Gestión

Virtual Desktop Service

NetApp
February 20, 2023

Tabla de Contenido

Gestión

Implementaciones

Colecciones de aprovisionamiento

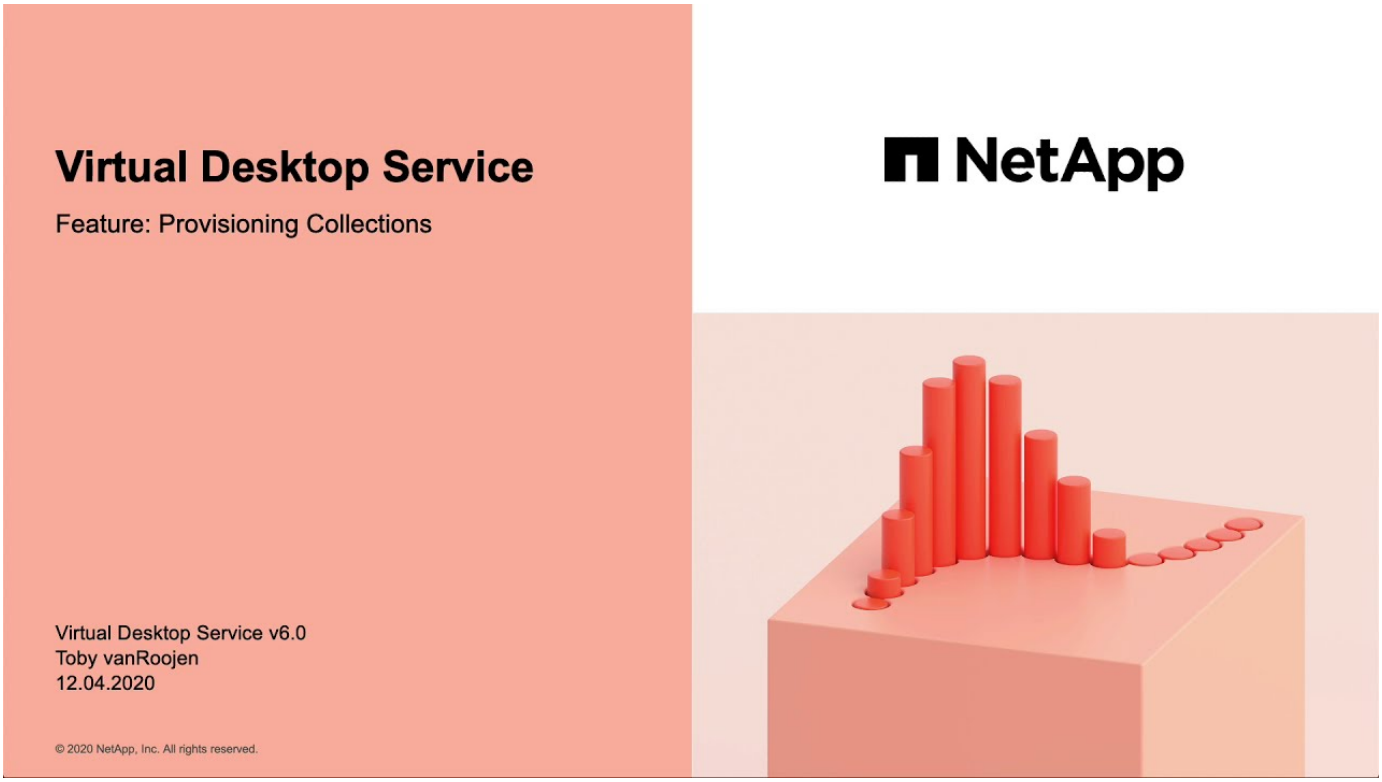
Descripción general

Provisioning Collections es una función de VDS relacionada con la creación y gestión de imágenes de VM.

En un nivel elevado, el flujo de trabajo de la recopilación de aprovisionamiento es el siguiente:

1. Se crea un equipo virtual temporal (por ejemplo, "CWT1") basado en una imagen existente (ya sea una imagen en stock o una colección de aprovisionamiento guardada previamente).
2. El administrador de VDS personaliza la máquina virtual temporal para que se ajuste a sus requisitos usando "Eventos programados", "Conéctese al servidor" o herramientas de gestión de terceros.
3. Una vez personalizado, el administrador de VDS hace clic en **Validar** y activa un proceso de validación que automatiza la finalización de la imagen, ejecutando Sysprep, eliminando la VM temporal y haciendo que la imagen esté disponible para su implementación en VDS.

Demostración de vídeo: Gestión de imágenes de máquinas virtuales para hosts de sesiones de VDI



Aprovisionamiento de tipos de colecciones

Hay dos tipos distintos de colección con casos de uso específicos, ***Shared*** y ***VDI***.

Compartido

El tipo ***Shared*** es una colección de imágenes de VM diseñadas para implementar un entorno completo con

varias imágenes de VM distintas y funciones de VM distintas.

VDI

El tipo ***VDI*** es una única imagen de VM diseñada para ser utilizada y reutilizada para implementar varias VM idénticas, normalmente usadas para alojar sesiones de usuario. Para todos los tipos de hosts de sesiones AVD, se debe seleccionar el tipo *VDI*, incluso para los hosts que ejecutan varias sesiones por VM.

Crear una nueva colección de aprovisionamiento

Las colecciones de aprovisionamiento se encuentran en la interfaz VDS de cada implementación, en la subpestaña ***Provisioning Collections***.

[anchura = 75%]

Para crear una nueva colección

1. Haga clic en el botón ***+ Agregar colección***.
2. Complete los siguientes campos:
    a. **Nombre**
    b. **Descripción** (opcional)
    c. **Tipo** - compartido o VDI
    d. **Sistema operativo**
    e. **Share Drive**: Si esta VM se utilizará para alojar perfiles de usuarios o datos compartidos de la empresa, elija la letra de unidad en la que se alojará. Si no es así, déjelo como "C"
    f. **Caché mínima**: SI usted y VDS crean equipos virtuales para la implementación instantánea, especifique el número mínimo de equipos virtuales en caché que deben mantenerse. Si poner en marcha nuevas máquinas virtuales puede esperar tanto tiempo como necesite el hipervisor para crear una máquina virtual, esta puede configurarse en «0» para ahorrar costes.
    g. **Agregar servidores**
        i. **Función** (si se ha seleccionado el tipo "compartido")
            A. **TS**: Este equipo virtual sólo actuará como host de sesión
            B. **Datos**: Este equipo virtual no alojará ninguna sesión de usuario
            C. **TSData**: Este equipo virtual será tanto el host de sesión como el host de almacenamiento (máximo: Un TSData por espacio de trabajo)
        ii. **VM Template** - Seleccione en la lista disponible, tanto las imágenes de hipervisor en stock como las colecciones de aprovisionamiento guardadas anteriormente están disponibles para seleccionar.
            A. NOTA: Las imágenes de Windows 7 de Azure Marketplace no tienen habilitada la opción Remoting de PowerShell. Para utilizar una imagen de Windows 7, deberá proporcionar una imagen personalizada en la galería de imágenes compartida con PowerShell Remoting activado.
            B. NOTA: Al utilizar una colección de aprovisionamiento existente, puede actualizar y volver a implementar las imágenes existentes como parte de un proceso de actualización de imágenes planificado.
        iii. **Tipo de almacenamiento**: Seleccione la velocidad del disco del sistema operativo considerando el coste y el rendimiento
        iv. **Unidad de datos**: Opcionalmente, activa un segundo disco conectado a esta imagen, normalmente para la capa de almacenamiento de datos mencionada anteriormente en 2.e.

A. **Tipo de unidad de datos**: Seleccione la velocidad del segundo disco (datos) teniendo en cuenta el coste y el rendimiento

B. **Tamaño de la unidad de datos (GB)**: Defina el tamaño del segundo disco (datos) teniendo en cuenta la capacidad, el coste y el rendimiento

h. **Agregar aplicaciones**: Seleccione cualquier aplicación de la Biblioteca de aplicaciones que vaya a instalar (1) en esta imagen y (2) gestionada por el derecho de aplicación VDS. (Esto solo es aplicable a implementaciones RDS. Debe permanecer vacío para los espacios de trabajo AVD)

Personalización del equipo virtual temporal

VDS incluye una funcionalidad que permite eliminar el acceso de las máquinas virtuales desde la interfaz web de VDS. De forma predeterminada, se crea una cuenta de administrador local de Windows con una contraseña rotativa y se pasa a la máquina virtual, lo que permite al administrador local de VDS acceder sin necesidad de conocer las credenciales de administrador local.

> La función Connect to Server tiene una configuración alternativa en la que se solicitará al administrador de VDS credenciales con cada conexión. Esta opción puede habilitarse o deshabilitarse si edita la cuenta de administrador de VDS desde la sección "Admin" de VDS. La funcionalidad se llama *Tech Account* y al activar la casilla se necesitará introducir la credencial al utilizar Connect to Server, al desactivar esta casilla se activará la inyección automática de las credenciales de administración locales de Windows en cada conexión.

El administrador de VDS simplemente debe conectarse a la máquina virtual temporal mediante Connect to Server u otro proceso y realizar los cambios necesarios para cumplir sus requisitos.

Validación de la colección

Una vez completada la personalización, el administrador de VDS puede cerrar la imagen y Sysprep haciendo clic en **Validar** en el icono acciones.

[Management.Deployments.provisioning colecciones ed97e] |

Management.Deployments.provisioning_collections-ed97e.png

Uso de la colección

Una vez finalizada la validación, el estado de la colección de aprovisionamiento cambiará a **disponible**. Desde dentro de la colección de aprovisionamiento, el administrador de VDS puede identificar el nombre **plantilla de VM** que se utiliza para identificar esta colección de aprovisionamiento a través de VDS.

[Management.Deployments.provisioning colecciones f5a49] |

Management.Deployments.provisioning_collections-f5a49.png

Nuevo servidor

En la página Workspace > Servers, se puede crear un nuevo servidor y el cuadro de diálogo solicitará la plantilla de VM. El nombre de la plantilla de arriba se encuentra en esta lista:

[anchura = 75%]

VDS proporciona una forma sencilla de actualizar los hosts de sesión en un entorno RDS mediante Provisioning Collections y la funcionalidad **Add Server**. Este proceso se puede realizar sin afectar a los usuarios finales y se puede repetir una y otra vez con las actualizaciones de imagen subsiguientes, basándose en las iteraciones de imagen anteriores. Para obtener un flujo de trabajo detallado de este proceso, consulte **"Proceso de actualización del host de sesión de RDS"** a continuación.

Nueva piscina de host AVD

En la página Workspace > AVD > Host Pools, se puede crear un nuevo grupo de hosts AVD haciendo clic en **+ Agregar grupo de hosts** y el cuadro de diálogo solicitará la plantilla VM. El nombre de la plantilla de arriba se encuentra en esta lista:

[Management.Deployments.provisioning colecciones ba2f5] |

Management.Deployments.provisioning_collections-ba2f5.png

Nuevos host(s) de sesión AVD

En la página Workspace > AVD > Host Pool > Session hosts, se pueden crear nuevos hosts de sesiones AVD haciendo clic en **+ Add Session Host** y el cuadro de diálogo solicitará la plantilla VM. El nombre de la plantilla de arriba se encuentra en esta lista:

[Management.Deployments.provisioning colecciones ba5e9] |

Management.Deployments.provisioning_collections-ba5e9.png

VDS proporciona una forma sencilla de actualizar los hosts de sesión en un grupo de hosts AVD mediante Provisioning Collections y la funcionalidad **Add Session Host**. Este proceso se puede realizar sin afectar a los usuarios finales y se puede repetir una y otra vez con las actualizaciones de imagen subsiguientes, basándose en las iteraciones de imagen anteriores. Para obtener un flujo de trabajo detallado de este proceso, consulte **"Proceso de actualización del host de sesión AVD"** a continuación.

Nuevo espacio de trabajo

En la página Workspaces, se puede crear un espacio de trabajo nuevo haciendo clic en **+ Nuevo espacio de trabajo** y el cuadro de diálogo solicitará la colección Provisioning. El nombre del conjunto de aprovisionamiento compartido se encuentra en esta lista.

[Management.Deployments.provisioning colecciones 5c941] |

Management.Deployments.provisioning_collections-5c941.png

Nueva colección de aprovisionamiento

En la página implementación > Colección de aprovisionamiento, se puede crear una nueva colección de aprovisionamiento haciendo clic en **+ Agregar colección**. Al agregar servidores a esta colección, el cuadro de diálogo le pedirá la plantilla de VM. El nombre de la plantilla de arriba se encuentra en esta lista:

[Management.Deployments.provisioning colecciones 9eac4] |

Management.Deployments.provisioning_collections-9eac4.png

Anexo 1: Hosts de sesiones de RDS

Proceso de actualización del host de sesión RDS

VDS proporciona una forma sencilla de actualizar los hosts de sesión en un entorno RDS mediante Provisioning Collections y la funcionalidad **Add Server**. Este proceso se puede realizar sin afectar a los usuarios finales y se puede repetir una y otra vez con las actualizaciones de imagen subsiguientes, basándose en las iteraciones de imagen anteriores.

El proceso de actualización del host de sesión de RDS es el siguiente:

1. Cree una nueva colección de aprovisionamiento VDI, personalice y valide la colección siguiendo las instrucciones anteriores.
    a. Por lo general, esta recopilación de aprovisionamiento se realizará en la plantilla de equipo virtual anterior, emulando un proceso "abierto, guardado como".
2. Una vez que la colección de aprovisionamiento se ha validado, vaya a la página *Workspace* > *Servers*, haga clic en **+ Add Server**

    [Management.Deployments.provisioning recolecciones.hosts de sesión rds e8204] |

Management.Deployments.provisioning_collections.rds_session_hosts-e8204.png

3. Seleccione **TS** como **función de servidor**
4. Seleccione la última **plantilla VM**. Realice las selecciones **Tamaño de máquina** y **Tipo de almacenamiento** adecuadas en función de sus requisitos. Deje **Unidad de datos** sin marcar.
5. Repita esto para el número total de hosts de sesión necesarios para el entorno.
6. Haga clic en **Agregar servidor**, los hosts de sesión se construirán en función de la plantilla de VM seleccionada y comenzarán a conectarse en tan sólo 10-15 minutos (dependiendo del hipervisor).
    a. Tenga en cuenta que los hosts de sesión que se encuentran actualmente en el entorno se retirará en última instancia después de que estos nuevos hosts se encuentren en línea. Planifique la creación de suficientes hosts nuevos para ser suficientes para admitir toda la carga de trabajo en este entorno.
7. Cuando un nuevo host se conecta, la configuración predeterminada es permanecer en **no permitir nuevas sesiones**. Para cada host de sesión, se puede utilizar el conmutador **permitir nuevas sesiones** para administrar qué hosts pueden recibir nuevas sesiones de usuario. Para acceder a esta configuración, edite la configuración de cada servidor host de sesión individual. Una vez que se han creado suficientes hosts nuevos y se ha confirmado la funcionalidad, este ajuste se puede gestionar tanto en los hosts nuevos como antiguos para enrutar todas las sesiones nuevas a los hosts nuevos. Los hosts antiguos, con **permitir nuevas sesiones** establecido en **desactivado**, pueden seguir ejecutándose y alojar sesiones de usuario existentes.

    [Management.Deployments.provisioning Colecciones.hosts de sesión rds 726d1] |

Management.Deployments.provisioning_collections.rds_session_hosts-726d1.png

8. A medida que los usuarios cierran la sesión del host antiguo y sin nuevas sesiones de usuario que se unan a los hosts antiguos, se pueden eliminar los hosts antiguos donde **sesiones = 0** haciendo clic en el icono **acciones** y seleccionando **borrar**.

   [Management.Deployments.provisioning Colecciones.host de sesión rds 45d32] |

Management.Deployments.provisioning_collections.rds_session_hosts-45d32.png

Addendum 2 - anfitriones de la sesión del AVD

Proceso de actualización del host de sesión de AVD

VDS proporciona una forma sencilla de actualizar los hosts de sesión en un grupo de hosts AVD mediante Provisioning Collections y la funcionalidad **Add Session Host**. Este proceso se puede realizar sin afectar a los usuarios finales y se puede repetir una y otra vez con las actualizaciones de imagen subsiguientes, basándose en las iteraciones de imagen anteriores.

El proceso de actualización del host de sesión de AVD es el siguiente:

1. Cree una nueva colección de aprovisionamiento VDI, personalice y valide la colección siguiendo las instrucciones anteriores.
    a. Por lo general, esta recopilación de aprovisionamiento se realizará en la plantilla de equipo virtual anterior, emulando un proceso "abierto, guardado como".
2. Una vez que la colección de aprovisionamiento se ha validado, desplácese a la página *Workspace* > *AVD* > *Host Pools* y haga clic en el nombre del grupo de hosts
3. Desde la página *Host Pool* > *Session hosts*, haga clic en **+ Add Session Host**

    [Management.Deployments.provisioning colecciones 9ed95] |

Management.Deployments.provisioning_collections-9ed95.png

4. Seleccione la última **plantilla VM**. Realice las selecciones **Tamaño de máquina** y **Tipo de almacenamiento** adecuadas en función de sus requisitos.
5. Introduzca el **número de instancias** igual al número total de hosts de sesión requeridos. Normalmente, este número será el mismo que el que se encuentra actualmente en el pool de hosts, pero puede ser cualquier número.
   a. Tenga en cuenta que los hosts de sesión que se encuentran actualmente en el pool de hosts se retirará en última instancia después de que estos nuevos hosts se conecten. Planificar el **número de instancias** introducido para que sea suficiente para soportar toda la carga de trabajo en este grupo de hosts.
6. Haga clic en **Guardar**, los hosts de sesión se construirán en función de la plantilla de VM seleccionada y comenzarán a conectarse en tan sólo 10-15 minutos (dependiendo del hipervisor).
7. Cuando un nuevo host se conecta, la configuración predeterminada es permanecer en **no permitir nuevas sesiones**. Para cada host de sesión, se puede utilizar el conmutador **permitir nuevas sesiones** para administrar qué hosts pueden recibir nuevas sesiones de usuario. Una vez que se han creado suficientes hosts nuevos y se ha confirmado la funcionalidad, este ajuste se puede gestionar tanto en los hosts nuevos como antiguos para enrutar todas las sesiones nuevas a los hosts nuevos. Los hosts antiguos, con **permitir nuevas sesiones** establecido en **desactivado**, pueden seguir ejecutándose y alojar sesiones de usuario existentes.

   [Management.Deployments.provisioning colecciones b47e] |

Management.Deployments.provisioning_collections-be47e.png

8. A medida que los usuarios cierran la sesión del host antiguo y sin nuevas sesiones de usuario que se unan a los hosts antiguos, se pueden eliminar los hosts antiguos donde **sesiones = 0** haciendo clic en el icono **acciones** y seleccionando **borrar**.

   [Management.Deployments.provisioning colecciones cefb9] |

Management.Deployments.provisioning_collections-cefb9.png

Visión General de la jerarquía lógica de VDS

Descripción general

VDS organiza los conceptos en varias capas de una jerarquía lógica. Este artículo ayuda a esbozar cómo encajan juntos.

Esquema organizativo VDS

El portal de gestión VDS se encuentra en https://manage.vds.netapp.com. Esta interfaz web es un único panel para administrar todos los objetos relacionados con VDS. Dentro de la interfaz de usuario web de VDS, existe la siguiente jerarquía de componentes y contenedores lógicos.

Implementación de VDS

El *Deployment* es un concepto de VDS que organiza y contiene *VDS Workspace(s)*. En algunas arquitecturas de implementación, una implementación puede contener múltiples espacios de trabajo VDS.

> La ejecución de varios espacios de trabajo VDS en una única implementación se denomina "Multi-Tenancy" y es solo una opción en implementaciones RDS, las implementaciones de AVD no admiten este método.

Una implementación está definida por su dominio de Active Directory y hay una relación 1:1 entre el dominio de AD y una implementación.

Existen determinados recursos de máquinas virtuales que se implementan para admitir una implementación que se comparten en todos los espacios de trabajo de VDS de la implementación. Por ejemplo, cada implementación contiene una máquina virtual denominada "CWMGR1", que es un servidor que ejecuta aplicaciones VDS, una base de datos de SQL Express y facilita la administración de los entornos de trabajo VDS (y los recursos contenidos) dentro de la implementación.

Espacio de trabajo VDS

> Existe una diferencia entre un espacio de trabajo "**VDS**" y un espacio de trabajo "**AVD**".

Un espacio de trabajo VDS es un contenedor lógico dentro de la implementación para los recursos del cliente (usuario final). Estos recursos incluyen máquinas virtuales (para hosts de sesión, servidores de aplicaciones, servidores de bases de datos, servidores de archivos, etc.), redes virtuales, almacenamiento y otra infraestructura de hipervisor.

El área de trabajo de VDS también contiene funciones de gestión para administrar usuarios, grupos de seguridad, programación de cargas de trabajo, aplicaciones, automatización, Equipos virtuales y configuración AVD.

Normalmente, un espacio de trabajo VDS se alinea con una sola empresa o (en implementaciones empresariales) con una unidad de negocio.

Sitios VDS

Dentro de una puesta en marcha, se pueden crear varios sitios para representar a distintos proveedores de infraestructura, todos gestionados dentro de una única puesta en marcha.

Esto resulta útil cuando una única empresa o unidad de negocio necesita alojar usuarios y aplicaciones en varias ubicaciones físicas (por ejemplo, Norteamérica y EMEA), suscripciones a hipervisores (para alinear los costes con las unidades de negocio) e incluso hipervisores (por ejemplo, usuarios en Azure, Google Compute y HCI en las instalaciones en vSphere).

Áreas de trabajo AVD

Existe una diferencia entre un espacio de trabajo "**VDS**" y un espacio de trabajo "**AVD**".

Un área de trabajo AVD es un contenedor lógico que se encuentra dentro de un espacio de trabajo VDS y un sitio VDS. Que se puede utilizar de forma similar a un sitio VDS para segmentar las políticas de gestión y operativas en la misma implementación.

Grupos de hosts AVD

Los grupos de host AVD son contenedores lógicos que se encuentran dentro de un área de trabajo AVD y mantienen a los usuarios de hosts de sesión y grupos de aplicaciones para servidor las sesiones de usuario y controlar el acceso a los recursos individuales.

Grupos de aplicaciones AVD

Cada grupo de host AVD comienza con un único grupo de aplicaciones "Desktop". Se pueden asignar usuarios o grupos a este (u otro) grupo de aplicaciones para permitir el acceso a los recursos del grupo de aplicaciones a los usuarios asignados.

Se pueden crear grupos de aplicaciones adicionales dentro de un grupo de hosts en VDS. Todos los grupos de aplicaciones adicionales son grupos de aplicaciones de "RemoteApp" y proporcionan recursos de RemoteApp en lugar de una experiencia de escritorio de Windows completa.

Más grandes

Autorización de aplicaciones

Descripción general

VDS dispone de una sólida funcionalidad de derechos y automatización de aplicaciones integrada. Esta funcionalidad permite a los usuarios tener acceso a diferentes aplicaciones mientras se conectan a los mismos hosts de sesión. Esto se logra mediante la ocultación de accesos directos de algunos GPO personalizados junto con la automatización, colocando de forma selectiva los accesos directos en los escritorios de los usuarios.

Este flujo de trabajo solo se aplica a implementaciones RDS. Para obtener la documentación sobre los derechos de aplicación de AVD, consulte "Flujo de trabajo de derechos de aplicación para AVD"

Las aplicaciones pueden asignarse a los usuarios directamente o a través de grupos de seguridad gestionados en VDS.

En líneas generales, el proceso de aprovisionamiento de aplicaciones sigue estos pasos.

1. Agregue las aplicaciones al catálogo de aplicaciones
2. Agregue las aplicaciones al área de trabajo

3. Instale la aplicación en todos los hosts Session
4. Seleccione la ruta de acceso directo
5. Asigne aplicaciones a usuarios y/o grupos

Los pasos 3 y 4 se pueden automatizar totalmente con los eventos con secuencias de comandos, como se muestra a continuación

Demostración de vídeo

Agregar aplicaciones al catálogo de aplicaciones

Derechos de aplicación de VDS comienza con App Catalog, esto es un listado de todas las aplicaciones disponibles para su implementación en entornos de usuario final.

Para agregar aplicaciones al catálogo, siga estos pasos

1. Inicie sesión en VDS en https://manage.cloudworkspace.com uso de las credenciales de administrador principales.
2. En la esquina superior derecha, haga clic en el icono de flecha situado junto a su nombre de usuario y seleccione Configuración.
3. Haga clic en la ficha Catálogo de aplicaciones.
4. Haga clic en la opción Agregar aplicación de la barra de título Catálogo de aplicaciones.
5. Para agregar un grupo de aplicaciones, elija la opción Importar aplicaciones.
    a. Aparecerá un cuadro de diálogo que proporciona una plantilla de Excel para descargar que crea el formato correcto para la lista de aplicaciones.
    b. Para esta evaluación, NetApp VDS ha creado una lista de aplicaciones de muestra para la importación, aquí se puede encontrar.

c. Haga clic en el área cargar y elija el archivo de plantilla de aplicación, haga clic en el botón Importar.

6. Para agregar aplicaciones individuales, elija el botón Agregar aplicación y aparecerá un cuadro de diálogo.
   a. Introduzca el nombre de la aplicación.
   b. El ID externo se puede utilizar para introducir un identificador de seguimiento interno, como un SKU de producto o un código de seguimiento de facturación (opcional).
   c. Marque la casilla Suscripción si desea informar sobre las aplicaciones como producto de suscripción (opcional).
   d. Si el producto no instala por versión (por ejemplo, Chrome), marque la casilla de verificación Versión no obligatoria. Esto permite instalar productos de "actualización continua" sin realizar un seguimiento de sus versiones.
   e. Por el contrario, si un producto admite varias versiones con nombre (por ejemplo, QuickBooks), debe marcar esta casilla de verificación para poder instalar varias versiones y tener VDS específicos cada versión disponible en la lista de aplicaciones que pueden tener derecho a y al usuario final.
   f. Marque “no hay icono de escritorio de usuario” si no desea que VDS suministre un icono de escritorio para este producto. Esto se utiliza para productos de "back-end" como SQL Server, ya que los usuarios finales no tienen una aplicación a la que acceder.
   g. “La aplicación debe estar asociada” hace que sea necesario instalar una aplicación asociada. Por ejemplo, una aplicación de servidor cliente puede requerir también la instalación de SQL Server o MySQL.
   h. Al activar la casilla Licencia necesaria, se indica que VDS debe solicitar que se cargue un archivo de licencia para una instalación de esta aplicación antes de establecer el estado de la aplicación en activo. Este paso se realiza en la página de detalles de la aplicación de VDS.
   i. Visible para todos: El derecho a las aplicaciones puede limitarse a subpartners específicos en una jerarquía multicanal. Para fines de evaluación, haga clic en la casilla de verificación para que todos los usuarios puedan verla en la lista de aplicaciones disponibles.

Agregue la aplicación al área de trabajo

Para iniciar el proceso de implementación, agregará la aplicación al espacio de trabajo.

Para ello, siga estos pasos

1. Haga clic en entornos de trabajo
2. Desplácese hacia abajo hasta aplicaciones
3. Haga clic en Añadir
4. Active la casilla de verificación aplicaciones, introduzca la información necesaria, haga clic en Agregar aplicación y, a continuación, en Agregar aplicaciones.

Instale manualmente la aplicación

Una vez que la aplicación se haya agregado al espacio de trabajo, deberá tener instalada esa aplicación en todos los hosts de sesión. Esto puede realizarse manualmente o puede automatizarse.

Para instalar manualmente aplicaciones en hosts de sesión, siga estos pasos

1. Vaya a Service Board.
2. Haga clic en la tarea de la placa de servicio.
3. Haga clic en el nombre del servidor para conectarse como administrador local.

4. Instale las aplicaciones, confirme que el acceso directo a esta aplicación se encuentra en la ruta del menú Inicio.
    a. Para Server 2016 y Windows 10: C:\ProgramData\Microsoft\Windows\Start Menu\Programs.
5. Vuelva a la tarea de la placa de servicio, haga clic en examinar y elija el acceso directo o una carpeta que contenga accesos directos.
6. Lo que seleccione es lo que se mostrará en el escritorio del usuario final cuando se asigne la aplicación.
7. Las carpetas son fantásticas cuando una aplicación es en realidad de varias aplicaciones. Por ejemplo, “Microsoft Office” es más fácil de implementar como una carpeta con cada aplicación como un acceso directo dentro de la carpeta.
8. Haga clic en completar instalación.
9. Si es necesario, abra el icono creado Agregar tarea de placa de servicio y confirme que se ha agregado el icono.

Asigne aplicaciones a los usuarios

Los derechos de aplicación se gestionan mediante VDS y la aplicación se puede asignar a los usuarios de tres formas distintas

Asigne aplicaciones a los usuarios

1. Desplácese a la página Detalles del usuario.
2. Vaya a la sección aplicaciones.
3. Marque la casilla junto a todas las aplicaciones requeridas por este usuario.

Asignar usuarios a una aplicación

1. Desplácese a la sección aplicaciones de la página Detalles del área de trabajo.
2. Haga clic en el nombre de la aplicación.
3. Marque la casilla junto a los usuarios de la aplicación.

Asignar aplicaciones y usuarios a grupos de usuarios

1. Desplácese hasta el Detalle de usuarios y grupos.
2. Agregue un nuevo grupo o edite un grupo existente.
3. Asigne usuarios y aplicaciones al grupo.

Flujo de trabajo de derechos de aplicación para AVD

Descripción general

En un entorno de Azure Virtual Desktop (AVD), el acceso a la aplicación se gestiona mediante la pertenencia a grupos de aplicaciones.

Este flujo de trabajo solo se aplica a las implementaciones de AVD. Para obtener la documentación sobre los derechos de aplicación de RDS, consulte "Flujo de trabajo de derechos de aplicaciones para RDS"

AVD es un servicio bien documentado y hay muchos "recursos públicos para información". VDS no superpone la forma estándar de funcionamiento del AVD. En su lugar, este artículo está diseñado para ilustrar cómo VDS se acerca al concepto estándar que se encuentra en todas las implementaciones de AVD.

Consulte la "Visión General de la jerarquía lógica de VDS" el artículo puede ser útil antes o durante la revisión de este artículo.

La vista del usuario final

En Azure Virtual Desktop, a cada usuario final se le asigna acceso a RemoteApp y/o escritorios por parte de su administrador de AVD. Esto se logra a través de la asignación de grupos de aplicaciones en VDS.

RemoteApp hace referencia a una aplicación que se ejecuta de forma remota en el host de sesión pero se presenta en el dispositivo local sin el contexto de escritorio. Esta aplicación, conocida normalmente como una "aplicación de streaming", tiene el aspecto de una aplicación local en el dispositivo local, pero se ejecuta en el contexto de seguridad, y en la capa de almacenamiento e informática del host de sesiones.

- Desktop* se refiere a la experiencia completa de Windows que se ejecuta en el host de sesión y se presenta en el dispositivo local, normalmente en una ventana de pantalla completa. Este escritorio contiene todas las aplicaciones instaladas en el host de sesión que el usuario puede iniciar desde la ventana de sesión del escritorio, lo que normalmente se conoce como "escritorio remoto".

En el inicio de sesión, el usuario final aparece con los recursos que le asigna su administrador. A continuación se muestra un ejemplo de la vista que un usuario final puede ver al iniciar sesión con su cliente AVD. Este es un ejemplo más complejo, a menudo un usuario final sólo tendrá asignado un escritorio dingle o RemoteApp. El usuario final puede hacer doble clic en cualquiera de estos recursos para iniciar la aplicación o el escritorio.

[Management.despliegues.vds sitios 0e49c] | *Management.Deployments.vds_sites-0e49c.png*

En este ejemplo más complejo, este usuario tiene acceso a dos sesiones de escritorio diferentes y 4 aplicaciones de streaming diferentes:

- **Escritorios disponibles**
  - Escritorio GPU de NVIDIA
  - Escritorio conjunto AVD compartido
  - Operación 2 Escritorio de la piscina
- **RemoteApps** disponible
  - AutoCAD 2021
  - Revisión 2021
  - Microsoft Edge
  - Bloc de notas

Entre bastidores, estas aplicaciones y escritorios se alojan en una gran variedad de hosts de sesiones, espacios de trabajo AVD e incluso se pueden alojar en diferentes regiones de Azure.

Este es un diagrama que ilustra dónde se aloja cada uno de estos recursos y la forma en que se asignaron a este usuario final.

[Management.despliegues.vds sites 0e880] | *Management.Deployments.vds_sites-0e880.png*

Como se ha mostrado anteriormente, los distintos recursos disponibles para este usuario final se alojan en diferentes hosts de sesión, en diferentes pools de host y son potencialmente gestionados por diferentes organizaciones DE TI en diferentes entornos de trabajo AVD. Si bien no se muestra en este ejemplo, estos recursos también podrían alojarse en distintas regiones y/o suscripciones de Azure mediante la función VDS Sites.

Acceso a escritorio

De forma predeterminada, cada pool de hosts comienza con un solo grupo de aplicaciones, utilizado para asignar acceso a la experiencia de escritorio de Windows. Todas las aplicaciones instaladas en estos hosts de sesión serán accesibles para los usuarios finales asignados a este grupo de aplicaciones.

Para habilitar el recurso Desktop para usuarios en VDS:

1. Desplácese a la página Workspaces > AVD > Host Pool > App Groups y haga clic en el grupo App para el recurso "Desktop".

   [Flujo de trabajo de derechos de aplicaciones Management.Applications.avd 349fe] |

Management.Applications.avd_application_entitlement_workflow-349fe.png

2. Una vez dentro del grupo de aplicaciones, haga clic en Editar

   [Management.Applications.avd flujo de trabajo de derechos de aplicación 3bcfc] |

Management.Applications.avd_application_entitlement_workflow-3bcfc.png

3. Desde el cuadro de diálogo de edición, puede agregar o quitar usuarios a este grupo de aplicaciones por usuario o por grupos.

   [Flujo de trabajo de derechos de aplicación Management.Applications.avd 07ff0] |

Management.Applications.avd_application_entitlement_workflow-07ff0.png

Acceso de RemoteApp

Para aprovisionar acceso a RemoteApps, es necesario crear un nuevo grupo de aplicaciones dentro del grupo de hosts. Una vez creadas, se deben asignar las aplicaciones adecuadas a este grupo de aplicaciones.

> Cualquier aplicación en estos hosts de sesiones estará disponible para cualquier usuario asignado al AppGroup "Desktop" de este grupo de hosts. No es necesario también aprovisionar acceso a través de un grupo de aplicación RemoteApp para proporcionar acceso a las aplicaciones. Un grupo de aplicaciones RemoteApp sólo es necesario para habilitar el acceso a aplicaciones que se ejecutan como si estuviera en el dispositivo local como una aplicación de streaming.

Cree un nuevo grupo de aplicaciones

1. Desplácese a la página Workspaces > AVD > Host Pool > App Groups y haga clic en el botón *+ Add App Group*

   [Management.Applications.avd flujo de trabajo de autorización de aplicaciones d33da] |

Management.Applications.avd_application_entitlement_workflow-d33da.png

2. Introduzca el nombre, el espacio de trabajo y el nombre descriptivo de este grupo de aplicaciones. Seleccione los usuarios o grupos que se deben asignar y haga clic en *Save*

   [Flujo de trabajo de concesión de aplicaciones Management.Applications.avd 242eb] |

Management.Applications.avd_application_entitlement_workflow-242eb.png

Agregar aplicaciones al grupo de aplicaciones

1. Desplácese a la página Workspaces > AVD > Host Pool > App Groups y haga clic en el grupo App para el recurso "RemoteApp".

   [Management.Applications.avd flujo de trabajo de derechos de aplicación 3dcde] |

Management.Applications.avd_application_entitlement_workflow-3dcde.png

2. Una vez dentro del grupo de aplicaciones, haga clic en Editar

[Management.Applications.avd flujo de trabajo de derechos de aplicación 27a41] |

Management.Applications.avd_application_entitlement_workflow-27a41.png

3. Desplácese hacia abajo hasta la sección "aplicaciones remotas". Esta sección puede tardar un momento en rellenarse ya que VDS consulta directamente a los hosts de sesión para mostrar las aplicaciones disponibles para streaming.

   [Management.Applications.avd flujo de trabajo de derechos de aplicación 1e9f2] |

Management.Applications.avd_application_entitlement_workflow-1e9f2.png

4. Busque y seleccione las aplicaciones a las que los usuarios de este grupo de aplicaciones tengan acceso como recurso RemoteApp.

Eventos programados

Eventos programados

Descripción general

Los eventos con secuencias de comandos proporcionan al administrador avanzado un mecanismo para crear automatización personalizada para el mantenimiento del sistema, alertas de usuario, administración de directivas de grupo u otros eventos. Las secuencias de comandos se pueden designar para ejecutarse como un proceso ejecutable con argumentos o pueden utilizarse como argumentos para un programa ejecutable diferente. Esta funcionalidad permite combinar y anidar scripts para que admitan complejas necesidades de personalización e integración.

Un ejemplo detallado de eventos con guión en acción se encuentra en la "Guía de derechos de aplicaciones".

Además, Eventos con secuencias de comandos permite la creación de automatización que no requiere un script para procesar, más bien el flujo de automatización es iniciado por un disparador del sistema y ejecuta un programa existente o una utilidad del sistema con argumentos opcionales.

Secuencias de comandos Eventos contiene un **repositorio** de secuencias de comandos y **actividades**. Los scripts contienen las instrucciones sobre **qué** hacer mientras las actividades vinculan los scripts con el desencadenador y el destino apropiado (**cuándo y dónde**) para el script.

Repositorio

La ficha repositorio muestra una lista de todas las secuencias de comandos disponibles para su implementación desde su cuenta VDS. Se trata de un repositorio personalizado que comparten todos los administradores de la instancia de VDS. El acceso a eventos con script se puede administrar en la página *VDS > Admins > Permissions*.

[Sub.Management.scripted Events.scripted events 1ce76] |

sub.Management.Scripted_Events.scripted_events-1ce76.png

Filtro de clientes

Cada organización de administrador de VDS tiene una biblioteca privada de scripts creados y/o personalizados por su organización. Estos scripts se definen como Tipo de secuencia de comandos "Cliente". Secuencias de comandos de cliente a las que cualquier administrador de VDS elimine y edite los permisos de administrador adecuados en la sección Eventos con secuencias de comandos.

Filtro global

NetApp también publica y mantiene una biblioteca de scripts "globales" que es la misma en todas las organizaciones de administradores de VDS. Estos scripts se definen como Tipo de secuencia de comandos "Global". Ningún administrador de VDS puede editar o eliminar los scripts globales. En cambio, los scripts globales se pueden "clonar" y el script resultante es un script de "cliente" que se puede editar y utilizar.

Descargar Script

La posibilidad de descargar el archivo de script asociado a un evento con guión permite al administrador de VDS revisar y editar el archivo de script subyacente antes de la implementación. Nunca es aconsejable ejecutar un script que no entienda por completo.

[Sub.Management.scripted Events.scripted events 02a9b] |

sub.Management.Scripted_Events.scripted_events-02a9b.png

Agregar script

Al hacer clic en el botón + *Add Script* se abre una nueva página para crear un script y guardarlo en el repositorio.

[Management.script Events.scripts eventos a53fa] | *Management.Scripted_Events.scripted_events-a53fa.png*

Es necesario completar los siguientes campos para crear un nuevo script:

- **Nombre**
- **Incluir archivo de secuencia de comandos**
  - Sí: Permite que un archivo de script (por ejemplo, un archivo .ps1) se cargue y ejecute con el ejecutable "Execute with".
  - No: Elimina el campo "Archivo de secuencia de comandos" (a continuación) y simplemente ejecuta el comando "Ejecutar con" y "argumentos"
- **Archivo de secuencia de comandos**
  - Si *Include Script File* = *Yes* este campo está visible y permite la carga de un archivo de script.
- **Ejecutar con**
  - Define la ruta del ejecutable que se utiliza para ejecutar el archivo de script o el comando que se ejecuta.
  - Por ejemplo, para ejecutar con PowerShell el valor "Execute with" sería *C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe*
- **Argumentos**
  - Define cualquier argumento adicional que se ejecute con el comando "se ejecuta con".
  - VDS ofrece algunas variables que tienen en cuenta el contexto que se pueden utilizar, entre las que se incluyen:
    - %Emprescode%: Código de empresa en tiempo de ejecución
    - %Servername%: Nombre de equipo virtual en tiempo de ejecución
    - %samaccountname% - <username>.<companycode>
    - %applicationname%: Nombre de aplicación solicitado en tiempo de ejecución
    - %Scriptname%: Nombre de secuencia de comandos en tiempo de ejecución
    - %username% - username@loginidentifier en tiempo de ejecución
- **URL de documentación**
  - Este campo permite al escritor de la secuencia de comandos vincularlo a la documentación que se encuentra fuera de VDS, como un sistema de base de conocimientos utilizado por la organización de administradores de VDS.

Editar script

Al hacer clic en el nombre de una secuencia de comandos en el repositorio se abre una nueva página con detalles sobre la secuencia de comandos y un botón de acción para **editar**.

Al editar una secuencia de comandos, se pueden editar los mismos campos que se documentan anteriormente en la "Agregar script" sección.

En esta página de detalles de scripts, también puede **borrar** el script y **descargar** cualquier archivo de script cargado.

[Management.scripted Events.scripted events 3e756] | *Management.Scripted_Events.scripted_events-*

3e756.png

Actividades

Las actividades vinculan un script del repositorio a una implementación, un subconjunto de máquinas virtuales y un evento de activación.

[Management.script Events.script events f971c] | *Management.Scripted_Events.scripted_events-f971c.png*

Añadir actividad

Al hacer clic en el botón + *Añadir actividad* se abre una nueva página para crear una actividad.

[Management.script Events.script eventos 02ef8] | *Management.Scripted_Events.scripted_events-02ef8.png*

Es necesario completar los siguientes campos para crear una nueva actividad:

- **Nombre**
- **Descripción** (opcional)
- **Despliegue**
- **Script**
- **Argumentos**
- Casilla de verificación **activada**
- **Ajustes de sucesos**

Activadores de actividad

[Sub.Management.script Events.script events cdfcd] | *sub.Management.Scripted_Events.scripted_events-*

cdfcd.png

- **Instalación de aplicaciones**
  - Esto se activa cuando el administrador de VDS hace clic en "+ Add…" En la página *Workspace* > *Applications*.
  - Esta selección permite seleccionar una aplicación de la Biblioteca de aplicaciones y definir previamente el acceso directo de la aplicación.
  - Las instrucciones detalladas para este activador se resaltan en la "*Instale la documentación del script de Adobe Reader DC*".
- **Desinstalar aplicaciones**
  - Esto se activa cuando el administrador de VDS hace clic en **acciones › Desinstalar** en la página *Workspace* > *Applications*.
  - Esta selección permite seleccionar una aplicación de la Biblioteca de aplicaciones y definir previamente el acceso directo de la aplicación.
  - Las instrucciones detalladas para este activador se resaltan en la "*Desinstalar la documentación del script de Adobe Reader DC*".
- **Servidor de clones**
  - Esto se activa cuando la función Clone se ejecuta en un equipo virtual existente
- **Crear caché**
  - Esto se activa cada vez que VDS crea una nueva máquina virtual para aprovisionar una caché de recogida
- **Crear cliente**
  - Esto se activa cada vez que se agrega una nueva organización de cliente a VDS
- **Crear servidor**
  - Esto se activa cada vez que VDS crea una nueva máquina virtual
- **Crear usuario**
  - Esto se activa cada vez que se agrega un nuevo usuario a través de VDS
- **Eliminar usuario**
  - Esto se activa cuando se elimina un nuevo usuario a través de VDS
- **Manual**
  - Esto lo activa un administrador de VDS manualmente desde la página **Eventos de secuencia de comandos › actividad**
- **Actualización manual de la aplicación**
- **Programado**
  - Esto se activa cuando se alcanza la fecha/hora definida
- **Iniciar servidor**
  - Esto se activa en una máquina virtual cada vez que arranca

Al hacer clic en *Name* se abre un cuadro de diálogo en el que se puede editar la actividad.

Centro de comandos

Comando del Centro de comandos: Descripción general

Descripción general

El Centro de comandos es un ejecutable que se ejecuta en el servidor de la plataforma CWMGR1 en la implementación. Se accede a él conectándose a la VM de CWMGR1 y ejecuándola localmente en esa VM.

Esta aplicación se ha diseñado para la resolución de problemas, el diagnóstico y las funciones avanzadas de administración. Esta aplicación la utilizan principalmente los equipos de desarrollo y soporte internos de NetApp; sin embargo, algunos administradores de clientes utilizan ocasionalmente algunas funciones. Esta documentación se proporciona para admitir el uso de funciones de selección. La utilización de estos comandos debe realizarse con cuidado y en colaboración con el equipo de soporte de NetApp.

Ejecutando el Centro de comandos

Para ejecutar la aplicación Command Center:

1. Conéctese al servidor desde la página *VDS* > *Deployment* > *Platform Servers*, haga clic en el icono *Actions* y seleccione "Connect".

   [Management.command Descripción general del centro 68087] | *Management.command_center_overview-*

68087.png

2. Cuando se le solicitan las credenciales, introduzca las credenciales de administrador del dominio
   a. El usuario deberá ser miembro del grupo de seguridad "CW-Infrastructure". Por razones de coherencia, recomendamos agregar esta pertenencia convirtiendo al usuario en miembro del grupo "técnicos de nivel 3" en *AD > espacio de trabajo en la nube > usuarios técnicos de área de trabajo en la nube > grupos*

      [Management.command vista general central 1c42d] | *Management.command_center_overview-*

1c42d.png

3. Busque el icono del escritorio de *Command Center* y ejecútelo

   [Management.command vista general central 3c860] | *Management.command_center_overview-*

3c860.png

a. Para activar la ficha avanzada, inicie la aplicación con el conmutador "-showadvancedtab".

Operaciones

[Management.command vista general central b614e] | *Management.command_center_overview-b614e.png*

En el menú **comando** puede seleccionar de una lista de acciones (que se muestra a continuación).

Una vez seleccionado un comando, los datos se pueden rellenar con datos de despliegue desde el botón **cargar datos**. El botón Load Data también se usa para consultar al hipervisor los datos una vez que se hayan realizado las selecciones anteriores (p. ej., cargar una lista de fechas de backup disponibles después de seleccionar una máquina virtual específica de una lista desplegable)

[Management.command Descripción general del centro 85417] | *Management.command_center_overview-*

85417.png

Después de realizar selecciones en un comando, al hacer clic en **Ejecutar comando** se ejecutará el proceso seleccionado.

Para revisar los registros, haga clic en el botón **Ver todos los registros**. Se abrirá el archivo de texto sin formato, con las entradas más recientes en la parte inferior.

Lista de comandos

- "Copiar plantilla en Galería"

Operaciones

Comando del Centro de comandos: Copiar plantilla en Galería

Advertencia del Centro de comandos

> El Centro de comandos es una aplicación que se ejecuta en el servidor de la plataforma CWMGR1 de la implementación. Esta aplicación se ha diseñado para la resolución de problemas, el diagnóstico y las funciones avanzadas de administración. Esta aplicación la utilizan principalmente los equipos de desarrollo y soporte internos de NetApp; sin embargo, algunos administradores de clientes utilizan ocasionalmente algunas funciones. Esta documentación se proporciona para admitir el uso de funciones de selección. La utilización de estos comandos debe realizarse con cuidado y en colaboración con el equipo de soporte de NetApp. Puede encontrar más información en la "Descripción general del Centro de comandos" artículo.

Copiar plantilla en Galería Descripción general

[Management.command centre.opers.copy template a la galería 67ea4] |

Management.command_center.operations.copy_template_to_gallery-67ea4.png

Cuando finaliza una colección de aprovisionamiento VDI, la imagen se almacena en Azure como una imagen y se puede implementar en el mismo sitio VDS. Para que la imagen esté disponible para su implementación en otra región de Azure dentro de la misma suscripción, se utiliza la función "Copiar plantilla a galería". Esta acción copiará la imagen de VM en la galería compartida y la replicará en todas las regiones seleccionadas.

[Management.command central.opers.copy template to gallery ed821] |

Management.command_center.operations.copy_template_to_gallery-ed821.png

Disponibilidad de plantilla de equipo virtual en la lista desplegable VDS

Una vez finalizada la replicación, la imagen aparecerá en VDS en el menú desplegable para seleccionar VM Templates al implementar nuevas máquinas virtuales. La imagen compartida estará disponible para su implementación en cualquier región seleccionada al copiar.

[Management.command central.opers.copy template to gallery 04bd8] |

Management.command_center.operations.copy_template_to_gallery-04bd8.png

Las imágenes de máquina virtual almacenadas en la Galería compartida se agregan con su versión en forma de "-x.x.x", donde la versión coincide con la versión de imagen del portal de Azure.

[Management.command Center.opers.copy template to gallery ee598] |

Management.command_center.operations.copy_template_to_gallery-ee598.png

La replicación de la imagen puede tomar un rato (dependiendo del tamaño de la imagen) y el estado se puede ver haciendo clic en la versión (p. ej. 1.0.0) en la columna "Nombre" como se resalta en la captura de pantalla anterior.

Disponibilidad regional

Las implementaciones sólo se pueden realizar en las regiones en las que se ha replicado la imagen. Esto se puede comprobar en el portal de Azure haciendo clic en 1.x.x y luego en *Update Replication*, como se muestra aquí:

[Management.command Center.opers.copy template to gallery 9b63a] |

Management.command_center.operations.copy_template_to_gallery-9b63a.png

Optimización de recursos

Programación de las cargas de trabajo

La programación de la carga de trabajo es una función que puede programar la ventana de tiempo en la que está activo el entorno.

La programación de las cargas de trabajo puede configurarse en "Always On", "Always Off" o "Scheduled". Cuando se establece en "programado", las horas de encendido y apagado se pueden establecer de manera tan granular como una ventana de hora diferente para cada día de la semana.

[]

Cuando se programa el apagado, ya sea a través de "Always Off" o "Scheduled", todas las máquinas virtuales de inquilino se apagarán. Los servidores de la plataforma (como CWMGR1) permanecerán activos para facilitar la funcionalidad como activar a petición.

El programa de cargas de trabajo funciona en combinación con otras funciones de optimización de recursos, como Live Scaling y Wake on Demand.

Activar a petición

Wake on Demand (WOD) es una tecnología pendiente de patente que puede activar los recursos de VM adecuados para un usuario final para facilitar el acceso desatendido 24/7, incluso cuando se ha programado que los recursos estén inactivos.

WOD para servicios de Escritorio remoto

En RDS, el cliente de Windows VDS cuenta con la integración de activación a petición incorporada y puede activar los recursos apropiados sin ninguna acción adicional del usuario final. Simplemente, necesitan iniciar su inicio de sesión normal y el cliente les notificará un breve retraso en el que se activan las máquinas virtuales. Este cliente (y, por lo tanto, esta función de activación automática a petición) sólo está disponible cuando se conecta desde un dispositivo Windows a un entorno RDS.

El cliente web VDS incluye una funcionalidad similar para las implementaciones RDS. VDS Web Client se encuentra en: ""

La funcionalidad Wake on Demand no está integrada en el cliente de Microsoft RD (para Windows o cualquier otra plataforma) ni en ningún otro cliente de RD de terceros.

Active On Demand para Azure Virtual Desktop

En AVD, los únicos clientes que se pueden utilizar para conectar son Microsoft proporcionados y, por lo tanto, no contienen la funcionalidad Wake on Demand.

VDS sí incluye una función de activación a petición de autoservicio para AVD a través del cliente web VDS. El cliente web puede utilizarse para activar los recursos adecuados y, a continuación, la conexión se puede iniciar a través del cliente AVD estándar.

Para activar los recursos de VM en AVD:

1. Conéctese al cliente web VDS en ""

2. Inicie sesión con las credenciales del usuario AVD
    - Un mensaje de advertencia le indicará *"que tiene los servicios AVD de Microsoft disponibles. Haga clic AQUÍ para ver el estado e iniciar grupos de hosts sin conexión."*
3. Después de hacer clic en "*HERE*" verá una lista de grupos de hosts disponibles junto con un enlace a "Click to Start" bajo la columna status

    []

4. *Haga clic en Inicio* el enlace y espere 1-5 minutos para que el estado cambie a "en línea" y muestre un icono de estado verde
5. Conéctese a AVD utilizando el proceso normal

Escalado en directo

Live Scaling funciona junto con la programación de cargas de trabajo mediante la gestión del número de hosts de sesiones en línea durante el tiempo activo programado, tal y como se configura en la programación de cargas de trabajo. Cuando la opción esté programada para estar sin conexión, Live Scaling no controlará la disponibilidad del host de sesión. El escalado en vivo solo afecta a usuarios compartidos y servidores compartidos en entornos RDS y AVD, los usuarios de VDI y los equipos virtuales de VDI quedan excluidos de estos cálculos. El resto de tipos de equipos virtuales no se ven afectados.

El ajuste AVD *Load equilibrador type* interactúa con esta configuración, por lo que debe tenerse cuidado al elegir ese ajuste también. El ahorro de costes se maximiza con un amplio primer tipo mientras el rendimiento del usuario final se maximiza con un amplio primer tipo.

Activación de escala en directo sin opciones marcadas, el motor de automatización seleccionará automáticamente los valores para el número de servidores con tecnología adicional, usuarios compartidos por servidor y usuarios compartidos máximos por servidor.

- El *Number of Extra Powered on Servers* se establece por defecto en 0, lo que significa que 1 servidor ejecutará 24/7.
- El *Shared Users per Server* toma por defecto el número de usuarios de la compañía dividido por el número de servidores.
- El valor predeterminado de *Max Shared Users per Server* es infinito.

Live Scaling activa los servidores cuando los usuarios inician sesión y los desactiva a medida que los usuarios cierran la sesión.

La activación de un servidor adicional se activa automáticamente una vez que el total de usuarios activos alcanza el número de usuarios compartidos por servidor multiplicado por el número total de servidores alimentados.

```
 e.g. With 5 Shared Users per Server set (this is the default # we'll use
for all examples in this article) and 2 servers running, a 3rd server
won't be powered up until server 1 & 2 both have 5 or more active users.
Until that 3rd server is available, new connections will be load balanced
all available servers. In RDS and AVD Breadth mode, Load balancing sends
users to the server with the fewest active users (like water flowing to
the lowest point). In AVD Depth mode, Load balancing sends users to
servers in a sequential order, incrementing when the Max Shared Users
number is reached.
Live Scaling también desactivará servidores para ahorrar costes. Cuando un
servidor tiene 0 usuarios activos y otro servidor tiene capacidad
disponible por debajo de _Shared Users per Server_ se apaga el servidor
vacío.
```

El encendido del siguiente servidor puede tardar unos minutos. En determinadas situaciones, la velocidad de los inicios de sesión puede superar la disponibilidad de nuevos servidores. Por ejemplo, si 15 personas inician sesión en 5 minutos, todos desembarcaran en el primer servidor (o se les deniega una sesión) mientras se inician la segunda y la tercera. Existen dos estrategias que se pueden utilizar para mitigar la sobrecarga de un único servidor en este escenario:

1. Active *Number of Extra Powered on Servers* para que los servidores adicionales estén activados y disponibles para aceptar conexiones y permitir que la plataforma acelere servidores adicionales.
    a. Cuando se activa, el número se agrega a la necesidad calculada. Por ejemplo, si se establece en 1 servidor adicional (y con 6 usuarios conectados), dos servidores estarían activos debido al número de usuarios, más un tercero debido al valor *Extra Powered on Servers*.
2. Active *Max Shared Users per Server* para colocar un límite mínimo en el número de usuarios permitidos por servidor. Se rechazarán las conexiones nuevas que superen este límite, el usuario final recibirá un mensaje de error y deberá volver a intentarlo dentro de unos minutos una vez que esté disponible el servidor adicional. Si se establece, este número también define la profundidad de los servidores compartidos AVD.
    a. Suponiendo que el delta entre *Shared Users per Server* y *Max Shared Users per Server* sea apropiado, los nuevos servidores deberían estar disponibles antes de que se alcance el máximo en todas las situaciones más extremas (tormentas de inicio de sesión inusualmente grandes).

Escalado de recursos de equipos virtuales

El escalado de recursos de VM es una función opcional que puede cambiar el tamaño y la cantidad de los equipos virtuales del host de sesión en un entorno.

Cuando se activa, VDS calcula el tamaño y la cantidad adecuados de las máquinas virtuales host de sesión en función de los criterios seleccionados. Estas opciones incluyen: Usuarios activos, usuarios con nombre, carga de servidor y fijo.

[]

El tamaño de los equipos virtuales se incluye con la familia de equipos virtuales seleccionada en la interfaz de usuario, que se puede cambiar mediante la lista desplegable. (Por ejemplo, *Standard DV3 Family* en Azure)

[]

Escalado basado en usuarios

> La siguiente función se comporta igual para "usuarios activos" o "recuento de usuarios". El recuento de usuarios es un simple recuento de todos los usuarios activados con un escritorio VDS. Active Users es una variable calculada basada en las 2 semanas anteriores de los datos de sesión de usuario.

Al calcular en función de los usuarios, el tamaño (y la cantidad) de los equipos virtuales del host de sesión se calculan en función de los requisitos de RAM y CPU definidos. El administrador puede definir los GB de la RAM y el número de núcleos vCPU por usuario junto con recursos no variables adicionales.

En la siguiente captura de pantalla, a cada usuario se le asignan 2 GB de RAM y 1/2 de un núcleo vCPU. Además, el servidor comienza con 2 núcleos vCPU y 8 GB de RAM.

[]

Además, el administrador puede definir el tamaño máximo que puede alcanzar una máquina virtual. Cuando se alcance, los entornos se escalarán horizontalmente añadiendo hosts adicionales de sesiones de equipos virtuales.

En la siguiente captura de pantalla, cada equipo virtual está limitado a 32 GB de RAM y 8 núcleos de vCPU.

[]

Con todas estas variables definidas, VDS puede calcular el tamaño y la cantidad adecuados de los equipos virtuales host de sesión, lo que simplifica en gran medida el proceso de mantenimiento de la asignación de recursos adecuada, incluso cuando se añaden y se quitan los usuarios.

Escalado basado en la carga de servidor

Cuando se calcula en función de la carga del servidor, el tamaño (y la cantidad) de los equipos virtuales del host de sesión se calcula en función de la tasa media de utilización de CPU/RAM observada por VDS durante el período de dos semanas anterior.

Cuando se supera el umbral máximo, VDS aumenta el tamaño o aumenta la cantidad para recuperar el uso medio dentro del intervalo.

Al igual que el escalado basado en el usuario, se puede definir la familia de equipos virtuales y el tamaño máximo de estos.

[]

Otros recursos activos

La programación de cargas de trabajo no controla los servidores de la plataforma como CWMGR1, ya que son necesarios para activar la funcionalidad Wake on Demand y facilitar otras tareas de la plataforma y debe ejecutar 24/7 para un funcionamiento ambiental normal.

Se puede obtener un ahorro adicional desactivando todo el entorno, pero sólo se recomienda para entornos que no sean de producción. Se trata de una acción manual que se puede realizar en la sección implementaciones de VDS. Para devolver el entorno a su estado normal, también es necesario realizar un paso manual en la misma página.

[] []

Administración de usuarios

Gestión de cuentas de usuario

Crear nuevos usuarios

Los administradores pueden agregar usuarios haciendo clic en entornos de trabajo > usuarios y grupos > Agregar o importar

Los usuarios pueden agregarse individualmente o con una importación masiva.

[anchura = 25%]

> La inclusión del correo electrónico y el número de teléfono móvil precisos en este momento mejora considerablemente el proceso de activación de la MFA más adelante.

Una vez que haya creado usuarios, puede hacer clic en su nombre para ver detalles como cuándo se crearon, su estado de conexión (ya estén o no conectados actualmente) y cuáles son sus configuraciones específicas.

Activación del escritorio virtual para los usuarios existentes de AD

Si los usuarios ya están presentes en AD, puede activar fácilmente el escritorio virtual de los usuarios haciendo clic en el equipo situado junto a su nombre y, a continuación, activando su escritorio.[anchura = 50%]

> Únicamente para Azure AD Domain Service: Para que los inicios de sesión funcionen, el hash de contraseña para los usuarios de Azure AD debe sincronizarse para admitir la autenticación NTLM y Kerberos. La forma más sencilla de realizar esta tarea consiste en cambiar la contraseña de usuario en Office.com o en el portal de Azure, lo que obligará a que se produzca la sincronización hash de contraseña. El ciclo de sincronización de los servidores de servicio de dominio puede tardar hasta 20 minutos, por lo que los cambios en las contraseñas de Azure AD suelen tardar 20 minutos en reflejarse en ADDS y, por tanto, en el entorno VDS.

Eliminar cuentas de usuario

Editar información del usuario

En la página de detalles del usuario se pueden realizar cambios en los datos del usuario, como el nombre de usuario y los datos de contacto. Los valores de correo electrónico y teléfono se utilizan para el proceso de restablecimiento automático de contraseñas (SSPR).

[]

Editar la configuración de seguridad del usuario

- Habilitado para el usuario de VDI: Configuración de RDS que, cuando está habilitada, crea un host de sesión de máquina virtual dedicado y asigna este usuario como el único usuario que conecta con él. Como parte de la activación de esta casilla de verificación, se solicita al administrador de CWMS que seleccione la imagen, el tamaño y el tipo de almacenamiento de VM.
  - Los usuarios de AVD VDI deben gestionarse en la página AVD como un pool de hosts VDI.
- Caducidad de cuenta activada: Permite al administrador de CWMS establecer una fecha de caducidad en la cuenta de usuario final.

- Forzar restablecimiento de contraseña en el siguiente inicio de sesión: Solicita al usuario final que cambie la contraseña al iniciar sesión.
- Autenticación multifactor habilitada: Habilita la MFA para el usuario final y los solicita a configurar la MFA en el siguiente inicio de sesión.
- Unidad móvil activada: Función heredada que no se utiliza en las implementaciones actuales de RDS o AVD.
- Acceso a la unidad local activado: Permite al usuario final acceder al almacenamiento del dispositivo local desde el entorno de la nube, incluidos copia/pegado, almacenamiento masivo USB y unidades del sistema.
- Activación a petición activada: Para usuarios de RDS que se conecten a través del cliente CW para Windows, lo que permite al usuario final tener permiso para llevar su entorno cuando se conecta fuera de las horas de trabajo normales definidas por el programa de carga de trabajo.

Cuenta bloqueada

De forma predeterminada, cinco intentos fallidos de inicio de sesión bloquearán la cuenta de usuario. La cuenta de usuario se desbloqueará después de 30 minutos a menos que se active *Enable Password complicado*. Con la complejidad de la contraseña activada, la cuenta no se desbloqueará automáticamente. En cualquier caso, el administrador de VDS puede desbloquear manualmente la cuenta de usuario desde la página Users/Groups de VDS.

Restablecer contraseña de usuario

Restablece la contraseña de usuario.

Nota: Cuando se restablecen las contraseñas de usuario de Azure AD (o se desbloquea una cuenta), puede haber un retraso de hasta 20 minutos a medida que el restablecimiento se propaga a través de Azure AD.

Acceso del administrador

Al habilitar esta opción, se proporciona al usuario final un acceso limitado al portal de gestión para su inquilino. Los usos comunes incluyen proporcionar acceso a un empleado in situ para restablecer las contraseñas de sus compañeros, asignar aplicaciones o permitir el acceso de activación manual del servidor. Aquí también se establecen permisos que controlan las áreas de la consola que se pueden ver.

Usuario(s) de cierre de sesión

El administrador de VDS puede cerrar la sesión de los usuarios conectados desde la página Users/Groups de VDS.

Más grandes

Muestra la aplicación desplegada en este espacio de trabajo. La casilla de verificación proporciona las aplicaciones a este usuario específico. Puede encontrar la documentación completa de Application Management aquí. El acceso a las aplicaciones también se puede otorgar desde la interfaz de la aplicación o a grupos de seguridad.

Ver/eliminar procesos de usuario

Muestra los procesos que se están ejecutando actualmente en la sesión de ese usuario. Los procesos también se pueden finalizar desde esta interfaz.

Gestión de permisos de datos

Perspectiva del usuario final

Los usuarios finales de escritorios virtuales pueden tener acceso a varias unidades asignadas. Estas unidades incluyen un recurso compartido de equipo accesible para FTs, un recurso compartido de archivos de la empresa y su unidad doméstica (para sus documentos, escritorio, etc.) . Todas estas unidades asignadas hacen referencia a una capa de almacenamiento central en un servicio de almacenamiento (como Azure NetApp Files) o en un equipo virtual de servidor de archivos.

Dependiendo de la configuración que el usuario pueda no tener las unidades H: O F: Expuestas, sólo pueden ver su escritorio, documentos, etc. carpetas. Además, ocasionalmente el administrador de VDS establece diferentes letras de unidad en la implementación.[]

[]

Gestión de permisos

VDS permite a los administradores editar grupos de seguridad y permisos de carpeta desde el portal VDS.

Grupos de seguridad

Los grupos de seguridad se gestionan haciendo clic en: Espacios de trabajo > Nombre de inquilino > usuarios y grupos > en la sección grupos

En esta sección puede:

1. Crear nuevos grupos de seguridad
2. Agregar o quitar usuarios a los grupos
3. Asignar aplicaciones a grupos
4. Habilitar/deshabilitar acceso de unidad local a los grupos

[]

Permisos de carpeta

Los permisos de carpeta se gestionan haciendo clic en: Áreas de trabajo > Nombre de inquilino > Administrar (en la sección carpetas).

En esta sección puede:

1. Agregar/eliminar carpetas
2. Asignar permisos a usuarios o grupos
3. Personalice los permisos para sólo lectura, Control total y Ninguno

[]

Autorización de aplicaciones

Descripción general

VDS dispone de una sólida funcionalidad de derechos y automatización de aplicaciones integrada. Esta funcionalidad permite a los usuarios tener acceso a diferentes aplicaciones mientras se conectan a los mismos hosts de sesión. Esto se logra mediante la ocultación de accesos directos de algunos GPO

personalizados junto con la automatización, colocando de forma selectiva los accesos directos en los escritorios de los usuarios.

Este flujo de trabajo solo se aplica a implementaciones RDS. Para obtener la documentación sobre los derechos de aplicación de AVD, consulte "Flujo de trabajo de derechos de aplicación para AVD"

Las aplicaciones pueden asignarse a los usuarios directamente o a través de grupos de seguridad gestionados en VDS.

En líneas generales, el proceso de aprovisionamiento de aplicaciones sigue estos pasos.

1. Agregue las aplicaciones al catálogo de aplicaciones
2. Agregue las aplicaciones al área de trabajo
3. Instale la aplicación en todos los hosts Session
4. Seleccione la ruta de acceso directo
5. Asigne aplicaciones a usuarios y/o grupos

Los pasos 3 y 4 se pueden automatizar totalmente con los eventos con secuencias de comandos, como se muestra a continuación

Demostración de vídeo

Agregar aplicaciones al catálogo de aplicaciones

Derechos de aplicación de VDS comienza con App Catalog, esto es un listado de todas las aplicaciones disponibles para su implementación en entornos de usuario final.

Para agregar aplicaciones al catálogo, siga estos pasos

1. Inicie sesión en VDS en https://manage.cloudworkspace.com uso de las credenciales de administrador principales.
2. En la esquina superior derecha, haga clic en el icono de flecha situado junto a su nombre de usuario y seleccione Configuración.
3. Haga clic en la ficha Catálogo de aplicaciones.
4. Haga clic en la opción Agregar aplicación de la barra de título Catálogo de aplicaciones.
5. Para agregar un grupo de aplicaciones, elija la opción Importar aplicaciones.
    a. Aparecerá un cuadro de diálogo que proporciona una plantilla de Excel para descargar que crea el formato correcto para la lista de aplicaciones.
    b. Para esta evaluación, NetApp VDS ha creado una lista de aplicaciones de muestra para la importación, aquí se puede encontrar.
    c. Haga clic en el área cargar y elija el archivo de plantilla de aplicación, haga clic en el botón Importar.
6. Para agregar aplicaciones individuales, elija el botón Agregar aplicación y aparecerá un cuadro de diálogo.
    a. Introduzca el nombre de la aplicación.
    b. El ID externo se puede utilizar para introducir un identificador de seguimiento interno, como un SKU de producto o un código de seguimiento de facturación (opcional).
    c. Marque la casilla Suscripción si desea informar sobre las aplicaciones como producto de suscripción (opcional).
    d. Si el producto no instala por versión (por ejemplo, Chrome), marque la casilla de verificación Versión no obligatoria. Esto permite instalar productos de "actualización continua" sin realizar un seguimiento de sus versiones.
    e. Por el contrario, si un producto admite varias versiones con nombre (por ejemplo, QuickBooks), debe marcar esta casilla de verificación para poder instalar varias versiones y tener VDS específicos cada versión disponible en la lista de aplicaciones que pueden tener derecho a y al usuario final.
    f. Marque “no hay icono de escritorio de usuario” si no desea que VDS suministre un icono de escritorio para este producto. Esto se utiliza para productos de "back-end" como SQL Server, ya que los usuarios finales no tienen una aplicación a la que acceder.
    g. “La aplicación debe estar asociada” hace que sea necesario instalar una aplicación asociada. Por ejemplo, una aplicación de servidor cliente puede requerir también la instalación de SQL Server o MySQL.
    h. Al activar la casilla Licencia necesaria, se indica que VDS debe solicitar que se cargue un archivo de licencia para una instalación de esta aplicación antes de establecer el estado de la aplicación en activo. Este paso se realiza en la página de detalles de la aplicación de VDS.
    i. Visible para todos: El derecho a las aplicaciones puede limitarse a subpartners específicos en una jerarquía multicanal. Para fines de evaluación, haga clic en la casilla de verificación para que todos los usuarios puedan verla en la lista de aplicaciones disponibles.

Agregue la aplicación al área de trabajo

Para iniciar el proceso de implementación, agregará la aplicación al espacio de trabajo.

Para ello, siga estos pasos

1. Haga clic en entornos de trabajo
2. Desplácese hacia abajo hasta aplicaciones
3. Haga clic en Añadir

4. Active la casilla de verificación aplicaciones, introduzca la información necesaria, haga clic en Agregar aplicación y, a continuación, en Agregar aplicaciones.

Instale manualmente la aplicación

Una vez que la aplicación se haya agregado al espacio de trabajo, deberá tener instalada esa aplicación en todos los hosts de sesión. Esto puede realizarse manualmente o puede automatizarse.

Para instalar manualmente aplicaciones en hosts de sesión, siga estos pasos

1. Vaya a Service Board.
2. Haga clic en la tarea de la placa de servicio.
3. Haga clic en el nombre del servidor para conectarse como administrador local.
4. Instale las aplicaciones, confirme que el acceso directo a esta aplicación se encuentra en la ruta del menú Inicio.
    a. Para Server 2016 y Windows 10: C:\ProgramData\Microsoft\Windows\Start Menu\Programs.
5. Vuelva a la tarea de la placa de servicio, haga clic en examinar y elija el acceso directo o una carpeta que contenga accesos directos.
6. Lo que seleccione es lo que se mostrará en el escritorio del usuario final cuando se asigne la aplicación.
7. Las carpetas son fantásticas cuando una aplicación es en realidad de varias aplicaciones. Por ejemplo, “Microsoft Office” es más fácil de implementar como una carpeta con cada aplicación como un acceso directo dentro de la carpeta.
8. Haga clic en completar instalación.
9. Si es necesario, abra el icono creado Agregar tarea de placa de servicio y confirme que se ha agregado el icono.

Asigne aplicaciones a los usuarios

Los derechos de aplicación se gestionan mediante VDS y la aplicación se puede asignar a los usuarios de tres formas distintas

Asigne aplicaciones a los usuarios

1. Desplácese a la página Detalles del usuario.
2. Vaya a la sección aplicaciones.
3. Marque la casilla junto a todas las aplicaciones requeridas por este usuario.

Asignar usuarios a una aplicación

1. Desplácese a la sección aplicaciones de la página Detalles del área de trabajo.
2. Haga clic en el nombre de la aplicación.
3. Marque la casilla junto a los usuarios de la aplicación.

Asignar aplicaciones y usuarios a grupos de usuarios

1. Desplácese hasta el Detalle de usuarios y grupos.
2. Agregue un nuevo grupo o edite un grupo existente.
3. Asigne usuarios y aplicaciones al grupo.

Restablecer contraseña de usuario

Restablecer pasos de contraseña de usuario

1. Desplácese hasta la página Detalles usados en VDS

   []

2. Busque la sección Contraseña, introduzca la nueva contraseña dos veces y haga clic en

   []

   []

Tiempo para tomar efecto

- Para entornos que ejecutan un AD “interno” en equipos virtuales del entorno, el cambio de contraseña debería aplicarse inmediatamente.
- En los entornos que ejecutan Azure AD Domain Services (ADDS), el cambio de contraseña debería tardar unos 20 minutos en aplicarse.
- El tipo AD se puede determinar en la página Detalles de la implementación:

  []

Restablecimiento de contraseña de autoservicio (SSRP)

El cliente Windows VDS de NetApp y el cliente web VDS de NetApp proporcionan un mensaje para los usuarios que deben introducir una contraseña incorrecta al iniciar sesión en la implementación del escritorio virtual v5.2 (o posterior). En caso de que el usuario haya bloqueado su cuenta, este proceso también desbloqueará la cuenta de un usuario.

Nota: Los usuarios deben haber introducido un número de teléfono móvil o una dirección de correo electrónico para que funcione este proceso.

SSPR es compatible con:

- Cliente VDS Window de NetApp
- VDS Web Client de NetApp

En este conjunto de instrucciones, se recorre el proceso de utilizar SSPR como un medio sencillo para permitir a los usuarios restablecer sus contraseñas y desbloquear sus cuentas.

Cliente Windows VDS de NetApp

1. Como usuario final, haga clic en el enlace Contraseña olvidada para continuar.

   []

2. Seleccione si desea recibir su código a través de su teléfono móvil o por correo electrónico.

   []

3. Si un usuario final sólo ha proporcionado uno de esos métodos de contacto, será el único método que se

muestra.

[]

4. Después de este paso, se presentará a los usuarios un campo de código en el que deben introducir el valor numérico recibido ya sea en su dispositivo móvil o en su bandeja de entrada (dependiendo de cuál haya sido seleccionado). Introduzca ese código seguido de la nueva contraseña y haga clic en Restablecer para continuar.

   []

5. Los usuarios verán un mensaje informándoles de que su restablecimiento de contraseña se ha completado correctamente; haga clic en hecho para continuar con el proceso de inicio de sesión.

   Si la implementación utiliza servicios de dominio de Azure Active Directory, hay un periodo de sincronización de contraseñas definido por Microsoft, cada 20 minutos. De nuevo, Microsoft controla este proceso y no se puede cambiar. Teniendo esto en cuenta, VDS muestra que el usuario debería esperar hasta 20 minutos para que su nueva contraseña surta efecto. Si su implementación no utiliza Azure Active Directory Domain Services, el usuario podrá iniciar sesión de nuevo en cuestión de segundos.

   []

Portal HTML5

1. Si el usuario no puede introducir la contraseña correcta al intentar iniciar sesión a través del HTML5, se le presentará una opción para restablecer la contraseña:

   []

2. Después de hacer clic en la opción para restablecer su contraseña, se les presentarán sus opciones de restablecimiento:

   []

3. El botón 'solicitud' enviará un código generado a la opción seleccionada (en este caso el correo electrónico del usuario). El código es válido durante 15 minutos.

   []

4. La contraseña se ha restablecido. Es importante recordar que Windows Active Directory necesitará a menudo un momento para propagar el cambio, así que si la nueva contraseña no funciona inmediatamente, espere unos minutos y vuelva a intentarlo. Esto es especialmente importante para los usuarios que residen en una implementación de Azure Active Directory Domain Services, donde el restablecimiento de la contraseña puede tardar hasta 20 minutos en propagarse.

   []

Habilitar el restablecimiento de contraseñas de autoservicio (SSPR) para los usuarios

Para utilizar el restablecimiento automático de contraseñas de autoservicio (SSPR), los administradores deben introducir primero un número de teléfono móvil y/o una cuenta de correo electrónico para un usuario final hay dos formas de introducir un número móvil y direcciones de correo electrónico para un usuario de escritorio virtual como se detalla a continuación.

En este conjunto de instrucciones, guiará el proceso de configuración de SSPR como un medio sencillo para que los usuarios finales restablezcan sus contraseñas.

Importación masiva de usuarios a través de VDS

Empiece por navegar al módulo Workspaces, usuarios y grupos y, a continuación, haga clic en Agregar o importar.

Se pueden introducir estos valores para los usuarios al crearlos uno por uno:[]

También puede incluir estos elementos cuando los usuarios importen grandes cantidades descargan y cargan el archivo XLSX de Excel preconfigurado con este contenido rellenado:[]

Suministrar los datos a través de la API VDS

API VDS de NetApp: Específicamente esta llamada https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – proporciona la capacidad de actualizar esta información.

Actualizando el teléfono de usuario existente

Actualice el número de teléfono del usuario en la página User Detail Overview (Resumen de detalles del usuario) en VDS.

[]

Uso de otras consolas

Nota: Actualmente no puede proporcionar un número de teléfono para un usuario a través de la consola de Azure, el centro de partners o desde la consola administrativa de Office 365.

Personalizar dirección de envío SSPR

Es posible configurar VDS de NetApp para enviar un correo electrónico de confirmación *from* una dirección personalizada. Se trata de un servicio proporcionado a nuestros partners proveedores de servicios que desean que sus usuarios finales reciban el correo electrónico de restablecimiento de contraseña que se envíe desde su propio dominio de correo electrónico personalizado.

Esta personalización requiere algunos pasos adicionales para verificar la dirección de envío. Para iniciar este proceso, abra un caso de soporte con compatibilidad con VDS que solicite una "Self Service Password Reset Source Address" personalizada. Defina lo siguiente:

- Su código de socio (se puede encontrar haciendo clic en *settings* en el menú de la flecha hacia abajo superior derecha. Consulte la captura de pantalla siguiente)

  []

- Dirección "de" deseada (que debe ser válida)
- A qué clientes debe aplicarse la configuración (o todas)

La apertura de un caso de soporte se puede realizar enviando un correo electrónico a: support@spotpc.netapp.com

Una vez recibido, el soporte de VDS funcionará para validar la dirección con nuestro servicio SMTP y activar esta configuración. Lo ideal es que pueda actualizar registros DNS públicos en el dominio de dirección de origen para maximizar la entrega de correo electrónico.

Complejidad de la contraseña

VDS se puede configurar para aplicar la complejidad de las contraseñas. La configuración de esta opción se encuentra en la página Detalle del área de trabajo de la sección Configuración del área de trabajo en la nube.

[]

[]

Complejidad de la contraseña: Desactivada

Política	Pautas
Longitud mínima de la contraseña	8 caracteres
Antigüedad máxima de la contraseña	110 días
Antigüedad mínima de la contraseña	0 días
Aplicar historial de contraseñas	24 contraseñas recordadas
Bloqueo de contraseña	El bloqueo automático se producirá después de 5 entradas incorrectas
Duración del bloqueo	30 minutos

Complejidad de la contraseña: Activado

Política	Pautas
Longitud mínima de la contraseña	8 caracteres no contienen el nombre de cuenta del usuario ni partes del nombre completo del usuario que excedan dos caracteres consecutivos contienen caracteres de tres de las siguientes cuatro categorías: Caracteres en mayúsculas (De La A a la Z) caracteres en minúsculas (de la a a la z) base 10 dígitos (de 0 a 9) caracteres no alfabéticos (por ejemplo, !, $, #, %) los requisitos de complejidad se aplican cuando se cambian o crean contraseñas.
Antigüedad máxima de la contraseña	110 días
Antigüedad mínima de la contraseña	0 días
Aplicar historial de contraseñas	24 contraseñas recordadas
Bloqueo de contraseña	El bloqueo automático se producirá tras 5 entradas incorrectas
Duración del bloqueo	Permanece bloqueado hasta que se desbloquea el administrador

Autenticación multifactor (MFA)

Descripción general

El servicio de escritorios virtuales (VDS) de NetApp incluye un servicio de MFA basado en SMS/correo electrónico sin coste adicional. Este servicio es independiente de cualquier otro servicio (por ejemplo, Azure

Conditional Access) y se puede utilizar para proteger los inicios de sesión de administrador en VDS y los inicios de sesión de usuario en escritorios virtuales.

Aspectos básicos de la MFA

- La MFA de VDS puede asignarse a los usuarios administradores, a los usuarios finales individuales o aplicarse a todos los usuarios finales
- La MFA de VDS puede enviar notificaciones de SMS o por correo electrónico
- La MFA de VDS tiene una función de configuración y restablecimiento inicial en el autoservicio

Alcance de la guía

Esta guía le guiará por la configuración de la MFA junto con una ilustración de la experiencia del usuario final

En esta guía se tratan los siguientes temas:

1. Habilitación de MFA para usuarios individuales
2. Que requiere MFA para todos los usuarios
3. Habilitar MFA para administradores individuales
4. Configuración inicial del usuario final

Habilitar MFA para usuarios individuales

La MFA se puede habilitar para usuarios individuales en la página de detalles del usuario haciendo clic en *Multi-factor Auth Enabled*

Áreas de trabajo > Nombre de área de trabajo > usuarios y grupos > Nombre de usuario > Auth multifactor activada > Actualizar

La MFA también se puede asignar a todos los usuarios, si esta configuración está en su lugar, se activa la casilla de verificación y se añade *(a través de la configuración del cliente)* a la etiqueta de la casilla de verificación.

Que requiere MFA para todos los usuarios

La MFA se puede habilitar y aplicar en todos los usuarios de la página de detalles del área de trabajo haciendo clic en *MFA para todos los usuarios habilitados*

Áreas de trabajo > Nombre del área de trabajo > MFA para todos los usuarios activados >Actualizar

Habilitación de MFA para administradores individuales

La MFA también está disponible para cuentas de administrador que acceden al portal de VDS. Esto se puede habilitar por administrador en la página de detalles admin. Admins > Admin Name > Multi-factor Auth required > Update

Configuración inicial

En el primer inicio de sesión después de habilitar la MFA, se solicitará al usuario o al administrador que introduzca una dirección de correo electrónico o un número de teléfono móvil. Recibirán un código de confirmación para introducir y confirmar la inscripción correcta.

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