# Implementación con VDS

## Virtual Desktop Service

NetApp
February 20, 2023

# Tabla de Contenido

# Implementación con VDS

# Azure

## Puesto de trabajo virtual de Azure

### Guía de implementación de AVD

#### Descripción general

Esta guía proporcionará las instrucciones paso a paso para crear una implementación de Azure Virtual Desktop (AVD) con Virtual Desktop Service (VDS) de NetApp en Azure.

La guía comienza en: https://cwasetup.cloudworkspace.com/

Esta guía de prueba de concepto (POC, por sus siglas en inglés) está diseñada para ayudarle a implementar y configurar rápidamente AVD en su propia suscripción a Azure de prueba. En esta guía se asume una puesta en marcha de campo verde para un inquilino de Azure Active Directory limpio que no es de producción.

Las puestas en marcha de producción, especialmente en entornos AD o Azure existentes son muy comunes; sin embargo, este proceso no se tiene en cuenta en esta guía de POC. Las pruebas de concepto complejas y las implementaciones de producción deben iniciarse con los equipos de ventas/servicios de VDS de NetApp, y no realizarse de forma autoservicio.

Este documento POC le llevará a través de toda la implementación de AVD y le ofrecerá un breve recorrido por las principales áreas de la configuración posterior a la implementación disponibles en la plataforma VDS. Una vez completado, dispondrá de un entorno AVD completamente implementado y funcional, completo con grupos de host, grupos de aplicaciones y usuarios. Opcionalmente, tendrá la opción de configurar la entrega automatizada de aplicaciones, grupos de seguridad, permisos de recursos compartidos de archivos, Azure Cloud Backup, optimización inteligente de costes. VDS implementa un conjunto de configuraciones de mejores prácticas mediante GPO. También se incluyen instrucciones sobre cómo deshabilitar opcionalmente esos controles, en caso de que su POC no tenga controles de seguridad, similares a un entorno de dispositivo local no administrado.

#### Aspectos básicos de AVD

Azure Virtual Desktop es un completo servicio de virtualización de aplicaciones y puestos de trabajo que se ejecuta en el cloud. A continuación se ofrece una lista rápida de algunas de las funciones y funciones clave:

- Servicios de plataforma que incluyen puertas de enlace, distribución, licencia e inicio de sesión, y que se incluyen como servicio de Microsoft. Esto minimiza la infraestructura que requiere alojamiento y gestión.
- Azure Active Directory puede utilizarse como proveedor de identidades, lo que permite la segmentación en capas de servicios de seguridad de Azure adicionales, como el acceso condicional.
- Los usuarios experimentan una experiencia de inicio de sesión único para los servicios de Microsoft.
- Las sesiones de usuario se conectan al host de sesión mediante una tecnología de conexión inversa propia. Esto significa que no es necesario abrir ningún puerto de entrada; en su lugar, un agente crea una conexión saliente al plano de administración AVD que, a su vez, se conecta al dispositivo de usuario final.
- La conexión inversa incluso permite que las máquinas virtuales se ejecuten sin quedar expuestas a la Internet pública, lo que permite cargas de trabajo aisladas incluso al tiempo que se mantiene la conectividad remota.

- AVD incluye acceso a Windows 10 Multi Session, lo que permite una experiencia con Windows 10 Enterprise con la eficacia de sesiones de usuario de alta densidad.
- La tecnología de contenerización de perfiles FSLogix incluye la mejora del rendimiento de las sesiones de usuario, la eficiencia del almacenamiento y la mejora de la experiencia de Office en entornos no persistentes.
- AVD admite acceso completo a escritorio y RemoteApp. Tanto persistentes como no persistentes, y experiencias dedicadas y de múltiples sesiones.
- Las organizaciones pueden ahorrar en licencias de Windows porque AVD puede aprovechar el "Windows 10 Enterprise E3 por usuario", que sustituye la necesidad de las CAL de RDS y reduce significativamente el coste por hora de las máquinas virtuales host de sesiones en Azure.

#### Alcance de la guía

Esta guía le guiará por el proceso de implementación de AVD mediante la tecnología VDS de NetApp desde la perspectiva de un administrador de Azure y VDS. Usted aporta al cliente de Azure y la suscripción sin preconfiguración, y esta guía le ayuda a configurar AVD de extremo a extremo

**En esta guía se describen los siguientes pasos:**

1. Confirme los requisitos previos de los permisos de la cuenta de administrador de Azure y la suscripción de Azure
2. Recopile los detalles de detección necesarios
3. Cree el entorno de Azure con el asistente de configuración de VDS para Azure de forma específica
4. Cree el primer grupo de hosts con una imagen EVD estándar de Windows 10
5. Asignación de escritorios virtuales a usuarios de Azure AD
6. Agregue usuarios al grupo de aplicaciones predeterminado para entregar el entorno de escritorio a los usuarios. Opcionalmente, Crear grupos de hosts adicionales para proporcionar servicios RemoteApp
7. Conéctese como usuario final a través del software cliente y/o el cliente web
8. Conéctese a la plataforma y a los servicios de cliente como administrador local y de dominio
9. <<Autenticación multifactor (MFA),Opcionalmente, habilite la autenticación multifactor de VDS para los usuarios finales de AVD de VDS
10. De forma opcional, realice un recorrido por todo el flujo de trabajo de derechos de aplicación, incluida la rellenado de la biblioteca de aplicaciones, la automatización de instalación de aplicaciones, el enmascaramiento de aplicaciones por parte de usuarios y grupos de seguridad
11. También puede crear y administrar grupos de seguridad de Active Directory, permisos de carpeta y derechos de aplicación por grupo.
12. También puede configurar tecnologías de optimización de costes, como la programación de la carga de trabajo y el escalado en tiempo real
13. Opcionalmente, cree, actualice y Sysprep una imagen de máquina virtual para futuras puestas en marcha
14. Opcionalmente, configure Azure Cloud Backup
15. Opcionalmente, desactive las directivas de grupo de control de seguridad predeterminadas

#### Requisitos previos de Azure

VDS utiliza el contexto de seguridad nativo de Azure para implementar la instancia de AVD. Antes de iniciar el asistente de configuración de VDS, existen algunos requisitos previos de Azure que se deben establecer.

Durante la implementación, las cuentas de servicio y los permisos se conceden a VDS a través de la

autenticación de una cuenta de administrador existente desde el inquilino de Azure.

### Lista rápida de verificación de requisitos previos

- Inquilino de Azure con instancia de Azure AD (puede ser Microsoft 365 Instance)
- Suscripción a Azure
- Cuota de Azure disponible para máquinas virtuales de Azure
- Cuenta de administrador de Azure con roles de administración global y propiedad de la suscripción

Los requisitos previos detallados se documentan en "Este PDF"

### Administrador de Azure en Azure AD

Este administrador existente de Azure debe ser una cuenta de Azure AD en el inquilino de destino. Las cuentas de AD de Windows Server se pueden implementar con la instalación de VDS, pero es necesario realizar pasos adicionales para configurar una sincronización con Azure AD (fuera del alcance de esta guía)

Para confirmarlo, puede encontrar la cuenta de usuario en Azure Management Portal en Users > All Users.[]

### Función de administrador global

Al administrador de Azure se le debe asignar el rol de administrador global en el inquilino de Azure.

**Para comprobar su rol en Azure AD, siga estos pasos:**

1. Inicie sesión en el portal de Azure en https://portal.azure.com/
2. Busque y seleccione Azure Active Directory
3. En el siguiente panel de la derecha, haga clic en la opción usuarios de la sección Administrar
4. Haga clic en el nombre del usuario Administrador que está comprobando
5. Haga clic en función de directorio. En el panel de la derecha, debe aparecer la función de administrador global[]

**Si este usuario no tiene la función de administrador global, puede realizar los siguientes pasos para agregarlo (tenga en cuenta que la cuenta que ha iniciado sesión debe ser un administrador global para realizar estos pasos):**

1. En la página de detalles de funciones del directorio de usuarios del paso 5 anterior, haga clic en el botón Agregar asignación en la parte superior de la página de detalles.
2. Haga clic en Administrador global en la lista de funciones. Haga clic en el botón Agregar.[]

### Propiedad de la suscripción de Azure

El administrador de Azure también debe ser propietario de la suscripción en la suscripción que contendrá la implementación.

**Para comprobar que el Administrador es un propietario de la suscripción, siga estos pasos:**

1. Inicie sesión en el portal de Azure en https://portal.azure.com/
2. Busque y seleccione Suscripciones
3. En el siguiente panel de la derecha, haga clic en el nombre de la suscripción para ver los detalles de la suscripción

4. Haga clic en el elemento de menú Control de acceso (IAM) del panel, en segundo lugar de la izquierda
5. Haga clic en la ficha asignaciones de funciones. El administrador de Azure debe aparecer en la sección propietario.[]

**Si el administrador de Azure no aparece en la lista, puede agregar la cuenta como propietario de una suscripción siguiendo estos pasos:**

1. Haga clic en el botón Agregar en la parte superior de la página y elija la opción Agregar asignación de función
2. Aparecerá un cuadro de diálogo a la derecha. Elija “propietario” en la lista desplegable rol y, a continuación, comience a escribir el nombre de usuario del administrador en el cuadro Seleccionar. Cuando aparezca el nombre completo del administrador, selecciónelo
3. Haga clic en el botón Guardar situado en la parte inferior del cuadro de diálogo[]

### Cuota del núcleo informático de Azure

El asistente de configuración de CWA y el portal VDS crearán nuevas máquinas virtuales y la suscripción de Azure debe tener una cuota disponible para poder ejecutarse correctamente .

**Para comprobar la cuota, siga estos pasos:**

1. Vaya al módulo Suscripciones y haga clic en “uso + cuotas”.
2. Seleccione todos los proveedores en el menú desplegable “proveedores”, seleccione “Microsoft.Compute en el menú desplegable “proveedores”
3. Seleccione la región de destino en la lista desplegable "Ubicaciones"
4. Debe aparecer una lista de cuotas disponibles por familia de máquinas virtuales[]Si se necesita aumentar la cuota, haga clic en Request aumentar y siga los mensajes para añadir capacidad adicional. Para la implementación inicial, solicite específicamente un aumento de presupuesto para las “vCPU estándar de la familia DSv3”.

### Recopilar detalles de detección

Una vez que se trabaja con el asistente de instalación de CWA, hay varias preguntas que deben ser contestadas. VDS de NetApp ha proporcionado un PDF vinculado que puede utilizarse para registrar estas selecciones antes de la implementación. El elemento incluye:

| Elemento | Descripción |
|---|---|
| Credenciales de administrador de VDS | Recoja las credenciales de administrador de VDS existentes si ya las tiene. De lo contrario, se creará una nueva cuenta de administrador durante la implementación. |
| Región de Azure | Determine la región de Azure de destino en función del rendimiento y la disponibilidad de los servicios. Este "Herramienta de Microsoft" puede estimar el usuario final experimentado en función de la región. |
| Tipo de Active Directory | Las máquinas virtuales tendrán que unirse a un dominio, pero no pueden unirse directamente a Azure AD. La implementación de VDS puede crear una máquina virtual nueva o utilizar un controlador de dominio existente. |

| Elemento | Descripción |
| --- | --- |
| Gestión de ficheros | El rendimiento depende en gran medida de la velocidad del disco, especialmente en relación con el almacenamiento de los perfiles de usuario. El asistente de configuración de VDS puede implementar un simple servidor de archivos o configurar Azure NetApp Files (ANF). Para prácticamente cualquier entorno de producción se recomienda ANF. Sin embargo, para una prueba de concepto, la opción de servidor de archivos proporciona suficiente rendimiento. Las opciones de almacenamiento se pueden revisar tras la puesta en marcha, incluido el uso de los recursos de almacenamiento existentes en Azure. Consulte los precios ANF para obtener más información: https://azure.microsoft.com/en-us/pricing/details/netapp/ |
| Alcance de la red virtual | Se requiere un rango de red /20 enrutable para la implementación. El asistente de configuración de VDS le permitirá definir este rango. Es importante que esta gama no se superponga con ningún vNets existente en Azure o en las instalaciones (si las dos redes se conectarán a través de una VPN o ExpressRoute). |

#### Secciones de configuración de VDS

Inicie sesión en https://cwasetup.cloudworkspace.com/ Con las credenciales de administrador de Azure disponibles en la sección de requisitos previos.

### IaaS y plataforma

[]

### Nombre de dominio de Azure AD

El inquilino seleccionado hereda el nombre de dominio de Azure AD.

### Ubicación

Seleccione una **Región de Azure** adecuada. Este "Herramienta de Microsoft" puede estimar el usuario final experimentado en función de la región.

### Tipo de Active Directory

VDS se puede aprovisionar con una **nueva máquina virtual** para la función o configuración del controlador de dominio a fin de aprovechar un controlador de dominio existente. En esta guía seleccionaremos New Windows Server Active Directory, que creará una o dos VM (basadas en las opciones realizadas durante este proceso) en la suscripción.

Encontrará un artículo detallado que trata una implementación de AD existente "aquí".

### Nombre de dominio de Active Directory

Introduzca un **nombre de dominio**. Se recomienda reflejar el nombre de dominio de Azure AD de arriba.

### Gestión de archivos

VDS puede aprovisionar una máquina virtual de servidor de archivos simple o configurar Azure NetApp Files. En producción, Microsoft recomienda asignar 30 gb por usuario y hemos observado que es necesario asignar

5-15 IOPS por usuario para un rendimiento óptimo.

En un entorno de prueba de concepto (distinto a la producción), el servidor de archivos es una opción de puesta en marcha sencilla y de bajo coste, sin embargo, el rendimiento disponible de los discos gestionados de Azure se puede desbordar por el consumo de IOPS de incluso una pequeña puesta en marcha de producción.

Por ejemplo, un disco SSD estándar de 4 TB en Azure admite hasta 500 000 IOPS, lo cual solo permitiría un máximo de 100 usuarios totales a 5 IOPS/usuario. Con ANF Premium, una configuración de almacenamiento del mismo tamaño admitirá 16,000 una tasa de IOPS de 32 veces más IOPS.

Para implementaciones de AVD en producción, **Azure NetApp Files es la recomendación de Microsoft**.

Debe poner a disposición de Azure NetApp Files la suscripción a la que desee aplicar. Póngase en contacto con su representante de cuenta de NetApp o utilice este enlace: https://aka.ms/azurenetappfiles

También es necesario que registre NetApp como proveedor de su suscripción. Esto se puede hacer haciendo lo siguiente:

- Acceda a las suscripciones en el portal de Azure
  - Haga clic en proveedores de recursos
  - NetApp es un filtro
  - Seleccione el proveedor y haga clic en Registrar

#### Número de licencia de RDS

Se puede utilizar VDS de NetApp para poner en marcha entornos RDS y/o AVD. Al implementar AVD, este campo puede **permanecer vacío**.

#### ThinPrint

Se puede utilizar VDS de NetApp para poner en marcha entornos RDS y/o AVD. Al implementar AVD, esta palanca puede permanecer **OFF** (alternar a la izquierda).

#### Correo electrónico de notificación

VDS enviará notificaciones de implementación e informes de estado en curso al **correo electrónico proporcionado**. Esto se puede cambiar más adelante.

#### Equipos virtuales y red

Hay una variedad de servicios que necesitan ejecutarse para admitir un entorno VDS, a los que se hace referencia colectivamente como la “plataforma VDS”. En función de la configuración, estos pueden incluir CWMGR, una o dos puertas de enlace RDS, una o dos puertas de enlace HTML5, un servidor FTPS y una o dos VM de Active Directory.

La mayoría de las puestas en marcha de AVD aprovechan la opción de una única máquina virtual, ya que Microsoft gestiona las puertas de enlace AVD como servicio PaaS.

En entornos más pequeños y más sencillos, que incluyen casos de uso de RDS, todos estos servicios pueden condensarse en la opción de un solo equipo virtual con el fin de reducir los costes de equipos virtuales (con escalabilidad limitada). Para casos de uso RDS con más de 100 usuarios, se recomienda la opción de varias

máquinas virtuales para facilitar la escalabilidad de la puerta de enlace RDS o HTML5[]

### Configuración de máquinas virtuales de plataforma

Se puede utilizar VDS de NetApp para poner en marcha entornos RDS y/o AVD. Al implementar AVD, se recomienda seleccionar una única máquina virtual. En el caso de las puestas en marcha de RDS, deberá poner en marcha y gestionar componentes adicionales como Brokers y Gpuertas de enlace, en producción estos servicios se deberán ejecutar en máquinas virtuales dedicadas y redundantes. Para AVD, todos estos servicios son proporcionados por Azure como un servicio incluido y, por lo tanto, se recomienda la configuración de **una sola máquina virtual**.

### Máquina virtual única

Esta es la selección recomendada para las implementaciones que utilizarán exclusivamente AVD (y no RDS o una combinación de ambas). En una sola puesta en marcha de máquinas virtuales, los siguientes roles se alojan en una única máquina virtual en Azure:

- Director de CW
- Puerta de enlace HTML5
- Puerta de enlace RDS
- Aplicación remota
- FTPS Server (opcional)
- Función de controlador de dominio

El número máximo recomendado de usuarios para casos de uso de RDS en esta configuración es de 100 usuarios. La carga de puertas de enlace RDS/HTML5 equilibradas no es una opción en esta configuración, lo que limita la redundancia y las opciones para aumentar el escalado en el futuro. De nuevo, este límite no se aplica a las implementaciones de AVD, ya que Microsoft administra las puertas de enlace como servicio PaaS.

Si este entorno se está diseñando para multi-tenancy, no se admite una única configuración de máquina virtual, ni AVD ni AD Connect.

### Múltiples equipos virtuales

Al dividir la plataforma VDS en varias máquinas virtuales, los siguientes roles se alojan en máquinas virtuales dedicadas en Azure:

- Puerta de enlace de Escritorio remoto

  La configuración VDS se puede utilizar para implementar y configurar una o dos puertas de enlace RDS. Estas puertas de enlace transmiten la sesión de usuario de RDS desde la conexión a Internet abierta a las máquinas virtuales host de sesión dentro de la implementación. Las puertas de enlace RDS manejan una función importante, lo que protege a RDS de los ataques directos desde Internet abierta y para cifrar todo el tráfico de RDS dentro y fuera del entorno. Cuando se seleccionan dos puertas de enlace de Escritorio remoto, el programa de instalación VDS implementa 2 máquinas virtuales y las configura para equilibrar la carga de las sesiones de usuario RDS entrantes.

- Puerta de enlace HTML5

  La configuración VDS se puede utilizar para implementar y configurar una o dos puertas de enlace HTML5. Estas puertas de enlace alojan los servicios HTML5 que utiliza la función *Connect to Server* en VDS y el cliente VDS basado en web (portal H5). Cuando se seleccionan dos portales HTML5, el

programa de instalación VDS implementa 2 máquinas virtuales y las configura para equilibrar la carga de las sesiones de usuario HTML5 entrantes.

> Si se utiliza la opción de varios servidores (incluso si los usuarios sólo se conectan a través del cliente VDS instalado), se recomienda al menos una puerta de enlace HTML5 para habilitar la funcionalidad *Connect to Server* desde VDS.

- Notas de escalabilidad de la puerta de enlace

  En los casos de uso de RDS, el tamaño máximo del entorno se puede escalar con VM de puerta de enlace adicionales, cada puerta de enlace RDS o HTML5 que admite aproximadamente 500 usuarios. Posteriormente, se pueden agregar gateways adicionales con la asistencia de servicios profesionales de NetApp mínima

Si este entorno se está diseñando para multi-tenancy, se requiere la selección de varias máquinas virtuales.

**Zona horaria**

Mientras que la experiencia de los usuarios finales reflejará su zona horaria local, debe seleccionarse una zona horaria predeterminada. Seleccione la zona horaria en la que se realizará la **administración primaria** del entorno.

**Alcance de la red virtual**

Se recomienda aislar las máquinas virtuales en diferentes subredes según su propósito. En primer lugar, defina el alcance de la red y agregue un intervalo /20.

El programa de instalación de VDS detecta y sugiere un rango que debería resultar satisfactorio. Según las prácticas recomendadas, las direcciones IP de subred deben encontrarse en un rango de direcciones IP privadas.

Estos intervalos son:

- 192.168.0.0 hasta 192.168.255.255
- 172.16.0.0 hasta 172.31.255.255
- 10.0.0.0 hasta 10.255.255.255

Revise y ajuste si es necesario, haga clic en Validar para identificar subredes para cada una de las siguientes:

- Inquilino: Este es el intervalo en el que residirán los servidores host de sesión y los servidores de base de datos
- Servicios: Este es el rango en el que residirán servicios PaaS como Azure NetApp Files
- Plataforma: Esta es la gama en la que residirán los servidores de la plataforma
- Directorio: Este es el intervalo en el que residirán los servidores AD

**Revisar**

La página final ofrece la oportunidad de revisar sus opciones. Cuando haya completado la revisión, haga clic en el botón Validar. El programa de instalación de VDS revisará todas las entradas y comprobará que la implementación puede continuar con la información proporcionada. Esta validación puede tardar 2-10 minutos. Para seguir el progreso, puede hacer clic en el logotipo del registro (esquina superior derecha) para ver la actividad de validación.

Una vez finalizada la validación, aparecerá el botón de aprovisionamiento verde en lugar del botón Validar. Haga clic en aprovisionar para iniciar el proceso de aprovisionamiento para su implementación.

## Estado

El proceso de aprovisionamiento tarda entre 2-4 horas en función de la carga de trabajo de Azure y las opciones que elija. Puede seguir el progreso del registro haciendo clic en la página Estado o esperar el correo electrónico que le indicará que el proceso de implementación ha finalizado. La implementación crea las máquinas virtuales y los componentes de Azure necesarios para admitir la implementación de VDS y Remote Desktop o AVD. Esto incluye una sola máquina virtual que puede actuar como host de sesión de Escritorio remoto y como servidor de archivos. En una implementación AVD, esta máquina virtual sólo actuará como servidor de archivos.

#### Instalar y configurar AD Connect

Inmediatamente después de que la instalación se realice correctamente, AD Connect debe instalarse y configurarse en el controlador de dominio. En una configuración de VM de plataforma de singe, la máquina CWMGR1 es el DC. Los usuarios de AD deben sincronizarse entre Azure AD y el dominio local.

**Para instalar y configurar AD Connect, siga estos pasos:**

1. Conéctese al controlador de dominio como administrador de dominio.
    a. Obtenga las credenciales del almacén de claves de Azure (consulte "Aquí encontrará instrucciones sobre el almacén de claves")
2. Instale AD Connect, inicie sesión con el administrador de dominio (con permisos de rol de administrador empresarial) y el administrador global de Azure AD

#### Activación de servicios AVD

Una vez completada la implementación, el siguiente paso es activar la funcionalidad AVD. El proceso de habilitación de AVD requiere que Azure Administrator realice varios pasos para registrar su dominio de Azure AD y su suscripción para acceder a través de los servicios de Azure AVD. De igual modo, Microsoft requiere VDS para solicitar los mismos permisos a nuestra aplicación de automatización en Azure. Los siguientes pasos le guian por ese proceso.

#### Crear grupo de hosts AVD

El acceso de usuario final a las máquinas virtuales AVD se gestiona mediante grupos de hosts , que contienen las máquinas virtuales y grupos de aplicaciones, que a su vez contienen los usuarios y el tipo de acceso de usuario.

**Para construir su primer grupo de hosts**

1. Haga clic en el botón Agregar situado en el lado derecho del encabezado de la sección grupos de hosts AVD.[]
2. Introduzca un nombre y una descripción para el pool de hosts.
3. Seleccione un tipo de pool de hosts
    a. **Agrupado** significa que varios usuarios tendrán acceso al mismo grupo de máquinas virtuales con las mismas aplicaciones instaladas.
    b. **Personal** crea un pool de hosts en el que se asigna a los usuarios su propio equipo virtual host de sesión.
4. Seleccione el tipo Load Balancer

a. **Depth First** llenará la primera máquina virtual compartida al máximo número de usuarios antes de comenzar en la segunda máquina virtual del grupo

b. **La amplitud primero** distribuirá a los usuarios a todas las máquinas virtuales del pool de forma rotacional

5. Seleccione una plantilla de máquinas virtuales Azure para crear las máquinas virtuales en este pool. Aunque VDS mostrará todas las plantillas disponibles en la suscripción, recomendamos seleccionar la compilación multiusuario de Windows 10 más reciente para ofrecer la mejor experiencia. La compilación actual es Windows-10-20h1-evd. (Si lo desea, puede crear una imagen Gold utilizando la función de recopilación de aprovisionamiento para crear hosts a partir de una imagen de máquina virtual personalizada).
6. Seleccione el tamaño de la máquina de Azure. Para fines de evaluación, NetApp recomienda la serie D (tipo de máquina estándar para varios usuarios) o la serie E (configuración de memoria mejorada para escenarios multiusuario de servicio más pesado). Los tamaños de la máquina pueden cambiarse posteriormente en VDS si desea experimentar con series y tamaños diferentes
7. Seleccione un tipo de almacenamiento compatible para las instancias de disco gestionado de las máquinas virtuales en la lista desplegable
8. Seleccione la cantidad de máquinas virtuales que desea crear como parte del proceso de creación del pool de hosts. Es posible añadir máquinas virtuales al pool más tarde, pero VDS genera la cantidad de máquinas virtuales que solicita y las añade al pool de hosts una vez creado
9. Haga clic en el botón Add host pool para iniciar el proceso de creación. Puede realizar un seguimiento del progreso en la página AVD o ver los detalles del registro de procesos en la página de nombres de implementaciones/implementación de la sección tareas
10. Una vez creado el pool de hosts, aparecerá en la lista de grupos de hosts de la página AVD. Haga clic en el nombre del grupo de hosts para ver su página de detalles, que incluye una lista de sus máquinas virtuales , grupos de aplicaciones y usuarios activos

> ⓘ Los hosts AVD en VDS se crean con un ajuste que evita la conexión de sesiones de usuario. Esto se debe a que el diseño permite la personalización antes de aceptar las conexiones del usuario. Este ajuste se puede cambiar mediante la edición de la configuración del host de sesión. []

#### Habilite escritorios VDS para usuarios

Como se ha indicado anteriormente, VDS crea todos los elementos necesarios para admitir los espacios de trabajo de los usuarios finales durante la implementación. Una vez completada la implementación, el siguiente paso es habilitar el acceso al espacio de trabajo para cada usuario que desee introducir en el entorno de AVD. En este paso se crea la configuración del perfil y el acceso a la capa de datos de usuario final que es la opción predeterminada para los escritorios virtuales. VDS reusa esta configuración para vincular a los usuarios finales de Azure AD a los grupos de aplicaciones de AVD.

**Para habilitar espacios de trabajo para usuarios finales, siga estos pasos:**

1. Inicie sesión en VDS en https://manage.cloudworkspace.com Usar la cuenta de administrador principal de VDS que creó durante el aprovisionamiento. Si no recuerda la información de su cuenta, póngase en contacto con VDS de NetApp para obtener ayuda a la hora de recuperarla
2. Haga clic en el elemento de menú entornos de trabajo y, a continuación, haga clic en el nombre del área de trabajo que se creó automáticamente durante el aprovisionamiento
3. Haga clic en la ficha usuarios y grupos[]
4. Para cada usuario que desee activar, desplácese sobre el nombre de usuario y, a continuación, haga clic en el icono engranaje

5. Seleccione la opción “Activar área de trabajo en la nube”[]
6. El proceso de habilitación tarda aproximadamente 30-90 segundos en completarse. Tenga en cuenta que el estado del usuario cambiará de pendiente a disponible

> La activación de Azure AD Domain Services crea un dominio gestionado en Azure, y cada máquina virtual AVD creada se unirán a ese dominio. Para que el inicio de sesión tradicional en las máquinas virtuales funcione, 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.

**Habilite sesiones de usuario**

De manera predeterminada, los hosts de sesión no pueden aceptar conexiones de usuario. Este ajuste se denomina normalmente “modo de drenaje”, ya que se puede utilizar en producción para evitar nuevas sesiones de usuario, lo que permite al host eliminar con el tiempo todas las sesiones de usuario. Cuando se permiten nuevas sesiones de usuario en un host, esta acción se denomina normalmente la colocación del host de sesión “en rotación”.

En producción tiene sentido iniciar nuevos hosts en modo de drenaje, ya que normalmente hay tareas de configuración que deben completarse antes de que el host esté listo para las cargas de trabajo de producción.

En pruebas y evaluaciones puede quitar inmediatamente los hosts del modo de drenaje para habilitar las conexiones de usuarios y confirmar la funcionalidad. .Para habilitar sesiones de usuario en los hosts de sesión, siga estos pasos:

1. Desplácese a la sección AVD de la página del área de trabajo.
2. Haga clic en el nombre del pool de hosts bajo “grupos de hosts AVD”.[]
3. Haga clic en el nombre de los host de sesión y seleccione la casilla “permitir nuevas sesiones”, haga clic en “Actualizar host de sesión”. Repita esto para todos los hosts que deben colocarse en rotación.[]
4. Las estadísticas actuales de “permitir nueva sesión” también se muestran en la página principal del AVD para cada elemento de línea de host.

**Grupo de aplicaciones predeterminado**

Tenga en cuenta que Desktop Application Group se crea de forma predeterminada como parte del proceso de creación del pool de hosts. Este grupo proporciona acceso interactivo de escritorio a todos los miembros del grupo. .Para agregar miembros al grupo:

1. Haga clic en el nombre del grupo de aplicaciones[]
2. Haga clic en el vínculo que muestra el número de usuarios agregados[]
3. Seleccione los usuarios que desea agregar al grupo de aplicaciones marcando la casilla situada junto a su nombre
4. Haga clic en el botón Seleccionar usuarios
5. Haga clic en el botón Actualizar grupo de aplicaciones

**Crear grupos de aplicaciones AVD adicionales**

Se pueden agregar grupos de aplicaciones adicionales al grupo de hosts. Estos grupos de aplicaciones

publicarán aplicaciones específicas desde las máquinas virtuales del grupo de hosts a los usuarios de App Group mediante RemoteApp.

> AVD sólo permite que los usuarios finales se asignen al tipo de grupo de aplicaciones de escritorio o tipo de grupo de aplicaciones de RemoteApp, pero no a ambos en el mismo grupo de hosts, por lo que debe asegurarse de segregar a los usuarios en consecuencia. Si los usuarios necesitan acceder a aplicaciones de escritorio y streaming, se requiere un segundo grupo de hosts para alojar las aplicaciones.

**Para crear un nuevo grupo de aplicaciones:**

1. Haga clic en el botón Agregar en el encabezado de la sección de grupos de aplicaciones[]
2. Introduzca un nombre y una descripción para el grupo de aplicaciones
3. Seleccione los usuarios que desea agregar al grupo haciendo clic en el enlace Agregar usuarios. Seleccione cada usuario haciendo clic en la casilla de verificación situada junto a su nombre y, a continuación, haga clic en el botón Seleccionar usuarios[]
4. Haga clic en el vínculo Agregar RemoteApps para agregar aplicaciones a este grupo de aplicaciones. AVD genera automáticamente la lista de posibles aplicaciones escaneando la lista de aplicaciones instaladas en la máquina virtual . Seleccione la aplicación haciendo clic en la casilla de verificación situada junto al nombre de la aplicación y, a continuación, haga clic en el botón Seleccionar RemoteApps.[]
5. Haga clic en el botón Agregar grupo de aplicaciones para crear el grupo de aplicaciones

#### Acceso AVD de usuario final

Los usuarios finales pueden acceder a entornos AVD mediante Web Client o un cliente instalado en una variedad de plataformas

- Cliente web: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web
- URL de inicio de sesión en Web Client: http://aka.ms/AVDweb
- Cliente Windows: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10
- Cliente Android: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android
- Cliente MacOS: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos
- Cliente iOS: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios
- Cliente ligero IGEL: https://www.igel.com/igel-solution-family/windows-virtual-desktop/

Inicie sesión con el nombre de usuario y la contraseña del usuario final. Tenga en cuenta que las conexiones de Escritorio y aplicaciones remotas (RADC), Conexión a Escritorio remoto (mstsc) y la aplicación CloudWorksapce Client para Windows no admiten actualmente la capacidad de iniciar sesión en instancias AVD.

#### Supervisar los inicios de sesión de usuario

La página de detalles del pool de hosts también mostrará una lista de usuarios activos cuando inicien sesión en una sesión AVD.

#### Opciones de conexión de administración

Los administradores de VDS pueden conectarse a máquinas virtuales del entorno de diversas formas.

### Conectarse al servidor

En todo el portal, los administradores de VDS encontrarán la opción “conectar al servidor”. De forma predeterminada, esta función conecta el administrador a la máquina virtual generando dinámicamente credenciales de administración locales e inyectándolas en una conexión de cliente web. El administrador no necesita conocer (y nunca se proporciona con) las credenciales para conectarse.

Este comportamiento predeterminado se puede deshabilitar por administrador tal como se describe en la sección siguiente.

### Cuentas de administración de nivel 3 y .tech

En el proceso de instalación de CWA se crea una cuenta de administrador de “nivel III”. El nombre de usuario tiene el formato username.tech@domain.xyz

Estas cuentas, normalmente llamadas una cuenta “.tech”, se denominan cuentas de administrador de nivel de dominio. Los administradores de VDS pueden utilizar su cuenta .tech al conectarse a un servidor CWMGR1 (plataforma) y, opcionalmente, al conectarse a todas las demás máquinas virtuales del entorno.

Para desactivar la función de inicio de sesión de administrador local automático y forzar el uso de la cuenta de nivel III, cambie esta configuración. Vaya a VDS > Admins > Admin Name > Check “Tech Account Enabled”. Con esta casilla activada, el administrador de VDS no se iniciará sesión automáticamente en las máquinas virtuales como administrador local y se le pedirá que introduzca sus credenciales .tech.

Estas credenciales y otras credenciales relevantes se almacenan automáticamente en *Azure Key Vault* y se puede acceder a ellas desde el portal de gestión de Azure en https://portal.azure.com/.

#### Acciones opcionales posteriores a la implementación

### Autenticación multifactor (MFA)

VDS de NetApp incluye SMS/MFA de correo electrónico sin coste adicional. Esta función se puede utilizar para proteger cuentas de administrador de VDS o cuentas de usuario final."Artículo de MFA"

### Flujo de trabajo de asignación de aplicaciones

VDS proporciona un mecanismo para asignar a los usuarios finales acceso a las aplicaciones desde una lista predefinida de aplicaciones denominada Catálogo de aplicaciones. El catálogo de aplicaciones abarca todas las implementaciones gestionadas.

> El servidor TSD1 implementado automáticamente debe seguir siendo compatible con los derechos de aplicación. Específicamente, no ejecute la función “convertir en datos” contra esta máquina virtual.

La gestión de aplicaciones se detalla en este artículo: ""

### Grupos de seguridad de Azure AD

VDS incluye la funcionalidad de crear, rellenar y eliminar grupos de usuarios respaldados por Azure AD Security Groups. Estos grupos se pueden utilizar fuera de VDS de la misma forma que cualquier otro grupo de seguridad. En VDS, estos grupos se pueden utilizar para asignar permisos de carpeta y derechos de aplicación.

### Crear grupos de usuarios

La creación de grupos de usuarios se realiza en la ficha usuarios y grupos dentro de un área de trabajo.

### Asignar permisos de carpeta por grupo

Los permisos para ver y editar carpetas en el recurso compartido de la empresa se pueden asignar a usuarios o grupos.

""

### Asignar aplicaciones por grupo

Además de asignar aplicaciones a usuarios individualmente, las aplicaciones pueden aprovisionarse a los grupos.

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.[]

### Configurar las opciones de optimización de costes

La gestión de espacios de trabajo también se amplía a la gestión de los recursos de Azure que dan soporte a la implementación de AVD. VDS permite configurar tanto las planificaciones de cargas de trabajo como Live Scaling para activar y desactivar las máquinas virtuales de Azure en función de las actividades del usuario final. Estas funciones tienen como resultado la equiparación de gastos y la utilización de recursos de Azure con el patrón de uso real de los usuarios finales. Además, si ha configurado una implementación de prueba de concepto AVD, puede convertir toda la implementación desde la interfaz VDS.

### Programación de las cargas de trabajo

La programación de la carga de trabajo es una función que permite al administrador crear una programación definida para que las máquinas virtuales del área de trabajo estén activas para admitir sesiones de usuario final. Cuando se alcanza el final del período de tiempo programado para un día específico de la semana, VDS detiene/desasigna las máquinas virtuales en Azure de modo que se detengan los cargos por hora.

**Para activar la programación de cargas de trabajo:**

1. Inicie sesión en VDS en https://manage.cloudworkspace.com Usar las credenciales de VDS.
2. Haga clic en el elemento de menú Área de trabajo y, a continuación, haga clic en el nombre del área de trabajo de la lista. []
3. Haga clic en la pestaña Workload Schedule. []
4. Haga clic en el enlace gestionar en el encabezado Workload Schedule. []
5. Seleccione un estado predeterminado en la lista desplegable Estado: Siempre activado (predeterminado), siempre desactivado o programado.
6. Si selecciona programado, las opciones de Programación incluyen:
    a. Ejecutar a intervalos asignados cada día. Esta opción configura la programación como la misma hora de inicio y hora de finalización para los siete días de la semana. []
    b. Ejecutar en intervalo asignado para días especificados. Esta opción establece la programación en la misma hora de inicio y finalización sólo para los días seleccionados de la semana. Los días de la semana no seleccionados provocarán que VDS no encienda las máquinas virtuales durante esos días.

[]

c. Ejecutar a intervalos de tiempo y días variables. Esta opción establece la programación en distintas horas de inicio y de finalización para cada día seleccionado. []

d. Haga clic en el botón Update schedule cuando termine de establecer la programación. []

### Escalado en directo

Live Scaling activa y desactiva automáticamente las máquinas virtuales de un pool de hosts compartido, en función de la carga de usuarios simultáneos. A medida que cada servidor se llena, se activa un servidor adicional para que esté preparado cuando el equilibrador de carga del pool de hosts envía solicitudes de sesión de usuario. Para un uso efectivo de Live Scaling, elija “Depth First” como tipo de equilibrador de carga.

**Para activar Live Scaling:**

1. Inicie sesión en VDS en https://manage.cloudworkspace.com Usar las credenciales de VDS.
2. Haga clic en el elemento de menú Área de trabajo y, a continuación, haga clic en el nombre del área de trabajo de la lista. []
3. Haga clic en la pestaña Workload Schedule. []
4. Haga clic en el botón de opción Activado de la sección escala en directo. []
5. Haga clic en el número máximo de usuarios por servidor e introduzca el número máximo. Según el tamaño de la máquina virtual, este número suele estar entre 4 y 20. []
6. OPCIONAL: Haga clic en los servidores con alimentación adicional activados e introduzca un número de servidores adicionales que desee activar para el pool de hosts. Esta configuración activa el número especificado de servidores además del servidor de llenado activo para que actúe como búfer para grupos grandes de usuarios que inicien sesión en la misma ventana de tiempo. []

> Live Scaling se aplica actualmente a todos los pools de recursos compartidos. En un futuro próximo cada piscina tendrá opciones independientes de escalado en vivo.

### Apague toda la puesta en marcha

Si planea utilizar únicamente la implementación de evaluación en una base esporádica que no sea de producción, puede desactivar todos los equipos virtuales de la implementación cuando no los esté utilizando.

**Para activar o desactivar la implementación (es decir, desactivar las máquinas virtuales en la implementación), siga estos pasos:**

1. Inicie sesión en VDS en https://manage.cloudworkspace.com Usar las credenciales de VDS.
2. Haga clic en el elemento de menú implementaciones. []Desplace el cursor sobre la línea de implementación de destino para mostrar el icono de engranaje de configuración. []
3. Haga clic en el engranaje y, a continuación, seleccione Detener. []
4. Para reiniciar o comenzar, siga los pasos 1-3 y luego elija Iniciar. []

> Todas las máquinas virtuales de la implementación pueden tardar varios minutos en detenerse o iniciarse.

### Cree y gestione imágenes de máquinas virtuales

VDS incluye funcionalidad para crear y gestionar imágenes de máquinas virtuales para futuras implementaciones. Para acceder a esta funcionalidad, vaya a: VDS > despliegues > Nombre de despliegue >

Colecciones de aprovisionamiento. Las funciones de “colección de imágenes VDI” se documentan a continuación: ""

### Configure Azure Cloud Backup Service

VDS puede configurar y gestionar de forma nativa Azure Cloud Backup, un servicio PaaS de Azure para realizar backups de máquinas virtuales. Las políticas de backup pueden asignarse a máquinas individuales o grupos de máquinas por tipo o pool de hosts. Encontrará más información aquí: ""

### Seleccione el modo de gestión de aplicaciones/política

De forma predeterminada, VDS implementa una serie de objetos de directiva de grupo (GPO) que bloquean el área de trabajo del usuario final. Estas normas impiden el acceso a las ubicaciones de la capa de datos principal (p. ej., c:\) y la capacidad para realizar instalaciones de aplicaciones como usuario final.

Esta evaluación está pensada para demostrar las capacidades de Windows Virtual Desktop, por lo que tiene la opción de quitar los GPO de modo que pueda implementar un “espacio de trabajo básico” que proporcione la misma funcionalidad y acceso que un espacio de trabajo físico. Para ello, siga los pasos de la opción “Área de trabajo básica”.

También puede elegir utilizar el conjunto completo de funciones de administración de escritorios virtuales para implementar un “espacio de trabajo controlado”. Estos pasos incluyen la creación y administración de un catálogo de aplicaciones para el derecho a la aplicación de usuario final y el uso de permisos de nivel de administrador para administrar el acceso a las aplicaciones y carpetas de datos. Siga los pasos de la sección “Área de trabajo controlada” para implementar este tipo de espacio de trabajo en los grupos de hosts de AVD.

### Área de trabajo AVD controlada (directivas predeterminadas)

El uso de un espacio de trabajo controlado es el modo predeterminado para las implementaciones de VDS. Las directivas se aplican automáticamente. Este modo requiere que los administradores de VDS instalen aplicaciones y, a continuación, se concede a los usuarios finales acceso a la aplicación mediante un acceso directo en el escritorio de sesión. De forma similar, el acceso a las carpetas de datos se asigna a los usuarios finales mediante la creación de carpetas compartidas asignadas y la configuración de permisos para ver sólo las letras de la unidad asignada en lugar de las unidades de arranque y/o datos estándar. Para administrar este entorno, siga los pasos que se indican a continuación para instalar aplicaciones y proporcionar acceso al usuario final.

### Revertir al espacio de trabajo básico de AVD

La creación de un área de trabajo básica requiere deshabilitar las directivas de GPO predeterminadas que se crean de forma predeterminada.

**Para ello, siga este proceso único:**

1. Inicie sesión en VDS en https://manage.cloudworkspace.com uso de las credenciales de administrador principales.
2. Haga clic en el elemento de menú implementaciones de la izquierda. []
3. Haga clic en el nombre de la implementación. []
4. En la sección servidores de plataforma (página central a la derecha), desplácese a la derecha de la línea para CWMGR1 hasta que aparezca la marcha. []
5. Haga clic en el engranaje y seleccione conectar. []
6. Introduzca las credenciales “Tech” que creó durante el aprovisionamiento para iniciar sesión en el servidor CWMGR1 mediante el acceso HTML5. []

7. Haga clic en el menú Inicio (Windows) y seleccione Herramientas administrativas de Windows. []
8. Haga clic en el icono Administración de directivas de grupo. []
9. Haga clic en el elemento AADDC Users en la lista del panel izquierdo. []
10. Haga clic con el botón derecho del ratón en la política “usuarios de área de trabajo en la nube” de la lista del panel derecho y, a continuación, anule la selección de la opción “Vincular activado”. Haga clic en Aceptar para confirmar esta acción. [] []
11. Seleccione Acción, actualización de directiva de grupo en el menú y, a continuación, confirme que desea forzar una actualización de directiva en esos equipos. []
12. Repita los pasos 9 y 10 pero seleccione “usuarios de ADDC” y “Empresas de área de trabajo en la nube” como política para desactivar el enlace. No es necesario forzar la actualización de una directiva de grupo después de este paso. [] []
13. Cierre las ventanas Editor de administración de directivas de grupo y Herramientas administrativas y, a continuación, cierre la sesión. []Estos pasos proporcionarán un entorno de espacio de trabajo básico para los usuarios finales. Para confirmar, inicie sesión como una de sus cuentas de usuario final: El entorno de sesión no debe tener ninguna restricción de área de trabajo controlada, como el menú Inicio oculto, acceso bloqueado a la unidad C:\ y el panel de control oculto.

La cuenta .tech que se creó durante la implementación tiene acceso completo para instalar aplicaciones y cambiar la seguridad en carpetas independientemente de VDS. No obstante, si desea que los usuarios finales del dominio de Azure AD tengan un acceso completo similar, debe añadirlos al grupo Administradores local en cada máquina virtual.

## Guía de despliegue de AVD - existente AD suplementario

#### Descripción general

El programa de instalación de VDS tiene la capacidad de conectar una nueva implementación a una estructura de AD existente. Estas instrucciones cubren esta opción en detalle. Este artículo no es independiente, más bien es una explicación detallada de una alternativa a la opción Nueva AD que se trata en el "Guía de implementación de AVD"

#### Tipo de Active Directory

La siguiente sección define el tipo de implementación de Active Directory para la implementación de VDS. En esta guía seleccionaremos Active Directory de Windows Server existente, que aprovechará una estructura de AD que ya existe.

#### Red AD existente

El programa de instalación de VDS mostrará una lista de vNets que podría representar la conexión entre la estructura de AD existente y Azure AD. El vNet que seleccione debe tener un centro de datos alojado en Azure que haya configurado en Azure. Además, vNet tendrá la configuración de DNS personalizada apuntando al DC alojado en Azure.

[]

#### Nombre de dominio de Active Directory existente

Introduzca el nombre de dominio existente que se utilizará. Nota: No desea utilizar el dominio que se encuentra en el portal de Azure en el módulo Active Directory, ya que puede provocar problemas de DNS. El ejemplo principal de esto es que los usuarios no podrán acceder al sitio web (<yourdomain>.com, por ejemplo)

desde el interior de su escritorio.

#### Nombre de usuario y contraseña de AD existentes

Existen tres formas de proporcionar las credenciales necesarias para facilitar una implementación utilizando una estructura AD existente.

1. Proporcione el nombre de usuario y la contraseña del administrador de dominio de Active Directory

   Este es el método más sencillo: Proporciona credenciales de administrador de dominio que se utilizan para facilitar la implementación.

   > Esta cuenta se puede crear para un fin único y se puede eliminar una vez completado el proceso de implementación.

2. Crear permisos necesarios de coincidencia de cuentas

   Este método implica a los administradores de clientes crear manualmente la estructura de permisos aquí y, a continuación, introducir las credenciales de la cuenta CloudWorkspaceSVC aquí y continuar.

3. Proceso de puesta en marcha manual

   Póngase en contacto con el soporte de VDS de NetApp para obtener ayuda en la configuración del acceso de AD con los principales de cuenta con privilegios menos.

#### Siguientes pasos

En este artículo se tratan los pasos exclusivos que se deben seguir para implementar en un entorno AD existente. Con estos pasos completos, puede volver a la guía de implementación estándar "aquí".

### Componentes y permisos de VDS

#### Servicios y entidades de seguridad AVD y VDS

Azure Virtual Desktop (AVD) requiere cuentas y componentes de seguridad tanto en Azure AD como en el Active Directory local para realizar acciones automatizadas. Virtual Desktop Service (VDS) de NetApp crea componentes y configuraciones de seguridad durante el proceso de implementación que permiten a los administradores controlar el entorno AVD. Este documento describe las cuentas, componentes y configuraciones de seguridad de VDS relevantes en ambos entornos.

Los componentes y permisos del proceso de automatización de implementación se diferencian en su mayor parte de los componentes del entorno implementado final. Por lo tanto, este artículo se construye en dos secciones principales, como en la sección de automatización de la puesta en marcha y en la sección de entorno puesto en marcha.

[anchura = 75%]

#### Componentes y permisos de automatización de implementación de AVD

La implementación de VDS utiliza múltiples componentes de Azure y NetApp y permisos de seguridad para implementar tanto implementaciones como espacios de trabajo.

### Aplicaciones de negocio

VDS utiliza aplicaciones empresariales y registros de aplicaciones en el dominio de Azure AD de un inquilino. Las aplicaciones empresariales son el conducto para las llamadas en el Administrador de recursos de Azure, Azure Graph y (si se utiliza la versión de otoño de AVD) extremos de la API AVD desde el contexto de seguridad de la instancia de Azure AD utilizando las funciones y permisos delegados otorgados al Director de servicios asociado. Los registros de aplicaciones se pueden crear en función del estado de inicialización de los servicios AVD para el inquilino a través de VDS.

Para permitir la creación y la gestión de estas máquinas virtuales, VDS crea varios componentes de soporte en la suscripción a Azure:

### Espacio de trabajo en cloud

Se trata de los administradores iniciales de la aplicación empresarial que conceden su consentimiento y se utilizan durante el proceso de implementación del Asistente para la instalación de VDS.

La aplicación Cloud Workspace Enterprise solicita un conjunto específico de permisos durante el proceso de instalación de VDS. Estos permisos son:

- Access Directory como usuario firmado en (delegado)
- Leer y escribir datos de directorio (delegado)
- Iniciar sesión y leer el perfil de usuario (delegado)
- Iniciar sesión de usuarios (delegado)
- Ver el perfil básico de los usuarios (delegado)
- Acceder a la gestión de servicios de Azure como usuarios de organización (delegados)

### API de espacio de trabajo en cloud

Gestiona las llamadas de administración generales para las funciones PaaS de Azure. Algunos ejemplos de funciones de PaaS de Azure son Azure Compute, Azure Backup, Azure Files, etc. Este Director de servicio requiere derechos de propietario para la suscripción de Azure de destino durante la implementación inicial y derechos de colaborador para la administración continua (nota: El uso de Azure Files requiere derechos de propietario de suscripción para establecer permisos por usuario en objetos de archivo de Azure).

La aplicación de empresa de la API de área de trabajo en la nube solicita un conjunto específico de permisos durante el proceso de instalación de VDS. Estos permisos son:

- Colaborador de la suscripción (o propietario de la suscripción si se utiliza Azure Files)
- Azure AD Graph
  - Leer y escribir todas las aplicaciones (aplicación)
  - Administrar las aplicaciones que esta aplicación crea o posee (aplicación)
  - Dispositivos de lectura y escritura (aplicación)
  - Acceder al directorio como usuario firmado (delegado)
  - Leer datos de directorio (aplicación)
  - Leer datos de directorio (delegados)
  - Datos de directorio de lectura y escritura (aplicación)

    - Leer y escribir datos de directorio (delegado)
    - Dominios de lectura y escritura (aplicación)
    - Leer todos los grupos (delegados)
    - Leer y escribir todos los grupos (delegados)
    - Leer todas las pertenencias ocultas (aplicación)
    - Leer miembros ocultos (delegados)
    - Iniciar sesión y leer el perfil de usuario (delegado)
    - Leer todos los perfiles completos de los usuarios (delegados)
    - Leer todos los perfiles básicos de los usuarios (delegados)
- Gestión de servicios de Azure
    - Acceder a la gestión de servicios de Azure como usuarios de organización (delegados)

**VDS de NetApp**

Los componentes VDS de NetApp se utilizan a través del plano de control VDS para automatizar la implementación y configuración de las funciones, los servicios y los recursos de AVD.

**Función personalizada**

La función Automation Contributor se crea para facilitar la implementación mediante metodologías con menos privilegios. Este rol permite que la máquina virtual CWMGR1 acceda a la cuenta de automatización de Azure.

**Cuenta de automatización**

Se crea una cuenta de automatización durante la puesta en marcha y es un componente necesario durante el proceso de aprovisionamiento. La cuenta de automatización contiene variables, credenciales, módulos y configuraciones de estado deseadas y hace referencia al almacén de claves.

**Configuración de estado deseada**

Este es el método utilizado para crear la configuración de CWMGR1 el archivo de configuración se descarga en el equipo virtual y se aplica a través del Administrador de configuración local en el equipo virtual. Entre los ejemplos de elementos de configuración se incluyen:

- Instalación de las características de Windows
- Instalando software
- Aplicación de configuraciones de software
- Asegurarse de que se aplican los conjuntos de permisos adecuados
- Aplicar el certificado Encripto de Let
- Asegurarse de que los registros DNS son correctos
- Asegurar que CWMGR1 se una al dominio

**Módulos:**

- ActiveDirectoryDsc: Recurso de configuración de estado deseado para la implementación y la configuración de Active Directory. Estos recursos le permiten configurar nuevos dominios, dominios secundarios y controladores de dominio de alta disponibilidad, establecer confianzas entre dominios y

administrar usuarios, grupos y UO.

- AZ.Accounts: Un módulo proporcionado por Microsoft que se utiliza para gestionar credenciales y elementos de configuración comunes para módulos de Azure
- AZ.Automation: Un módulo proporcionado por Microsoft para commandlets de Azure Automation
- Az.Compute:A Microsoft proporcionó un módulo para commandlets de Azure Compute
- AZ.KeyVault: Un módulo proporcionado por Microsoft para los commandlets de Azure Key Vault
- AZ.Resources: Un módulo proporcionado por Microsoft para commandlets de Azure Resource Manager
- CChoco: Recurso de configuración de estado deseado para descargar e instalar paquetes usando Chocolatey
- CjAz: Este módulo creado por NetApp proporciona herramientas de automatización para el módulo de automatización de Azure
- CjAzACS: Este módulo creado por NetApp contiene funciones de automatización del entorno y procesos de PowerShell que se ejecutan desde el contexto del usuario.
- CjAzBuild: Este módulo creado por NetApp contiene procesos de automatización de compilación y mantenimiento y de PowerShell que se ejecutan desde el contexto del sistema.
- CNtfsAccessControl: Recurso de configuración de estado deseado para la administración de control de acceso NTFS
- ComputerManagementDsc: Recurso de configuración de estado deseado que permite tareas de administración de equipos como unirse a un dominio y programar tareas, así como configurar elementos como memoria virtual, registros de eventos, zonas horarias y configuración de energía.
- CUserRightsAssignment: Recurso de configuración de estado deseado que permite la administración de derechos de usuario, como derechos de inicio de sesión y privilegios
- NetworkingDsc: recurso de configuración de estado deseado para la red
- XCertificate: Recurso de configuración de estado deseado para simplificar la administración de certificados en Windows Server.
- XDnsServer: Recurso de configuración de estado deseado para la configuración y administración de Windows Server DNS Server
- XNetworking: Recurso de configuración de estado deseado relacionado con las redes.
- "XRemoteDesktopAdmin": Este módulo utiliza un repositorio que contiene los recursos de configuración de estado deseados para configurar la configuración de escritorio remoto y el firewall de Windows en una máquina local o remota.
- XRemoteDesktopSessionHost: Recurso de configuración de estado deseado (xRDSessionDeployment, xRDSessionCollection, xRDSessionCollectionConfiguration y xRDRemoteApp) que permite la creación y configuración de una instancia de Remote Desktop Session Host (RDSH)
- XSmbShare: Recurso de configuración de estado deseado para la configuración y administración de un recurso compartido SMB
- XSystemSecurity: Recurso de configuración de estado deseado para administrar UAC e IE Esc

Azure Virtual Desktop también instala componentes de Azure, como aplicaciones empresariales y registros de aplicaciones para Azure Virtual Desktop y Azure Virtual Desktop Client, AVD Tenant, AVD Host Pools, AVD App Groups y AVD Registered Virtual Machines. Aunque los componentes de VDS Automation gestionan estos componentes, AVD controla su configuración predeterminada y su conjunto de atributos, consulte la documentación de AVD para obtener más información.

### Componentes AD híbridos

Para facilitar la integración con AD existente o en ejecución en el cloud público, se necesitan componentes y permisos adicionales en el entorno AD existente.

### Controlador de dominio

El controlador de dominio existente se puede integrar en una puesta en marcha de AVD a través de AD Connect y/o una VPN sitio a sitio (o Azure ExpressRoute).

### Conexión DE ANUNCIOS

Para facilitar la autenticación de usuarios con éxito a través de los servicios PaaS de AVD, se puede utilizar AD Connect para sincronizar el controlador de dominio con Azure AD.

### Grupo de seguridad

VDS utiliza un grupo de seguridad de Active Directory denominado CW-Infrastructure para contener los permisos necesarios para automatizar las tareas dependientes de Active Directory, como la unión de dominio y los datos adjuntos de directivas de GPO.

### Cuenta de servicio

VDS utiliza una cuenta de servicio de Active Directory denominada CloudworkspaceSVC que se utiliza como identidad para los servicios de Windows VDS y el servicio de aplicación IIS. Esta cuenta no es interactiva (no permite el inicio de sesión RDP) y es el miembro principal de la cuenta CW-Infrastructure

### VPN o ExpressRoute

Se puede utilizar una VPN de sitio a sitio o Azure ExpressRoute para unir directamente las máquinas virtuales de Azure con el dominio existente. Se trata de una configuración opcional disponible cuando lo exijan los requisitos del proyecto.

### Delegación local de permisos de AD

NetApp proporciona una herramienta opcional que puede agilizar el proceso de AD híbrido. Si se utiliza la herramienta opcional de NetApp, deberá:

- Ejecute en un sistema operativo de servidor en lugar de en un sistema operativo de estación de trabajo
- Se ejecuta en un servidor que está Unido al dominio o es un controlador de dominio
- Tener instalado PowerShell 5.0 o posterior en el servidor que ejecuta la herramienta (si no se ejecuta en el controlador de dominio) y en el controlador de dominio
- Ser ejecutado por un usuario con privilegios de administrador de dominio O ser ejecutado por un usuario con permisos de administrador local y capacidad de proporcionar una credencial de administrador de dominio (para utilizarla con runas)

Tanto si se crea manualmente como si se aplica a la herramienta de NetApp, los permisos necesarios son los siguientes:

- Grupo CW-Infrastructure
  - El grupo de seguridad Infraestructura de área de trabajo en la nube (**CW-Infrastructure**) tiene el control total al nivel OU de área de trabajo en la nube y a todos los objetos descendientes

    - Zona DNS de <deployment code>.cloudWorkspace.app: El grupo CW-Infrastructure otorgó a CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree ExtendedRight, Delete, GenericWrite
    - Servidor DNS: Grupo CW-Infrastructure concedido a ReadProperty, GenericExecute
    - Acceso de administración local para equipos virtuales creados (CMMGR1, equipos virtuales de sesión AVD) (realizado por la política de grupo en los sistemas AVD gestionados)
- Grupo CW-CWMGRACcess este grupo proporciona derechos administrativos locales a CWMGR1 en todas las plantillas, el único servidor, la nueva plantilla nativa de Active Directory utiliza los grupos integrados operadores de servidor usuarios de escritorio remoto y operadores de configuración de red.

#### Componentes y permisos del entorno AVD

Una vez completado el proceso de automatización de la puesta en marcha, el uso y la administración constantes de implementaciones y espacios de trabajo requiere un conjunto distinto de componentes y permisos, tal como se define a continuación. Muchos de los componentes y permisos anteriores siguen siendo relevantes pero esta sección se centra en definir la estructura de un despliegue.

Los componentes de las implementaciones y áreas de trabajo de VDS se pueden organizar en varias categorías lógicas:

- Clientes de usuario final
- Componentes del plano de control VDS
- Componentes de Microsoft Azure AVD-PaaS
- Componentes de la plataforma VDS
- Componentes de espacio de trabajo VDS en Azure Tenant
- Componentes AD híbridos

### Clientes de usuario final

Los usuarios pueden conectarse a su escritorio AVD y/o desde una variedad de tipos de punto final. Microsoft ha publicado aplicaciones de cliente para Windows, MacOS, Android e iOS. Además, hay un cliente web disponible para el acceso sin cliente.

Hay algunos proveedores de Thin-Client de Linux que han publicado el cliente de extremo para AVD. Se enumeran en https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

### Componentes del plano de control VDS

### API REST DE VDS

VDS se basa en API DE REST totalmente documentadas de forma que todas las acciones disponibles en la aplicación web también estén disponibles a través de la API. La documentación de la API está aquí: https://api.cloudworkspace.com/5.4/swagger/ui/index#

### Aplicación web VDS

Los administradores de VDS pueden interactuar con LA aplicación ADS a través de la aplicación web VDS. Este portal web está en: https://manage.cloudworkspace.com

### Base de datos del plano de control

Los datos y la configuración de VDS se almacenan en la base de datos de SQL del plano de control, que NetApp aloja y gestiona.

### Comunicaciones VDS

### Componentes de inquilino de Azure

La automatización de la implementación de VDS crea un único grupo de recursos de Azure para contener los otros componentes de AVD, incluidas las máquinas virtuales, las subredes de red, los grupos de seguridad de red y los contenedores de Azure Files o los pools de capacidad de Azure NetApp Files. Nota: El valor predeterminado es un solo grupo de recursos, pero VDS tiene herramientas para crear recursos en grupos de recursos adicionales, si lo desea.

### Componentes de Microsoft Azure AVD-PaaS

### API REST AVD

Microsoft AVD se puede administrar a través de la API. VDS aprovechó estas API de forma extensiva para automatizar y gestionar entornos AVD. La documentación se encuentra en: https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/

### Agente de sesiones

El agente determina los recursos autorizados para el usuario y organiza la conexión del usuario a la puerta de enlace.

### Diagnóstico de Azure

Azure Diagnostics se ha creado especialmente para admitir las puestas en marcha de AVD.

### Cliente web AVD

Microsoft ha proporcionado un cliente Web para que los usuarios se conecten a sus recursos AVD sin un cliente instalado localmente.

### Puerta de enlace de la sesión

El cliente RD instalado localmente se conecta a la puerta de enlace para comunicarse de forma segura con el entorno AVD.

### Componentes de la plataforma VDS

### CWMGR1

CMWGR1 es la VM de control de VDS para cada implementación. De forma predeterminada, se crea como máquina virtual de Windows 2019 Server en la suscripción de Azure de destino. Consulte la sección implementación local para obtener la lista de componentes VDS y de terceros instalados en CWMGR1.

AVD requiere que los equipos virtuales AVD se unen a un dominio de Active Directory. Para facilitar este proceso y proporcionar las herramientas de automatización para administrar el entorno VDS, se instalan varios componentes en la VM de CWMGR1 descrita anteriormente y se agregan varios componentes a la instancia de AD. Entre los componentes se incluyen:

- **Servicios de Windows**: VDS utiliza servicios de Windows para realizar acciones de automatización y administración desde una implementación:
  - **CW Automation Service** es un servicio de Windows implementado en CWMGR1 en cada implementación de AVD que realiza muchas de las tareas de automatización orientadas al usuario en el entorno. Este servicio se ejecuta en la cuenta de AD **CloudWorkspaceSVC**.
  - **CW VM Automation Service** es un servicio de Windows implementado en CWMGR1 en cada implementación de AVD que realiza las funciones de administración de máquinas virtuales. Este servicio se ejecuta en la cuenta de AD **CloudWorkspaceSVC**.
  - **CW Agent Service** es un servicio de Windows implementado en cada máquina virtual bajo administración VDS, incluido CWMGR1. Este servicio se ejecuta bajo el contexto **LocalSystem** de la máquina virtual.
  - **CWManagerX API** es un listener basado en grupos de aplicaciones de IIS instalado en CWMGR1 en cada implementación de AVD. De esta forma se manejan las solicitudes entrantes desde el plano de control global y se ejecuta en la cuenta de AD **CloudWorkspaceSVC**.
- **SQL Server 2017 Express** – VDS crea una instancia de SQL Server Express en el equipo virtual CWMGR1 para administrar los metadatos generados por los componentes de automatización.
- **Servicios de Internet Information Server (IIS)**: IIS está habilitado en CWMGR1 para alojar la aplicación IIS CWManagerX y CWApps (sólo si está habilitada la funcionalidad RemoteApp de RDS). VDS requiere IIS versión 7.5 o superior.
- **HTML5 Portal (opcional)** – VDS instala el servicio Spark Gateway para proporcionar acceso HTML5 a los equipos virtuales en la implementación y desde la aplicación web VDS. Se trata de una aplicación basada en Java y se puede desactivar y eliminar si no se desea utilizar este método de acceso.
- **Puerta de enlace de RD (opcional)** – VDS permite que la función Puerta de enlace de RD en CWMGR1 proporcione acceso RDP a agrupaciones de recursos basadas en colección RDS. Este rol se puede deshabilitar/desinstalar si sólo se desea acceder a AVD Reverse Connect.
- **RD Web (opcional)** – VDS activa la función Web de RD y crea la aplicación web de CWApps IIS. Esta función se puede desactivar si sólo se desea el acceso AVD.
- **Configuración de DC**: Aplicación de Windows que se utiliza para realizar tareas de configuración avanzadas y configuración específicas del sitio de implementación y VDS.
- **Herramientas de VDC de prueba**: Aplicación de Windows que admite la ejecución directa de tareas para los cambios de configuración de Virtual Machine y a nivel de cliente utilizados en el raro caso en que las tareas de API o aplicaciones Web necesitan ser modificadas para la solución de problemas.
- **A continuación, cifrar certificado comodín (opcional)** – creado y gestionado por VDS – todas las VM que requieren tráfico HTTPS sobre TLS se actualizan con el certificado todas las noches. La renovación también se gestiona mediante una tarea automatizada (los certificados son de 90 días, por lo que la renovación comienza poco antes). El cliente puede proporcionar su propio certificado comodín si lo desea. VDS también requiere varios componentes de Active Directory para admitir las tareas de automatización. La intención del diseño es utilizar un número mínimo de componentes de AD y adiciones de permisos, al tiempo que se da soporte al entorno para una gestión automatizada. Entre estos componentes se incluyen:
- **Unidad organizativa de espacio de trabajo en la nube (OU)**: Esta Unidad de organización actuará como contenedor principal de AD para los componentes secundarios necesarios. Los permisos para los grupos de acceso de CW-Infrastructure y DHP Client se establecerán en este nivel y en sus componentes secundarios. Consulte el Apéndice A para obtener información sobre las subunidades organizativas creadas en esta unidad organizativa.
- **Cloud Workspace Infrastructure Group (CW-Infrastructure)** es un grupo de seguridad creado en el AD local que permite asignar los permisos delegados requeridos a la cuenta de servicio VDS (**CloudWorkspaceSVC**)

- **Client DHP Access Group (ClientDHPAccess)** es un grupo de seguridad creado en el AD local para permitir que VDS gobierne la ubicación en la que residen los datos de perfil y de casa de usuario compartidos de la empresa.
- **Cuenta de servicio CloudWorkspaceSVC** (miembro del grupo de infraestructura de Cloud Workspace)
- **Zona DNS para el dominio <deployment code>.cloudWorkspace.app** (este dominio administra los nombres DNS creados automáticamente para los equipos virtuales host de sesión ), creados mediante la configuración de implementación.
- **GPO específicos de NetApp** vinculado a varias unidades organizativas secundarias de la unidad organizativa de espacio de trabajo cloud. Estos GPO son:
  - **GPO de área de cloud (vinculado a unidad organizativa de área de cloud)**: Define protocolos y métodos de acceso para miembros del grupo de infraestructura CW. También agrega el grupo al grupo de administradores local en los hosts de sesión de AVD.
  - **GPO** de firewall de área de trabajo en la nube (vinculado a servidores dedicados de clientes, unidades de escritorio remotas y unidades organizativas de ensayo): Crea una directiva que garantiza y aísla las conexiones a los hosts de sesiones desde servidores de plataforma.
  - **RDS** de espacio de trabajo en la nube (servidores de clientes dedicados, unidades de escritorio remotas y unidades de control de estado): Límites de definición de directivas para la calidad de la sesión, la fiabilidad y los límites de tiempo de espera de desconexión. Para las sesiones RDS, se define el valor del servidor de licencias TS.
  - **Empresas de área de trabajo en la nube** (NO VINCULADAS de forma predeterminada) – GPO opcional para "bloquear" una sesión/espacio de trabajo de usuario impidiendo el acceso a herramientas y áreas administrativas. Se puede vincular/activar para proporcionar un espacio de trabajo de actividad restringida.

> Las configuraciones predeterminadas de la configuración de la directiva de grupo se pueden proporcionar a petición.

**Componentes del área de trabajo VDS**

**Capa de datos**

**Azure NetApp Files**

Se creará un pool de capacidad de Azure NetApp Files y los volúmenes asociados si selecciona Azure NetApp Files como la opción de capa de datos en la configuración de VDS. El volumen aloja el almacenamiento archivado compartido para perfiles de usuario (a través de contenedores FSLogix), carpetas personales de usuario y la carpeta de recursos compartidos de datos corporativos.

**Azure Files**

Se creará un recurso compartido de archivos de Azure y su cuenta de almacenamiento de Azure asociada si eligió Azure Files como opción de capa de datos en el programa de instalación de CWS. Azure File Share aloja el almacenamiento compartido archivado para perfiles de usuario (a través de contenedores FSLogix), carpetas personales de usuario y la carpeta de recursos compartidos de datos corporativos.

**Servidor de archivos con disco gestionado**

Se crea una máquina virtual de Windows Server con un disco gestionado si se elige servidor de archivos como la opción capa de datos en la instalación de VDS. El servidor de archivos aloja el almacenamiento archivado compartido para perfiles de usuario (a través de contenedores FSLogix), carpetas personales de

usuario y la carpeta de recursos compartidos de datos corporativos.

### Redes de Azure

#### Red virtual de Azure

VDS crea una red virtual de Azure y admite subredes. VDS requiere una subred independiente para los equipos host de CWMGR1, AVD y los controladores de dominio de Azure y la interconexión entre las subredes. Tenga en cuenta que la subred del controlador AD normalmente ya existe, de modo que las subredes implementadas VDS tendrán que tener una relación entre iguales con la subred existente.

#### Grupos de seguridad de red

Se crea un grupo de seguridad de red para controlar el acceso a la máquina virtual CWMGR1.

- Inquilino: Contiene direcciones IP para utilizarlas por host de sesión y máquinas virtuales de datos
- Servicios: Contiene direcciones IP que los utilizan los servicios PaaS (por ejemplo, Azure NetApp Files).
- Plataforma: Contiene direcciones IP para usarlas como equipos virtuales de la plataforma de NetApp (CWMGR1 y cualquier servidor de pasarela)
- Directorio: Contiene direcciones IP para utilizarlas como equipos virtuales de Active Directory

### Azure AD

La automatización y orquestación de VDS implementan máquinas virtuales en una instancia de Active Directory de destino y, a continuación, las une al pool de hosts designado. Las máquinas virtuales AVD se rigen a nivel de equipo por la estructura AD (unidades organizativas, política de grupo, permisos de administrador de equipos locales, etc.) y la pertenencia a la estructura AVD (pools de hosts, pertenencia a grupos de aplicaciones de área de trabajo), que se rigen por entidades y permisos de Azure AD. VDS gestiona este entorno de “control doble” mediante la aplicación VDS Enterprise/Azure Service Principal para las acciones AVD y la cuenta de servicio AD local (CloudWorkspaceSVC) para las acciones locales de AD y equipos locales.

Los pasos específicos para crear una máquina virtual AVD y agregarla al grupo de hosts AVD incluyen:

- Crear una máquina virtual desde Azure que sea visible para la suscripción de Azure asociada con AVD (utiliza los permisos de Azure Service Principal)
- Comprobar/configurar la dirección DNS de la nueva máquina virtual utilizando la vnet de Azure designada durante la implementación de VDS (requiere permisos AD locales (todo delegado a CW-Infrastructure anteriormente) establece el nombre de la máquina virtual utilizando el esquema de nomenclatura VDS estándar ***{emprescode}TS{sequencenumber}***. Ejemplo: XYZTS3. (Requiere permisos AD locales (colocados en la estructura de unidad organizativa que hemos creado en las instalaciones (escritorio remoto/empresa/compartido) (mismo permiso/descripción de grupo que anteriormente)
- Coloca la máquina virtual en la unidad organizativa (AD) designada de Active Directory (requiere los permisos delegados a la estructura de la unidad organizativa (designados durante el proceso manual anterior).
- Actualizar el directorio DNS interno de AD con la nueva dirección IP/nombre del equipo (requiere permisos locales de AD)
- Unir una nueva máquina virtual al dominio de AD local (requiere permisos locales de AD)
- Actualizar la base de datos local VDS con información de servidor nueva (no requiere permisos adicionales)

- Unirse a VM al grupo de hosts AVD designado (requiere permisos del director del servicio AVD)
- Instalar los componentes de Chocolatey en la nueva máquina virtual (requiere privilegios administrativos locales para la cuenta **CloudWorkspaceSVC**)
- Instalar componentes FSLogix para la instancia AVD (requiere permisos administrativos de equipo local en la unidad organizativa AVD en el AD local)
- Actualice el GPO de Firewall de Windows AD para permitir el tráfico a la nueva máquina virtual (requiere crear/modificar GPO de AD para las directivas asociadas con la unidad organizativa AVD y sus máquinas virtuales asociadas. Requiere la creación/modificación de directivas de GPO de AD en la unidad organizativa AVD en el AD local. Es posible desactivar la instalación posterior si no se gestionan máquinas virtuales mediante VDS.)
- Establecer el indicador “permitir nuevas conexiones” en la nueva máquina virtual (requiere permisos de Azure Service Principal)

#### Unión de máquinas virtuales a Azure AD

Las máquinas virtuales del inquilino de Azure deben unirse al dominio, pero las máquinas virtuales no se pueden unir directamente a Azure AD. Por lo tanto, VDS implementa el rol de controladora de dominio en la plataforma VDS y, a continuación, lo sincronizamos con Azure AD mediante AD Connect. Las opciones de configuración alternativas incluyen el uso de Azure AD Domain Services (ADDS), la sincronización con un centro de datos híbrido (una máquina virtual local o en otro lugar) mediante AD Connect o la unión directa de los equipos virtuales a un centro de datos híbrido a través de una VPN de sitio a sitio o Azure ExpressRoute.

#### Piscinas de host AVD

Los pools de hosts son una colección de una o más máquinas virtuales idénticas (VM) dentro de los entornos de Azure Virtual Desktop. Cada pool de hosts puede contener un grupo de aplicaciones con el que los usuarios pueden interactuar como lo harían en un escritorio físico.

#### Hosts de sesión

Dentro de cualquier pool de hosts es una o más máquinas virtuales idénticas. Estas sesiones de usuario que se conectan a este grupo de hosts están equilibradas por el servicio de equilibrador de carga AVD.

#### Grupos de aplicaciones

De forma predeterminada, el grupo de aplicaciones *Desktop Users* se crea en la implementación. Todos los usuarios de este grupo de aplicaciones se presentan con una experiencia de escritorio de Windows completa. Además, se pueden crear grupos de aplicaciones para prestar servicios de aplicaciones de streaming.

#### Espacio de trabajo de análisis de registros

Se crea un espacio de trabajo de análisis de registros para almacenar registros de los procesos de implementación y DSC y de otros servicios. Esto se puede eliminar después de la implementación, pero no se recomienda, ya que permite otras funciones. Los registros se conservan durante 30 días de forma predeterminada, sin gastos de retención.

#### Conjuntos de disponibilidad

Se configura un conjunto de disponibilidad como parte del proceso de puesta en marcha para permitir la separación de equipos virtuales compartidos (pools de hosts AVD compartidos, pools de recursos RDS) entre dominios de fallo. Esto se puede eliminar después de la puesta en marcha si se desea, pero sí se puede deshabilitar la opción de proporcionar una tolerancia a fallos adicional para los equipos virtuales compartidos.

### Almacén de recuperación de Azure

La automatización de VDS crea un almacén de servicios de recuperación durante la implementación. Esto se activa actualmente de forma predeterminada, ya que Azure Backup se aplica a CWMGR1 durante el proceso de implementación. Esto se puede desactivar y eliminar si lo desea, pero se volverá a crear si Azure Backup está habilitado en el entorno.

### Almacén de claves de Azure

Se crea un almacén de claves de Azure durante el proceso de implementación y se utiliza para almacenar certificados, claves de API y credenciales que utilizan las cuentas de automatización de Azure durante la implementación.

#### Apéndice A – estructura de unidades organizativas predeterminadas de Cloud Workspace

- Espacio de trabajo en cloud
  - Empresas de espacio de trabajo en la nube
  - Servidores de área de trabajo en la nube
    - Servidores dedicados del cliente
    - De almacenamiento
- Servidores CWMGR
- Servidores de puerta de enlace
- Servidores FTP
- Equipos virtuales de plantilla
  - Escritorio remoto
  - Estadificación
    - Cuentas de servicios de área de trabajo en la nube
  - Cuentas de servicio de cliente
  - Cuentas de servicio de infraestructura
    - Usuarios técnicos de Cloud Workspace
  - Grupos
  - Técnicos del Tech 3

## Requisitos previos de AVD y VDS v5.4

#### Requisitos y notas del AVD y VDS

Este documento describe los elementos necesarios para poner en marcha Azure Virtual Desktop (AVD) mediante Virtual Desktop Service (VDS) de NetApp. La “Lista de comprobación rápida” proporciona una breve lista de los componentes necesarios y los pasos previos a la implementación que se deben llevar a cabo para garantizar una implementación eficiente. El resto de la guía ofrece mayor detalle para cada elemento, dependiendo de las opciones de configuración que se tomen.

#### Lista de comprobación rápida

### Requisitos de Azure

- Azure AD inquilino
- Licencia de Microsoft 365 para admitir AVD
- Suscripción a Azure
- Cuota de Azure disponible para máquinas virtuales de Azure
- Cuenta de administrador de Azure con roles de administración global y propiedad de la suscripción
- Cuenta de administrador de dominio con la función "Enterprise Admin" para la configuración de AD Connect

### Información previa a la implementación

- Determinar el número total de usuarios
- Determine la región de Azure
- Determinar el tipo de Active Directory
- Determinar el tipo de almacenamiento
- Identifique los requisitos o la imagen del equipo virtual del host de sesión
- Evaluar la configuración de redes existente de Azure y en las instalaciones

#### Requisitos detallados de la implementación de VDS

### Requisitos de conexión de usuario final

**Los siguientes clientes de Escritorio remoto son compatibles con Azure Virtual Desktop:**

- Escritorio de Windows
- Web
- MacOS
- IOS
- Cliente IGEL Think (Linux)
- Android (Vista previa)

Azure Virtual Desktop no es compatible con el cliente RADC (RemoteApp y Desktop Connections) ni con el cliente MSTSC (Remote Desktop Connection).

En la actualidad, Azure Virtual Desktop no es compatible con el cliente de Escritorio remoto desde el almacén de Windows. La compatibilidad con este cliente se añadirá en una futura versión.

**Los clientes de Escritorio remoto deben tener acceso a las siguientes direcciones URL:**

| Dirección | Puerto TCP de salida | Específico | Cliente(s) |
|---|---|---|---|
| *.AVD.microsoft.com | 443 | Tráfico de servicios | Todo |
| *.servicebus.windows.net 443 solución de problemas de datos | Todo | go.microsoft.com | 443 |

| Dirección | Puerto TCP de salida | Específico | Cliente(s) |
|---|---|---|---|
| Microsoft FWLinks | Todo | aka.ms | 443 |
| Reducción de URL de Microsoft | Todo | docs.microsoft.com | 443 |
| Documentación | Todo | privacy.microsoft.com | 443 |
| Declaración de privacidad | Todo | query.prod.cms.rt.microsoft.com | 443 |

Abrir estas URL es esencial para una experiencia de cliente fiable. El bloqueo del acceso a estas URL no es compatible y afectará a la funcionalidad del servicio. Estas direcciones URL solo se corresponden con los sitios y recursos del cliente, y no incluyen direcciones URL para otros servicios como Azure Active Directory.

### Punto de inicio del asistente de configuración de VDS

El asistente de configuración de VDS puede gestionar gran parte de la configuración de requisitos previos necesaria para una implementación de AVD correcta. El asistente de configuración ("") crea o utiliza los siguientes componentes.

### Inquilino de Azure

**Necesario:** un inquilino de Azure y Azure Active Directory

La activación de AVD en Azure es una configuración para todo el cliente. VDS admite la ejecución de una instancia AVD por inquilino.

### Suscripción a Azure

**Requerido:** una suscripción a Azure (tenga en cuenta el ID de suscripción que desea utilizar)

Todos los recursos de Azure puestos en marcha deben configurarse en una suscripción dedicada. Esto facilita en gran medida el seguimiento de costes de AVD y simplifica el proceso de puesta en marcha. NOTA: Las pruebas gratuitas de Azure no son compatibles, ya que no tienen suficientes créditos para poner en marcha una puesta en marcha de AVD funcional.

### Cuota central de Azure

Cuota suficiente para las familias de equipos virtuales que utilizará; concretamente, 10 núcleos de la familia DS v3 para la puesta en marcha de la plataforma inicial (pueden usarse solo 2 núcleos, pero 10 cubren todas las posibilidades de la puesta en marcha inicial).

### Cuenta de administrador de Azure

**Necesario:** una cuenta de administrador global de Azure.

El asistente de configuración de VDS solicita que el administrador de Azure conceda permisos delegados al principal del servicio VDS e instale la aplicación VDS Azure Enterprise. El administrador debe tener asignados los siguientes roles de Azure:

- Administrador global en el inquilino

- Función de propietario en la suscripción

**Imagen de máquina virtual**

**Requerido:** una imagen de Azure que admite Windows 10 con varias sesiones.

Azure Marketplace proporciona las versiones más recientes de su imagen básica de Windows 10 y todas las suscripciones de Azure tienen acceso a ellas automáticamente. Si desea utilizar otra imagen o una imagen personalizada, quiere que el equipo de VDS le proporcione asesoramiento sobre la creación o modificación de otras imágenes o que tenga preguntas generales sobre las imágenes de Azure que nos lo comenten y podemos programar una conversación.

**Active Directory**

AVD requiere que la identidad del usuario forme parte de Azure AD y que las VM se unen a un dominio de Active Directory que se sincroniza con la misma instancia de Azure AD. Los equipos virtuales no se pueden conectar directamente a la instancia de Azure AD, por lo que es necesario configurar y sincronizar una controladora de dominio con Azure AD.

**Estas opciones admitidas incluyen:**

- Generación automatizada de una instancia de Active Directory dentro de la suscripción. La instancia de AD suele crearse por VDS en la máquina virtual de control de VDS (CWMGR1) para implementaciones de Azure Virtual Desktop que utilizan esta opción. AD Connect debe estar instalado y configurado para sincronizarse con Azure AD como parte del proceso de configuración.

  []

- Integración en un dominio de Active Directory existente al que se puede acceder desde la suscripción de Azure (normalmente mediante VPN de Azure o Express Route) y con su lista de usuarios sincronizada con Azure AD mediante AD Connect o un producto de terceros.

  []

**Capa de almacenamiento**

En AVD, la estrategia de almacenamiento se ha diseñado de modo que no haya datos persistentes de usuarios o empresas en los equipos virtuales de sesión de AVD. Los datos persistentes de perfiles de usuario, archivos y carpetas de usuario, y datos de aplicación/empresa se alojan en uno o más volúmenes de datos alojados en una capa de datos independiente.

FSLogix es una tecnología de agrupación en contenedores de perfiles que resuelve muchos problemas de perfil de usuario (como la dispersión de datos y los inicios de sesión lentos) mediante el montaje de un contenedor de perfiles de usuario (formato VHD o VHDX) en el host de sesión durante la inicialización de la sesión.

Gracias a esta arquitectura, es necesaria una función de almacenamiento de datos. Esta función debe ser capaz de gestionar la transferencia de datos necesaria cada mañana/tarde cuando una parte significativa del inicio de sesión/cierre de sesión de los usuarios al mismo tiempo. Incluso los entornos de tamaño moderado pueden tener requisitos significativos de transferencia de datos. El rendimiento de disco de la capa de almacenamiento de datos es una de las variables de rendimiento del usuario final principal y se debe tener cuidado en cuenta para ajustar el tamaño del rendimiento de este almacenamiento, no solo la cantidad de almacenamiento. Por lo general, se debe ajustar el tamaño de la capa de almacenamiento para que admita 5-15 IOPS por usuario.

**El asistente de configuración de VDS admite las siguientes configuraciones:**

- Instalación y configuración de Azure NetApp Files (ANF) (recomendado). El nivel de servicio estándar de *ANF admite hasta 150 usuarios, mientras que se recomienda el uso de entornos de 150-500 usuarios ANF Premium. Para más de 500 usuarios, se recomienda ANF Ultra.*

  []

- Instalación y configuración de un equipo virtual del servidor de archivos

  []

### Redes

**Requerido:** un inventario de todas las subredes de red existentes, incluyendo todas las subredes visibles para la suscripción a Azure a través de una ruta de Azure Express o VPN. La implementación debe evitar que se solapen las subredes.

El asistente de configuración de VDS permite definir el ámbito de red en caso de que sea necesario o necesario evitarlo, como parte de la integración planificada con las redes existentes.

Determine un rango de IP para el usuario durante la implementación. Según las prácticas recomendadas de Azure, solo se admiten direcciones IP en un rango privado.

**Las opciones admitidas incluyen las siguientes, pero por defecto, en un intervalo de /20:**

- 192.168.0.0 hasta 192.168.255.255
- 172.16.0.0 hasta 172.31.255.255
- 10.0.0.0 hasta 10.255.255.255

### CWMGR1

Algunas de las funciones exclusivas de VDS, como la programación de cargas de trabajo de ahorro de costes y la función de escalado en tiempo real, requieren una presencia administrativa dentro del inquilino y la suscripción. Por lo tanto, se implementa una VM administrativa denominada CWMGR1 como parte de la automatización del asistente de configuración de VDS. Además de las tareas de automatización VDS, esta máquina virtual también contiene la configuración VDS en una base de datos SQL Express, archivos de registro local y una utilidad de configuración avanzada denominada DCConfig.

**En función de las selecciones realizadas en el asistente de configuración de VDS, esta máquina virtual se puede usar para alojar funcionalidades adicionales como:**

- Una puerta de enlace RDS (solo utilizada en las puestas en marcha de RDS)
- Una puerta de enlace HTML 5 (solo se utiliza en las implementaciones RDS)
- Un servidor de licencia RDS (utilizado solo en las implementaciones RDS)
- Un controlador de dominio (si se ha elegido)

### Árbol de decisiones en el Asistente para implementación

Como parte de la implementación inicial, se responden una serie de preguntas para personalizar la configuración del nuevo entorno. A continuación se presenta un resumen de las principales decisiones que se deben tomar.

### Región de Azure

Decida qué región o regiones de Azure alojarán sus máquinas virtuales AVD. Tenga en cuenta que Azure NetApp Files y ciertas familias de equipos virtuales (VM habilitadas para GPU, por ejemplo) tienen una lista definida de soporte de región de Azure, mientras que AVD está disponible en la mayoría de las regiones.

- Este enlace se puede utilizar para identificar "Disponibilidad de productos Azure por región"

### Tipo de Active Directory

Decida qué tipo de Active Directory desea utilizar:

- Active Directory en las instalaciones existente
- Consulte la "Componentes y permisos de AVD VDS" Documentar para obtener una explicación de los permisos y los componentes necesarios tanto en Azure como en el entorno local de Active Directory
- Nueva instancia de Active Directory basada en suscripción de Azure
- Servicios de dominio de Azure Active Directory

### Almacenamiento de datos

Decida dónde se colocarán los datos de perfiles de usuario, archivos individuales y recursos compartidos de la empresa. Las opciones incluyen:

- Azure NetApp Files
- Azure Files
- Servidor de archivos tradicional (máquina virtual de Azure con disco gestionado)

#### Requisitos de implementación de VDS de NetApp para los componentes existentes

### Implementación de VDS de NetApp con controladores de dominio de Active Directory existentes

Este tipo de configuración amplía un dominio de Active Directory existente para admitir la instancia de AVD. En este caso, VDS implementa un conjunto limitado de componentes en el dominio para admitir tareas de aprovisionamiento y administración automatizadas para los componentes de AVD.

**Esta configuración requiere:**

- Una controladora de dominio de Active Directory existente a la que pueden acceder las máquinas virtuales en Azure vnet, normalmente a través de Azure VPN o Express Route O de una controladora de dominio creada en Azure.
- Adición de componentes y permisos de VDS necesarios para la gestión de VDS de los pools de hosts AVD y los volúmenes de datos a medida que se unen al dominio. La guía de componentes y permisos de AVD VDS define los componentes y permisos necesarios y el proceso de implementación requiere un usuario de dominio con privilegios de dominio para ejecutar la secuencia de comandos que creará los elementos necesarios.
- Tenga en cuenta que la implementación de VDS crea una vnet de forma predeterminada para las máquinas virtuales creadas por VDS. El vnet puede tener una relación entre iguales con los VNets de la red de Azure existente o el equipo virtual CWMGR1 se puede mover a una vnet existente con las subredes requeridas predefinidas.

### Credenciales y herramienta de preparación de dominios

Los administradores deben proporcionar una credencial de administrador de dominio en algún momento del proceso de implementación. Se puede crear, utilizar y eliminar posteriormente una credencial temporal del Administrador de dominio (una vez completado el proceso de implementación). Como alternativa, los clientes que necesiten ayuda para crear los requisitos previos pueden aprovechar la herramienta de preparación de dominios.

### Implementación de VDS de NetApp con un sistema de archivos existente

VDS crea recursos compartidos de Windows que permiten acceder a los perfiles de usuario, carpetas personales y datos corporativos desde los equipos virtuales de sesión de AVD. VDS implementará las opciones File Server o Azure NetApp File de forma predeterminada, pero si tiene un componente de almacenamiento de archivos existente VDS puede dirigir los recursos compartidos a ese componente una vez completada la implementación de VDS.

**Requisitos para utilizar y el componente de almacenamiento existente:**

- El componente debe ser compatible con SMB v3
- El componente debe estar Unido al mismo dominio de Active Directory que los hosts de sesión de AVD
- El componente debe ser capaz de exponer una ruta UNC que se utilizará en la configuración de VDS; se puede utilizar una ruta para los tres recursos compartidos o se pueden especificar rutas independientes para cada uno de ellos. Tenga en cuenta que VDS establecerá permisos de nivel de usuario en estos recursos compartidos, por lo que consulte el documento VDS AVD Components and Permissions para asegurarse de que se han concedido los permisos correspondientes a VDS Automation Services.

### Implementación de VDS de NetApp con servicios de dominio de Azure AD existentes

Esta configuración requiere un proceso para identificar los atributos de la instancia existente de servicios de dominio de Azure Active Directory. Póngase en contacto con su gestor de cuentas para solicitar una implementación de este tipo. Implementación de VDS de NetApp con una puesta en marcha de AVD existente este tipo de configuración asume que ya existen los componentes de Azure vnet, Active Directory y AVD necesarios. La implementación de VDS se realiza de la misma manera que la configuración “NetApp VDS Deployment with existing AD”, pero añade los siguientes requisitos:

- Es necesario otorgar el rol DE PROPIETARIO AL inquilino AVD a las aplicaciones de empresa VDS en Azure
- Las máquinas virtuales del grupo de hosts AVD y del grupo de hosts AVD deben importarse a VDS mediante la función de importación de VDS en el explorador web VDS. Este proceso recopila el pool de host de AVD y los metadatos de VM de sesión y los almacena en VDS de TI para que estos elementos se puedan gestionar mediante VDS
- Los datos de usuario de AVD deben importarse a la sección Usuario de VDS mediante la herramienta CRA. Este proceso inserta metadatos acerca de cada usuario en el plano de control VDS para que VDS pueda gestionar su pertenencia al grupo de aplicaciones AVD e información de sesión

#### APÉNDICE A: Direcciones IP y URL del plano de control VDS

Los componentes VDS de la suscripción a Azure se comunican con los componentes del plano de control global de VDS, como la aplicación web VDS y los extremos API VDS. Para el acceso, las siguientes direcciones URI base deben ser safelisted para el acceso bidireccional en el puerto 443:

"" "" "" "" ""

Si su dispositivo de control de acceso sólo puede hacer una lista segura por dirección IP, se debe garantizar la

siguiente lista de direcciones IP. Tenga en cuenta que VDS utiliza el servicio Azure Traffic Manager, de manera que esta lista puede cambiar con el tiempo:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239 52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

#### APÉNDICE B: Requisitos de Microsoft AVD

Esta sección de requisitos de AVD de Microsoft es un resumen de los requisitos de AVD de Microsoft. Los requisitos de AVD completos y actuales se pueden encontrar aquí:

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

### Licencias de host de sesión de Azure Virtual Desktop

Azure Virtual Desktop admite los siguientes sistemas operativos, así que asegúrese de tener las licencias adecuadas para los usuarios en función del escritorio y las aplicaciones que desee implementar:

| SO | Licencia requerida |
|---|---|
| Windows 10 Enterprise Multisession o Windows 10 Enterprise | MICROSOFT 365 E3, E5, A3, A5, F3 Business Premium Windows E3, E5, A3, A5 |
| Windows 7 Enterprise | MICROSOFT 365 E3, E5, A3, A5, F3 Business Premium Windows E3, E5, A3, A5 |
| Windows Server 2012 R2, 2016 y 2019 | Licencia de acceso de cliente (CAL) de RDS con garantía de software |

### Acceso a URL para máquinas AVD

Las máquinas virtuales Azure que cree para Azure Virtual Desktop deben tener acceso a las siguientes direcciones URL:

| Dirección | Puerto TCP de salida | Específico | Etiqueta de servicio |
|---|---|---|---|
| *.AVD.microsoft.com | 443 | Tráfico de servicios | WindowsVirtualDesktop |
| mrsglobalsteus2prod.blob.core.windows.net | 443 | Actualizaciones de la pila Agent y SXS | Cloud AzureCloud |
| *.core.windows.net | 443 | Tráfico de agentes | Cloud AzureCloud |
| *.servicebus.windows.net | 443 | Tráfico de agentes | Cloud AzureCloud |
| prod.warmpath.msftcloudes.com | 443 | Tráfico de agentes | Cloud AzureCloud |
| catalogartifact.azureedge.net | 443 | Azure Marketplace | Cloud AzureCloud |
| kms.core.windows.net | 1688 | Activación de Windows | Internet |
| AVDportalstorageblob.blob.core.windows.net | 443 | Soporte del portal de Azure | Cloud AzureCloud |

La tabla siguiente enumera las URL opcionales a las que pueden acceder las máquinas virtuales de Azure:

| Dirección | Puerto TCP de salida | Específico | Etiqueta de servicio |
|---|---|---|---|
| *.microsoftonline.com | 443 | Autenticación a MS Online Services | Ninguno |
| *.events.data.microsoft.com | 443 | Servicio de telemetría | Ninguno |
| www.msftconnecttest.com | 443 | Detecta si el sistema operativo está conectado a Internet | Ninguno |
| *.prod.do.dsp.mp.microsoft.com | 443 | Windows Update | Ninguno |
| login.windows.net | 443 | Inicie sesión en MS Online Services, Office 365 | Ninguno |
| *.sfx.ms | 443 | Actualizaciones del software del cliente de OneDrive | Ninguno |
| *.digicert.com | 443 | Comprobación de revocación de certificados | Ninguno |

**Factores de rendimiento óptimos**

Para obtener un rendimiento óptimo, asegúrese de que la red cumple los siguientes requisitos:

- La latencia de ida y vuelta (RTT) desde la red del cliente hasta la región de Azure, donde se han puesto en marcha pools de hosts, debe ser inferior a 150 ms.
- El tráfico de red puede fluir fuera de las fronteras del país o de la región cuando las máquinas virtuales que alojan escritorios y aplicaciones se conectan al servicio de gestión.
- Para optimizar el rendimiento de la red, recomendamos que las máquinas virtuales del host de sesión se encuentren en la misma región de Azure que el servicio de gestión.

**Imágenes de SO de máquina virtual admitidas**

Azure Virtual Desktop es compatible con las siguientes imágenes del sistema operativo x64:

- Windows 10 Enterprise Multisession, versión 1809 o posterior
- Windows 10 Enterprise, versión 1809 o posterior
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop no admite imágenes de sistemas operativos x86 (32 bits), Windows 10 Enterprise N o Windows 10 Enterprise KN. Windows 7 tampoco admite ninguna solución de perfil basada en VHD o VHDX alojada en el almacenamiento Azure gestionado debido a una limitación del tamaño del sector.

Las opciones de automatización y puesta en marcha disponibles dependen del sistema operativo y la versión que elija, como se muestra en la siguiente tabla:

| Sistema operativo | Galería de imágenes de Azure | Puesta en marcha manual de máquinas virtuales | Integración de plantillas ARM | Aprovisione los pools de hosts en Azure Marketplace |
|---|---|---|---|---|
| Múltiples sesiones de Windows 10, versión 1903 | Sí | Sí | Sí | Sí |
| Múltiples sesiones de Windows 10, versión 1809 | Sí | Sí | No | No |
| Windows 10 Enterprise, versión 1903 | Sí | Sí | Sí | Sí |
| Windows 10 Enterprise, versión 1809 | Sí | Sí | No | No |
| Windows 7 Enterprise | Sí | Sí | No | No |
| Windows Server 2019 | Sí | Sí | No | No |
| Windows Server 2016 | Sí | Sí | Sí | Sí |
| Windows Server 2012 R2 | Sí | Sí | No | No |

## Requisitos previos de AVD y VDS v6.0

#### Requisitos y notas del AVD y VDS

Este documento describe los elementos necesarios para poner en marcha Azure Virtual Desktop (AVD) mediante Virtual Desktop Service (VDS) de NetApp. La “Lista de comprobación rápida” proporciona una breve lista de los componentes necesarios y los pasos previos a la implementación que se deben llevar a cabo para garantizar una implementación eficiente. El resto de la guía ofrece mayor detalle para cada elemento, dependiendo de las opciones de configuración que se tomen.

#### Lista de comprobación rápida

### Requisitos de Azure

- Azure AD inquilino
- Licencia de Microsoft 365 para admitir AVD
- Suscripción a Azure
- Cuota de Azure disponible para máquinas virtuales de Azure
- Cuenta de administrador de Azure con roles de administración global y propiedad de la suscripción
- Cuenta de administrador de dominio con la función "Enterprise Admin" para la configuración de AD Connect

### Información previa a la implementación

- Determinar el número total de usuarios
- Determine la región de Azure
- Determinar el tipo de Active Directory

- Determinar el tipo de almacenamiento
- Identifique los requisitos o la imagen del equipo virtual del host de sesión
- Evaluar la configuración de redes existente de Azure y en las instalaciones

#### Requisitos detallados de la implementación de VDS

### Requisitos de conexión de usuario final

**Los siguientes clientes de Escritorio remoto son compatibles con Azure Virtual Desktop:**

- Escritorio de Windows
- Web
- MacOS
- IOS
- Cliente IGEL Think (Linux)
- Android (Vista previa)

Azure Virtual Desktop no es compatible con el cliente RADC (RemoteApp y Desktop Connections) ni con el cliente MSTSC (Remote Desktop Connection).

En la actualidad, Azure Virtual Desktop no es compatible con el cliente de Escritorio remoto desde el almacén de Windows. La compatibilidad con este cliente se añadirá en una futura versión.

**Los clientes de Escritorio remoto deben tener acceso a las siguientes direcciones URL:**

| Dirección | Puerto TCP de salida | Específico | Cliente(s) |
|---|---|---|---|
| *.wvd.microsoft.com | 443 | Tráfico de servicios | Todo |
| *.servicebus.windows.net | 443 | Datos de resolución de problemas | Todo |
| go.microsoft.com | 443 | Microsoft FWLinks | Todo |
| aka.ms | 443 | Reducción de URL de Microsoft | Todo |
| docs.microsoft.com | 443 | Documentación | Todo |
| privacy.microsoft.com | 443 | Declaración de privacidad | Todo |
| query.prod.cms.rt.microsoft.com | 443 | Actualizaciones del cliente | Escritorio de Windows |

Abrir estas URL es esencial para una experiencia de cliente fiable. El bloqueo del acceso a estas URL no es compatible y afectará a la funcionalidad del servicio. Estas direcciones URL solo se corresponden con los sitios y recursos del cliente, y no incluyen direcciones URL para otros servicios como Azure Active Directory.

### Punto de inicio del asistente de configuración de VDS

El asistente de configuración de VDS puede gestionar gran parte de la configuración de requisitos previos necesaria para una implementación de AVD correcta. El asistente de configuración ("") crea o utiliza los siguientes componentes.

### Inquilino de Azure

**Necesario:** un inquilino de Azure y Azure Active Directory

La activación de AVD en Azure es una configuración para todo el cliente. VDS admite la ejecución de una instancia AVD por inquilino.

### Suscripción a Azure

**Requerido:** una suscripción a Azure (tenga en cuenta el ID de suscripción que desea utilizar)

Todos los recursos de Azure puestos en marcha deben configurarse en una suscripción dedicada. Esto facilita en gran medida el seguimiento de costes de AVD y simplifica el proceso de puesta en marcha. NOTA: Las pruebas gratuitas de Azure no son compatibles, ya que no tienen suficientes créditos para poner en marcha una puesta en marcha de AVD funcional.

### Cuota central de Azure

Cuota suficiente para las familias de equipos virtuales que utilizará; concretamente, 10 núcleos de la familia DS v3 para la puesta en marcha de la plataforma inicial (pueden usarse solo 2 núcleos, pero 10 cubren todas las posibilidades de la puesta en marcha inicial).

### Cuenta de administrador de Azure

**Necesario:** una cuenta de administrador global de Azure.

El asistente de configuración de VDS solicita que el administrador de Azure conceda permisos delegados al principal del servicio VDS e instale la aplicación VDS Azure Enterprise. El administrador debe tener asignados los siguientes roles de Azure:

- Administrador global en el inquilino
- Función de propietario en la suscripción

### Imagen de máquina virtual

**Requerido:** una imagen de Azure que admite Windows 10 con varias sesiones.

Azure Marketplace proporciona las versiones más recientes de su imagen básica de Windows 10 y todas las suscripciones de Azure tienen acceso a ellas automáticamente. Si desea utilizar otra imagen o una imagen personalizada, quiere que el equipo de VDS le proporcione asesoramiento sobre la creación o modificación de otras imágenes o que tenga preguntas generales sobre las imágenes de Azure que nos lo comenten y podemos programar una conversación.

### Active Directory

AVD requiere que la identidad del usuario forme parte de Azure AD y que las VM se unen a un dominio de Active Directory que se sincroniza con la misma instancia de Azure AD. Los equipos virtuales no se pueden conectar directamente a la instancia de Azure AD, por lo que es necesario configurar y sincronizar una

controladora de dominio con Azure AD.

**Estas opciones admitidas incluyen:**

- Generación automatizada de una instancia de Active Directory dentro de la suscripción. La instancia de AD suele crearse por VDS en la máquina virtual de control de VDS (CWMGR1) para implementaciones de Azure Virtual Desktop que utilizan esta opción. AD Connect debe estar instalado y configurado para sincronizarse con Azure AD como parte del proceso de configuración.

  []

- Integración en un dominio de Active Directory existente al que se puede acceder desde la suscripción de Azure (normalmente mediante VPN de Azure o Express Route) y con su lista de usuarios sincronizada con Azure AD mediante AD Connect o un producto de terceros.

  []

### Capa de almacenamiento

En AVD, la estrategia de almacenamiento se ha diseñado de modo que no haya datos persistentes de usuarios o empresas en los equipos virtuales de sesión de AVD. Los datos persistentes de perfiles de usuario, archivos y carpetas de usuario, y datos de aplicación/empresa se alojan en uno o más volúmenes de datos alojados en una capa de datos independiente.

FSLogix es una tecnología de agrupación en contenedores de perfiles que resuelve muchos problemas de perfil de usuario (como la dispersión de datos y los inicios de sesión lentos) mediante el montaje de un contenedor de perfiles de usuario (formato VHD o VHDX) en el host de sesión durante la inicialización de la sesión.

Gracias a esta arquitectura, es necesaria una función de almacenamiento de datos. Esta función debe ser capaz de gestionar la transferencia de datos necesaria cada mañana/tarde cuando una parte significativa del inicio de sesión/cierre de sesión de los usuarios al mismo tiempo. Incluso los entornos de tamaño moderado pueden tener requisitos significativos de transferencia de datos. El rendimiento de disco de la capa de almacenamiento de datos es una de las variables de rendimiento del usuario final principal y se debe tener cuidado en cuenta para ajustar el tamaño del rendimiento de este almacenamiento, no solo la cantidad de almacenamiento. Por lo general, se debe ajustar el tamaño de la capa de almacenamiento para que admita 5-15 IOPS por usuario.

**El asistente de configuración de VDS admite las siguientes configuraciones:**

- Instalación y configuración de Azure NetApp Files (ANF) (recomendado). El nivel de servicio estándar de *ANF admite hasta 150 usuarios, mientras que se recomienda el uso de entornos de 150-500 usuarios ANF Premium. Para más de 500 usuarios, se recomienda ANF Ultra.*

  []

- Instalación y configuración de un equipo virtual del servidor de archivos

  []

### Redes

**Requerido:** un inventario de todas las subredes de red existentes, incluyendo todas las subredes visibles para la suscripción a Azure a través de una ruta de Azure Express o VPN. La implementación debe evitar que se solapen las subredes.

El asistente de configuración de VDS permite definir el ámbito de red en caso de que sea necesario o necesario evitarlo, como parte de la integración planificada con las redes existentes.

Determine un rango de IP para el usuario durante la implementación. Según las prácticas recomendadas de Azure, solo se admiten direcciones IP en un rango privado.

**Las opciones admitidas incluyen las siguientes, pero por defecto, en un intervalo de /20:**

- 192.168.0.0 hasta 192.168.255.255
- 172.16.0.0 hasta 172.31.255.255
- 10.0.0.0 hasta 10.255.255.255

### CWMGR1

Algunas de las funciones exclusivas de VDS, como la programación de cargas de trabajo de ahorro de costes y la función de escalado en tiempo real, requieren una presencia administrativa dentro del inquilino y la suscripción. Por lo tanto, se implementa una VM administrativa denominada CWMGR1 como parte de la automatización del asistente de configuración de VDS. Además de las tareas de automatización VDS, esta máquina virtual también contiene la configuración VDS en una base de datos SQL Express, archivos de registro local y una utilidad de configuración avanzada denominada DCConfig.

**En función de las selecciones realizadas en el asistente de configuración de VDS, esta máquina virtual se puede usar para alojar funcionalidades adicionales como:**

- Una puerta de enlace RDS (solo utilizada en las puestas en marcha de RDS)
- Una puerta de enlace HTML 5 (solo se utiliza en las implementaciones RDS)
- Un servidor de licencia RDS (utilizado solo en las implementaciones RDS)
- Un controlador de dominio (si se ha elegido)

### Árbol de decisiones en el Asistente para implementación

Como parte de la implementación inicial, se responden una serie de preguntas para personalizar la configuración del nuevo entorno. A continuación se presenta un resumen de las principales decisiones que se deben tomar.

### Región de Azure

Decida qué región o regiones de Azure alojarán sus máquinas virtuales AVD. Tenga en cuenta que Azure NetApp Files y ciertas familias de equipos virtuales (VM habilitadas para GPU, por ejemplo) tienen una lista definida de soporte de región de Azure, mientras que AVD está disponible en la mayoría de las regiones.

- Este enlace se puede utilizar para identificar "Disponibilidad de productos Azure por región"

### Tipo de Active Directory

Decida qué tipo de Active Directory desea utilizar:

- Active Directory en las instalaciones existente
- Consulte la "Componentes y permisos de AVD VDS" Documentar para obtener una explicación de los permisos y los componentes necesarios tanto en Azure como en el entorno local de Active Directory
- Nueva instancia de Active Directory basada en suscripción de Azure
- Servicios de dominio de Azure Active Directory

### Almacenamiento de datos

Decida dónde se colocarán los datos de perfiles de usuario, archivos individuales y recursos compartidos de la empresa. Las opciones incluyen:

- Azure NetApp Files
- Azure Files
- Servidor de archivos tradicional (máquina virtual de Azure con disco gestionado)

#### Requisitos de implementación de VDS de NetApp para los componentes existentes

### Implementación de VDS de NetApp con controladores de dominio de Active Directory existentes

Este tipo de configuración amplía un dominio de Active Directory existente para admitir la instancia de AVD. En este caso, VDS implementa un conjunto limitado de componentes en el dominio para admitir tareas de aprovisionamiento y administración automatizadas para los componentes de AVD.

**Esta configuración requiere:**

- Una controladora de dominio de Active Directory existente a la que pueden acceder las máquinas virtuales en Azure vnet, normalmente a través de Azure VPN o Express Route O de una controladora de dominio creada en Azure.
- Adición de componentes y permisos de VDS necesarios para la gestión de VDS de los pools de hosts AVD y los volúmenes de datos a medida que se unen al dominio. La guía de componentes y permisos de AVD VDS define los componentes y permisos necesarios y el proceso de implementación requiere un usuario de dominio con privilegios de dominio para ejecutar la secuencia de comandos que creará los elementos necesarios.
- Tenga en cuenta que la implementación de VDS crea una vnet de forma predeterminada para las máquinas virtuales creadas por VDS. El vnet puede tener una relación entre iguales con los VNets de la red de Azure existente o el equipo virtual CWMGR1 se puede mover a una vnet existente con las subredes requeridas predefinidas.

### Credenciales y herramienta de preparación de dominios

Los administradores deben proporcionar una credencial de administrador de dominio en algún momento del proceso de implementación. Se puede crear, utilizar y eliminar posteriormente una credencial temporal del Administrador de dominio (una vez completado el proceso de implementación). Como alternativa, los clientes que necesiten ayuda para crear los requisitos previos pueden aprovechar la herramienta de preparación de dominios.

### Implementación de VDS de NetApp con un sistema de archivos existente

VDS crea recursos compartidos de Windows que permiten acceder a los perfiles de usuario, carpetas personales y datos corporativos desde los equipos virtuales de sesión de AVD. VDS implementará las opciones File Server o Azure NetApp File de forma predeterminada, pero si tiene un componente de almacenamiento de archivos existente VDS puede dirigir los recursos compartidos a ese componente una vez completada la implementación de VDS.

**Requisitos para utilizar y el componente de almacenamiento existente:**

- El componente debe ser compatible con SMB v3
- El componente debe estar Unido al mismo dominio de Active Directory que los hosts de sesión de AVD
- El componente debe ser capaz de exponer una ruta UNC que se utilizará en la configuración de VDS; se puede utilizar una ruta para los tres recursos compartidos o se pueden especificar rutas independientes

para cada uno de ellos. Tenga en cuenta que VDS establecerá permisos de nivel de usuario en estos recursos compartidos, por lo que consulte el documento VDS AVD Components and Permissions para asegurarse de que se han concedido los permisos correspondientes a VDS Automation Services.

### Implementación de VDS de NetApp con servicios de dominio de Azure AD existentes

Esta configuración requiere un proceso para identificar los atributos de la instancia existente de servicios de dominio de Azure Active Directory. Póngase en contacto con su gestor de cuentas para solicitar una implementación de este tipo. Implementación de VDS de NetApp con una puesta en marcha de AVD existente este tipo de configuración asume que ya existen los componentes de Azure vnet, Active Directory y AVD necesarios. La implementación de VDS se realiza de la misma manera que la configuración “NetApp VDS Deployment with existing AD”, pero añade los siguientes requisitos:

- Es necesario otorgar el rol DE PROPIETARIO AL inquilino AVD a las aplicaciones de empresa VDS en Azure
- Las máquinas virtuales del grupo de hosts AVD y del grupo de hosts AVD deben importarse a VDS mediante la función de importación de VDS en el explorador web VDS. Este proceso recopila el pool de host de AVD y los metadatos de VM de sesión y los almacena en VDS de TI para que estos elementos se puedan gestionar mediante VDS
- Los datos de usuario de AVD deben importarse a la sección Usuario de VDS mediante la herramienta CRA. Este proceso inserta metadatos acerca de cada usuario en el plano de control VDS para que VDS pueda gestionar su pertenencia al grupo de aplicaciones AVD e información de sesión

#### APÉNDICE A: Direcciones IP y URL del plano de control VDS

Los componentes VDS de la suscripción a Azure se comunican con los componentes del plano de control global de VDS, como la aplicación web VDS y los extremos API VDS. Para el acceso, las siguientes direcciones URI base deben ser safelisted para el acceso bidireccional en el puerto 443:

"" "" "" "" ""

Si su dispositivo de control de acceso sólo puede hacer una lista segura por dirección IP, se debe garantizar la siguiente lista de direcciones IP. Tenga en cuenta que VDS utiliza el servicio Azure Traffic Manager, de manera que esta lista puede cambiar con el tiempo:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239 52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

#### APÉNDICE B: Requisitos de Microsoft AVD

Esta sección de requisitos de AVD de Microsoft es un resumen de los requisitos de AVD de Microsoft. Los requisitos de AVD completos y actuales se pueden encontrar aquí:

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

### Licencias de host de sesión de Azure Virtual Desktop

Azure Virtual Desktop admite los siguientes sistemas operativos, así que asegúrese de tener las licencias adecuadas para los usuarios en función del escritorio y las aplicaciones que desee implementar:

| SO | Licencia requerida |
|---|---|
| Windows 10 Enterprise Multisession o Windows 10 Enterprise | MICROSOFT 365 E3, E5, A3, A5, F3 Business Premium Windows E3, E5, A3, A5 |
| Windows 7 Enterprise | MICROSOFT 365 E3, E5, A3, A5, F3 Business Premium Windows E3, E5, A3, A5 |
| Windows Server 2012 R2, 2016 y 2019 | Licencia de acceso de cliente (CAL) de RDS con garantía de software |

**Acceso a URL para máquinas AVD**

Las máquinas virtuales Azure que cree para Azure Virtual Desktop deben tener acceso a las siguientes direcciones URL:

| Dirección | Puerto TCP de salida | Específico | Etiqueta de servicio |
|---|---|---|---|
| *.AVD.microsoft.com | 443 | Tráfico de servicios | WindowsVirtualDesktop |
| mrsglobalsteus2prod.blob.core.windows.net | 443 | Actualizaciones de la pila Agent y SXS | Cloud AzureCloud |
| *.core.windows.net | 443 | Tráfico de agentes | Cloud AzureCloud |
| *.servicebus.windows.net | 443 | Tráfico de agentes | Cloud AzureCloud |
| prod.warmpath.msftcloudes.com | 443 | Tráfico de agentes | Cloud AzureCloud |
| catalogartifact.azureedge.net | 443 | Azure Marketplace | Cloud AzureCloud |
| kms.core.windows.net | 1688 | Activación de Windows | Internet |
| AVDportalstorageblob.blob.core.windows.net | 443 | Soporte del portal de Azure | Cloud AzureCloud |

La tabla siguiente enumera las URL opcionales a las que pueden acceder las máquinas virtuales de Azure:

| Dirección | Puerto TCP de salida | Específico | Etiqueta de servicio |
|---|---|---|---|
| *.microsoftonline.com | 443 | Autenticación a MS Online Services | Ninguno |
| *.events.data.microsoft.com | 443 | Servicio de telemetría | Ninguno |
| www.msftconnecttest.com | 443 | Detecta si el sistema operativo está conectado a Internet | Ninguno |
| *.prod.do.dsp.mp.microsoft.com | 443 | Windows Update | Ninguno |
| login.windows.net | 443 | Inicie sesión en MS Online Services, Office 365 | Ninguno |

| Dirección | Puerto TCP de salida | Específico | Etiqueta de servicio |
|---|---|---|---|
| *.sfx.ms | 443 | Actualizaciones del software del cliente de OneDrive | Ninguno |
| *.digicert.com | 443 | Comprobación de revocación de certificados | Ninguno |

### Factores de rendimiento óptimos

Para obtener un rendimiento óptimo, asegúrese de que la red cumple los siguientes requisitos:

- La latencia de ida y vuelta (RTT) desde la red del cliente hasta la región de Azure, donde se han puesto en marcha pools de hosts, debe ser inferior a 150 ms.
- El tráfico de red puede fluir fuera de las fronteras del país o de la región cuando las máquinas virtuales que alojan escritorios y aplicaciones se conectan al servicio de gestión.
- Para optimizar el rendimiento de la red, recomendamos que las máquinas virtuales del host de sesión se encuentren en la misma región de Azure que el servicio de gestión.

### Imágenes de SO de máquina virtual admitidas

Azure Virtual Desktop es compatible con las siguientes imágenes del sistema operativo x64:

- Windows 10 Enterprise Multisession, versión 1809 o posterior
- Windows 10 Enterprise, versión 1809 o posterior
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop no admite imágenes de sistemas operativos x86 (32 bits), Windows 10 Enterprise N o Windows 10 Enterprise KN. Windows 7 tampoco admite ninguna solución de perfil basada en VHD o VHDX alojada en el almacenamiento Azure gestionado debido a una limitación del tamaño del sector.

Las opciones de automatización y puesta en marcha disponibles dependen del sistema operativo y la versión que elija, como se muestra en la siguiente tabla:

| Sistema operativo | Galería de imágenes de Azure | Puesta en marcha manual de máquinas virtuales | Integración de plantillas ARM | Aprovisione los pools de hosts en Azure Marketplace |
|---|---|---|---|---|
| Múltiples sesiones de Windows 10, versión 1903 | Sí | Sí | Sí | Sí |
| Múltiples sesiones de Windows 10, versión 1809 | Sí | Sí | No | No |
| Windows 10 Enterprise, versión 1903 | Sí | Sí | Sí | Sí |
| Windows 10 Enterprise, versión 1809 | Sí | Sí | No | No |

| Sistema operativo | Galería de imágenes de Azure | Puesta en marcha manual de máquinas virtuales | Integración de plantillas ARM | Aprovisione los pools de hosts en Azure Marketplace |
|---|---|---|---|---|
| Windows 7 Enterprise | Sí | Sí | No | No |
| Windows Server 2019 | Sí | Sí | No | No |
| Windows Server 2016 | Sí | Sí | Sí | Sí |
| Windows Server 2012 R2 | Sí | Sí | No | No |

# Google

## Guía de implementación de RDS para Google Cloud (GCP)

### Descripción general

Esta guía proporcionará las instrucciones paso a paso para crear una implementación del servicio de puesto de trabajo remoto (RDS) con Virtual Desktop Service (VDS) de NetApp en Google Cloud.

Esta guía de prueba de concepto (POC) está diseñada para ayudarle a implementar y configurar rápidamente RDS en su propio proyecto de prueba de GCP.

Las implementaciones de producción, especialmente en entornos AD existentes, son muy comunes; sin embargo, el proceso no se tiene en cuenta en esta guía de POC. Las pruebas de concepto complejas y las implementaciones de producción deben iniciarse con los equipos de ventas/servicios de VDS de NetApp, y no realizarse de forma autoservicio.

Este documento POC le llevará a través de toda la implementación de RDS y le ofrecerá un breve recorrido por las principales áreas de configuración posterior a la implementación disponibles en la plataforma VDS. Una vez completado, dispondrá de un entorno RDS completamente implementado y funcional, completo con hosts de sesión, aplicaciones y usuarios. Opcionalmente, tendrá la opción de configurar la entrega automatizada de aplicaciones, grupos de seguridad, permisos de recursos compartidos de archivos, Cloud Backup, optimización inteligente de costes. VDS implementa un conjunto de configuraciones de mejores prácticas mediante GPO. También se incluyen instrucciones sobre cómo deshabilitar opcionalmente esos controles, en caso de que su POC no tenga controles de seguridad, similares a un entorno de dispositivo local no administrado.

### Arquitectura de puesta en marcha

[anchura = 75%]

### Información básica de RDS

VDS implementa un entorno RDS completamente funcional, con todos los servicios de soporte necesarios desde cero. Esta funcionalidad puede incluir:

- Servidores de puerta de enlace RDS
- Servidores de acceso de clientes web
- Servidores del controlador de dominio

- Servicio de licencias RDS
- Servicio de licencias de ThinPrint
- Servicio de servidor FileZilla FTPS

**Alcance de la guía**

Esta guía le guiará por el proceso de implementación de RDS mediante la tecnología VDS de NetApp desde el punto de vista de un administrador de GCP y VDS. Puede llevar el proyecto GCP sin preconfiguración y esta guía le ayudará a configurar los servicios RDS de extremo a extremo

**Crear una cuenta de servicio**

1. En GCP, desplácese hasta (o busque) *IAM & Admin > Cuentas de servicio*

   []

2. HAGA CLIC EN + *CREAR CUENTA DE SERVICIO*

   []

3. Introduzca un nombre de cuenta de servicio único y haga clic en *CREATE*. Anote la dirección de correo electrónico de la cuenta de servicio que se utilizará en un paso posterior.

   []

4. Seleccione la función *Owner* de la cuenta de servicio y haga clic en *CONTINUE*

   []

5. No es necesario realizar cambios en la página siguiente (*conceder a los usuarios acceso a esta cuenta de servicio (opcional)*), haga clic en *DONE*

   []

6. En la página *Service Accounts*, haga clic en el menú de acciones y seleccione *Create key*

   []

7. Seleccione *P12* y haga clic en *CREATE*

   []

8. Descargue el archivo .P12 y guárdelo en el ordenador. Se ha dejado sin cambios la *Private Key Password*.

   []

   []

**Habilite Google Compute API**

1. En GCP, desplácese hasta (o busque) *API y servicios > Biblioteca*

   []

2. En la Biblioteca de API de GCP, desplácese hasta (o busque) *Compute Engine API*, haga clic en *ENABLE*

   []

### Cree una nueva implementación de VDS

1. En VDS, desplácese a *despliegues* y haga clic en + *New Deployment*

   []

2. Escriba un nombre para la implementación

   []

3. Seleccione *Google Cloud Platform*

   []

#### Plataforma de infraestructura

1. Introduzca la dirección de correo electrónico *Project ID* y OAuth. Cargue el archivo .P12 de anteriormente en esta guía y seleccione la zona adecuada para esta implementación. Haga clic en *Test* para confirmar que las entradas son correctas y que se han establecido los permisos adecuados.

   > El correo electrónico de OAuth es la dirección de la cuenta de servicio creada anteriormente en esta guía.

   []

2. Una vez confirmado, haga clic en *Continue*

   []

#### Cuentas

### Cuentas de equipo virtual locales

1. Proporcione una contraseña para la cuenta de administrador local. Documente esta contraseña para su uso posterior.
2. Introduzca una contraseña para la cuenta de SQL SA. Documente esta contraseña para su uso posterior.

> La complejidad de la contraseña requiere un mínimo de 8 caracteres con 3 de los 4 siguientes tipos de caracteres: Mayúsculas, minúsculas, número, carácter especial

### Cuenta SMTP

VDS puede enviar notificaciones por correo electrónico mediante una configuración SMTP personalizada o el servicio SMTP integrado se puede utilizar seleccionando *Automatic*.

1. Introduzca una dirección de correo electrónico que se utilizará como dirección *de* cuando VDS envíe una notificación por correo electrónico. *no-reply@<your-domain>.com* es un formato común.

2. Introduzca una dirección de correo electrónico donde se deben dirigir los informes de éxito.
3. Introduzca una dirección de correo electrónico donde se deben dirigir los informes de errores.

[]

### Técnicos de nivel 3

Cuentas de técnicos de nivel 3 (también conocido como *.tech Accounts*) son cuentas a nivel de dominio para que los administradores de VDS las utilicen al realizar tareas administrativas en los equipos virtuales del entorno VDS. Se pueden crear cuentas adicionales en este paso o posteriormente.

1. Introduzca el nombre de usuario y la contraseña de las cuentas de administrador de nivel 3. ".tech" se adjuntará al nombre de usuario que introduzca para ayudar a diferenciar entre usuarios finales y cuentas técnicas. Documente estas credenciales para su uso posterior.

> ⓘ La práctica recomendada es definir cuentas con nombre para todos los administradores de VDS que deben tener credenciales a nivel de dominio para el entorno. Los administradores de VDS sin este tipo de cuenta pueden seguir teniendo acceso de administrador a nivel de VM mediante la funcionalidad *Connect to Server* integrada en VDS.

[]

#### Dominios

### Directorio activo

Introduzca el nombre de dominio de AD que desee.

### Dominio público

El acceso externo se protege mediante un certificado SSL. Esto se puede personalizar con su propio dominio y un certificado SSL autogestionado. De forma alternativa, al seleccionar *Automatic*, VDS puede administrar el certificado SSL, incluida una actualización automática de 90 días del certificado. Cuando se utiliza la opción automática, cada implementación usa un subdominio único de *cloudWorkspace.app*.

[]

#### Equipos virtuales

Para las puestas en marcha de RDS, los componentes requeridos, como controladoras de dominio, los agentes RDS y las puertas de enlace RDS, deben instalarse en servidores de plataforma. En producción, estos servicios deben ejecutarse en máquinas virtuales dedicadas y redundantes. Para las implementaciones de pruebas de concepto, se puede usar un solo equipo virtual para alojar todos estos servicios.

### Configuración de máquinas virtuales de plataforma

### Máquina virtual única

Esta es la selección recomendada para implementaciones de pruebas de concepto. En una sola puesta en marcha de máquinas virtuales, los siguientes roles se alojan en un único equipo virtual:

- Director de CW

- Puerta de enlace HTML5
- Puerta de enlace RDS
- Aplicación remota
- FTPS Server (opcional)
- Controlador de dominio

El número máximo recomendado de usuarios para casos de uso de RDS en esta configuración es de 100 usuarios. La carga de puertas de enlace RDS/HTML5 equilibradas no es una opción en esta configuración, lo que limita la redundancia y las opciones para aumentar el escalado en el futuro.

Si este entorno se diseñó para multi-tenancy, no se admite una única configuración de máquina virtual.

**Varios servidores**

Al dividir la plataforma VDS en varias máquinas virtuales, las siguientes funciones se alojan en equipos virtuales dedicados:

- Puerta de enlace de Escritorio remoto

  La configuración VDS se puede utilizar para implementar y configurar una o dos puertas de enlace RDS. Estas puertas de enlace transmiten la sesión de usuario de RDS desde la conexión a Internet abierta a las máquinas virtuales host de sesión dentro de la implementación. Las puertas de enlace RDS manejan una función importante, lo que protege a RDS de los ataques directos desde Internet abierta y para cifrar todo el tráfico de RDS dentro y fuera del entorno. Cuando se seleccionan dos puertas de enlace de Escritorio remoto, el programa de instalación VDS implementa 2 máquinas virtuales y las configura para equilibrar la carga de las sesiones de usuario RDS entrantes.

- Puerta de enlace HTML5

  La configuración VDS se puede utilizar para implementar y configurar una o dos puertas de enlace HTML5. Estas puertas de enlace alojan los servicios HTML5 que utiliza la función *Connect to Server* en VDS y el cliente VDS basado en web (portal H5). Cuando se seleccionan dos portales HTML5, el programa de instalación VDS implementa 2 máquinas virtuales y las configura para equilibrar la carga de las sesiones de usuario HTML5 entrantes.

  Si se utiliza la opción de varios servidores (incluso si los usuarios sólo se conectan a través del cliente VDS instalado), se recomienda al menos una puerta de enlace HTML5 para habilitar la funcionalidad *Connect to Server* desde VDS.

- Notas de escalabilidad de la puerta de enlace

  En los casos de uso de RDS, el tamaño máximo del entorno se puede escalar con VM de puerta de enlace adicionales, cada puerta de enlace RDS o HTML5 que admite aproximadamente 500 usuarios. Posteriormente, se pueden agregar gateways adicionales con la asistencia de servicios profesionales de NetApp mínima

Si este entorno se está diseñando para multi-tenancy, se requiere la selección de *Multiple Server*.

**Funciones de servicio**

- Cwmgr1

  Esta máquina virtual es la máquina virtual administrativa VDS de NetApp. Ejecuta la base de datos SQL Express, las utilidades auxiliares y otros servicios administrativos. En una implementación de *single Server*, esta VM también puede alojar los otros servicios, pero en una configuración de *Multiple Server*, esos servicios se mueven a diferentes equipos virtuales.

- CWPortal1(2)

  La primera puerta de enlace HTML5 se llama *CWPortal1*, la segunda es *CWPortal2*. En la implementación se pueden crear uno o dos. Se pueden agregar servidores adicionales después de la implementación para aumentar la capacidad (unas 500 conexiones por servidor).

- CWRDSGateway1 (2)

  La primera puerta de enlace RDS se llama *CWRDSGateway1*, la segunda es *CWRDSGateway2*. En la implementación se pueden crear uno o dos. Se pueden agregar servidores adicionales después de la implementación para aumentar la capacidad (unas 500 conexiones por servidor).

- Aplicación remota

  App Service es una colección dedicada para alojar aplicaciones RemotApp, pero utiliza las puertas de enlace RDS y sus funciones RDWeb para enrutar las solicitudes de sesión de usuario final y alojar la lista de suscripción de aplicaciones RDWeb. No se ha puesto en marcha ningún equipo virtual dedicado para esta función de servicio.

- Controladores de dominio

  En la implementación se pueden crear y configurar automáticamente uno o dos controladores de dominio para que funcionen con VDS.

[]

**De NetApp**

Seleccione el sistema operativo del servidor que desea implementar para los servidores de la plataforma.

**Zona horaria**

Seleccione la zona horaria deseada. Los servidores de plataforma se configurarán para esta hora y los archivos de registro reflejarán esta zona horaria. La sesión de usuario final seguirá reflejando su propia zona horaria, independientemente de esta configuración.

**Servicios adicionales**

**FTP**

VDS puede instalar y configurar Filezilla de forma opcional para ejecutar un servidor FTPS con el fin de mover datos dentro y fuera del entorno. Esta tecnología es antigua y se recomiendan métodos de transferencia de datos más modernos (como Google Drive).

[]

#### Red

Se recomienda aislar las máquinas virtuales en diferentes subredes según su propósito.

Defina el alcance de la red y agregue un intervalo /20.

El programa de instalación de VDS detecta y sugiere un rango que debería resultar satisfactorio. Según las prácticas recomendadas, las direcciones IP de subred deben encontrarse en un rango de direcciones IP privadas.

Estos intervalos son:

- 192.168.0.0 hasta 192.168.255.255
- 172.16.0.0 hasta 172.31.255.255
- 10.0.0.0 hasta 10.255.255.255

Revise y ajuste si es necesario, haga clic en Validar para identificar subredes para cada una de las siguientes:

- Inquilino: Este es el intervalo en el que residirán los servidores de host de sesión y los servidores de base de datos
- Servicios: Esta es la gama en la que residirán los servicios de PaaS como Cloud Volumes Service
- Plataforma: Esta es la gama en la que residirán los servidores de la plataforma
- Directorio: Este es el intervalo en el que residirán los servidores AD

[]

#### Licencia

### NO SPLA

Introduzca su número SPLA para que VDS pueda configurar el servicio de licencia RDS para un informe de CAL de SPLA más sencillo. Se puede introducir un número temporal (como 12345) para la implementación de una prueba de concepto, pero tras un periodo de prueba (~120 días) las sesiones de RDS dejarán de conectarse.

### Productos SPLA

Introduzca los códigos de licencia de MAK para cualquier producto de Office con licencia a través de SPLA para habilitar informes SPLA simplificados desde los informes de VDS.

### ThinPrint

Elija instalar el servidor de licencias y la licencia de ThinPrint incluidos para simplificar la redirección de la impresora del usuario final.

[]

#### Revisión y aprovisionamiento

Una vez completados todos los pasos, revise las selecciones y, a continuación, valide y aprovisione el entorno.[]

#### Siguientes pasos

El proceso de automatización de implantación implementará ahora un nuevo entorno RDS con las opciones seleccionadas en el asistente de implementación.

Recibirá varios correos electrónicos cuando finalice la implementación. Una vez terminado, dispondrá de un entorno listo para su primer espacio de trabajo. Un espacio de trabajo contendrá los hosts de sesión y los servidores de datos necesarios para dar soporte a los usuarios finales. Vuelva a esta guía para seguir los siguientes pasos una vez que finalice la automatización de la puesta en marcha en 1-2 horas.

### Cree una nueva colección de aprovisionamiento

El aprovisionamiento de colecciones es una funcionalidad en VDS que permite la creación, personalización y Sysprep de imágenes de equipos virtuales. Una vez que entremos en la implementación en el lugar de trabajo, necesitaremos una imagen para implementarla. Los siguientes pasos le guiarán a través de la creación de una imagen de VM.

**Siga estos pasos para crear una imagen básica para la implementación:**

1. Vaya a *despliegues > Cobranzas de aprovisionamiento* y haga clic en *Add*

   []

2. Introduzca un nombre y una descripción. Elija *Type: Shared*.

   Puede elegir Shared o VDI. Compartido admitirá un servidor de sesión más (opcionalmente) un servidor empresarial para aplicaciones como una base de datos. VDI es una única imagen de máquina virtual para equipos virtuales que se dedicará a usuarios individuales.

3. Haga clic en *Add* para definir el tipo de imagen de servidor que se va a generar.

   []

4. Seleccione TSData como el *Server role*, la imagen VM adecuada (en este caso, el servidor 2016) y el tipo de almacenamiento deseado. Haga clic en *Add Server*

   []

5. Opcionalmente, seleccione las aplicaciones que se instalarán en esta imagen.
   a. La lista de aplicaciones disponibles se rellena desde la Biblioteca de aplicaciones a la que se puede acceder haciendo clic en el menú de nombres de administrador en la esquina superior derecha, debajo de la página *Settings > App Catalog*.

      []

6. Haga clic en *Add Collection* y espere a que se cree la máquina virtual. VDS creará una máquina virtual a la que se puede acceder y personalizar.
7. Una vez finalizada la compilación del equipo virtual, conéctese al servidor y realice los cambios deseados.
   a. Una vez que el estado muestre *Collection Validation*, haga clic en el nombre de la colección.

      []

   b. A continuación, haga clic en el *Server template name*

[]

c. Por último, haga clic en el botón *Connect to Server* para conectarse y iniciar sesión automáticamente en la máquina virtual con credenciales de administrador local.

[]

[]

8. Una vez completadas todas las personalizaciones, haga clic en *Validate Collection* para que VDS pueda sysprep y finalizar la imagen. Una vez finalizada, la máquina virtual se eliminará y la imagen estará disponible para la implementación dentro de los asistentes de implementación de VDS.

[]5

### Crear un espacio de trabajo nuevo

Un área de trabajo es una colección de hosts de sesión y servidores de datos que admiten un grupo de usuarios. Una implementación puede contener un solo espacio de trabajo (un solo inquilino) o varios espacios de trabajo (multi-tenant).

Los espacios de trabajo definen la colección del servidor RDS para un grupo específico. En este ejemplo, pondremos en marcha un único conjunto para demostrar la funcionalidad de los escritorios virtuales. Sin embargo, el modelo se puede ampliar a varios espacios de trabajo/colecciones RDS para admitir diferentes grupos y ubicaciones dentro del mismo espacio de dominio de Active Directory. De manera opcional, los administradores pueden restringir el acceso entre los espacios de trabajo y las colecciones para dar soporte a casos de uso que requieran un acceso limitado a aplicaciones y datos.

#### Cliente y configuración

1. En VDS de NetApp, desplácese hasta *Workspaces* y haga clic en *+ New Workspace*

   []

2. Haga clic en *Add* para crear un nuevo cliente. Los detalles del cliente normalmente representan la información de la compañía o la información de una ubicación o departamento específico.

   []

   a. Introduzca los detalles de la empresa y seleccione la implementación en la que se va a implementar este espacio de trabajo.
   b. **Unidad de datos:** defina la letra de unidad que se va a utilizar para la unidad de asignación de recursos compartidos de la empresa.
   c. **Unidad de inicio de usuario:** defina la letra de unidad que se va a utilizar para la unidad asignada de la persona.
   d. **Ajustes adicionales**

      Los siguientes ajustes se pueden definir en la implementación y/o después de la implementación seleccionada.

      i. *Enable Remote App:* la aplicación remota presenta aplicaciones como aplicaciones de streaming en lugar de (o además) presentar una sesión de escritorio remota completa.
      ii. *Enable App Locker:* VDS contiene la funcionalidad de implementación y asignación de

aplicaciones, de forma predeterminada, el sistema mostrará/ocultará las aplicaciones a los usuarios finales. La activación de App Locker obligará el acceso a la aplicación a través de una lista de seguridad de GPO.

iii. *Enable Workspace User Data Storage:* determine si los usuarios finales necesitan tener acceso al almacenamiento de datos en su escritorio virtual. Para las puestas en marcha de RDS, este valor debe comprobarse siempre para habilitar el acceso a los datos para ver los perfiles de usuario.

iv. *Disable Printer Access:* VDS puede bloquear el acceso a las impresoras locales.

v. *Permitir acceso al Administrador de tareas:* VDS puede habilitar/deshabilitar el acceso de usuario final al Administrador de tareas en Windows.

vi. *Requerir contraseña de usuario compleja:* la necesidad de contraseñas complejas habilita las reglas nativas de contraseñas complejas de Windows Server. También deshabilita el desbloqueo automático de cuentas de usuario bloqueadas con retraso de tiempo. De este modo, cuando se habilita esta opción, se requiere la intervención del administrador cuando los usuarios finales bloquean sus cuentas con varios intentos fallidos de contraseña.

vii. *Enable MFA for All Users:* VDS incluye un servicio MFA de correo electrónico/SMS sin coste que se puede utilizar para proteger el acceso a la cuenta de administrador de VDS o de usuario final. Para habilitar esto, todos los usuarios finales de este espacio de trabajo deberán autenticarse con MFA para acceder a sus escritorios y/o aplicaciones.

#### Elija aplicaciones

Seleccione la versión del sistema operativo Windows y la colección de aprovisionamiento creadas anteriormente en esta guía.

En este punto se pueden agregar aplicaciones adicionales, pero en esta prueba de concepto trataremos el derecho a las aplicaciones tras la puesta en marcha.

[]

#### Agregar usuarios

Se pueden añadir usuarios seleccionando grupos de seguridad de AD o usuarios individuales. En esta guía de prueba de concepto añadiremos usuarios tras la puesta en marcha.

[]

#### Revisión y aprovisionamiento

En la página final, revise las opciones elegidas y haga clic en *Provision* para iniciar la creación automatizada de los recursos RDS.

[]

Durante el proceso de implementación, los registros se crean y se puede acceder a ellos en *Task History*, cerca de la parte inferior de la página de detalles de la implementación. Para acceder, vaya a *VDS > despliegues > Deployment Name*

#### Siguientes pasos

El proceso de automatización del lugar de trabajo implementará ahora nuevos recursos RDS con las opciones seleccionadas en el asistente de implementación.

Una vez finalizado, existen varios flujos de trabajo comunes que deberá seguir para personalizar la puesta en marcha de RDS típica.

- "Agregar usuarios"
- "Acceso del usuario final"
- "Autorización de aplicaciones"
- "Optimización de costes"

## Requisitos previos de Google Compute Platform (GCP) y VDS

### Requisitos y notas de GCP y VDS

Este documento describe los elementos necesarios para la implementación de Servicios de Escritorio remoto (RDS) mediante el Servicio de puestos de trabajo virtuales (VDS) de NetApp. La “Lista de comprobación rápida” proporciona una breve lista de los componentes necesarios y los pasos previos a la implementación que se deben llevar a cabo para garantizar una implementación eficiente. El resto de la guía ofrece mayor detalle para cada elemento, dependiendo de las opciones de configuración que se tomen.

[anchura = 75%]

### Lista de comprobación rápida

#### Requisitos para GCP

- Cliente GCP
- Proyecto GCP
- Cuenta de servicio con la función de propietario asignada

#### Información previa a la implementación

- Determinar el número total de usuarios
- Determine la región y zona de GCP
- Determinar el tipo de directorio activo
- Determinar el tipo de almacenamiento
- Identifique los requisitos o la imagen del equipo virtual del host de sesión
- Evaluar la configuración de redes existente para GCP y en las instalaciones

### Requisitos detallados de la implementación de VDS

#### Requisitos de conexión de usuario final

**Los siguientes clientes de Escritorio remoto admiten RDS en GCP:**

- "Cliente VDS de NetApp para Windows"
  - Requisitos de seguridad de la URL de salida de Windows del cliente VDS de NetApp
    - api.cloudworkspace.com
    - vdsclient.app
    - api.vdsclient.app

        - bin.vdsclient.app
    - Funciones mejoradas:
        - Activación de VDS bajo demanda
        - Cliente ThinPrint y piojos
        - Restablecimiento de contraseña de autoservicio
        - Negociación automática de direcciones de servidor y puerta de enlace
        - Compatibilidad total con aplicaciones de streaming y escritorio
        - Marca personalizada disponible
        - Switches de instalador para la implementación y la configuración automatizadas
        - Herramientas integradas de solución de problemas
- "Cliente web VDS de NetApp"
- "Cliente RD de Microsoft"
    - Windows
    - MacOS
    - ISO
    - Android
- clientes ligeros o de software de terceros
    - Requisito: Admitir la configuración de puerta de enlace de Escritorio remoto

**Capa de almacenamiento**

En RDS implementado por VDS, la estrategia de almacenamiento se ha diseñado de forma que no haya datos persistentes de usuarios o empresas en los equipos virtuales de sesión de AVD. Los datos persistentes de perfiles de usuario, archivos y carpetas de usuario, y datos de aplicación/empresa se alojan en uno o más volúmenes de datos alojados en una capa de datos independiente.

FSLogix es una tecnología de agrupación en contenedores de perfiles que resuelve muchos problemas de perfil de usuario (como la dispersión de datos y los inicios de sesión lentos) mediante el montaje de un contenedor de perfiles de usuario (formato VHD o VHDX) en el host de sesión durante la inicialización de la sesión.

Gracias a esta arquitectura, es necesaria una función de almacenamiento de datos. Esta función debe ser capaz de gestionar la transferencia de datos necesaria cada mañana/tarde cuando una parte significativa del inicio de sesión/cierre de sesión de los usuarios al mismo tiempo. Incluso los entornos de tamaño moderado pueden tener requisitos significativos de transferencia de datos. El rendimiento de disco de la capa de almacenamiento de datos es una de las variables de rendimiento del usuario final principal y se debe tener cuidado en cuenta para ajustar el tamaño del rendimiento de este almacenamiento, no solo la cantidad de almacenamiento. Por lo general, se debe ajustar el tamaño de la capa de almacenamiento para que admita 5-15 IOPS por usuario.

**Redes**

**Requerido:** un inventario de todas las subredes de red existentes incluyendo todas las subredes visibles para el proyecto GCP a través de una VPN. La implementación debe evitar que se solapen las subredes.

El asistente de configuración de VDS permite definir el ámbito de red en caso de que sea necesario o necesario evitarlo, como parte de la integración planificada con las redes existentes.

Determine un rango de IP para el usuario durante la implementación. Según las prácticas recomendadas, sólo se admiten direcciones IP de un rango privado.

**Las opciones admitidas incluyen las siguientes, pero por defecto, en un intervalo de /20:**

- 192.168.0.0 hasta 192.168.255.255
- 172.16.0.0 hasta 172.31.255.255
- 10.0.0.0 hasta 10.255.255.255

### CWMGR1

Algunas de las funciones exclusivas de VDS, como la programación de cargas de trabajo de ahorro de costes y la funcionalidad de ampliación en tiempo real, requieren una presencia administrativa dentro de la organización y el proyecto. Por lo tanto, se implementa una VM administrativa denominada CWMGR1 como parte de la automatización del asistente de configuración de VDS. Además de las tareas de automatización VDS, esta máquina virtual también contiene la configuración VDS en una base de datos SQL Express, archivos de registro local y una utilidad de configuración avanzada denominada DCConfig.

**En función de las selecciones realizadas en el asistente de configuración de VDS, esta máquina virtual se puede usar para alojar funcionalidades adicionales como:**

- Una puerta de enlace RDS
- Una puerta de enlace HTML 5
- Un servidor de licencias RDS
- Un controlador de dominio

#### Árbol de decisiones en el Asistente para implementación

Como parte de la implementación inicial, se responden una serie de preguntas para personalizar la configuración del nuevo entorno. A continuación se presenta un resumen de las principales decisiones que se deben tomar.

### GCP, región

Decidir qué región o regiones de GCP alojarán las máquinas virtuales VDS. Tenga en cuenta que la región debe seleccionarse en función de la proximidad con los usuarios finales y los servicios disponibles.

### Almacenamiento de datos

Decida dónde se colocarán los datos de perfiles de usuario, archivos individuales y recursos compartidos de la empresa. Las opciones incluyen:

- Cloud Volumes Service para GCP
- Servidor de ficheros tradicional

## Requisitos de implementación de VDS de NetApp para los componentes existentes

#### Implementación de VDS de NetApp con controladores de dominio de Active Directory existentes

Este tipo de configuración amplía un dominio de Active Directory existente para admitir la instancia de RDS. En este caso, VDS implementa un conjunto limitado de componentes en el dominio para admitir tareas de aprovisionamiento y administración automatizadas para los componentes RDS.

**Esta configuración requiere:**

- Una controladora de dominio de Active Directory existente a la que se puede acceder mediante máquinas virtuales en la red VPC de GCP, normalmente a través de VPN o de una controladora de dominio creada en GCP.
- Adición de componentes y permisos de VDS a la gestión de hosts de RDS y volúmenes de datos a medida que se unen al dominio. El proceso de implementación requiere un usuario de dominio con privilegios de dominio para ejecutar la secuencia de comandos que creará los elementos necesarios.
- Tenga en cuenta que la implementación de VDS crea una red VPC de forma predeterminada para las máquinas virtuales creadas por VDS. La red VPC puede realizarse una relación entre iguales con las redes VPC existentes, o bien la máquina virtual CWMGR1 se puede mover a una red VPC existente con las subredes predefinidas necesarias.

### Credenciales y herramienta de preparación de dominios

Los administradores deben proporcionar una credencial de administrador de dominio en algún momento del proceso de implementación. Se puede crear, utilizar y eliminar posteriormente una credencial temporal del Administrador de dominio (una vez completado el proceso de implementación). Como alternativa, los clientes que necesiten ayuda para crear los requisitos previos pueden aprovechar la herramienta de preparación de dominios.

#### Implementación de VDS de NetApp con un sistema de archivos existente

VDS crea recursos compartidos de Windows que permiten acceder a los perfiles de usuario, carpetas personales y datos de la empresa desde los hosts de sesión de RDS. VDS implementará el servidor de archivos de forma predeterminada, pero si tiene un componente de almacenamiento de archivos existente VDS puede señalar los recursos compartidos a ese componente una vez completada la implementación de VDS.

**Requisitos para utilizar y el componente de almacenamiento existente:**

- El componente debe ser compatible con SMB v3
- El componente debe estar Unido al mismo dominio de Active Directory que los hosts de sesión de RDS.
- El componente debe ser capaz de exponer una ruta UNC que se utilizará en la configuración de VDS; se puede utilizar una ruta para los tres recursos compartidos o se pueden especificar rutas independientes para cada uno de ellos. Tenga en cuenta que VDS establecerá los permisos de nivel de usuario para estos recursos compartidos, asegúrese de que se han concedido los permisos correspondientes a los Servicios de automatización de VDS.

### APÉNDICE A: Direcciones IP y URL del plano de control VDS

Los componentes VDS del proyecto GCP se comunican con los componentes del plano de control global VDS que están alojados en Azure, incluidos la aplicación web VDS y los extremos API VDS. Para el acceso, las siguientes direcciones URI base deben ser safelisted para el acceso bidireccional en el puerto 443:

"" "" "" ""

Si su dispositivo de control de acceso sólo puede hacer una lista segura por dirección IP, se debe garantizar la siguiente lista de direcciones IP. Tenga en cuenta que VDS utiliza un equilibrador de carga con direcciones IP públicas redundantes, por lo que esta lista puede cambiar con el tiempo:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178 13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239 52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

#### Factores de rendimiento óptimos

Para obtener un rendimiento óptimo, asegúrese de que la red cumple los siguientes requisitos:

- La latencia de ida y vuelta (RTT) desde la red del cliente hasta la región de GCP donde se hayan implementado los hosts de sesión deben ser inferiores a 150 ms.
- El tráfico de red puede fluir fuera de las fronteras del país o de la región cuando las máquinas virtuales que alojan escritorios y aplicaciones se conectan al servicio de gestión.
- Para optimizar el rendimiento de la red, recomendamos que los equipos virtuales del host de la sesión se encuentren ubicados en la misma región que el servicio de gestión.

#### Imágenes de SO de máquina virtual admitidas

Los puntos de sesión de RDS, implementados por VDS, admiten las siguientes imágenes del sistema operativo x64:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

## Información de copyright



## Información de la marca comercial