Administración de usuarios

Virtual Desktop Service

NetApp
February 20, 2023

Tabla de Contenido

Administración de usuarios

Gestión de cuentas de usuario

Crear nuevos usuarios

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

Los usuarios pueden agregarse individualmente o con una importación masiva.

[anchura = 25%]

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

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

Activación del escritorio virtual para los usuarios existentes de AD

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

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

Eliminar cuentas de usuario

Editar información del usuario

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

[]

Editar la configuración de seguridad del usuario

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

la cuenta de usuario final.

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

Cuenta bloqueada

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

Restablecer contraseña de usuario

Restablece la contraseña de usuario.

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

Acceso del administrador

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

Usuario(s) de cierre de sesión

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

Más grandes

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

Ver/eliminar procesos de usuario

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

Gestión de permisos de datos

Perspectiva del usuario final

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

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

[]

Gestión de permisos

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

Grupos de seguridad

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

En esta sección puede:

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

[]

Permisos de carpeta

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

En esta sección puede:

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

[]

Autorización de aplicaciones

Descripción general

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

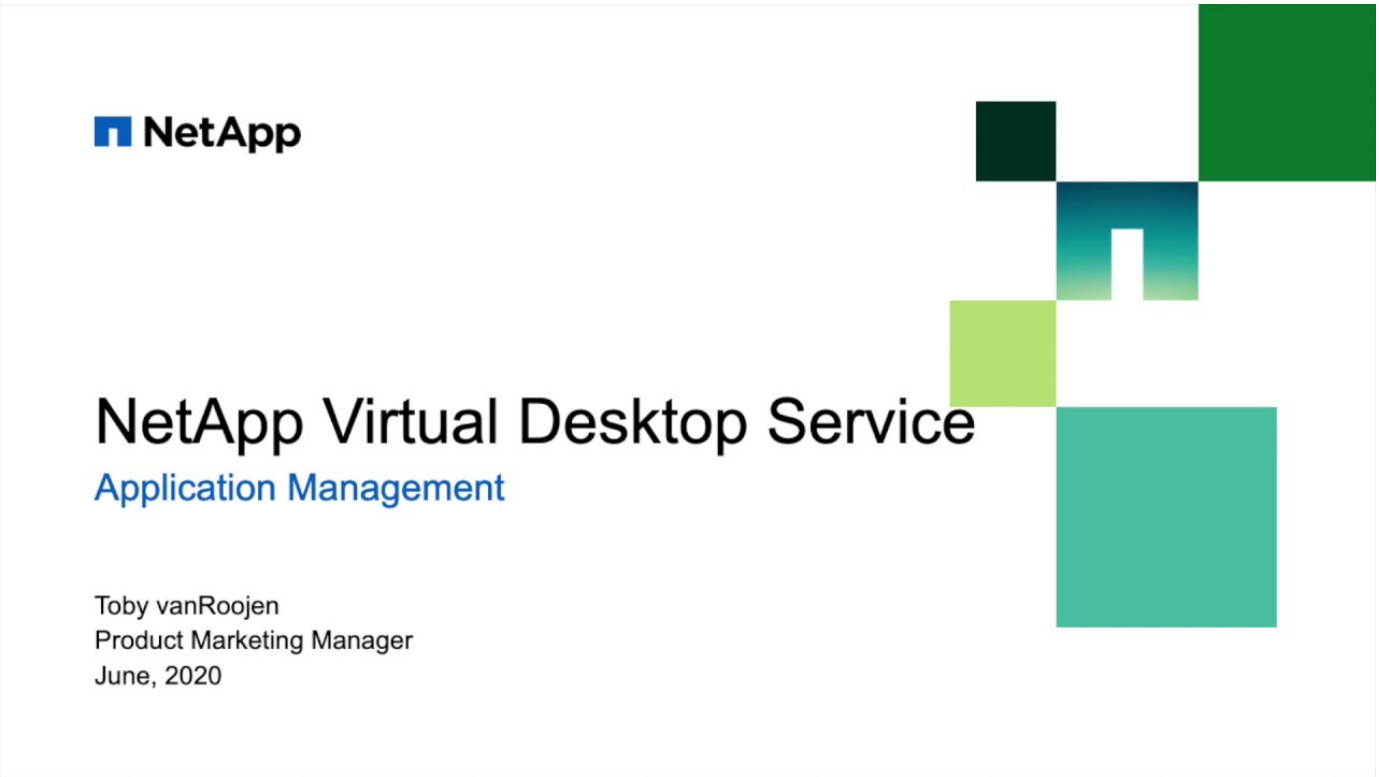
Este flujo de trabajo solo se aplica a implementaciones RDS. Para obtener la documentación sobre los derechos de aplicación de AVD, consulte "Flujo de trabajo de derechos de aplicación para AVD"

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

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

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

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



Demostración de vídeo

Agregar aplicaciones al catálogo de aplicaciones

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

Para agregar aplicaciones al catálogo, siga estos pasos

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

Agregue la aplicación al área de trabajo

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

Para ello, siga estos pasos

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

Instale manualmente la aplicación

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

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

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

Asigne aplicaciones a los usuarios

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

Asigne aplicaciones a los usuarios

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

Asignar usuarios a una aplicación

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

Asignar aplicaciones y usuarios a grupos de usuarios

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

Restablecer contraseña de usuario

Restablecer pasos de contraseña de usuario

1. Desplácese hasta la página Detalles usados en VDS

   []

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

   []

   []

Tiempo para tomar efecto

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

  []

Restablecimiento de contraseña de autoservicio (SSRP)

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

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

SSPR es compatible con:

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

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

Cliente Windows VDS de NetApp

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

[]

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

   []

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

   []

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

   []

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

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

   []

Portal HTML5

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

   []

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

   []

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

   []

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

   []

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

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

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

Importación masiva de usuarios a través de VDS

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

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

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

Suministrar los datos a través de la API VDS

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

Actualizando el teléfono de usuario existente

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

[]

Uso de otras consolas

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

Personalizar dirección de envío SSPR

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

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

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

  []

- Dirección "de" deseada (que debe ser válida)

- A qué clientes debe aplicarse la configuración (o todas)

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

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

Complejidad de la contraseña

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

[]

[]

Complejidad de la contraseña: Desactivada

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

Complejidad de la contraseña: Activado

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

Política	Pautas
Duración del bloqueo	Permanece bloqueado hasta que se desbloquea el administrador

Autenticación multifactor (MFA)

Descripción general

El servicio de escritorios virtuales (VDS) de NetApp incluye un servicio de MFA basado en SMS/correo electrónico sin coste adicional. Este servicio es independiente de cualquier otro servicio (por ejemplo, Azure Conditional Access) y se puede utilizar para proteger los inicios de sesión de administrador en VDS y los inicios de sesión de usuario en escritorios virtuales.

Aspectos básicos de la MFA

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

Alcance de la guía

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

En esta guía se tratan los siguientes temas:

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

Habilitar MFA para usuarios individuales

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

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

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

Que requiere MFA para todos los usuarios

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

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

Habilitación de MFA para administradores individuales

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

Configuración inicial

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