

Privileged Session Manager

Emisión, control y grabación del acceso privilegiado

Beneficios

- Delega acceso privilegiado.
- Limita los trabajos y los comandos de Unix y Windows que pueden ejecutarse.
- Habilita el inicio de sesión automático.
- Graba, archiva y reproduce sesiones para las auditorías.

Privileged Session Manager es ideal para asegurar el acceso de:

- Proveedores remotos
- Asesores remotos
- Desarrolladores remotos
- Acceso privilegiado interno
- Acceso de desarrollador a los entornos de producción
- Acceso a llamadas de emergencia ante incendios

Otorgar acceso no controlado a sistemas valiosos al personal interno del área de TI, los administradores de sistemas, los contratistas y los proveedores de servicio puede ser la causa de problemas graves, como lo han demostrado los incidentes recientes tan publicitados. Sin embargo, para conseguir seguridad y cumplimiento verdaderos se necesita más que el control del acceso proporcionado a los usuarios privilegiados; también puede supervisar proactivamente qué hacen y tomar medidas cuando las actividades no son adecuadas.

Privileged Session Manager le permite otorgar acceso con privilegios, durante una sesión o período específico, a administradores, proveedores remotos y usuarios de alto riesgo, y ofrecer grabación y reproducción completas para fines de auditoría y cumplimiento. Se proporciona un único punto de control desde el que puede autorizar conexiones, limitar el acceso a recursos específicos, permitir que solo se ejecuten ciertos comandos, ver conexiones activas, grabar toda la actividad, alertar si las conexiones superan límites preestablecidos y cerrar conexiones. Privileged Session Manager es un componente crítico de los productos de administración de acceso con privilegios de One Identity, y se implementa en un dispositivo seguro y reforzado.

Características

Acceso controlado: Los usuarios autorizados pueden solicitar una sesión en recursos específicos o a través de cuentas administrativas determinadas, mediante una conexión de navegador web seguro. Cada usuario puede ver solo los recursos específicos para los cuales está autorizado a solicitar acceso. Puede configurar la conexión para el flujo de trabajo de autorización para aumentar aún más el control y lograr el cumplimiento.

Acceso a través de proxy: Privileged Session Manager transmite todas las sesiones a recursos de destino. Dado que los usuarios no tienen acceso directo a los recursos, la empresa está protegida contra virus, software malicioso (malware) y otros elementos peligrosos en el sistema del usuario. Privileged Session Manager puede transmitir y grabar Unix/Linux, Windows, AS/400, aplicaciones web, dispositivos de red, firewalls, enrutadores y más.

Control de comandos: Puede permitir que se ejecuten solo comandos específicos durante una sesión según el usuario que obtiene acceso al sistema o el sistema al cual se obtiene acceso. Además, puede restringir los comandos que el usuario puede ejecutar durante una sesión; si el usuario intenta ejecutar un comando prohibido, usted puede notificar automáticamente a una persona específica, terminar el comando, terminar el inicio de sesión o terminar toda la sesión.

Auditoría de sesión completa, registro y reproducción: Toda la actividad de la sesión, cada acción que tiene lugar en la pantalla, incluso los movimientos del mouse, los clics y las pulsaciones de teclas, se graba

y se pone a disposición para análisis forenses y revisión de cumplimiento mediante el uso de controles similares a los de DVR. Solo se graba la actividad real y las grabaciones se comprimen a una fracción del tamaño requerido por otras soluciones, para minimizar los requisitos de almacenamiento fuera de línea.

Reproducción sencilla: Los administradores pueden buscar eventos específicos a través de sesiones y agregar marcadores para regresar a un punto específico en esa sesión en una fecha posterior.

Dispositivo seguro: El dispositivo reforzado no tiene un puerto de consola o una interfaz a nivel de consola, y solo se puede obtener acceso a través de una interfaz web segura y basada en los roles. Esto ofrece protección contra ataques de administrador de host, así como también otras modificaciones a nivel del sistema, base de datos o sistema operativo. El dispositivo también posee un firewall interno que ofrece protección contra ataques externos basados en la red y proporciona capacidades adicionales de auditoría.

Flujo de trabajo sencillo: Los usuarios autorizados simplemente seleccionan el recurso o la cuenta a la que necesitan conectarse; en la lista se muestran solo los elementos para los cuales el usuario está autorizado a solicitar acceso. El solicitante especifica la duración prevista de la sesión, el motivo de la solicitud y, si es necesario, un número de ticket que se puede integrar en su sistema de tickets existente.

Inicio de sesión automático: Cuando se combina con Privileged Password Manager, el acceso de Privileged Session Manager puede configurarse para el inicio de sesión automático. El inicio

de sesión automático aumenta la seguridad y el cumplimiento, ya que nunca se exponen las credenciales de la cuenta al usuario.

El enfoque de One Identity hacia la administración de cuentas con privilegios

Los productos de One Identity incluyen el conjunto más completo de la industria de soluciones de administración de cuentas con privilegios, que se ajustan de manera óptima a las necesidades de cualquier empresa. Además de la poderosa funcionalidad de administración de sesiones de Privileged Session Manager, los productos de One Identity también ofrecen contraseña segura con privilegios, la cual puede ejecutarse en el mismo dispositivo reforzado seguro. Los productos de One Identity también pueden ofrecer soluciones específicas basadas en agentes para la delegación granular de la cuenta raíz de Unix y la cuenta de administrador de Active Directory, funciones adicionales para sudo de código abierto preparado para uso empresarial y registro de pulsaciones de tecla para las actividades raíz de Unix, todo perfectamente integrado en la solución de puente de Active Directory, líder de la industria.

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.

Obtenga más información en [OneIdentity.com](https://www.oneidentity.com).