

Dispositivo de cuentas con privilegios

Seguridad para las soluciones que protegen las cuentas con privilegios

Beneficios

- Se instala fácilmente.
- Brinda protección frente a ataques externos basados en la red con firewall integrado.
- Elimina las inquietudes sobre la protección del hardware básico.
- Escala para satisfacer las necesidades futuras de rendimiento.
- Maximiza la disponibilidad con opciones de recuperación ante desastres y continuidad empresarial.
- Soporta opciones de hardware redundante.

Cuando su empresa implementa soluciones para administrar las credenciales de acceso, monitorear el acceso a activos de gran valor y aprovisionar acceso para programas, tareas y comandos específicos, también es esencial controlar el acceso a estas soluciones.

El dispositivo de cuentas con privilegios de One Identity ofrece la seguridad y la confianza que las empresas necesitan al implementar las soluciones de Privileged Password Manager (PPM) y Privileged Session Manager (PSM).

Como un dispositivo sin cliente y sin agente, diseñado específicamente para hospedar aplicaciones de PPM y PSM, el dispositivo de cuentas con privilegios se refuerza desde el primer momento con el fin de garantizar los más altos niveles de protección para los activos más importantes de la empresa.

Características

Acceso seguro basado en roles:

Ya que el dispositivo no cuenta con puerto o interfaz a nivel de consola, se puede acceder a él a través de una interfaz web segura basada en roles. De esta manera se proporciona protección contra ataques al host administrador y modificaciones del sistema operativo, la base de datos y otras modificaciones a nivel del sistema.

Firewall interno: Un firewall interno protege contra ataques externos basados en la red y proporciona capacidades adicionales de auditoría.

Cifrado de contraseñas

almacenadas: El cifrado de AES de 256 bits garantiza la protección de todas las contraseñas almacenadas.

Cifrado completo de disco

duro: El disco duro del dispositivo se cifra mediante BitLocker™ Drive Encryption.

Comunicación segura: Todas las conexiones del usuario se protegen mediante HTTPS/SSLv3 que usa el nivel de protocolo más alto, según la negociación del cliente. One Identity firma el certificado inicial y puede reemplazarse por un certificado específico del cliente. Las conexiones proxy del usuario se protegen a través de SSH. Las transmisiones de las sesiones de destino se realizan a través del protocolo nativo más seguro, en la mayoría de los casos será SSH. La comunicación programática (CLI/API) se protege a través de SSH2, mediante claves asimétricas de DSS para autenticación.

Seguridad de base de datos:

La comunicación entre la aplicación web basada en roles y la base de datos subyacente se protege mediante la prohibición del acceso directo a cualquier objeto o dato de la base de datos. Solo los procedimientos almacenados pueden convocarse desde la aplicación; no se permite SQL ad hoc.

Seguridad de la aplicación:

La separación de tareas (SoD) se aplica a través del control de acceso basado en roles (RBAC), que está integrado en la aplicación.

Hardware de dispositivo de cuentas con privilegios

Nombre del modelo	Dispositivo estándar	Dispositivo estándar
Procesador	Familia de procesadores E3-1220 Intel® Xeon®	Familia de procesadores E5-2600 Intel® Xeon®
Cantidad de procesadores	1	2
Cantidad de núcleos por procesador	Cuatro	Seis
Caché L2/L3	10 MB	10 MB
Chipset	Intel® C236	Intel® C610 series
DIMM	DDR4 R-DIMM	DDR4 R-DIMM
RAM	8 GB como mínimo	32 GB como mínimo
Plataformas de HD	Hot plug de 4 x 3,5	Hot plug de 4 x 3,5
Tipos de HD	SATA/SAS	Controladora integrada de SAS
Controladora de HD interna	Controladora RAID integrada de PERC H310	Controladora RAID integrada de PERC H710P, caché NV de 1 GB
Disco	2 X 500 GB	4 x 300 15.000 RPM GB SAS
Disponibilidad	Intercambio de memoria ECC HDD, PSU redundante, TPM	Intercambio directo HDD, PSU redundante, reflejo de memoria, TPM
Ranuras de E/S	2 x PCIe 3.0	2 x PCIe x16; media altura, longitud media
RAID	RAID 1 duplicado	RAID 10
NIC/LOM	2x GbE LOM	2x GbE LOM
DRAC	iDRAC8 Enterprise	iDRAC8 Enterprise
USB	2 frontal/2 trasero/2 interno	2 frontal/2 trasero/2 interno
Fuentes de alimentación/ detalles de alimentación	Redundante, 350 W, ajuste automático (100 V~240 V), compatible con ACPI	Redundante, 550 W, ajuste automático (100 V~240 V), cumple con ACPI
Ventiladores	3 no redundante, sin intercambio en caliente	4 no redundante, sin intercambio en caliente
Chasis	Rack de 1U	Rack de 1U
Dimensión	42,8 x 434,0 x 625,0 (mm) (sin panel) (1,68 x 17,08 x 24,6 in)	42,8 x 434,0 x 607,0 (mm) (sin auricular, sin panel) (1,68 x 17,08 x 23,9 in)
Peso	Máx. 30,42 lb (13,8 kg)	Máx.: 43,87 lb (19,9 kg)
Otras	El switch de intrusiones detecta cuando se abre la cubierta, hyper-threading (8 subprocesos), panel LCD de 128 x 120	El switch de intrusiones detecta cuando se abre la cubierta, multi-threading simultáneo, módulo LCD
Temperatura de funcionamiento	10 °C a 35 °C	10 °C a 35 °C
Certificaciones normativas	Clase A:	Clase A:
La información adicional de certificación por país está disponible previa solicitud.	Australia/N. Z. – AMCA o C-Tick Canadá– SCC, ICES Unión Europea – CE Alemania–TUV Estados Unidos – FCC, NRT	Australia/N. Z. – AMCA o C-Tick Canadá– SCC, ICES Unión Europea – CE Alemania–TUV Estados Unidos – FCC, NRT

En esta tabla se muestra la plataforma de hardware actual para cada configuración de dispositivo de cuentas con privilegios. Los componentes enumerados son los que se encuentran en las unidades que se envían al momento de la publicación de este documento, pero están sujetos a cambio sin previa notificación debido a obsolescencia, falta de disponibilidad o notificación de defectos de los componentes.

Acerca de One Identity

La familia de soluciones de administración de identidades y acceso (IAM) de One Identity ofrece IAM para el mundo real, incluidas las soluciones centradas en la empresa, modulares e integradas, además de listas para el futuro orientadas a la gestión de identidades,

la administración del acceso y la administración de privilegios.

Más información

Para obtener más información sobre Privileged Password Manager, visite oneidentity.com/privileged-password-manager.