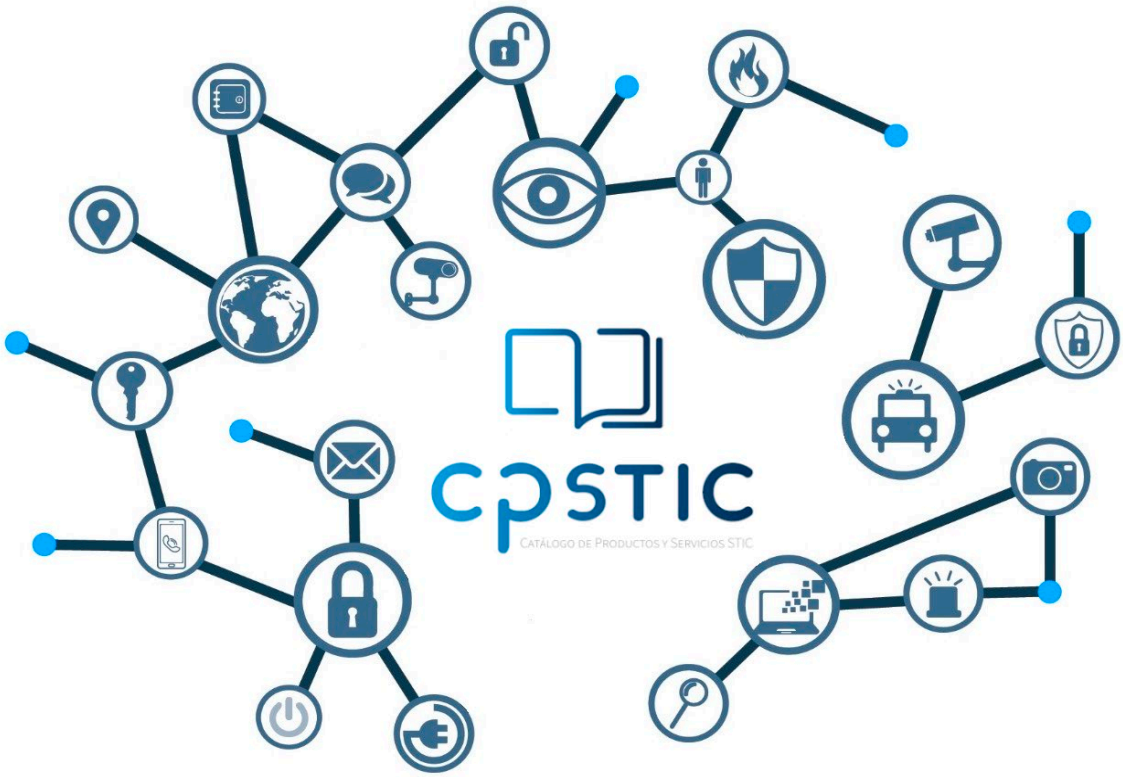
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1108

Procedimiento de Empleo Seguro
CyberArk Privileged Account Security Solution



Agosto de 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-016-6.
Fecha de Edición: Agosto de 2023

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.30 10:03:02 +01'00'

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

ÍNDICE

TABLAS

ILUSTRACIONES

1. INTRODUCCIÓN

1. **CyberArk PAS** 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.
2. 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*.
3. Además, al controlar la actividad de las cuentas privilegias, 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.
4. El producto está formado por diferentes componentes, los cuales se usan para tareas específicas y proporcionan diferentes funcionalidades. Estos componentes son:
    - *Enterprise Password Vault* (**EPV**). Es el componente principal del producto. Se encarga de almacenar las contraseñas de una manera segura. También se denomina ***Vault***. Además, en el EPV, se encuentran los componentes de alta disponibilidad (*High Availability Vault*), de recuperación frente a desastres (*Disaster Recovery Vault*), la solución de backups (*Backup solution*) y el cliente administrativo (*PrivateArk Administrative Client*), entre otros.
    - *Central Policy Manager* (**CPM**). Componente encargado de gestionar las claves y contraseñas. Permite la rotación automática de claves de los usuarios finales y las almacena en el EPV sin interacción humana. Además, es el encargado de mantener y gestionar las políticas de contraseñas.

- *Privileged Session Manager* (**PSM**). Es el encargado de gestionar, controlar y monitorizar de manera segura el acceso privilegiado a los dispositivos.
- *Privileged Session Manager SSH Proxy* (**PSMP**). Es el componente encargado de gestionar, monitorizar y controlar de manera segura el acceso privilegiado, al igual que PSM, pero para los dispositivos finales UNIX/Linux.
- *Password Vault Web Access* (**PVWA**). Es la interfaz web que proporciona una única consola para peticiones, acceso y gestión de contraseñas privilegiadas. Además, permite la gestión de la solución vía web.

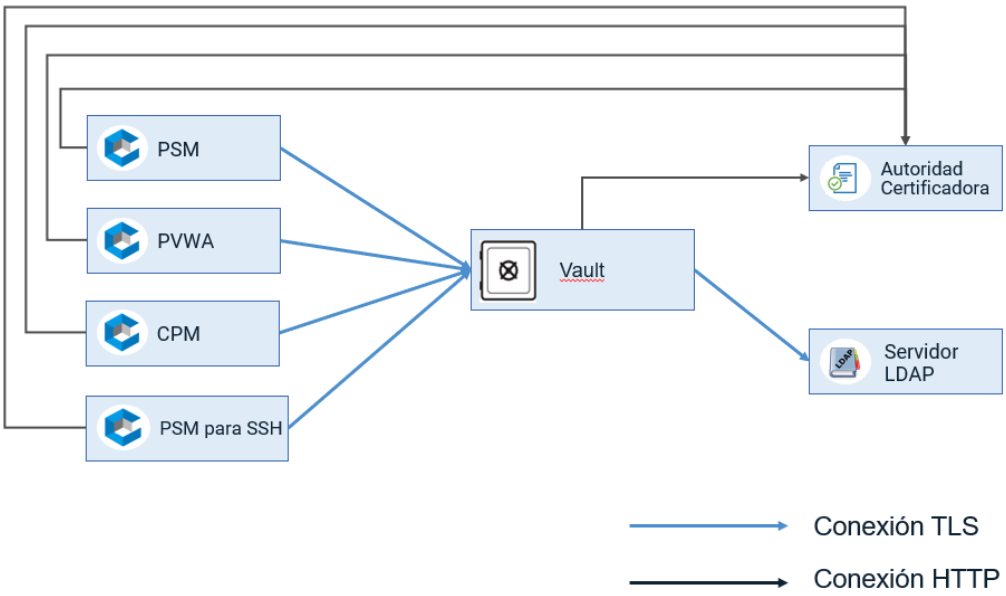


Ilustración 1 – Distribución de los diferentes componentes

2. OBJETO Y ALCANCE

5. Esta guía recoge el procedimiento de empleo seguro de los diferentes componentes pertenecientes a **CyberArk PAS**. 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.

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

Componente	Requisitos
EPV	• *Windows Server 2012 R2* o *Windows Server 2016.* • *.NET Framework 4.5.2.*
PVWA	• *Windows Server 2019, Windows Server 2016* o *Windows Server 2012 R2.* • *IIS 10.0, 8.5* • *. NET Framework 4.5.2-4.7.2.*
CPM	• *Windows Server 2019, Windows Server 2016* o *2012 R2.* • *.NET Framework 4.5.2-4.7.2.*
PSM	• *Windows Server 2019, Windows Server 2016* o *Windows Server 2012 R2.* • *.NET Framework 4.5.2-4.7.2.* • *Remote Desktop Services Session Host.* • Opcionalmente, instalar *Microsoft Remote Desktop Services Gateway.*
PSMP	• *Red Hat Enterprise Linux*, versión *7.X o 8.X.* • *Se puede usar CentOS Linux 7.9* • *SUSE Linux Enterprise Server,* versión *11 SP4 o 12.*

Tabla 1 Plataformas Compatibles

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

8. Además, los servidores RHEL deben tener:

   - *RHEL OpenSSH Server Cryptographic Module containing OpenSSH Server* (incluida en la instalación de RHEL).
   - *RHEL OpenSSL Cryptographic Module containing OpenSSL* (incluida en la instalación de RHEL).

9. Para mayor detalle de los requisitos de cada componente, se recomienda ver la documentación de la solución:

   https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/Landing%20Pages/lpSystemRequirements.htm

3. ORGANIZACIÓN DEL DOCUMENTO

10. El presente documento se divide en los siguientes apartados:

    a) **Apartado 4.** En este apartado se recogen **aspectos y recomendaciones** a considerar, antes de proceder a la instalación del producto.

    b) **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la **fase de instalación** del producto.

    c) **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.

    d) **Apartado 7.** En este apartado se recogen las tareas recomendadas para la **fase de operación** o mantenimiento del producto.

    e) **Apartado 8.** En este apartado se recoge una *checklist* con las tareas a realizar y el estado de cada una de ellas.

    f) **Apartado 9.** Referencias utilizadas en el presente documento.

    g) **Apartado 10.** En este apartado se hace referencia a las diferentes nomenclaturas utilizadas.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Para poder descargar el *software* de la solución, se debe contar con un usuario con acceso al CyberArk Marketplace:

    a) Registrarse como usuario en el portal de comunidad técnica: https://cyberark-customers.force.com/s/login/

12. Es necesario descargar por lo menos los siguientes ficheros para la instalación de producto:

    - *CyberArk PAS Self Hosted -> PAS Components ->*
        - *CPM -> Central Policy Manager-Rls.zip*
        - *Vault -> Client-Rls.zip*
        - *PVWA -> Password Vault Web Access-Rls.zip*
        - *Vault->Server-Rls-.zip*
        - *PSM -> Privileged Session Manager-Rls.zip*
        - *PSM for SSH -> Privileged Session Manager SSH Proxy-Rls.zip*

13. Para hacer uso del *software*, se envían por separado un par de claves de seguridad. Las claves de *Master* y *Operator* (claves criptográficas únicas para cada instancia de *Vault* licenciada) se entregan utilizando una solución de correo cifrado con resgistro de descarga y duración limitada. Se hará referencia a estas claves más adelante en este documento durante la instalación de producto.

14. Las claves criptográficas de *Master* y *Operator* se entregan por separdo. La clave *Master* para hacer uso del usuario *'master'* para operaciones específicas de recuperación. La clave *Operator* requerida por el Vault para arrancar los servicios de este mismo.

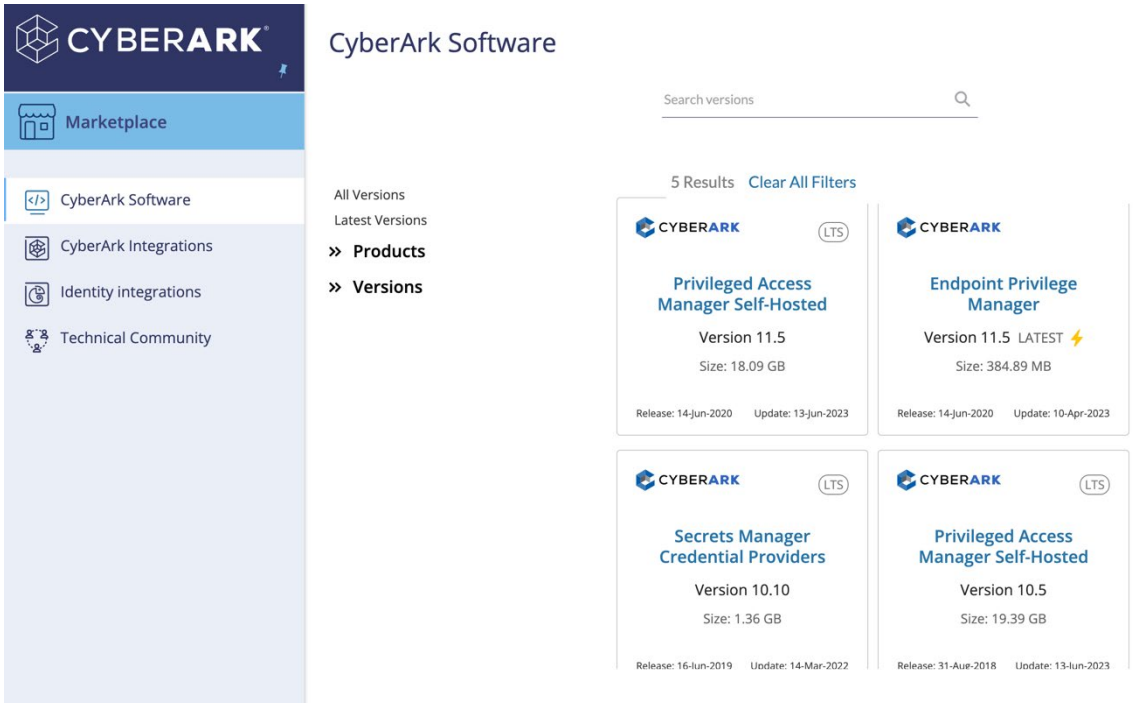


Ilustración 2 – Descargando paquetes desde CyberArk Marketplace

4.1.1 VERIFICACIÓN DE LA DESCARGA EN WINDOWS

15. El *software* de instalación está en formato *zip*, el cual está digitalmente firmado por CyberArk. Se debe verificar la firma en las carpetas dentro del fichero *zip*, para asegurar que no han sido modificadas completando los siguientes pasos de verificación de integridad:

    - Descargar e instalar el JDK: *http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html*
        a. Aceptar el acuerdo de licencia.
        b. Descargar *Windows x64 (jdk-8u301-windows-x64.exe*).
        c. Se debe verificar la firma digital del archivo descargado, *jdk.8u301-windows-x64.exe*. El enlace de la firma digital se encuentra encima del título *Java SE Development Kit 8u301*. Si la firma no coincide, se debe volver a descargar el producto.
        d. En caso de que la firma coincida, se debe hacer doble clic en el archivo *jdk.8u301-windows-x64.exe,* luego haga clic en *Run*.
        e. Hacer clic en *Next* para iniciar el asistente de instalación.
        f. Hacer clic en *Next* en la siguiente ventana.
        g. Hacer clic en *OK* en el cuadro de diálogo *Change in License Terms*.
        h. Se ha de esperar hasta que aparezca un cuadro de diálogo con la carpeta de instalación predeterminada. Hacer clic en *Next*.

i. Hacer clic en *Next* para aceptar la ubicación de instalación predeterminada *C:\Archivos de programa\Java\jre1.8.301*

j. Cuando aparezca el cuadro de diálogo **Java SE Development Kit Update 301 (64 bits) - Complete**, se ha de comprobar que aparece el siguiente mensaje "*Java SE Development Kit 8201 (64 bits) Successfully Installed*".

k. Hacer clic en *Close*.

- Descargar e instalar los archivos de *JCE Unlimited Strength Jurisdiction Policy* (políticas de jurisdicción de fuerza ilimitada de JCE).

  a. La descarga se realizará desde el siguiente enlace *http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html*

  b. Hacer clic en el botón de opción *Aceptar acuerdo de licencia*.

  c. En la fila 8 de *Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files*, bajo el encabezado *Download*, se debe hacer clic en *jce_policy-g.zip* para descargar el archivo.

  d. Descomprimir el archivo y abrir la carpeta *UnlimitedJCEPolicyJDK8.*

  e. Instalar los archivos *local__policy.jar* y *US_export_policy.jar* en la carpeta *C:\Program File\Java\jre1.8.0_301\lib\ security.*

- Ejecutar el siguiente comando sin comillas para llevar a cabo la verificación de la firma del fichero .zip:

  % JDK_Home% \ jarsigner.exe -verify -verbose -certs <nombre de archivo>.zip
  Para más información sobre las diferentes opciones de *jarsigner*, se recomienda acceder al siguiente enlace:
  https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html#CCHFIDAB

- En la salida del comando ejecutado, se mostrará algo como la siguiente imagen. Se deberá verificar que esté firmado por la empresa *CyberArk*:

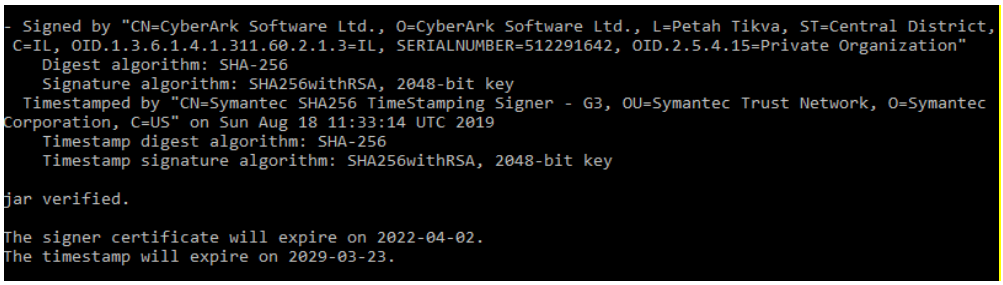


Ilustración 3 – Verificando autenticidad de fichero zip

16. Además, los archivos individuales son firmados digitalmente mediante la herramienta *MS Sign.* Para verificar la integridad de dichos archivos, una vez extraídos los ficheros individuales, se deberán seguir los siguientes pasos de ejemplo en cada archivo:

    - Ir al archivo correspondiente, por ejemplo:

\Server\setup.exe

- Hacer clic derecho sobre el archivo, e ir a *Properties > Digital Signatures*.
- Deberá estar seleccionado "*CyberArk Software Ltd.*" como firmante.
- Hacer clic en *Details*, y de la lista *Signature List* seleccionar *CyberArk Software Ltd*.
- Hacer clic en el botón *Details* y verificar los detalles de la firma para asegurar que fue firmado por CyberArk.

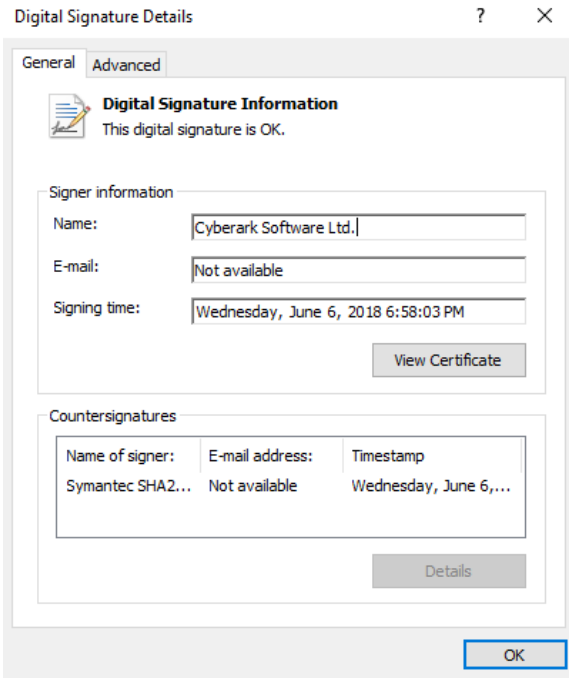


Ilustración 4 – Verificar la firma digital de los ficheros

4.1.2 VERIFICACIÓN DE LA DESCARGA EN LINUX

17. En caso del sistema operativo **Linux**, se verificará el *software* con los siguientes pasos:
    - Importar la clave pública *RPM-GPG-KEY-CyberArk*, proporcionada junto con el paquete de instalación del componente, mediante el comando: *rpm --import RPM-GPG-KEY-CyberArk*
    - Una vez importada la clave pública, se verifica la firma digital del paquete ejecutando el siguiente comando: *rpm –K –v <nombre_del_paquete.rpm>.*

4.2 ENTORNO DE INSTALACIÓN SEGURO

18. 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

19. La licencia adquirida previa a la instalación del EPV, determinará el número de usuarios, contraseñas y archivos que se pueden almacenar en el EPV. Además, determina los tipos de usuarios y las interfaces a las que se puede acceder.
20. La licencia será utilizada durante el proceso de instalación de EPV. El resto de los componentes se instalan sin necesidad de copiar esta licencia, que residirá solamente en el *Vault*. Para instalar la licencia de producto, se deben seguir los siguientes pasos:
    - Iniciar sesión en el sistema operativo de *Vault* como administrador y copiar el archivo de licencia (*license.xml*) a la carpeta "*Server*"; *<Drive>:\Program Files (x86)\PrivateArk\Server*. La ruta podría cambiar, en función del sistema operativo.
    - Si *Vault* no está en un clúster de alta disponibilidad, se ha de detener y reiniciar el servicio del servidor de *Vault* desde el icono del escritorio del SO para la consola de administración central del servidor.
    - Si es un entorno de clúster de alta disponibilidad, se deberá copiar el archivo *license.xml* en ambos nodos del clúster y mover los recursos del nodo activo al inactivo.
21. Para más información sobre la instalación y gestión de las licencias, se recomienda https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PASIMP/Managing-the-CyberArk-License.htm

4.4 CONSIDERACIONES PREVIAS

22. La solución Cyberark PAS permite la implementación de una arquitectura de **alta disponibilidad** para evitar la inactividad del producto por causas planificadas, como puede ser la actualización del *software* o la instalación de parches, o por causas no planificadas, como son los ataques malintencionados. Se recomienda realizar esta configuración, para ello ver el apartado 6.7 ALTA DISPONIBILIDAD.
23. Por otro lado, el producto cuenta con diferentes métodos de autenticación, los cuales se indican en el apartado 6.2 AUTENTICACIÓN. Se recomienda instalar un servidor de autenticación LDAP para autenticar las cuentas de usuarios.
24. Además, para una mejor configuración del entorno de operación, se deberá contar con un **servidor de certificación** (CA) en la organización que actúe como entidad certificadora y se encargue de verificar los certificados del producto. Posteriormente, se requerirá su dirección IP durante el proceso de instalación, ver apartado 5. FASE DE INSTALACIÓN.
25. Para cada uno de los componentes de la solución, se indicarán sus respectivas consideraciones previas en la fase de instalación.

5. FASE DE INSTALACIÓN

26. En esta sección se indicarán los principales pasos del proceso de instalación de cada uno de los componentes de la solución.
27. En el siguiente enlace de la documentación pública, se puede consultar el detalle de instalación de cada componente.

5.1 INSTALACIÓN EPV

5.1.1 PASOS INICIALES PARA CONFIGURAR EL SERVIDOR EPV

28. El administrador requiere acceso físico o remoto al servidor que será destinado para la función *Vault*, en la cual se almacenan todas las claves y contraseñas de la organización. Se deben realizar los siguientes pasos, antes de proceder a la instalación del *software*:
    1. Se deberá elegir un directorio donde instalar el *software* de EPV y otro directorio separado para almacenar los *Safes* (grupos lógicos particionados que almacenan las claves y contraseñas) que serán creados por el EPV.
    2. Se deberán preparar las claves de servidor (*Server Key*) y recuperación (*Recovery Public Key*) para EPV. Estas claves se se requieren durante el proceso de instalación y cada vez que se reinicie el servidor EPV.
    3. Para mayor seguridad, se recomienda mantener estas claves en un dispositivo HSM (*Hardware Security Module*). Si no, se deberá asegurar el mantenimiento de las claves en un directorio NTFS con permisos de lectura/escritura, limitado al grupo de administradores del sistema.
    4. En los servidores destinados a EPV o PVWA, para poder crear objetos en español es necesario modificar el idioma. Para ello, se deberán seguir los siguientes pasos:
        - Ir a *Control Panel* > *Clock, Language and Region*.
        - Seleccionar la opción *Region and Language*.
        - En la pestaña *Administrative*, hacer clic en *Change system locale* y se ha de seleccionar el lenguaje deseado, en este caso, español.

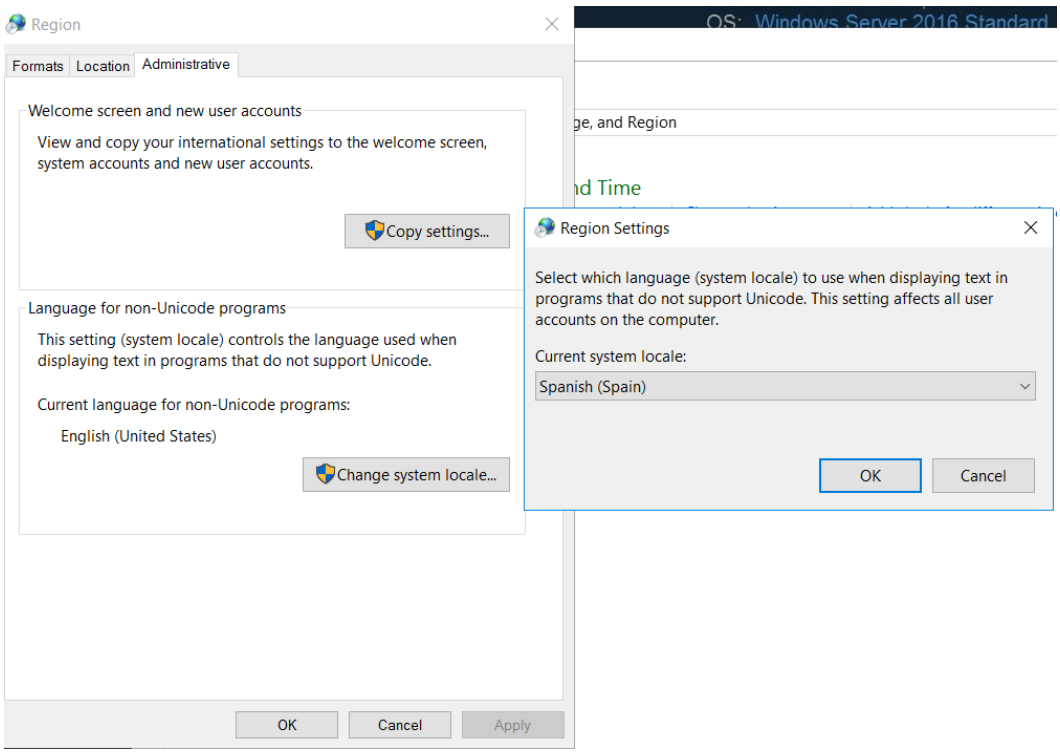


Ilustración 5 – Cambio de ajustes de región

5. Si los componentes de la solución van a acceder al *Vault* a través de un cortafuegos (p.e. desde la DMZ), se deberá crear una regla en él que permita el tráfico por el puerto 443 desde las máquinas donde se instalarán los componentes hacia el *Vault*.
6. Se deberá configurar una IP estática en la máquina en la cual se va a realizar la instalación de EPV.
7. En las propiedades de *Network Connection,* se deberán eliminar los servidores DNS. La conectividad DNS no es posible para el servidor *Vault*, por lo que no se deberán seleccionar ningún servidor DNS.
8. Desinstalar todos los protocolos de comunicación, a excepción de TCP/IP. Para hacer esto, habrá que editar las propiedades de la tarjeta de red del sistema operativo. Dentro de las propiedades de la tarjeta, se enumeran los protocolos de red instalados. Se puede seleccionar cualquiera y presionar el botón *Uninstall*. Hacer esto para todos los protocolos, a excepción de TCP/IPv4 y TCP/IPv6.

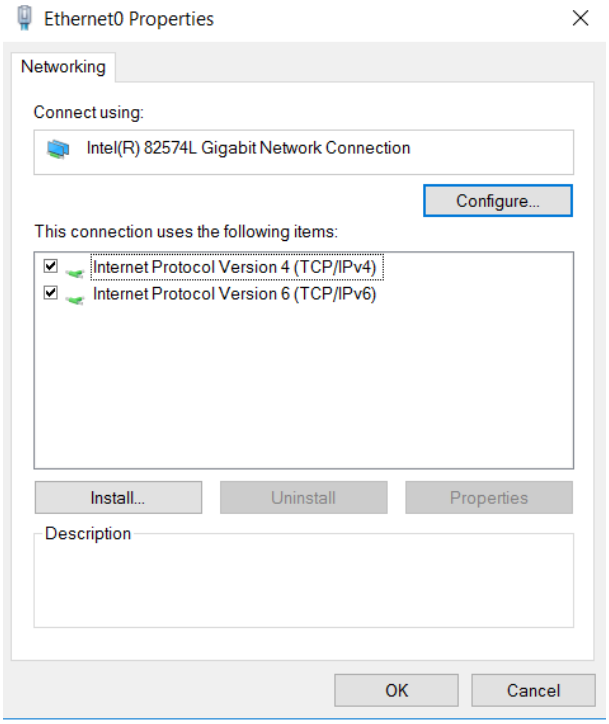


Ilustración 6 – Desinstalación de protocolos de comunicación

9. Eliminar todos los usuarios y grupos por defecto de Windows, no necesarios para la instalación del *Vault*.
10. Se recomienda que el servidor donde se realice la instalación pertenezca a un grupo de trabajo local de Windows (por ejemplo, "*WORKGROUP*" por defecto).
11. En la BIOS del sistema, asegurar que, en la secuencia de arranque, sea siempre desde el disco duro primero. Además, la BIOS debe estar protegida con contraseña.
12. Habilitar DEP (*Data Execution Prevention*) en la máquina en la cual se va a realizar la instalación de EPV, si no está activado. Se encuentra habilitado por defecto.

29. Una vez realizados los pasos anteriores, se deberá reiniciar el servidor donde se va a instalar EPV para que se actualice la configuración.

5.1.2 INSTALACIÓN DEL EPV

30. Es importante tener en cuenta que, si el servidor EPV se instala remotamente, se ha de utilizar un cliente *Remote Desktop Protocol* (RDP).
31. Se deberá descargar el *software* necesario para el EPV y verificarlo, tal y como se ha indicado en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO. A continuación, se indican los pasos a seguir para la instalación del servidor EPV:
    1. Copiar el archivo de instalación en el directorio del servidor EPV. Ir a dicho directorio y ejecutar *setup.exe* con permisos de administrador.

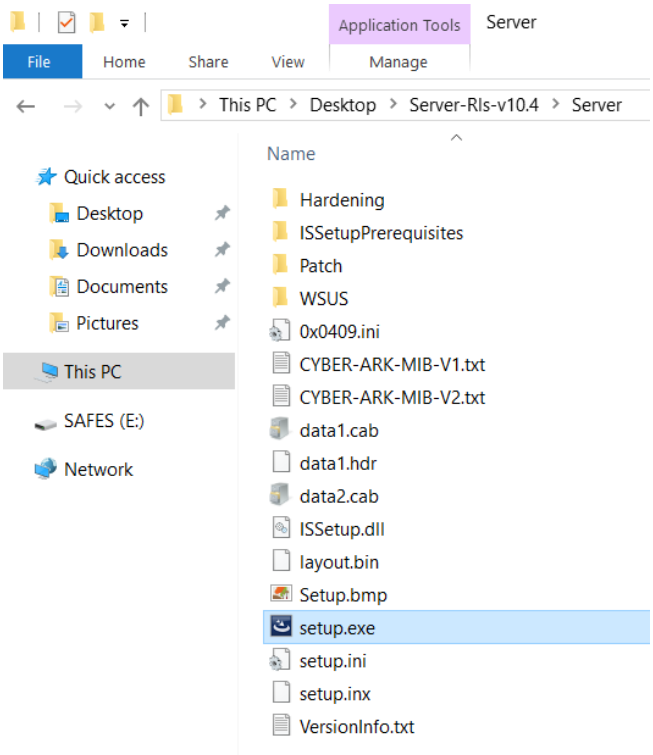


Ilustración 7 – Carpeta de instalación de EPV

2. Se iniciará el *wizard* de instalación, el cual verifica que se encuentren instalados en el dispositivo todos los programas o librerías necesarios. En caso de faltar alguno, el *wizard* mostrará un mensaje de error, en cuyo caso deberá instalarse dicho requisito.
3. Incluir los detalles necesarios y elegir como tipo de instalación *Standalone Vault Installation.*
4. Elegir las siguientes rutas:
    - Ruta de instalación.
    - Ruta donde almacenar los *Safe*.
    - Ruta de instalación del fichero de licencia.
    - Ruta de claves de operador.
5. No instalar un agente de control remoto, seleccionando *Skip Remote Control Agent Configuration.*
6. Permitir al instalador ejecutar el proceso de *hardening* en el sistema operativo. Este proceso realiza un bastionado del sistema sobre el que se instala el producto, mejorando así su seguridad y solo se puede eliminar reinstalando el sistema operativo.
7. Definir la contraseña los usuarios *Master* y *Administrator*. El usuario *Administrator* se utilizará posteriormente para las labores de gestión del producto. El usuario *Master* permite acceso completo al sistema y está pensado para uso en caso de emergencias.

8. Se ha de poner especial atención en la contraseña perteneciente a *Master*, ya que es el usuario por defecto con máximos permisos. En caso de pérdida de dicha contraseña, se perderá de forma completa el acceso al usuario *Master,* por lo tanto, se recomienda almacenarla de forma segura.
9. Para finalizar, se deberá reiniciar el servidor.

32. Una vez instalado, se deberá comprobar que los siguientes servicios se han activado y se están ejecutando:
    - *CyberArk Logic Container.*
    - *CyberArk Event Notification Engine.*
    - *CyberArk Hardened Windows Firewall.*
    - *PrivateArk Database.*
    - *PrivateArk Server.*
33. Seguidamente se deberá hacer doble clic sobre el icono de *PrivateArk Server*, para abrir la consola GUI instalada automáticamente durante este proceso (*PrivateArk Server Management Console*) y verificar la configuración. Estos parámetros no son configurables y debe comprobarse que coinciden con los siguientes:
    a) "*Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA-512 (Protocol Integrity), SHA-512 (Files Integrity).*"
    b) "*Successfully connected to Database, Database id 0.*"
    c) "*Firewall is open for client communication.*"
    d) "*Server X.X.X is up*", lo que indica que el componente de la versión X.X.X se ha instalado correctamente.
34. A continuación, se configurará la comunicación con el servidor CA y se obtendrá un certificado de la autoridad certificadora para poder iniciar sesiones seguras. Se debe apagar el servicio *Vault* desde la GUI de *PrivateArk*, y hacer las siguientes modificaciones en los archivos *.ini*:
    a) Abrir el archivo *dbparm.ini*, el cual está localizado en "*C:\Program Files (x86)\PrivateArk\Server\Conf*".
        - Añadir *TLSPort=443* en la sección principal para definir el puerto de sesiones confiadas.
        - Añadir *TrustedCAStoreForTLSClient=[Ruta completa al certificado CA]* en la sección principal. Se deberá exportar el certificado raíz del servidor CA y colocarlo en una ruta accesible al *Vault*. Esta instrucción se da en el siguiente paso (párrafo 35).
        - Añadir *AllowNonStandardFWAddresses=[IP del servidor CA],Yes,80:outbound/tcp* en la sección principal.

NOTA: El servidor puede necesitar que se edite el archivo *%WINDIR%\System32\drivers\etc\hosts* y agregar los detalles del servidor *host* para traducir la IP de la CA.

b) Abrir el archivo *vault.ini*, localizado en "*C:\Program Files (x86)\PrivateArk\Server\Conf*".

- Añadir *TLSPort=443* para definir el puerto de sesiones confiadas.

35. Para continuar, se deberá descargar el certificado de la CA y crear un nuevo certificado para el *Vault* mediante los siguientes pasos. Dicho certificado será utilizado como certificado de servidor en las comunicaciones entre componentes del producto (mediante TLSv1.2) y por el componente PVWA para las conexiones mediante HTTPS:

    1. Parar el servicio de *CyberArk Hardened Windows Firewall* para poder acceder al servidor CA de la organización.
    2. Hacer uso de un navegador para acceder a la CA mediante *https://<CA server IP>/certsrv*.
    3. Obtener el certificado de la CA mediante los siguientes pasos:
        - Hacer clic en *Download a CA certificate, certificate chain, or CRL.*
        - Seleccionar el certificado CA de la lista.
        - Seleccionar el botón *Base64*, y hacer clic en *Download CA Certificate*.
        - Guardar el certificado de la CA en una carpeta local.
    4. Volver a la dirección *https://<CA server IP>/certsrv* para crear un certificado para el *Vault*, este certificado deberá hacer uso de RSA con claves de 3072b o superiores o de ECDSA con curvas P-256 o superiores. Esto se hará con los siguientes pasos:
        - Hacer clic en *Request a certificate*.
        - Hacer clic en *Advanced certificate request*.
        - Hacer clic en *Create and submit a request to this CA*.
        - Elegir una plantilla que tenga un uso de clave mejorado para la autenticación del servidor y un uso para la firma digital y cifrado.
        - Introducir la información para su identificación, **asegurando que el *Subject Name* coincide con la dirección IP del servidor Vault**.
        - Asegurar que esté seleccionada la opción *Create new key set*.
        - Seleccionar la opción de formato *PKCS10*.
        - Hacer clic en *Submit*.
        - Hacer uso del link para instalar el certificado en el servidor Windows.
        - Buscar en *Start Menu* por *Manage user certificates*.

- Expandir la carpeta *Personal* y seleccionar la carpeta *Certificates*.
- Localizar el certificado, hacer clic derecho sobre él y seleccionar *All Tasks > Export*.
- Escoger la clave privada para exportarla.
- Escoger la opción *PKCS#12* junto con el resto de opciones al incluir los certificados y exportar todas las propiedades extendidas.
- Poner una contraseña al archivo.
- Elegir un nombre de archivo y terminar la exportación.

5. Importar el nuevo par de claves al servidor *Vault* con el comando *CACert import /InFile c:\certificates\<certfile.pfx>*. Una vez introducido el comando, requerirá que se introduzca la contraseña que se indicó durante su exportación.
6. Anotar donde se guardan los archivos *pem* y *pvk*. Estas localizaciones han de indicarse en el archivo *dbparm.ini,* en los valores *ServerCertificateFile* y *ServerPrivateKey* respectivamente.
7. Añadir el valor de *TrustedCAPath* al archivo *dbparm.ini* indicando la ruta del certificado de la CA.
8. Crear el almacenamiento de certificados de la CA en el servidor ***Vault*** ejecutando *CACert* para generar el almacenamiento y añadir los ficheros de los certificados CA al mismo. Esto se realiza con el siguiente comando *CACert setca /Add <CAcertificate.cer>*.

36. Para finalizar, se deberá reiniciar el servicio *CyberArk Hardened Windows Firewall* e iniciar el servidor *PrivateArk* desde la GUI.

5.1.3 INSTALACIÓN DE *PRIVATEARK CLIENT*

37. El *PrivateArk Client* es una aplicación de Windows que es usada como el cliente administrativo de la solución PAS, y se debe instalar después de haber realizado la instalación del EPV.
38. A continuación, se indican los pasos necesarios para instalarlo.
    1. Dentro del fichero de instalación de EPV, existe un componente *Client*. Se deberá ejecutar el fichero *setup.exe* de este componente con permisos de administrador.
    2. Se iniciará el *wizard* de instalación, el cual verifica que se encuentren instalados en el dispositivo todos los programas o librerías necesarios. En caso de faltar alguno, el *wizard* mostrará un mensaje de error, en cuyo caso deberá instalarse dicho requisito.
    3. Incluir los detalles necesarios y proseguir escogiendo la ruta de instalación.
    4. Realizar una instalación *Typical* y definir en el cliente el *Vault* a conectar.

5. Hacer clic en OK para definir los detalles del *Vault*.
6. Para la configuración inicial de forma local se instalará el cliente en el mismo servidor que el *Vault*. Posteriormente, se podrá instalar en las ubicaciones deseadas. Se recomienda instalarlo solo en aquellas ubicaciones seguras necesarias para la gestión.

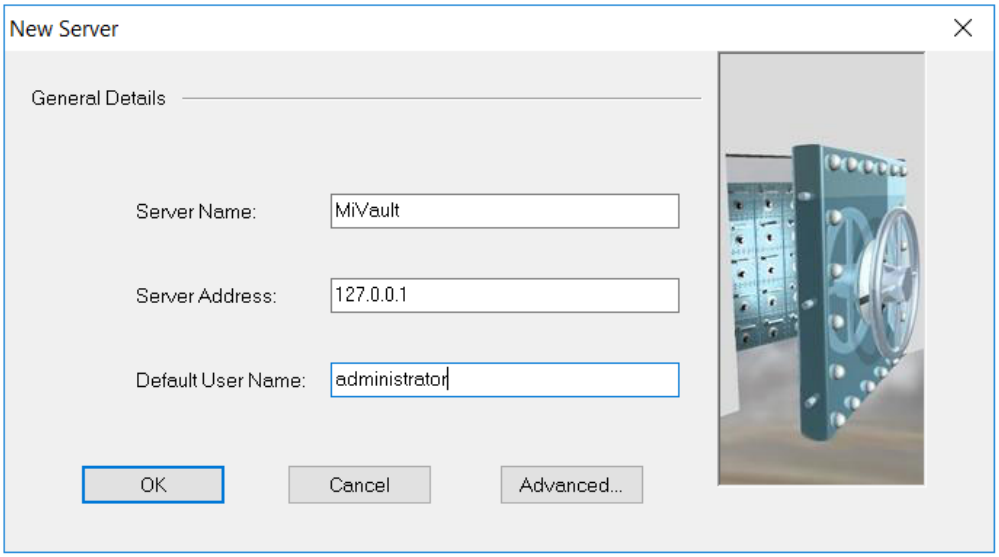


Ilustración 8 – Selección del servidor *Vault*

7. Se reiniciará el servidor y, posteriormente, se comprobará que se puede entrar en el *Vault* con las credenciales creadas anteriormente. Para poder acceder a la funcionalidad recién instalada, será necesario reiniciar el equipo al completo.

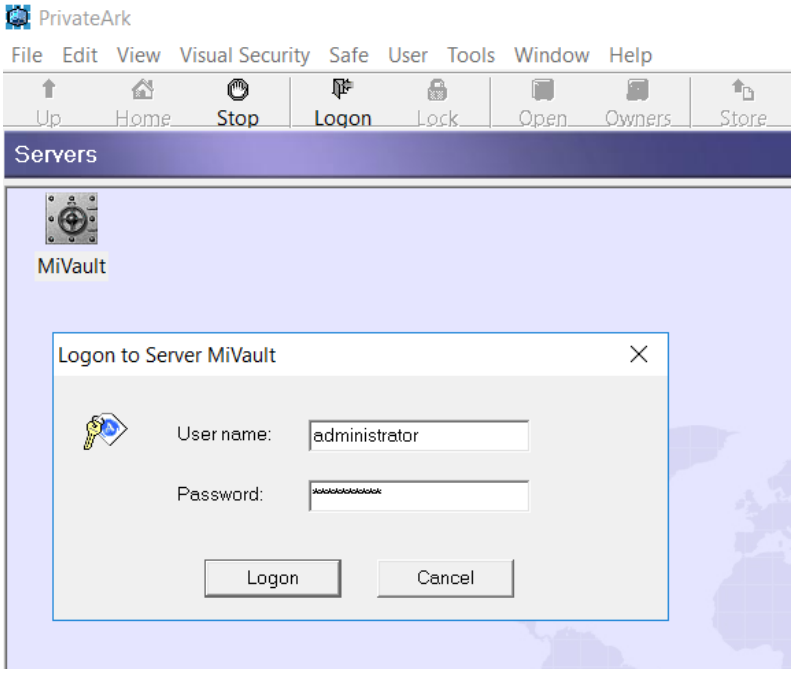


Ilustración 9 – Visualización gráfica del cliente PrivateArk

5.2 INSTALACIÓN CPM

39. La siguiente sección describe los pasos necesarios para instalar el *Central Policy Manager* (CPM), componente que se encarga de rotar las claves y contraseñas según las políticas establecidas.

5.2.1 PASOS INICIALES PARA CONFIGURAR EL SERVIDOR CPM

40. Se deben tener en cuenta aspectos de seguridad a la hora de configurar este servidor. Se deben aplicar políticas estrictas para restringir su acceso físico y lógico, aplicar políticas de monitorización y auditoría. Se debe también realizar el mantenimiento del servidor, instalando los parches de seguridad más actuales de Microsoft. El servidor CPM no deberá tener acceso a Internet ni ser accesible desde ninguna red que se considere insegura dentro de la red organizativa.

41. El servidor debe poder comunicarse con el puerto TCP 1858 del servidor EPV. Es también necesario establecer comunicación con los puertos destinos en las máquinas donde se vaya a gestionar la rotación de claves. Para más información sobre estos puertos de comunicación, se puede consultar la información de este enlace:

    https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20SysReq/Standard%20Ports%20-%20CPM.htm

5.2.2 INSTALACIÓN DEL *SOFTWARE* CPM

42. Se deberá descargar el *software* necesario previo a la instalación del CPM y verificarlo, tal y como se ha indicado en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO.

43. Después, se deberá proceder a la instalación siguiendo los siguientes pasos:

    a) En la máquina destinada a CPM, se deberá crear un directorio y copiar el contenido del archivo de instalación (tendrá un nombre similar a *Central Policy Manager-Rls*). Seguidamente, se deberá ejecutar el *setup.exe* con permisos de administrador.

    b) Se iniciará el *wizard* de instalación, el cual verifica que se encuentren instalados en el dispositivo todos los programas o librerías necesarios. En caso de faltar alguno, el *wizard* mostrará un mensaje de error, en cuyo caso deberá instalarse. También se deberá aceptar la licencia.

    c) Elegir una ruta de instalación.

    d) El instalador preguntará si hay otro CPM instalado. En esta guía se asume que este es el primer CPM a instalar. Se deberá seleccionar *No Policy Manager was previously installed*.

    e) Definir la dirección IP y el puerto de comunicación con el servidor *Vault* (puerto 443).

f) Introducir el usuario y contraseña de *Vault* con permisos administrativos para instalar nuevos componentes (usuario "*administrator*" creado anteriormente).

g) Una vez creado el entorno *Vault*, el instalador pregunta si se quiere instalar el cliente de Oracle. Hacer clic en *No*.

h) Finalizar la instalación y verificar que los siguientes servicios están ejecutándose: *CPM* y *CPM Scanner*.

44. Una vez instalado, **se deberá activar el modo FIPS**, ya que está desactivado por defecto. Para habilitarlo se deberá editar el registro de Windows:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CyberArk Password Manager\ImagePath

45. Se deberá cambiar el valor del registro a:

    "C:\Program Files (x86)\CyberArk\Password Manager\PMEngine.exe" /SERVICE /AdvancedFipsCryptography

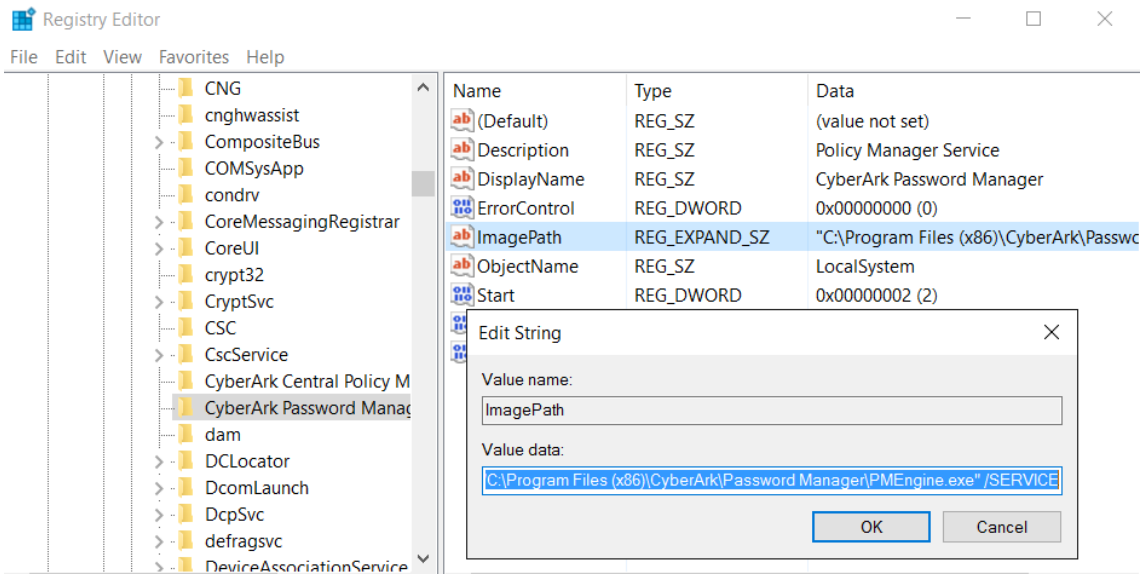


Ilustración 10 – Activación del modo FIPS en CPM

46. Para que se apliquen los cambios, se deberá reiniciar el servidor.

47. Una vez reiniciado el servicio, ir a la carpeta de la aplicación, normalmente ubicada en *C:\inetpub\wwwroot\Passwordvault* y abrir el archivo *web.config* para editarlo y añadir en <appsettings> la siguiente clave:

    <add key="AdvancedFIPSCryptography" value="yes"/>

48. Una vez realizado ese último paso, se deberá reiniciar el servidor CPM.

5.2.3 CREAR ÁREA DE RED CONFIABLE

49. En este apartado se indicará cómo crear un área de red confiable para que el usuario de CPM pueda entrar en el *Vault* solo desde la máquina donde se instaló el *software*. Para realizarlo, se deberán seguir los siguientes pasos:

    1. En el cliente *PrivateArk*, ir a *Tools > Administrative Tools > Network Areas.*

2. Crear una nueva área de red para el componente CPM, tal y como se muestra en la siguiente imagen.

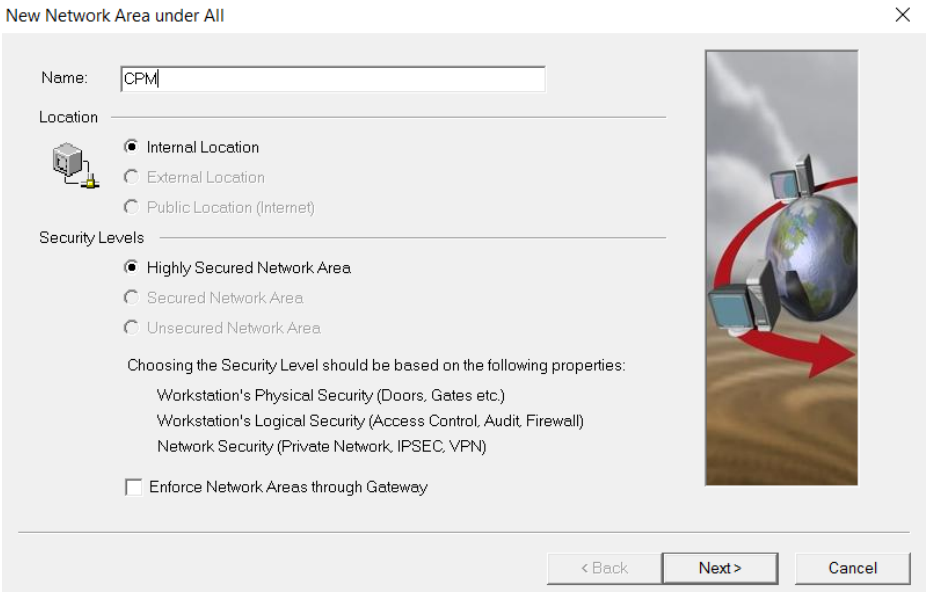


Ilustración 11 – Creación de nueva área de red para CPM

3. Para restringir el uso, se especifica la dirección de la máquina donde se quiere limitar el acceso, con una **máscara de 32**.

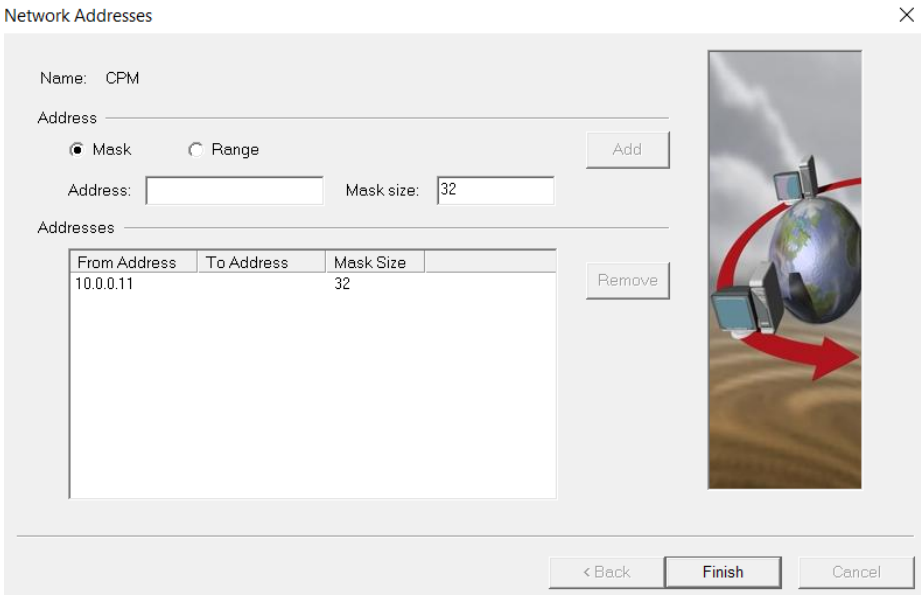


Ilustración 12 – Selección de máscara 32

4. La nueva zona creada cuelga de la zona *All*.
5. En *Tools > Administrative Tools > Users and Groups*, se ha de elegir el usuario relacionado a este componente y pulsar el botón *Trusted Net Areas*.
6. Desactivar el área *All* y agregar la nueva área definido previamente.

7. Reiniciar ambos servicios *CyberArk Password Manager* y *CyberArk Central Policy Manager Scanner* para confirmar que se ha configurado correctamente.

5.2.4 DESHABILITAR DEP PARA LOS FICHEROS UTILIZADOS POR CPM

50. Es necesario agregar excepciones en DEP (*Data Execution Prevention*) para los archivos usados frecuentemente por CPM para prevenir que el sistema operativo bloquee el uso de estos ejecutables necesarios por el producto para su correcto funcionamiento al momento de verificar y rotar contraseñas en sistemas remotos. Para ello se seguirán los siguientes pasos:

    a) Ir a *This PC* y hacer clic con el botón derecho.

    b) Ir a *Properties > Advanced System Settings*.

    c) *En la pestaña Advanced, hacer clic sobre Settings.*

    d) En la pestaña *Data Execution Prevention*, se han de agregar excepciones para los dos siguientes ejecutables:

        - *PMTerminal.exe*
        - *Telnet.exe*
        - *Plink.exe*

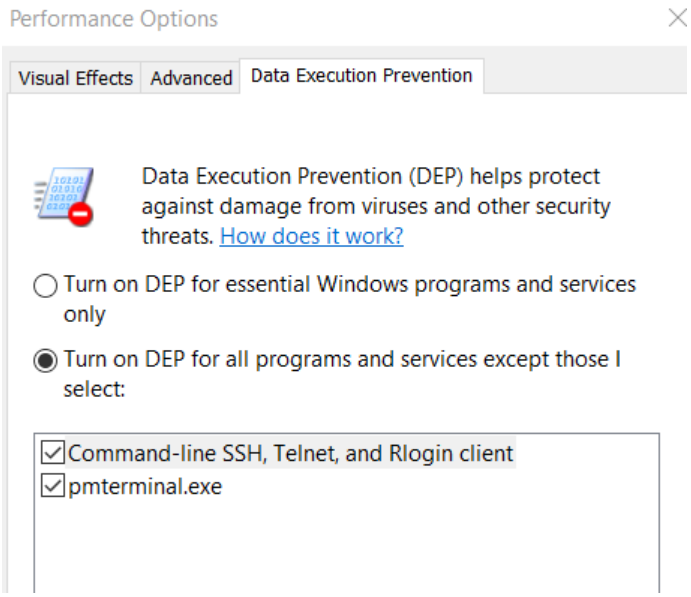


Ilustración 13 – Añadir excepciones en DEP

    e) Reiniciar el servidor para que los cambios tengan efecto.

5.2.5 CONFIGURACIÓN SEGURA DE CPM

Se debe realizar un bastionado (*hardening)* del servidor CPM para asegurar una configuración segura del sistema operativo. Se puede realizar de manera manual o

automática. A continuación, se indica la manera automática, mediante el uso de un *script* proporcionado por CyberArk en el fichero .zip de instalación del componente.

a) Abrir una consola *Powershell* con permisos de administrador.

b) Ir a la carpeta que contiene los archivos de instalación para CPM y acceder al subdirectorio *Automatic_Deploy.*

c) Ejecutar el archivo *CPM_Hardening.ps1.*

d) Reiniciar el servidor.

5.3 INSTALACIÓN PVWA

51. En esta sección se describen los pasos para instalar el servidor destinado a ser el *Password Vault Web Access (PVWA)*. Esta sección asume la instalación de un solo servidor Web. En el caso de haber múltiples PVWA, se requerirá un balanceador por delante.

52. **Se debe instalar un certificado SSL para crear una conexión HTTPS** (tal como se ha visto en el apartado 5.1.2 INSTALACIÓN DEL EPV) y proteger las claves y contraseñas durante la transferencia de datos.

5.3.1 INSTALACIÓN DE PRE-REQUISITOS

53. CyberArk proporciona un *script* para automatizar la configuración de prerrequisitos, necesarios en el sistema operativo de forma previa a la instalación del componente. Este *script* agrega el rol de servidor Web para *Windows Server* y configura el **canal de comunicación segura HTTPS**. Previamente se ha de haber descargado el *software* de la manera indicada en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO.

a) Primero se deberá copiar el archivo de instalación al servidor.

b) Abrir una consola *Powershell* con permisos de administrador.

c) Dentro del directorio de instalación de PVWA, navegar al sub-directorio *Automatic_Deploy*.

d) Ejecutar el comando .*PVWA_Prerequisites.ps1*

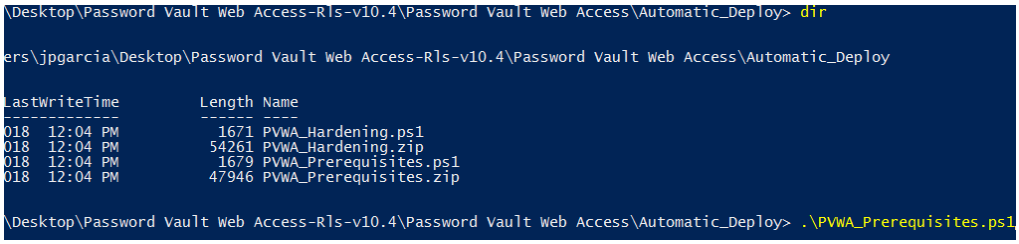


Ilustración 14 – Ejecución de los prerrequisitos de PVWA

5.3.2 INSTALACIÓN DEL *SOFTWARE* PVWA

54. A continuación, se indican los pasos a seguir para instalar el *software* en el servidor destinado a PVWA.

    1. Copiar el archivo de instalación en el servidor donde se va a instalar el componente PVWA.
    2. Navegar al directorio copiado y ejecutar *setup.exe* con permisos de administrador.
    3. Se iniciará el *wizard* de instalación, el cual verifica que se encuentren instalados en el dispositivo todos los programas o librerías necesarios. En caso de faltar alguno, el *wizard* mostrará un mensaje de error, en cuyo caso deberá instalarse dicho requisito.
    4. Introducir los detalles necesarios y la ruta de instalación de *software*. Se recomienda dejar dicha ruta por defecto.
    5. Una vez seleccionada la ruta para la aplicación web, se deberá especificar dónde se instalarán los ficheros de configuración. Se recomienda dejar la ruta de los ficheros por defecto.
    6. En la ventana de *Setup Type*, se recomienda desmarcar la opción de "*Install Mobile Password Vault Web Access*".
    7. Escoger los métodos de autenticación que se deberán instalar para esta plataforma. Se recomienda seleccionar únicamente LDAP y CyberArk.

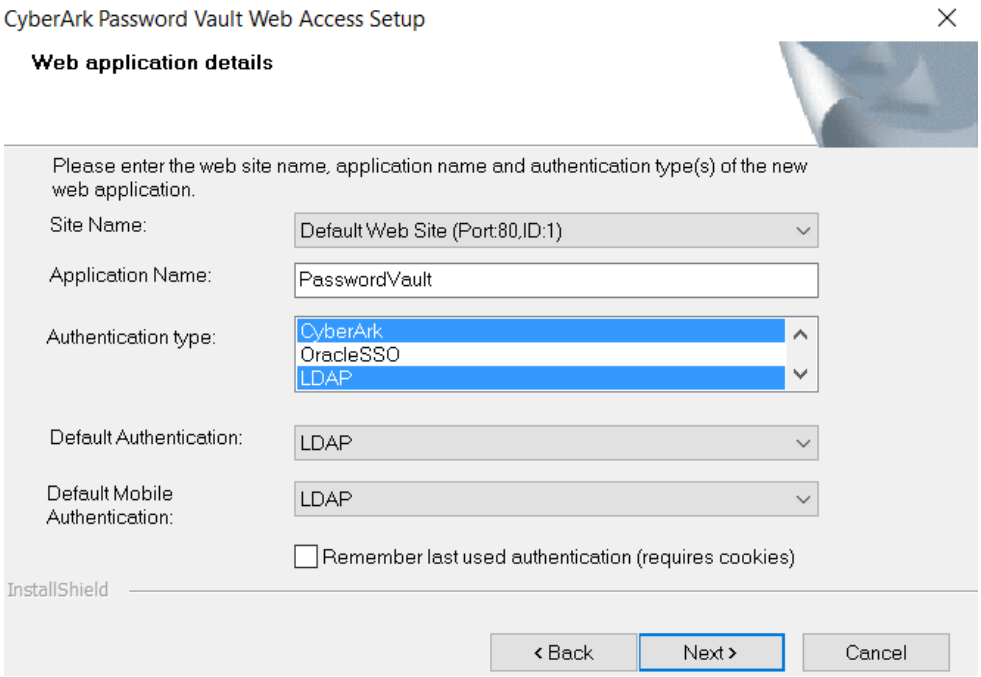


Ilustración 15 – Selección de los servidores de autenticación

    8. Si se ha instalado un certificado SSL, se deberá seleccionar "*Require secure channel (SSL)*".

9. Indicar los detalles de conexión con el *Vault* (dirección IP y puerto 443).
10. En el usuario y contraseña del *Vault*, indicar la del administrador creada anteriormente.
11. Finalizar la instalación.

55. Una vez terminada la instalación, se recomienda usar un navegador e ir a la dirección de PVWA **¡Error! Referencia de hipervínculo no válida.**. Se verá la página de *login* en el caso de haberse instalado correctamente.
56. Además, se recomienda revisar los logs de instalación ubicados en el directorio *C:\Users\{usuario_de_instalación}\AppData\Local\Temp*. Cualquier error creado se especifica en los ficheros de log *PVWAInstallError.log* y *PVWAInstallErrorEnv.log*.

5.3.3 CONFIGURACIÓN SEGURA DE PVWA

57. Una vez finalizada la instalación de PVWA, se debe realizar el *hardening* del servidor para configurar de forma segura del sistema operativo. Para ello, CyberArk proporciona un *script* para automatizar dicho proceso. Los pasos a seguir son los siguientes:
    a) Abrir una consola *Powershell* con permisos de administrador.
    b) Dentro de la carpeta de instalación de PVWA, navegar al directorio *Automatic_Deploy*.
    c) Ejecutar el archivo *PVWA_Hardening.ps1.*
    d) Reiniciar el servidor.
58. Para comprobar que el portal web de acceso funciona, se recomienda navegar a la url *https://{nombre de host}/passwordvault*.

5.4 INSTALACIÓN PSM

59. En esta sección se describen los pasos para instalar el componente dedicado a gestionar las sesiones privilegiadas de la red a proteger. El componente *Privileged Session Manager* (PSM) ayuda a aislar los servidores de los *workstations* para limitar ataques y graba toda la actividad del administrador en máquinas remotas.

5.4.1 CONSIDERACIONES PREVIAS

60. Se deberán revisar los siguientes puntos antes de realizar la instalación:
    a) Verificar que la licencia de CyberArk abarca PSM. Cada instalación de un servidor PSM requiere estar licenciada. Esta información se incluye en la licencia instalada al principio de la guía. Se recomienda verificar que la licencia indica el número de servidores que se tiene intención de instalar.
    b) Para la conexión desde *Microsoft Remote Desktop Services (RDS) Session Host* al PSM se deberá disponer de licencias RDS CAL apropiadas (adquiridas por separado con *Microsoft*) para la conexión remota a terminales Windows

por RDP. Deberá estar presente un servidor de licencias *Remote Desktop* al que se pueda conectar el servidor PSM para que se gestionen las licencias según se conecten los usuarios (*https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-install-cals*).

c) El entorno puede contar con múltiples instancias de PSM para trabajar en conjunto con un solo *Vault*. Esto permite poder balancear la carga entre los distintos PSM o simplemente trabajar con distintas redes segmentadas del entorno.

d) En la configuración del *firewall* de Windows, se deben habilitar las reglas *"File and Printer Sharing (NV-Session-In)"* y *"File and Printer Sharing (SMB-In)"*.

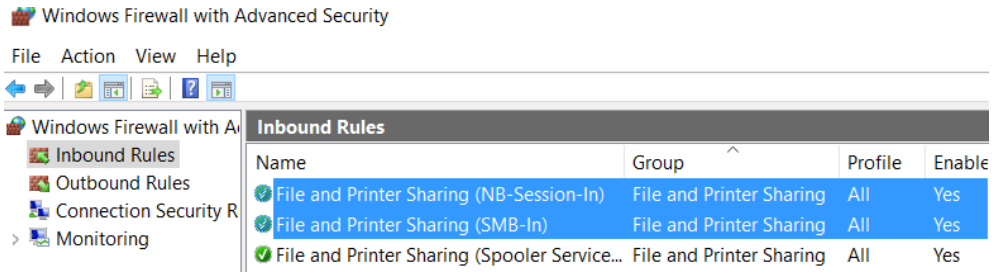


Ilustración 16 – Reglas del cortafuegos a habilitar

5.4.2 INSTALACIÓN DE PRERREQUISITOS

61. 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. Es importante tener en cuenta que se deberá instalar el componente PSM en una máquina diferente a la del *Vault*.

62. Antes de iniciar la instalación, será necesario instalar los prerrequisitos del *software*. A continuación, se indican los pasos a seguir:

    1. Copiar el contenido del archivo de instalación al servidor donde se va a instalar el componente PSM.
    2. Dentro del directorio, navegar a:

       {Directorio_con_instalador}\InstallationAutomation\Prerrequisites.
    3. Editar el fichero *PrerequisitesConfig.xml*.
    4. En dicho fichero se indica mediante la variable *Enable=Yes*, los pasos que se llevarán a cabo. Si se desea, los pasos correspondientes a RDS y .NET 4.5.2 se pueden desactivar para realizar su instalación manualmente.

```
<Stage Name="Prerequisites" version="1.0">
    <!-- The following step verifies that .NET 4.5.2 (or above) is installed
    on the PSM machine  -->
    <Step Name="InstallDotNet" DisplayName="Install the .NET 4.5.2 package"
    ScriptName="InstallDotNet.psm1"  Enable="Yes" />
    <!-- The following step installs the RDS rules the PSM machine -->
    <Step Name="InstallRDS" DisplayName="Install RDS rules" ScriptName=
    "InstallRDS.psm1"  Enable="Yes" />
  <!-- The following step disables the NLA authentication on the PSM
  machine  -->
  <Step Name="DisableNLA" DisplayName="Disable NLA authentication" ScriptName
  ="DisableNLA.psm1"  Enable="No" />
  <!-- The following step updates the RDS security layer on the PSM machine
  to 1 - negotiate  -->
  <Step Name="UpdateRDSSecurityLayer" DisplayName="Update RDS security layer"
   ScriptName="UpdateRDSSecurityLayer.psm1"  Enable="No" />
</Stage>
```

Ilustración 17 – Fichero *PrerequisitesConfig.xml* de PSM

5. Abrir una consola *Powershell* con permisos de administrador.
6. Se deberán ejecutar los siguientes comandos:
   - *cd {Directorio_con_instalador}\InstallationAutomation*
   - *.\Execute-Stage.ps1 "C:{RUTA ABSOLUTA A INSTALADOR}\InstallationAutomation\Prerequisites\PrerequisitesConfig.xml"*
7. Al finalizar, se deberá reiniciar el sistema para que se ejecuten los cambios.

5.4.3 INSTALACIÓN DEL *SOFTWARE* PSM CON *WIZARD*

63. Una vez descargado, se deberán seguir los siguientes pasos a través de *Wizard*, interfaz gráfica para la instalación del componente:
    1. Navegar al directorio copiado y ejecutar *setup.exe* con permisos de administrador.
    2. Se iniciará el *wizard* de instalación, el cual verifica que se encuentren instalados en el dispositivo todos los programas o librerías necesarios. En caso de faltar alguno, el *wizard* mostrará un mensaje de error, en cuyo caso deberá instalarse.
    3. En la página *Customer Information*, introducir los datos necesarios.
    4. En *Destination Location*, se recomienda dejar el valor por defecto para la ruta de instalación.
    5. En *Recordings Folder,* se recomienda dejar por defecto el valor de la ruta donde se almacenarán las grabaciones de videos de sesión.
    6. Si se va a realizar la instalación de múltiples PSM, se deberá asegurar que el directorio de instalación y el directorio para las grabaciones son los mismos en todas las instancias.
    7. En *Password Vault Web Access Environment,* se recomienda dejar el *Safe* por defecto. Este *Safe* será donde se almacenen las configuraciones Web.

8. En *Vault's Connection Details* se deben introducir la dirección IP y puerto (443) del *Vault*.
9. En la siguiente página se deberá introducir el nombre y contraseña del usuario administrador del *Vault*.

64. Al finalizar la instalación, se deberá reiniciar el servidor para que los cambios tomen efecto.

5.4.4 POST-INSTALACIÓN DE PSM

65. Para finalizar la instalación, se deberán seguir las siguientes instrucciones:
    a) Acceder al componente como administrador.
    b) Editar el fichero:

    {Directorio_con_instalador}\InstallationAutomation\PostInstallation\PostInstallationConfig.xml.

    c) Habilitar los pasos deseados modificando el valor de la variable *Enable* a *Yes*. Los valores por defecto deshabilitan aplicaciones Web y comparten servicios de impresión. En esta ocasión, basta revisar que esté deshabilitado el salvapantallas para los usuarios locales *PSMConnect y PSMAdminConnect.*
    d) Abrir una consola *Powershell* con un usuario administrador.
    e) Ejecutar los siguientes comandos:
        - *cd {Directorio_con_instalador}\InstallationAutomation*
        - *.\Execute-Stage.ps1 "C:\{RUTA ABSOLUTA A INSTALADOR}\InstallationAutomation\PostInstallation\PostInstallationConfig.xml"*.

    f) Opcionalmente, si hay usuarios de mantenimiento que deban entrar remotamente al servidor PSM, estos deben ser miembros del grupo *RemoteDesktopUsers.* Además, habrá que otorgarles el permiso *Allow log on through Remote Desktop Services* en la política de seguridad de *Windows*.

5.4.5 CONFIGURACIÓN SEGURA DE PSM

66. Para proceder con el proceso de *hardening* del servidor para asegurar una configuración segura del sistema operativo, se deben seguir los siguientes pasos:
    a) Editar el fichero *{Directorio_con_instalador}\InstallationAutomation\Hardening\HardeningConfig.xml*
    b) Editar el valor de la variable *Enable* a *Yes*:
        - Se recomienda dejar deshabilitados los sub-parámetros *SupportWebApplications* y *ClearRemoteDesktopUsers.*
        - Bloquear las herramientas de desarrollador en IE y esconder los discos del PSM durante la gestión de sesiones.

- Prohibir la ejecución de ficheros no autorizados.

c) Si es necesario autorizar aplicaciones, editar el fichero *C:\Program Files (x86)\CyberArk\PSM\Hardening\PSMConfigureAppLocker.xml* antes de ejecutar el *script* de *hardening*. Este fichero controla las aplicaciones que se pueden ejecutar en este entorno. Si se quiere integrar plataformas Web, por ejemplo, se pueden descomentar las secciones relevantes a *Google Chrome* y *Microsoft Internet Explorer*.

d) Abrir una consola *Powershell* con permisos de administrador y ejecutar los siguientes comandos:

- *cd {Directorio_con_instalador}\InstallationAutomation*
- *.\Execute-Stage.ps1 "C:{RUTA ABSOLUTA A INSTALADOR}\InstallationAutomation\Hardening\HardeningConfig.xml"*

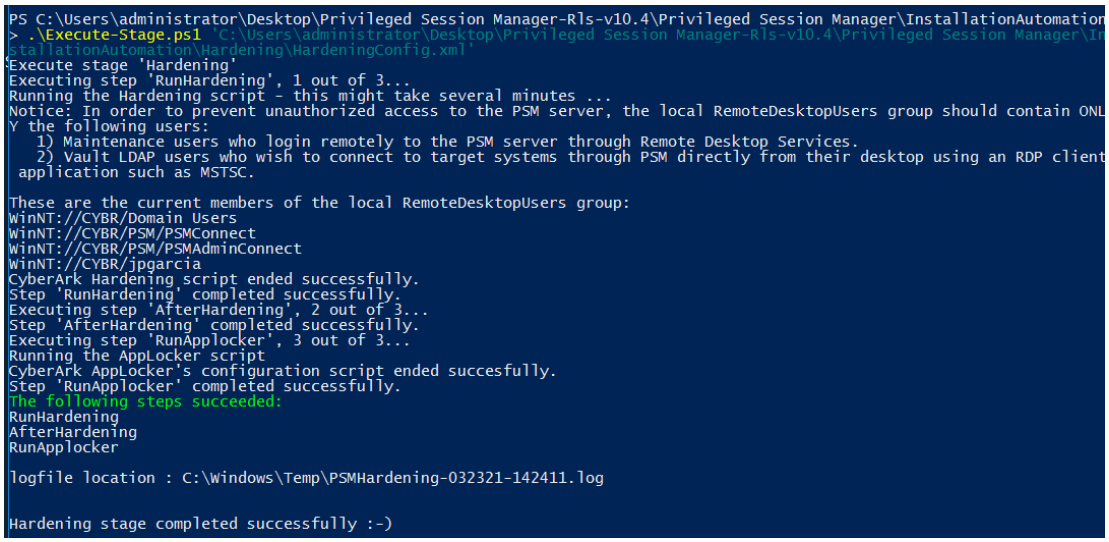


Ilustración 18 – Proceso de configuración segura de PSM

5.5 INSTALACIÓN PSM PARA SSH

67. 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.

5.5.1 CREAR USUARIO ADMINISTRATIVO PARA SERVIDOR PSMP

68. 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.*

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

70. 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.

5.5.2 HABILITAR SELINUX

71. 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:

    1. Para habilitar SELINUX en Redhat 7.x, siga las indicaciones en este enlace:

       https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-working_with_selinux-changing_selinux_modes#sect-Security-Enhanced_Linux-Enabling_SELinux-

5.5.3 INSTALACIÓN DE PSMP

72. 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. Recordar que PSMP se instalará sobre una máquina con sistema operativo Linux.

73. Se continua 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 CyberArk 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*.

     NOTA: En el caso de una implementación de alta disponibilidad o de recuperación de desastres, se puede especificar más de una dirección de *Vault*, separadas mediante comas. Por ejemplo: *Address=1.1.1.102,1.1.1.232.* La primera dirección será la utilizada al crear el entorno de PSMP durante la instalación.
   - 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 6.4.1 CERTIFICADOS PERSONALES PARA AUTENTICACION 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 CyberArk.
   - 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.

5.5.4 POST-INSTALACIÓN

74. 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) Se puede integrar PSMP con LDAP. Para más información sobre este aspecto, se recomienda ir al siguiente enlace:

    https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/10.10/en/Content/PAS%20INST/Configuring-User-Management-via-LDAP.htm

    c) 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

75. **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, sin embargo, el componente EPV cuenta con el modo FIPS activado por defecto.

76. Para los componentes Windows, es decir, CPM, PSM y PVWA, 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 CPM, se activa el modo FIPS durante su configuración para que se utilicen protocolos seguros en sesiones a máquinas objetivo.

77. Para los componentes Linux, es decir, PSMP y OPM, se han de realizar los siguientes pasos para habilitar FIPS:

    a) Para PSMP:

        - 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.

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

79. 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).

6.2 AUTENTICACIÓN

80. Para el acceso al *Vault* se requiere de un mecanismo de autenticación que verifique los usuarios que se conectan a él. Este está basado en contraseñas, certificados PKI, *tokens RSA SecurID* (desde PVWA), RADIUS, *tokens* USB o autenticación Windows (es decir, tras acceder al sistema operativo no será necesario autenticarse además en CyberArk). Además, también se soporta la integración con métodos de autenticación externos, como LDAP.

81. Además de los métodos de autenticación indicados, 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: autenticación NT/Windows, autenticación con RSA SecurID (desde PVWA), certificado PKI, SSO de Oracle (desde PVWA) y SAML. Además, se permite el uso de

RADIUS, LDAP o la autenticación de CyberArk, como segundo factor de autenticación.

82. La autenticación de usuarios se puede realizar las siguientes maneras:

    a) **Contraseña almacenada en CyberArk (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. CyberArk es compatible con:

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

    c) **Autenticación Windows**: Se puede configurar la característica de autenticación de Windows. Esto habilita que el usuario acceda a CyberArk sin realizar el procedimiento de validación de usuario, una vez que el usuario se haya autenticado ante Windows. No se recomienda el uso de esta opción.

    d) **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.

    e) **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.

    f) **RSA SecurID**: La solución de SecurID puede utilizarse para el método de autenticación primaria en PVWA.

    g) **PKI**: Infraestructuras de claves públicas (o PKI por sus siglas en inglés de *Public Key Infrastructure*) permite el uso de certificados para que servidores y usuarios se identifiquen entre sí y establezcan una conexión segura. Opcionalmente, se puede además solicitar a los usuarios que proporcionen una autenticación adicional por contraseña cuando inician sesión en CyberArk a través de PVWA.

    h) **Google**: Autenticación por Google permite a los usuarios validarse en CyberArk con una cuenta pre-definida de Google, de acuerdo a la política organizacional.

    i) **Oracle SSO**: El vault de CyberArk puede trabajar con *Oracle Identity Management.* Este permite a las empresas gestionar los ciclos de vida, de principio a fin, para todos los usuarios de los sistemas de red.

83. Cada componente de la solución se comunica únicamente con el EPV y con la autoridad certificadora (CA) (ver apartado 5.1.2 INSTALACIÓN DEL EPV). Cuando un componente se comunica con el EPV, realiza la validación del certificado X.509 del EPV durante la autenticación TLS.

6.2.1 CONFIGURACIÓN DE LA AUTENTICACIÓN

84. Para llevar a cabo la configuración del método de autenticación deseado, se recomienda consultar los detalles específicos en el siguiente enlace a la documentación pública del producto.

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

    a) Primero, será necesario configurar la cuenta de usuario. Para ello, desde *PrivateArk Client*, desplegar las propiedades del usuario deseado e ir a la pestaña *Authentication*.

    b) En el menú desplegable, seleccionar el método deseado de los vistos anteriormente y hacer clic en *OK*.

    c) Tras esto, es necesario configurar la autenticación en el módulo PVWA. Para ello ir a *Administration > System Configuration > Options*, expandir el desplegable *Authentication Methods* y seleccionar el método deseado. Hacer clic en *Apply*.

    d) Por último, es necesario configurar la autenticación desde PrivateArk Client. Para ello, desde el cliente, ir a *Properties > Advanced*. En el desplegable seleccionar la opción deseada y hacer clic en *OK*.

6.2.2 CONFIGURACIÓN DE LDAP

86. A modo de ejemplo y debido a que es el método de autenticación recomendado, se muestra el proceso de configuración completo para el caso de LDAP.

87. Se deberá configurar un usuario en el directorio LDAP para permitir que *Vault* acceda con permisos de lectura y pueda obtener la información necesaria.

88. Una vez creado dicho usuario de "solo lectura" (por ejemplo*, cyberark-lectura@midominio.loc*), se deben otorgar los permisos necesarios a este usuario para leer de las unidades organizativas que contienen los usuarios y grupos que requieran acceso al *Vault*.

6.2.2.1 USO DE LDAP CON CERTIFICADO SSL EN EL VAULT

89. En la máquina *Vault* (servidor EPV), se deberá importar el certificado de la CA que firmó el certificado utilizado por el directorio LDAP externo en el almacén de certificados de Windows. Las siguientes indicaciones describen los pasos necesarios para este fin:

1. En la máquina con EPV instalado, abrir una nueva ventana para *Microsoft Management Console* y agregar un nuevo *Snap-in* para la gestión de certificados en ordenador local. En la consola de MMC, seleccionar *File -> Add/Remove Snap-in…*

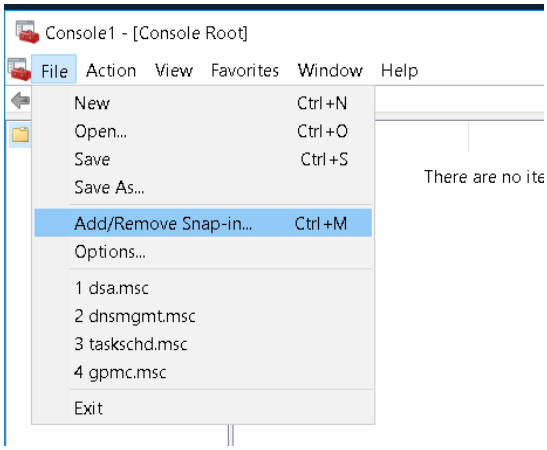


Ilustración 19 – Agregar *Snap-in* para gestión de certificados en MMC

2. Saldrá un nuevo dialogo donde se deberá elegir *Certificates* y presionar en el botón '*Add >*' para agregar el snap-in.

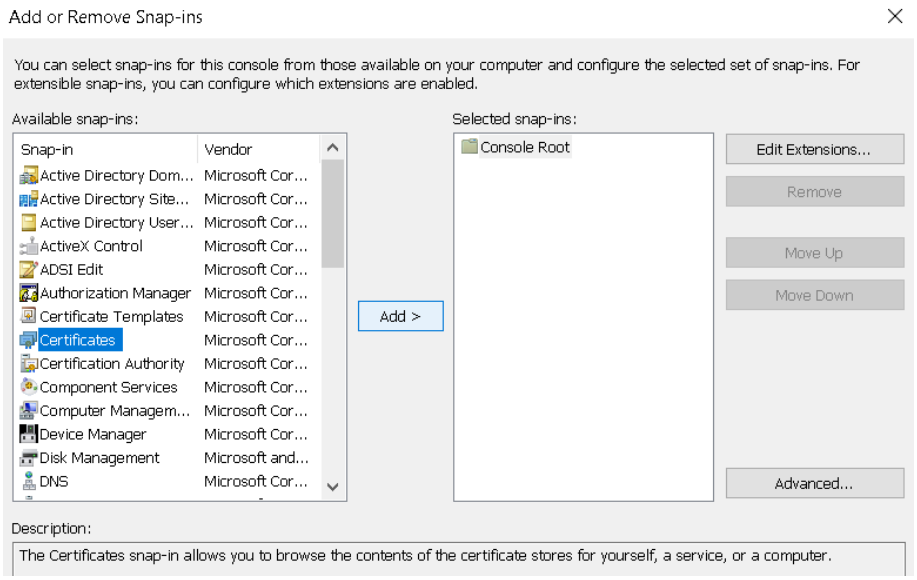


Ilustración 20 – Agregar *Snap-in* para gestión de certificados en MMC

3. Aparecerá un nuevo dialogo donde se deberá elegir *Computer account* para especificar que se quieren gestionar certificados para el ordenador.

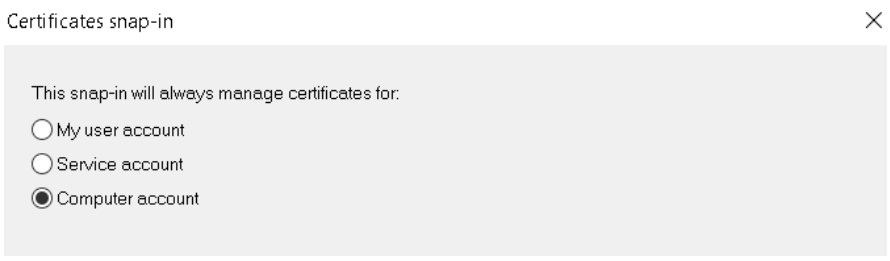


Ilustración 21 – Agregar *Snap-in* para gestión de certificados en MMC

4. En el siguiente paso del dialogo, especificar que se quieren gestionar los certificados del ordenador local.

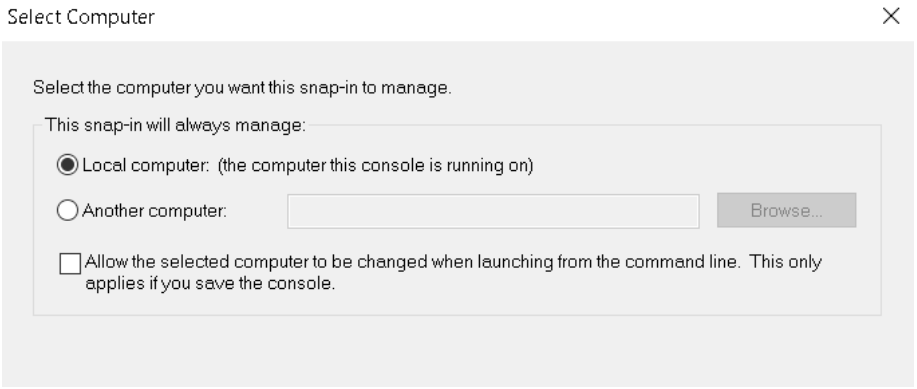


Ilustración 22 – Agregar *Snap-in* para gestión de certificados en MMC

5. En *Certificates (Local Computer) > Trusted Root Certification Authorities*; aparece la carpeta *Certificates* donde se importarán los certificados.
6. Hacer clic con el botón derecho sobre el directorio *Certificates*. Seleccionar *All Tasks > Import* y aparecerá un asistente de importación de certificados.

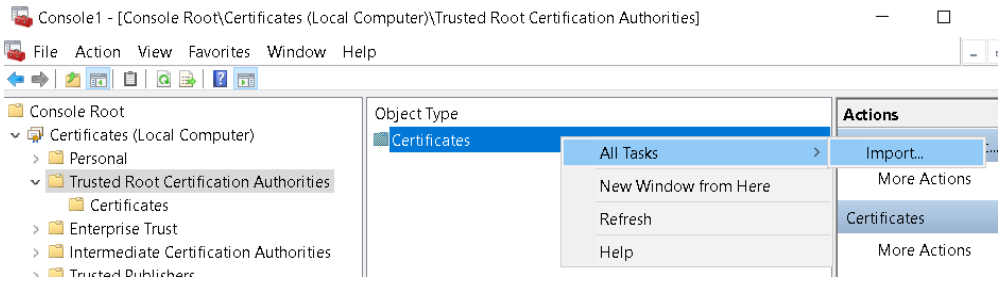


Ilustración 23 – Importar certificados

7. Hacer clic en *Next* y seleccionar el certificado a importar. Hacer clic en *Next* y aparecerá la ventana de *Certificate Store***.**
8. Seleccionar *Place all certificates in the following store*, y hacer clic en *Next***.**
9. Una vez terminado la importación del certificado, hacer clic en *Next*. El certificado seleccionado se importa a la cuenta del ordenador y ahora se puede usar para autenticar usuarios externos en *CyberArk Vault*.
10. Por defecto, el *Vault* establece automáticamente el *Distinguished Name* de los usuarios externos. Si el usuario tiene un certificado en el directorio, el atributo DN se tomará del certificado. De lo contrario, se establecerá el DN de usuario en el directorio.
11. Para especificar el DN de usuario manualmente con el cliente *PrivateArk*, se deberá editar el fichero Directory.ini y especificar el siguiente parámetro: *UseLDAPCertificatesOnly=no*.

12. En el fichero *%systremroot%\System32\Drivers\Etc\hosts* del *Vault*, definir el host DNS del servidor LDAP.

6.2.2.2 INTEGRACIÓN LDAP EN PVWA

90. Para que los usuarios se puedan autenticar en LDAP, hay que definir los detalles del directorio a utilizar. Para ello se deberá entrar en el portal de PVWA como administrador y realizar los siguientes pasos:

    1. Hacer clic en *Administration* > *Configuration Options* y presionar sobre el enlace de *Setup Wizard*.

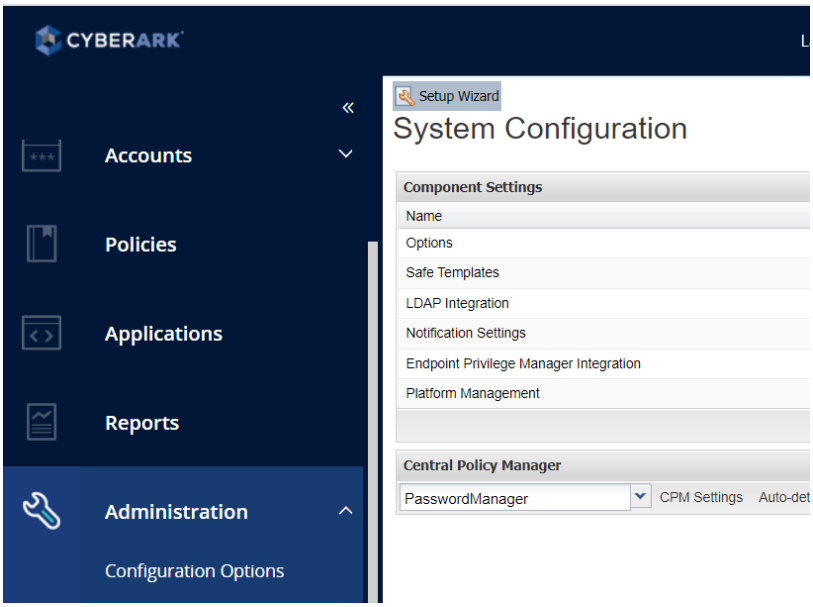


Ilustración 24 – Botón de *Setup Wizard*

    2. Seleccionar la opción de integrar un directorio LDAP y especificar los detalles de integración como se muestra a continuación en las siguientes imágenes:

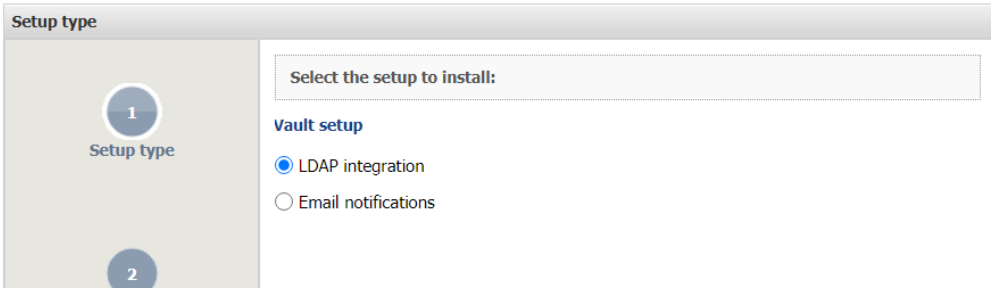


Ilustración 25 – Integración de LDAP en PVWA

    3. Aparecerá un dialogo de configuración donde se deberá especificar:

        - *Name*: Nombre del directorio LDAP.
        - *Directory Type*: Se debe especificar uno de los perfiles del directorio LDAP a utilizar. Habrá que elegir uno de los siguientes perfiles en base al servidor LDAP que se posea:

a. IBMTdsProfile.ini
b. MicrosoftADProfile.ini
c. OracleProfile.ini
d. SunOneProfile.ini
e. eDirectoryProfile.ini

- *Address*: Dirección IP o *hostname* del servidor LDAP
- *Port*: El puerto a utilizar. En este caso 636 para utilizar LDAPS
- *LDAP Bind User*: El usuario de solo lectura que se pide crear al principio para poder leer el directorio LDAP y obtener detalles de los objetos almacenados ahí.
- *LDAP Bind Password*: Contraseña del usuario anteriormente puesto.
- *LDAP Base Context*: El contexto base o raíz escrito con la notación para objetos LDAP.

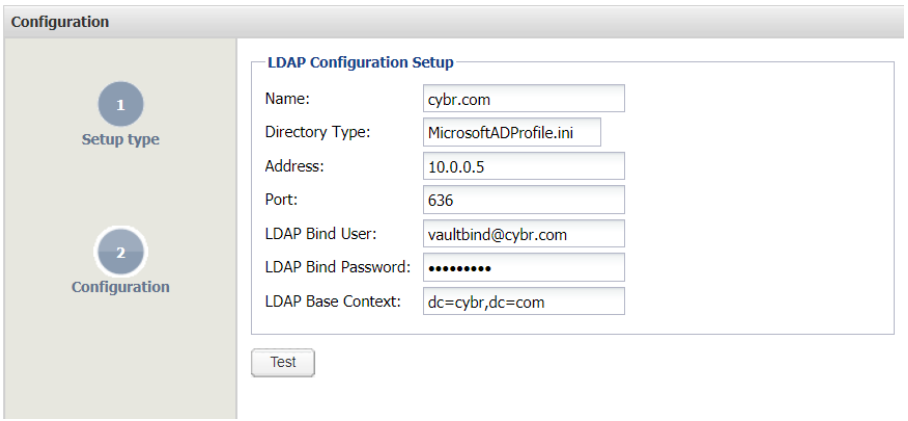


Ilustración 26 – Datos de configuración de LDAP

4. Presionar el botón *Test* y realizar la prueba de conectividad.

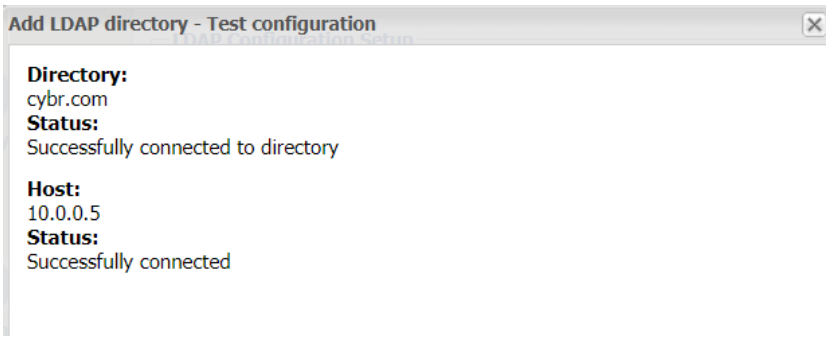


Ilustración 27 – Realización de test de conectividad con LDAP

5. En la siguiente ventana, simplemente presionar el botón *Finish* para finalizar el proceso y confirmar que no se quiere configurar los *mappings* por defecto.

6.2.2.3 MAPEAR USUARIOS CYBERARK AL DIRECTORIO LDAP

91. Para poder autenticar usuarios en el portal Web utilizando un directorio LDAP, se deberá crear un *directory mapping*, que permite al *Vault* localizar al usuario en el directorio de la organización. Para otorgar permisos al usuario:

    1. Utilizando el cliente de *PrivateArk*, entrar en el *Vault* con el usuario administrador y seleccionar *Tools > Administrative Tools > Directory Mapping***.**

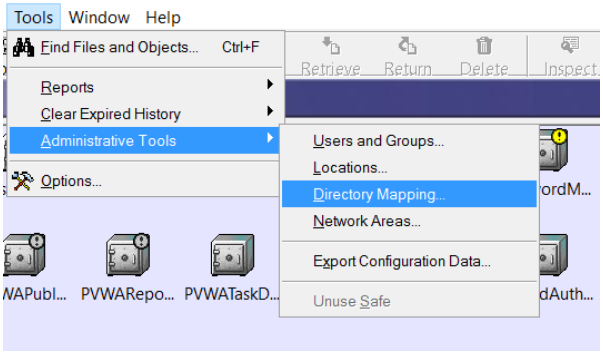


Ilustración 28 – Mapeo de usuarios LDAP

    2. Agregar un nuevo *directory mapping* haciendo clic en el botón *Add***.**
    3. Posteriormente, agregar una regla para mapear este grupo a alguna unidad organizativa de LDAP que contenga los usuarios del dominio.

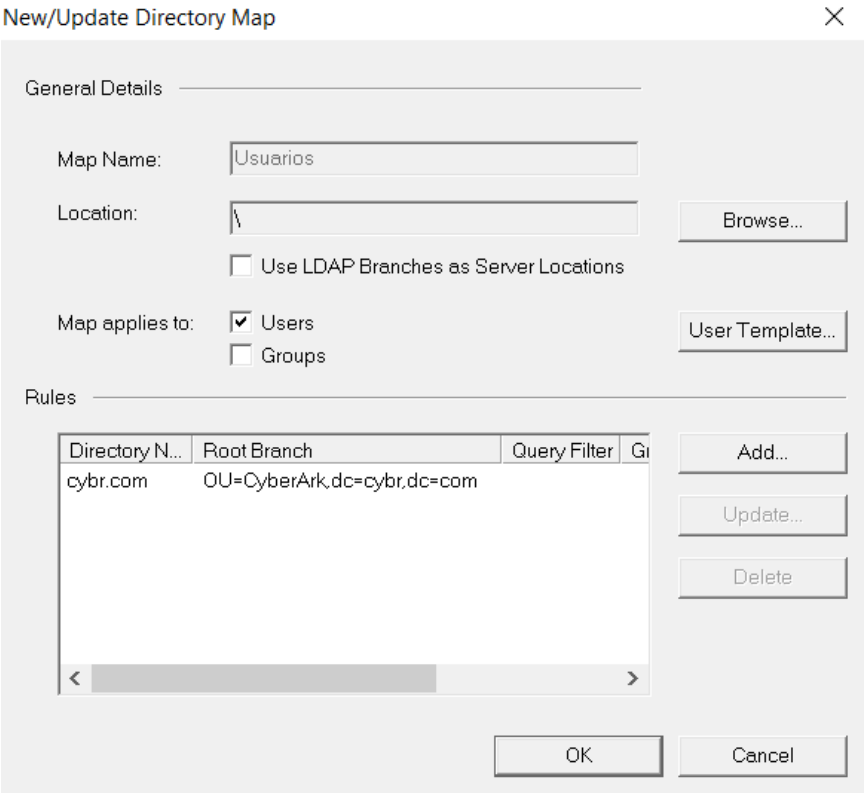


Ilustración 29 – Creación de regla de mapeo

NOTA: De la misma manera que se ha definido una unidad organizativa para usuarios, se recomienda especificar un *directory mapping* a una unidad organizativa específica para auditores y administradores de *Vault*.

4. Seleccionar el botón *User Template*, lo cual abrirá una nueva ventana donde se podrán definir los permisos del grupo/usuarios en la pestaña *Authorizations*.
5. Ahora solo queda realizar la prueba de que se puede validar con un usuario de la organización en CyberArk. Cuando se valida por primera vez, CyberArk creará el usuario en el Vault de manera automática.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

92. El producto permite la **administración local** mediante el acceso al sistema operativo Windows que tenga el *Vault* instalado. Además de poder editar los ficheros locales como *vault.ini*, que determinan el comportamiento del *Vault*, se pueden utilizar uno de los dos (2) clientes previamente instalados:

    - *PrivateArk Server Management Console*: Esta consola (instalada con el producto de forma automática) permite verificar el estado del servicio del *Vault* además de permitir parar/iniciar el servicio en sí.
    - *PrivateArk Client*: El cliente *PrivateArk* (ver apartado 5.1.3 INSTALACIÓN DE *PRIVATEARK CLIENT*) es una consola mínima que permite la gestión del *Vault*. Este cliente será utilizado, entre otras cosas, para agregar usuarios y gestionar el tipo de autenticación que deberán utilizar. El cliente también se utiliza para visualizar los distintos *Safe* que el producto crea para funcionamiento propio y de aquellos *Safe* que se crean para almacenar los objetos usuario con sus claves asociadas.

93. La **gestión remota** del producto se puede realizar de las siguientes formas:

    - Mediante la instalación de *PrivateArk Client* en una estación de trabajo para realizar la conexión con *Vault* de forma remota (ver apartado 5.1.3 INSTALACIÓN DE *PRIVATEARK CLIENT*). Estas comunicaciones se realizan con TLSv1.2 por defecto y no son configurables.
    - Mediante PSM, el cual incluye un componente de conexión con PrivateArk para gestionar el *Vault* de manera que se pueda grabar la sesión (ver apartado 5.4 INSTALACIÓN PSM). Estas comunicaciones se realizan con TLSv1.2 por defecto y no son configurables.
    - Mediante la autenticación en PVWA (Servidor Web, ver apartado 5.3 INSTALACIÓN PVWA). Estas comunicaciones se realizan con TLSv1.2 por defecto y no son configurables.

94. Varias operaciones de gestión se deberán realizar a través de PVWA. El usuario administrador de CyberArk (administrator) se puede conectar por PVWA utilizando

su contraseña almacenada en CyberArk. La interfaz de gestión en CyberArk mediante PVWA 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 CyberArk deberá conectarse para configurar funcionalidades (ejemplo: servidores LDAP, *ticketing* y balanceadores de carga).

95. Opcionalmente, si se desea gestionar el Vault de manera remota y por línea de comando, como alternativa al cliente *PrivateArk*, se puede utilizar *Remote Control Client.* Este provee una interfaz por línea de comando y ejecuta las tareas en el Vault donde previamente se ha instalado *Remote Control Agent.*

96. 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 POLÍTICA DE CONTRASEÑAS

97. 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.

98. La configuración de la política de contraseñas del producto se realiza desde el fichero *PassParn.*ini. Para la protección adecuada del producto frente a usuarios no autorizados, se deben seguir las siguientes instrucciones:

    a) Acceder a *Vault* con privilegios de administrador.

    b) Editar el archivo *C:\Program Files (x86)\PrivateArk\Server\passparm.ini* siguiendo las siguientes recomendaciones:

        - Configurar con *Yes* el parámetro *CheckUserName*, para prevenir que se pueda utilizar el nombre de usuario en la contraseña.
        - Configurar con, al menos, uno (1) el parámetro *MinAlphabetic*, para exigir el uso de, mínimo, una letra.
        - Configurar con *Yes* el parámetro *MustMixCase*, para exigir el uso de letras mayúsculas y minúsculas.
        - Configurar con, al menos, uno (1) el parámetro *MinNumeric*, para exigir el uso de un número, como mínimo.
        - Configurar con, al menos, uno (1) el parámetro *MinPunctuation*, para exigir el uso de mínimo un carácter especial. Adicionalmente deberá configurarse el parámetro *PunctuationCharacters* con los caracteres especiales permitidos.
        - Configurar con, al menos, doce (12) el parámetro *MinLength*, para exigir el uso de contraseñas de una longitud mínima de 12 caracteres.

- Configurar el parámetro *DaysForPasswordExpiration*, con el valor en días tras el cual será necesario cambiar la contraseña. Se recomienda un valor no superior a 60 días.
- El parámetro *PaswordsRemembered* permite evitar la reutilización del número configurado de contraseñas pasadas. Se recomienda un valor mínimo de 5.
- El parámetro *MinAge* representa el número mínimo de días tras el cual se permite un nuevo cambio de contraseña, para evitar ataques de fuerza bruta. Se recomienda un valor mínimo de 3 días.

c) En caso de modificar el fichero, se deberá reiniciar el servidor *PrivateArk Server*, para que se actualicen los cambios en la política.

99. 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 CyberArk 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 CyberArk: Unix vía SSH).

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

a) Entrar en PVWA como usuario administrador de CyberArk.

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 CyberArk. 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.

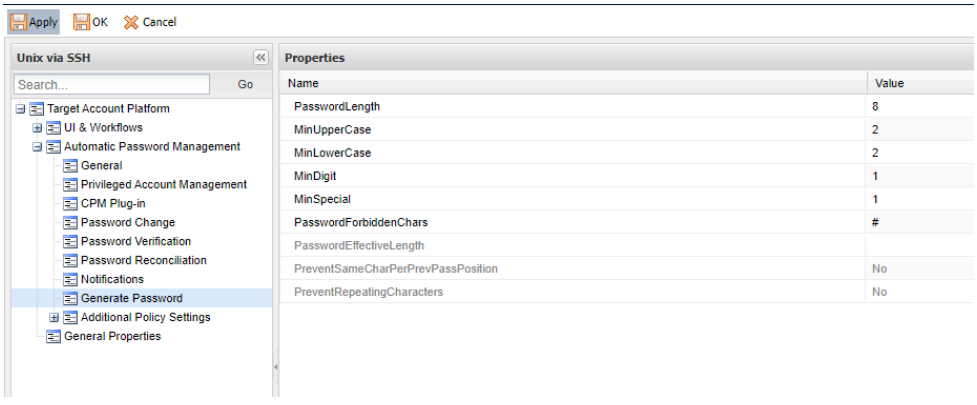


Ilustración 30 – Configurar política de contraseña en sistemas remotos gestionados

6.3.3 CONFIGURACIÓN DE ADMINISTRADORES

101. El producto cuenta con dos (2) usuarios administradores creados por defecto. El más importante es el usuario *Master*. Este usuario solo se puede utilizar conjuntamente con la clave criptográfica (llamada clave *master*) para garantizar la cadena de custodia. Se trata de un usuario para casos de emergencia, por lo tanto, tiene acceso completo en el *Vault* y se puede utilizar para reiniciar la contraseña de otros usuarios, además de recuperar los contenidos del *Vault* cifrado.

102. El usuario *Master* es el que puede descifrar el sistema entero, y puede realizar recuperaciones completas, siempre que sea necesario. Solo puede acceder al Vault a través del terminal del servidor. Para acceder, se deben utilizar las credenciales de usuario creadas durante la 5.1.2 INSTALACIÓN DEL EPV y para realizar las acciones de descifrado del *Vault* se requiere, adicionalmente, la clave Master.

103. El segundo usuario por defecto que se crea durante el proceso de instalación es *Administrator*. Este usuario se utilizaría para toda operación de configuración del *Vault*.

104. El producto permite crear nuevos usuarios administrativos con acceso al *Vault*, y con las autorizaciones que se deseen. Para dicha creación se han de seguir los siguientes pasos:

    a) En *PrivateArk*, como un usuario administrador o utilizando el usuario por defecto *Administrator*, ir a *Tools > Administrative Tools > Users and Groups.*

    b) Seleccionar la localización donde estará el usuario, luego hacer clic en *New*, y después en *User*.

    c) En la pestaña *General*, añadir el nombre del usuario en *User Name*. En *User Type*, seleccionar las interfaces a las cuales podrá acceder dicho usuario.

    d) En la pestaña *Authentication* se deberá seleccionar el método de autenticación deseado. Este por defecto está puesto a *Password*. Si se deja esa opción, **se deberá seleccionar la opción de *User Must Change Password at Next Logon*, para que el usuario cambie la contraseña nada más entrar.** Los distintos métodos disponibles y su configuración se describen en 6.2 AUTENTICACIÓN.

    e) En la pestaña de *Authorization*, se deberán seleccionar las diferentes acciones que podrá llevar a cabo el usuario. Se corresponden con los permisos que dicho usuario tendrá. Se encuentran detallado en el apartado 6.3.5 PERMISOS DE ADMINISTRACIÓN.

    f) En la pestaña *Member*, se puede configurar la pertenencia a grupos de dicho usuario. A través de los grupos se pueden configurar los permisos de varios usuarios simultáneamente.

    g) Para finalizar, se hace clic en *OK* y *Close*.

105. El detalle de configuración de los usuarios se puede consultar en el siguiente enlace a la documentación pública.

106. Se recomienda también configurar los siguientes parámetros, disponibles en el fichero *DBParm.ini* del servidor EPV:

    a) *LockTimeout*: define el número de minutos tras el cual se cierra una sesión de usuario. El valor por defecto son 30 minutos.

    b) *IdleTimeout*: define el número de minutos de inactividad tras el cual se cierra una sesión de usuario. El valor por defecto son 20 minutos. **El valor mínimo permitido y recomendado es de 10 minutos.**

6.3.4 CREACIÓN DE GRUPOS DE USUARIOS

107. Como se ha mencionado anteriormente, los grupos permiten la configuración conjunta de los permisos de varios usuarios. El detalle de configuración de los grupos se puede consultar en el siguiente enlace a la documentación pública.

108. A continuación, se indican los pasos para la creación de grupos:

    a) Ir a *Tools > Administrative Tools > Users and Groups*.

    b) Seleccionar la localización en la que se ubicará dicho grupo.

    c) Hacer clic en *New*, seleccionar *Group*.

    d) Introducir el nombre y descripción deseados. Se pueden incluir en este paso usuarios o durante la creación de los mismos como se ha visto anteriormente.

    e) Por último, hacer clic en *OK*.

109. La asignación de permisos a los usuarios pertenecientes a un grupo se realiza mediante el mapeo de usuarios LDAP, para ello consultar el apartado 6.2.2.3 MAPEAR USUARIOS CYBERARK AL DIRECTORIO LDAP.

6.3.5 PERMISOS DE ADMINISTRACIÓN

110. Las distintas autorizaciones administrativas o permisos que mantiene el producto son:

- *Add Safes*: permite agregar *Safes* en el *Vault*.
- *Audit Users*: permite rastrear actividad de usuarios en el *Vault*.
- *Add/Update Users:* permite agregar y editar usuarios, gestionar áreas de red de donde se pueden conectar y gestionar jerarquías (*Locations*) de *Vault* que puedan operar.
- *Reset Users' Passwords*: permite reiniciar contraseñas de usuario y poner la opción "*User Must Change Password at Next Logon*" para aquellos usuarios del mismo nivel u más bajo en la jerarquía establecida del *Vault*.

- *Activate Users*: permite activar o desactivar las áreas de red confiables (*trusted network areas*) para aquellos usuarios en el mismo nivel u más bajo en la jerarquía establecida del *Vault*.
- *Add Network Areas*: permite agregar, actualizar y eliminar áreas de red en el Vault que especifican de dónde se puede acceder al *Vault*.
- *Manage Directory Mapping*: permite agregar, actualizar y eliminar mapas de directorios que gestionen a los usuarios almacenados en repositorios externos de manera transparente en *Vault*.
- *Manage Server File Categories*: permite agregar, actualizar y eliminar *file categories* (propiedades editables en objetos de cuentas usuario) en el *Vault*.
- *Backup All Safes*: permite realizar procedimientos de respaldo.
- *Restore All Safes*: permite ejecutar procedimientos de recuperación.

111. Cuando el objeto usuario está almacenado en un directorio externo LDAP, la primera vez que se valide, se crea su objeto usuario en CyberArk. Las autorizaciones que puedan tener se definen mediante *directory mappings* que determina las propiedades a crear según la pertenencia a un grupo. Esta funcionalidad se explica más adelante en esta guía en el apartado 6.2.2 CONFIGURACIÓN DE LDAP.

6.4 GESTIÓN DE CERTIFICADOS

112. Para la validación de los componentes con el servidor EPV, se hacen uso de certificados X.509 emitidos por la entidad certificadora del entorno. Este certificado es creado por la CA durante el proceso de instalación, tal y como se indica en el apartado 5.1 INSTALACIÓN EPV.

113. Para las comunicaciones seguras con el servidor de autenticación externo LDAP es necesario importar el certificado de la CA utilizado por el servidor, tal como se ha visto en el apartado 6.2.2.1 USO DE LDAP CON CERTIFICADO SSL EN EL VAULT.

114. Además, la solución permite a los usuarios autenticarse mediante el uso de certificados PKI, que se pueden crear mediante la herramienta *CACert*, que se instala junto con el *Vault*. Se puede encontrar en *C:\Program Files (x86)\PrivateArk\Server\CACert.exe*

115. La configuración de dichos certificados se detalla a continuación.

6.4.1 CERTIFICADOS PERSONALES PARA AUTENTICACION DE CLIENTE

116. A la hora de crear certificados, es importante tener en cuenta **que los algoritmos usados en el certificado deberán cumplir con las siguientes restricciones**, según indica la guía CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad:

- **RSA con claves de, al menos, 3072 bits de longitud.**

- **ECDSA con curvas P-256 o superior.**
- **Funciones hash SHA-256 o superior.**

117. Para la generación de los certificados de los usuarios, se puede hacer uso de la herramienta *OpenSSL*, la cual se instala al mismo tiempo que los componentes Linux.

NOTA: La utilidad de OpenSSL en los componentes Windows se debe instalar por separado eligiendo una distribución compatible. Este enlace provee un listado de distintos OpenSSL para Windows: *https://wiki.openssl.org/index.php/Binaries.*

118. Para generar los certificados se deberán seguir los siguientes pasos:

a) Ir al fichero de configuración de *OpenSSL* y, en la sección *"[alt_names]"* cambiar la dirección IP del parámetro IP.1, y poner la dirección del servidor que se está configurando.

b) Ejecutar el siguiente comando en la consola, dependiendo del sistema operativo:

- En Windows: *openssl.exe genpkey –algorithm RSA –pkeyopt rsa_keygen_bits:3072 –out CertPrivate.key –aes-256-gcm –pass pass:[Passphrase]*
- En Linux: *openssl genkey –algorithm RSA –pkeyopt rsa_keygen_bits:3072 –out CertPrivate.key –aes-256-gcm –pass pass:[Passphrase]*

c) Se deberá reemplazar *[Passphrase]* por una contraseña segura, y se recomienda almacenarla en "*ENV_PASSPHRASE*".

d) Seguidamente, ejecutar el siguiente comando:

- En Windows: *openssl.exe req –new –key CertPrivate.key –config [Ruta al fichero openssl.cnf] –out CertReq.csr*
- En Linux: *openssl req –new –key CertPrivate.key –config [Ruta al fichero openssl.cnf] –out CertReq.csr*

e) Ir a *https://<IP de la CA>/certsrv* para obtener el certificado para el componente.

f) Hacer clic en *Request a certificate*.

g) Hacer clic en *Advanced certificate request*.

h) Hacer clic en *Submit a certificate request* y copiar el contenido del fichero **CertReq.csr** en el campo *Saved Request*.

i) Escoger una plantilla que tenga lo siguiente:

- El parámetro *Client Authentication*.
- Habilidad de recibir el parámetro SAN.

j) Dejar el campo *Attributes* en blanco.

k) Hacer clic en el botón *Submit* para finalizar y enviar la petición del certificado a la entidad certificadora del entorno.

6.5 SINCRONIZACIÓN HORARIA

119. **Los diferentes componentes de la herramienta deben estar sincronizados con una fuente de tiempo fiable.** Para ello, se recomienda hacer uso de un servidor NTP. Para ello, se deben seguir las siguientes indicaciones:

- Acceder como administrador en el servidor EPV y disponer de la(s) dirección(es) del servidor NTP de la organización.
- Editar el fichero *C:\Program Files\PrivateArk\Server\DBParm.ini* e insertar el siguiente parámetro:

  AllowNonStandardFWAddresses=[X.X.X.X,Y.Y.Y.Y],Yes,123:outbound/udp

  Donde X.X.X.X es la dirección IP del primer servidor NTP y Y.Y.Y.Y es la dirección del segundo. El puerto 123 es el puerto para servicios horarios en Windows.
- Reiniciar el servicio *Vault* desde *Private-Ark Administration Console* (el icono "*PrivateArk Server*" en el escritorio).

120. De esta forma, se permite la conexión con las direcciones IP de los servidores NTP deseados. Tras esto, se deberá configurar el servidor NTP en el servidor Windows sobre el cual se ha desplegado EPV. Se recomienda hacer uso de autenticación NTP para mayor seguridad.

6.6 ACTUALIZACIONES

121. Cuando una nueva versión del producto está disponible, CyberArk envía una notificación vía correo electrónico al administrador del producto. En el correo electrónico se incluyen los enlaces para la descarga de la actualización, junto con las *Release Notes* de dicha actualización.

122. **Se deben utilizar únicamente versiones del producto que dispongan de soporte de seguridad por parte del fabricante y se deben instalar todos los parches de seguridad para que el producto esté exento de vulnerabilidades conocidas.**

123. El siguiente proceso se usa comprobar la versión de cada componente: para subir los nuevos ficheros al *Vault* y buscar actualizaciones:

a) Mostrar las propiedades del fichero dbmain.exe para ver la versión del Vault. Por defecto, el fichero se encuentra en: *C:\Program Files (x86)\PrivateArk\Server\dbmain.exe.*

b) Mostrar las propiedades del fichero PMEngine.exe para ver la versión del CPM. Por defecto, el fichero se encuentra en: *C:\Program Files (x86)\CyberArk\Password Manager\PMEngine.exe*

c) Mostrar las propiedades del fichero CAPSM.exe para ver la versión del PSM. Por defecto, el fichero se encuentra en: *C:\Program Files (x86)\CyberArk\PSM\CAPSM.exe.*

d) Para ver la versión de PVWA, desde la interfaz web hay que dirigirse a "About"

e) Para ver la versión de PSM SSH (PSMP), ejecutar*:*

"cat /var/opt/CARKpsmp/.version_info".

6.7 ALTA DISPONIBILIDAD

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

- Instalar al menos una instancia de recuperación ante desastres del *Vault* (*Vault* DR). Esta instancia replica los datos constantemente del *Vault* principal. En el momento que la instancia DR no detecte conectividad con el *Vault* principal, este cambia a modo activo y los componentes como PSM, PVWA y CPM estarán configurados para consultar esta segunda instancia en el caso de perder conectividad con la instancia del *Vault* principal. Es necesario editar el fichero *Vault.ini* y especificar las múltiples direcciones de *Vault*, separadas por comas, en el orden de prioridad. Se deben tener en cuenta los siguientes requisitos al instalar la instancia DR:
    - Claves criptográficas: Habrá que utilizar las mismas claves que se utilizaron para instalar el *Vault* principal.
    - Versión: Habrá que instalar la misma versión del *Vault* principal.
    - NTP: Se debe de asegurar de tener los *Vaults* sincronizados con el mismo servidor NTP para asegurar que las actividades estén sincronizadas con los registros almacenados.
    - Licencia: Utilizar la licencia provista para la instancia DR.
- Instalar más de un componente PVWA. Para asegurar conectividad al portal Web de usuarios, el componente PVWA se puede instalar múltiples veces, pero se requiere por separado un balanceador de carga. Este balanceador proveerá un enlace al usuario y se encargará de redirigirle al dispositivo correcto. Es importante tener los siguientes requisitos en cuenta para el balanceador:
    - El balanceador de carga no deberá alterar el contenido del sitio Web o incluir un mecanismo que prevenga que el portal sea alterado.
    - El balanceador no deberá alterar las rutas URL (dejar la ruta de aplicación por default tal cual como está)-
    - El balanceador debe soportar y tener habilitado *sticky sessions*.
- 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 una 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.

- Configurar una instancia de contingencia para CPM (acción opcional): El servicio de CPM se encarga de rotar las claves y contraseñas en los sistemas operativos remotos. Si ocurre un problema, no interrumpe la productividad de los usuarios (los usuarios se pueden seguir conectando a los sistemas). Pero de ser necesario, se puede mantener una instancia DR de CPM. Al igual que el *Vault* DR, esta segunda instancia permanece en modo pasivo hasta que el primero ya no esté disponible.

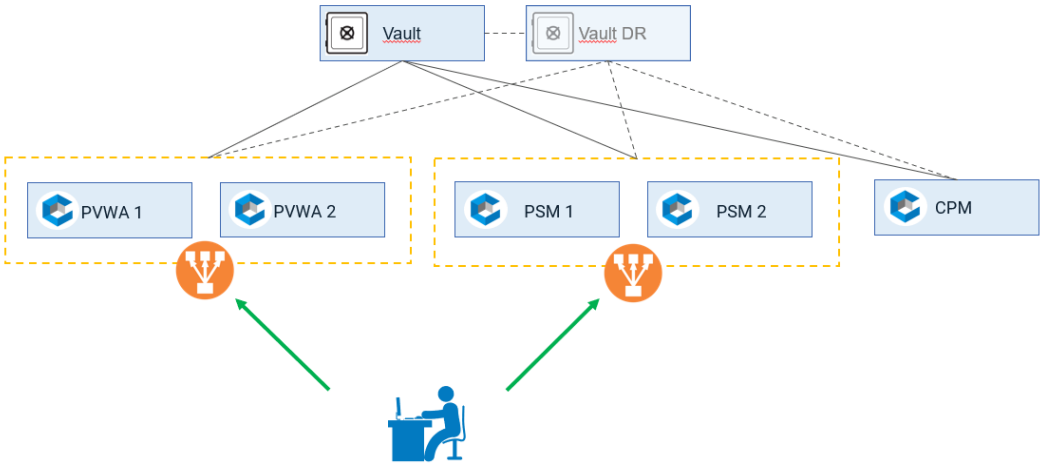


Ilustración 31 – Infraestructura de alta disponibilidad

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

125. 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.

126. Los usuarios pueden ver esta información de auditoría en la sección de *Monitoring* desde PVWA 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.

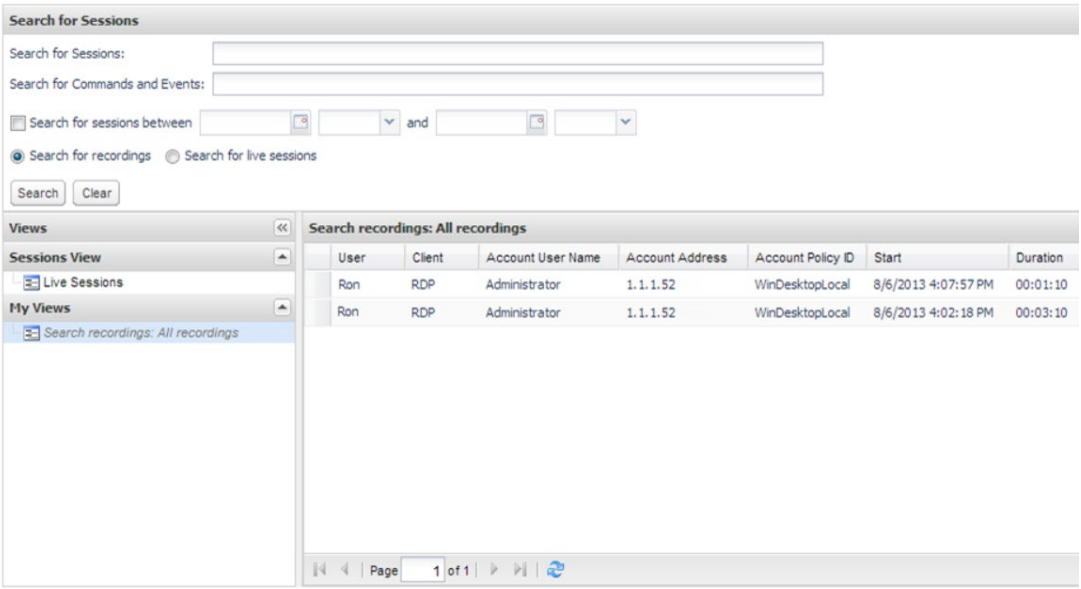


Ilustración 32 – Monitorización de sesiones

6.8.2 ALMACENAMIENTO LOCAL

127. 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 PVWA, se puede acceder a la sección de *POLICIES -> Master Policy.*

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

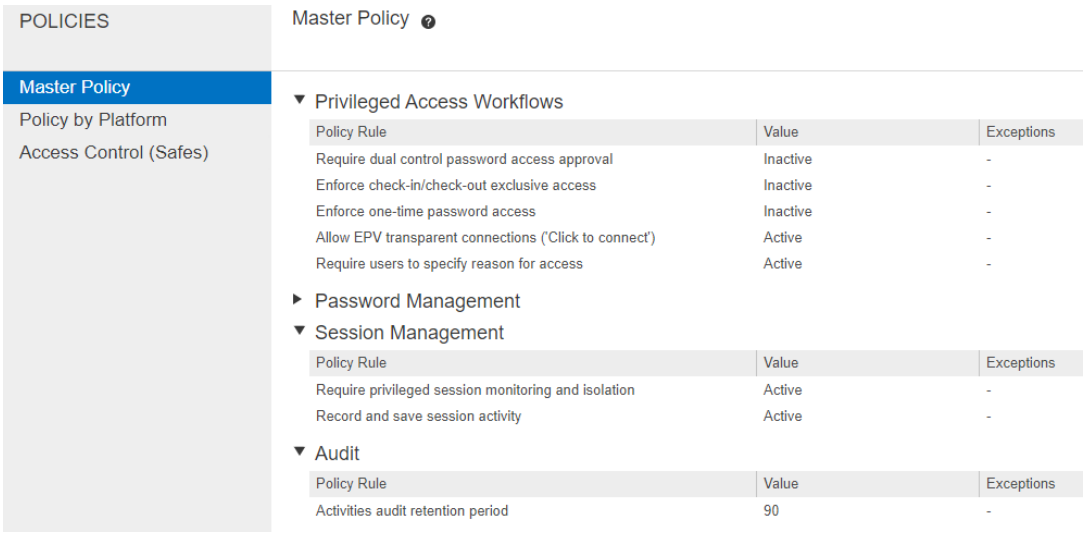


Ilustración 33 – *Master Policy*

6.8.3 ALMACENAMIENTO REMOTO

129. El producto permite agregar un servidor *syslog* para el envío de logs. Para ello, se deberán realizar los siguientes pasos:

a) Elegir una plantilla XSL que coincida con la tecnología buscada. En esta guía se toma como ejemplo Splunk y PTA.

b) Estas plantillas se encuentran en el sistema de ficheros. Para elegir una, ir a *C:\Program Files (x86)\PrivateArk\Server\Syslog*

c) Guardar en el servidor donde se encuentra instalado EPV la plantilla XSL seleccionada. Se recomienda ver la documentación del siguiente enlace.

d) Una vez modificado, se deberá editar el fichero *C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini*.

e) En este fichero se deberá especificar la ruta del "*fichero traductor*" en el parámetro *SyslogTranslatorFile*, la referencia al protocolo utilizado para la comunicación en el parámetro *SyslogServerProtocol*. Se debe hacer uso de TLSv1.2. Por último, se debe incluir el puerto y la dirección IP del servidor en los parámetros *SyslogServerPort* y *SyslogServerIP*.

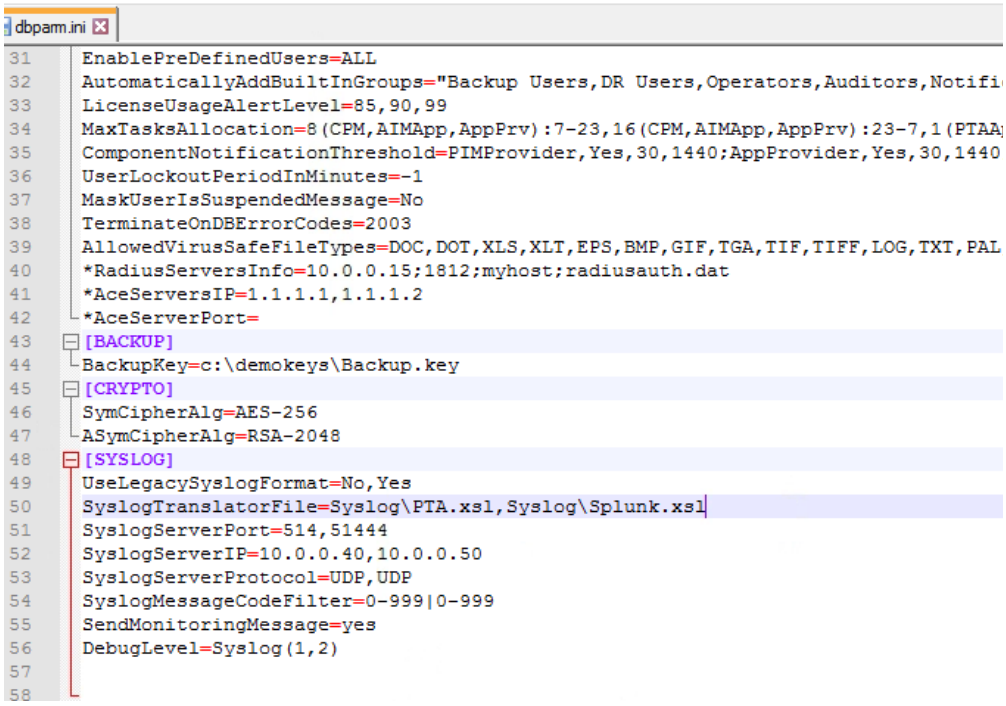


Ilustración 34 – Fichero *dbparm.ini*

f) En la imagen anterior, se definen dos dispositivos diferentes, uno es PTA y el otro es *Splunk*.

g) Para ver una descripción de los códigos para *SyslogMessageCodeFilter*, se recomienda ir al siguiente enlace.

h) Una vez finalizados los cambios, se deberá reiniciar el servidor.

6.9 *BACKUP*

130. Para la realización de las copias de seguridad, el producto cuenta con una solución para los *backups*, *Vault Backup Solution*. Esta proporciona una manera segura de realizar copias de seguridad del componente *Vault*, sin comprometer la información sensible que almacena. Puede ser implementado en dos escenarios:

- Replicación. La utilidad de *Vault Backup* exporta toda la información del *Vault* a un ordenador de la red, al que, posteriormente, el sistema global de *backup* de la organización podrá acceder y obtener los archivos de dicho ordenador. Todo el proceso tiene lugar en el *Vault*, manteniendo así el mayor nivel de seguridad posible, y sin la necesidad de que una aplicación externa acceda a la red. Todos los contenidos de la réplica están cifrados, asegurando que están seguros todo el tiempo.

  NOTA: Los datos extraídos están cifrados en AES-256. Esto no es configurable.

- Sistema de *backup* de terceros. El *Vault* se integra con diversas aplicaciones de *backup*. Se debe configurar el *firewall* para permitir el acceso de dichas

aplicaciones a las carpetas de *backup* del *Vault*. Al introducir una aplicación externa se reduce el nivel de seguridad de la información almacenada.

131. Se recomienda el uso de la utilidad *Vault Backup Solution* proporcionada por el propio producto, para mantener el mayor nivel de seguridad posible de la información contenida en el Vault. Esta utilidad proporciona una copia de seguridad completa de los *Safes* y *Vaults*, y permite su recuperación en cualquier momento.

6.9.1 CONSIDERACIONES PREVIAS

132. La utilidad de *Vault Backup* debe ser instalada en un equipo dedicado a la tarea de *backup*. **No puede estar instalado en el mismo ordenador que el *Vault***.

133. Además, es necesario comprobar que la máquina donde se va a configurar cuenta con las siguientes características:

- Tiene, al menos, el mismo espacio en disco que el *Vault*.
- La unidad donde se almacenarán los archivos replicados debe ser NTFS.
- Cuenta con accesibilidad al *Vault* a través del puerto 1858.
- Cuenta con accesibilidad por el sistema de *backup* de la organización.
- Tiene seguridad física que solo permite el acceso a usuarios autorizados.
- Configuración regional y de idioma idéntica a la de la máquina *Vault*.

134. Una vez comprobado que la máquina donde se va a instalar la utilidad de *Vault Backup* cuenta con dichas propiedades, se pasa a la instalación.

6.9.2 INSTALACIÓN

135. Para realizar la instalación de la utilidad, se han de seguir los siguientes pasos:

a) En la carpeta de instalación que se ha copiado del CD de instalación, se ha de obtener la carpeta *Replicate* con sus respectivos archivos. El fichero de instalación de la utilidad se deberá llamar *Replicate-Rls.zip.*

b) Ejecutar el fichero *Setup.exe* con permisos de administrador.

c) Seguir las indicaciones del *Wizard* de instalación. Añadir los detalles de la organización y escoger una ruta de instalación.

136. La utilidad instalada se llama *PrivateArk Replicator* y se instala en la subcarpeta de *Replicate*. Durante su instalación, se instalan las siguientes tres (3) utilidades:

a) *PAPrebackup:* Prepara los *Safes* para la copia de seguridad.

b) *PAReplicate*: Realiza las copias de seguridad de los *Safes*.

c) *PARestore*: Restaura los *Safes*.

137. Para finalizar la instalación, se recomienda crear un usuario para realizar los *backups*. Para ello se deberán seguir los siguientes pasos:

a) Conectarse al *Vault* con *PrivateArk* como usuario administrador.

b) Crear un usuario específico para realizar las copias de seguridad.

c) Generar un *credential file* para autenticar al usuario en el *Vault*, sin necesidad de una contraseña.

CreateCredFile.exe backupuser.ini Password /username <username> /password <password> /AppType CABACKUP

NOTA: Para más información sobre la utilización de *credential files* y sus parámetros, consultar el siguiente enlace:

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/CreateCredFile-Utility.htm?tocpath=Administration%7CUtilities%7CUser%20credential%20files%7C 2

6.9.3 UTILIDAD PAPREBACKUP

138. La utilidad *PAPrebackup* es utilizada por *PAReplicate*, por lo que no es necesario ejecutarla por separado. Esta se encarga de preparar los *Safe* para el respaldo.

139. Los metadatos se almacenan en la subcarpeta destinada a metadatos y los ficheros de datos son almacenados en la subcarpeta destinada a datos. Antes de iniciarse el *backup*, se copian los archivos de metadatos en la carpeta *Metadata Backup*. Si se solicita una copia de seguridad completa, se crea una copia de toda la base de datos y se almacena en la subcarpeta de copia de seguridad de metadatos. En el caso de que se solicite una copia incremental, los registros binarios de *MySQL* que contienen los cambios realizados en los metadatos, se copian en la subcarpeta de respaldo de *Metadata*.

140. A continuación, el proceso de *backup* copia los archivos de las carpetas *"Copia de seguridad de metadatos"* y "*Datos*" sin tocar los archivos de metadatos originales en la carpeta de metadatos.

NOTA: Cualquier usuario con la autorización *Backup All Safes* y la autorización *Backup Safe* en los *Safes* específicos, puede emitir el comando *PAPrebackup* para ellos mismos.

6.9.4 UTILIDAD PAPREPLICATE

141. La utilidad *PAReplicate* copia los archivos seguros del *Vault* a un ordenador específico de la red en una estructura similar a la de la carpeta *Safes*.

142. Al igual que con la utilidad *PAPrebackup*, cualquier usuario con la autorización *Backup All Safes* y la autorización *Backup Safe* en los *Safes* específicos, puede emitir el comando *PAReplicate* para ellos mismos.

143. Se puede hacer uso de la utilidad para hacer una copia de seguridad de un *Safe* específico o de un grupo de ellos. Cuando se realiza la copia de seguridad, los archivos de datos solicitados se copian en la ubicación especificada en el mismo

formato en el que están almacenados en el servidor, y la copia de seguridad de metadatos del *Vault* se copia en la ubicación especificada en la subcarpeta destinada a metadatos.

144. Para ejecutar la utilidad, se hará de la siguiente manera:

Pareplicate C:\PrivateArk\Server\Conf\Vault.ini /logonfromfile backupuser.ini /FullBackup

145. Los diferentes parámetros usados son:

a) *C:\PrivateArk\Server\Conf\Vault.ini:* El archivo que contiene toda la información sobre el *Vault* y los *Safe* que contiene. De forma predeterminada, este archivo se llama *Vault.ini.*

b) */logonfromfile*: El nombre de ruta de un *credential file* creado para el usuario de respaldo que se utilizará para iniciar sesión, en lugar de una contraseña.

c) *backupuser.ini*: El *credential file* antes mencionado.

d) */FullBackup*: Parámetros para realizar un respaldo completo.

146. Este comando se deberá ejecutar periódicamente, de acuerdo con la política de *backups* de la organización.

6.9.5 UTILIDAD PARESTORE

147. Por último, la utilidad *PARestore* permite restaurar *Safes* que previamente han sido replicadas o guardas en una copia de seguridad.

148. A continuación, se detalla el procedimiento para restaurar un respaldo completo realizado con *PAReplicate*. Para restaurar sólo objetos determinados del *backup* o una restauración parcial, se recomienda ir a la documentación oficial del producto.

149. La restauración completa del *Vault* se lleva a cabo en el caso de una caída general y la información no puede ser recuperada por ningún medio. Esta restauración implica restaurar los *Safes* a un nuevo *Vault*. Después de instalar y configurar el servidor *Vault*, el nuevo *Vault* tendrá los mismos nombres, usuarios y autorizaciones que el antiguo. Dicho *Vault* deberá utilizar las mismas claves maestras y de operador que el antiguo.

150. Los pasos a seguir para la restauración completa del *Vault* son los siguientes:

a) Instalar una nueva instancia de la misma versión de *PrivateArk Server* y asegurarse de que funciona de manera correcta.

b) Habilitar el usuario *Operador* u otro usuario que tenga los permisos necesarios en el *Vault* para restaurar todos los *Safe*.

c) En *DBParm.imi,* establecer *el siguiente parámetro:*

BackupFilesDeletion=No

d) Utilizar *PARestore.exe* con el fin de copiar todos los archivos de la copia de seguridad pertinentes (metadatos y datos) a la carpeta *Safes* restaurada en el *Vault*. Un ejemplo: *PARestore operador vault.ini / FullVaultRestore*

e) Abrir la consola de administración de *PrivateArk* y detener el servicio de *CiberArk Vault Server*. Seguidamente, cerrar la consola.

f) En la carpeta de instalación del servidor, ejecutar la utilidad *CAVaultManager*, de la siguiente manera:

CAVaultManager RecoverBackupFiles

NOTA: Este comando necesita las claves del usuario *Master*.

g) En la misma carpeta, ejecutar de nuevo *CAVaultManager*, de la siguiente manera:

CAVaultManager RestoreDB

Esto completará el proceso de restauración y sincronizará los metadatos y los datos restaurados.

h) En *DBParm.ini,* restablecer el parámetro *BackupFilesDeletion*. El valor por defecto de este parámetro es el siguiente:

BackupFilesDeletion = yes, 24,1,5,7d

Es recomendable mantener estos valores.

i) Modificar los archivos de configuración del *Vault* para establecer los valores del *Vault* anterior.

j) Iniciar el servicio *CyberArk Vault Server*.

7. FASE DE OPERACIÓN

151. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

- El producto debe estar instalado y mantenido en un entorno físico seguro. Esto incluye un edificio seguro con control de acceso o un entorno móvil controlado por el administrador.
- Se deben realizar comprobaciones periódicas del *software* para asegurar que no se ha introducido *software* no autorizado.
- El producto debe contar con las últimas actualizaciones de seguridad para preservar al mismo de amenazas y vulnerabilidades conocidas.
- Se deben mantener y analizar los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- Se deben gestionar correctamente los certificados utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
- Se deben realizar copias de seguridad de manera periódica, así como configurar el envío periódico de copias a un servidor externo.

8. *CHECKLIST*

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro y aplicación de las licencias	☐	☐	
Instalación de los componentes	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo de operación seguro (modo FIPS)	☐	☐	
Configuración Servidor NTP	☐	☐	
Configuración servidor syslog para enviar los registros de auditoría	☐	☐	
Configuración de *backup* & archivado periódico	☐	☐	
Configuración de los certificados de cliente, maquina, CA's de confianza, etc.	☐	☐	
Aplicación de requisitos mínimos de contraseñas	☐	☐	
Configuración de *timeouts* de sesión	☐	☐	
Creación e instalación de certificados	☐	☐	
Configuración del *logging* de todo el tráfico relevante	☐	☐	
OPERACIÓN			
Mantenimiento del producto en un entorno físico seguro			
Comprobación periódica del *software* instalado			
Actualización del producto e instalación de parches de seguridad			
Mantenimiento y análisis de los *logs*			
Gestión de los certificados			
Realización de copias de seguridad			

9. REFERENCIAS

La documentación de producto está disponible en el siguiente enlace: https://docs.cyberark.com/

10. ABREVIATURAS

AES	*Advanced Encryption Standard*
CA	*Certificate Authority*
CCN	*Centro Criptológico Nacional*
CPM	*Central Policy Manager*
CPSTIC	*Catálogo de Productos de Seguridad TIC*
DNS	*Domain Name System*
ENS	*Esquema Nacional de Seguridad*
EPV	*Enterprise Password Vault*
HTTPS	*Hypertext Transfer Protocol Secure*
IIS	*Internet Information Service*
IP	*Internet Protocol*
OPM	*On-Demand Privilege Management*
OS	*Operating System*
PAS	*Privileged Access Security*
PSM	*Privileged Session Manager*
PSMP	*Privileged Session Manager SSH Proxy*
PVWA	*Password Vault Web Access*
RDP	*Remote Desktop Protocol*
RHEL	*Red Hat Enterprise Linux*
SHA	*Secure Hash Algorithm*
SSH	*Secure Shell Protocol*
TLS	*Transport Layer Security Protocol*
TOE	*Target of Evaluation*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL