



Cambiar la capa de datos

Virtual Desktop Service

NetApp

February 20, 2023

This PDF was generated from https://docs.netapp.com/es-es/virtual-desktop-service/Architectural.change_data_layer.Azure_Files.html on February 20, 2023. Always check docs.netapp.com for the latest.

Tabla de Contenido

- Redirigiendo plataforma de almacenamiento..... 1
 - Descripción general 1
 - Redirigiendo la plataforma de almacenamiento a Azure Files..... 3

Redirigiendo plataforma de almacenamiento

Descripción general

Las tecnologías de implementación del servicio de escritorios virtuales permiten diversas opciones de almacenamiento en función de la infraestructura subyacente, esta guía aborda cómo realizar un cambio tras la puesta en marcha.

El rendimiento de los escritorios virtuales depende de diversos recursos clave; el rendimiento del almacenamiento es una de las variables principales. A medida que cambian los requisitos y las cargas de trabajo evolucionan, la necesidad de cambiar la infraestructura de almacenamiento es una tarea común. En casi todos los casos esto implica la migración desde una plataforma de servidor de archivos a la tecnología de almacenamiento de NetApp (como Azure NetApp Files, Cloud Volumes Service de NetApp en Google o Cloud Volumes ONTAP de NetApp en AWS), ya que estas tecnologías suelen ofrecer el mejor perfil de rendimiento para los entornos de computación de usuario final.

Creando la nueva capa de almacenamiento

Debido a la gran variedad de servicios de almacenamiento potenciales en una amplia variedad de proveedores de infraestructuras cloud y HCI, en esta guía se supone que ya se ha establecido un nuevo servicio de almacenamiento y que se conocen las rutas para SMB.

Cree carpetas de almacenamiento

1. En el nuevo servicio de almacenamiento, cree tres carpetas:

- /Datos
- /Inicio
- /Pro

[]

2. Establecer permisos de carpeta

a. En Propiedades de carpeta, seleccione *Security*, >*Advanced* > *Disable Herencia*

[]

b. Ajuste el resto de la configuración para que coincida con la configuración de la capa de almacenamiento original creada originalmente por la automatización de la puesta en marcha.

Mover datos

Los directorios, datos, ficheros y configuraciones de seguridad se pueden mover de diferentes maneras. La siguiente sintaxis de robocopy conseguirá los cambios necesarios. Es necesario cambiar las rutas para adecuarse a su entorno.

```
robocopy c:\data\zucd \\uyy-1c37.deskapps.mobi\zucd-data /xd ~snapshot  
/MIR /CopyAll /R:1 /W:1 /tee /log:C:\temp\roboitD.txt
```

Redirigir la ruta del SMB en la transición

Cuando llegue el momento de la transición, algunos cambios redirigirán todas las funcionalidades del almacenamiento en el entorno VDS.

Actualizar GPO

1. El GPO usuarios (denominado <company-code>-users) debe actualizarse con la nueva ruta de acceso al recurso compartido. Seleccione *Configuración de usuario > Configuración de Windows > Preferencias > Mapas de unidad*

□

2. Haga clic con el botón derecho del ratón en *H:*, seleccione *Propiedades > Editar > Acción: Reemplazar e* introduzca la nueva ruta

□

3. Con AD clásico o híbrido, actualice el recurso compartido definido en ADUC en la unidad organizativa de la empresa. Esto se refleja en la gestión de carpetas VDS.

□

Actualice las rutas de perfil de FSLogix

1. Abra Regedit en el servidor de archivos original y cualquier otro host de sesión aprovisionado.



Esto también se puede establecer mediante una directiva de GPO si se desea.

2. Edite el valor *VHDLocations* con el nuevo valor. Debe ser la nueva ruta SMB más *pro/profilainers* como se muestra en la captura de pantalla siguiente.

□

Actualice la configuración de redirección de carpetas para los directorios iniciales

1. Open Group Policy Management, seleccione usuarios GPO vinculados a DC=dominio,DC=mobi/espacio de trabajo en la nube/Empresas de entornos de trabajo en la nube/<company-code>/usuarios de escritorios <company-code>.
2. Edite las rutas de redirección de carpetas en Configuración de usuario>Directivas>Configuración de Windows>Redirección de carpetas.
3. Sólo es necesario actualizar el escritorio y los documentos y las rutas deben coincidir con el nuevo punto de montaje de la ruta SMB para el volumen inicial

□

Actualice la base de datos de VDS SQL con Command Center

CWMGR1 contiene una utilidad auxiliar llamada Command Center que puede actualizar por lotes la base de datos VDS.

Para realizar las actualizaciones finales de la base de datos:

1. Conéctese a CWMGR1, navegue y ejecute CommandCenter.exe

[]

2. Desplácese hasta la ficha *Operations*, haga clic en *Load Data* para rellenar la lista desplegable Código de compañía, seleccione el código de compañía e introduzca las nuevas rutas de almacenamiento para la capa de almacenamiento y, a continuación, haga clic en *Execute Command*.

[]

Redirigiendo la plataforma de almacenamiento a Azure Files

Descripción general

Las tecnologías de puesta en marcha de Virtual Desktop Service permiten disfrutar de diversas opciones de almacenamiento en función de la infraestructura subyacente. Esta guía trata cómo realizar un cambio en el uso de Azure Files después de la implementación.

Requisitos previos

- AD Connect instalado y configurado
- Cuenta de administración global de Azure
- Módulo AZFilesHybrid PowerShell <https://github.com/Azure-Samples/azure-files-samples/releases>
- Módulo PowerShell de AZ
- Módulo PowerShell de ActiveDirectory

Cree la nueva capa de almacenamiento

1. Inicie sesión en Azure con la cuenta de administrador global
2. Cree una nueva cuenta de almacenamiento en la misma ubicación y grupo de recursos que el área de trabajo

[]

3. Cree los recursos compartidos de archivos de datos, casa y profesionales en la cuenta de almacenamiento

[]

Configure Active Directory

1. Cree una nueva unidad organizativa llamada «cuenta de almacenamiento» en la OU de cuentas de servicio de área de trabajo cloud > Área de trabajo cloud

[]

2. Habilitar la autenticación de AD DS (se debe realizar mediante PowerShell) <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable>
 - a. DomainAccountType debería ser "ServiceLogonAccount"

- b. `OrganizationalUnitDistinguishedName` es el nombre distinguido de la OU creada en el paso anterior (es decir "`OU=Storage Account,OU=Cloud Workspace Service Accounts,OU=Cloud Workspace,DC=TrainingKrisG,DC=onmicrosoft,DC=com`")

Configure los roles para los recursos compartidos

1. En el portal de Azure, proporcione a los técnicos de `CloudWorkspaceSVC` y `Level3` la función "almacenamiento de datos compartidos de SMB elevado colaborador"
2. Proporcione la función "Colaborador de recurso compartido de datos de archivo de almacenamiento" a "`<company code>-all users`grupo`"

[]

[]

Cree los directorios

1. Crear un directorio en cada recurso compartido (datos, inicio, pro) utilizando el código de la empresa como nombre (en este ejemplo, el código de la empresa es "`kift`")
2. En el directorio `<company code>` del recurso compartido pro, cree un directorio "`ProfileContainers`"

[]

[]

Establezca los permisos NTFS

1. Conéctese a los recursos compartidos
 - a. Desplácese hasta el recurso compartido situado bajo la cuenta de almacenamiento del portal de Azure, haga clic en los tres puntos y, a continuación, haga clic en `Connect`
 - b. Elija el método de autenticación de Active Directory y haga clic en el icono Copiar en el portapapeles en la esquina inferior derecha del código
 - c. Inicie sesión en el servidor `CWMGR1` con una cuenta que es miembro del grupo de técnicos `Level3`
 - d. Ejecute el código copiado en PowerShell para asignar la unidad
 - e. Haga lo mismo para cada recurso compartido mientras selecciona una letra de unidad diferente para cada uno
2. Desactive la herencia en los directorios de `<company code>`
3. El sistema y el grupo `AD ClientDHPAccess` deben tener control completo en los directorios de `<company code>`
4. Los equipos de dominio deben tener control total en el directorio `<company code>` del recurso compartido pro, así como en el directorio `ProfileContainers` de
5. El grupo AD de usuarios de `<company code>-All` debe tener permisos de carpeta/datos de lectura en los directorios `<company code>` de los recursos compartidos home y pro

6. El grupo AD de usuarios de <company code>-All debe tener los siguientes permisos especiales para el directorio en el recurso compartido de datos

[]

7. El grupo AD de usuarios <company code>-All debe tener el permiso Modificar en el directorio ProfileContainers

Actualizar objetos de directiva de grupo

1. Actualice los usuarios de GPO <company code> ubicados en espacio de trabajo en nube > Empresas de área de trabajo en nube > <company code> > usuarios de escritorios <company code>

- a. Cambie la asignación de la unidad de inicio para que apunte el nuevo recurso compartido

[]

- b. Cambie la redirección de carpetas para que apunte el recurso compartido principal para el escritorio y los documentos

[]

[]

Actualice el recurso compartido en usuarios y equipos de Active Directory

1. Con AD clásico o híbrido, el recurso compartido en la unidad organizativa de código de empresa debe actualizarse a la nueva ubicación

[]

Actualizar rutas de datos/inicio/Pro en VDS

1. Inicie sesión en CWMGR1 con una cuenta en el grupo de técnicos de nivel 3 e inicie el Command Center
2. En la lista desplegable comando, seleccione Cambiar datos/Inicio/carpetas Pro
3. Haga clic en el botón cargar datos y asegúrese de que el código de empresa correcto está seleccionado en la lista desplegable
4. Introduzca el nuevo patsh para las ubicaciones de datos, de inicio y de profesionales
5. Desactive la casilla es Windows Server
6. Haga clic en el botón Ejecutar comando

[]

Actualice las rutas de perfil de FSLogix

1. Abra el repositorio del registro en los hosts de sesión
2. Edite la entrada VHDRoccations de HKLM\SOFTWARE\FSLogix\Profiles para que sea la ruta UNC al nuevo directorio ProfileContainers

[]

Configurar copias de seguridad

1. Se recomienda configurar y configurar una política de backup para los nuevos recursos compartidos
2. Cree un nuevo almacén de servicios de recuperación en el mismo grupo de recursos
3. Desplácese hasta el almacén y seleccione copia de seguridad en primeros pasos
4. Elija Azure para la ubicación en la que se ejecuta la carga de trabajo y el recurso compartido de archivos de Azure para el backup. A continuación, haga clic en Backup
5. Seleccione la cuenta de almacenamiento utilizada para crear los recursos compartidos
6. Añada los recursos compartidos para realizar el backup
7. Edite y cree una política de backup que se ajuste a sus necesidades

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.