Administración del sistema

Virtual Desktop Service

NetApp
February 20, 2023

Tabla de Contenido

Administración del sistema

Cree una cuenta de administrador de dominio ("nivel 3")

Descripción general

En ocasiones, los administradores de VDS necesitan credenciales a nivel de dominio para gestionar el entorno. En VDS, se denominan cuentas de "nivel 3" o ".tech".

Estas instrucciones muestran cómo se pueden crear estas cuentas con los permisos correspondientes.

Controlador de dominio de Windows Server

Al ejecutar un controlador de dominio alojado internamente (o un DC local vinculado a Azure a través de una ruta VPN/Express), las cuentas .tech se pueden realizar directamente en Active Directory Manager.

1. Conéctese al controlador de dominio (CWMGR1, DC01 o a la VM existente) con una cuenta de administrador de dominio (.tech).
2. Cree un nuevo usuario (si es necesario).
3. Añada el usuario al grupo de seguridad "técnicos de nivel 3"

   [Management.System Administration.create dominio admin account 9ee17] |

Management.System_Administration.create_domain_admin_account-9ee17.png

a. Si falta el grupo de seguridad "técnicos de nivel 3", cree el grupo y haga que sea miembro del grupo de seguridad "CW-Infrastructure".

   [Management.System Administration.create domain admin account 0fc27] |

Management.System_Administration.create_domain_admin_account-0fc27.png

Agregar “.tech” al final del nombre de usuario es una práctica recomendada para ayudar a delinear las cuentas de administración de las cuentas de usuario final.

Servicios de dominio de Azure AD

Si se ejecuta en Azure AD Domain Services o se administra un usuario en Azure AD, estas cuentas pueden gestionarse (es decir, cambiar contraseña) en el portal de gestión de Azure como un usuario normal de Azure AD.

Se pueden crear nuevas cuentas, si se añaden a estos roles, se deberán otorgar los permisos necesarios:

1. Administradores de DC de AAD
2. ClientDHAccess
3. Administrador global en el directorio.

Agregar “.tech” al final del nombre de usuario es una práctica recomendada para ayudar a delinear las cuentas de administración de las cuentas de usuario final.

[]

Acceso temporal a terceros

Descripción general

Ofrecer acceso a terceros es una práctica habitual a la hora de migrar a cualquier solución cloud.

Los administradores de VDS suelen optar por no ofrecer a estos terceros el mismo nivel de acceso que tienen, para seguir una política de acceso de seguridad “menos necesaria”.

Para configurar el acceso de administrador para terceros, inicie sesión en VDS y navegue hasta el módulo Organizations, haga clic en la organización y haga clic en Users & Groups.

A continuación, cree una nueva cuenta de usuario para el tercero y desplácese hacia abajo hasta que vea la sección Admin Access y marque la casilla para habilitar los derechos de administrador.

[]

A continuación, se presenta el Administrador de VDS con la pantalla de configuración de Admin Access. No es necesario cambiar el nombre, el inicio de sesión o la contraseña del usuario; sólo tiene que agregar el número de teléfono y/o el correo electrónico si desea aplicar la autenticación multifactor y seleccionar el nivel de acceso que se va a conceder.

Para administradores de bases de datos como VAR o ISV, *Servers* es normalmente el único módulo de acceso necesario.

[]

Una vez guardado, el usuario final tendrá acceso a las funciones de autogestión iniciando sesión en VDS con sus credenciales de usuario estándar de escritorio virtual.

Cuando el usuario recién creado inicie sesión, solo verá los módulos que les haya asignado. Pueden seleccionar la organización, desplazarse hacia abajo hasta la sección servidores y conectarse al nombre de servidor que les indica (por ejemplo, <XYZ> ITM, donde XYZ es el código de su compañía y D1 designa que el servidor es un servidor de datos. En el siguiente ejemplo, les diremos que se conecten al servidor TSD1 para realizar sus asignaciones.

[]

Configurar la programación de copia de seguridad

Descripción general

VDS tiene la capacidad de configurar y gestionar servicios de backup nativos en algunos proveedores de infraestructura como Azure.

Azure

En Azure, VDS puede configurar automáticamente los backups con las funcionalidades nativas "Backup en el cloud de Azure" Con almacenamiento redundante local (LRS). El almacenamiento redundante (GRS) se puede configurar en el portal de gestión de Azure si es necesario.

- Se pueden definir políticas de backup individuales para cada tipo de servidor (con recomendaciones predeterminadas). Además, se puede asignar a máquinas individuales una programación independiente (desde su tipo de servidor) desde la interfaz de usuario de VDS. Esta opción se puede aplicar desplazando a la vista Detalle del servidor haciendo clic en el nombre del servidor en la página espacio de trabajo (vea el vídeo siguiente: Configuración de políticas de copia de seguridad individuales).
  - SQL Server
    - Backup con 7 copias de seguridad diarias, 5 semanales y 2 mensuales. Aumente los períodos de retención en función de los requisitos del negocio.
    - Esto es válido tanto para un servidor de datos dedicado como para equipos virtuales VPS adicionales para aplicaciones y bases de datos.
  - De almacenamiento
    - CWMGR1 – copia de seguridad diaria y mantener 7 días, 5 semanas, 2 meses.
    - Puerta de enlace RDS: Realice una copia de seguridad semanal y mantenga las 4 horas del día.
    - Puerta de enlace HTML5: Realice una copia de seguridad semanal y mantenga 4 horas al día.
  - PowerUser (también conocido como usuario de VDI)
    - No haga una copia de seguridad del equipo virtual ya que los datos deberían almacenarse en un servidor D1 o TSD1.
    - Tenga en cuenta que algunas aplicaciones almacenan los datos localmente y deben tenerse en cuenta consideraciones especiales si este es el caso.
    - En caso de fallo de una máquina virtual, es posible integrar un nuevo equipo virtual mediante el procedimiento de clonación de otro. En caso de que solo haya un equipo virtual de VDI (o una compilación única de equipo virtual), es recomendable realizar un backup de dicho equipo virtual para que no se requiera una recompilación completa de dicho equipo virtual.
    - Si es necesario, en lugar de realizar backups de todos los servidores VDI, puede minimizar los costes mediante la configuración manual de una única máquina virtual para realizar backups directamente en el portal de gestión de Azure.

- LA PANTALLA
  - No haga una copia de seguridad del equipo virtual ya que los datos deberían almacenarse en un servidor D1 o TSD1.
  - Tenga en cuenta que algunas aplicaciones almacenan los datos localmente y deben tenerse en cuenta consideraciones especiales si este es el caso.
  - En caso de fallo de una máquina virtual, es posible integrar un nuevo equipo virtual mediante el procedimiento de clonación de otro. En caso de que sólo exista un VM de TS, es recomendable realizar una copia de seguridad para que no se requiera una reconstrucción completa de ese equipo virtual.
  - Si es necesario, en lugar de realizar backups de todos los servidores TS, los costes pueden minimizarse configurando manualmente un único equipo virtual para realizar backups directamente en el portal de gestión de Azure.
- TSData
  - Backup con 7 copias de seguridad diarias, 5 semanales y 2 mensuales. Aumente los períodos de retención en función de los requisitos del negocio.

- Las políticas se pueden configurar para realizar backups diarios o semanales; Azure no admite programaciones más frecuentes.
- En el caso de las programaciones diarias, introduzca la hora preferida para realizar el backup. En el caso de las programaciones semanales, introduzca el día y la hora preferidos para llevar a cabo el backup. Nota: Si se configura la hora exactamente a las 12:00 am, se pueden generar problemas en Azure Backup, de modo que se recomienda hacerlo a las 12:01 am.
- Definir cuántos backups diarios, semanales, mensuales y anuales debe conservarse.

Configuración de los valores predeterminados de la implementación

[]

Para configurar el backup de Azure en toda la implementación, siga estos pasos:

1. Desplácese hasta la página de detalles implementaciones, seleccione Backup Defaults
2. Seleccione un tipo de servidor en el menú desplegable. Los tipos de servidor son:

```
Data: these are for LOB/database server types
Infrastructure: these are platform servers
Power User: these are for Users with a TS server dedicated solely to
them
TS: these are terminal servers that Users launch sessions on
TSData: these are servers doubling as terminal and data servers.
```

   - Esto definirá los ajustes de backup globales para toda la puesta en marcha. Si lo desea, pueden anularse y establecerse en un nivel específico del servidor.
3. Haga clic en la rueda de configuración y, a continuación, en la ventana emergente Editar que aparece.
4. Seleccione los siguientes ajustes de backup:

```
On or off
Daily or weekly
What time of day backups take place
How long each backup type (daily, weekly, etc.) should be retained
```

5. Por último, haga clic en Crear (o Editar) Programación para establecer esta configuración.

Configurar políticas de backup individuales

Para aplicar la configuración de copia de seguridad integrada específica del servidor, desplácese a una página de detalles de Workspace.

1. Desplácese hasta la sección servidores y haga clic en el nombre de un servidor
2. Haga clic en Add Schedule
3. Aplique la configuración de copia de seguridad como desee y haga clic en Crear programación

Restaurar a partir de un backup

Para restaurar las copias de seguridad de un equipo virtual determinado, comience por navegar a esa página de detalles de Workspace.

1. Desplácese hasta la sección servidores y haga clic en el nombre de un servidor
2. Desplácese hacia abajo hasta la sección copias de seguridad y haga clic en la rueda para expandir las opciones y, a continuación, seleccione cualquiera de las dos opciones
3. Restaurar en servidor o Restaurar en disco (asociar una unidad del backup para que pueda copiar los datos del backup a la versión existente de la máquina virtual).
4. Continúe con la restauración desde este punto como lo haría en cualquier otro escenario de restauración.

Los costes dependen de la programación que desee mantener y se basa por completo en el coste de backup de Azure. Los precios del backup para las máquinas virtuales se encuentran en la Calculadora de coste de Azure: https://azure.microsoft.com/en-us/pricing/calculator/

Clonar máquinas virtuales

Descripción general

Virtual Desktop Service (VDS) permite clonar una máquina virtual existente. Esta funcionalidad se ha diseñado para aumentar automáticamente la disponibilidad de recuento de unidades del servidor a medida que aumenta el número de usuarios definido O crece el número de servidores adicionales a los pools de recursos disponibles.

Los administradores usan el clonado en VDS de dos formas:

1. Creación automatizada bajo demanda de un nuevo servidor desde un servidor cliente existente
2. Creación automática proactiva de nuevos servidores cliente para la ampliación automática de recursos basada en reglas definidas y controladas por los socios

Clonado para agregar servidores compartidos adicionales

Un clon es una copia de un equipo virtual existente. La funcionalidad de clonado ahorra tiempo y ayuda a los administradores a escalar porque la instalación de un sistema operativo invitado y las aplicaciones puede requerir mucho tiempo. Con los clones, puede realizar muchas copias de un equipo virtual desde un único proceso de instalación y configuración. Normalmente tiene el aspecto siguiente:

1. Instale todas las aplicaciones y configuraciones deseadas en un servidor TS o TSD
2. Vaya a: Áreas de trabajo > Sección servidores > icono de engranaje para el servidor de origen > haga clic en Clonar
3. Permitir que se ejecute el proceso de clonación (normalmente 45-90 minutos)
4. En el paso final, active el servidor clonado, situándolo en el pool RDS para aceptar conexiones nuevas. Los servidores clonados pueden requerir configuración individual después de clonarse, de modo que VDS espera a que el administrador gire manualmente el servidor.

Repita tantas veces como sea necesario.[]

Para aumentar la capacidad de los usuarios en un entorno de host de sesión compartida, clonar un host de sesión es un proceso sencillo que requiere tan solo unos pasos.

1. Seleccione un host de sesión que clonar, compruebe que ningún usuario haya iniciado sesión actualmente en el equipo.
2. En VDS, desplácese al espacio de trabajo del cliente de destino. Desplácese hasta la sección Servers, haga clic en el icono Gear y seleccione Clone. Este proceso tarda mucho tiempo y desconecta la máquina de origen. Se tardan más de 30 minutos en finalizar.

   [] []

3. El proceso cerrará el servidor, clonará el servidor en otra imagen y Sysprep la imagen en la siguiente TS# para el cliente. El servidor se muestra como *Type=preconfigurado* y *Status=Activation Required* en la lista servidores.

   []

4. Inicie sesión en el servidor y compruebe que el servidor está listo para la producción.

   []

5. Cuando esté listo, haga clic en Activar para agregar el servidor al grupo de host de sesión para comenzar a aceptar conexiones de usuario.

   []

Definición del proceso de clonación de VDS

El proceso paso a paso se detalla en VDS > Deployment > Task History en cualquier operación de Clone Server. El proceso tiene más de 20 pasos, que comienzan con el acceso al hipervisor para iniciar el proceso de clonación y finaliza con la activación del servidor clonado. El proceso de clonación incluye los siguientes pasos clave, como:

- Configure DNS y establezca el nombre del servidor
- Asigne StaticIP

- Agregar a dominio
- Actualizar Active Directory
- Actualizar base de datos VDS (instancia de SQL en CWMGR1)
- Cree reglas de firewall para el clon

Además del Historial de tareas, los pasos detallados para cualquier proceso de clonación se pueden ver en el registro CwVmAutomationService en CWMGR1 en la implementación de escritorios virtuales de cada partner. Se documenta la revisión de estos archivos de registro "aquí".

Creación automatizada de nuevos servidores

Esta funcionalidad VDS está diseñada para aumentar automáticamente la disponibilidad de recuento de unidades de servidor conforme aumenta el número de usuarios definido.

El partner define y gestiona mediante VDS ("") > Cliente > Descripción general – Recursos de equipos virtuales > escala automática. Se exponen varios controles para permitir a los partners habilitar/deshabilitar el escalado automático, así como crear reglas personalizadas para cada cliente como: Número/usuarios/servidor, RAM adicional por usuario y número de usuarios por CPU.

Arriba asume que la clonación automatizada está activada para toda la implementación de escritorios virtuales. Por ejemplo, para detener la clonación automática, utilice DCConfig, en la ventana Avanzado, desactive la opción creación del servidor→clonación automatizada activada.

¿Cuándo se ejecuta el proceso de clonación automatizada?

El proceso de clonación automatizado se ejecuta cuando se configura el mantenimiento diario para que se ejecute. El valor predeterminado es medianoche, pero se puede editar. Parte del mantenimiento diario consiste en ejecutar el subproceso Change Resources para cada pool de recursos. El subproceso Change Resources determina el número de servidores compartidos necesarios en función del número de usuarios que la configuración del grupo requiere (personalizable; puede ser de 10, 21, 30, etc. usuarios por servidor).

Creación automatizada de un nuevo servidor "bajo demanda"

Esta funcionalidad VDS permite la clonación automatizada “bajo demanda” de servidores adicionales a grupos de recursos disponibles.

El administrador de VDS inicia sesión en VDS y, en los módulos de organizaciones o áreas de trabajo, busca el cliente específico y abre la ficha Descripción general. En el mosaico de servidores se enumeran todos los servidores (TSD1, TS1, D1, etc.). Para clonar cualquier servidor individual, simplemente haga clic en el botón que se encuentra a la derecha del nombre del servidor y seleccione Clone Option.

Normalmente, el proceso debe tardar aproximadamente una hora. Sin embargo, la duración depende del tamaño de la máquina virtual y de los recursos disponibles del hipervisor subyacente. Tenga en cuenta que el servidor que se clona deberá reiniciarse, por lo que los partners normalmente realizan después de horas o durante una ventana de mantenimiento programada.

Al clonar un servidor TSData, uno de los pasos es eliminar las carpetas c:\Home, c:\Data y c:\Pro para que no sean archivos duplicados. En este caso, se ha producido un error en el proceso de clonado, pero se han producido problemas al eliminar estos archivos. Este error es vago. Normalmente, esto significa que el evento del clon ha fallado porque hay un archivo o proceso abierto. A continuación, desactive cualquier AV (ya que podría explicar este error).

Función de aumento automático del espacio en disco

Descripción general

NetApp reconoce la necesidad de proporcionar a los administradores un método sencillo para asegurarse de que los usuarios siempre tienen espacio para acceder a los documentos y guardarlos. Esto también garantiza que las máquinas virtuales tengan suficiente espacio libre para completar los backups correctamente, lo que permite a los administradores y sus planes de recuperación ante desastres y continuidad del negocio. Teniendo esto en cuenta, creamos una función que amplía automáticamente el disco gestionado en uso hasta el siguiente nivel cuando una unidad se queda sin espacio.

Se trata de un valor que se aplica de forma predeterminada en todas las nuevas implementaciones de VDS en Azure, lo que garantiza que todas las implementaciones protejan a los usuarios y las copias de seguridad del inquilino de forma predeterminada.

Los administradores pueden validar que esto está en su sitio navegando a la ficha implementaciones y, a continuación, seleccionando una implementación y, a continuación, conectando con su servidor CWMGR1 desde allí. A continuación, abra el acceso directo DCConfig en el escritorio y haga clic en Avanzado y desplácese hacia abajo hasta la parte inferior.

[]

Los administradores pueden cambiar la cantidad de espacio libre que se desea en GB libre o el porcentaje de la unidad que debe estar libre antes de pasar al siguiente nivel de discos administrados en la misma sección Avanzado de DCConfig.

[]

Algunos ejemplos prácticos de aplicación:

- Si desea asegurarse de que hay al menos 50 GB disponibles en su unidad, establezca MinFreeSpaceGB en 50
- Si desea asegurarse de que al menos el 15% de su unidad es gratuita, establezca MinFreeSpacePercent de 10 a 15.

Esta acción tiene lugar a medianoche en la zona horaria del servidor.

Acceso a credenciales de VDS en el almacén de claves de Azure

Descripción general

CWASetup 5.4 se diferencia de los métodos de implementación anteriores de Azure. El proceso de configuración y validación se ha optimizado para reducir la cantidad de información necesaria para iniciar una puesta en marcha. Muchos de estos mensajes eliminados son para credenciales o cuentas como administrador de máquina virtual local, cuenta SMTP, cuenta técnica, SQL SA, etc. Estas cuentas ahora se generan y almacenan automáticamente en un almacén de claves de Azure. De forma predeterminada, el acceso a estas cuentas generadas automáticamente requiere un paso adicional, que se describe a continuación.

- Encuentre el recurso "Key vault" y haga clic en él:

[anchura = 75%]

- En ‘Configuración’, haga clic en ‘Ajustes’. Verá un mensaje que indica que no está autorizado a ver:

  [anchura = 75%]

- Agregue una ‘Directiva de acceso’ para conceder acceso a una cuenta de Azure AD (como un administrador global o un administrador del sistema) a estas claves confidenciales:

  [anchura = 75%]

- En este ejemplo se usa un administrador global. Después de seleccionar el principal, haga clic en ‘Seleccionar’ y, a continuación, en ‘Agregar’:

  [anchura = 75%]

- Haga clic en ‘Guardar’:

  [anchura = 75%]

- La directiva de acceso se ha agregado correctamente:

  [anchura = 75%]

- Vuelva a visitar los ‘elementos’ para comprobar que la cuenta ahora tiene acceso a las cuentas de implementación:

  [anchura = 75%]

- Por ejemplo, si necesita que la credencial del administrador de dominio inicie sesión en CWMGR1 y actualice la directiva de grupo, compruebe las cadenas en cjDomainAdministratorName y cjDomainAdministratorPassword haciendo clic en cada entrada:

  [anchura = 75%]

  [anchura = 75%]

- Mostrar o copiar el valor:

  [anchura = 75%]

Aplicar Control y antivirus

Descripción general

Los administradores de Virtual Desktop Service (VDS) son responsables de supervisar tanto la infraestructura de su plataforma (que consistirá en CWMGR1 como mínimo) como el resto de las infraestructuras y máquinas virtuales (VM). En la mayoría de los casos, los administradores organizan la supervisión de la infraestructura (hipervisor/SAN) directamente con su proveedor de centro de datos/IaaS. Los administradores son responsables de supervisar los servidores de terminal y los servidores de datos, normalmente mediante la implementación de su solución de gestión y supervisión remotas preferida (RMM).

Antivirus es responsabilidad del administrador (tanto para infraestructuras de plataforma como para equipos virtuales de terminal o servidor de datos). Para simplificar este proceso, los servidores VDS para Azure han

aplicado Windows Defender de forma predeterminada.

> Al instalar soluciones de terceros, asegúrese de no incluir Firewalls ni cualquier otro componente que pueda interferir con la automatización VDS.

Más específicamente, cuando se aplican de forma predeterminada políticas antivirus muy específicas, esto puede provocar efectos adversos cuando estos agentes antivirus se instalan en un servidor gestionado por Virtual Desktop Service.

Nuestra guía general es que aunque la automatización de la plataforma VDS generalmente no se ve afectada por los productos antivirus o antimalware, es una práctica recomendada agregar excepciones/exclusiones para los siguientes procesos en todos los servidores de plataforma (CWMGR1, RDGpuertas de enlace, HTML5Gpuertas de enlace, FTP, etc.):

```
*\paexec.exe
*\paexec_1_25.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CW Automation
Service\cw.automation.service.exe
C:\Program
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Printer.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Services.exe
```

Además, recomendamos que se enumeren de forma segura los siguientes procesos en los servidores cliente:

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe
C:\Program Files\CloudWorkspace\Pen\Pen.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

Añadir y mover unidades asignadas

Descripción general

De forma predeterminada, hay tres carpetas compartidas expuestas a las sesiones del usuario final. Estas carpetas se encuentran en la capa de almacenamiento definida. Esto podría estar en el servidor de archivos (TSD1 o D1) o en un servicio de almacenamiento como Azure Files, Azure NetApp Files, NetApp CVO y NetApp CVS.

Para ayudar con claridad, este artículo utilizará un cliente de ejemplo con el código de compañía “NECA”. En este ejemplo se supone que se ha implementado un único servidor TDS1, denominado NECATSD1. Trabajaremos durante el proceso de mover una carpeta a otra VM (llamada “NECAD1”). Esta estrategia se puede utilizar para moverse entre la partición de la misma máquina o a otra máquina, como se muestra en el ejemplo siguiente…

Ubicación de inicio de carpetas:

- Datos: NECATSD1\C:\data\NECA\ (TSD1significa que es el primer servidor Terminal Server y también funciona como servidor de datos)
- FTP: NECATSD1\C:\FTP\NECA\
- Inicio: NECATSD1\C:\home\NECA\

Ubicación de finalización de carpetas:

- Datos: NECAD1\G:\data\NECA\ (D1significa que es el primer servidor de datos)
- FTP: El mismo proceso se aplica, sin necesidad de describirlo 3x
- Inicio: El mismo proceso se aplica, sin necesidad de describirlo 3x

Agregar disco para G: En NECAD1

1. Para poner la carpeta compartida en la unidad E: Tendremos que añadirla a través del hipervisor (por ejemplo, el portal de administración de Azure) y, a continuación, inicializarla y formatearla

   []

2. Copie la carpeta existente (en la ruta NECATSD1, C:\) a la nueva ubicación (en NECAD1, G:\)
3. Copie las carpetas de la ubicación original en la nueva ubicación.

   []

Recopilar información del recurso compartido de carpetas original (NECATSD1, C:\data\NECA\)

1. Comparta la nueva carpeta con la misma ruta de acceso que la carpeta en la ubicación original.
2. Abra la nueva carpeta NECAD1, G:\data\ y verá una carpeta denominada código de empresa, “NECA” en nuestro ejemplo.

   []

3. Tenga en cuenta los permisos de seguridad del recurso compartido de carpeta original:

   []

4. Esta es la configuración típica, sin embargo, es importante copiar la configuración original en caso de que haya personalizaciones existentes que tenemos que conservar. Todos los demás permisos de usuario/grupo deben eliminarse del nuevo recurso compartido de carpetas
   - SISTEMA:todos los permisos permitidos
   - LocalClientDHAccess (en el equipo local):todos los permisos permitidos
   - ClientDHAccess (en el dominio): Todos los permisos permitidos
   - NECA-All users (en el dominio): Todos los permisos excepto “Control total” permitidos

Replicar la ruta de acceso compartida y los permisos de seguridad en la nueva carpeta compartida

1. Vuelva a la nueva ubicación (NECAD1, G:\data\NECA\ y comparta la carpeta NECA con la misma ruta de red (excluyendo la máquina), en nuestro ejemplo “neca-data$”

   []

2. Para que la seguridad del usuario agregue todos los usuarios, defina sus permisos para que coincidan.

   []

3. Elimine cualquier otro permiso de usuario/grupo que ya exista.

   []

Editar directiva de grupo (sólo si la carpeta se ha movido a un equipo nuevo)

1. A continuación, edite Drive Maps en el Editor de administración de directivas de grupo. Para Azure AD Domain Services, la asignación se encuentra en:

   ```
   “Cloud Workspace Users > User Configuration > Preferences > Windows Settings> Drive Maps”
   ```

   []

2. Una vez que se actualice la directiva de grupo, la próxima vez que se conecte cada usuario, verán las unidades asignadas que se redirigen a la nueva ubicación.
3. En este punto puede eliminar las carpetas originales, en NECATSD1, C:\.

Resolución de problemas

Si el usuario final ve las unidades asignadas con una X roja, haga clic con el botón derecho del ratón en la unidad y seleccione desconectar. Cerrar sesión y volver a hacerlo en la unidad aparecerá correctamente.[]

Información de copyright

Información de la marca comercial