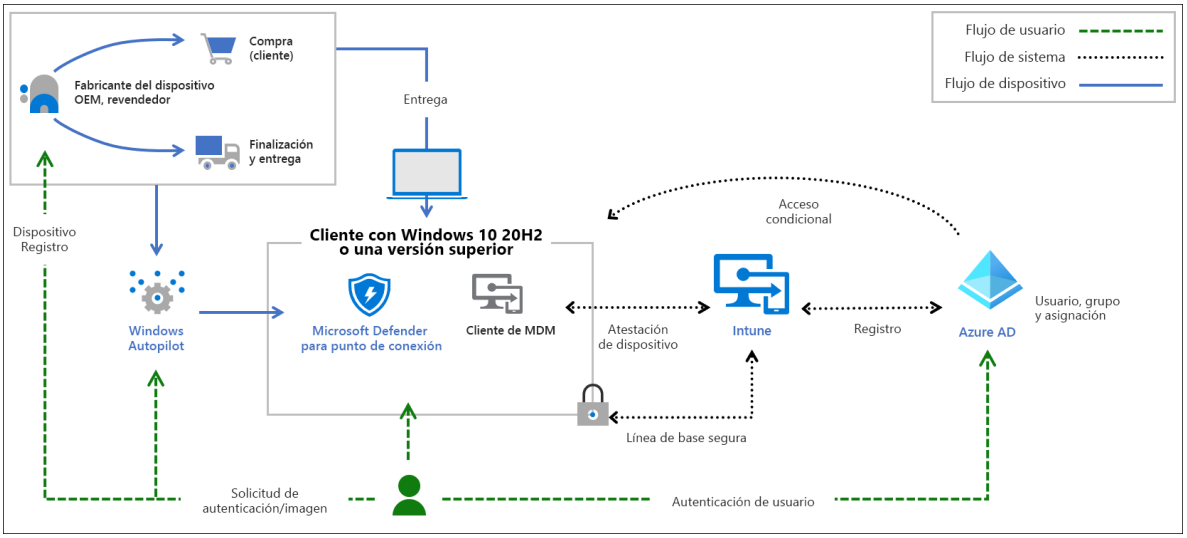
Definición de una estrategia para dispositivos con privilegios de acceso

Se trata de una guía relativamente nueva de Microsoft. Para garantizar las condiciones más seguras para su empresa, es necesario garantizar la seguridad desde el momento de la compra de un nuevo dispositivo, hasta su primer uso, y más allá. Confianza cero significa que no compra a minoristas genéricos, sino que solo se suministra hardware de un OEM autorizado que admita Autopilot.

En esta solución, el certificado raíz de confianza se implementará con la tecnología Windows Autopilot, con hardware que cumpla los requisitos técnicos modernos. Para proteger una estación de trabajo, Autopilot le permite aprovechar los dispositivos de Windows 10 optimizados para fabricantes de equipos originales de Microsoft. Estos dispositivos vienen en un buen estado conocido de fábrica. En lugar de restablecer la imagen inicial de un dispositivo potencialmente inseguro, Autopilot puede transformar un dispositivo con Windows 10 en un dispositivo en estado "preparado para la empresa". Autopilot aplica valores y directivas, instala aplicaciones e incluso cambia la edición de Windows 10.



Raíz de confianza de hardware

Para tener una estación de trabajo protegida, debe asegurarse de que se incluyen las siguientes tecnologías de seguridad en el dispositivo:

- Módulo de plataforma segura (TPM) 2.0
- Cifrado BitLocker de unidades
- Arranque seguro de la UEFI
- Controladores y firmware distribuidos mediante Windows Update
- Virtualización y HVCI habilitados
- Controladores y aplicaciones HVCI-Ready
- Windows Hello

- Protección de E/S de DMA
- Iniciar protección del sistema
- Modo de espera moderno

Implementación de estaciones de trabajo con privilegios de acceso

Las estaciones de trabajo con privilegios de acceso proporcionan un sistema dedicado para tareas confidenciales que están protegidas frente a ataques de Internet y vectores de amenazas. La separación de estas tareas y cuentas delicadas de las estaciones de trabajo y dispositivos de uso diario proporciona una protección muy eficaz contra ataques de suplantación de identidad (phishing), las vulnerabilidades de las aplicaciones o del sistema operativo, diversos ataques de suplantación y ataques de robo de credenciales, como registro de pulsaciones de teclas, y ataques pass-the-hash y pass-the-ticket.

Estaciones de trabajo con privilegios de acceso

La estación de trabajo con privilegios de acceso es una estación de trabajo reforzada y bloqueada, diseñada para proporcionar altas garantías de seguridad para las cuentas y tareas confidenciales. Las PAW se recomiendan para la administración de sistemas de identidad, servicios en la nube y tejido de nube privada, así como para funciones empresariales de carácter delicado. Con el fin de proporcionar la mayor seguridad, las PAW siempre deben ejecutar el sistema operativo más actualizado y seguro disponible: Microsoft recomienda encarecidamente Windows 10 Enterprise, que incluye varias características de seguridad adicionales que no están disponibles en otras ediciones (en particular, Credential Guard y Device Guard).

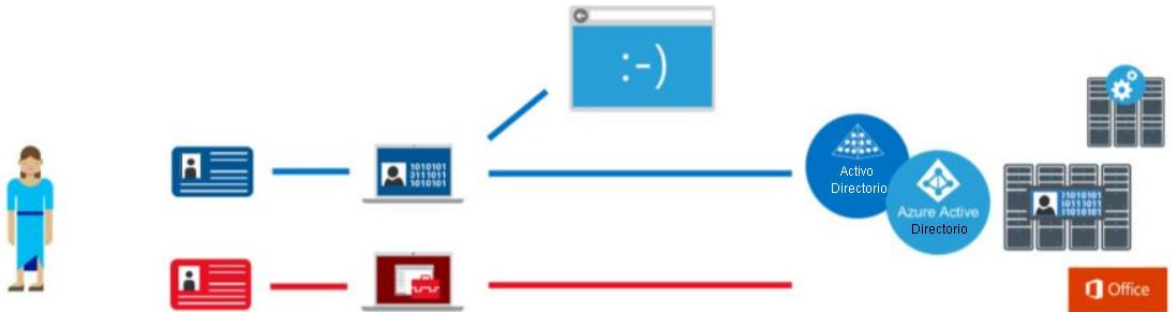
Los controles de seguridad de PAW se centran en mitigar los riesgos de alto impacto y alta probabilidad de riesgo. Por ejemplo, puedes mitigar los ataques en el entorno y los riesgos que pueden limitar la efectividad de los controles de PAW con el tiempo:

- **Ataques a través de Internet**: aislar estación de trabajo con privilegios de acceso de la red abierta Internet es un elemento clave para asegurar que la estación de trabajo no se vea comprometida.
- **Riesgo de facilidad de uso**: si una PAW es demasiado difícil de usar para las tareas diarias, los administradores se sentirán empujados a crear soluciones para que sus trabajos sean más fáciles.
- **Riesgos del entorno**: minimizar el uso de las herramientas de administración y las cuentas que tienen acceso a las estaciones de trabajo con privilegios de acceso para proteger y supervisar estas estaciones de trabajo especializadas.
- **Alteración de la cadena de suministro**: adoptar algunas medidas clave puede mitigar los vectores de ataque críticos que están fácilmente disponibles para los atacantes. Esto incluye validar la integridad de todos los medios de instalación (principio de origen limpio) y usar un proveedor de confianza para el hardware y el software.

- **Ataques físicos**: como las PAW se pueden mover físicamente y se usan fuera de instalaciones físicamente seguras, se deben proteger frente a ataques que aprovechan el acceso físico no autorizado al equipo.

Introducción a la arquitectura

El siguiente diagrama representa un "canal" aparte para la administración (una tarea enormemente confidencial) que se crea al mantener cuentas y estaciones de trabajo administrativas dedicadas.



Este enfoque de arquitectura se basa en las protecciones encontradas en las características Credential Guard y Device Guard de Windows 10 y va más allá de esas protecciones para abarcar las cuentas y las tareas confidenciales.

Esta metodología es apropiada para las cuentas con acceso a recursos de alto valor:

- **Privilegios administrativos:** las PAW proporcionan mayor seguridad en roles y tareas administrativos de TI de gran impacto. Esta arquitectura se puede aplicar a la administración de muchos tipos de sistemas, incluidos dominios y bosques de Active Directory, inquilinos de Microsoft Azure Active Directory, inquilinos de Microsoft 365, redes de control de procesos (PCN), sistemas de control de supervisión y adquisición de datos (SCADA), cajeros automáticos y dispositivos de punto de venta.
- **Trabajadores que administran información de alta confidencialidad:** el enfoque usado en una PAW puede proporcionar también protección para las tareas y el personal que trabaja con información confidencial, como aquellos relacionados con la actividad de fusiones y adquisiciones con anuncio previo, informes financieros previos al lanzamiento, presencia de medios sociales organizativos, comunicaciones ejecutivas, secretos comerciales sin patentar, investigaciones confidenciales u otros datos propietarios o confidenciales. En esta guía no se analiza en profundidad la configuración de estos escenarios de trabajadores de la información ni se incluye este escenario de instrucciones técnicas.

La protección del acceso con privilegios es un primer paso crítico para establecer controles de seguridad para los recursos empresariales de una organización moderna. La seguridad de la mayoría, si no todos, los recursos empresariales de una organización de TI depende de la integridad de las cuentas con privilegios que realizan tareas de administración, gestión y desarrollo.

Jump Box

Las arquitecturas administrativas "Jump Box" establecen un pequeño número de servidores de consola administrativos y restringen al personal a utilizarlos para tareas administrativas. Normalmente se basan en servicios de escritorio remoto, soluciones de virtualización de presentación de terceros o en una tecnología de Infraestructura de escritorio virtual (VDI).

Este enfoque se propone con frecuencia para mitigar el riesgo para la administración y proporciona algunas garantías de seguridad, pero el enfoque de la jump box por sí mismo es vulnerable a ciertos ataques porque infringe el principio de **origen limpio**. El principio de origen limpio requiere que todas las dependencias de seguridad sean tan confiables como el objeto que se protege.

Esta ilustración representa una relación de control sencilla. Cualquier sujeto con el control de un objeto es una dependencia de seguridad de dicho objeto. Si un adversario puede controlar una dependencia de seguridad de un objeto de destino (sujeto), puede controlar ese objeto.

La sesión administrativa en el servidor de salto depende de la integridad del equipo local que accede a él. Si este equipo es una estación de trabajo de usuario sujeta a ataques de suplantación y a otros vectores de ataques basados en Internet, la sesión administrativa está sujeta también a esos riesgos.

Aunque algunos controles de seguridad avanzados, como la autenticación multifactor, pueden aumentar la dificultad de que un atacante tome el control de esta sesión administrativa desde la estación de trabajo de usuario, ninguna característica de seguridad puede proteger completamente frente a ataques técnicos cuando un atacante tiene acceso administrativo al equipo de origen (por ejemplo, insertando comandos ilícitos en una sesión legítima, secuestrando procesos legítimos, etc.).

La configuración predeterminada en esta guía de PAW instala herramientas administrativas en la PAW, pero una arquitectura de servidor de salto también se puede agregar en caso necesario.

La figura anterior muestra cómo al invertir la relación de control y acceder a las aplicaciones de usuario desde una estación de trabajo de administrador, el atacante no puede acceder al objeto pretendido. La jump box del usuario sigue expuesta al riesgo, por lo que se deben seguir aplicando

los controles de protección, los controles de detección y los procesos de respuesta adecuados para ese equipo con conexión a Internet.

Crear plantillas de máquina virtual

Antes de entrar en la configuración de plantillas y directivas de máquina virtual, debe comprender las características y la funcionalidad de Azure Resource Manager.

Resource Manager es el servicio de implementación y administración de la suscripción de Azure. Proporciona una capa de administración coherente que le permite crear, actualizar y eliminar recursos en su suscripción de Azure. Puede usar sus características de control de acceso, auditoría y etiquetado para ayudar a proteger y organizar los recursos después de la implementación.

Al realizar acciones a través de Azure Portal, Azure PowerShell, la CLI de Azure, las API REST o los SDK de cliente, la API de Resource Manager es quien administra la solicitud. Dado que la misma API controla todas las solicitudes, se obtienen resultados y funcionalidades coherentes en todas las distintas herramientas.

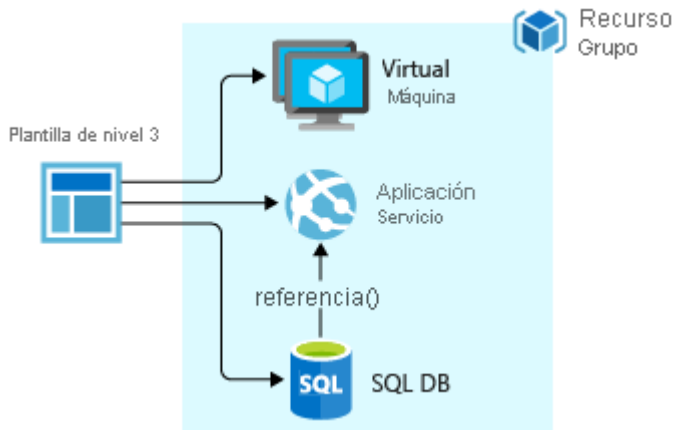
Estos son algunos términos adicionales que debe conocer al usar Resource Manager:

- **Proveedor de recursos**. Un servicio que proporciona recursos de Azure. Por ejemplo, un proveedor de recursos común es Microsoft.Compute, que proporciona el recurso de máquina virtual. Microsoft.Storage es otro proveedor de recursos común.
- **Plantilla de Resource Manager**. Un archivo JSON que define uno o varios recursos para implementar en un grupo de recursos o una suscripción. Puede usar la plantilla para implementar los recursos de forma coherente y repetida.
- **Sintaxis declarativa**. Sintaxis que le permite decir "Esto es lo que quiero crear" sin tener que escribir la secuencia de comandos de programación para crearla. La plantilla de Resource Manager es un ejemplo de sintaxis declarativa. En el archivo, puede definir las propiedades de la infraestructura que se va a implementar en Azure.

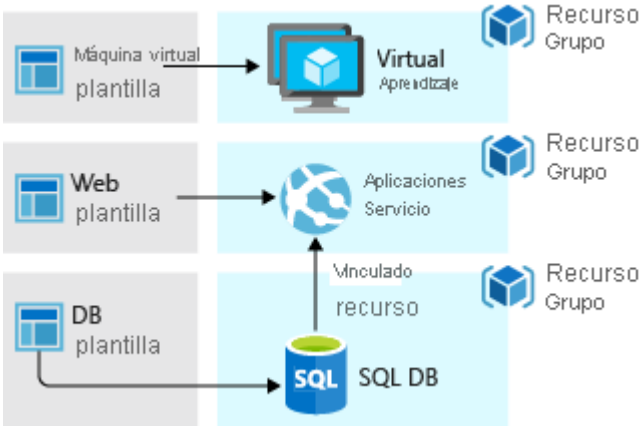
Puede usar la plantilla Resource Manager para definir las máquinas virtuales. Una vez definidas, puede implementarlas y volver a implementarlas fácilmente. Se recomienda volver a implementar periódicamente las máquinas virtuales para forzar la implementación de un sistema operativo de la máquina virtual recién actualizado y con mayor seguridad.

Diseño de plantilla

La definición de plantillas y grupos de recursos depende únicamente de usted, al igual que la administración de la solución. Por ejemplo, puede implementar su aplicación de tres niveles a través de una única plantilla en un único grupo de recursos.



No obstante, no es necesario que defina toda la infraestructura en una sola plantilla. A menudo, tiene sentido dividir los requisitos de implementación en un conjunto de plantillas seleccionadas, específicas para un propósito. Estas plantillas se pueden reutilizar fácilmente para distintas soluciones. Para implementar una solución concreta, cree una plantilla maestra que vincule todas las plantillas necesarias. Si desea que sus niveles tengan ciclos de vida independientes, puede implementar los tres niveles en grupos de recursos independientes. Observe que todavía se pueden vincular los recursos a los recursos de otros grupos.



Importante

Cuando se implementa una plantilla, Resource Manager la convierte en operaciones de la API de REST.

Habilitación y protección de la administración de acceso remoto

En este tema se explica cómo conectarse a las máquinas virtuales (VM) que creó en Azure e iniciar sesión en ellas. Cuando se haya conectado correctamente, puede trabajar con la máquina virtual como si hubiera iniciado sesión localmente en su servidor host.

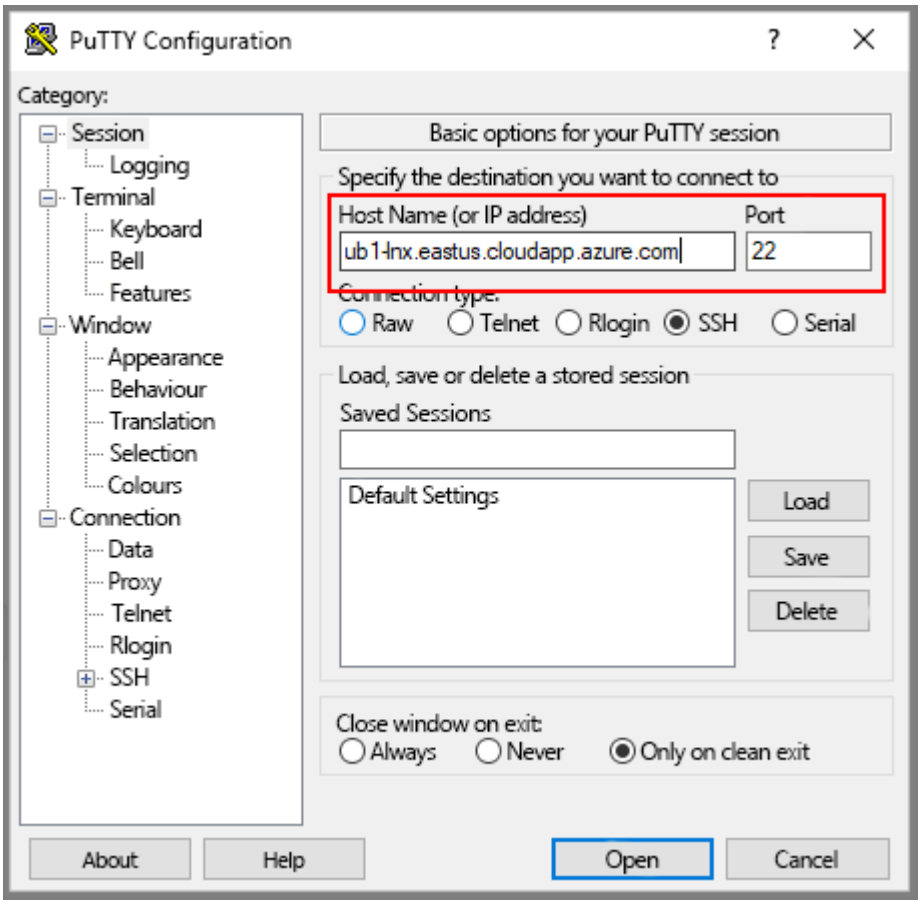
Conexión a una máquina virtual Windows

La forma más común de conectarse a una VM basada en Windows que se ejecuta en Azure es mediante el Protocolo de Escritorio Remoto (RDP). . La mayoría de las versiones de Windows incluyen compatibilidad de forma nativa con el Protocolo de escritorio remoto (RDP). Si se conecta a una máquina Windows virtual desde un equipo Mac, deberá instalar un cliente RDP para Mac.

Si utiliza PowerShell y tiene instalado el módulo Azure PowerShell, también puede conectarse utilizando el cmdlet `Get-AzRemoteDesktopFile`.

Conectarse a una máquina virtual basada en Linux

Para conectarse a la máquina virtual basada en Linux, necesita un cliente de protocolo Secure Shell (SSH). La herramienta gratuita más utilizada es el terminal SSH **PuTTY**. A continuación se muestra el cuadro de diálogo de configuración de PuTTY.



Azure Bastion

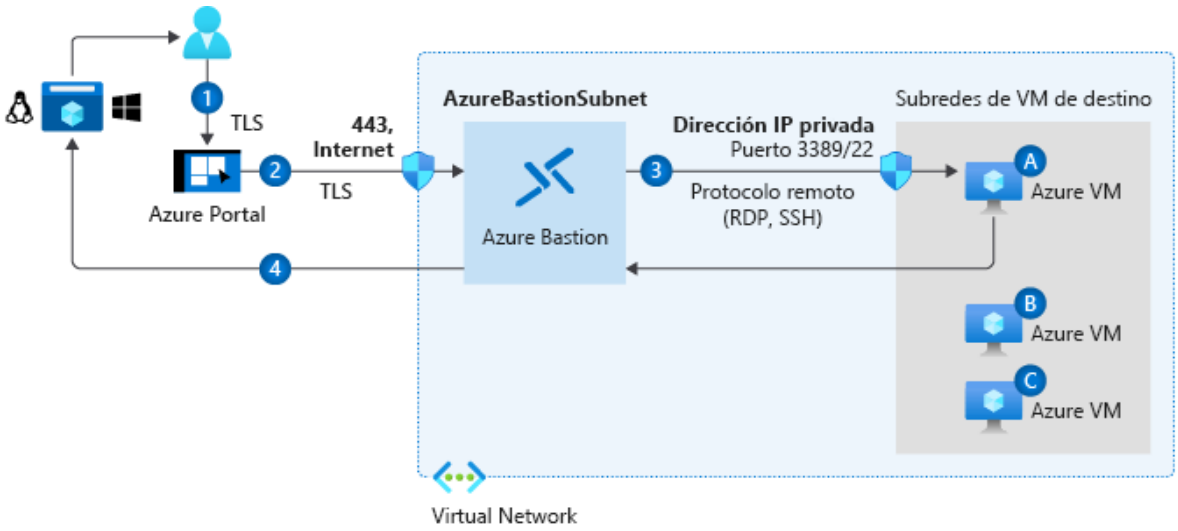
Azure Bastion es un nuevo servicio PaaS totalmente administrado por la plataforma que se aprovisiona en las redes virtuales. Proporciona una conectividad RDP/SSH segura e ininterrumpida a las máquinas virtuales directamente en Azure Portal a través de TLS. Cuando se conecta mediante Azure Bastion, las máquinas virtuales no necesitan una dirección IP pública.

Bastion proporciona conectividad RDP y SSH segura a todas las máquinas virtuales de la red virtual en la que se aprovisiona. El uso de Azure Bastion protege las máquinas virtuales frente a la exposición de los puertos de RDP/SSH al mundo exterior, al tiempo que ofrece acceso seguro mediante RDP/SSH. Con Azure bastión, puede contarse a la máquina virtual directamente desde Azure Portal.

Architecture

Azure Bastion se implementa en una red virtual y admite el emparejamiento de red virtual. En concreto, Azure Bastion administra la conectividad RDP/SSH con máquinas virtuales creadas en las redes virtuales locales o emparejadas.

RDP y SSH son algunos de los medios fundamentales a mediante los que puede conectarse a las cargas de trabajo que se ejecutan en Azure. La exposición de los puertos RDP/SSH a través de Internet no se conveniente y se considera una superficie de amenaza considerable. Esto suele deberse a las vulnerabilidades del protocolo. Para contener esta superficie de amenaza, puede implementar hosts de bastión (también conocidos como servidores de salto) en la parte pública de la red perimetral. Los servidores host de bastión están diseñados y configurados para resistir los ataques. Los servidores de bastión también proporcionan conectividad RDP y SSH con las cargas de trabajo que se encuentran detrás del bastión, así como más adentro en la red.



Esta ilustración muestra la arquitectura de una implementación de Azure Bastion. En este diagrama:

- El host de Bastion se implementa en la red virtual.
- El usuario se conecta a Azure Portal con cualquier explorador HTML5.
- El usuario selecciona la máquina virtual a la que conectarse.
- Con un solo clic, la sesión RDP/SSH se abre en el explorador.
- No se requiere ninguna dirección IP pública en la máquina virtual de Azure.

Principales características

Las siguientes características están disponibles:

- **RDP y SSH directamente en el portal de Azure**: puede acceder a la sesión RDP y SSH directamente en Azure Portal mediante una experiencia sin fisuras de un solo clic.
- **Sesión remota a través de TLS y cruce de firewall para RDP/SSH**: Azure Bastion utiliza un cliente web basado en HTML5 que se transmite automáticamente a su dispositivo local, de modo que obtiene su sesión RDP/SSH a través de TLS en el puerto 443 permitiéndole cruzar los firewall corporativos de forma segura.
- **No se requiere ninguna dirección IP pública en la VM de Azure:** Azure Bastion abre la conexión RDP/SSH a la máquina virtual de Azure con la dirección IP privada en la VM. No necesita una dirección IP pública en su máquina virtual.

- **No hay problemas de administración de los NSG:** Azure Bastion es un servicio PaaS de Azure de plataforma totalmente administrada que se refuerza internamente para proporcionar una conexión RDP/SSH segura. No es necesario aplicar los NSG en la subred de Azure Bastion. Dado que Azure Bastion se conecta a las máquinas virtuales a través de la dirección IP privada, puede configurar los NSG para permitir RDP o SSH solo desde Azure Bastion.
- **Protección frente al examen de puertos:** ya no es necesario exponer las máquinas virtuales a la red Internet pública, las máquinas virtuales están protegidas contra la exploración de puertos por parte de usuarios malintencionados o no autorizados que se encuentran fuera de la red virtual.
- **Protección contra las vulnerabilidades de seguridad de día cero.** Refuerzo en un solo lugar: Azure Bastion es un servicio PaaS totalmente administrado por la plataforma. Dado que se encuentra en el perímetro de la red virtual, no es necesario preocuparse por proteger cada una de las máquinas virtuales de la red virtual.

Configurar administración de actualizaciones

Azure Update Management es un servicio incluido como parte de su suscripción de Azure. Con Update Management, puede evaluar el estado de actualización en todo el entorno y administrar las actualizaciones de los servidores Windows Server y Linux desde una sola ubicación, tanto para los entornos locales como para los entornos de Azure.

Update Management está disponible sin costo adicional (solo paga por los datos de registro que almacena Azure Log Analytics) y puede habilitarlo fácilmente para máquinas virtuales locales y de Azure. Para probarlo, vaya a la pestaña **VM** en Azure y, a continuación, habilite Update Management para una o varias de las máquinas virtuales. También puede habilitar Update Management para VM directamente desde su cuenta de Azure Automation. Facilitar las actualizaciones es uno de los factores clave para mantener una buena higiene de seguridad.

Información general de Update Management de Azure

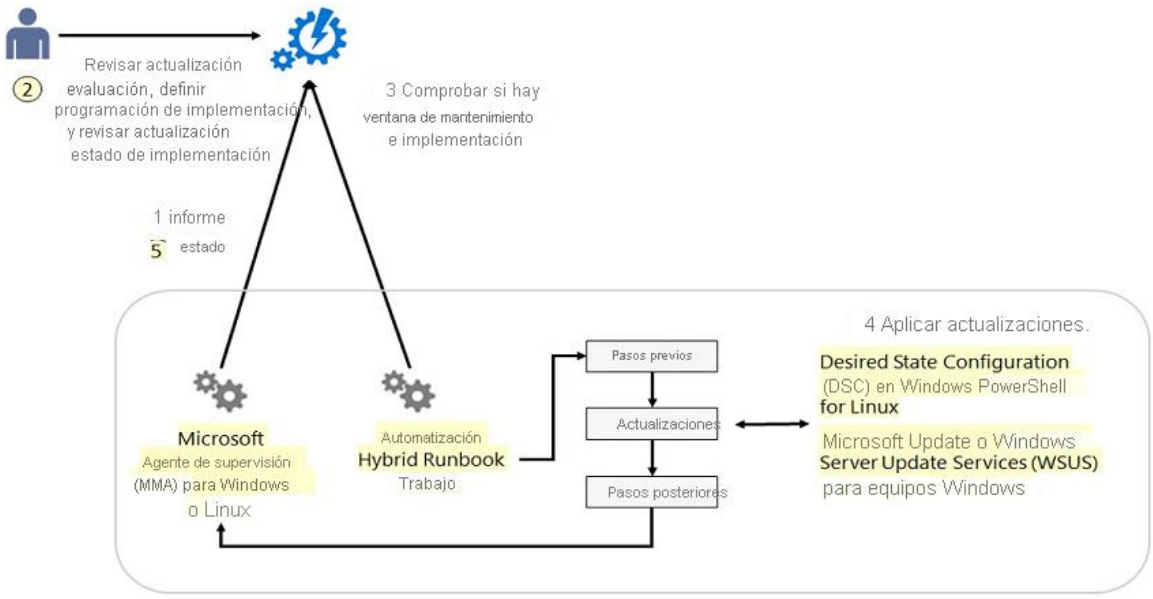
Los equipos que administra Update Management utilizan las siguientes configuraciones para realizar la evaluación y la implementación de las actualizaciones:

- Microsoft Monitoring Agent (MMA) para Windows o Linux
- Desired State Configuration (DSC) en Windows PowerShell para Linux
- Hybrid Runbook Worker en Azure Automation
- Microsoft Update o Windows Server Update Services (WSUS) para equipos Windows

Azure Automation usa runbooks para instalar actualizaciones. No puede ver estos runbooks, que no requieren ninguna configuración. Cuando se crea una implementación de

actualizaciones, esta crea una programación que inicia un runbook de actualización maestro a la hora especificada para los equipos incluidos. El runbook maestro inicia un runbook secundario en cada agente para instalar las actualizaciones necesarias.

El siguiente diagrama muestra una vista conceptual del comportamiento y un flujo de datos que refleja cómo la solución evalúa todos los equipos Windows Server y Linux conectados en un área de trabajo y les aplica actualizaciones de seguridad.



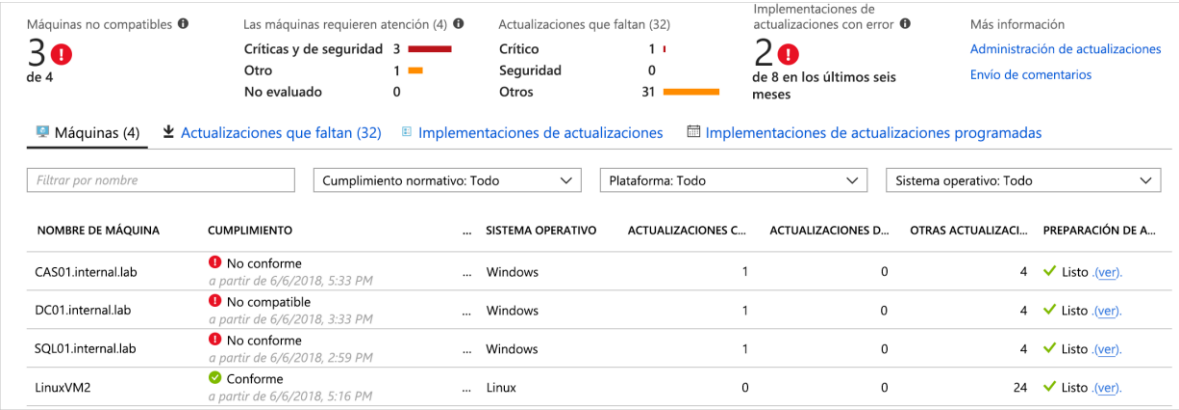
Administración de actualizaciones para varias máquinas

Puede usar la solución Update Management para administrar las actualizaciones y las revisiones de las máquinas Windows y Linux. Desde la cuenta de Azure Automation, puede:

- Incorporar máquinas virtuales
- Evaluar el estado de las actualizaciones disponibles
- Programar la instalación de las actualizaciones necesarias
- Revisar los resultados de la implementación para comprobar que se han aplicado correctamente actualizaciones a todas las máquinas virtuales para las cuales se ha habilitado Update Management

El agente de Log Analytics para Windows y Linux debe instalarse en las máquinas virtuales que se ejecutan en la red corporativa o en otro entorno en la nube con el fin de habilitarlos con Update Management.

Después de habilitar Update Management en las máquinas, puede ver información sobre ellas si selecciona **Equipos**. Puede ver información sobre el nombre de la máquina, el estado de cumplimiento, el entorno, el tipo de sistema operativo, las actualizaciones críticas y de seguridad instaladas, otras actualizaciones instaladas y la preparación del agente de actualización para los equipos.



Es posible que los equipos que no se hayan habilitado recientemente para Update Management no se hayan evaluado aún. En este caso, el estado de cumplimiento de esos equipos es **No evaluado**.

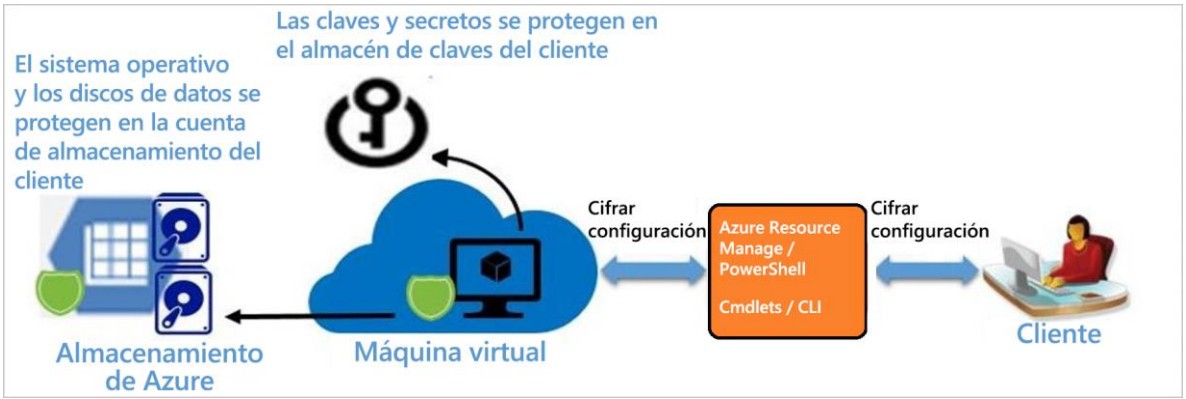
Inclusión de actualización

Azure Update Management proporciona la capacidad de implementar revisiones basadas en clasificaciones. Sin embargo, hay escenarios en los que puede que desee enumerar explícitamente el conjunto exacto de revisiones. Entre los escenarios comunes se incluye permitir revisiones específicas después de las pruebas de entorno controlado y los lanzamientos de revisiones de día cero.

Con las listas de inclusión de actualizaciones puede elegir exactamente qué revisiones quiere implementar en lugar de basarse en las clasificaciones de las revisiones.

Implementación del cifrado de disco

Azure Disk Encryption para VM de Windows ayuda a custodiar y proteger sus datos con el fin de satisfacer los compromisos de cumplimiento y seguridad de su organización. Usa la característica BitLocker de Windows para proporcionar cifrado de volumen al SO y los discos de datos de las máquinas virtuales (VM) de Azure y se integra con Azure Key Vault para ayudar a controlar y administrar las claves de cifrado de disco y los secretos.



Si usa Microsoft Defender for Cloud, se le avisará si tiene máquinas virtuales que no están cifradas. Estas alertas se muestran con gravedad alta y se recomienda cifrar estas máquinas virtuales.

Azure Disk Encryption es resistente a zona, de la misma manera que Virtual Machines.

VM y sistemas operativos compatibles

Máquinas virtuales admitidas

Las máquinas virtuales Windows están disponibles en una variedad de tamaños. Azure Disk Encryption es compatible con las máquinas virtuales de Gen1 y Gen2. Azure Disk Encryption también está disponible para las VM con almacenamiento Premium.

Azure Disk Encryption no está disponible en máquinas virtuales básicas o de la serie A ni en máquinas virtuales que tengan menos de 2 GB de memoria.

Sistemas operativos compatibles

- Cliente Windows: Windows 8 y versiones posteriores.
- Windows Server: Windows Server 2008 R2 y versiones posteriores.
- Sesión múltiple de Windows 10 Enterprise.

Requisitos de red

Para habilitar Azure Disk Encryption, las máquinas virtuales deben cumplir los siguientes requisitos de configuración de los puntos de conexión de red:

- Para que un token se conecte al almacén de claves, la máquina virtual Windows debe poder conectarse a un punto de conexión de Azure Active Directory, [login.microsoftonline.com].
- Para escribir las claves de cifrado en el almacén de claves, la máquina virtual Windows debe poder conectarse al punto de conexión del almacén de claves.
- La máquina virtual Windows debe poder conectarse al punto de conexión de Azure Storage que hospeda el repositorio de extensiones de Azure y la cuenta de Azure Storage que hospeda los archivos del VHD.

- Si su directiva de seguridad limita el acceso desde máquinas virtuales de Azure a Internet, puede resolver el URI anterior y configurar una regla concreta para permitir la conectividad de salida para las direcciones IP.

Requisitos de la directiva de grupo

Azure Disk Encryption usa el protector de claves externas de BitLocker para las máquinas virtuales Windows. Para las máquinas virtuales unidas en un dominio, no cree ninguna directiva de grupo que exija protectores de TPM.

La directiva de BitLocker en máquinas virtuales unidas a un dominio con una directiva de grupo personalizada debe incluir la configuración siguiente: Configurar el almacenamiento de usuarios de información de recuperación de BitLocker > Permitir clave de recuperación de 256 bits. Azure Disk Encryption presentará un error cuando la configuración de la directiva de grupo personalizada para BitLocker sea incompatible. En máquinas que no tengan la configuración de directiva correcta, puede que sea necesario aplicar la nueva directiva, forzar la nueva directiva a actualizarse (gpupdate.exe /force) y luego reiniciar.

Azure Disk Encryption producirá un error si la directiva de grupo de nivel de dominio bloquea el algoritmo AES-CBC, que BitLocker usa.

Requisitos de almacenamiento de la clave de cifrado

Azure Disk Encryption requiere Azure Key Vault para controlar y administrar las claves y los secretos de cifrado de discos. El almacén de claves y las máquinas virtuales deben residir en la misma región y suscripción de Azure.

Azure Disk Encryption para VM Linux

Azure Disk Encryption ayuda a custodiar y proteger sus datos con el fin de satisfacer los compromisos de cumplimiento y seguridad de su organización. Usa la característica DM-Crypt de Linux para proporcionar cifrado de volumen tanto a los discos de datos como a los del sistema operativo de máquinas virtuales (VM) de Azure y se integra con Azure Key Vault para ayudarlo a controlar y administrar las claves y los secretos del cifrado de disco.

Para las máquinas virtuales Windows, si usa Microsoft Defender for Cloud, se le avisará si tiene máquinas virtuales que no están cifradas. Estas alertas se muestran con gravedad alta y se recomienda cifrar estas máquinas virtuales.

VM y sistemas operativos compatibles

Máquinas virtuales admitidas

Las VM Linux están disponibles en una variedad de tamaños. Azure Disk Encryption es compatible con las máquinas virtuales de Gen1 y Gen2. Azure Disk Encryption también está disponible para las VM con almacenamiento Premium.

Nota: Azure Disk Encryption no está disponible en máquinas virtuales básicas o de la serie A ni en máquinas virtuales que no cumplan estos requisitos mínimos de memoria:

Máquina virtual

Requisito mínimo de memoria

VM de Linux cuando solo se cifran volúmenes de datos

2 GB

VM de Linux cuando se cifran volúmenes de datos y del SO, y donde el uso del sistema de archivos raíz (/) es 4 GB o menos

8 GB

VM de Linux cuando se cifran volúmenes de datos y del SO, y donde el uso del sistema de archivos raíz (/) es mayor que 4 GB

El uso del sistema de archivos raíz * 2. Por ejemplo, un uso de 16 GB del sistema de archivos raíz requiere al menos 32 GB de RAM

Una vez completado el proceso de cifrado de disco del sistema operativo en las máquinas virtuales de Linux, la VM se puede configurar para que se ejecute con menos memoria.

Azure Disk Encryption también está disponible para las VM con almacenamiento Premium. Azure Disk Encryption no está disponible en VM de segunda generación ni en las VM de la serie Lsv2.

Azure Disk Encryption requiere que los módulos dm-crypt y vfat estén presentes en el sistema. La eliminación o deshabilitación de vfat de la imagen predeterminada impedirá que el sistema lea el volumen de claves y obtenga la clave necesaria para desbloquear los discos en los siguientes reinicios. Los pasos de protección del sistema que eliminan el módulo vfat del sistema no son compatibles con Azure Disk Encryption

---