

Antes de cada ejecución, la herramienta busca este archivo. Si el archivo está presente, la herramienta utiliza la fecha de creación que contiene como marcador para el siguiente lote de archivos. La herramienta no elimina el archivo temporal al finalizar una determinada operación. En cambio, el administrador de zona puede eliminar el archivo una vez que se hayan completado todos los lotes de una operación determinada. Debido a esta situación, cuando se complete una operación completa, el archivo temporal, si está presente, debe eliminarse manualmente antes de realizar otra operación diferente.

Ejecución de la herramienta con PsExec

Abra una ventana de comandos y ejecute PsExec con el siguiente comando.

```
PsExec.exe -i -u "nt authority\network service"

"C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
```

Esto abre PowerShell ejecutándose como servicio de red. Para comprobar que realmente se está ejecutando como servicio de red, ejecuta **whoami** y comprueba el resultado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Una vez que PowerShell esté abierto, ejecute la herramienta allí directamente para realizar cualquier tarea necesaria.

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

Opciones de línea de comandos

Están disponibles las siguientes opciones para ejecutar la herramienta:

- **-runscan** (obligatorio): esta opción se utiliza para especificar qué tipo de archivos se van a poner en cola para su análisis. Subopciones:
  - **Unscanned**: Archivos sin escanear. Por ejemplo, archivos de la era anterior a DLP que no se escaneaban.
  - **ScannedOK**: Archivos escaneados que se han marcado como limpios.
  - **ScannedRejected**: Archivos escaneados que se han marcado como no limpios.
  - **Scanned**: Todos los archivos escaneados.
- **-queueLimit** (opcional): Esta opción se utiliza para especificar el número de elementos permitidos en la cola antes de que la herramienta se detenga.
- **-date** (opcional): La fecha máxima de creación de los elementos que se pondrán en cola para su escaneo. Por ejemplo, si la fecha se especifica como “30/10/2017 11:30 a. m.”, solo los archivos que se crearon antes de esta fecha/hora se pondrán en cola para su escaneo.

Ejemplos:

Para ver todos los ejemplos, abra **PowerShell como servicio de red a través de PsExec**. Para obtener instrucciones, consulta los pasos anteriores en este artículo.

Para poner en cola los elementos no escaneados en una zona, ejecute el siguiente comando.

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

Para poner en cola todos los elementos escaneados dentro de una zona con un límite de 100 colas, ejecute el siguiente comando.

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

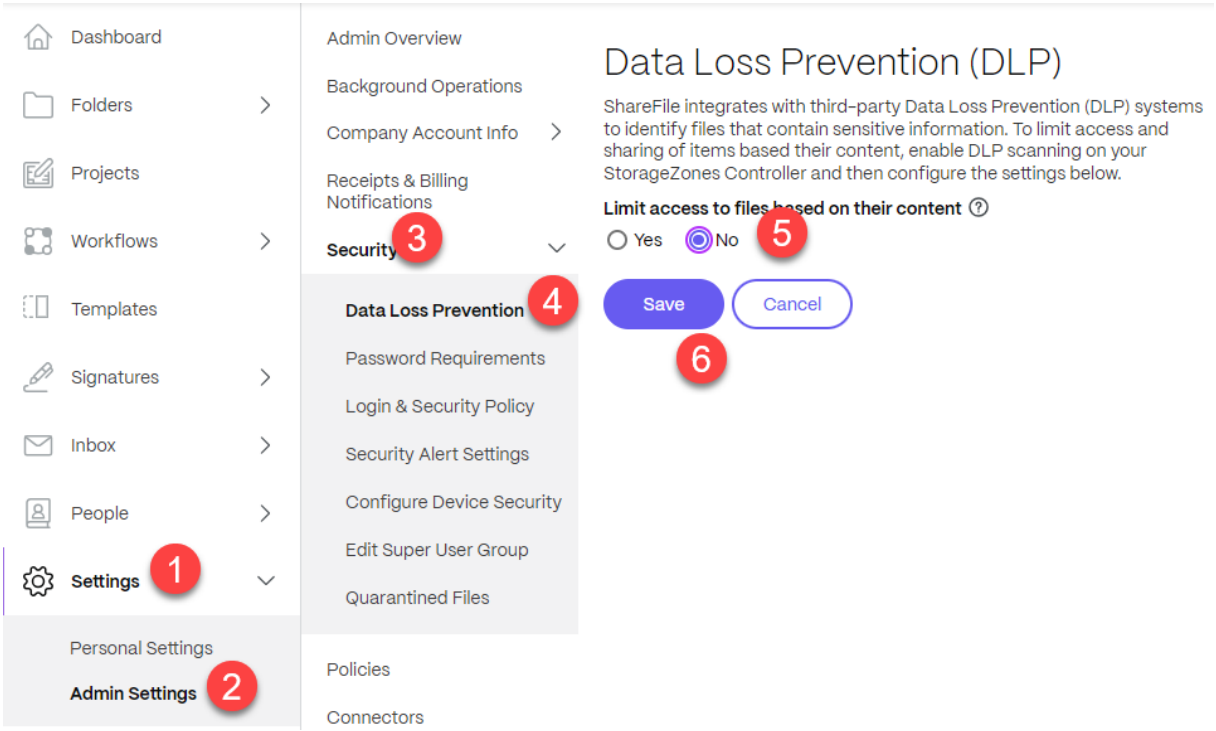
Para poner en cola todos los elementos escaneados creados antes de las 11:30 de la mañana del 30 de octubre de 2017 con las siguientes características: marcados como limpios, en una zona con un límite de 200 colas, ejecuta el siguiente comando.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Inhabilitar DLP

Para inhabilitar DLP para ShareFile y el controlador de zonas de almacenamiento, realice las acciones siguientes:



1. Inicie sesión en su cuenta de ShareFile y haga clic en **Configuración**.
2. En la lista desplegable que se abre, seleccione **Configuración de administrador**.
3. En el menú que se abre, haga clic en **Seguridad**.
4. En el menú Seguridad, elija la opción **Prevención de pérdida de datos**.
5. En la pantalla DLP, vaya a la sección **Limitar el acceso a los archivos según su contenido** y haga clic en **No**.
6. Seleccione **Guardar**.

Supervisar

February 9, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El controlador de zonas de almacenamiento y la interfaz de administrador de ShareFile incluyen varios recursos para ayudarlo a supervisar la actividad del controlador de zonas de almacenamiento y solucionar problemas:

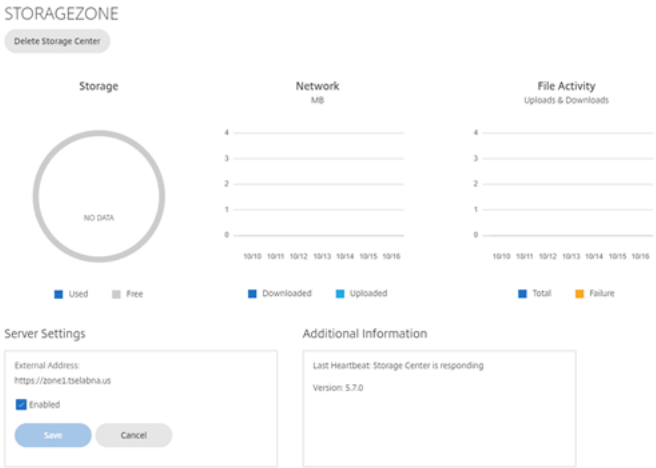
- **Estado general de los componentes**: La ficha Supervisión en la consola del controlador de zonas de almacenamiento proporciona el estado de los componentes para ayudarlo a iniciar el proceso de solución de problemas. El estado se proporciona para elementos como los permisos de acceso, el estado del servicio y el estado del latido, que indica la conectividad saliente del controlador de zonas de almacenamiento al plano de control de ShareFile.

  El controlador de zonas de almacenamiento envía actualizaciones a la aplicación web ShareFile cada 5 minutos. Si la aplicación web ShareFile no recibe una actualización en 10 minutos, marca el controlador de zonas de almacenamiento como sin conexión.

  Para los elementos de la ficha Supervisión que aparecen en rojo, revise los archivos de registro para obtener información detallada.

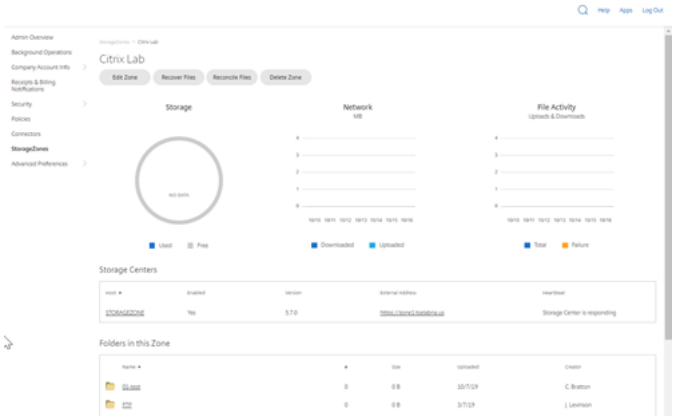
  La ficha Supervisión no indica si una zona de almacenamiento funciona en términos de conectividad. Esto incluye si el plano de control de ShareFile puede alcanzar la URL de las zonas de almacenamiento externas o si un cliente puede llegar a la zona.

- **Información del servidor del controlador de zonas de almacenamiento**: Para obtener información sobre el uso del almacenamiento, el uso de la red y la actividad de archivos del servidor: En la interfaz de ShareFile, inicie sesión en su cuenta de ShareFile Enterprise, vaya a **Admin > StorageZones**, haga clic en la zona de almacenamiento y, a continuación, haga clic en un almacenamiento nombre de host del controlador de zonas.



- **Información de zona**: Para obtener información sobre el uso del almacenamiento, el uso de la red y la actividad de archivos para una zona: En la interfaz de ShareFile, inicie sesión en su cuenta de ShareFile Enterprise, vaya a **Admin > StorageZones**y haga clic en el nombre de una zona.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Estado del controlador de zonas de almacenamiento**: Para determinar si ShareFile.com recibe mensajes de latido de los controladores de zonas de almacenamiento unidos a la zona, consulte el estado: En la interfaz de ShareFile, inicie sesión en su cuenta de ShareFile Enterprise, vaya a **Admin > StorageZones**, verifique que la columna Salud tenga una marca de verificación verde y, a continuación, haga clic en el nombre del sitio para verificar que el mensaje Heartbeat indica que el controlador de zonas de almacenamiento responde.

- **Archivos de registro**: Los archivos de registro proporcionan información detallada sobre la configuración del controlador de zonas de almacenamiento y sus componentes, como se describe en la siguiente sección.

Archivos de registros

Los siguientes archivos de registro para el controlador de zonas de almacenamiento se encuentran de forma predeterminada en `C:\inetpub\wwwroot\Citrix\StorageCenter\SC\logs`:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del archivo de registro	Contiene información de registro para
cfgsrv-%fecha%.txt	acciones de configuración del controlador de zonas de almacenamiento, incluida la modificación de una configuración de zonas de almacenamiento existente, la creación de una nueva zona de almacenamiento y la unión de un nuevo controlador de zonas de almacenamiento a un controlador de zonas de almacenamiento principal
sc-%fecha%.txt	Actividad de carga y descarga de datos de ShareFile para zonas estándar
CIFS-%fecha%.txt	conectores de zona de almacenamiento para la actividad de carga y descarga de archivos compartidos de red
sharepoint-%fecha%.txt	conectores de zona de almacenamiento para la actividad de carga y descarga de SharePoint
cloudstorageuploader-%fecha%.txt	Servicio de carga de almacenamiento en la nube (a un sistema de almacenamiento de terceros compatible)
copy-%fecha%.txt	Servicio de copia de ShareFile
delete–%fecha%.txt	Servicio de limpieza de ShareFile, para la memoria caché de almacenamiento persistente
s3uploader–%date%.txt	Servicio de administración de ShareFile. Incluye mensajes de estado de latidos

El registro extendido está disponible para cada uno de los siguientes componentes y es útil cuando necesita proporcionar información detallada para ofrecer asistencia.

Componente	Ubicación de AppSettingsRelease.config
Datos de ShareFile	C:\inetpub\wwwroot\Citrix\StorageCenter
conectores de zona de almacenamiento para los recursos compartidos de archivos	C:\inetpub\wwwroot\Citrix\StorageCenter\cifs
conectores de zona de almacenamiento para SharePoint	C:\inetpub\wwwroot\Citrix\StorageCenter\sp

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para habilitar el registro extendido

Los siguientes pasos permiten el registro extendido para todos los componentes y servicios del controlador de zonas de almacenamiento:

1. En el servidor del controlador de zonas de almacenamiento, abra IIS.
2. Vaya al sitio web predeterminado y, a continuación, abra Configuración de la aplicación.
3. Cambie el valor de habilitar registro extendido de 0 a 1.
4. Reinicie el servicio de administración de Citrix ShareFile.
5. Una vez resuelto el problema, le recomendamos que borre el registro extendido para reducir la cantidad de registros.

Para habilitar el registro extendido para un componente en particular, modifique su archivo AppSettingsRelease.config: Cambie el valor de `<add key="enable-extended-logging"value="0"/>` de 0 a 1.

También puede comprobar los registros de IIS para determinar si el tráfico llega al controlador de zonas de almacenamiento. Los registros de IIS muestran todas las solicitudes entrantes. Los registros de IIS del controlador de zonas de almacenamiento se encuentran en c:\inetpub\logs\LogFiles\W3SVC1.

Para habilitar el registro extendido de IIS, consulte http://support.microsoft.com/kb/313437.

Solucionar problemas de instalación y configuración

Problema	Descripción y solución
Aparece “Error HTTP 404: archivo o directorio no encontrado”durante la configuración del controlador de zonas de almacenamiento	El mensaje suele deberse a un problema con IIS o `ASP.NET`. Asegúrese de que la función de IIS esté habilitada en la instalación de Windows y de que la función `ASP.NET` esté habilitada en IIS.
Aparece “HTTP Error 404.2 —Not Found”cuando se navega por localhost en el controlador de zonas de almacenamiento	El mensaje indica que las restricciones ISAPI y CGI de `ASP.NET` no están configuradas en Permitidas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problema	Descripción y solución
Aparece “Error HTTP 413: la entidad de solicitud es demasiado grande”después de un intento de carga	El mensaje puede aparecer en un seguimiento de red después de un intento de carga fallido en una zona de almacenamiento y puede ser el resultado de una configuración de certificado de cliente en IIS. Para evitar este problema, en el servidor del controlador de zonas de almacenamiento, abra IIS. Vaya hasta el sitio web predeterminado y, a continuación, abra Configuración de SSL. Para los certificados de cliente, seleccione Ignorar. Reinicie el servicio de administración de Citrix ShareFile.
Se producen errores IIS durante la configuración del controlador de zonas	Los errores de IIS suelen indicar que ASP.NET no está completamente configurado. Compruebe en el Administrador de IIS, en Restricciones de ISAPI y CGI, que la Restricción esté establecida en Permitida para todos los listados de ASP.NET. Comprobar que ASP.NET está registrado en IIS: en el Administrador de IIS, en Grupos de aplicaciones, compruebe que hay listados de ASP.NET. Para registrar manualmente ASP.NET, consulte las líneas de comandos que están a continuación de esta tabla. Si sigue teniendo problemas, revise su IIS y la configuración de ASP.NET.
“Error al guardar el enlace del centro de almacenamiento”aparece durante la configuración del controlador de zonas de almacenamiento	El mensaje indica un problema de permisos en el usuario del grupo de cuentas de IIS. De forma predeterminada, los grupos de aplicaciones funcionan en la cuenta de usuario del servicio de red. El controlador de zonas de almacenamiento usa la cuenta de servicio de red de forma predeterminada. Si usa una cuenta de usuario nominal en lugar de la cuenta de servicio de red, la cuenta de usuario nominal debe tener acceso completo al recurso compartido de red utilizado para el almacenamiento de datos privados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problema	Descripción y solución
Aparece “Acceso denegado”durante la configuración de zona	El mensaje puede aparecer si la cuenta de ShareFile con la que ha iniciado sesión no tiene permiso para crear y administrar zonas. Use la consola de administrador de ShareFile para establecer ese permiso.
Las solicitudes salientes están bloqueadas	Cuando se bloquean las solicitudes salientes, el registro cfgsrv incluye System.net.WebException: El servidor remoto devolvió un error: (403) Forbidden. Es probable que este problema se deba a que el servidor proxy bloquea las solicitudes salientes. Compruebe que el firewall cumpla con los requisitos especificados en los requisitos del sistema del controlador de zonas de almacenamiento
Aparece “No se puede conectar al servidor remoto”cuando inicia sesión en el controlador de zonas de almacenamiento	El mensaje suele indicar un problema de proxy. Asegúrese de que la configuración de proxy esté configurada. Si la configuración del proxy es correcta, verifique que puede iniciar sesión en su cuenta de ShareFile desde el controlador de zonas de almacenamiento. Compruebe que tiene permisos de nivel de administrador para configurar el controlador de zonas de almacenamiento y que el puerto 443 esté abierto en el firewall externo.
La carpeta denominada ShareFileStorage en el recurso compartido de red no incluye SCKeys.txt después de habilitar y configurar las zonas de almacenamiento para ShareFile Data	el controlador de zonas de almacenamiento crea SCKeys.txt durante la instalación, a menos que la cuenta que utilizó para instalar el controlador de zona de almacenamiento no esté en la lista de control de acceso. Actualice la lista de control de acceso y reinstale el controlador de zonas de almacenamiento.
Las cargas de archivos a una carpeta compartida fallan después de crear una zona	Este problema indica que hay un problema con el DNS interno. Debe tener un registro DNS interno y externo para el FQDN del controlador de zonas de almacenamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problema	Descripción y solución
En la ficha **Monitorización**, el estado del latido está en rojo	Un icono rojo indica que el controlador de zona de almacenamiento no puede enviar mensajes de latido al sitio web de ShareFile. Compruebe si los iconos de otros componentes están en rojo. Si es así, consulte los registros para obtener más información. Si el registro s3uploader muestra un error al enviar el latido, es posible que el servidor del controlador de zonas de almacenamiento no pueda ponerse en contacto con el sitio web de ShareFile a menos que pase por un servidor proxy. Para especificar un servidor proxy para el controlador de zonas de almacenamiento, abra la consola del controlador y vaya a la ficha Redes. Si el servidor del controlador de zonas de almacenamiento no puede acceder al sitio web de ShareFile mediante un usuario de servicio de red, permita que el usuario del servicio de red acceda al sitio web de ShareFile o configure una cuenta de usuario de Windows con acceso saliente al servidor proxy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problema	Descripción y solución
Una zona de almacenamiento no aparece en la interfaz de administrador de ShareFile	Este problema puede indicar un problema con la dirección externa o el firewall. Primero verifique en la consola del controlador de zonas de almacenamiento que la dirección externa no incluya el puerto. Si lo hace, extraiga el puerto y, a continuación, reinicie el controlador. Si la dirección externa no incluye el puerto, asegúrese de que el firewall de Windows esté configurado correctamente. De forma predeterminada, la configuración del firewall de Windows permite el tráfico saliente para los servicios de ShareFile en el puerto 443. El controlador de zonas de almacenamiento requiere esa configuración. Compruebe que el firewall de Windows permite el tráfico saliente en el puerto 443 para los siguientes procesos: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc\FileDeleteService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCopySvc\FileCopyService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\s3uploader\S3UploaderService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\CloudStorageUploaderSvc\CloudStorageUploaderService.exe`, `C:\inetpub\wwwroot\Citrix\StorageCenter\SCProxyEmailSvc\ProxyEmailService.exe`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problema	Descripción y solución
El controlador de zonas de almacenamiento no carga datos en ShareFile	En la consola de Citrix ADC, haga clic con el botón derecho en el servidor virtual de equilibrio de carga para obtener estadísticas, para verificar si el tráfico llega a Citrix ADC desde el plano de control de ShareFile, el controlador de zonas de almacenamiento y los clientes de ShareFile. Cuando carga un archivo y el servidor virtual muestra un aumento en los resultados, el tráfico pasa a través de Citrix ADC. Verificar el tráfico para cada punto de la conexión de Citrix ADC: servidor virtual de conmutación de contenido, servidores virtuales de equilibrio de carga para conectores y datos de ShareFile, llamadas HTTP enlazadas a uno de los dos servidores virtuales, directiva de respuesta enlazada al servidor virtual de datos de ShareFile, servidor virtual de conectores enlace a Citrix ADC AAA. A continuación, pruebe las cargas de datos de ShareFile desvinculando la directiva de respuesta en el servidor virtual de equilibrio de carga para los datos de ShareFile. (La directiva de respuesta descarta el tráfico entrante que no está firmado por el plano de control de ShareFile. En un explorador web, escriba el FQDN externo del controlador de zonas de almacenamiento. Si hay conectividad, aparece el logotipo de ShareFile. En un explorador web, escriba la URL de un conector. Si las siguientes URL logran probar la accesibilidad de los conectores de la zona de almacenamiento, se le solicitarán las credenciales incluso si el servidor back-end está inactivo. O bien, si ha iniciado sesión como usuario, recibirá una respuesta de la API. `https://szc-address/cifs/v3/Items/ByPath?path=\\path`, `https://szc-address/sp/v3/Items/ByPath?path=http://sharepoint-server`. La respuesta de la API tiene este formato: {“Name”:”connectorName”, “FileName”:”FileName”,“CreationDate”:”date”, “ProgenyEditDate”:”date”,“IsHidden”:false, “Path”:”“,”StreamID”:”id”,“odata.metadata”:” `https://szc-address/cifs/v3/$metadata#`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problema	Descripción y solución
El estado de Conectividad de ShareFile desde File Cleanup Services es un icono rojo después de actualizar el controlador de zonas de almacenamiento	Aparece un icono rojo si Windows inicia el Servicio de limpieza de archivos antes de que el controlador de zonas de almacenamiento establezca una conexión de red. El estado volverá a un icono verde después de que el servidor del Controller vuelva a estar en la red.
Aparece “La ruta supera la longitud máxima (1024)”durante la creación del conector	El mensaje puede aparecer si la dirección externa configurada para el controlador de zonas de almacenamiento apunta al sitio web de ShareFile en lugar del FQDN del servidor del controlador de zonas de almacenamiento.
Aparece un “nombre no válido”cuando se configura un nuevo controlador de zonas de almacenamiento después de eliminar uno antiguo.	El mensaje puede aparecer si aún existen entidades relacionadas con el controlador de zonas de almacenamiento antiguo. Para resolver este problema: desinstale el nuevo controlador de zonas de almacenamiento. Elimine la carpeta de red compartida. Elimine la carpeta c:\inetpub\wwwroot\Citrix. Abra regedit y elimine la clave **HKEY_LOCAL_MACHINE/Software/Wow6432Note/Citrix**. Instale y configure un nuevo controlador de zonas de almacenamiento. Si el problema persiste, contacte con su representante de asistencia. Este mensaje se produce cuando los servidores de zonas de almacenamiento no pueden resolver el FQDN de la zona de almacenamiento mediante DNS o el archivo de hosts locales.

Para registrarse manualmente ASP.NET

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
7 %systemroot%\system32\inetsrv\appcmd set config /section:
    isapiCgiRestriction
8 /[path='%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll'
    ].allowed:True
```

Solucionar problemas de clientes y aplicaciones web de ShareFile

Si un dispositivo móvil no se conecta a un conector, verifique la conectividad. En la tabla anterior se tratan muchos problemas de conectividad. Asegúrese de que el controlador de zona de almacenamiento esté en línea. Sube un archivo a la zona. Si la carga funciona, el problema es específico de los conectores. Intente conectarse desde el dispositivo móvil a través de la red móvil y de la empresa. Compruebe que el servidor de archivos o el servidor de SharePoint estén disponibles.

Si aparece un "Error HTTP 401: no autorizado"al intentar acceder a un conector, puede deberse a alguno de los siguientes problemas que pueden impedir que un usuario acceda a un conector desde los clientes de ShareFile o la aplicación web de ShareFile:

- Configuración incorrecta de IIS: compruebe que la función Servicios web (IIS) tenga habilitadas la autenticación básica y la autenticación de Windows. Si esas opciones no se enumeran en Seguridad, use el Administrador del servidor para instalarlas y, a continuación, reinicie IIS.
- Permisos de usuario incorrectos: compruebe que el usuario de AD tiene acceso al recurso compartido. En el Administrador del servidor, vaya a Administración de recursos compartidos y almacenamiento y agregue el usuario o cambie los permisos del usuario según sea necesario.
- Un problema con la autenticación, la autorización y el acceso a grupos de auditoría de Citrix ADC.

Si aparece un "Error HTTP 403: prohibido"al conectarse a un sitio de SharePoint, es posible que el servidor de SharePoint esté configurado para la autenticación básica, pero es posible que el controlador de zona de almacenamiento no esté configurado para almacenar en caché las credenciales. Para resolver este problema, agregue `<add key="CacheCredentials"value="1"/>` a `C:\inetpub\wwwroot\Citrix\StorageCenter\sp\AppSettingsRelease.config`.

Si aparece un "Error HTTP 503: servicio no disponible"cuando las aplicaciones móviles intentan acceder a un conector, los conectores envían una respuesta pero no pueden gestionar la solicitud HTTP. Esto puede ocurrir si las directivas de conmutación de contenido, las VIP de equilibrio de carga o la directiva de respuesta están configuradas o enlazadas incorrectamente en Citrix ADC. Para resolver este problema, revise la configuración de Citrix ADC para ShareFile y corrija la configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Referencia: archivos de configuración del controlador de zonas de almacenamiento

December 5, 2022

Esta referencia proporciona una descripción general de los archivos de configuración del controlador de zonas de almacenamiento:

- Configurar el controlador de zonas de almacenamiento con datos de ShareFile en Microsoft Azure
- AppSettingsRelease.config
- FileDeLeteService.exe.config
- sfantivirus.exe.config
- Web.config

El instalador del controlador de zonas de almacenamiento crea esos archivos. Los cambios que realice en la consola del controlador de zonas de almacenamiento se guardan en los archivos.

Para usar o configurar determinadas funciones, debe agregar o actualizar manualmente algunos ajustes en los archivos de configuración. Esta referencia enumera esa configuración y proporciona vínculos a información relacionada.

Datos de ShareFile en Microsoft Azure Storage

Las zonas de almacenamiento administradas por el cliente permiten alojar datos de Citrix ShareFile de forma nativa en su cuenta de Microsoft Azure. El uso de almacenamiento de terceros compatible ayuda al departamento de TI a crear una solución rentable y personalizada para su organización. Esta solución integra ShareFile con el almacenamiento de objetos grandes (Blob) binarios de Microsoft Azure. Este almacenamiento es un servicio en la nube para almacenar grandes cantidades de datos no estructurados a los que se puede acceder desde cualquier lugar mediante HTTP o HTTPS.

Configurar el controlador de zonas de almacenamiento con datos de ShareFile en Microsoft Azure

Antes de crear una zona de almacenamiento con ShareFile Data en Microsoft Azure, consulte los requisitos del sistema y los pasos de instalación:

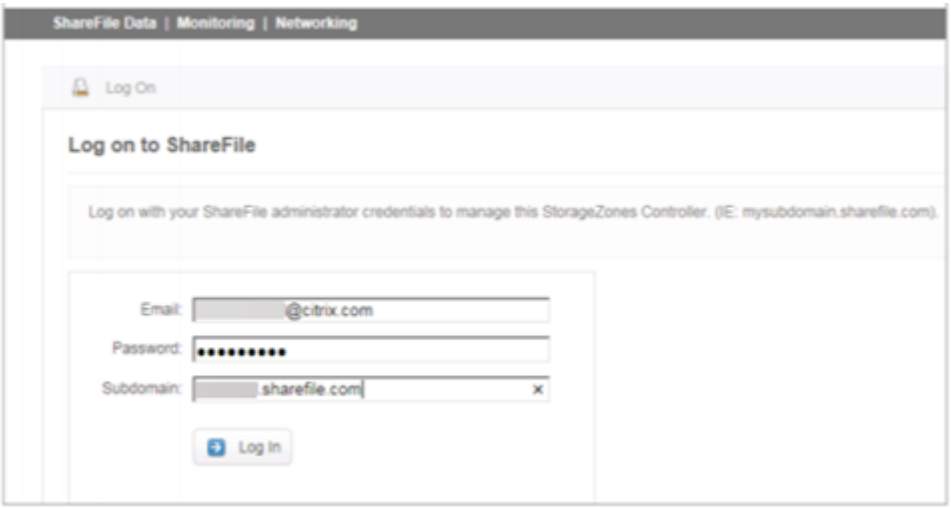
- Cree un recurso compartido de red para la memoria caché de almacenamiento. Para obtener más información, consulte Crear un recurso compartido de red para el almacenamiento de datos privado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

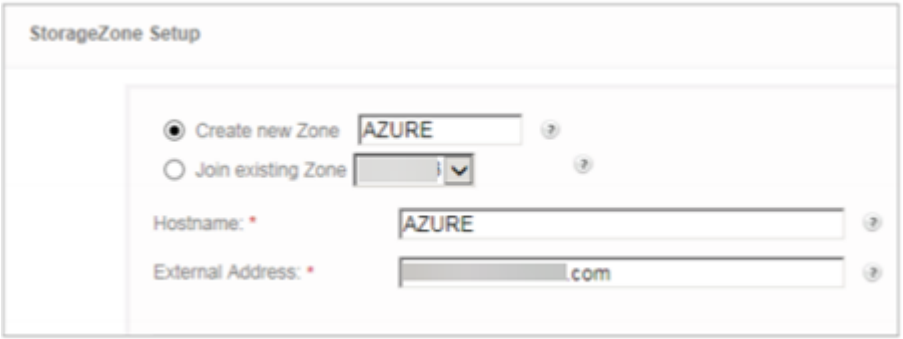
- Instale los certificados SSL necesarios. Para obtener más información, consulte Instalar un certificado SSL.
- Prepare el servidor para la instalación de la zona de almacenamiento. Para obtener más información, consulte Preparar el servidor para los datos de ShareFile.

Una vez instalado el software del controlador de zonas de almacenamiento, vaya a **Citrix ShareFile Storage Zones Controller** y seleccione **la página de configuración**.

1. Inicie sesión en ShareFile con la cuenta de administrador asignada.



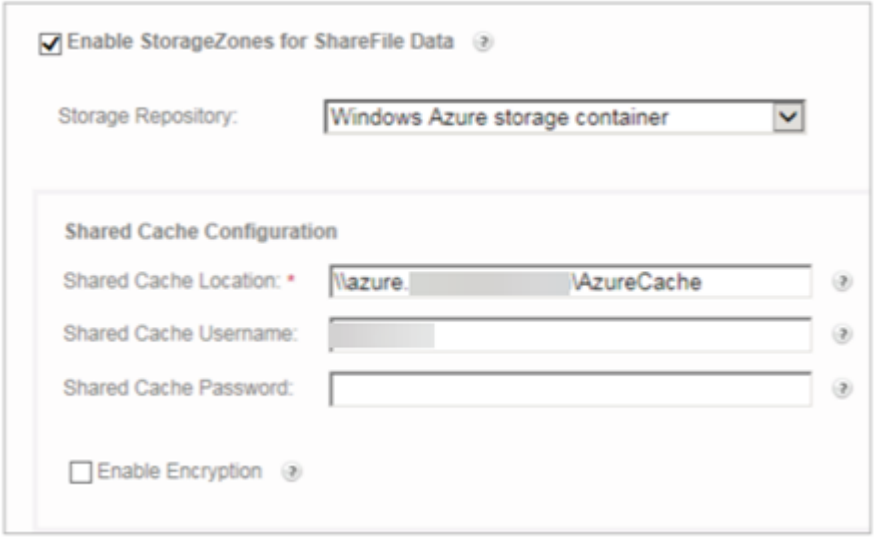
2. Seleccione la opción **Crear nueva zona** e introduzca un nombre único para la nueva zona.
3. Introduzca el **nombre del**servidor, normalmente se utilizará el nombre del equipo del servidor.
4. Introduzca la **dirección externa** de esta zona. Esta es la dirección FQDN de este servidor o balanceador de cargas que se puede resolver públicamente.



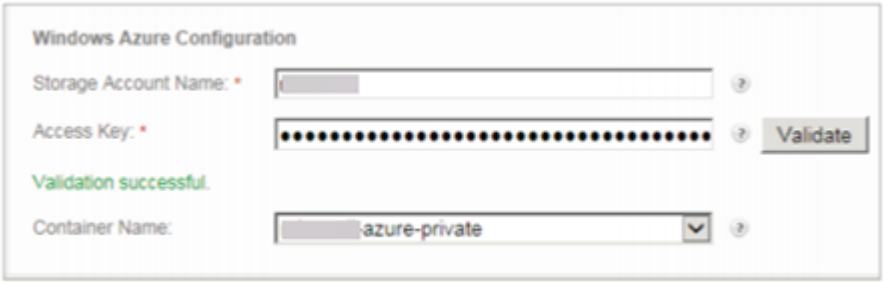
5. Marque la casilla **Activar zonas de almacenamiento para datos de ShareFile** .
6. Seleccione el **contenedor de almacenamiento de Windows Azure** en el menú desplegable del **repositorio de almacenamiento** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Introduzca la **ubicación de caché compartida** creada durante la instalación de requisitos previos. Consulte Crear un recurso compartido de red para el almacenamiento privado de datos. Introduzca un nombre de usuario y una contraseña con acceso a la carpeta Caché compartida.



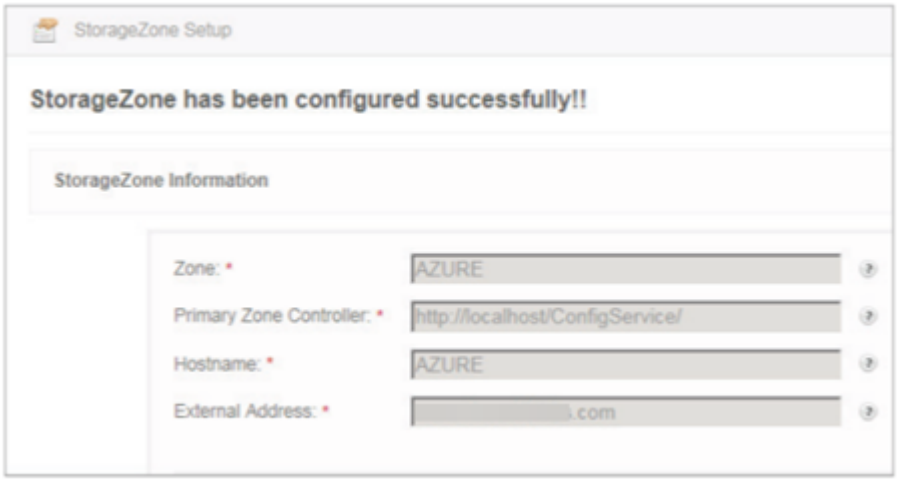
8. Introduzca el **nombre de la cuenta de almacenamiento** y **la clave de acceso**. Esta información proviene de su cuenta de Microsoft Azure.
9. Selecciona **Validar**.
10. Una vez validados, se le presentarán los contenedores que tiene disponibles en Azure. Seleccione el contenedor apropiado en el menú desplegable **Nombre del contenedor** .



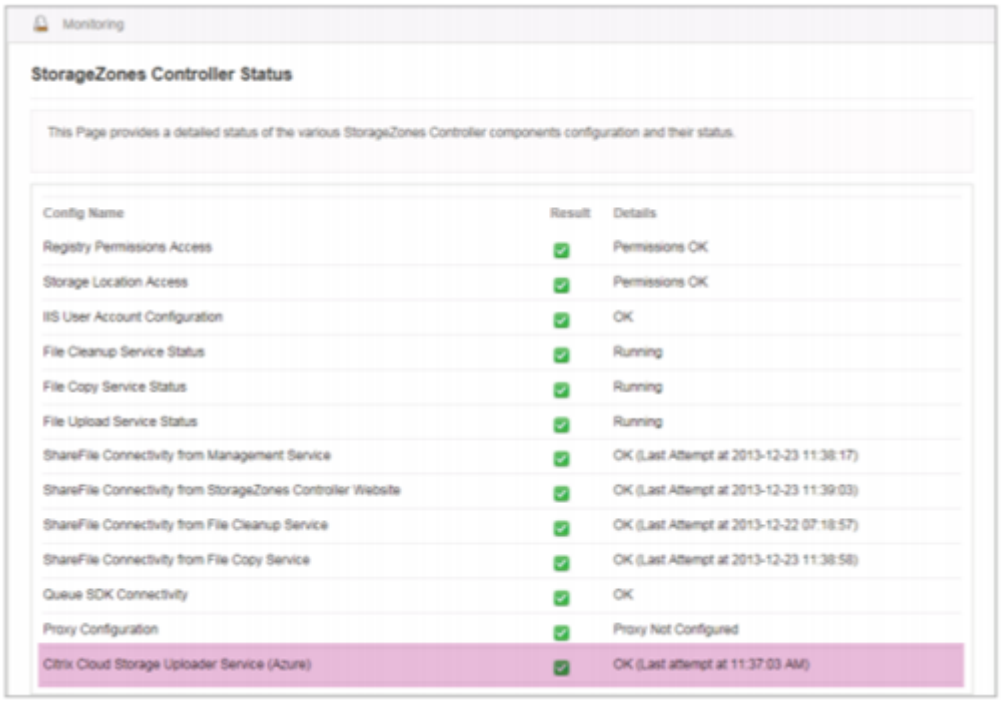
11. En la parte inferior de la página, introduce una contraseña y vuelve a escribirla para verificarla.
12. Seleccione **Register**.

    Una vez completado, aparece el siguiente mensaje: ¡StorageZone se ha configurado correctamente!

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

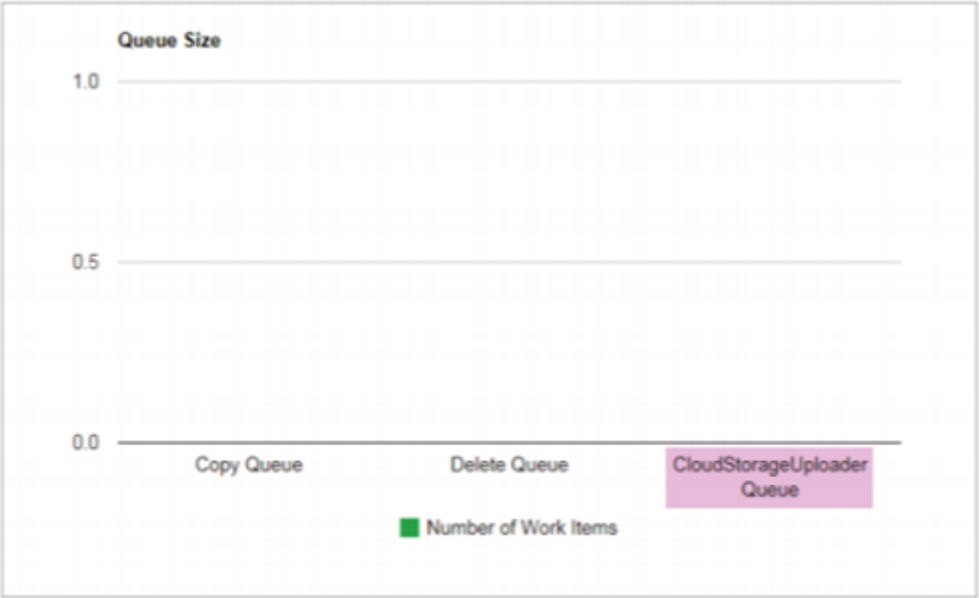


13. Seleccione la pestaña **Monitorización** y verifique el estado del StorageZones Controller. El servicio de carga de archivos en segundo plano de Citrix Cloud Storage (Azure) supervisa el servicio de carga en segundo plano de Azure.



La **cola de carga de CloudStorageUploader** supervisa la carpeta de colas de carga de Azure.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



AppSettingsRelease.config

Los archivos AppSettingsRelease.config se encuentran en las siguientes carpetas de la ruta de instalación del controlador de zonas de almacenamiento (C:\inetpub\wwwroot\Citrix\):

- Centro de almacenamiento

  Define la configuración global del controlador de zonas de almacenamiento.

- StorageCenter\ cifs

  Define la configuración de los conectores de zonas de almacenamiento para recursos compartidos de archivos de red.

- StorageCenter\ sp

  Define la configuración de los conectores de zonas de almacenamiento para SharePoint.

Antes de editar un archivo AppSettingsRelease.config, compruebe que está trabajando en la ubicación correcta.

FileDeLeteService.exe.config

FileDeleteService.exe.config proporciona los controles que utiliza el controlador de zonas de almacenamiento para administrar la caché de almacenamiento persistente. Este archivo de configuración se encuentra en: `C:\inetpub\wwwroot\Citrix\StorageCenter\SCFileCleanSvc`

Para obtener más información, consulte Personalizar las operaciones de la memoria caché de almacenamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sfantivirus.exe.config

SFAntivirus.exe.config proporciona al software del escáner información sobre la configuración del controlador de zonas de almacenamiento, la ubicación del software del escáner y varias opciones de comandos. Este archivo de configuración se encuentra en: `C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SFAntiVirus`

Para obtener más información, consulte Configurar los análisis antivirus de los archivos cargados.

Web.config

En general, `C:\inetpub\wwwroot\Citrix\StorageCenter\ConfigService\Web.config` contiene controles que normalmente no se deben cambiar. Sin embargo, tendrá que actualizarlo si utiliza controladores de zonas de almacenamiento más antiguos con un servidor proxy.

Solo para StorageZones Controller 2.2 a 2.2.2: si una zona tiene varios controladores de zonas de almacenamiento y todo el tráfico HTTP utiliza un servidor proxy, debe agregar una lista de omisiones a Web.config para cada servidor secundario.

Nota: A partir de la versión 2.2.3, la configuración de omisión se incluye en la página Red de la consola de controladores de zonas de almacenamiento.

1. Abra el archivo en un editor de texto y localice la `<system.net>` sección. A continuación se muestra un ejemplo de esa sección después de configurar un servidor proxy:

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

2. Añada una lista de omisiones a esa sección, como se muestra:

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

El servidor principal es una dirección IP o un nombre de host (servername.subdomain.com).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si más adelante cambia la dirección IP o el nombre de host del controlador de zonas de almacenamiento principal, debe actualizar esa información en ConfigService\ Web.config para cada servidor secundario.

3. Reinicie el servidor IIS de todos los miembros de la zona.

© 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).