HOT BULLETIN

¿Qué hay de nuevo en CyberArk?

23 de agosto de 2022

Devel
CYBERSECURITY REDEFINED

- Web: www.devel.group
- Email: info@develsecurity.com
- Guatemala - El Salvador - Honduras - Rep. Dominicana

Qué hay de nuevo

Las siguientes características se introdujeron o mejoraron en Privileged Access Manager - Self-Hosted versión 12.6.

LTS

Esta versión está designada como soporte a largo plazo. Los clientes que instalen esta versión seguirán recibiendo actualizaciones de seguridad y correcciones de errores críticos según nuestra política.

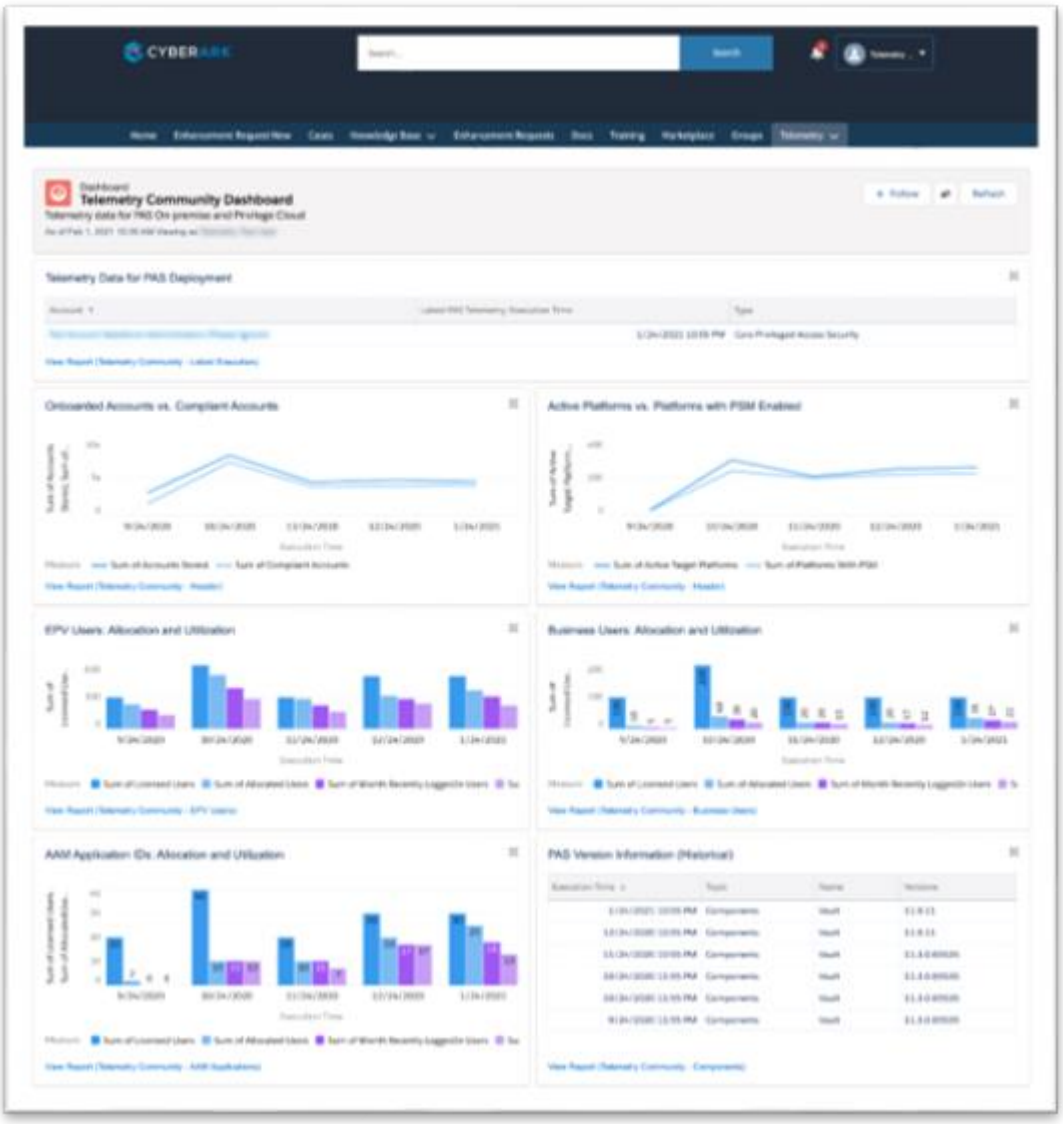
Para obtener más detalles, consulte nuestra política de fin de vida.

Plataforma tecnológica compartida

Compatibilidad con Microsoft Windows 2019 para los componentes de Privilege Access Management implementados en la nube

Estamos ampliando nuestro soporte actual que ya existe para los componentes de Privilege Access Management implementados en las instalaciones a sus imágenes homólogas que se implementan en la nube (AWS y Azure).

Las mejoras de la herramienta de telemetría ofrecen una mayor visibilidad de la gestión de contraseñas



Las nuevas funciones y opciones de visualización permiten a los clientes obtener una mejor visibilidad del cumplimiento de la herramienta de telemetría de CyberArk. Los atributos relacionados con la política de administración de contraseñas recientemente agregados permiten a los clientes analizar los niveles generales de seguridad de las contraseñas y obtener información procesable.

Las métricas recién agregadas incluyen:

Plataformas con verificación periódica

Plataformas con conciliación automática

Plataformas con cambio periódico

Bóveda

Mejora continua del cumplimiento y seguridad de la Bóveda

Windows Server 2019 Hardening revisado para seguir los estándares CIS

Muchas organizaciones utilizan las pautas de CIS como estándares de seguridad y mejores prácticas para defender los sistemas de TI.

En consecuencia, el fortalecimiento de Digital Vault se revisó para alinearse con las pautas del Centro para la Seguridad de Internet (CIS) diseñadas específicamente para el servidor independiente de Digital Vault.

El nuevo endurecimiento logra más del 90 % de cumplimiento con el informe CIS de enero de 2022 y proporciona pautas de endurecimiento adicionales que no están cubiertas o no aseguradas al estándar de Vault por el informe CIS.

PAKeygen para admitir la biblioteca pkcs11 de 64 bits y HSM que requiere integración de PIN

Al expandir la capacidad de Vault para integrarse con una gama más amplia de módulos de seguridad de hardware (HSM), la utilidad PAKeyGen se actualiza para admitir la biblioteca PKCS # 11 de 64 bits al generar claves de servidor con integración HSM. Además, también se admiten los proveedores de HSM que utilizan un número de identificación personal (PIN).

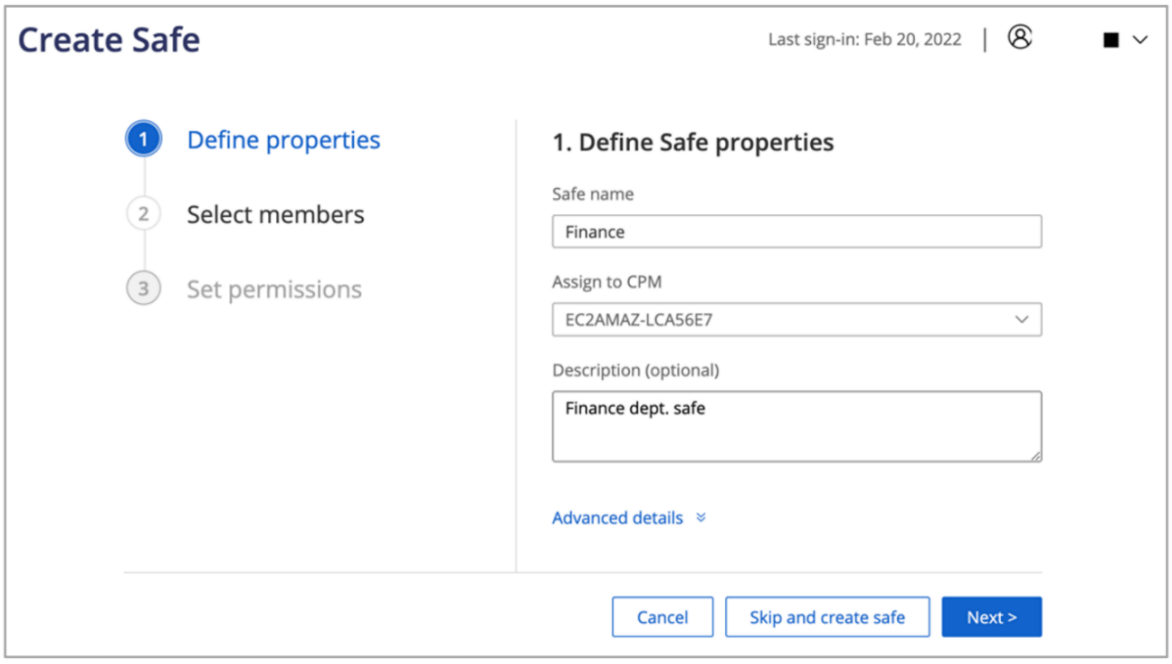
Acceso web a la bóveda de contraseñas

Interfaz de usuario de gestión segura simplificada

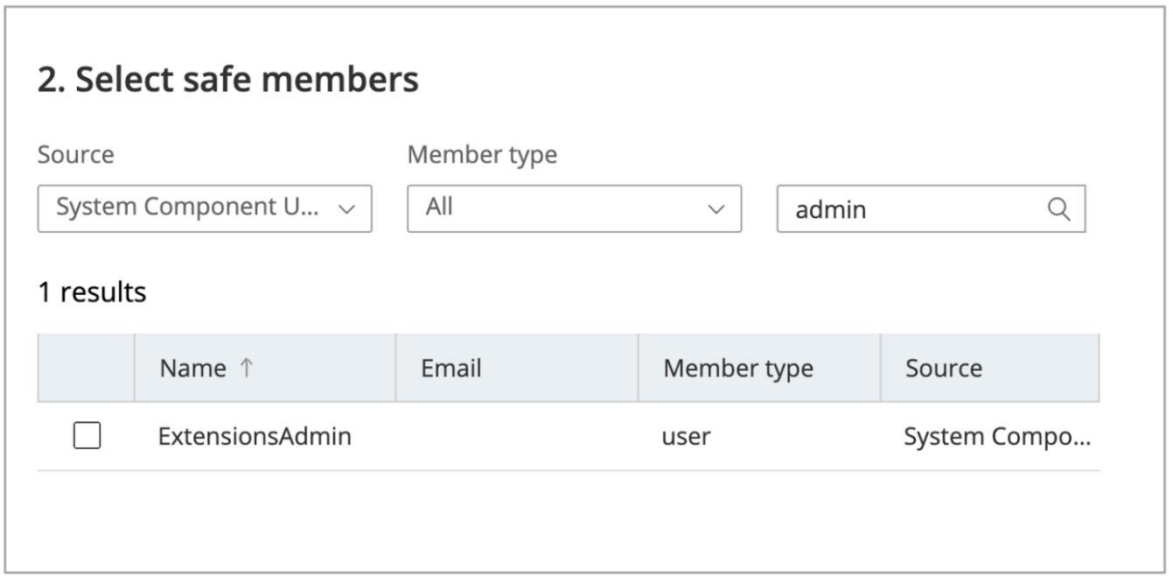
Password Vault Web Access 12.2 introdujo la nueva vista Cajas fuertes que se alinea con la apariencia más limpia y moderna. En esta versión, ampliamos la nueva interfaz de Cajas fuertes para ofrecer un flujo de trabajo guiado por un asistente que brinda simplificación y una mejor visibilidad que mejorará el proceso de administración de cajas fuertes.

La nueva vista Cajas fuertes en PVWA reemplaza la interfaz clásica y ofrece capacidades de gestión ampliadas para:

Cree y edite cajas fuertes dentro de un nuevo flujo de trabajo flexible respaldado por pasos dirigidos por un asistente

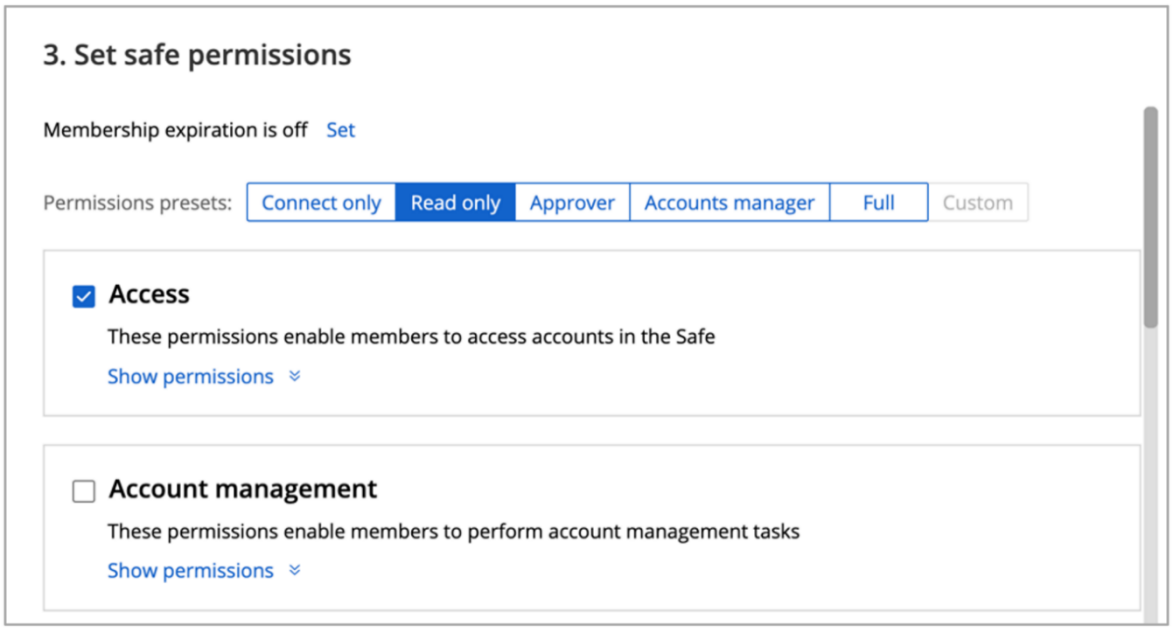


Asigne fácilmente miembros a cajas fuertes gracias a las capacidades mejoradas de filtrado de usuarios

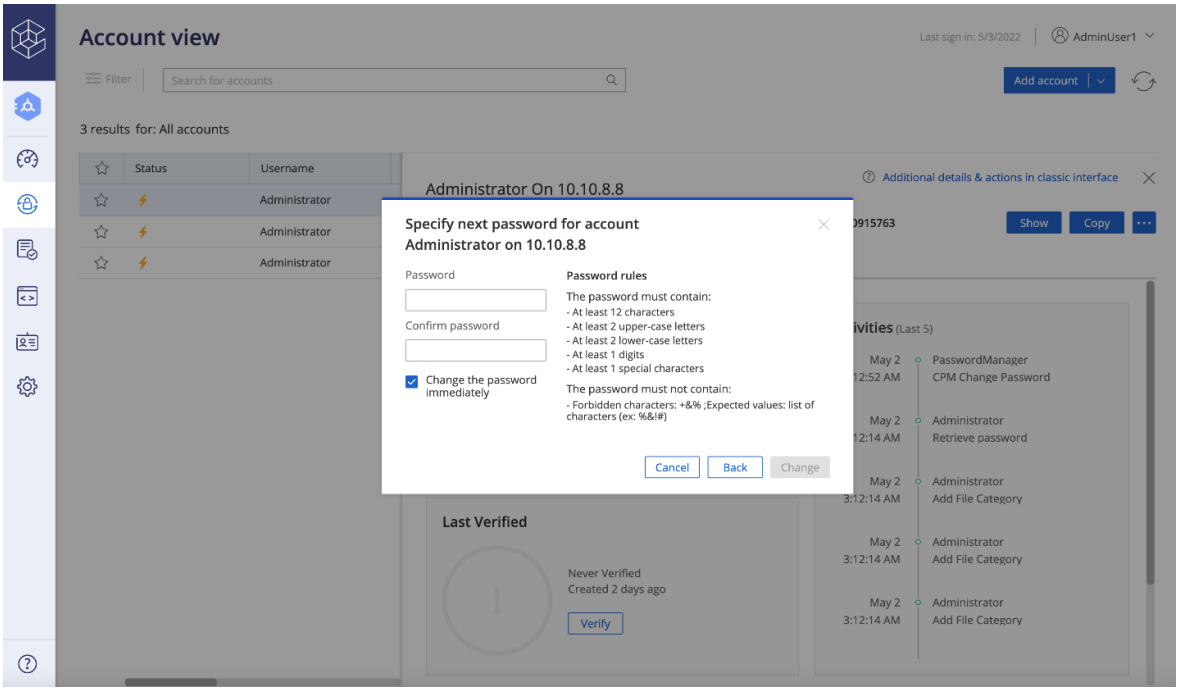


Administre miembros y permisos de Safe como parte del flujo de creación y edición de Safe. Los permisos son más fáciles de administrar gracias a los conjuntos de permisos predefinidos (Solo

lectura, Aprobador, Administrador de cuentas, Completo, Personalizado).



Cambiar contraseña: establezca el siguiente valor de contraseña



Es posible que los clientes deban especificar la siguiente contraseña que utilizará el CPM para actualizar las credenciales de una cuenta.

En tales casos, los administradores de Vault pueden, directamente desde la interfaz de usuario de PVWA predeterminada, cambiar la contraseña en Vault, que el CPM reconciliará en la máquina remota durante el próximo proceso de CPM. Hasta ahora, esta opción solo estaba disponible en la interfaz de usuario clásica.

Validación del emisor del certificado a la autenticación PKI/PKIPN

PKI permite el uso de certificados para que servidores y usuarios se identifiquen entre sí y establezcan una conexión segura. Los certificados contienen valores de cifrado, o claves, que se utilizan para cifrar y garantizar la integridad de los mensajes enviados entre las dos partes.

Cuando un usuario inicia sesión en PVWA utilizando el método de autenticación PKI/PKIPN, el usuario y el Servidor establecen una conexión SSL (Secure Socket Layer). Durante el protocolo de enlace SSL, las partes intercambian certificados y verifican su validez. También comprueban que el certificado de la otra parte haya sido emitido por una CA (Autoridad de Certificación) de confianza.

En esta versión, mejoramos la autenticación para validar que el certificado que usa el usuario final fue emitido solo por ese emisor específico. Esto permitirá a los administradores configurar qué emisor es el emisor válido para la autenticación PKI/PKIPN.

API REST

La gestión de usuarios y la gestión de cuentas son los elementos clave en los procesos automatizados de incorporación de la organización.

Esta versión incluye varias mejoras en nuestros servicios web REST API específicamente en torno a estas áreas para facilitar la automatización y el uso.

Se agregaron las siguientes nuevas API:

- Deshabilitar usuario : deshabilita a un usuario
- Habilitar usuario : habilita un usuario que estaba deshabilitado
- Obtener detalles del grupo : recupera los detalles de un solo grupo de usuarios

Además, mejoramos la API REST Obtener cuentas para filtrar la lista devuelta según un conjunto de vistas. Estos filtros guardados permiten al desarrollador mostrar cuentas de acuerdo con criterios predefinidos basados en el estado de la cuenta y la operación, como Eliminado, DeshabilitadoContraseñaPorCPM y Programado para reconciliación. Ahora también devolvemos el DeletedTimestamp por cada una de las cuentas devueltas que se eliminan, con la hora en que se eliminó la cuenta.

Registrador de aplicaciones PVWA mejorado

CyberArk introdujo en V11.4 el nuevo registrador de aplicaciones de PVWA que mejoró y simplificó el proceso de resolución de problemas. En esta versión completaremos la migración y se convertirá en el registrador principal del PVWA que reemplazará a dos de los registros existentes.

Además, agregaremos un nuevo registro de consola mejorado que reemplazará el antiguo registro de consola CyberArk.WebConsole.log.

Estos nuevos registros mejorarán nuestras capacidades de registro al proporcionar una estructura de registro clara que permite una solución de problemas más rápida y determina fallas sin la necesidad de habilitar el modo de depuración explícitamente.

Para fin de año, esperamos que los clientes completen su transición al nuevo registrador de aplicaciones y, por lo tanto, los archivos de registro CyberArk.WebConsole.log, CyberArk.WebApplication.log y CyberArk.WebSession<sessionId>.log estarán deshabilitados de forma predeterminada. sobre instalaciones limpias y actualizaciones de próximas versiones.

Administrador central de políticas

Conector STS de AWS

Amazon Web Services Console es la interfaz principal que los usuarios aprovechan para realizar cambios administrativos en los servicios de AWS. Esta poderosa herramienta es un objetivo principal para el abuso por parte de los atacantes. Es fundamental que las organizaciones aseguren el acceso a la consola de AWS, asegurándose de que solo los usuarios apropiados tengan acceso y solo a los servicios necesarios para su función laboral. La mejor práctica recomendada por AWS para el acceso privilegiado a la consola es restringir el tráfico a estaciones de trabajo específicas, pero esto puede ser un desafío en organizaciones grandes.

Nos complace presentar una nueva consola de Amazon Web Services (AWS) con STS para conectarse a través de AWS STS que reemplazará nuestro complemento anterior y, según el marco de aplicaciones web para PSM, es compatible con Chrome e Internet Explorer.

Esta integración permite a las organizaciones aislar y monitorear por completo las sesiones de la consola de AWS mediante Amazon Secure Token Service (STS), que proporciona credenciales temporales.

Para obtener más información, consulte Administración de servicios en la nube de AWS.

Administrador de sesión privilegiado

Llevando la aplicación de acceso al siguiente nivel y mejorando el control de cumplimiento de la ruta de PSM a los activos críticos de la organización.

Control de acceso basado en red a conexiones ad hoc

Con el cambio de los perímetros de las oficinas y los empleados que ya no están en la oficina y en movimiento, es esencial tener una mejor aplicación de su acceso a los recursos de la organización y poder aplicar regulaciones de acceso y cumplimiento a nivel mundial.

En esta versión, los clientes ahora pueden aplicar reglas basadas en subredes para controlar el acceso de los usuarios finales a objetivos específicos según su ubicación.

Las reglas se pueden crear en un enfoque de lista de permitidos o denegados, según la configuración de la organización.

Cumplimiento del marco de tiempo de Dual Control en sesiones de PSM en curso

Controlar el período de tiempo para el acceso de los usuarios finales a los activos de la organización es importante desde una perspectiva de responsabilidad y cumplimiento.

En esta versión, hemos agregado la opción de hacer cumplir el período de tiempo de la solicitud de control dual que está asociado con la sesión y desencadenar la finalización de la sesión una vez que ese período de tiempo llega a su fin.

Flexibilidad de registro de PSM

Cuando se registra una nueva instancia de PSM en Vault durante la etapa de registro de la instalación, su dirección IP se escribe en los datos de conexión del servidor de PSM en las opciones de configuración. En esta versión, hemos agregado la opción de registrar PSM con su nombre DNS (FQDN), lo que brinda flexibilidad en redes que cambian dinámicamente y facilita la protección de la conectividad de PSM con certificados SSL.

Esta opción se alterna con un nuevo parámetro en la configuración de la etapa de registro y no está disponible al instalar PSM a través del asistente de instalación.

Administrador de sesión privilegiado para SSH

Mejora continua de la oferta de cumplimiento y seguridad de las sesiones basadas en SSH

Auditoría mejorada para sesiones de transferencia de archivos

Estamos aumentando la cobertura de cumplimiento de las grabaciones de sesiones SFTP al agregar capacidades de auditoría e incluir actividades de usuario, así como información de archivos en la página de monitoreo.

Tunelización SSH en PSM para el modo integrado SSH

PSM para SSH permite a los usuarios autorizados iniciar y utilizar un túnel SSH para acceder a un servidor SSH de destino, al mismo tiempo que proporciona capacidades de auditoría de sesión de

túnel de inicio/finalización. A través de este túnel, los usuarios pueden iniciar aplicaciones GUI como Web o SQL desde su estación de trabajo, manteniendo su flujo de trabajo existente.

Con PSM para SSH, los administradores de seguridad pueden controlar el acceso al determinar qué usuarios pueden acceder a diferentes sistemas de destino.

En esta versión, PSM para el Modo Integrado de SSH brinda la flexibilidad de configurar túneles SSH para sistemas específicos, de acuerdo con las necesidades de acceso y seguridad de la organización.

Análisis de amenazas privilegiadas

Instalación y actualización simplificadas

Con la alta frecuencia actual de vulnerabilidades de seguridad en varias plataformas y aplicaciones, es importante brindar a los clientes un control y una alineación totales sobre las versiones y actualizaciones de los paquetes sin necesidad de un parche de la PTA.

A partir de esta versión, los procesos de instalación y actualización de PTA solo incluirán actualizaciones para los siguientes terceros:

apache-activemq

apache-tomcat

mongodb

mongodb_exportador

monitorear

nodo_exportador

Prometeo

Pasarela de empuje

Azul Zulú OpenJDK

Esto permitirá a los clientes reaccionar rápidamente en caso de que se publique una vulnerabilidad relacionada con los paquetes que ya no forman parte del proceso de instalación de PTA.

El resto de los paquetes que solían ser parte de la instalación y actualización de PTA se considerarán como requisitos previos y su instalación será verificada por PTA antes de iniciar el proceso de instalación y actualización.

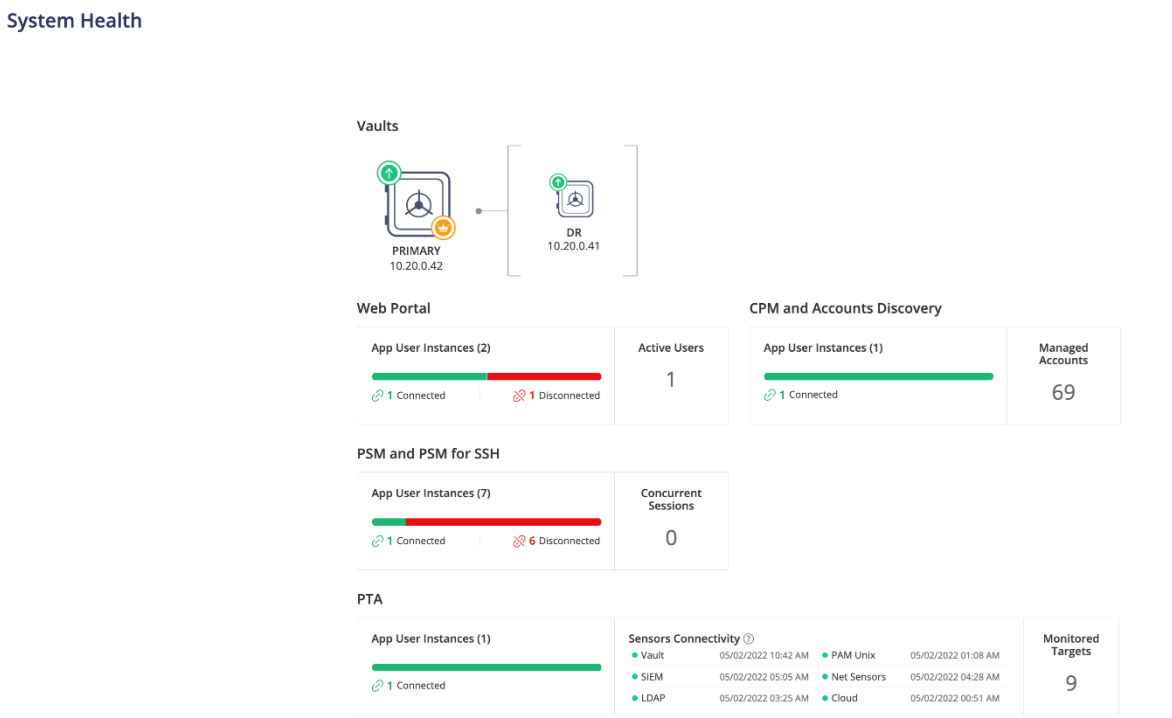
Cuando se implementa PTA desde la imagen del disco, la instalación aún incluirá todos los paquetes de terceros. Sin embargo, luego de la implementación inicial y en el futuro, los clientes deben administrar las actualizaciones futuras y los parches de seguridad de estos paquetes de terceros.

Actualización de la versión de MongoDB

La versión integrada de MongoDB utilizada por PTA se actualizó de la versión 3.6 a la versión 4.4.

Indicación de conectividad del sensor en la página de estado del sistema

Mejorando la visibilidad de la salud de PTA, en esta versión la página de salud del sistema se ha ampliado con información sobre la última vez que cada sensor se comunicó por última vez con la PTA.



Protección contra falsificación de solicitud entre sitios (CSRF)

La vulnerabilidad CSRF está relacionada con el comportamiento del navegador. Utiliza parámetros de sesión existentes para cualquier solicitud al mismo sitio, lo que permite a un atacante falsificar una solicitud de modificación y manipular al usuario para activarla.

Con la protección CSRF, cada solicitud contiene un token CSRF que es único para la sesión de usuario actual, lo que hace que sea imposible falsificar una solicitud genérica.

En esta versión, agregamos protección CSRF en la interfaz de usuario clásica de PTA.

Expansión de comandos arriesgados a los comandos de Google Cloud

La lista predeterminada actual de comandos riesgosos se amplió para incluir comandos que son relevantes para Google Cloud.

Lista de exclusión de acceso privilegiado no administrado (UPA)

A partir de esta versión, brindamos a los clientes la flexibilidad de excluir ciertos nombres de usuario que consideran irrelevantes para el proceso de detección de usuarios privilegiados no administrados.

Mejoras de seguridad

Compatibilidad con TLS 1.2

CPM

CPM admite el uso de TLS 1.2 para conexiones entrantes a CPM y conexiones salientes a destinos. Es una práctica recomendada de seguridad deshabilitar TLS 1.0 y 1.1 para garantizar el uso del protocolo de cifrado de nivel superior.

> A partir de esta versión, deshabilitaremos TLS 1.0 y 1.1 en el servidor CPM de manera predeterminada como parte del fortalecimiento de CPM. Los clientes que deseen utilizar versiones anteriores de TLS pueden configurar el sistema para permitir estas versiones después de que se complete la fase de endurecimiento, o excluir este paso de la fase de endurecimiento por adelantado. Consulte Actualizaciones de la configuración IIS SSL/TLS para obtener más información.

PAM: alojamiento propio en la nube: integración de Vault con Azure Key Vault

Microsoft ha anunciado la obsolescencia de TLS 1.0 y TLS 1.1 a partir del 31 de mayo de 2022 cuando se integre con el servicio Azure Key Vault.

Dado que las imágenes de CyberArk Azure se integran con Azure Key Vault para proteger la clave del servidor, las imágenes de Cyberark Vault se han actualizado en consecuencia para admitir TLS 1.2 para.NET Framework.

PTA: aplicación de TLS 1.2 durante la instalación

Siguiendo las mejores prácticas de seguridad, a partir de esta versión, las nuevas implementaciones de PTA utilizarán la comunicación basada en TLS 1.2 de forma predeterminada para los puertos syslog entrantes.

Los clientes pueden cambiar esta configuración durante el proceso de instalación o manualmente a través del archivo de propiedades del sistema.

Este cambio no se aplica a las implementaciones existentes, aunque recomendamos enfáticamente que los clientes actualicen manualmente y comiencen a usar TLS 1.2 si aún no lo han hecho.

Actualización de componentes internos de PVWA

Los componentes internos se actualizaron para mejorar la seguridad y realizar mejoras tecnológicas en el sistema operativo y los componentes de terceros para el servidor PVWA. El proceso de endurecimiento de PVWA se actualizó en consecuencia.

Por favor comunícate con nosotros a soporte@develsecurity.com ante cualquier soporte, reporte de amenaza o cualquier otro incidente sobre este boletín de seguridad.