centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1017

Procedimiento de Empleo Seguro
Idira (CyberArk) Privilege Cloud



Noviembre 2026

Edita:

centro criptológico nacional

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 7
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 10
5.1 INSTALACIÓN DEL CONECTOR 10
5.1.1 PASOS INICIALES PARA CONFIGURAR EL CONECTOR 10
5.1.2 PREPARANDO EL SERVIDOR 10
5.1.3 INSTALACIÓN DEL CONECTOR 11
5.1.4 INSTALACIÓN DEL PSM 13
5.1.5 HARDENIZACIÓN DEL CONECTOR 14
5.2 INSTALACIÓN PSM PARA SSH 17
5.2.1 CREAR USUARIO ADMINISTRATIVO PARA SERVIDOR PSMP 17
5.2.2 HABILITAR SELINUX 17
5.2.3 INSTALACIÓN DE PSMP 17
5.2.4 POST-INSTALACIÓN 19
6 FASE DE CONFIGURACIÓN 20
6.1 MODO DE OPERACIÓN SEGURO 20
6.2 AUTENTICACIÓN 21
6.3 ADMINISTRACIÓN DEL PRODUCTO 22
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 22
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 22
6.3.3 ROLES DE ADMINISTRACIÓN PRINCIPALES 24
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 25
6.5 GESTIÓN DE CERTIFICADOS 26
6.6 SERVIDORES DE AUTENTICACIÓN 26
6.7 SINCRONIZACIÓN 27
6.8 ACTUALIZACIONES 27
6.9 AUTO-CHEQUEOS 32
6.10 ALTA DISPONIBILIDAD 32
6.10.1 REGISTRO DE EVENTOS 32
6.10.2 ALTA DISPONIBILIDAD PSM 34
6.11 AUDITORÍA 35
6.11.1 REGISTRO DE EVENTOS 35
6.11.2 ALMACENAMIENTO LOCAL 35
6.11.3 ALMACENAMIENTO REMOTO 36
6.12 BACKUP 37
7 REFERENCIAS 38
8 ABREVIATURAS 40

ÍNDICE DE TABLAS

Tabla 1: Requisitos de Software 5
Tabla 2: Instalación PSM I 14
Tabla 3: Instalación PSM II 14
Tabla 4: Creación de GPO 16
Tabla 5: Actualización de GPO 30

ÍNDICE DE FIGURAS

Figura 1: Descarga de paquetes desde Connector Management 6
Figura 2: Descargando paquetes desde Idira Marketplace 7
Figura 3: Distribución de los diferentes componentes 9
Figura 4: Instalando el agente de gestión del conector 11
Figura 5: Instalando el agente de gestión del conector 12
Figura 6: Conectores instalados en el entorno 13
Figura 7: Agregar Componente PSM 13
Figura 8: Verificación del estado del PSM 14
Figura 9: Creación de nueva GPO 15
Figura 10: Verificación de los ajustes de GPO 16
Figura 11: Configurar política de contraseña en sistemas remotos gestionados 24
Figura 12: Creación de nueva GPO 29
Figura 13: Verificación de los ajustes de GPO 30
Figura 14: Actualización del conector 31
Figura 15: Monitorización de sesiones 35
Figura 16: Master Policy 36

1 INTRODUCCIÓN

Idira PAM es una solución de **Gestión de Acceso Privilegiado (PAM)** que permite proteger, controlar y monitorizar el acceso privilegiado a infraestructuras locales, en la nube e híbridas.

El presente documento hace referencia a la plataforma de seguridad de identidades operada históricamente bajo la marca "CyberArk". Tras la reciente adquisición de la compañía por parte de **Palo Alto Networks**, la plataforma y sus servicios asociados están en proceso de transición hacia su nueva denominación comercial: **"Idira"**.

Permite a las organizaciones proteger, aprovisionar, administrar, controlar y monitorear todas las actividades asociadas con las identidades privilegiadas, en todo su ciclo de vida, tales como:

- Administrador en un servidor Windows.
- *Root* en un servidor UNIX.
- *Cisco Enable* en un dispositivo Cisco.
- Contraseñas embebidas en aplicaciones y *scripts*.

Además, al controlar la actividad de las cuentas privilegiadas, puede realizar la identificación de actividades sospechosas y responder ante posibles amenazas. Otras características del producto son:

- Asegurar y controlar de forma centralizada el acceso a las credenciales privilegiadas basadas en políticas de seguridad definidas.
- Aislar y asegurar sesiones de usuarios privilegiados. Las capacidades de monitorización y grabación permiten a los equipos de seguridad ver sesiones privilegiadas en tiempo real, suspender automáticamente y terminar remotamente las sesiones sospechosas.
- Detectar, alertar y responder a actividades privilegiadas anómalas.
- Controlar el acceso de privilegios mínimos para UNIX y Windows. La solución permite a los usuarios con privilegios ejecutar comandos administrativos autorizados desde sus sesiones nativas y limitar los privilegios de raíz innecesarios.
- Proteger los controladores de dominio de Windows.

2 OBJETO Y ALCANCE

Esta guía recoge el procedimiento de empleo seguro de los diferentes componentes pertenecientes a **Idira PAM**. Esta guía no tiene la intención de explicar de forma exhaustiva los detalles de la propia configuración del entorno. Se centra en los parámetros de seguridad recomendados.

A continuación, se indica el *software* mínimo necesario para desplegar cada uno de los componentes del producto:

Componente	Requisitos
Conector	• *Windows Server 2019, Windows Server 2022 Windows Server 2025.* • *.NET Framework 4.8* • *.NET Runtime 8.0.16 or later.* • *Windows Remote Management with WinRMListener and PSRemoting functionality.* • *Remote Desktop Services Session Host.* • Opcionalmente, instalar *Microsoft Remote Desktop Services Gateway*.
PSMP	• *Red Hat Enterprise Linux*, versión *8.X o 9.X.* • *Se puede usar Rocky Linux 8.x* • *SUSE Linux Enterprise Server,* versión *12 y 15*

Tabla 1: Requisitos de Software

Las versiones de los componentes *software* listados en la tabla anterior deben disponer de soporte de seguridad por parte del fabricante y estar actualizados.

Para mayor detalle de los requisitos de cada componente, se recomienda ver la documentación de la solución [REF1].

El producto **Idira PAM** ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF16].

3 ORGANIZACIÓN DEL DOCUMENTO

El presente documento se divide en los siguientes apartados:

- **Apartado 4**. En este apartado se recogen **aspectos y recomendaciones** a considerar, antes de proceder a la instalación del producto.
- **Apartado 5**. En este apartado se recogen recomendaciones a tener en cuenta durante la **fase de instalación** del producto.
- **Apartado 6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la **fase de configuración** del producto, para lograr una configuración segura.
- **Apartado 7**. Referencias utilizadas en el presente documento.
- **Apartado 8**. En este apartado se hace referencia a las diferentes nomenclaturas utilizadas.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Para la implementación de los componentes locales del conector de Idira Privilege Cloud, se dispone de dos metodologías oficiales de descarga y despliegue. La elección entre un método y otro dependerá de la arquitectura del entorno y del modelo de gestión adoptado por la organización:

a) Método 1: Despliegue Automatizado desde la Plataforma (*Connector Management*)

Este método consiste en una gestión centralizada directamente desde el *tenant* del cliente, accediendo a la sección de **Setup > Deployment > Connector Management**. Desde esta interfaz, la plataforma genera un script de orquestación ligero (PowerShell) que se ejecuta en el servidor local de destino. Este script instala un agente de gestión que se comunica de forma segura con la nube para automatizar la descarga, instalación y posterior actualización remota de los componentes del conector, reduciendo significativamente la intervención manual.



Figura 1: Descarga de paquetes desde Connector Management

b) Método 2: Descarga Manual desde el Portal Corporativo (*Idira Marketplace*)

Este es el método tradicional y el canal de contingencia para arquitecturas estándar. Requiere el acceso autenticado de un usuario con credenciales autorizadas (*S-User*) al portal oficial de **Idira Marketplace** [REF2]. A través de este repositorio, el administrador descarga de forma manual los paquetes de software binarios correspondientes a la versión del conector requerida, incluyendo los ejecutables del sistema, las políticas de hardenización (*GPO Hardening*) y las herramientas de verificación de prerrequisitos, para su posterior transferencia y ejecución local en los servidores de la infraestructura.

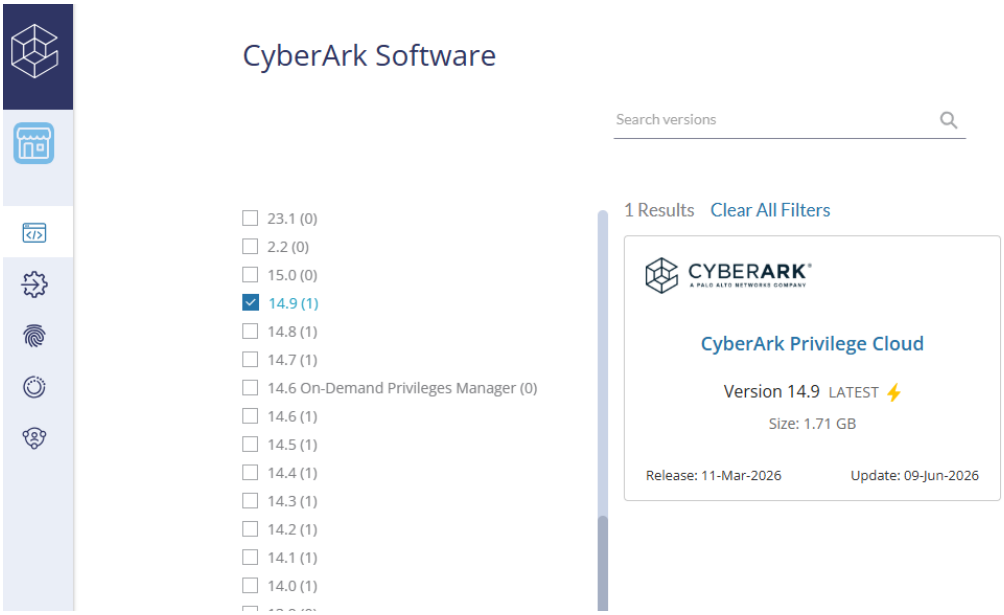


Figura 2: Descargando paquetes desde Idira Marketplace

4.2 ENTORNO DE INSTALACIÓN SEGURO

Los componentes del producto deben instalarse en un entorno en el que el personal técnico encargado disponga de autorización para la configuración, despliegue y mantenimiento del producto. Además, se requiere de un control de acceso físico para limitar el personal con acceso al producto.

4.3 REGISTRO Y LICENCIAS

El licenciamiento de la solución Idira Privilege Cloud se gestiona bajo un modelo de provisión automática inherente a su arquitectura SaaS. Por tanto, no se requiere ninguna acción manual previa ni la instalación de ficheros de licencia por parte de la organización antes de su despliegue y puesta en marcha.

Desde la perspectiva del control de acceso y la seguridad, este modelo de licenciamiento actúa como un mecanismo de control técnico. Las licencias provisionadas desde el origen determinan de manera estricta el número máximo de usuarios (identidades) autorizados que tendrán acceso a la plataforma de gestión de la solución. Asimismo, el licenciamiento define y restringe de forma granular los perfiles, capacidades y las interfaces específicas a las que cada identidad puede acceder. Esto garantiza la aplicación del principio de mínimo privilegio y asegura que únicamente el personal explícitamente licenciado y autorizado pueda interactuar con la plataforma y los activos críticos que esta protege.

4.4 CONSIDERACIONES PREVIAS

La plataforma central de Idira Privilege Cloud se ofrece como servicio (SaaS), por lo que la alta disponibilidad, redundancia y recuperación ante desastres (DR) del núcleo de la solución (Vault y portal web) son gestionadas y garantizadas nativamente por el fabricante. Sin embargo, para evitar interrupciones en el servicio, **se recomienda implementar una arquitectura de alta disponibilidad para los componentes que se**

despliegan en la red de la organización. Esto implica, por ejemplo, desplegar múltiples servidores de gestión de sesiones balanceados para evitar puntos únicos de fallo en la conexión a los activos locales.

Privilege Cloud utiliza los servicios compartidos de identidad de la plataforma de Idira para el acceso de los administradores y usuarios. Como consideración previa, **se recomienda planificar la integración con el proveedor de identidades (IdP) corporativo** mediante protocolos estándar (como SAML) o instalar el Conector de Identidad para la autenticación delegada contra el Directorio Activo/LDAP local. Asimismo, es requisito indispensable prever la aplicación de políticas de Autenticación Multifactor (MFA) para asegurar el acceso al portal.

Aunque los certificados públicos del portal SaaS son gestionados íntegramente por Idira, para una configuración segura del entorno de operación local **se deberá contar con un servidor de certificación (CA) en la organización**. Esta entidad certificadora se encargará de emitir y confiar en los certificados internos necesarios para los componentes locales, garantizando que las sesiones y las comunicaciones dentro de la red corporativa estén debidamente cifradas.

Como requisito crítico previo a la instalación, **la organización debe configurar sus firewalls y/o proxys web para permitir el tráfico saliente seguro** (habitualmente HTTPS/puerto 443) desde las redes donde se alojen los conectores locales hacia las URLs y direcciones IP específicas del *tenant* en la nube proporcionado por Idira.

Para cada uno de los componentes de la solución, se indicarán sus respectivas consideraciones previas en la fase de instalación.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El producto está formado por diferentes componentes, los cuales se usan para tareas específicas y proporcionan diferentes funcionalidades. Estos componentes se despliegan bajo una arquitectura dividida en dos tramos principales y se distribuyen de la siguiente manera:

1. **Entorno de Cliente.** Este entorno aloja el dominio del cliente y las máquinas locales, configuradas siguiendo las directrices de seguridad. Contiene los siguientes componentes locales (*on-premises*):

- **Conector:** Se encarga de ejecutar el módulo **Privileged Session Manager (PSM**). Su objetivo es asegurar, controlar y monitorizar el acceso a dispositivos de red, permitiendo a los usuarios iniciar sesiones en máquinas remotas a través de un proxy seguro. Las sesiones se aíslan por completo y las credenciales permanecen ocultas para el usuario final.
- **PSM for SSH:** Componente dedicado a establecer sesiones privilegiadas de manera segura específicamente con máquinas de destino Unix.

2. **Back-end de la solución.** Alojado en la nube, este tramo contiene el almacenamiento central de credenciales, los mecanismos de seguridad, las aplicaciones de usuario y los servicios principales de la infraestructura:

- **Portal de Privilege Cloud:** Es la interfaz de usuario principal. Permite a los administradores configurar y gestionar los Safes (cajas fuertes) y cuentas, conectar con los objetivos organizacionales y monitorizar las sesiones.

- **Vault:** Es la bóveda central de almacenamiento. Permite a la organización asegurar, gestionar, rotar automáticamente y registrar cualquier actividad asociada con contraseñas privilegiadas y claves SSH.
- **Administración de Identidad:** Solución IAM (Gestión de Acceso a Identidades) que asegura entornos DevOps y aplica privilegios. Permite integrar Proveedores de Identidad (IdP) externos como LDAP, RADIUS o directorios Cloud, proporcionando una interfaz para asignar roles y permisos.
- **Servicio de Rotación de Secretos (conocido antes como CPM):** Gestiona las políticas de contraseñas, configurando las reglas de rotación y reconciliación para las distintas plataformas y cuentas.
- **Servicio de Descubrimiento:** Escanea activamente la infraestructura para identificar nuevas cuentas de cliente y aplica reglas predefinidas para incorporarlas automáticamente al sistema.
- **Portal de Gestión de Conectores:** Interfaz en la nube que mantiene el registro de versiones y el estado de salud de los componentes, comunicándose directamente con el Agente instalado en el entorno del cliente.

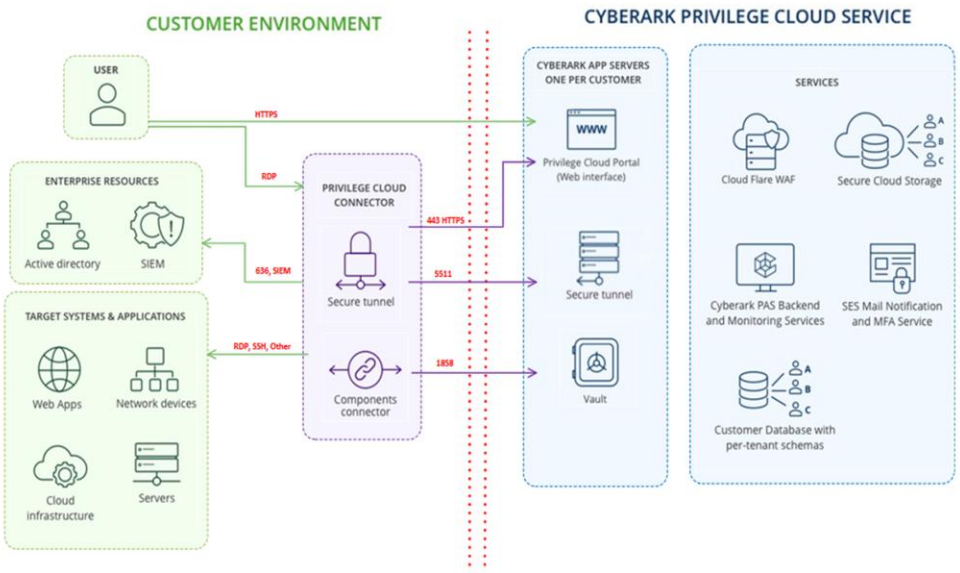


Figura 3: Distribución de los diferentes componentes

5 FASE DE INSTALACIÓN

5.1 INSTALACIÓN DEL CONECTOR

5.1.1 PASOS INICIALES PARA CONFIGURAR EL CONECTOR

Antes de iniciar el despliegue, es fundamental asegurar que se cumplen los siguientes requisitos en orden:

1. **Configurar la lista de IPs permitidas (Allowlist):**
   - Se deben configurar en Privilege Cloud las direcciones IP públicas (no rangos privados) del entorno para permitir la comunicación segura de salida hacia el *backend* de Idira.
2. **Preparar las credenciales necesarias:**
   - Credenciales de administrador de Privilege Cloud.
   - La contraseña del usuario instalador (Installeruser).
   - Un usuario Administrador Local del servidor con derechos completos (debe ser un usuario de dominio si la implementación es dentro de un dominio).
3. **Certificados para PSM (LDAPs):**
   - El certificado de la Autoridad Certificadora (CA) que firmó el certificado utilizado para LDAPs debe existir en el almacén de certificados de Windows del servidor del Conector.
4. **Permisos de Identity Administration:**
   - El usuario administrador local debe tener asignado un rol en *Identity Administration* que incluya permisos para ejecutar el servicio de *Connector Management* (ej. rol de System Administrator o Connector Management Admin).
5. **Reglas de Firewall (Tráfico de salida):**
   - Es necesario que el firewall permita los puertos y el tráfico de red de salida necesarios según tu región para descargar el agente de gestión.
6. **Restricciones del servidor y entorno:**
   - **El nombre del servidor (Hostname)** no podrá ser modificado durante ni después del despliegue debido a limitaciones de Microsoft.
7. **Fundamentos de Seguridad**. Se deben revisar las recomendaciones de seguridad que se pueden encontrar en [REF3].

5.1.2 PREPARANDO EL SERVIDOR

Aunque Idira Privilege Cloud es una solución de servicio en la nube, se requiere desplegar un componente conector en el entorno del cliente que actúe de proxy. Este elemento es fundamental para permitir la comunicación, el aislamiento de sesiones y la gestión de credenciales entre la plataforma en la nube y los sistemas objetivo locales.

1. **Descarga y extrae el script de comprobación de prerrequisitos de Connector Management:**
   - Desde el área de *Idira Integrations and Tools*, descarga el paquete *Privilege Cloud Tools* (Herramientas de Privilege Cloud), incluyendo todos los archivos disponibles, y guarda el paquete en una carpeta dedicada, comúnmente llamada *Privilege Cloud Tools*.

- En *Privilege Cloud Tools* > *Connector Management Prerequisites*, extrae el archivo ConnectorCheckPrerequisites_PrivilegeCloud.zip.
  Se extraerán los siguientes archivos:
  - CM Readme.txt
  - ConnectorCheckPrerequisites_PrivilegeCloud.ps1
  - Carpeta VaultOperationsTester

2. **Copia los paquetes de Unified GPO Hardening al servidor de dominio y extrae los paquetes zip.**
3. **Deshabilita el agente antivirus si está instalado en tu servidor.**
4. **Chequear pre-requisitos.** Utilizando los archivos descargados en el paso 1, ejecuta el siguiente comando de PowerShell con un usuario Administrador Local. Esta comprobación de requisitos mostrará una lista de los elementos evaluados, junto con una indicación de si cada chequeo fue exitoso o falló.
   - Para instalaciones dentro del dominio:
   .\ConnectorCheckPrerequisites_PrivilegeCloud.ps1

   - Para instalaciones fuera del dominio:
   .\ConnectorCheckPrerequisites_PrivilegeCloud.ps1 -OutOfDomain

5.1.3 INSTALACIÓN DEL CONECTOR

En Conectores del Sistema (**System Connectors**), haz clic en Agregar un conector (**Add a connector**). En el asistente de Agregar conector > pestaña Definir detalles de instalación (**Define installation details**), define los siguientes detalles para el Agente de Gestión (**Management Agent**) en el servidor destino:

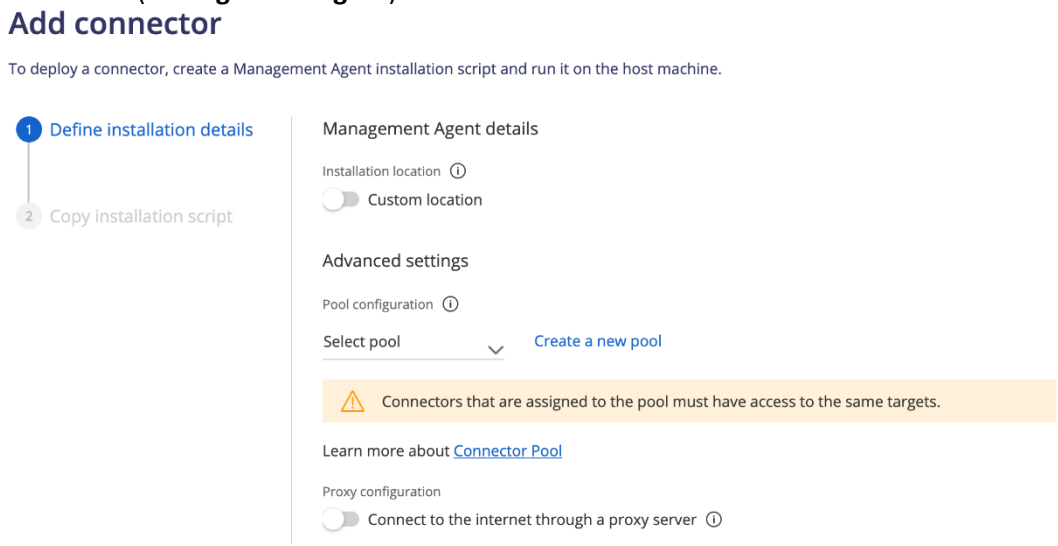


Figura 4: Instalando el agente de gestión del conector

Ubicación de instalación: Define la ubicación de instalación predeterminada y personalizada en la máquina anfitriona.

- **Ubicación predeterminada:** Esta es la ubicación de instalación por defecto en la máquina anfitriona. El Agente de Gestión se instala por defecto en C:\Program

Files. Si tu carpeta \Program Files está ubicada en cualquier otra unidad, se instalará allí.
    - El agente se instala en una subcarpeta \CyberArk\Management Agent.
    - El nombre de la carpeta debe estar en inglés.
    - En el campo de la ruta de instalación (*Installation path*), ingresa la ruta completa en inglés, incluyendo la unidad y la ruta de la carpeta, por ejemplo, D:\Program.
- **Ubicación personalizada:** El Agente de Gestión se instala por defecto en C:\Program Files. Si tu carpeta \Program Files está ubicada en cualquier otra unidad, se instalará allí.
    - Opcionalmente, ingresa una ruta completa hacia una carpeta de instalación alternativa.
    - El agente se instala en una subcarpeta \CyberArk\Management Agent.
    - El nombre de la carpeta debe estar en inglés.
    - El Agente de Gestión se instala en la ubicación seleccionada, en la subcarpeta \CyberArk\Management Agent.

Configuración de grupo (*Pool configuration*) En la sección de configuraciones avanzadas (*Advanced settings*), necesitas asignar el conector a un grupo de Conectores (*Connector pool*). Esto permite la alta disponibilidad para los componentes que soportan esta opción y están asignados a los mismos objetivos de red. *Esta opción estará disponible en breve. Mantén la asignación del grupo predeterminada.*

Configuración de Proxy Configura el conector para que se ejecute en una máquina que esté configurada para conectarse a Internet a través de un proxy específico.

Revisa los ajustes seleccionados y copia el script para instalar el agente en el servidor final. Este script estará disponible durante 5 minutos.

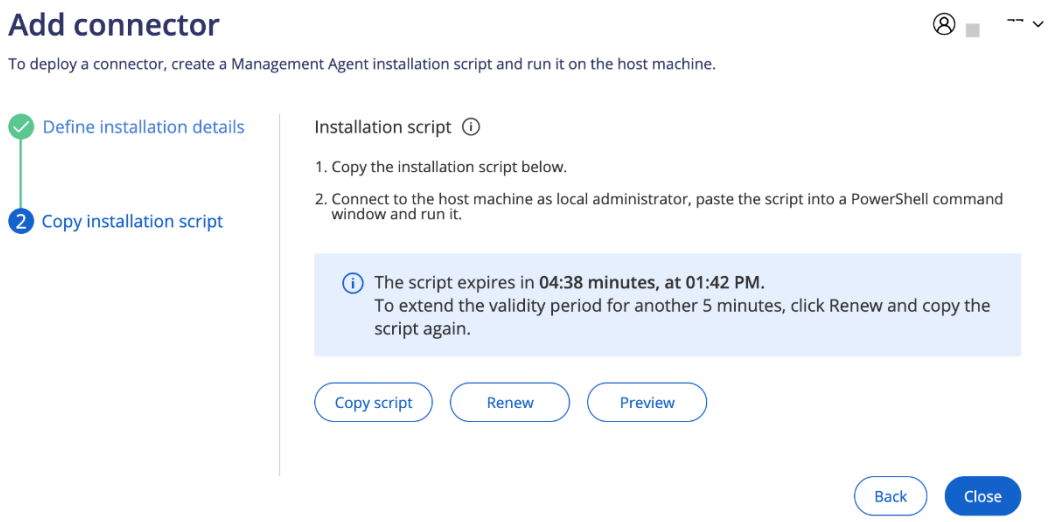


Figura 5: Instalando el agente de gestión del conector

En la instancia de Windows que estás utilizando como servidor del conector, copia el script de instalación en una ventana de comandos de PowerShell y ejecútalo.

En el servicio de *Connector Management*, haz clic en **Conectores**. La lista de conectores muestra todos los conectores del sistema y sus detalles. Haz clic en un filtro para mostrar una lista reducida de los conectores requeridos.

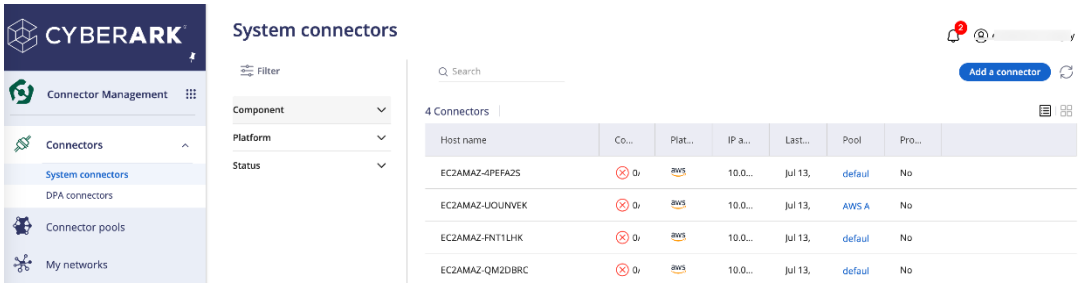


Figura 6: Conectores instalados en el entorno

Puedes filtrar la lista de conectores basándote en las características principales. En la lista de conectores, haz clic en el conector recién agregado. Verifica que el Agente de Gestión esté instalado.

5.1.4 INSTALACIÓN DEL PSM

En el servicio de *Connector Management*, selecciona la fila del conector donde deseas agregar el componente PSM, y desde el menú de opciones adicionales haz clic en **Agregar componente**.

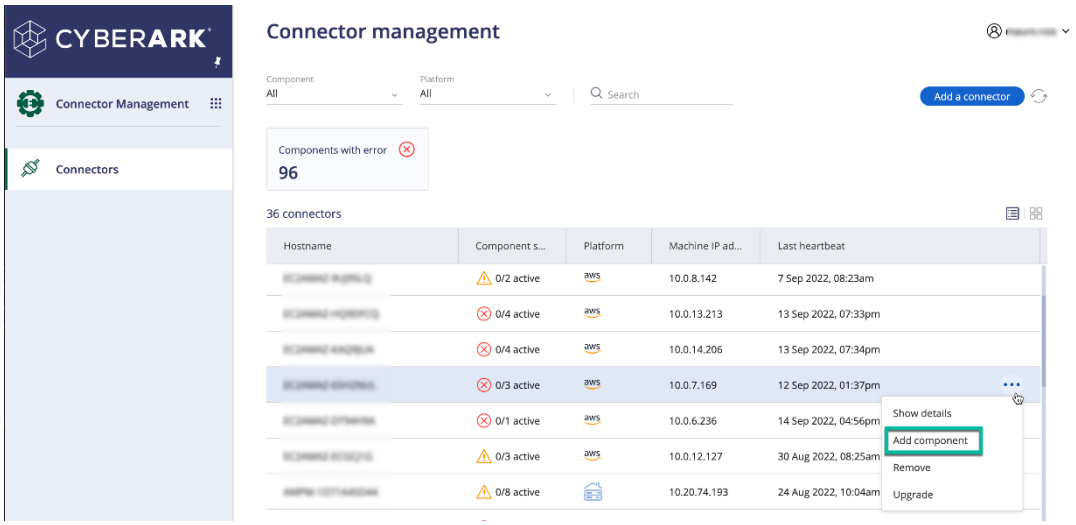


Figura 7: Agregar Componente PSM

Selecciona PSM y continúa con la instalación. Es necesario completar los siguientes detalles:

CAMPO	DESCRIPCIÓN
Modo de Instalación	Selecciona modo de Producción
Installeruser login	El usuario utilizado para la instalación de componentes locales (*on-prem*). Ingresa el nombre de usuario instalador (installeruser@<sufijo>) que configuraste en *Identity Administration* > *Users* > *Service Users*.
Installeruser login password	Ingresa la contraseña que configuraste para el usuario instalador (*installeruser*) de *Identity Administration*. Para más detalles, consulta [REF4].
Vault FQDN en el backend de Privilege Cloud	La dirección FQDN del Vault se ingresa automáticamente. Mantén la dirección FQDN del Vault o ingresa la dirección IP específica del Vault.

Tabla 2: Instalación PSM I

Una vez completados estos datos, es necesario completar los siguientes relacionados con la instalación de PSM:

CAMPO	DESCRIPCIÓN
Usuario Local	Para un entorno en dominio, ingresa **el Dominio, Nombre de usuario y Contraseña**. Asegúrate de que el usuario tenga derechos administrativos en el servidor.
Partición de instalación (opcional)	Elige una partición lógica para la instalación del PSM. Si no eliges una partición, el PSM se instalará en la unidad C

Tabla 3: Instalación PSM II

Haz clic en Siguiente e Instalar. Es necesario reiniciar la máquina donde está instalado el PSM.
En la página de Connector Management, verifica el estado de los componentes.

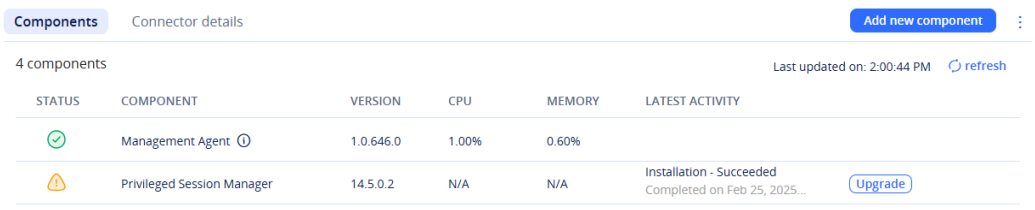


Figura 8: Verificación del estado del PSM

5.1.5 HARDENIZACIÓN DEL CONECTOR

Cuando el Conector se despliega en un servidor en dominio, el procedimiento automático de *hardening* se basa en un GPO (Objeto de Directiva de Grupo) predefinido, el cual establece la política de seguridad.

Consideraciones:

- **OU dedicada en el *Directorio Activo.*** Para asegurar que el hardenizado por GPO se aplique a todos los servidores del Conector en el directorio activo y no afecte a otros servidores, asegúrate de que todos estén ubicados bajo una unidad organizativa (OU) dedicada en el directorio activo.
- **Archivo GPO.** El hardenizado por GPO del servidor del Conector se basa en un archivo GPO unificado.

Para aplicar el GPO de hardenización:

1. Descarga el archivo GPO de hardenización unificado de PSM de Privilege Cloud correspondiente a tu versión, tal como se describe en 5.1.2 PREPARANDO EL SERVIDOR.
2. Importa el archivo GPO a tu dominio de *Active Directory*.
   a. Abre la Consola de administración de directivas de grupo (GPMC.msc).
   b. Crea un GPO: Expande **Administración de directivas de grupo** (*Group Policy Management*) > <tuDominio>, luego haz clic derecho en **Objetos de directiva de grupo** y selecciona **Nuevo**. Aparecerá la ventana de Nuevo GPO.

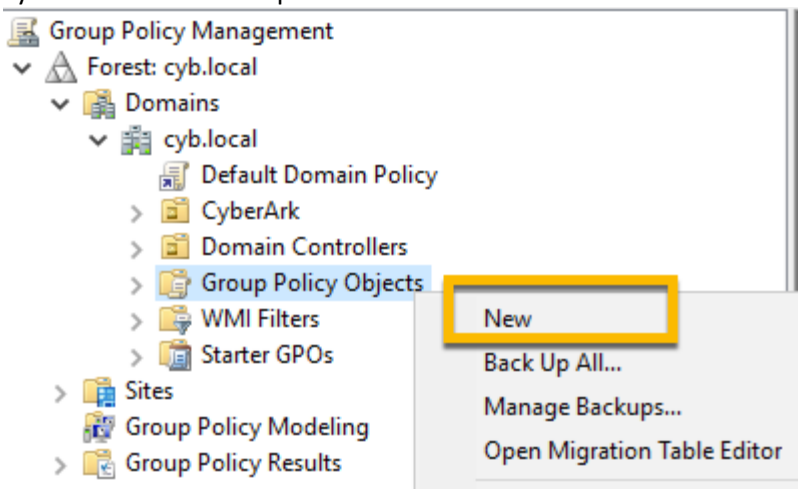


Figura 9: Creación de nueva GPO

   c. En el campo Nombre, especifica un nombre para el GPO Unificado que indique el propósito y la versión actual (por ejemplo, *Unified Hardening vN.N*), y haz clic en Aceptar.
   d. En la lista de Objetos de directiva de grupo, haz clic derecho en el nuevo GPO de hardenización y selecciona Importar configuración.
   e. En la ventana de bienvenida del Asistente para importar configuración, haz clic en Siguiente y define lo siguiente:

CAMPO	DESCRIPCIÓN
Ventana de la copia de seguridad de GPO	Haz clic en Siguiente.
Ubicación de la copia de seguridad	Haz clic en Examinar y selecciona la ubicación donde guardaste la configuración del GPO de hardenización de la versión, por ejemplo, *Privilege Cloud Connector Unified Hardening GPO*, y haz clic en Aceptar.
Ventana de GPO de Origen	Haz clic en Siguiente.
Ventana de Examen de copia de seguridad	Haz clic en Siguiente.
Ventana de Finalización del asistente para importar configuración	Haz clic en Finalizar. La ventana de Importación aparecerá indicando el progreso de la importación del GPO.

Tabla 4: Creación de GPO

Cuando el proceso de importación del GPO haya finalizado, haz clic en Aceptar. Después de la importación, selecciona el GPO y en la pestaña Configuración verifica que los ajustes se hayan importado correctamente.

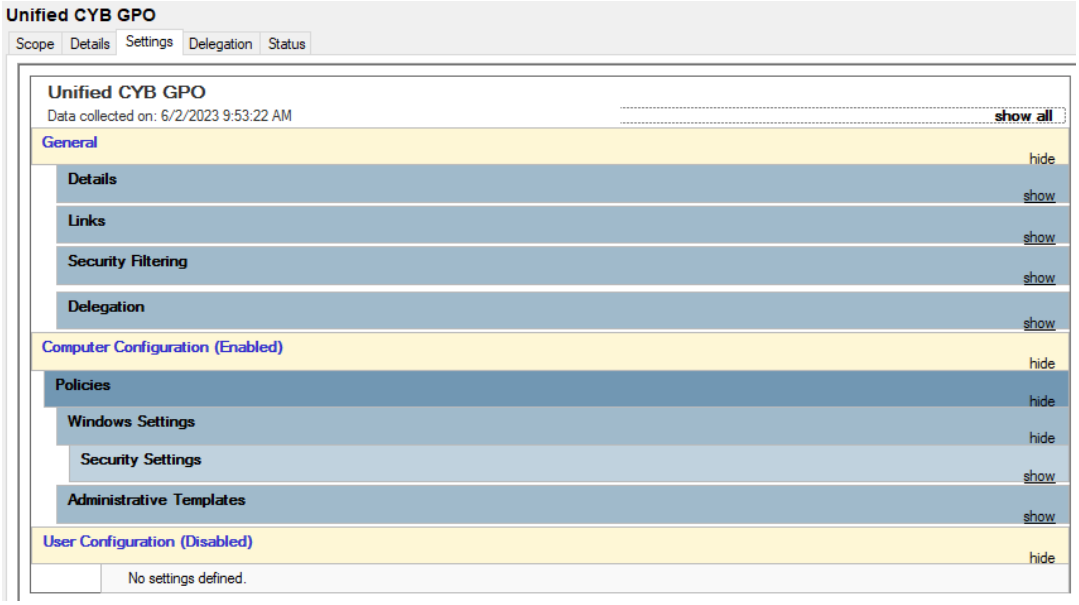


Figura 10: Verificación de los ajustes de GPO

Vincula el archivo GPO a la unidad organizativa (OU) dedicada de Idira que contiene los servidores de Idira.

a. Asegúrate de que todos los servidores del Conector estén ubicados bajo la OU dedicada, para que el GPO no afecte a ningún otro servidor.
b. En la Consola de administración de directivas de grupo, haz clic derecho en la OU y luego selecciona **Vincular un GPO existente**.
c. Selecciona el GPO de Endurecimiento Unificado y haz clic en Aceptar. La política del GPO de Endurecimiento Unificado aparecerá en la pestaña de Objetos de directiva de grupo vinculados.

Reinicia la máquina para que aplique el GPO actualizado.

5.2 INSTALACIÓN PSM PARA SSH

En esta sección se indican los pasos para la instalación del componente PSM para SSH (PSMP). PSMP crea un servidor proxy que permite a los usuarios conectarse desde su puesto de trabajo, con un cliente SSH, directamente a los dispositivos de red o servidores *NIX.

5.2.1 CREAR USUARIO ADMINISTRATIVO PARA SERVIDOR PSMP

Los usuarios administrativos Vault pueden conectarse a la máquina PSMP para la realización de tareas de gestión en la propia máquina, sin ser reenviado a una máquina de destino. Además del usuario root, PSMP identifica a los siguientes usuarios como usuarios administrativos cuando estos se conectan al servidor:

- *proxymng*
- *proxymng<número>*
- Usuarios especificados en el parámetro *PSMP_MaintenanceUsers* del fichero configuración *sshd_config.*

Se recomienda crear un usuario nominal, diferente de root, para que se pueda acceder a la máquina PSMP para gestionarla.

Es importante tener en cuenta que, como parte del proceso de hardening, una vez instalado PSMP, el usuario root no podrá autenticarse de manera remota en el servidor PSMP. Por lo que, si no se crea un usuario administrativo para realizar las tareas de gestión del PSMP, solo se podrá acceder mediante consola o a través del root con una clave SSH.

5.2.2 HABILITAR SELINUX

Antes de realizar la instalación del *software*, es recomendable habilitar *SELinux*. De esta manera, el proceso de instalación solo se encarga de habilitar las opciones de configuración necesarias para que el *software* funcione con *SELinux* habilitado. Para habilitar esta característica, se debe consultar la documentación del fabricante para cada versión de sistema operativo Linux:

- Para instalar correctamente el PSM for SSH SELinux policy en versiones principales de Red Hat y Rocky posteriores a la 7, debes instalar el paquete policycoreutils-python-utils utilizando el siguiente comando:

  yum install -y policycoreutils-python-utils

5.2.3 INSTALACIÓN DE PSMP

Al igual que con los componentes anteriores, se deberá referir al apartado 4.1 Entrega segura del producto para realizar la descarga del *software* necesario, y verificar su integridad. Recordad que PSMP se instalará sobre una máquina con sistema operativo Linux.

Se continúa la instalación con los siguientes pasos:

1. En la máquina PSMP se deberá crear un nuevo directorio donde se copiarán los archivos de instalación (paquete de instalación *Privileged Session Manager SSH Proxy*).
2. Se deberán crear los archivos de credenciales necesarios para la instalación siguiendo los siguientes pasos:
    - Ejecutar el comando *chmod 755 CreateCredFile* para dar permisos de ejecución sobre el fichero.
    - Ejecutar el comando *./CreateCredFile user.cred* para ejecutar el programa.
    - Rellenar con la información requerida.
3. Crear el archivo de parámetros de PSMP con los siguientes pasos:
    - Mover el archivo *psmpparms.sample* al directorio */var/tmp* y se renombra a *psmpparms*.
    - Abrir dicho fichero, y especificar los siguientes parámetros:
        i. "*InstallationFolder*" debe tener como valor la ruta a la carpeta PSMP que contiene el archivo *vault.ini*.
        ii. "*InstallCyberArkSSHD=Integrated*". Indica si el instalador de PSMP instala o no el servicio Idira SSHD, o si este está integrado con el servicio SSHD original.
        iii. "*Hardening=Yes*". Se pone a *yes* si es necesario aplicar configuraciones de *hardening* del S.O.
        iv. "*AcceptCyberArkEULA=Yes*". Para seguir con la instalación, se deberán aceptar los términos de licencia con el valor *yes*.
4. Se deberán realizar los siguientes cambios en el archivo *vault.ini*:
    - Poner en "*Address=*" la dirección IP del *Vault*.
    - Añadir "*TLSPort=443*" para las comunicaciones seguras con otros componentes.
    - Poner un puerto que no esté usado en "*Port*", como por ejemplo 1859.
5. Adicionalmente, se recomienda configurar un certificado en el lado de cliente utilizado para autenticación entre los dispositivos. Se deberá generar un certificado de cliente tal como se describe en la sección 6.5 Certificados Personales Para Autenticación de Cliente. Este certificado es opcional ya que no es necesario para que la conexión entre componentes se realice de manera correcta.
6. Si el certificado de cliente se ha creado, habrá que realizar los siguientes cambios:
    - Crear una variable de entorno que se llame ENV_PASSPHRASE y el valor deberá corresponder a la contraseña del certificado. Esta contraseña se utiliza para hacer uso de la clave privada de TLS y deberá ser introducida antes de iniciar los servicios de Idira.
    - Se deberá añadir lo siguiente en el archivo *vault.ini*:

1. En *ClientCertificate* se pone la ruta al certificado del cliente.
2. En *ClientCertificatePrivateKey* se deberá indicar la ruta a la clave privada del certificado del cliente. Esta clave deberá estar en formato PKCS#8, el cual es el único admitido en modo seguro.

7. En la carpeta PSMP, ejecutar el siguiente comando para iniciar la instalación: *sudo rpm –i <rpm-file-name>*.
8. Reiniciar el servicio *sshd*.
9. Usar el comando *rpm –q CARKpsmp* desde la terminal para mostrar el nombre del archivo y la versión del PSMP instalado.

5.2.4 POST-INSTALACIÓN

Tras finalizar la instalación, se deben realizar diferentes tareas, entre ellas las siguientes:

a) Borrar los ficheros de instalación que ya no son necesarios. Es decir:
   - El fichero *vault.ini*.
   - Los ficheros de credenciales creados para la instalación (p.e.:*user.ini*, *user.cred*).
   - Borrar la utilidad *CreateCredFile*.

b) Ejecutar un procedimiento de *hardening* para PSMP. Dicho proceso se realiza de manera automática durante el proceso de instalación en Red Hat y Centos.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Se debe configurar el producto para que funcione con el modo de operación seguro FIPS. La configuración de este modo depende del componente a configurar. Para algunos componentes, es necesario realizar tareas adicionales.

Para los componentes Windows, es decir, el conector, se configuran las conexiones seguras durante la instalación para asegurar utilizar protocolos seguros como HTTPS y TLS con el certificado de la organización (estos pasos se han detallado en cada sección de instalación de componente). Para los componentes Linux, es decir, PSMP, se han de realizar los siguientes pasos para habilitar FIPS:

- Crear el archivo "*/etc/opt/CARKpsmp/clients/clients.conf*".
- Editar el archivo y añadir "*AdvancedFIPSCryptography=Yes*".
- Editar el archivo "*/etc/opt/CARKpsmp/conf/basic_psmpserver.conf*" y añadir "*AdvancedFIPSCryptography=Yes*".
- Reiniciar el servicio PSMP.

En el entorno de la solución, las comunicaciones entre los componentes **están restringidas a usar únicamente el protocolo TLS 1.2**.

Durante el proceso de configuración segura del producto, llevado a cabo durante la instalación de cada componente, se cierran todos los puertos a excepción de aquellos especificados para las comunicaciones TLS (443) y LDAPS (636).

Para el acceso al *Vault* se requiere de un mecanismo de autenticación que verifique los usuarios que se conectan a él. El producto permite establecer un segundo factor de autenticación, proporcionando así una mayor seguridad. Como segundo factor, el producto permite los siguientes métodos de autenticación. Esta autenticación se puede realizar las siguientes maneras:

a) **Contraseña almacenada en Idira (Local)**: El producto cuenta con una base de datos propia donde almacena los diferentes usuarios y credenciales.

b) **LDAP**: Como se ha mencionado anteriormente, el producto permite integrar un sistema de autenticación externo con un servidor LDAP. Idira es compatible con:

   - *Microsoft Active Directory*
   - *Sun One*
   - *IBM Tivoli Directory Server*
   - *Novell eDirectory*
   - *Oracle Internet Directory*

c) **RADIUS**: Este método supone que el usuario valida mediante credenciales almacenadas en un servidor RADIUS externo. El *Vault* también soporta el método de autenticación de RADIUS *challenge-response* para un segundo factor de autenticación.

d) **SAML**: Este método de autenticación permite la implementación de una solución *Identity Provider* para una autenticación federada. Beneficia a los clientes de un flujo de trabajo SSO cuando trabajan con múltiples dominios.

e) **OpenID**: La autenticación OIDC te permite autenticarte en Idira utilizando una cuenta de inicio de sesión único (SSO) a través del proveedor de tu organización.

6.2 AUTENTICACIÓN

Para llevar a cabo la configuración del método de autenticación deseado, se recomienda consultar los detalles específicos en [REF5].

A continuación, se describen los principales pasos para implementar dicha configuración:

1. Habilitar los factores de autenticación (MFA).
   a. Inicia sesión en el portal de **Identity Administration** con un usuario administrador.
   b. En el panel de navegación izquierdo, ve a **Core Services** (Servicios Principales) > **Policies** (Políticas) o **Manage > Policies**.
   c. Selecciona un conjunto de políticas existente que aplique a tus usuarios o haz clic en **Add Policy Set** para crear uno nuevo.
   d. Dentro de la política, navega a **User Security Policies** > **User Account Settings** (Configuraciones de la cuenta de usuario).
   e. En esta sección, **habilita los factores de MFA** que desees permitir. Por ejemplo:
      - **Permit device enrollment** (Permitir inscripción de dispositivos): Necesario para usar la aplicación Idira Mobile Authenticator.
      - **FIDO2 / Passkeys**: Para llaves de seguridad físicas o biometría.
      - **OATH OTP**: Para aplicaciones de terceros como Google Authenticator o Microsoft Authenticator (asegúrate de permitir la integración OATH OTP).
      - **Security questions** (Preguntas de seguridad).
      - Teléfono móvil (para SMS).
2. Crear un perfil de autenticación.

Una vez habilitados los métodos, debes agruparlos en un "Perfil" que dicte cómo se presentarán al usuario durante el inicio de sesión.

   a. En el panel izquierdo, ve a Settings (Configuración) > Authentication > Authentication Profiles.
   b. Haz clic en **Add Profile** (Añadir Perfil).
   c. Asigna un nombre al perfil (ej. "Acceso a Privilege Cloud MFA").
   d. Define los "Retos" (Challenges):
      - **Challenge 1:** Selecciona el método principal (normalmente Password o contraseña).
      - **Challenge 2:** Selecciona los métodos adicionales requeridos para MFA (por ejemplo, marca las casillas de Mobile Authenticator, OATH OTP Client, FIDO2, etc.). El usuario podrá elegir uno de los métodos marcados aquí.
   e. Haz clic en **OK** y luego en **Guardar**.
3. Aplicar el Perfil mediante reglas de autenticación.

Finalmente, debemos indicar a la plataforma que utilice ese perfil de autenticación cuando los usuarios intenten acceder.

a. Vuelve a Core Services > Policies y abre la política que editaste en el Paso 1.
b. Ve a **Authentication Policies** > **Idira Identity** (o selecciona el acceso a la aplicación específica de Privilege Cloud).
c. Selecciona **Si** en Habilitar controles de política de autenticación.
d. Haz clic en Añadir regla. Puedes definir condiciones (por ejemplo, si el usuario se conecta desde fuera de la red corporativa).
e. En la columna **Default Profile**, selecciona el perfil de autenticación que creaste en el Paso 3.
f. Haz clic en **Guardar**.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

Las operaciones de gestión se deberán realizar a través del Portal Web. El usuario administrador de Idira se puede conectar por el portal web de Privilege Cloud utilizando su contraseña almacenada en Idira. La interfaz de gestión en Idira mediante portal web permite agregar y configurar plataformas y componentes de conexión a sistemas remotos. También se utiliza para implementar los métodos de autenticación que utilizarán los usuarios y en general definir los sistemas externos donde Idira deberá conectarse para configurar funcionalidades (ejemplo: soluciones de ticketing, SIEM y balanceadores de carga).

Toda comunicación con el Vault se realiza de manera segura por defecto. Dichas comunicaciones utilizan TLSv1.2, con cifrado AES 256. Estos parámetros no son configurables.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

6.3.2.1 POLÍTICA DE CONTRASEÑAS

Tanto los administradores, como el resto de los usuarios, han de contar con **una contraseña segura para su acceso al producto**. En el caso de utilizar autenticación con servidores externos, se utilizará la política de contraseñas definida en los mismos, por lo que se debe configurar en los servidores de autenticación una política similar a la indicada en el presente apartado.

La configuración de la política de contraseñas del producto se realiza de forma centralizada desde el portal web. A continuación, aparecen detallados los pasos para configurar esta política desde el portal de administración.

1. Acceso a las políticas de usuario.
   a. Inicia sesión en el Portal de Administración con una cuenta de Administrador de la plataforma.
   b. En el panel de navegación izquierdo, dirígete a Servicios Principales > Políticas. Aquí puedes hacer dos cosas:

- **Editar una política existente:** Selecciona la política que ya esté aplicando a tus usuarios (por ejemplo, la política *Default*).
- **Crear una nueva política:** Haz clic en Añadir conjunto de políticas, asígnale un nombre (ej. *Política de Contraseñas Corporativa*) y define a qué usuarios o roles se aplicará en la pestaña *Policy Assignment*.

2. Configurar la complejidad y longitud de la contraseña.
   a. Dentro de la política elegida, en el menú izquierdo, navega a Políticas de Seguridad de Usuario > Configuraciones de Contraseña.
   b. Modifica los parámetros de complejidad según los estándares de tu organización. En [REF6] se pueden observar todos los parámetros disponibles. Entre ellos destacan:
      - **Minimum Password Length:** Define el número mínimo de caracteres (por ejemplo, si ENS alto, el requisito mínimo será de 12 caracteres).
      - **Require Uppercase / Lowercase Letters:** Exigir mayúsculas y minúsculas.
      - **Require Consecutive Characters / Numbers:** Exigir números y caracteres especiales.
      - **Prevent Password Reuse (History):** Define cuántas contraseñas antiguas debe recordar el sistema para evitar que el usuario repita una clave anterior (por ejemplo, recordar las últimas 5 o 10 contraseñas).
3. Configurar la caducidad de contraseñas y el autoservicio.
   a. En la misma pantalla, desplázate hacia abajo para configurar el ciclo de vida de la contraseña:
      - **Maximum Password Age (Days):** Cada cuántos días caducará la contraseña obligando al usuario a cambiarla (por ejemplo, 90 días).
      - **Minimum Password Age:** El tiempo mínimo que debe pasar antes de que un usuario pueda volver a cambiar su contraseña.
      - **Password Expiration Warning (Days):** Con cuántos días de anticipación se le notificará al usuario mediante un mensaje en el portal que su contraseña está próxima a vencer (por ejemplo, 7 días antes).

4. Configurar el bloqueo de cuenta.

Para proteger las cuentas contra ataques de fuerza bruta, debes configurar las reglas de bloqueo:

   a. En el menú de la política, ve a User Security Policies > Account Lockout Settings (Configuraciones de Bloqueo de Cuenta).
   b. Configura los siguientes campos:
      - **Enable Account Lockout:** Asegúrate de marcarlo en Yes.
      - **Maximum login attempts:** Número máximo de intentos fallidos permitidos antes de bloquear la cuenta (por ejemplo, 5 intentos).
      - **Lockout duration:** El tiempo que la cuenta permanecerá bloqueada. Puedes configurarlo en un tiempo específico (ej. 30 minutos) o marcar **"Lock out until administrator unlocks"** si prefieres que un administrador deba intervenir manualmente para desbloquearla.

Por otra parte, cada plataforma de integración configurada para rotar las contraseñas de las cuentas en sistemas remotos contiene sus propias políticas de contraseñas. Si se desea que Idira rote las contraseñas en sistemas remotos (un ejemplo de sistema

remoto gestionado sería, por ejemplo, el sistema operativo UNIX) aplicando una política de contraseña más fuerte de lo que está especificado por defecto, es necesario editar la plataforma relacionada al sistema gestionado (ejemplo de plataforma en Idira: Unix vía SSH).

1. Para configurar dichas políticas, se deben seguir las siguientes indicaciones:

   a. Entrar en Privilege Cloud como usuario administrador de Idira.
   b. En el menú en la izquierda, hacer clic en *Administration -> Platform Management*
   c. Se carga una página en la que aparecen enumeradas todas las plataformas activas e inactivas en Idira. Elegir una plataforma (ejemplo: Unix vía SSH) para que aparezcan las opciones de configuración.
   d. Para modificar las políticas de contraseña, acceder a *Target Account Platform -> Automatic Password Management -> Generate Password*.
   e. Aparecerán las opciones de cambio de contraseña para esta plataforma específicamente. Además de longitud y complejidad, se incluye un campo para especificar caracteres prohibidos por si el sistema objetivo tuviese problemas con algunos caracteres especiales.



Figura 11: Configurar política de contraseña en sistemas remotos gestionados

6.3.3 ROLES DE ADMINISTRACIÓN PRINCIPALES

Los principales roles que proporciona la plataforma por defecto son los siguientes:

- **System Administrator (Administrador del Sistema):** Es el rol de superadministrador en el portal de Identity Administration. Tiene control total sobre políticas, configuraciones de red, autenticación (MFA) y gestión del resto de roles.
- **Privilege Cloud Administrators:** Administradores encargados de configurar y gestionar el entorno de Privilege Cloud. Tienen permisos completos de auditoría, gestión de plataformas, políticas maestras (Master Policy) y configuración del CPM/PSM.
- **Privilege Cloud Auditors:** Rol con privilegios de solo lectura enfocado en cumplimiento normativo. Pueden acceder a auditorías, informes y grabaciones de sesiones, pero no pueden modificar configuraciones ni contraseñas.
- **Privilege Cloud Safe Managers:** Encargados de administrar las bóvedas (Safes) a nivel operativo, incluyendo la gestión de permisos de otros usuarios sobre esas bóvedas específicas.

a gestión de estos roles se encuentra centralizada a través del portal de **Identity Administration**. Para llevar a cabo su configuración, se deben realizar los siguientes pasos:

1. Accede al portal de **Identity Administration** con una cuenta que disponga de privilegios de *System Administrator*.
2. En el panel de navegación izquierdo, selecciona **Servicios Principales** > **Roles**.
3. Para la asignación de miembros a estos roles, accede a la pestaña **Miembros** y pulsa en **Añadir** para seleccionar los grupos o usuarios correspondientes. Para mayor seguridad, se recomienda utilizar usuarios nominales.
4. Para otorgar los privilegios operativos, dirígete a la pestaña **Derechos Administrativos** y selecciona las capacidades específicas requeridas en la plataforma.

En el siguiente link de la documentación están descritos todos los roles de usuario que están preconfigurados en el producto [REF7].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Configuración de Conectividad hacia Sistemas Objetivo

A efectos de este documento, se denominan sistemas objetivo a todos los servidores y equipos presentes en la infraestructura y/o centro de datos (DC) del cliente que son gestionados y protegidos por la plataforma.

Estas reglas permiten que los componentes de rotación de contraseñas, aislamiento y grabación de sesiones interactúen con la infraestructura de la organización del cliente.

- Plataformas Windows (Servidores y Dominio):
  - Habilitar puertos 445/TCP (SMB) y 135/TCP (RPC) desde los conectores hacia los objetivos Windows para la gestión de contraseñas y cuentas locales.
  - Habilitar el rango de puertos dinámicos 49152-65535/TCP (RPC/WMI).
  - Abrir puerto 3389/TCP (RDP) desde el conector hacia los servidores para que el PSM pueda establecer las sesiones proxy seguras.
- Plataformas UNIX / Linux / Dispositivos de Red:
  - Abrir el puerto 22/TCP (SSH) desde el conector hacia los endpoints para la gestión de credenciales y el aislamiento de sesiones.
  - Bases de Datos: Garantizar conectividad TLS desde el conector a los puertos nativos de bases de datos. Ejemplos comunes:
    - Oracle: 1521/TCP o 2484/TCP (TCPS).
    - SQL Server: 1433/TCP. MySQL / MariaDB: 3306/TCP.
    - PostgreSQL: 5432/TCP.

Tareas adicionales - abrir conectividad hacia los servicios en nube de Idira

- Prueba de resolución DNS: Comprobar que los servidores locales del conector resuelven correctamente tanto los FQDN internos como los externos (*.cyberark.cloud)

- Desactivación de Inspección SSL (SSL Decryption): Asegurar en el Firewall/Proxy de la empresa que el tráfico hacia los dominios de Idira esté excluido de la inspección SSL/TLS profunda, ya que interfiere con el cifrado de Idira y rompe la confianza de los certificados mutuos (mTLS).
- Permitir tráfico HTTPS / REST API: Abrir el puerto 443/TCP saliente hacia los FQDN dinámicos de tu instancia (https://*.cyberark.cloud o https://*.privilegecloud.cyberark.com)
- Habilitar comunicación con el Backend: Abrir el puerto 1858/TCP saliente para la comunicación directa de los conectores con la Vault en la nube.

Podéis encontrar todas las configuraciones de red detalladas en [REF8].

6.5 GESTIÓN DE CERTIFICADOS

El Idira Digital Vault es la piedra angular del servicio Privilege Cloud. La base de datos altamente segura mantiene las credenciales de cuentas privilegiadas de los clientes, las políticas de control de acceso, las políticas de gestión de credenciales y la información de auditoría. Idira aprovecha algoritmos de cifrado jerárquico de múltiples capas que cumplen con FIPS 140-2 para proteger el Digital Vault y sus datos. Los secretos almacenados en Privilege Cloud se cifran de forma única utilizando una clave AES-256 generada aleatoriamente. Esta clave luego se cifra en sobre (envelope encrypted) con una Customer Managed Key (CMK) almacenada en Amazon Web Services Key Management Service (AWS KMS). El acceso a los datos almacenados en el vault requiere permiso de descifrado para todas las claves en la jerarquía de cifrado.

Existe también la opción de Bring Your Own Key (BYOK). Con BYOK, la clave de cifrado de AWS KMS de Idira se reemplaza por su propia clave de AWS KMS. Los flujos de almacenamiento y cifrado de datos siguen siendo los mismos, y solo se reemplaza la clave de cifrado de AWS KMS. Esto pone todas las responsabilidades de gestión y rotación de la clave de cifrado de AWS KMS en sus manos, de modo que usted controla el acceso a la clave de cifrado, determina la política de rotación de la clave de cifrado y puede revocar el acceso de Idira a la clave cuando sea necesario.

Los certificados PKI de los servicios en la nube estarán gestionados por Idira.

Para más detalles, por favor revisad [REF9].

6.6 SERVIDORES DE AUTENTICACIÓN

Integración con LDAP como Active Directory

El Idira Identity Connector añade AD como un servicio de directorio al habilitar la comunicación segura entre Idira Identity y su dominio de AD.El Idira Identity Connector se instala en su red dentro del firewall, se ejecuta en un servidor Windows unido al dominio y monitorea AD en busca de cambios en usuarios y grupos. También monitorea Active Directory en busca de cambios en las políticas de grupo, los cuales envía a Idira Identity para actualizar los dispositivos inscritos. Los cambios de AD se sincronizan con Idira Identity cada 5 minutos de forma predeterminada.Puede instalar conectores adicionales para equilibrio de carga y failover. También es posible que desee instalar más de un conector si utiliza múltiples tenants de Idira Identity. En la mayoría de los casos, debe instalar dos conectores en un entorno de producción. Idira

Identity determina qué conector utilizar al monitorear la salud del conector y realizar una selección aleatoria con una inclinación hacia los conectores saludables. [REF10]

Federación con IDPs externos

Esta sección describe cómo configurar la federación con proveedores de identidad (IdPs) externos como Microsoft Entra ID, Okta, etc… La federación permite la integración de su tenant de Idira con otras fuentes de identidad con single sign-on (SSO) para sus usuarios a través de diferentes aplicaciones y plataformas. Cuando configura la federación, puede aprovechar las políticas de autenticación y autorización de los IdPs.

Detalles para establecer la federación vía SAML u OIDC, consulte [REF11].

6.7 SINCRONIZACIÓN

La gestión del tiempo en el *backend* (Vault) es responsabilidad del proveedor. Sin embargo, los componentes (PSM y PSMP) tienen que mantener una sincronización horaria precisa para garantizar la integridad de los logs, la correcta operación de protocolos de autenticación (LDAPS) y la correlación de eventos de seguridad.

Se debe asegurar que todos los servidores locales (Conectores y PSMP) estén sincronizados con una fuente de tiempo fiable mediante el protocolo NTP (*Network Time Protocol*).

- Entorno Windows (PSM): Es obligatorio configurar la sincronización horaria mediante *Group Policy* (GPO) o configuración local de servidor para garantizar que el sistema utiliza un servidor NTP corporativo autorizado y seguro.
- Entorno Linux (PSMP): Se recomienda habilitar y configurar el servicio ntpd o chronyd para sincronizar el tiempo contra el mismo servidor NTP corporativo utilizado por la infraestructura Windows.

6.8 ACTUALIZACIONES

Todos los servicios que se dan como servicio siguen su propio calendario y metodología de actualizaciones, siendo transparentes para nuestros clientes. Los detalles se pueden consultar en [REF12].

En cuanto a los conectores que sirven para el rotado de contraseñas y la gestión segura de sesiones, consulte [REF13].

Paso 1: Antes de comenzar

- Prepare las credenciales de usuario:
  - Contraseña de Installeruser.
  - Usuario Local Admin, con derechos de Admin completos. Para despliegues In-domain, este debe ser un usuario de dominio.
- Asegúrese de que el PSM confíe en el certificado utilizado por LDAPs. Para garantizar la conectividad de PSM, el Connector Manager ejecuta una comprobación de credenciales para verificar que el usuario de dominio y la contraseña que ingresa sean viables. El Connector Manager se conecta a LDAP sobre TLS para comprobar la conexión.

- Asegúrese de que el CA Certificate que firmó el certificado utilizado por los LDAPs exista en la máquina del Connector.
- Si no es así, importe el CA Certificate al almacén de certificados de Windows en la máquina del Connector: Certificates (Local Computer)/Trusted Root Certification Authorities

- Si la máquina del Privilege Cloud Connector se instaló inicialmente utilizando Connector Management, y el Management Agent todavía está instalado en la máquina, continúe con el siguiente paso. Si la máquina del Privilege Cloud Connector se instaló utilizando el Privilege Cloud Installer, instale el Connector Management Agent para poder actualizar fácilmente los componentes utilizando Connector Management.
- Prepare la máquina del Privilege Cloud Connector:
  - Tome un snapshot de la máquina del Connector antes de actualizar. Detenga el servidor, tome un snapshot, reinicie el servidor e inicie sesión de nuevo.
  - Genere un informe de Group Policy del servidor del Connector. En la línea de CMD o PowerShell, ejecute Gpresult /h C:\PolicyBeforeUpgrade.html
  - Verifique las versiones actuales.

    Click derecho en Start menu > Application and Features

  - Descargue el paquete de software de Privilege Cloud más reciente desde el área de descargas del marketplace de Idira
  - Copie el paquete de GPO Hardening requerido al servidor de dominio y extraiga el paquete zip.
    - En el servidor del Connector, navegue a Program Files > Idira > Management Agent > workspace del servidor
    - Acceda a la carpeta de instalación del componente PSM que contiene los archivos de hardening para Unified, PSM y out of domain y localice el archivo Idira Hardening - In-Domain - PSM v[latest].zip
- Deshabilite el agente de antivirus si está instalado en su servidor. En algunos casos, dependiendo del nivel de intrusión del antivirus, es posible que deba eliminar el antivirus temporalmente para realizar la actualización.
- Antes del Upgrade:
  - Realice una copia de seguridad de estos archivos:
    - PSM\Refuerzo\PSMHardening.ps1
    - PSM\Hardening\PSMConfigureAppLocker.xml
    - PSM\basic_psm.ini
    - Todos los registros de la carpeta PSM\Logs
  - Para usuarios de dominio PSMConnect / PSMAdminConnect :
    - Compruebe que los usuarios locales de PSMConnect y PSMAdminConnect estén en el grupo Built-in \ Users del conector:
    - Desde MMC o lusrmgr.msc > Usuarios y grupos > vea los usuarios de PSMConnect/PSMAdminConnect y agréguelos al grupo Integrado \ Usuarios , o vea el grupo Integrado \ Usuarios y agregue los usuarios de PSMConnect/PSMAdminConnect .

        - Aplique la gestión de secretos a los usuarios de PSMConnect y PSMAdminConnect
    - Consulta el archivo PSMConfigureAppLocker.xml , que contiene reglas personalizadas para los archivos ejecutables de tu organización.
        - Si dispone de un archivo PSMConfigureAppLocker.xml modificado que contiene reglas personalizadas para sus archivos ejecutables, conserve el archivo actual.
        - Valide todos los cambios personalizados en el archivo PSMConfigureAppLocker.xml personalizado antes de ejecutar el script de endurecimiento.
- En la herramienta de administración de conectores, compruebe si hay actualizaciones disponibles.
- Seleccione el conector que desea actualizar y siga los pasos que se detallan a continuación, según el flujo de actualización.
- Para sistemas con alta disponibilidad de PSM, garantice un tiempo de inactividad mínimo desviando temporalmente el tráfico del PSM en actualización.
- Compruebe la actualización del conector de Privilege Cloud mediante la administración de conectores.

Paso 2:Actualizar las GPO

Para aplicar el GPO de hardenización:

3. Descarga el archivo GPO de hardenización unificado de PSM de Privilege Cloud correspondiente a tu versión, tal como se describe en 5.1.2PREPARANDO EL SERVIDOR.
4. Importa el archivo GPO a tu dominio de *Active Directory*.
    a. Abre la Consola de administración de directivas de grupo (GPMC.msc).
    b. Crea un GPO: Expande **Administración de directivas de grupo** (*Group Policy Management*) > <tuDominio>, luego haz clic derecho en **Objetos de directiva de grupo** y selecciona **Nuevo**. Aparecerá la ventana de Nuevo GPO.

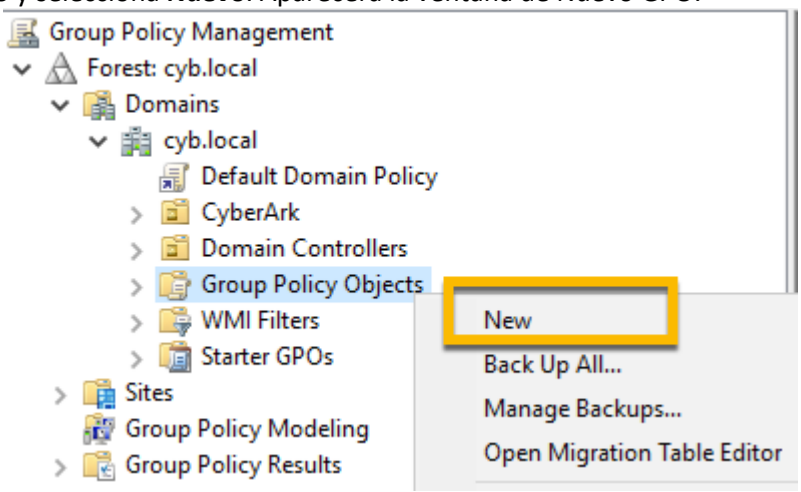


Figura 12: Creación de nueva GPO

- En el campo Nombre, especifica un nombre para el GPO Unificado que indique el propósito y la versión actual (por ejemplo, *Unified Hardening vN.N*), y haz clic en Aceptar.
- En la lista de Objetos de directiva de grupo, haz clic derecho en el nuevo GPO de hardenización y selecciona Importar configuración.

- En la ventana de bienvenida del Asistente para importar configuración, haz clic en Siguiente y define lo siguiente:

CAMPO	ACCiON
Ventana de la copia de seguridad de GPO	Haz clic en Siguiente.
Ubicación de la copia de seguridad	Haz clic en Examinar y selecciona la ubicación donde guardaste la configuración del GPO de hardenización de la versión, por ejemplo, *Privilege Cloud Connector Unified Hardening GPO*, y haz clic en Aceptar.
Ventana de GPO de Origen	Haz clic en Siguiente.
Ventana de Examen de copia de seguridad	Haz clic en Siguiente.
Ventana de Finalización del asistente para importar configuración	Haz clic en Finalizar. La ventana de Importación aparecerá indicando el progreso de la importación del GPO.

Tabla 5: Actualización de GPO

Cuando el proceso de importación del GPO haya finalizado, haz clic en Aceptar. Después de la importación, selecciona el GPO y en la pestaña Configuración verifica que los ajustes se hayan importado correctamente.

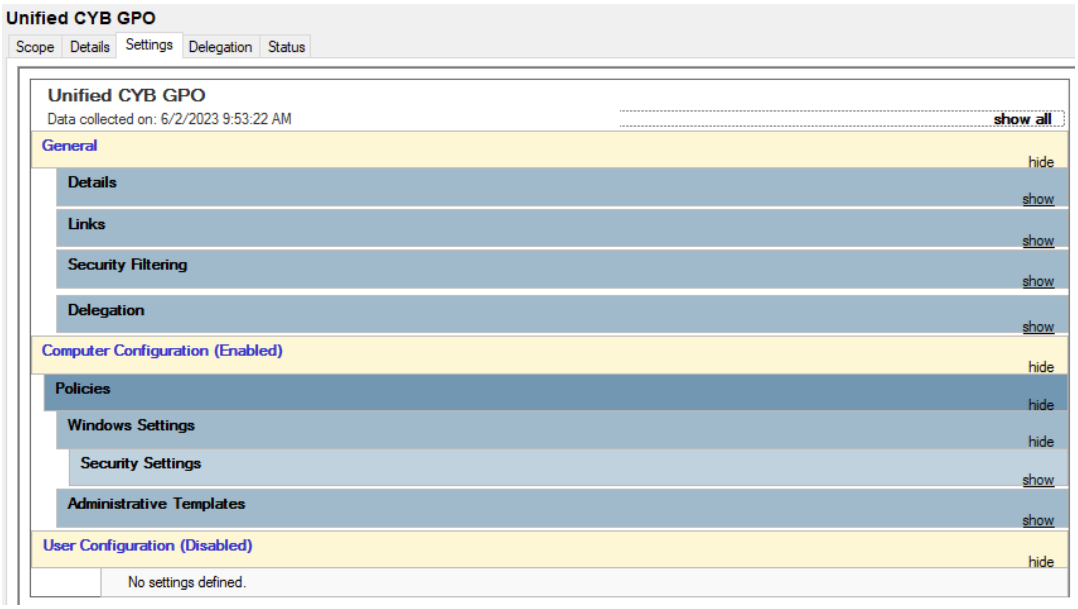


Figura 13: Verificación de los ajustes de GPO

Vincula el archivo GPO a la unidad organizativa (OU) dedicada de Idira que contiene los servidores de Idira.

- Asegúrate de que todos los servidores del Conector estén ubicados bajo la OU dedicada, para que el GPO no afecte a ningún otro servidor.
- En la Consola de administración de directivas de grupo, haz clic derecho en la OU y luego selecciona **Vincular un GPO existente**.
- Selecciona el GPO de Endurecimiento Unificado y haz clic en Aceptar. La política del GPO de Endurecimiento Unificado aparecerá en la pestaña de Objetos de directiva de grupo vinculados.

Reinicia la máquina para que aplique el GPO actualizado

Paso 3:Actualizar el conector

- En Administración de conectores > Lista de conectores , haga clic en Actualizaciones disponibles para ver los conectores que tienen componentes con versiones más recientes.

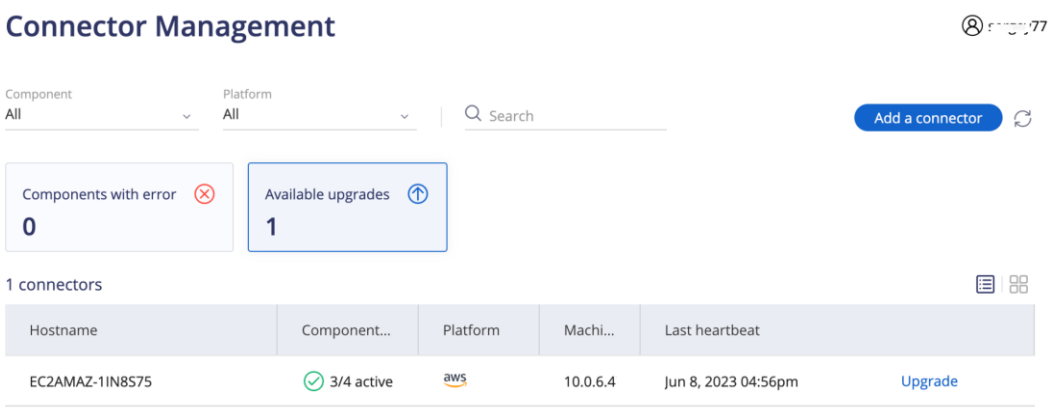


Figura 14: Actualización del conector

- En la fila del conector que indica las actualizaciones disponibles, coloque el cursor sobre el icono de estado o el enlace Actualizar para ver los componentes que se pueden actualizar.
- Si el componente con actualizaciones disponibles es CPM, verifique si se trata del CPM activo o del CPM pasivo (DR CPM). Anote el tipo de CPM para las acciones posteriores.
- En la lista de conectores, haga clic en Actualizar y continúe con el asistente de actualización según las actualizaciones disponibles.
- Seleccione la casilla de verificación PSM y haga clic en Siguiente.
- En la pestaña Configurar, introduzca los siguientes datos:
    - Modo de instalación. Conservar el modo de producción seleccionado.
    - nombre de usuario del instalador. El usuario de administración de identidades integrado se utiliza para instalar componentes locales. Introduzca el nombre de usuario del instalador (installeruser@<sufijo>) que actualizó en Administración de identidades > Usuarios > Usuarios de servicio.
    - Contraseña del usuario instalador. Introduzca la contraseña que configuró para el usuario instalador de Administración de identidades.
    - Cuenta de instalador de PSM. Seleccione el tipo de cuenta de usuario que utilizó para iniciar sesión en el equipo.
    - Usuario local: Seleccione Usuario local para reemplazar el usuario de dominio predeterminado. No se requieren más detalles.
    - Usuario de dominio: Esta es la configuración predeterminada. Asegúrese de que su usuario de dominio tenga derechos de administrador local en el servidor.
    - Introduzca lo siguiente:
        - Dominio. El dominio para el que el usuario tiene derechos de administración.
        - Nombre de usuario
        - Contraseña

- Compruebe la columna Estado para ver el icono Activo, que indica que la actualización se completó correctamente. Actualice la página para ver el indicador de estado actualizado.
- Reinicie la máquina del conector. Este paso es crucial para que la máquina del conector funcione correctamente.

6.9 AUTO-CHEQUEOS

La plataforma Idira Privilege Cloud realiza una serie de procesos automáticos de auto-chequeo (*self-test*) para garantizar la integridad del software y el correcto funcionamiento de las funciones criptográficas, asegurando el cumplimiento de los estándares FIPS 140-2.

Estos procesos incluyen:

- **Verificación de Integridad en el Inicio:** Cada componente (Vault, PSM, CPM) ejecuta una validación de firmas digitales y sumas de verificación (*checksums*) en sus binarios y módulos críticos durante la fase de arranque (*startup*) para detectar cualquier modificación no autorizada o corrupción del software.
- **Chequeos Criptográficos:** Durante el inicio y de forma continua en tiempo de ejecución, el motor criptográfico valida los algoritmos y las llaves de cifrado para confirmar que la capa de seguridad funciona correctamente.
- **Monitorización de Salud:** El "Connector Management Agent" supervisa constantemente el estado de los componentes locales, realizando latidos (*heartbeats*) y pruebas de conectividad hacia el backend para asegurar que la comunicación y los servicios críticos están operativos.
- **Acciones en caso de fallo:**
    - Ante un fallo en el arranque (ej. integridad de binarios comprometida), el servicio no iniciará, bloqueando la ejecución para evitar operar en un estado inseguro, y registrará un error crítico en los logs del sistema.
    - Ante una anomalía en la conectividad o en los servicios durante la operación, el componente entrará en estado de alerta o error en el portal de administración, permitiendo al administrador realizar una revisión manual, ejecutar un reinicio del servicio o solicitar el despliegue automático de una instancia nueva si el componente es inmutable.
- **Ejecución bajo demanda:** Los administradores pueden ejecutar pruebas de salud adicionales mediante las herramientas provistas en el *Privilege Cloud Tools* (ej. el script de comprobación de prerrequisitos) para validar la configuración actual sin necesidad de esperar a un evento de inicio.

6.10 ALTA DISPONIBILIDAD

6.10.1 REGISTRO DE EVENTOS

El servicio Idira Privilege Cloud proporciona a sus clientes una disponibilidad del 99,95%. La disponibilidad de Idira Privilege Cloud se fundamenta en los siguientes pilares:

- **Amazon Relational Database Service (RDS) Aurora:** Cada cliente de Privilege Cloud dispone de su propio esquema dentro de una base de datos RDS compartida.
- **Amazon RDS** proporciona alta disponibilidad y soporte de conmutación por error (*failover*) para las instancias de la base de datos mediante implementaciones en Múltiples Zonas de Disponibilidad (AZ). Amazon se compromete a un SLA de disponibilidad del 99,95% para RDS.
- **Amazon Elastic Block Store (EBS):** Todas las grabaciones de sesiones se almacenan en Amazon EBS, el cual ofrece fiabilidad para aplicaciones de misión crítica. Cada volumen está diseñado para proteger contra fallos mediante replicación dentro de la Zona de Disponibilidad (AZ). Amazon se compromete a un 99,999% para EBS.

Adicionalmente, tanto el portal de Privilege Cloud como las instancias del Vault son completamente inmutables. Se aprovisionan automáticamente; todos los datos se almacenan y ubican en RDS y EBS, por lo que, en caso de cualquier problema, se pueden crear instancias nuevas de forma inmediata y automática.

Este nivel de disponibilidad se logra orquestando múltiples servicios y soluciones para garantizar un tiempo de actividad casi constante para el servicio Privilege Cloud. Privilege Cloud cuenta con herramientas de monitorización 24x7 que supervisan constantemente la disponibilidad y el estado de salud de todos los componentes dentro del servicio. Cualquier problema se envía de inmediato al equipo de operaciones, y se tomarán medidas de resolución inmediatas cuando sea necesario. Un equipo de Ingenieros de Fiabilidad del Servicio (SRE) tiene la tarea de mejorar constantemente la disponibilidad de Privilege Cloud mediante la creación de herramientas de monitorización adicionales y la mejora de las capacidades de mitigación automatizada del servicio.

Privilege Cloud también tiene un compromiso de Mantenimiento del Servicio, lo que significa: (i) mantenimiento de rutina semanal realizado por Idira durante una ventana programada previamente; (ii) otras actualizaciones del sistema, mejoras o mantenimiento de rutina que se anuncian por correo electrónico con al menos dos días de antelación; o (iii) mantenimiento de emergencia de los Servicios fuera de la ventana de mantenimiento de rutina o programada previamente mencionada, que sea razonablemente necesario para completar la aplicación de parches o correcciones, o para llevar a cabo otras actividades de mantenimiento urgentes. Idira se esforzará por limitar la ventana de Mantenimiento del Servicio al mínimo posible para evitar interrupciones del servicio. Tenga en cuenta que la ventana de mantenimiento para actualizaciones ocurre típicamente una vez cada cuatro meses y requiere hasta 15 minutos de tiempo de inactividad. Los parches de seguridad ocurren generalmente de forma mensual, lo que ocasionalmente resulta en un tiempo de inactividad debido al reinicio que puede tomar hasta 4 minutos.

En términos del Objetivo de Tiempo de Recuperación (RTO), Idira compromete a Privilege Cloud a un tiempo de entre unos pocos segundos y hasta 24 horas, dependiendo del tipo de fallo. Sin embargo, en la mayoría de los casos, el RTO es cercano a cero y se encuentra dentro de los 20 minutos. En cuanto al Objetivo de Punto de Recuperación (RPO) para los datos del sistema, como las cuentas privilegiadas almacenadas en la base de datos, el RPO es de tan solo unos segundos

desde el momento del fallo, y de hasta 12 horas para las grabaciones y cambios de configuración desde el último punto de funcionamiento.

¿Cómo se logra esto?

Idira Privilege Cloud se despliega en una plataforma de AWS y reside en tres Zonas de Disponibilidad (AZ) diferentes en caso de interrupciones en uno de los centros de datos de la AZ. Cada AZ incluye la aplicación y todas las entidades de soporte necesarias para la correcta funcionalidad de la monitorización de la solución y las mitigaciones activadas automáticamente.

Los sistemas de monitorización recopilan todos los elementos del servicio (métricas del sistema operativo, registros del sistema y de aplicaciones, datos de red, auditoría y latidos de los componentes), los analizan y generan alertas en caso de problemas de disponibilidad u otras indicaciones sospechosas.

Un servicio de vigilancia (*watchdog*) es responsable de desencadenar procedimientos automáticos basados en las alertas generadas por el sistema de monitorización. El *watchdog* elimina la necesidad de intervención humana para mitigar problemas con el servicio (por ejemplo, levantar un nuevo servidor de aplicaciones en una o más AZ y terminar el antiguo sin ningún paso manual).

Se puede encontrar más información sobre la disponibilidad de la plataforma en el siguiente enlace de la documentación oficial: [REF14].

6.10.2 ALTA DISPONIBILIDAD PSM

Para mantener una alta disponibilidad de la solución, se deben seguir los siguientes pasos:

- Instalar más de un componente PSM. Para garantizar una alta disponibilidad sobre el componente de gestión de sesiones, el componente PSM puede ser instalado múltiples veces, pero se requiere por separado un balanceador de carga. PSM puede determinar la disponibilidad del servicio y lo reporta, bajo demanda, al balanceador de carga. Para la implementación de PSM en alta disponibilidad, se recomienda:
    - Balanceador de aplicaciones: se recomienda la implementación de un balanceador de aplicaciones desplegado como proxy inverso.
    - Monitorizando salud de PSM: se debe configurar el balanceador de carga para que combine la monitorización a nivel de aplicación para RDS (Remote Desktop Services) y PSM. Para PSM, hay que instalar y configurar PSM Health Check web service y configurar monitorización por TCP para el health check de RDS (recomendado por Microsoft para cumplir con una monitorización completa a nivel de aplicación)
    - Configuración SSL: habilitar SSL passthrough para proteger la comunicación entre el balanceador y los nodos PSM.
    - Algoritmo de enrutamiento: configurar el método de balanceo para que seleccione el dispositivo con la menor cantidad de conexiones, para distribuir la carga entre los nodos.
    - Alta disponibilidad para el balanceador: se recomienda que el balanceador en sí esté configurado en alta disponibilidad.

- Balancear DNS: se recomienda balancear la carga para peticiones DNS.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

El producto almacena registros de actividad que detallan cada acción asociada al uso de contraseñas y grabación de sesiones privilegiadas. La información de auditoría incluye:

- *User name:* El usuario que accedió a la contraseña o fichero de grabación.
- *Password or recording file*: El nombre de la contraseña o fichero de grabación al que se accedió.
- *Destination address*: La dirección IP o nombre DNS de la ubicación remota donde se utilizó la contraseña.
- *Protocol*: El protocolo utilizado para llegar a la máquina destino.
- *PSM ID*: El identificador único del servidor PSM que gestionó la sesión.
- *Session ID:* El identificador único de la sesión PSM donde está grabado la actividad del usuario.
- *Session duration*: La duración de la sesión de usuario.

Los usuarios pueden ver esta información de auditoría en la sección de *Monitoring* desde el portal web para incluso repasar las grabaciones realizadas. Pueden buscar las grabaciones utilizando un motor de búsqueda que filtra por propiedades como: nombre de usuario, dirección, nombre de máquina o cualquier otra palabra clave que esté almacenado como propiedad de la sesión.

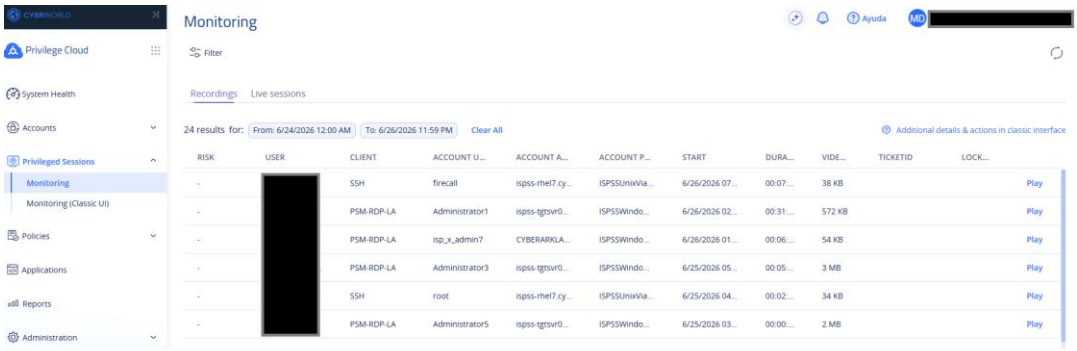


Figura 15: Monitorización de sesiones

6.11.2 ALMACENAMIENTO LOCAL

Por defecto, almacena los últimos 90 días de actividad. Cuando se llega a este límite, se borran los registros más antiguos para ubicar los más recientes. Para configurar el parámetro de número de días, desde el portal web, se puede acceder a la sección de *POLICIES -> Master Policy.*

El almacenamiento de las grabaciones de sesiones dentro de **Idira PAM** se realiza de manera íntegra en el ***Vault*** centralizado, el cual está plenamente gestionado en la infraestructura **de nube del producto**.

Con el fin de asegurar la confidencialidad de la información, estos archivos de auditoría disponen de un cifrado simétrico **AES-256** bajo una arquitectura jerárquica robusta, complementada con el uso de claves asimétricas RSA de 2048 bits para los procesos de recuperación de datos.

Por diseño, el acceso a estos archivos de auditoría está fuertemente restringido mediante controles de acceso basados en políticas (RBAC). **Solo los usuarios explícitamente permitidos y autorizados** (como aquellos con roles de Auditor o miembros específicos del Safe/Bóveda que tengan los privilegios de visualización habilitados) pueden acceder a visualizar o recuperar estas grabaciones cifradas.

Debido al borrado periódico de los registros almacenados localmente, **se recomienda configurar un método de almacenamiento remoto**, tal como se detalla a continuación.

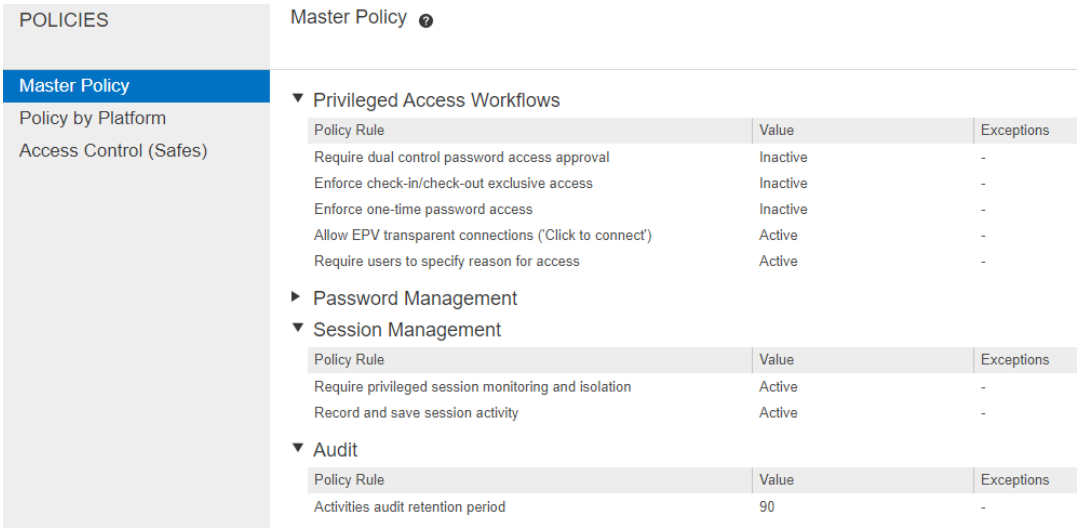


Figura 16: Master Policy

6.11.3 ALMACENAMIENTO REMOTO

La plataforma permite el envío periódico de los registros almacenados localmente a una herramienta SIEM. Esta integración se realiza directamente de nube a nube (o de nube a red local) a través de APIs REST bajo el protocolo estándar HTTPS (TLS 1.2 o superior), garantizando que el transporte de datos siempre esté cifrado.

Esta integración mediante APIs permitirá que la herramienta SIEM se autentique de manera segura contra la nube de Idira y extraiga los eventos periódicamente.

Para configurar integración hay que seguir los siguientes pasos:

1. Para que tu SIEM pueda extraer estos registros de forma segura, debes generar un acceso programático mediante OAuth2:

a. Crear una Aplicación OAuth2:

- Accede a tu portal de administración de *Identity*.
- Ve a **Apps & Widgets** > **Web Apps** y añade una aplicación personalizada del tipo **OAuth2 Server**.

- Debes configurar el *Scope* (alcance) mediante un script para otorgar el permiso específico de auditoría: isp.audit.events:read.

b. Crear un Usuario de Servicio:

- Ve a **Servicios principales** > **Usuarios** y haz clic en **Añadir Usuario**.
- Crea un usuario de servicio (por ejemplo, SIEM_Integrator) y, en el apartado de estado, marca la opción **"Is OAuth confidential client"**.

c. Vincular y otorgar permisos:

- Abre los detalles del usuario de servicio que acabas de crear, ve a la pestaña **Configuración de la Aplicación** y añádelo a la aplicación OAuth2 del Paso 1.
- Por último, ve a las propiedades de la aplicación OAuth2, en la pestaña **Permisos**, añade al usuario de servicio y concédele permisos de ejecución (*Run*).

2. Una vez generada la aplicación, obtendrás un **Client ID**, un **Client Secret** y la **URL de tu Tenant**.
   - **Integraciones Nativas:** Si utilizas soluciones como **Splunk** o **Microsoft Sentinel**, Idira ofrece *plugins* oficiales. Solo debes instalar la aplicación de Idira en el mercado de tu SIEM e introducir estas credenciales. El plugin se encarga automáticamente de realizar las llamadas a la API sobre TLS 1.2, descargar los registros en JSON y mapearlos correctamente.
   - **Integración Genérica:** Si usas otra herramienta, puedes configurar tu SIEM para que realice llamadas de tipo GET al endpoint /audit/events de Idira, autenticándose con el token de portador (Bearer Token) generado por OAuth2.

Para revisar esta configuración en más profundidad, es posible consultar la guía en la documentación oficial de Idira: [REF15].

6.12 BACKUP

En el marco del servicio Idira Privilege Cloud, la gestión de las copias de seguridad (backup) y la recuperación ante desastres (restore) es una responsabilidad íntegramente gestionada por el proveedor del servicio. La arquitectura SaaS garantiza la resiliencia mediante redundancia de base de datos (Amazon RDS Aurora) y almacenamiento (Amazon EBS) en múltiples Zonas de Disponibilidad. Por tanto, no requiere configuración ni ejecución de tareas de backup por parte del cliente.

7 REFERENCIAS

ID	Descripción
REF1	Guía de despliegue y requisitos del sistema Idira Privilege Cloud https://docs.cyberark.com/setup/latest/en/content/ispss-deployment/privilege%20cloud/privcloud-sys-req-srs-psm.htm
REF2	Idira Marketplace https://community.cyberark.com/marketplace/s/
REF3	Fundamentos de Seguridad https://docs.cyberark.com/snapshot/ispss-deployment/en/content/security/security%20fundamentals-ispss.htm
REF4	Set Installer User https://docs.cyberark.com/snapshot/ispss-deployment/en/content/ispss/ispss-installeruser-password.htm
REF5	Forzar Autenticación https://docs.cyberark.com/setup/latest/en/content/setup-space/authentication/enforce-strong-authentication.htm
REF6	Requisitos de complejidad de contraseñas https://docs.cyberark.com/manage/latest/en/content/identity/coreservices/usersroles/password-requirements.htm
REF7	Roles de usuario predefinidos https://docs.cyberark.com/manage/latest/en/content/identity/coreservices/usersroles/predefinedroles.htm
REF8	Configuración de conectividad https://docs.cyberark.com/privilege-cloud-standard/latest/en/content/privilege%20cloud/privcloud-sys-req-networks.htm
REF9	Configuración Bring Your Own Key (BYOK) https://docs.cyberark.com/snapshot/ispss-deployment/en/content/privilege%20cloud/privcloud-byok-setup.htm
REF10	Integración de Directorio Activo (AD) https://docs.cyberark.com/setup/latest/en/content/identity/coreservices/connector/add-ad.htm
REF11	Federación de Identidades (IdP) https://docs.cyberark.com/setup/latest/en/content/identity/coreservices/usersroles/partnersetup.htm
REF12	Actualización del backend https://docs.cyberark.com/setup/latest/en/content/ispss-deployment/privilege%20cloud/privcloud-upgrade-backend.htm

ID	Descripción
REF13	Actualización de componentes https://docs.cyberark.com/setup/latest/en/content/ispss-deployment/privilege%20cloud/privcloud-upgrade-connector-12.7-later-cm.htm
REF14	Datos de Seguridad de la Plataforma https://www.cyberark.com/resources/product-datasheets/cyberark-privilege-cloud-security-datasheet
REF15	Integración SIEM https://docs.cyberark.com/setup/latest/en/content/siem-integration/siem-export-3rd-party.htm
REF16	CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

Acrónimo	Significado
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Services
AZ	Availability Zone
BYOK	Bring Your Own Key
CA	Certificate Authority
CMK	Customer Managed Key
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
DNS	Domain Name System
EBS	Elastic Block Store
ENS	Esquema Nacional de Seguridad
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GPO	Group Policy Object
IAM	Identity and Access Management
IdP	Identity Provider
KMS	Key Management Service
LDAP	Lightweight Directory Access Protocol
OIDC	OpenID Connect
PAM	Privileged Access Management
PSM	Privileged Session Manager
PSMP	Privileged Session Manager Proxy
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RPO	Recovery Point Objective
RPC	Remote Procedure Call
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMB	Server Message Block
SRE	Site Reliability Engineer
SSH	Secure Shell
SSO	Single Sign-On
TLS	Transport Layer Security
WMI	Windows Management Instrumentation