Arquitectura

Virtual Desktop Service

NetApp
February 20, 2023

Tabla de Contenido

Arquitectura

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. OraganizationalUnitDistinguishedName 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 Backukp
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

Consideraciones sobre la migración de datos

Descripción general

La migración de datos es un requisito casi universal al migrar a una solución cloud de cualquier tipo. Mientras que los administradores son responsables de la migración de datos a sus escritorios virtuales, la experiencia de NetApp está disponible y ha demostrado ser inestimable para innumerables migraciones de clientes. El entorno de escritorio virtual es simplemente un entorno Windows alojado, por lo que es probable que se acomode cualquier método deseado.

Datos que se migran normalmente:

- Perfiles de usuario (Escritorio, Documentos, Favoritos, etc.)
- Recursos compartidos del servidor de archivos
- Recursos compartidos de datos (datos de aplicaciones, bases de datos, caché de backup)

En el entorno de escritorio virtual existen dos lugares principales donde se almacenan y organizan los datos:

- La unidad de usuario (normalmente H:\): Es la unidad asignada visible para cada usuario.
  - Esto se asigna de nuevo a la ruta <DRIVE>:\home\CustomerCode\user.name\
  - Cada usuario tiene su propia unidad H:\ y no puede ver a otro usuario
- La unidad compartida (normalmente i:\): Es la unidad asignada compartida visible para todos los usuarios
  - Esto se asigna de nuevo a la ruta <DRIVE>:\data\CustomerCode\
  - Todos los usuarios pueden acceder a esta unidad. Su nivel de acceso a carpetas/archivos contenidos se gestiona en la sección carpetas de VDS.

Proceso de migración genérico

1. Replicar datos en el entorno de cloud
2. Mueva los datos a la ruta adecuada para las unidades H:\ e I:\
3. Asigne los permisos adecuados en el entorno de escritorio virtual

Transferencias y consideraciones de FTPS

Migración con FTPS

1. Si la función de servidor FTPS se habilitó durante el proceso de implementación de CWA, recopile las credenciales de FTPS iniciando sesión en VDS, navegando a Informes y ejecutando el informe de cliente maestro de su organización
2. Cargar datos
3. Mueva los datos a la ruta adecuada para las unidades H:\ e I:\
4. Asigne los permisos adecuados en el entorno de escritorio virtual mediante el módulo carpetas

> Al transferir datos a través de FTPS, cualquier interrupción impedirá que los datos se transfieran según lo previsto. Dado que los servidores gestionados por Virtual Desktop Services se reinician todas las noches, es probable que se interrumpa la estrategia de transmisión estándar de una noche a la mañana. Para evitar esto, los administradores pueden habilitar el modo de migración para evitar que se reinicien los equipos virtuales durante 1 semana.

Habilitar el modo de migración es sencillo: Desplácese a la organización y desplácese hasta la sección Configuración de escritorio virtual y marque la casilla de verificación modo de migración y, a continuación, haga clic en Actualizar.

> NetApp recomienda a los administradores habilitar una configuración de cumplimiento que ayude a las organizaciones a cumplir los controles PCI, HIPAA y NIST mediante el endurecimiento de las puertas de enlace de la implementación, etc. Esto también impide que la función predeterminada del servidor FTP, si está habilitada, acepte transmisiones predeterminadas sin cifrar a través del puerto 21. FileZilla no permite SFTP, lo que significa que las conexiones deben realizarse con FTPS en el puerto 990.

Para habilitar esta configuración, conéctese a CWMGR1 y navegue hasta el programa CwVmAutomationService y, a continuación, habilite el cumplimiento de PCI v3.

Herramientas y consideraciones de sincronización

Enterprise File Sync y Share, a menudo conocidas como herramientas EFSS o SYNC, pueden ser extremadamente útiles en la migración de datos, ya que la herramienta capturará los cambios en cada lado hasta la transición. Herramientas como OneDrive, que viene con Office 365, pueden ayudarle a sincronizar datos del servidor de archivos. También resulta útil para puestas en marcha de usuarios de VDI, donde existe una relación 1:1 entre el usuario y el equipo virtual, siempre y cuando el usuario no intente sincronizar contenido compartido en su servidor VDI cuando los datos compartidos se pueden poner en marcha una vez en el compartido (normalmente yo:\) impulse el uso de toda la organización. Migración de SQL y datos similares (Archivos abiertos)

Las soluciones comunes de sincronización y migración no transfieren archivos abiertos, lo que incluye tipos de archivo como:

- Archivos del buzón (.ost)
- Archivos de QuickBooks
- Archivos de Microsoft Access
- Bases de datos de SQL

Esto significa que si un único elemento de todo el archivo (aparece 1 correo electrónico nuevo, por ejemplo) o base de datos (se introduce 1 registro nuevo en el sistema de una aplicación), el archivo completo es diferente y las herramientas de sincronización estándar (Dropbox, por ejemplo) pensará que es un archivo completamente nuevo y necesita ser movido de nuevo. Si lo desea, existen herramientas especializadas

disponibles para su compra a proveedores externos.

Otra forma en que se gestionan estas migraciones es mediante el acceso a VAR de terceros, que a menudo han simplificado la importación y exportación de bases de datos.

Unidades de transporte

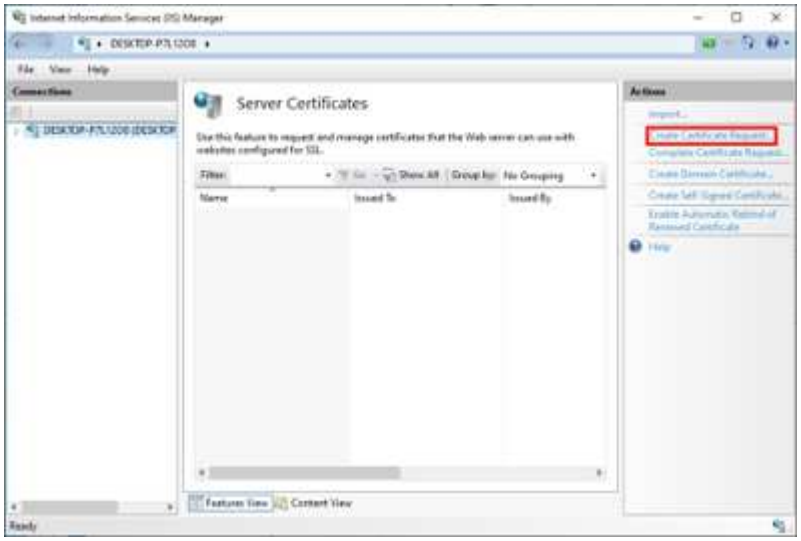
Muchos proveedores de centros de datos ya no incluyen unidades de disco duro, ni eso, ni requieren que siga sus políticas y procedimientos específicos.

Microsoft Azure permite a las organizaciones utilizar Azure Data Box, que los administradores podrán aprovechar mediante la coordinación con sus representantes de Microsoft.

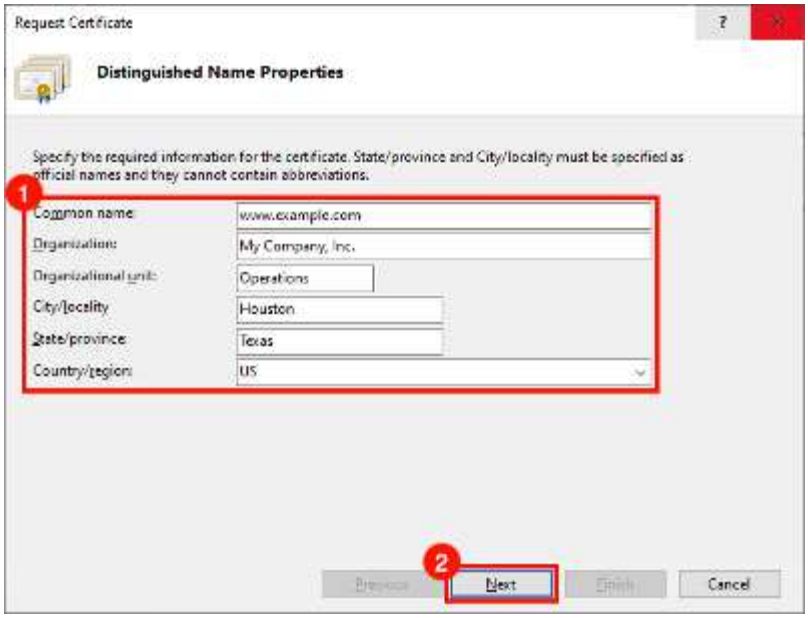
Proceso de renovación del certificado SSL comodín

Cree una solicitud de firma de certificación (CSR):

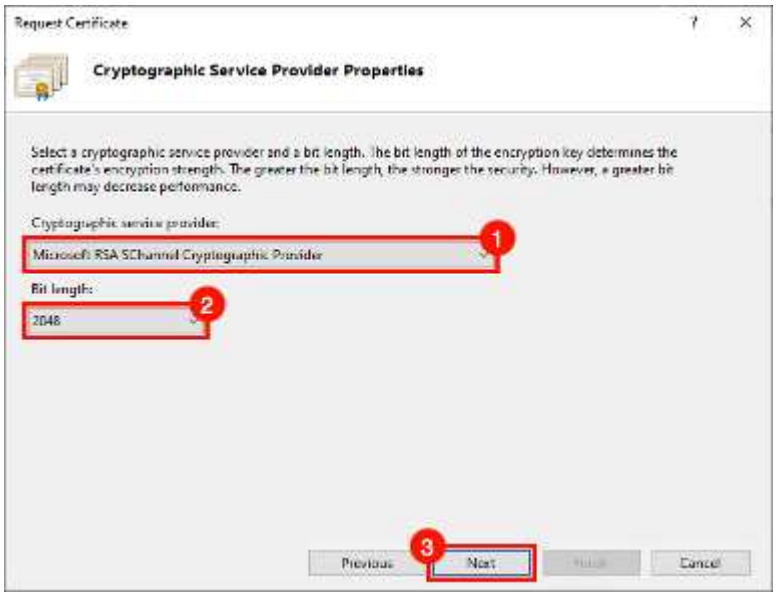
1. Conecte a CWMGR1
2. Abra el Administrador de IIS desde Herramientas de administrador
3. Seleccione CWMGR1 y abra certificados de servidor
4. Haga clic en Crear solicitud de certificado en el panel acciones



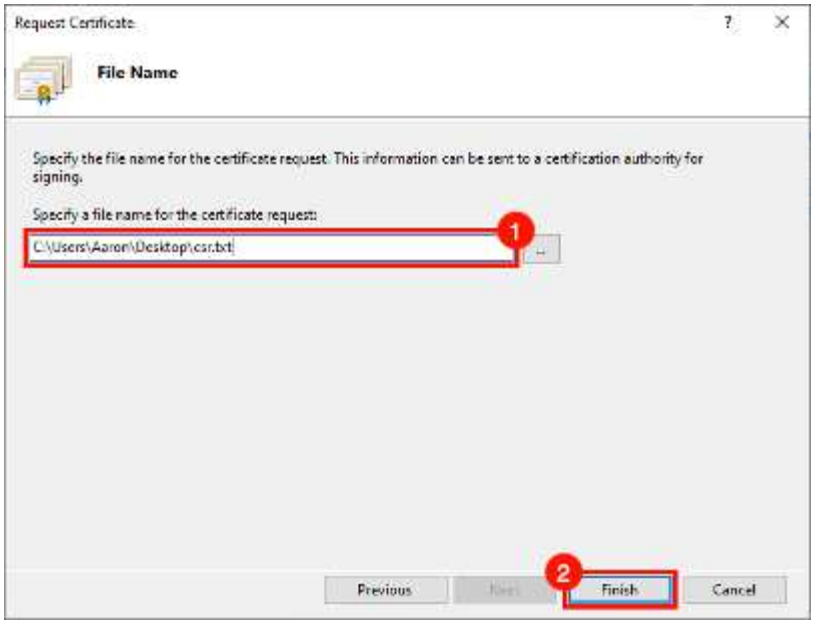
5. Rellene las propiedades de nombre completo en el Asistente para solicitar certificado y haga clic en Siguiente:
   a. Nombre común: FQDN de comodín - *.domain.com
   b. Organización: Nombre legalmente registrado de su empresa
   c. Unidad organizativa: «Funciona bien»
   d. Ciudad: Ciudad donde se encuentra la empresa
   e. Estado: Estado donde se encuentra la empresa
   f. País: País donde se encuentra la empresa



6. En la página Propiedades del proveedor de servicios de cifrado, compruebe que aparece lo siguiente y haga clic en Siguiente:



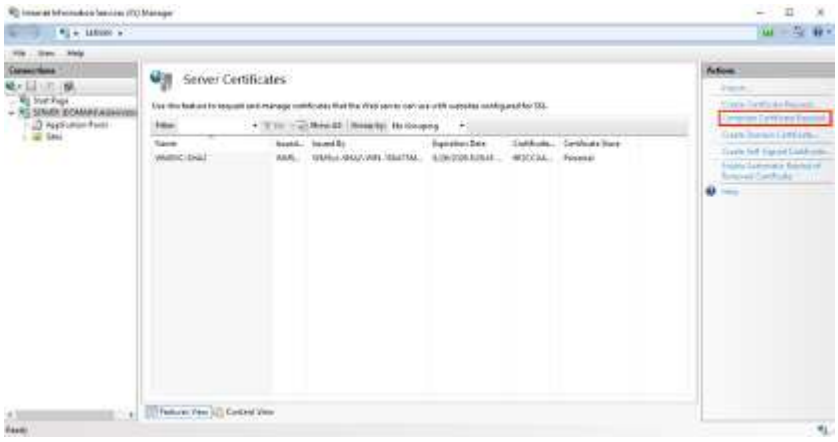
7. Especifique un nombre de archivo y busque la ubicación en la que desea guardar la CSR. Si no especifica una ubicación, la CSR estará en C:\Windows\System32:



8. Haga clic en Finalizar cuando termine. Usted utilizará este archivo de texto para enviar su pedido al registrador de certificados
9. Póngase en contacto con el apoyo del registrador para comprar un nuevo comodín SSL para su certificado: *.domain.com
10. Después de recibir el certificado SSL, guarde el archivo .cer de certificado SSL en una ubicación de CWMGR1 y siga los pasos que se indican a continuación.

Instalación y configuración de CSR:

1. Conecte a CWMGR1
2. Abra el Administrador de IIS desde Herramientas de administrador
3. Seleccione CWMGR1 y abra ‘certificados del servidor’
4. Haga clic en completar solicitud de certificado en el panel acciones



5. Complete los campos siguientes en la solicitud de certificado completa y haga clic en Aceptar:

a. Nombre de archivo: Seleccione el archivo .cer que se guardó anteriormente

b. Nombre descriptivo: *.domain.com

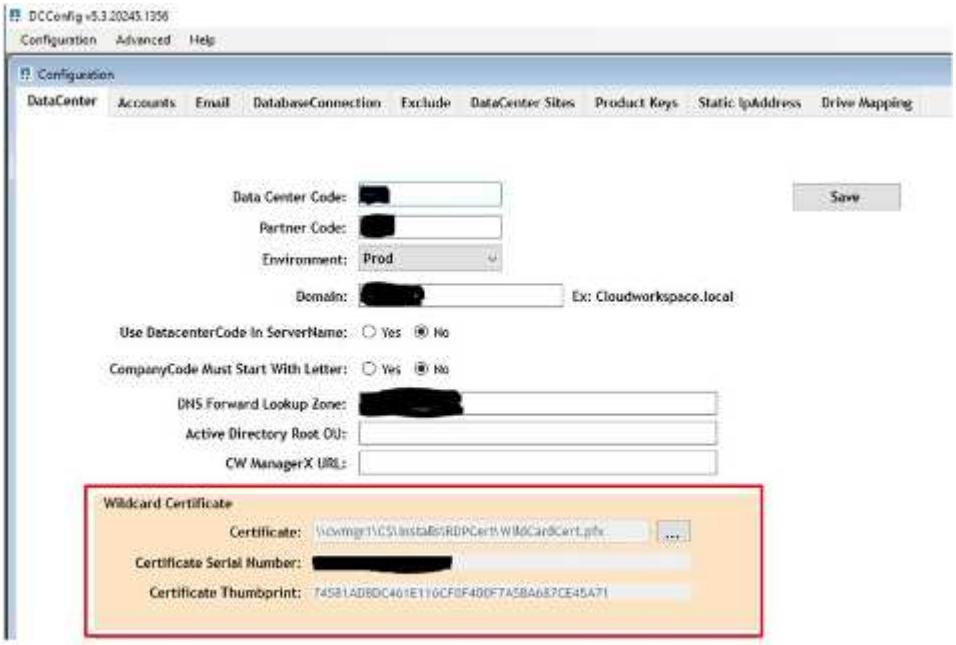
c. Almacén de certificados: Seleccione Web Hosting o personal

Asignando certificado SSL:

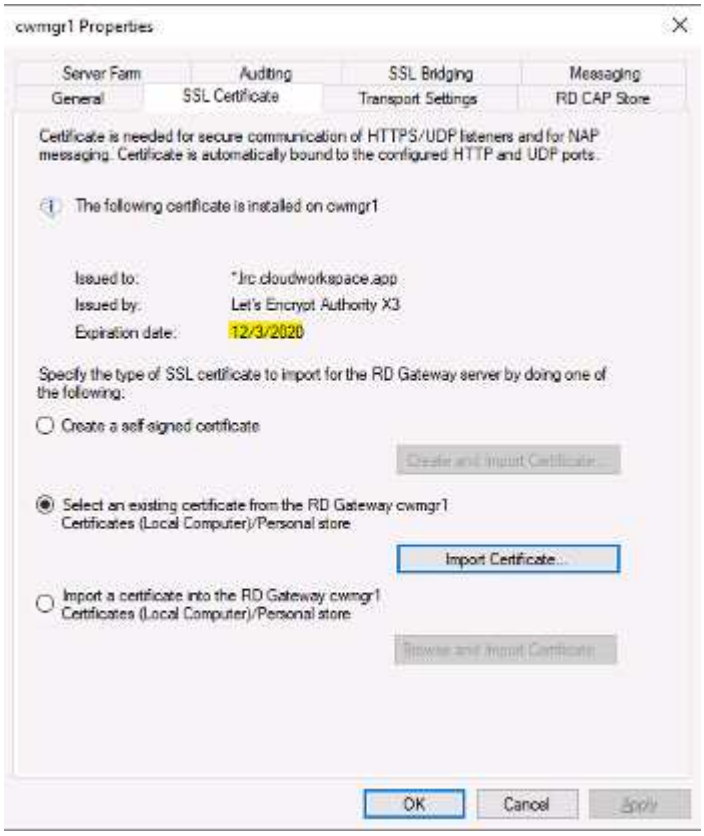
1. Compruebe que el modo de migración no está habilitado. Esto se puede encontrar en la página Resumen de área de trabajo, en Configuración de seguridad en VDS.

2. Conecte a CWMGR1
3. Abra el Administrador de IIS desde Herramientas de administrador
4. Seleccione CWMGR1 y abra ‘certificados del servidor’
5. Haga clic en Exportar en el panel acciones
6. Exporte el certificado en formato .pfx
7. Cree una contraseña. Almacene la contraseña tal y como será necesario para importar o volver a utilizar el archivo .pfx en el futuro
8. Guarde el archivo .pfx en el directorio C:\instals\RDPcert
9. Haga clic en Aceptar y cierre el Administrador de IIS

10. Abra DCConfig
11. En Certificado comodín, actualice la ruta de acceso del certificado al nuevo archivo .pfx
12. Introduzca la contraseña .pfx cuando se le solicite
13. Haga clic en Guardar



14. Si el certificado es válido durante 30 días más, permita que la automatización aplique el nuevo certificado durante la tarea de acciones diarias de la mañana durante toda la semana
15. Compruebe periódicamente los servidores de la plataforma para verificar que el nuevo certificado se ha propagado. Valide y pruebe la conectividad de usuarios para confirmar.
    a. En el servidor, vaya a Herramientas de administración
    b. Seleccione Servicios de Escritorio remoto > Administrador de puerta de enlace de Escritorio remoto
    c. Haga clic con el botón derecho del ratón en el nombre del servidor de puerta de enlace y seleccione Propiedades. Haga clic en la ficha Certificado SSL para revisar la fecha de caducidad

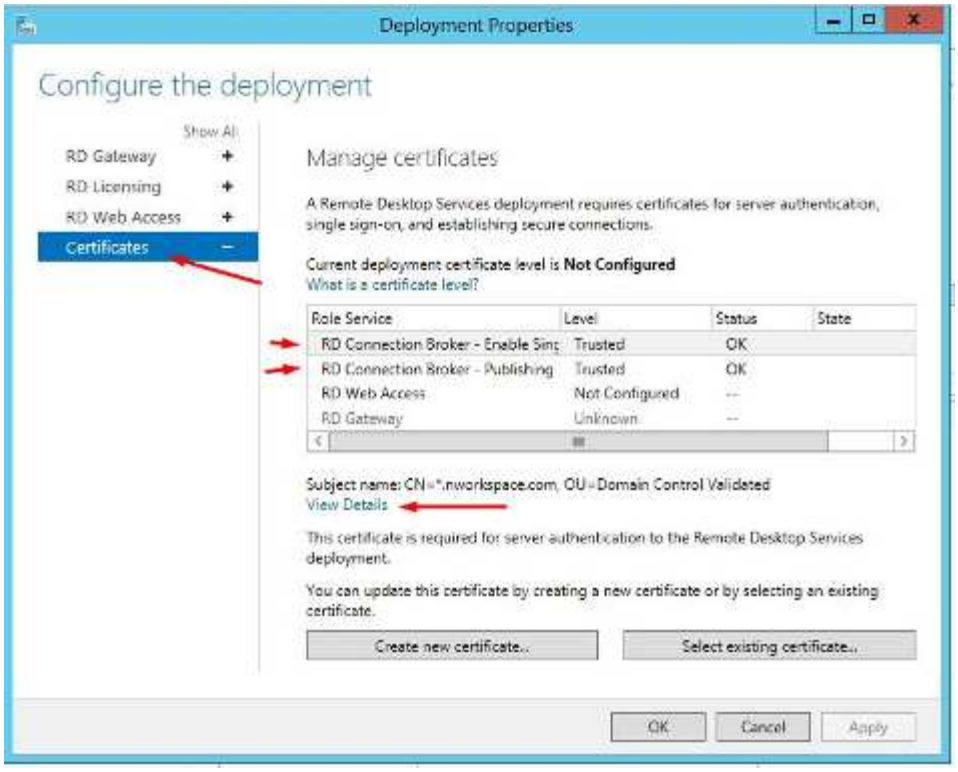


16. Compruebe periódicamente las máquinas virtuales del cliente que ejecutan la función Connection Broker

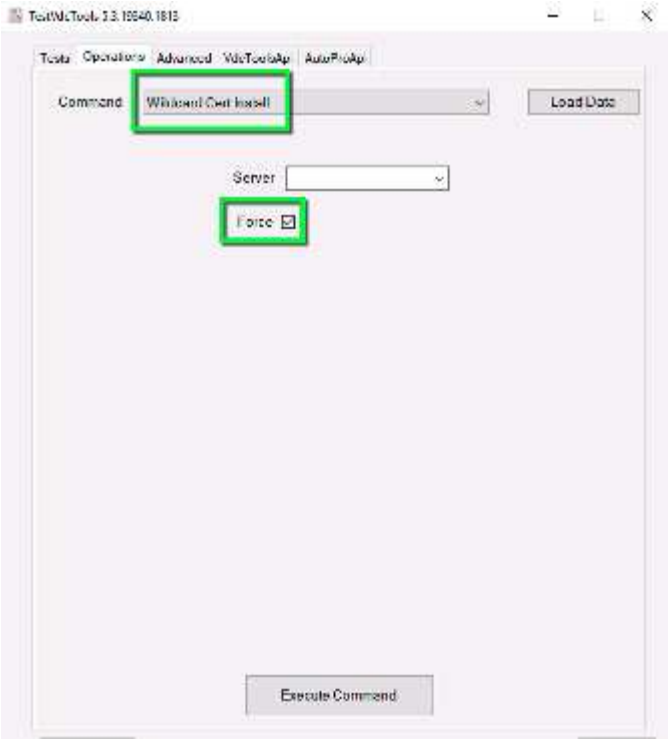
    a. Vaya a Administrador de servidores > Servicios de Escritorio remoto

    b. En Resumen de la implementación, seleccione la lista desplegable tareas y seleccione Editar propiedades de la implementación

    c. Haga clic en certificados, seleccione certificado y haga clic en Ver detalles. Se mostrará la fecha de caducidad.



17. Si tiene menos de 30 días o prefiere extraer el nuevo certificado inmediatamente, fuerce la actualización con TestVdcTools. Esto se debe realizar durante una ventana de mantenimiento, ya que se perderá la conectividad de los usuarios que hayan iniciado sesión y la conexión con CWMGR1.
    a. Vaya a C:\Archivos de programa\CloudWorkspace\TestVdcTools, haga clic en la ficha Operaciones y seleccione el comodín comando Cert-Install
    b. Deje el campo servidor en blanco
    c. Active la casilla Fuerza
    d. Haga clic en Ejecutar comando
    e. Verifique que el certificado se propaga con los pasos indicados anteriormente



Guía de Teardown AVD

Descripción general

Este artículo trata la eliminación de VDS y el control de NetApp a la vez que se mantiene el acceso de los usuarios finales de AVD. La gestión futura sería con las herramientas de administración nativas de Azure/Windows. Una vez completado este proceso, se recomienda contactar con support@spotpc.netapp.com para que NetApp pueda limpiar nuestros sistemas de back-end y facturación.

Estado inicial

- Implementación de AVD
- TDS1 es FS Logix fileshare
- TS1 es Host de sesión
- El usuario ha iniciado sesión y se ha creado el disco FS Logix en:

```
\\****TSD1\****-Pro$\ProfileContainers (**** = Unique Company Code)
```

Eliminar el servicio del agente CW

El agente CW se ejecuta en todas las máquinas del entorno. El servicio que inicia este proceso debe desinstalarse con el siguiente comando en cada VM del entorno. CWMGR1 se puede omitir ya que esa VM se apagará y finalmente se eliminará en la mayoría de los casos. Lo ideal sería ejecutar esta acción a través de la automatización basada en scripts. El siguiente vídeo muestra que se ha realizado manualmente.

```
C:\Program files\CloudWorkspace\CwAgent\CwAgent.exe -u
```

Eliminar el vídeo del servicio del agente CW

[] | *https://img.youtube.com/vi/l9ASmM5aap0/maxresdefault.jpg*

Eliminar directorio de agente CW

La desinstalación anterior quitó el servicio que inicia CW Agent pero los archivos permanecen. Eliminar el directorio:

```
"C:\Program Files\CloudWorkspace"
```

Eliminar vídeo del directorio del agente CW

[] | *https://img.youtube.com/vi/hMM_z4K2-il/maxresdefault.jpg*

Quitar accesos directos de inicio

El directorio de elementos de inicio contiene dos accesos directos a los archivos eliminados en el paso anterior. Para evitar los mensajes de error del usuario final, estos archivos deben eliminarse.

```
"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Pen.lnk"
"C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\StartUp\CwRemoteApps.lnk"
```

Eliminar vídeo de accesos directos de inicio

[] | *https://img.youtube.com/vi/U0YLZ3Qfu9w/maxresdefault.jpg*

Desenlazar los GPO de ‘usuarios’ y ‘Empresas’

Hay tres GPO implementados por VDS. Recomendamos desvincular dos de ellos y revisar el contenido del tercero.

Desvincular:

- Usuarios de ADDC > Empresas de Cloud Workspace
- Usuarios de ADDC > usuarios de Cloud Workspace

Revisión:

- Equipos AADDC > equipos de Cloud Workspace

Desenlazar vídeo de GPO de ‘usuarios’ y ‘Empresas’

[] | *https://img.youtube.com/vi/cb68ri3HKUw/maxresdefault.jpg*

Cierre CWMGR1

Con los cambios de GPO aplicados, ahora podemos apagar el equipo virtual CWMGR1. Una vez confirmada la función AVD continua, esta VM se puede eliminar permanentemente.

En casos extremadamente raros, es necesario mantener este equipo virtual si se está ejecutando otra función de servidor (p. ej., DC, servidor FTP…). En ese caso, se pueden deshabilitar tres servicios para deshabilitar la funcionalidad VDS en CWMGR1:

- Agente CW (ver arriba)
- CW Automation Service
- Automatización de CW VM

Vídeo de apagado de CWMGR1

[] | *https://img.youtube.com/vi/avk9HyIiC_s/maxresdefault.jpg*

Elimine cuentas de servicios VDS de NetApp

Es posible quitar las cuentas de servicio de Azure AD que utiliza VDS. Inicie sesión en Azure Management Portal y elimine a los usuarios:

- CloudWorkspaceSVC
- CloudWorkspaceCASVC

Se pueden conservar otras cuentas de usuario:

- Usuarios finales
- Administrador de Azure
- administradores de dominio .tech

Elimine el vídeo de cuentas de servicio VDS de NetApp

[] | *https://img.youtube.com/vi/_VToVNp49cg/maxresdefault.jpg*

Eliminar registros de aplicaciones

Al implementar VDS, se realizan dos registros de aplicaciones. Se pueden eliminar:

- API de espacio de trabajo en cloud
- Área de trabajo en la nube AVD

Eliminar vídeo de registros de aplicaciones

[] | *https://img.youtube.com/vi/iARz2nw1Oks/maxresdefault.jpg*

Eliminar aplicaciones empresariales

Al implementar VDS, se implementan dos aplicaciones empresariales. Se pueden eliminar:

- Espacio de trabajo en cloud

- API de gestión de área de trabajo en la nube

Elimine el vídeo de las aplicaciones empresariales

[] | *https://img.youtube.com/vi/3eQzTPdilWk/maxresdefault.jpg*

Confirme que el CWMGR1 está detenido

Antes de comprobar que los usuarios finales aún pueden conectarse, confirme que el CWMGR1 está detenido para realizar una prueba realista.

Confirme que el vídeo de CWMGR1 está detenido

[] | *https://img.youtube.com/vi/Ux9nkDk5lU4/maxresdefault.jpg*

Inicio de sesión y usuario final

Para confirmar que se ha realizado correctamente, inicie sesión como usuario final y confirme que se mantiene la funcionalidad.

Inicio de sesión y vídeo para el usuario final

[] | *https://img.youtube.com/vi/SuS-OTHJz7Y/maxresdefault.jpg*