Prácticas recomendadas de User-ID

10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

November 16, 2020

Table of Contents

Prácticas recomendadas de User-ID

Introducción a las prácticas recomendadas de User ID

User-ID™ aprovecha el contexto de usuario de una amplia gama de repositorios, como servidores de directorio, controladores de LAN inalámbrica, VPN, NAC, proxies y más, lo que le permite:

- Identificar a los usuarios y aplicar el principio de privilegio mínimo a los usuarios en función de su nivel de confianza y comportamiento, independientemente de:
  - las ubicaciones de los usuarios (como la oficina o el hogar)
  - qué dispositivos están usando (como iOS, dispositivos móviles Android, macOS, Windows, ordenadores Linux, ordenadores portátiles, Citrix, Microsoft VDI o Terminal Servers)
  - a qué aplicaciones acceden los usuarios
- Proteger sus credenciales corporativas del uso en sitios web de terceros y evite la reutilización de credenciales robadas habilitando la autenticación multifactor (MFA) en la capa de red para cualquier aplicación sin cambios en la aplicación.

La capacidad de identificar consistentemente a los usuarios en su red, independientemente de la ubicación, proporciona una mejor visibilidad de la actividad del usuario, habilita la política de seguridad basada en usuarios y grupos, y le ayuda a obtener análisis más profundos (registro, informes y análisis forense). Utilice las siguientes pautas de prácticas recomendadas para aprender a planificar, implementar y mantener User-ID en su red.

User-ID admite varias funciones; esta guía cubre las siguientes características:

- GlobalProtect
- Supervisión de Syslog
- Redistribución
- Asignación de grupos
- Grupos de usuarios dinámicos

Las características adicionales que aún no se cubren en esta guía incluyen:

- Acceso a Prisma gestionado por Panorama
- Prevención de phishing de credenciales
- Asignaciones de dirección IP a nombre de usuario de:
  - Dispositivos de control de acceso a la red (NAC)
  - Portal de autenticación
  - Active Directory

Prácticas recomendadas de User ID para GlobalProtect

Palo Alto Networks recomienda GlobalProtect como una solución de prácticas recomendadas para User-ID. GlobalProtect proporciona conectividad a usuarios remotos y utiliza puertas de enlace internas para recopilar asignaciones para usuarios en redes internas. Debido a que GlobalProtect requiere que los usuarios se autentiquen con sus credenciales siempre que haya un cambio en la conectividad de la red, la postura del dispositivo o el estado de autenticación del usuario, este garantiza asignaciones de usuarios precisas para la aplicación de políticas basadas en el usuario.

Planificación de las prácticas recomendadas de User-ID para la implementación de GlobalProtect

- Siga la Guía de configuración rápida de GlobalProtect para determinar la mejor forma de implementar GlobalProtect. Para User-ID, utilice la Configuración de VPN siempre activada y Configuración de puerta de enlace externa e interna combinada.
- Instale la aplicación GlobalProtect en todos los endpoints en los que desee identificar a los usuarios.
- Determine los atributos de directorio para los nombres de usuario (como UserPrincipalName, sAMAccountName o common-name) que utiliza para la autenticación de GlobalProtect. Especifique estos atributos como el nombre de usuario principal o alternativo en el Perfil de asignación de grupo.
- Si utiliza la autenticación de certificado de cliente, el campo Nombre del sujeto del certificado debe identificar el nombre de usuario. User-ID no admite certificados de máquina.
- Si solo tiene una puerta de enlace interna pero tiene otros cortafuegos que necesitan aprender asignaciones de esa puerta de enlace, planifique cómo implementará la redistribución para enviar asignaciones a otros cortafuegos.
- Determine si recibe asignaciones de varias fuentes. Si es así, evalúe las fuentes mediante la interfaz web o la CLI para determinar si las asignaciones de dirección IP a nombre de usuario recopiladas de GlobalProtect podrían ser sobrescritas por fuentes que proporcionen asignaciones que pueden ser menos precisas u oportunas que GlobalProtect.

Implemente GlobalProtect utilizando las prácticas recomendadas para User-ID

- Implemente portales y puertas de enlace de GlobalProtect. Implemente puertas de enlace internas y externas para identificar de forma coherente a los usuarios, independientemente de su ubicación.
- Utilice el método de conexión anterior al inicio sesión (siempre activada) o inicio de sesión de usuario (siempre activada) para habilitar el acceso a la red cuando utilice puertas de enlace internas y externas.
- Si usa certificados para la autenticación, implemente Certificados de cliente específicos del usuario para la autenticación utilizando el Protocolo simple de inscripción de certificados (SCEP).
- Si utiliza puertas de enlace internas, utilice la Detección de host interno para que la aplicación GlobalProtect sepa cuándo enviar un usuario a una puerta de enlace interna.
- Habilite la identificación de usuario solo en las zonas de origen. Por ejemplo, si utiliza una puerta de enlace externa de GlobalProtect, habilite User-ID en la zona asociada con la interfaz del túnel [**Network (Red)** > **Zones (Zonas)** > *tunnel-zone*].
- Si recibe asignaciones de usuarios de varias fuentes, excluya las subredes de GlobalProtect para puertas de enlace externas de GlobalProtect en los agentes de User-ID para que las asignaciones de usuarios

que proporciona GlobalProtect no sean sobrescritas por fuentes que proporcionan asignaciones que son menos precisas u oportunas que GlobalProtect.

- Configure la redistribución para compartir las asignaciones que recopilan las puertas de enlace de GlobalProtect con otros cortafuegos.
- Especifique todos los formatos de nombre de usuario que permiten a los usuarios autenticarse en GlobalProtect como el Nombre de usuario principal o como Atributos de nombre de usuario alternativo en el Perfil de asignación de grupos. Habilite **Allow matching usernames without domains (Permitir nombres de usuario coincidentes sin dominios)** [**Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User mapping (Asignación de usuarios)** > **Palo Alto Networks User-ID Agent Setup (Configuración del agente de identificación de usuario de Palo Alto Networks)**] si los usuarios no proporcionan el nombre de dominio durante la autenticación de GlobalProtect.
- Cree sus reglas de política de seguridad y compruebe que coincidan con los flujos de tráfico de usuarios previstos.

Utilice las prácticas recomendadas posteriores a la implementación de GlobalProtect para User-ID

- Mantenga y actualice las aplicaciones de GlobalProtect en los endpoints. Si tiene muchos endpoints para actualizar, aloje las actualizaciones de las aplicaciones en un servidor web para reducir la carga en el cortafuegos cuando los usuarios se conectan y descargan la aplicación o usan una herramienta de distribución de software para enviar las actualizaciones a los hosts gestionados.
- En la aplicación de GlobalProtect, confirme que los usuarios pueden conectarse correctamente a una puerta de enlace externa.
- Verifique que el cortafuegos reciba las asignaciones de dirección IP a nombre de usuario de GlobalProtect.
  - En la interfaz web, seleccione **Monitor (Supervisar)** > **User- ID** y confirme que se muestran los nombres de usuario en la columna **User (Usuario)**.
  - Utilice Comandos CLI para confirmar que el cortafuegos recibe correctamente las asignaciones.

Prácticas recomendadas de User-ID para la Supervisión de Syslog

Los cortafuegos de Palo Alto Networks pueden analizar los mensajes de Syslog para obtener asignaciones de dirección IP a nombre de usuario. Puede utilizar eventos de autenticación de dispositivos y servicios de red existentes, como soluciones VPN de terceros, soluciones de control de acceso a la red (NAC) o sistemas de gestión de eventos e información de seguridad (SIEM) mediante el uso de mensajes Syslog. Para mantener actualizadas las asignaciones de usuarios, también puede configurar el cortafuegos para analizar los mensajes de syslog para eventos de cierre de sesión, para eliminar automáticamente las asignaciones obsoletas.

Planificación de las prácticas recomendadas de User-ID para la implementación de la Supervisión de Syslog

- Revise los formatos que usan los remitentes de syslog para determinar qué sintaxis usan, si incluyen nombres de dominio y si cumplen con los criterios.
- Determine si desea supervisar eventos de inicio de sesión, eventos de cierre de sesión o ambos. Si desea supervisar los eventos de cierre de sesión, verifique que el remitente de syslog incluya tanto la dirección IP como el nombre de usuario en el mensaje.
- Según los mensajes de syslog, determine si necesita usar identificadores de campo o expresiones regulares. Si el mensaje de syslog es coherente y predecible, utilice identificadores de campo. Si el mensaje es más complejo y menos predecible, utilice regex.
- Planificación de la implementación de la Supervisión de Syslog utilizando el agente de User-ID integrado de PAN-OS en el cortafuegos y no el agente de ID de usuario de Windows.

Implemente la supervisión de Syslog utilizando las prácticas recomendadas para User-ID

- Si los remitentes de Syslog utilizan diferentes formatos, configure un perfil de análisis de Syslog para cada formato.
- Si desea supervisar los eventos de inicio de sesión y cierre de sesión, configure un perfil de análisis de Syslog para cada tipo de evento.
- Habilite **Allow matching usernames without domains (Permitir nombres de usuario coincidentes sin dominios)** si los mensajes de syslog no incluyen el nombre de dominio y los nombres de usuario son únicos en todos los dominios.
- En el agente de User-ID integrado en PAN-OS, utilice siempre SSL para escuchar los mensajes de syslog porque el tráfico está cifrado. Dado que UDP envía el tráfico en texto no cifrado, asegúrese de que tanto el emisor syslog como el cliente estén en una red dedicada y segura para evitar que hosts no fiables puedan enviar tráfico UDP al cortafuegos.
- Verifique que todos los remitentes de Syslog que desea supervisar estén incluidos como entradas en la lista de Supervisión del servidor, ya que el cortafuegos ignora los mensajes de Syslog de los remitentes que no están en esta lista.
- Ordene las entradas en la Lista de filtros en el orden de la coincidencia más probable. Por ejemplo, si cree que el 80 % de los mensajes de syslog coincidirán con filter1 y el 20 % con filter2, asegúrese de que filter1 preceda a filter2 en la lista.

Utilice las prácticas recomendadas posteriores a la implementación de la Supervisión de Syslog para User-ID

- Valide que los mensajes de syslog coincidan con los perfiles de análisis de Syslog y que el cortafuegos reciba la asignación de dirección IP a nombre de usuario de los mensajes de syslog.
- Utilice el Comando de la CLI `show user server-monitor statistics` para validar que el cortafuegos recibe los mensajes de los remitentes de syslog y asigna los usuarios de forma correcta.

Prácticas recomendadas de User ID para la redistribución

En una red a gran escala, en lugar de configurar todos sus cortafuegos para consultar directamente la asignación de fuentes de información, puede dinamizar el uso de recursos configurando cortafuegos para recoger la información de asignación que ya existe en otros cortafuegos a través de la redistribución.

Planifique las prácticas recomendadas de User-ID para la Implementación de redistribución

- Planifique la arquitectura de redistribución. Algunos factores que deben considerarse son los siguientes:
  - ¿Qué cortafuegos aplicarán políticas para todos los tipos de datos (como asignaciones de dirección IP a nombre de usuario o información de cuarentena de dispositivos) y qué cortafuegos deberían recibir un subconjunto de datos?
  - ¿Qué rangos de IP requieren asignaciones de dirección IP a nombre de usuario?
  - Si tiene una puerta de enlace interna que proporciona asignación de usuarios, ¿qué otros dispositivos requieren esos datos? ¿Qué función y rol tendrán?
  - ¿Cómo se puede minimizar el número de saltos necesarios para agregar todos los datos? El número máximo de saltos permitido para asignaciones de dirección IP a nombre de usuario es diez y el número máximo de saltos permitido para asignaciones de nombre de usuario a etiqueta y asignaciones de dirección IP a etiqueta es uno.
  - ¿Cómo puede minimizar la cantidad de cortafuegos que consultan las fuentes de información de asignación de usuarios? Mientras menor sea la cantidad de cortafuegos que consultan, menor será la carga de procesamiento en los cortafuegos y las fuentes.
- Determine la mejor opción para su hub de redistribución:
  - Un cortafuegos VM-Series dedicado es más adecuado para las implementaciones de User-ID a gran escala. Si solo está redistribuyendo asignaciones de usuarios, un modelo VM-50 es suficiente. Si planifica redistribuir también las asignaciones de dirección IP a etiqueta, le recomendamos que utilice un modelo VM-300 o superior.
  - Panorama es más adecuado para entornos de mediana a pequeña escala, y si no utiliza syslog o la supervisión del servidor para recopilar asignaciones de usuarios.
- Según los requisitos de su red, determine qué tipo de topología desea utilizar:
  - Hub-and-spoke para una sola región
  - Hub-and-spoke para múltiples regiones
  - Jerárquica

Implementación de la redistribución con las prácticas recomendadas para User-ID

- Configure las fuentes de la información que desea redistribuir:
  - Asignaciones de dirección IP a nombre de usuario de User-ID (incluidos los agentes de User-ID de Windows)
  - Asignaciones de dirección IP a etiqueta para grupos de direcciones dinámicas
  - Asignaciones de nombre de usuario a etiqueta para grupos de usuarios dinámicos

- Datos para la Aplicación de políticas basadas en HIP
- Información de cuarentena del dispositivo

- Configure qué redes desea que el agente o agentes incluyan en la redistribución de datos y qué redes desea excluir de la redistribución de asignaciones de dirección IP a etiqueta o asignaciones de dirección IP a nombre de usuario.
- Utilice la Lista incluir/excluir redes para definir las subredes que el agente de redistribución incluye o excluye cuando redistribuye las asignaciones.
- Configure qué redes o recursos reciben tipos de datos específicos a través de la redistribución.
- Habilite la Autenticación con certificados personalizados para redistribución para utilizar un certificado personalizado para la autenticación mutua entre los agentes de redistribución y los clientes.
- Utilice un cortafuegos VM-Series o Panorama para redistribuir los datos. Dado que Panorama puede ser un agente o un cliente, utilice **Panorama** > **Data Redistribution (Redistribución de datos)** para configurar la redistribución de datos en Panorama.
- Si un cortafuegos que aplica políticas necesita asignaciones de usuarios remotos y locales porque también es una puerta de enlace de GlobalProtect y un centro de datos, habilite la redistribución bidireccional.
- Para garantizar una resistencia óptima, debe habilitar la redistribución bidireccional solo dentro de una región, no entre regiones.

Utilice las prácticas recomendadas posteriores a la implementación de redistribución para User-ID

- Siga los dos últimos pasos en Configuración de la redistribución de datos para verificar que los agentes redistribuyan correctamente los datos a los clientes.

Prácticas recomendadas de User ID para la asignación de grupos

La definición de reglas de políticas que se basen en la pertenencia a grupos de usuarios en lugar de en usuarios individuales simplifica la administración porque usted no tiene que actualizar las reglas siempre que cambia a pertenencia al grupo. Se recomiendan las siguientes prácticas recomendadas para configurar la asignación de grupo para implementaciones del Protocolo ligero de acceso a directorios (LDAP).

Las siguientes secciones describen las prácticas recomendadas para implementar la asignación de grupo para servicios de directorio in situ.

Planificación de las prácticas recomendadas de User-ID para la implementación de mapas de grupo

- Identifique su servicio de directorio (como Active Directory o un servicio basado en LDAP como OpenLDAP) e identifique la topología para sus servidores de directorio. Algunas preguntas a tener en cuenta son:
  - ¿Cuántos servidores de directorio, centros de datos y controladores de dominio hay?
  - ¿Cuáles son sus fuentes principales de información de grupo?
  - ¿Dónde están ubicados los controladores de dominio en relación con sus servidores de directorio?
  - ¿Están los servidores de directorio y los controladores de dominio en diferentes regiones?
  - ¿Qué recursos son locales y cuáles regionalizados?
- Para implementaciones en las que su fuente principal de asignaciones de grupos es un servidor de Active Directory:
  - Si tiene un único dominio, solamente necesita una configuración de asignación de grupos con un perfil de servidor LDAP que conecte el cortafuegos con el controlador de dominio utilizando la mejor conectividad. Añadir hasta cuatro controladores de dominio al perfil de servidor LDAP para redundancia.
  - Si tiene grupos universales, cree un perfil de servidor LDAP para conectarse al dominio raíz del servidor de catálogo global en el puerto 3268 o 3269 para SSL y, después, cree otro perfil de servidor LDAP para conectarse a los controladores de dominio raíz utilizando LDAPS en el puerto 636. Si no utiliza TLS, use el puerto 389. Esto ayuda a garantizar que la información de usuarios y grupos esté disponible para todos los dominios y subdominios.
  - Si no tiene Grupos universales y tiene varios dominios o varios bosques, debe crear una configuración de asignación de grupo con un perfil de servidor LDAP que conecte el cortafuegos a un servidor de dominio en cada dominio/bosque. Tome las medidas oportunas para garantizar que los nombres se usuarios son exclusivos en los distintos bosques.
  - Antes de utilizar la asignación de grupos, configure un Nombre de usuario principal para las políticas de seguridad basadas en el usuario, dado que este atributo identifica a los usuarios en la configuración de la política, los logs y los informes.
- Para crear un grupo personalizado que aún no está disponible en su directorio LDAP, utilice atributos de usuario para crear grupos personalizados.
- Asegúrese de que las configuraciones de asignación de grupos no contengan grupos superpuestos, si crea varias configuraciones de asignación de grupos que utilizan el mismo nombre distinguido (DN) base

o servidor LDAP. Por ejemplo, la Lista de inclusión para una configuración de asignación de grupo no puede contener un grupo que también esté en una configuración de asignación de grupo diferente.

- Asegúrese de que los nombres de usuario y los atributos de grupo sean únicos para todos los usuarios y grupos dentro de cada dominio.
- Recupere solo los grupos que va a utilizar en su política de seguridad basada en grupos y en su configuración utilizando la lista de inclusión de grupos o aplicando un filtro de búsqueda personalizado.
- Evalúe la frecuencia con la que cambian los grupos en sus directorios para determinar el valor óptimo del **Update Interval (Intervalo de actualización)** para su Perfil de asignación de grupos. Por ejemplo, si sus grupos cambian con frecuencia, configure un valor menor, pero si por lo general son estáticos, introduzca un valor mayor.
- Determine el atributo de nombre de usuario que desea que representen a los usuarios en los logs, informes y en la configuración de políticas. Si sus fuentes de User-ID envían nombres de usuario en diferentes formatos, especifique esos nombres de usuario como atributos alternativos.

Asegúrese de que el nombre de usuario principal, el nombre de usuario alternativo y el atributo de correo electrónico sean únicos para cada usuario.

Implementación de la asignación de grupos mediante las prácticas recomendadas para User-ID

- Si está utilizando solo grupos personalizados de un directorio, añada un grupo no utilizado a la Lista de inclusión para evitar que User-ID recupere todos los grupos del directorio.
- Utilice la **Group Include List (Lista de inclusión de grupos)** para limitar las reglas de política a grupos específicos. De forma alternativa, filtre los grupos que el cortafuegos supervisa para la asignación de grupos introduciendo un **Search Filter (Filtro de búsqueda)** (consulta LDAP) y **Object Class (Clase de objeto)** (definición de grupo). Si no tiene un grupo disponible en su directorio LDAP, puede usar atributos de usuario para crear grupos personalizados en el cortafuegos. Asegúrese de que los atributos utilizados para formar grupos personalizados sean atributos indexados en el directorio.
- Especifique el nombre de usuario principal que identifica a los usuarios en informes y logs.

Utilice las prácticas recomendadas posteriores a la implementación de asignación de grupos para User-ID

- Para confirmar la conectividad al servidor LDAP, utilice el comando de la CLI `show user group-mapping state all`.
- Para ver las pertenencias a grupos, ejecute el comando `show user group name <nombre de grupo>`.
- Confirme que el usuario existe en un grupo antes de usar ese grupo en su política de seguridad. Para verificar qué grupos puede utilizar actualmente en las reglas de la política, utilice el comando de la CLI `show user group`.
- Si realiza cambios en la asignación de grupos, actualice la caché manualmente. Para actualizar manualmente la caché, ejecute el comando `debug user-id refresh group-mapping all`.

Prácticas recomendadas de User ID para grupos de usuarios dinámicos

Los grupos de usuarios dinámicos le permiten responder a los cambios en el comportamiento de los usuarios, las necesidades comerciales o las amenazas potenciales sin cambios manuales en las políticas, o sin crear y actualizar los grupos. Los grupos de usuarios dinámicos le ayudan a crear una política de seguridad que proporcione:

- Acceso a recursos por tiempo limitado para usuarios
- Corrección automática para el comportamiento anómalo del usuario y la actividad maliciosa mientras se mantiene la visibilidad del usuario

Después de definir los criterios del grupo mediante etiquetas y confirmar los cambios, la pertenencia del grupo de usuarios dinámicos se actualiza automáticamente en función de las etiquetas del usuario.

Planificación de las prácticas recomendadas de User-ID para la implementación dinámica de grupos de usuarios

- ❑ En función de factores como los cambios en las necesidades comerciales o el comportamiento del usuario, identifique cómo desea que el cortafuegos controle el acceso de los usuarios:
  - ❑ ¿Quiere permitir o restringir el acceso a través de la política de seguridad?
  - ❑ ¿Quiere exigir una autenticación multifactor (MFA) a los usuarios?
  - ❑ ¿Quiere descifrar el tráfico del usuario para obtener más visibilidad de la actividad del usuario?
- ❑ Determine la duración de la pertenencia del usuario a un grupo dinámico de usuarios específico.
  - ❑ ¿Debería el cortafuegos eliminar automáticamente al usuario del grupo en función del tiempo (por ejemplo, el número de horas que un servicio externo necesita para acceder temporalmente a los recursos)?
  - ❑ ¿Debería el cortafuegos requerir un evento específico para asociar o desvincular a los usuarios del grupo (por ejemplo, actividad maliciosa)?
- ❑ Evalúe qué eventos genera el cortafuegos que pueden identificar un cambio en el comportamiento del usuario o las necesidades comerciales. Puede asignar etiquetas a través de la API, auto-tagging o manualmente mediante la interfaz web.
  - ❑ Según sus casos de uso, determine qué etiquetas utilizará para agrupar usuarios y cómo generará la etiqueta.
  - ❑ Por ejemplo, evalúe el nivel de riesgo del usuario en función de su comportamiento, como "riesgo alto", "riesgo medio" y "riesgo bajo" según la información de los dispositivos y aplicaciones de seguridad, y asigne etiquetas automáticamente a los usuarios en base a esos eventos.
- ❑ Identifique las fuentes de información del usuario para las etiquetas:
  - ❑ Logs del cortafuegos
    - Para los logs de autenticación, datos, amenazas, tráfico, inspección de túnel, URL y WildFire, cree un perfil de reenvío de logs y utilice las acciones integradas.
    - Para los logs de User-ID, coincidencias HIP, GlobalProtect e IP-Tag, establezca la configuración de log.
  - ❑ Cortex XSOAR
  - ❑ Sistemas de gestión de eventos e información de seguridad (SIEMS), como Splunk

- Secuencias de comandos API personalizadas
- Combine etiquetas de varias fuentes para definir los criterios para grupos de usuarios dinámicos. Por ejemplo, es posible que desee denegar el acceso al usuario solo si recibe alertas de varias aplicaciones de seguridad indicándole que las credenciales del usuario se han visto comprometidas, en lugar de solo una aplicación, según el nivel de confianza.

Implementación de grupos de usuarios dinámicos utilizando las prácticas recomendadas para User-ID

- Si tiene una gran cantidad de usuarios que desea añadir a un grupo de usuarios dinámico o si desea añadir usuarios en función de eventos de otras aplicaciones de seguridad, utilice las API para añadir los usuarios en lugar de la interfaz web .
- Utilice la API o defina manualmente el **Timeout (Tiempo de espera)** que representa cuándo eliminar usuarios de este grupo (por ejemplo, al vencimiento del contrato).
- Cree reglas de política de seguridad que utilicen el grupo de usuarios dinámicos como el usuario de origen para controlar el acceso de los usuarios, habilitar MFA o descifrar el tráfico de los usuarios que son miembros de los grupos de usuarios dinámicos.
- Configure fuentes para proporcionar información para las etiquetas de usuario:
  - Si usa logs de cortafuegos, configure el etiquetado automático para etiquetar al usuario.
  - Si usa Splunk, puede asignar etiquetas a los usuarios con la Aplicación de Palo Alto Networks para Splunk.
  - Utilice libros de estrategia en Cortex XSOAR u otras plataformas de organización, automatización y respuesta de seguridad (SOAR) para aplicar etiquetas a los usuarios en función de eventos específicos.
  - Si utiliza secuencias de comandos personalizadas, modifique la secuencia de comandos para completar las etiquetas utilizando la API.
  - Añada usuarios a los grupos manualmente mediante la interfaz web del cortafuegos.

Utilice las prácticas recomendadas posteriores a la implementación del grupo de usuarios dinámicos para User-ID

- Revise la pertenencia de su grupo para asegurarse de que solo los usuarios que desea incluir sean miembros del grupo. Si el grupo incluye usuarios que no pertenecen al grupo (por ejemplo, empleados permanentes en el grupo "acceso de contratista"), debe **Unregister Users (Anular el registro de usuarios)** para eliminar sus asignaciones de nombre de usuario a etiqueta y **Delete (Eliminar)** las asignaciones del grupo.
- Revise los logs de ID de usuario para verificar que el cortafuegos genere correctamente las etiquetas para los usuarios.
- Utilice los Comandos de la CLI para obtener más información sobre sus grupos de usuarios dinámicos (por ejemplo, para ver qué usuarios están asociados con los grupos).
- Utilice la columna de grupo de usuarios dinámicos en los logs de tráfico y amenazas para asegurarse de que el cortafuegos haga coincidir los grupos con las políticas de seguridad previstas.
- Redistribuya las etiquetas de usuario a otros cortafuegos para garantizar que todos los cortafuegos apliquen la política de seguridad de forma coherente. Tenga en cuenta que puede redistribuir las etiquetas de usuario para un solo salto.