Panda SIEMFeeder

Guía de infraestructura de Panda SIEMFeeder

Autor: Panda Security

Versión: 3.10.00

Fecha: 10/04/2025

panda

Aviso legal.

Marcas registradas.

Información de contacto.

Oficinas centrales:

Panda Security

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 España.

https://www.pandasecurity.com/es/office-locator/

Acerca de la Guía de infraestructura de Panda SIEMFeeder

Para obtener la versión más reciente de la documentación en formato PDF consulta la dirección web:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-ES.pdf

Descarga del software Panda SIEMFeeder

Para obtener el paquete de instalación Panda SIEMFeeder consulta la url **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA**

Guía de eventos Panda SIEMFeeder

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-ManualDescripcionEventos-ES.pdf

Guía de administración de Panda Adaptive Defense 360y Panda Adaptive Defense

Guías de administración para productos Aether:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSE360oAP-guia-ES.pdf

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSEoAP-guia-ES.pdf

Guía de uso de Panda Partner Center

Para obtener la versión más reciente de esta guía consulta la dirección web:

http://documents.managedprotection.pandasecurity.com/AdvancedGuide/PARTNERCENTER- Manual-ES.pdf

Para consultar un tema específico, accede a la ayuda online del producto en la dirección web:

https://documents.managedprotection.pandasecurity.com/Help/v77000/Partners/es-es/Content/index.htm

Soporte técnico

Panda Security ofrece un soporte técnico global cuyo objetivo principal es responder a cuestiones especificas sobre el funcionamiento de sus productos. El equipo de soporte técnico también genera documentación sobre detalles técnicos del producto, que ofrece a través de su portal eKnowledge Base.

Para acceder a información específica del producto consulta la siguiente URL:

https://www.pandasecurity.com/es/support/siemfeeder/

Encuesta sobre la Guía de infraestructura de Panda SIEMFeeder

Evalúa esta guía para administradores y enviamos sugerencias y peticiones para próximas versiones de la documentación en:

https://es.surveymonkey.com/r/feedbackSIEMFeederInfManES

Tabla de contenidos

Capítulo 2

Prólogo

Esta guía contiene la información y los procedimientos de uso necesarios para la puesta en marcha del servicio Panda SIEMFeeder y Panda SIEMFeeder for Partners.

Contenido del capítulo

Público objetivo de la documentación

Esta documentación está dirigida a dos tipos de publico objetivo:

- Al personal técnico que gestiona los sistemas informáticos de las empresas que han contratado el servicio Panda SIEMFeeder.
- Al personal técnico del proveedor de servicios de seguridad (MSSP) que ha contratado el servicio Panda SIEMFeeder for Partnersde Panda.

Productos de seguridad compatibles

Panda SIEMFeeder y Panda SIEMFeeder for Partners requieren alguno de los productos siguientes instalados en los equipos protegidos:

- Panda Adaptive Defense (compatible con Panda SIEMFeedery Panda SIEMFeeder for Partners)
- Panda Adaptive Defense 360 (compatible con Panda SIEMFeedery Panda SIEMFeeder for Partners)

Los procedimientos e indicaciones mostradas en este manual son aplicables a todos los productos mencionados. En este manual se hace referencia a "Panda Adaptive Defense" de forma genérica, dado que no se establecen diferencias con respecto al servicio.

Estructura de la documentación suministrada

La información recogida en este manual se divide en tres bloques, dirigidos a diferentes áreas o perfiles técnicos dentro del departamento de IT de la empresa o del MSSP:

- **Información de arquitectura**: incluida en los capítulos 2 y 3, dirigida al arquitecto de sistemas que necesita obtener una visión general del servicio para valorar el alcance de los cambios en la infraestructura IT y generar procedimientos de gestión y recuperación.
- **Información de requisitos del servicio**: incluida en el capítulo 4, dirigida al administrador de sistemas que necesita aprovisionar los recursos necesarios para el buen funcionamiento del servicio.
- **Información para el despliegue del servicio**: incluida en los capítulos 5 y 6, dirigida al especialista en seguridad informática que configura los accesos de red necesarios para habilitar la integración del servicio en el servidor SIEM de la empresa o del MSSP.

Iconos

En esta guía se utilizan los siguientes iconos:

Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consulta en otro capítulo o punto del manual.

Capítulo 3

Arquitectura Panda SIEMFeeder

Panda SIEMFeeder es el servicio de Panda para clientes finales que entrega a la plataforma SIEM instalada en tu infraestructura toda la información y conocimiento generado por los productos Panda Adaptive Defense.

Panda SIEMFeeder te permite:

- Descubrir amenazas desconocidas, ataques dirigidos y malware avanzado de tipo APT (Advanced Persistent Threats)
- Ampliar la visibilidad de la actividad de los procesos ejecutados en los equipos de las organizaciones.

Para conocer más detalles de la solución equivalente a Panda SIEMFeeder para proveedores de servicios de seguridad Panda SIEMFeeder for Partners, consulta ***Arquitectura Panda SIEMFeeder for Partners*** *en la página* ***17***.

Contenido del capítulo

Objetivos del servicio

Panda SIEMFeeder sirve de nexo o unión entre el software de protección instalado en los equipos de la red que gestionas y el servidor SIEM de tu organización. Panda SIEMFeeder establece el flujo de información siguiente:

1. La monitorización permanente de Panda Adaptive Defense envía a la nube de Panda la información de telemetría generada por la actividad de las aplicaciones ejecutadas en los equipos del parque informático del cliente.
2. Panda SIEMFeeder enriquece esta información con la inteligencia de seguridad generada por Panda.
3. Panda Importer recupera la información enriquecida desde la plataforma Azure que tienes asignada, y la envía directamente a tu servidor SIEM o a alguna de las plataformas compatibles (Kafka y Syslog) para que puedas explotarla posteriormente.

Enriquecimiento de la actividad monitorizada

Panda Adaptive Defense monitoriza las acciones ejecutadas por los procesos en los equipos de tu infraestructura. Estas acciones se envían a la plataforma Cloud de Panda, donde se analizan mediante técnicas Machine Learning ejecutadas sobre una infraestructura Big data, para extraer inteligencia de seguridad. Con esta información, Panda clasifica todos y cada uno de los procesos que ejecutan tus usuarios con una fiabilidad del 99'999%.

Panda SIEMFeeder reúne la información de los eventos monitorizados por Panda Adaptive Defense y la información de seguridad generada, creando un único flujo de datos compatible con el servidor SIEM instalado en tu infraestructura.

Panda SIEMFeeder no requiere cambios de configuración en los equipos de tus usuarios: el servicio opera dentro de la infraestructura de Panda y recibe los datos de forma centralizada desde cada uno de los puestos y servidores que pertenecen a tu infraestructura. Estos datos son normalizados, enriquecidos y enviados a tu servidor SIEM para su explotación.

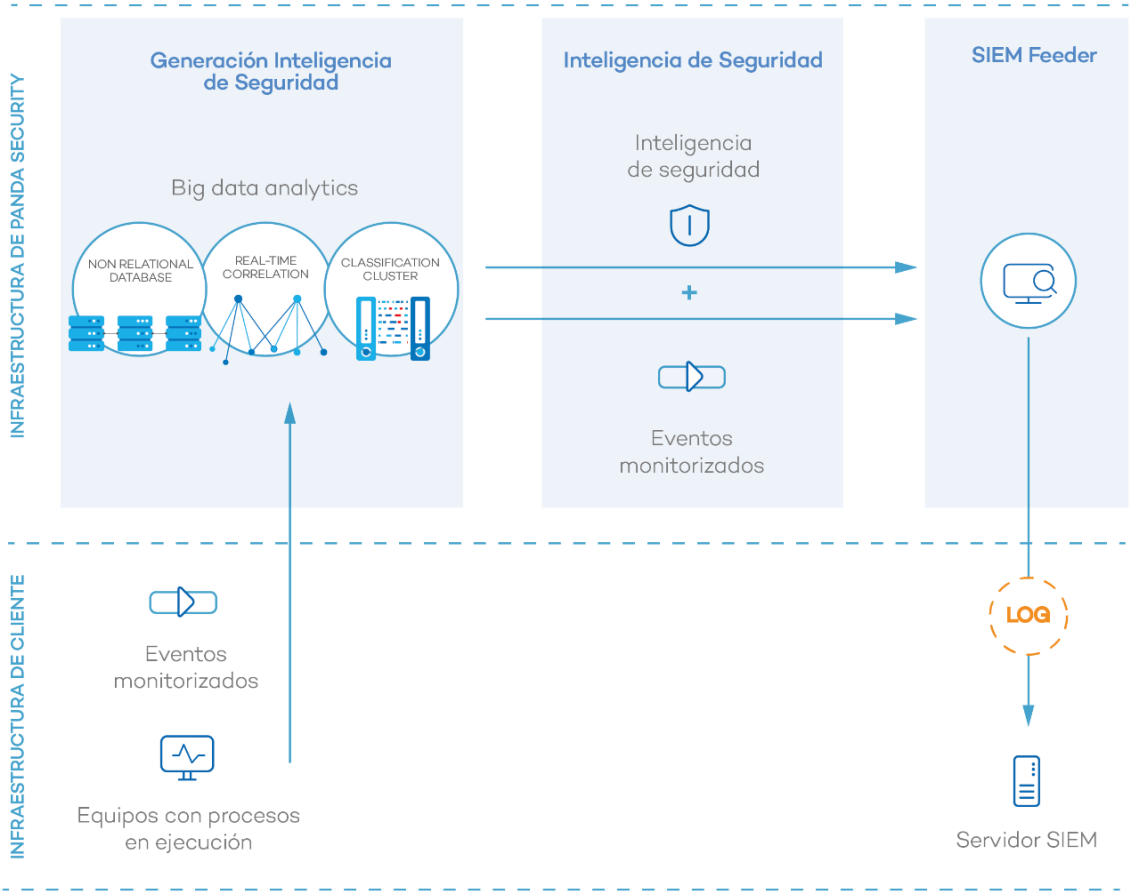

Figura 3.1: Flujo de información generada por Panda Adaptive Defense y Panda SIEMFeeder

Beneficios del servicio

Panda SIEMFeeder suministra información sobre la actividad de los procesos ejecutados en el parque que administras. Con esta información puedes:

- **Visualizar la evolución del estado del malware detectado en la red**, indicando si fue ejecutado o no, el vector de infección y las acciones ejecutadas por el proceso. De esta forma puedes elegir la estrategia de resolución y adaptar las políticas de seguridad de tu empresa.
- **Visualizar las acciones ejecutadas por cada proceso** independientemente de su clasificación, para detectar actividades sospechosas de los programas ejecutados. Panda SIEMFeeder recopila indicios que te permiten obtener conclusiones acerca de su potencial peligrosidad.
- **Visualizar los accesos de los procesos a la información confidencial de tu empresa** para prevenir su extracción o robo.Panda SIEMFeeder te muestra los ficheros de ofimática accedidos, bases de datos y otros repositorios de información confidencial.

- **Visualizar las conexiones de red establecidas por los procesos** para identificar destinos sospechosos y susceptibles de extraer datos.
- **Localizar todos los programas ejecutados**, y especialmente aquellos instalados en los equipos de los usuarios y que contengan vulnerabilidades conocidas, para ayudarte a diseñar un plan de actualización de software y afinar las políticas de seguridad establecidas.

Arquitectura general

El servicio Panda SIEMFeeder está formado por los módulos mostrados en el diagrama:

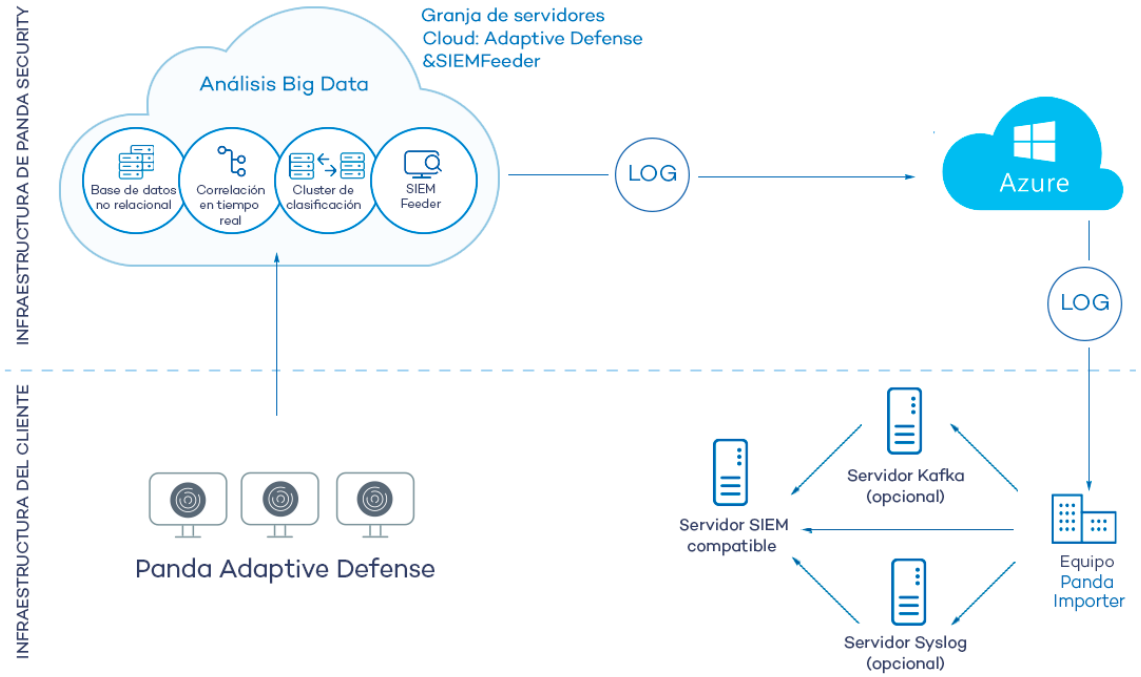

Figura 3.2: Esquema lógico de los módulos que constituyen Panda SIEMFeeder y su relación

En la figura se representan los siguientes elementos:

- **Equipos de la infraestructura de red**: protegidos con Panda Adaptive Defense o Panda Adaptive Defense 360.
- **Nube de Panda**: almacena la información de los procesos ejecutados y los analiza para extraer inteligencia de seguridad.
- **Servicio Panda SIEMFeeder**: recoge los eventos y la información de inteligencia de seguridad para empaquetarlos en forma de logs y enviarlos a la plataforma Azure.
- **Infraestructura Azure**: recibe los logs del servicio Panda SIEMFeeder y los almacena temporalmente en espera de la descarga desde Panda Importer.
- **Equipo Panda Importer**: equipo en la red del cliente que ejecuta el proceso Panda Importer para comprobar si hay logs nuevos disponibles en la plataforma Azure para descargarlos y

almacenarlos.

- **Servidor Kafka (opcional)**: equipo que pertenece a la infraestructura del cliente que gestiona las colas de los logs recibidos por Panda Importer y los envía al servidor SIEM.
- **Servidor Syslog (opcional)**: equipo que pertenece a la infraestructura del cliente que recoge los logs recibidos por Panda Importer y los envía al servidor SIEM.
- **Servidor SIEM**: equipo que pertenece a la infraestructura del cliente y recoge los datos descargados por el equipo Panda Importer para generar paneles de control que ayudan a localizar los procesos sospechosos de ser una amenaza para la seguridad del cliente.
- **Cortafuegos perimetrales y locales**: protegen la salida y entrada de datos entre el equipo Panda Importer y la plataforma Azure.

Beneficios de la plataforma Azure

Panda SIEMFeeder genera logs de forma asíncrona y los almacena temporalmente hasta que Panda Importer los recupera e integra en tu sistema SIEM. Para ello, utiliza servicios Cloud alojados en la plataforma Azure, con las siguientes características:

- **Almacenamiento en la nube**: servicio configurado en alta disponibilidad, accesible desde cualquier lugar y en cualquier momento las 24 horas del día. Con un es espacio asignado de 80 Gigabytes y máximo de 7 días de retención.
- **Comunicaciones cifradas**: el intercambio de información entre el equipo Panda Importer y la plataforma Azure se cifra con el protocolo de encriptación SSL.
- **Comunicaciones autenticadas**: para gestionar la autenticación y la autorización, Panda Importer utiliza dos tokens independientes que le permiten negociar la clave compartida necesaria para acceder a la plataforma Panda SIEMFeeder. Cada token tiene un tiempo de caducidad diferente que garantiza la confidencialidad del acceso a la información.

*Para obtener mas información, consulta **Apéndice II: Arquitectura de seguridad** en la página **63***

- **Comunicaciones comprimidas**: la plataforma Azure almacena los datos comprimidos para minimizar el ancho de banda requerido de la descarga.
- **Mecanismo PUSH de entrega**: para facilitar la configuración de los cortafuegos, la dirección de las conexiones con la infraestructura Azure es saliente desde tu red. Una vez que Panda Importer establece el canal de comunicación, Azure le envía los logs nuevos disponibles en la plataforma mediante mensajes de tipo PUSH.

Recorrido del flujo de información

1. Panda Adaptive Defense recoge la actividad de los procesos ejecutados gracias a la monitorización permanente, y envía la información a la nube de Panda.
2. En la nube de Panda la información se completa con inteligencia de seguridad y se deposita en la infraestructura Azure, donde residirá temporalmente.
3. El programa Panda Importer se ejecuta en un servidor de tu infraestructura, descarga los logs almacenados en la plataforma Azure y, dependiendo de su configuración, los gestiona de distintas maneras:
    1. Almacena los logs en una carpeta directamente accesible por el servidor SIEM de tu organización, y gestiona el volumen de ficheros guardados para no sobrepasar los límites que has fijados.
    2. Envía los logs a un servidor de colas Kafka en tu organización para que el servidor SIEM los recoja al ritmo que le permitan sus recursos.
    3. Envía los logs a un servidor de Syslog en tu organización para que el servidor SIEM los recoja al ritmo que le permitan sus recursos disponibles.
4. El servidor SIEM importará los logs y los analizará periódicamente para incorporar la información a su repositorio y generar los paneles de control apropiados.

Capítulo 4

Arquitectura Panda SIEMFeeder for Partners

Panda SIEMFeeder for Partners es el servicio de Panda para partners que entrega a la plataforma SIEM instalada en tu infraestructura toda la información y conocimiento generado por los productos Panda Adaptive Defense instalados en los equipos de tus clientes.

Panda SIEMFeeder for Partners te permite:

- Descubrir amenazas desconocidas, ataques dirigidos y malware avanzado de tipo APT (Advanced Persistent Threats)
- Ampliar la visibilidad de la actividad de los procesos ejecutados en los equipos de las organizaciones.

Contenido del capítulo

Objetivos del servicio

Panda SIEMFeeder for Partners sirve de nexo o unión entre el software de protección instalado en los equipos de tus clientes y tu servidor SIEM. Panda SIEMFeeder establece el flujo de información siguiente:

1. La monitorización permanente de Panda Adaptive Defense envía a la nube de Panda la información de telemetría generada por la actividad de las aplicaciones ejecutadas en los equipos de tus clientes.

2. Panda SIEMFeeder for Partners enriquece esta información con la inteligencia de seguridad generada por Panda.
3. Panda Importer recupera la información enriquecida desde la plataforma Azure que tienes asignada, y la envía directamente a tu servidor SIEM o a alguna de las plataformas compatibles (Kafka y Syslog) para que puedas explotarla posteriormente.

Enriquecimiento de la actividad monitorizada

Panda Adaptive Defense monitoriza las acciones ejecutadas por los procesos en los equipos de tus clientes. Estas acciones se envían a la plataforma Cloud de Panda, donde se analizan mediante técnicas Machine Learning ejecutadas sobre una infraestructura Big data, para extraer de forma automatizada inteligencia de seguridad avanzada. Con esta información, Panda clasifica todos los procesos que ejecutan tus clientes con una fiabilidad del 99'999%.

Panda SIEMFeeder for Partners reúne la información de los eventos monitorizados por Panda Adaptive Defense y la información de seguridad generada, creando un único flujo de datos compatible con el servidor SIEM instalado en tu infraestructura.

Panda SIEMFeeder for Partners no requiere cambios de configuración en los equipos de tus clientes: el servicio opera dentro de la infraestructura de Panda, y recibe los datos de forma centralizada desde cada uno de los puestos y servidores que pertenecen a la infraestructura IT tus clientes. Estos datos son normalizados, enriquecidos y enviados tu servidor SIEM para su explotación.

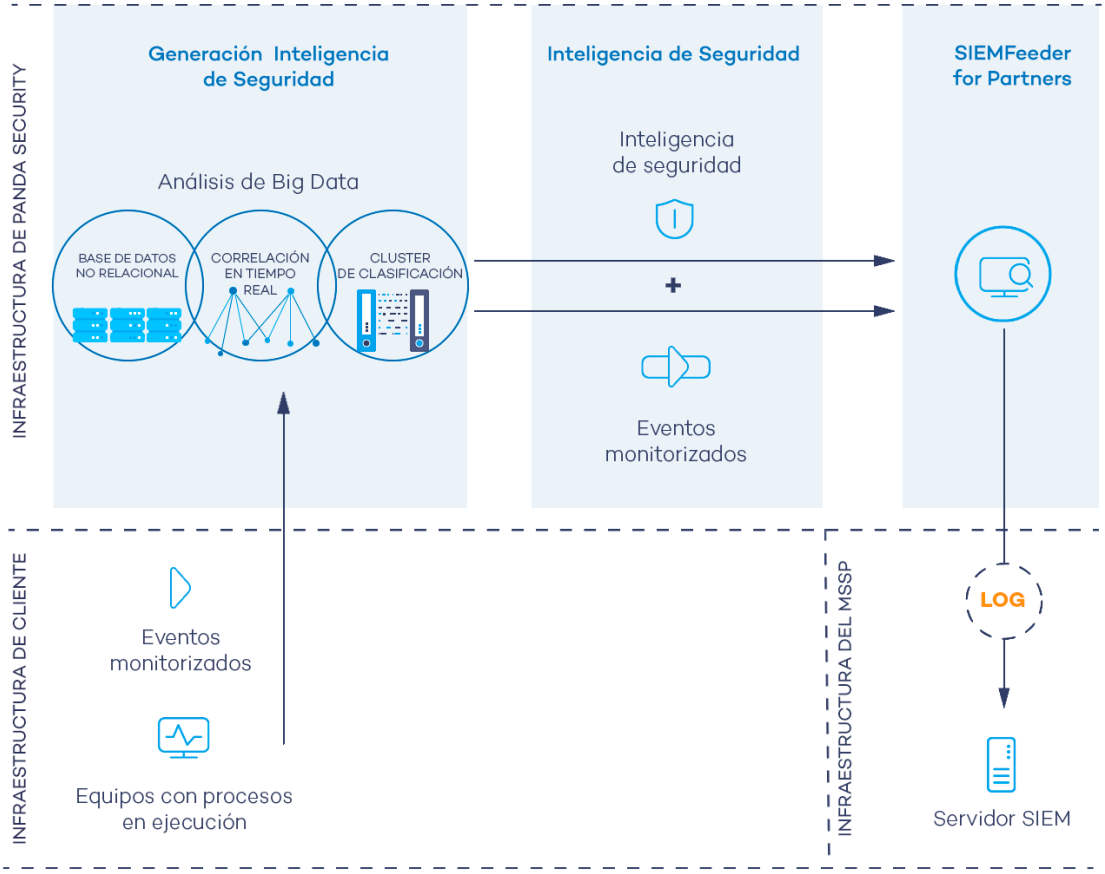

Figura 4.1: Flujo de información generada por Panda Adaptive Defense y Panda SIEMFeeder

Beneficios del servicio

Panda SIEMFeeder for Partners suministra información sobre la actividad de los procesos ejecutados en el parque de tus clientes. Con esta información puedes:

- **Visualizar la evolución del estado del malware detectado en la red de tus clientes**, indicando si fue ejecutado o no, el vector de infección y las acciones ejecutadas por el proceso. De esta forma puedes elegir las estrategias de resolución y adaptar las políticas de seguridad de las empresas que gestionas.
- **Visualizar las acciones ejecutadas por cada proceso**, independientemente de su clasificación, para detectar actividades sospechosas de los programas. Panda SIEMFeeder for Partners recopila indicios que permiten obtener conclusiones acerca de su potencial peligrosidad.
- **Visualizar los accesos de los procesos a la información confidencial de tus clientes** para prevenir su extracción o robo. Panda SIEMFeeder te muestra los ficheros de ofimática accedidos, bases de datos y otros repositorios de información confidencial.

- **Visualizar las conexiones de red establecidas por los procesos** para identificar destinos sospechosos y susceptibles de extraer datos.
- **Localizar todos los programas ejecutados**, y especialmente aquellos instalados en los equipos de los usuarios que contengan vulnerabilidades conocidas, para ayudarte a diseñar de un plan de actualización de software y a refinar las políticas de seguridad establecidas en las empresas que gestionas.
- **Aplicar configuración centralizada a través de Panda Partner Center**, que te permite asignar configuraciones para todos tus clientes de forma simultánea.
- **Instalar el servicio con seguridad y fácilmente** ya que se puedes configurar el servicio de descarga de la telemetría una sola vez, y añadir nuevos clientes sin tener que desplegar ni instalar ningún elemento adicional. Además, Panda SIEMFeeder for Partners garantiza la seguridad en las descargas mediante el uso de conexiones seguras TLS (Transport Layer Security) desde la nube de Panda.
- **Controlar los costes de almacenamiento** al filtrar los eventos antes de que lleguen a tu infraestructura, lo que supone minimizar el ancho de banda y el almacenamiento que consumirás.

Arquitectura

El servicio Panda SIEMFeeder for Partners está formado por los módulos mostrados en el diagrama:

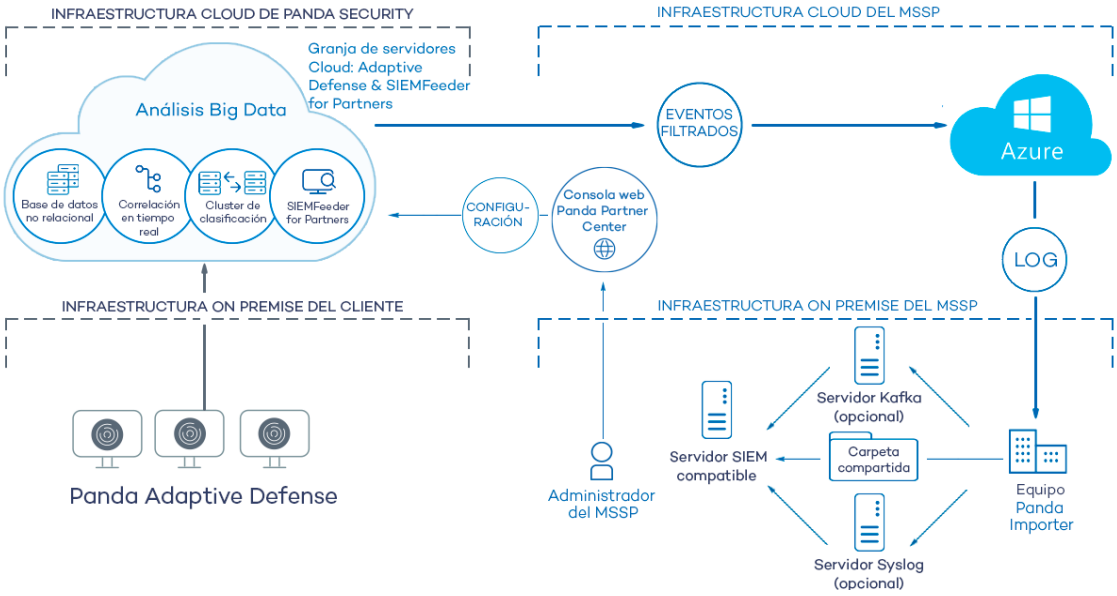

Figura 4.2: Esquema lógico de los módulos que constituyen Panda SIEMFeeder for Partners y su relación

En la figura se representan los siguientes elementos:

- **Equipos de la red del cliente**: protegidos con Panda Adaptive Defense o Panda Adaptive Defense 360.

- **Nube de Panda**: almacena la información de los procesos ejecutados y los analiza para extraer inteligencia de seguridad.
- **Servicio Panda SIEMFeeder for Partners**: recibe los eventos y la información de inteligencia de seguridad y los empaqueta en forma de logs para enviarlos a la plataforma Azure.
- **Infraestructura Azure del MSSP**: recibe los logs del servicio Panda SIEMFeeder for Partners y los almacena temporalmente en espera de la descarga desde Panda Importer.
- **Equipo Panda Importer**: equipo en la red del MSSP que ejecuta el proceso Panda Importer para comprobar si hay logs nuevos disponibles en la plataforma Azure para descargarlos y almacenarlos.
- **Servidor Kafka (opcional)**: equipo de la red del MSSP que gestiona las colas de los logs recibidos por Panda Importer y los envía al servidor SIEM.
- **Servidor Syslog (opcional)**: equipo de la red del MSSP que recoge los logs recibidos por Panda Importer y los envía al servidor SIEM.
- **Carpeta compartida (opcional)**: sistema de almacenamiento en la red del MSSP donde Panda Importer deposita los logs en ausencia de recursos más avanzados, como un servidor Syslog o un servidor Kafka.
- **Servidor SIEM**: equipo en la red del MSSP que recoge los datos descargados por el equipo Panda Importer para generar paneles de control que ayuden a localizar los procesos sospechosos de ser una amenaza para la seguridad de sus clientes.
- **Cortafuegos perimetrales y locales**: protegen la salida y entrada de datos entre el equipo Panda Importer y la infraestructura Azure.
- **Consola Panda Partner Center**: permite al MSSP activar el servicio Panda SIEMFeeder for Partners para sus clientes y configurarlo para recibir únicamente los eventos de interés.

Beneficios de la plataforma Azure

Panda SIEMFeeder for Partners genera logs de forma asíncrona y los almacena temporalmente hasta que son recuperados e integrados en un servidor SIEM. Para ello, utiliza servicios Cloud alojados en la plataforma Azure, con las siguientes características:

- **Almacenamiento en la nube**: servicio configurado en alta disponibilidad, accesible desde cualquier lugar y en cualquier momento las 24 horas del día. Con un espacio asignado de 80 Gigabytes y máximo de 7 días de retención.
- **Comunicaciones cifradas**: el intercambio de información entre el equipo Panda Importer del MSSP y la plataforma Azure se cifra con el protocolo de encriptación SSL.
- **Comunicaciones autenticadas**: para gestionar la autenticación y la autorización, Panda Importer utiliza dos tokens independientes que le permiten negociar la clave compartida necesaria para acceder a la plataforma Panda SIEMFeeder for Partners. Cada token tiene

un tiempo de caducidad diferente que garantiza la confidencialidad del acceso a la información.

Para obtener más información, consulta ***Apéndice II: Arquitectura de seguridad*** *en la página* ***63***

- **Comunicaciones comprimidas**: la plataforma Azure almacena los datos comprimidos para minimizar el ancho de banda requerido de la descarga.
- **Mecanismo PUSH de entrega**: para facilitar la configuración de los cortafuegos, la dirección de las conexiones con la infraestructura Azure es saliente desde tu red. Una vez establecido el canal de comunicación, Azure envía los logs nuevos disponibles en la plataforma mediante mensajes de tipo PUSH.

Recorrido del flujo de información

1. Panda Adaptive Defense recoge la actividad de los procesos ejecutados gracias a la monitorización permanente, y envía la información a la nube de Panda.
2. En la nube de Panda la información se completa con inteligencia de seguridad y se deposita en la infraestructura Azure, donde residirá temporalmente.
3. El programa Panda Importer se ejecuta en un servidor de tu infraestructura, descarga los logs almacenados en la plataforma Azure y, dependiendo de su configuración, los gestiona de distintas maneras:
    1. Almacena los logs en una carpeta directamente accesible por el servidor SIEM de tu organización, y gestiona el volumen de ficheros guardados para no sobrepasar los límites que has fijados.
    2. Envía los logs a un servidor de colas Kafka en tu organización para que el servidor SIEM los recoja al ritmo que le permitan sus recursos.
    3. Envía los logs a un servidor de Syslog en tu organización para que el servidor SIEM los recoja al ritmo que le permitan sus recursos disponibles.
4. El servidor SIEM importará los logs y los analizará periódicamente para incorporar la información a su repositorio y generar los paneles de control apropiados.

Operativa general del proveedor de servicios

1. Verifica que la suscripción al servicio Panda SIEMFeeder for Partners continúa vigente en Panda Partner Center. Consulta **Gestión de productos y licencias**. Si tu suscripción ha caducado o no eres cliente de Panda SIEMFeeder for Partners, consulta con el comercial de Panda asignado.

2. Comprueba la conectividad de todos los elementos mostrados en el diagrama del apartado **Arquitectura**, especialmente los relativos a la comunicación entre Panda Importer y Azure. Consulta **Configuración de los cortafuegos** en la página **27**.
3. Revisa los requisitos de despliegue e instalación. Consulta **Requisitos de despliegue e integración** en la página **26**.
4. Instala Panda Importer en tu infraestructura de IT. Consulta **Instalación y configuración de Panda Importer en sistemas Windows** en la página **33** o **Instalación y configuración de Panda Importer en sistemas Linux** en la página **45**.
5. Crea una configuración de Panda SIEMFeeder for Partners en Panda Partner Center indicando los grupos de eventos que se enviarán a la plataforma Azure. Consulta **Configuración Panda SIEMFeeder for Partners**.
6. Asocia la configuración recién creada a los clientes. Consulta **Asignar y enviar configuraciones**. Dependiendo de la opción **Activar la comunicación en tiempo real** elegida en la consola del producto de seguridad de cada cliente, la asignación de la configuración se ejecutará de forma inmediata o con un retardo de 10 minutos como máximo. Consulta **Configuración de la comunicación en tiempo real** para acceder a la guía de administración del producto contratado por el cliente.

Una vez completados todos los pasos, los equipos de tus clientes comenzarán a enviar información que se almacenará temporalmente en la plataforma Azure , hasta que el equipo Panda Importer la descargue.

Capítulo 5

Requisitos de despliegue e integración

Los requisitos para implementar correctamente el servicio Panda SIEMFeeder y Panda SIEMFeeder for Partners se resumen en tres apartados:

- Licencias e información del usuario
- Despliegue y funcionamiento
- Integración en la infraestructura IT existente

Contenido del capítulo

Licencias e información necesaria

Tanto para Panda SIEMFeeder como para Panda SIEMFeeder for Partners, necesitarás el identificador del cliente enviado en el mail de bienvenida, y un usuario de la consola de administrador del producto de seguridad contratado que sea compatible con el servicio:

- Panda Adaptive Defense (compatible con Panda SIEMFeeder con Panda SIEMFeeder for Partners)
- Panda Adaptive Defense 360 (compatible con Panda SIEMFeeder y con Panda SIEMFeeder for Partners)

Panda SIEMFeeder

- Dirección de correo electrónico y contraseña de un usuario de tu consola Panda Adaptive Defense o Panda Adaptive Defense 360 con el rol Control total asignado.
- Cuenta de correo gestionada por un administrador, que se utilizará para enviar notificaciones sobre el estado del servicio.
- Código de cliente que aparece en el mail de bienvenida que recibiste en el momento de aprovisionar el servicio Panda Adaptive Defense.

Panda SIEMFeeder for Partners

- Dirección de correo electrónico y contraseña de un usuario de Panda Adaptive Defense o Panda Adaptive Defense 360 del MSSP que tenga asignado el rol Control total.
- El código de cliente que aparece en el mail de bienvenida enviado al técnico del MSSP en el momento de aprovisionar el servicio Panda Adaptive Defense.
- Una cuenta de correo gestionada por el administrador, que se utilizará para enviar notificaciones sobre el estado del servicio.

Requisitos de despliegue e integración

- Equipos de usuario protegidos con Panda Adaptive Defense.
- Licencia Panda SIEMFeeder o Panda SIEMFeeder for Partners activada.
- Equipo con Panda Importer instalado. Consulta **Equipo de Panda Importer**.
- Configuración de los cortafuegos. Consulta **Configuración de los cortafuegos**.
- Configuración del servidor proxy. **Configuración del servidor proxy**.
- Ancho de banda de red suficiente para la recepción de datos. Consulta **Dimensionamiento del ancho de banda**.

Equipo de Panda Importer

Equipo con las características mínimas siguientes:

- Un procesador de 1 Ghz o superior.
- 512 Megabytes de Ram
- Espacio suficiente para almacenar la información recibida. El consumo medio de espacio en el dispositivo de almacenamiento es de 1 Megabyte por equipo y hora. La información se almacena en logs descomprimidos y en formato LEEF.

Para cambiar el formato de los logs a CEF en Panda SIEMFeeder, envía un correo a la dirección panda.ad_siemfeeder@watchguard.com.
Para cambiar el formato de los logs a CEF en Panda SIEMFeeder for Partners, accede a Panda Partner Center y modifica la configuración asignada. Consulta ***Configuración Panda SIEMFeeder for Partners****.*

- El programa Panda Importer correctamente configurado. Para más información, consulta **Instalación y configuración de Panda Importer en sistemas Windows** en la página **33** o **Instalación y configuración de Panda Importer en sistemas Linux** en la página **45**.
- La información de acceso indicada en el apartado **Licencias e información necesaria**.
- Uso de un servidor NTP para la sincronización horaria del equipo.

Configuración de los cortafuegos

Para que el equipo Panda Importer pueda descargar los logs desde la plataforma Azure, todos los cortafuegos intermedios de tu infraestructura deberán permitir el tráfico de red con las siguientes características:

- Acceso a la url **https://auth.pandasecurity.com**.
- Acceso a la url **https://storage.accesscontrolmngr.pandasecurity.com**.
- Acceso a la url **sb://pac100siemfeeder.servicebus.windows.net**
- **Origen de la comunicación**: equipo Panda Importer.
- **Destino de la comunicación**: plataforma Azure.
- **Tipo de conexión**: saliente desde la red del cliente.
- **Protocolo nivel 3 (transporte)**: TLS 1.2.
- **Protocolo nivel 4 (aplicación)**: HTTPS (puerto 443), Amqp (puertos 5671 y 5672), AmqpWebSockets (puerto 443).

Configuración del servidor proxy

Si Panda Importer accede a la nube de Panda a través de un proxy, es necesario que éste tenga activado el acceso por websockets. Panda Importer utilizará en este caso el protocolo AmqpWebSockets, en vez de Amqp.

Ancho de banda

Cada equipo de usuario genera de media 500 Kbytes por hora de información comprimida en formato gzip.

El ancho de banda requerido depende directamente del número de equipos de usuario monitorizados en la red, y del retraso máximo admitido según las necesidades. De esta manera, se establecen umbrales con las siguientes características:

- **Umbral mínimo**: ancho de banda mínimo necesario para poder recibir todos los logs sin incurrir en descartes por expirar el plazo de retención. Para más información, consulta el apartado **Disponibilidad del servicio**. La velocidad de generación de logs depende de muchos factores (actividad de los equipos, rol del equipo dentro de la organización etc.) y un dimensionamiento a la baja puede aprovechar las "horas valle" (horario fuera de oficina con la mayor parte de los equipos apagados) para recibir los logs generados en las "horas pico" (horas de actividad con la mayor parte de los equipos en funcionamiento).

Dimensionar el ancho de banda según el umbral mínimo impondrá retrasos en la recepción de logs e impedirá su llegada y procesamiento en tiempo real en el SIEM.

- **Umbral máximo**: es el ancho de banda necesario para descargar todos los logs según se generan.

Requisitos para la explotación de la información

Para la explotación de la información entregada, instala y configura correctamente un servidor SIEM compatible con alguno de los formatos compatibles.

Servidores SIEM compatibles

Los productos SIEM compatibles con el servicio Panda SIEMFeeder o Panda SIEMFeeder for Partners admiten logs en formato Common Event Format (CEF) de ArcSight o Log Event Extended Format (LEEF) de Qlabs.

La información se recibe en uno de los dos formatos (CEF o LEEF). A continuación, se presenta un listado parcial de servidores SIEM compatibles:

- AlienVault Unified Security Management (USM)
- Fortinet (AccelOps) FortiSIEM
- Hewlett Packard Enterprise (HPE) ArcSight
- IBM's QRadar Security Intelligence Platform
- Intel Security provides McAfee Enterprise Security Manager (ESM)
- LogRhythm

- SolarWinds Log & Event Manager (LEM)
- Splunk Security Intelligence Platform

Configuración del servidor SIEM

Para que el servidor SIEM reciba los ficheros log, configura una fuente válida para el almacenamiento de datos y mapea correctamente los eventos y campos entregados. Las fuentes válidas son:

- La carpeta donde el equipo Panda Importer deposita los logs recibidos.
- El servidor de colas Kafka que recoge los logs enviados por Panda Importer.
- El servidor Syslog que recoge los logs enviados por Panda Importer.

Para una descripción completa de la información entregada, consulta ***Panda SIEMFeeder Manual de descripción de eventos****.*

Características de los ficheros log

- Cada fichero log tiene un tamaño máximo de 256 Kbytes comprimido.
- Panda Importer almacena los logs descomprimidos en la carpeta especificada en su configuración.
- El nombre de cada fichero log respeta el formato **yyyymmdd-hhmm-(xxxxxx)** donde:
  - **yyyy**: año de creación.
  - **mm**: mes de creación.
  - **dd**: día de creación.
  - **hh**: hora de creación.
  - **mm**: minuto de creación.
  - **-(xxxxxx)**: número del log creado si se crean más de uno en el mismo minuto.

Dimensionamiento del equipo Panda Importer

Dimensionamiento del ancho de banda

- Calcula el ancho de banda necesario en función del número de equipos de usuario monitorizados (500 Kbytes por equipo y hora).

- Utiliza el valor calculado en el punto anterior para establecer reglas de QoS en el router de tu organización que conecta el equipo Panda Importer con Internet, y monitoriza de forma constante el flujo de datos consumido.
- Compara la fecha de recepción de los logs en el equipo Panda Importer con la fecha de generación de los eventos, para determinar si hay retrasos en la llegada de los datos. La fecha de generación del fichero log la ofrece el propio sistema operativo. La fecha de generación de cada evento es parte del esquema de información interno del fichero log. Para obtener una descripción detallada de todos los campos incluidos en los ficheros log consulta **Panda SIEMFeeder Manual de descripción de eventos**.
- Si la diferencia entre la fecha de recepción y de generación de los eventos se amplía progresivamente a lo largo del tiempo, comprueba el flujo de datos recibidos.
- Si el flujo de datos cubre todo el ancho de banda reservado por la regla QoS, Panda SIEMFeeder estará generando un volumen de logs mayor que el que el ancho de banda asignado al equipo Panda Importer permite consumir. Si pasados 7 días (una semana completa para incluir periodos de actividad menor) esta diferencia no se reduce, o la organización tiene como requisito un menor tiempo de recepción, amplía el ancho de banda asignado al servicio por la regla QoS.
- Si el ancho de banda asignado no llega a consumirse pero la diferencia de fechas se incrementa, indica que el cuello de botella se encuentra en el hardware del equipo Panda Importer. Consulta **Dimensionamiento del hardware del equipo Panda Importer**.

Dimensionamiento del hardware del equipo Panda Importer

Si la diferencia entre la fecha de recepción de los logs y la fecha de generación de los eventos recibidos se amplía progresivamente con el tiempo, pero el flujo de datos recibido no llega a cubrir el ancho de banda asignado, es muy probable que exista un cuello de botella en el hardware del equipo Panda Importer.

Debido a que Panda Importer es un programa dedicado a recuperar mensajes de una estructura de tipo cola, sus requisitos de CPU y memoria RAM son relativamente bajos. En un esquema de red complejo con un gran número de equipos monitorizados, la principal causa de ralentizaciones en la descarga suele deberse a un cuello de botella en el sistema de almacenamiento del equipo que ejecuta Panda Importer. Sigue la lista de consejos mostrada a continuación para determinar el origen de los cuellos de botella y resolverlos. Para observar las estadísticas de rendimiento de CPU y disco duro, necesitarás iniciar el administrador de tareas de Windows con el programa Panda Importer en ejecución, en modo línea de comandos o servicio.

- **Alto consumo de CPU con núcleos libres**: el programa Panda Importer es monohilo, de forma que solo aprovecha uno de los núcleos del procesador instalado en el servidor. Si el administrador de tareas de Windows muestra un uso sostenido de más del 80% en uno de los núcleos, ejecuta varias instancias del programa con distintas carpetas de destino. Una

recomendación conservadora es ejecutar tantas instancias de Panda Importer como núcleos tenga el equipo. Para más información, consulta **Configurar múltiples instancias** en la página **39**

- **Alto consumo de CPU sin núcleos libres**: si el administrador de tareas muestra un uso por encima del 80% sostenido en todos los núcleos, se recomienda instalar Panda Importer en un servidor adicional o cambiar la CPU del equipo por una más potente.
- **Alto consumo del ancho de banda en el sistema de almacenamiento**: si el administrador de tareas muestra un uso elevado de los discos duros, se recomienda la sustitución de alguno o todos los componentes del subsistema de almacenamiento:
    - Sustitución de los discos duros mecánicos por otros de tecnología SSD (Solid-State Drive, unidad de estado sólido).
    - Instalación de un sistema RAID - 0 o equivalente que permita escribir los datos en varios discos a la vez.
    - Sustitución de la interface de bus de datos por una versión superior de SATA, eSATA, SAS etc.

Disponibilidad del servicio

Panda SIEMFeeder está disponible en modo 24x7. Cualquier interrupción del servicio es notificada mediante correo electrónico a la cuenta del administrador suministrada en el proceso de alta.

Para evitar la pérdida de información en caso de un fallo de conectividad, falta de disponibilidad del equipo Panda Importer del cliente o de cualquier otro tipo, Panda retiene los logs generados y no entregados al cliente durante el tiempo indicado a continuación:

- **Máximo número de días de retención de logs en la plataforma Azure**: 7 días
- **Máximo volumen de datos retenidos en la plataforma Azure**: 80 Gigabytes por cliente.

Capítulo 6

Instalación y configuración de Panda Importer en sistemas Windows

Panda Importer es la aplicación encargada de descargar desde la infraestructura Azure los eventos registrados por Panda Adaptive Defense y Panda Adaptive Defense 360 . Estos eventos se almacenan empaquetados en ficheros log y, dependiendo de la configuración que elijas, Panda Importer los descomprime y deposita en una carpeta (local o remota), o los envía a un servidor compatible (Kafka o Syslog).

Contenido del capítulo

Requisitos de instalación

Información necesaria

Para conocer la información requerida por Panda Importer consulta **Licencias e información necesaria** en la página **25**.

Sistema operativo y librerías necesarias

Comprueba que el equipo que ejecutará el programa Panda Importer cumple con los requisitos:

- **.NET Framework 4.6.2 o superior instalado**: en caso de tener una versión anterior, consulta la url **https://dotnet.microsoft.com/en- us/download/dotnet- framework/net462** para su descarga. Panda Importer es compatible con .NET Framework hasta la versión 4.8.
- **Sistemas operativos compatibles**: Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7 Service Pack 1, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1.

Permisos necesarios

Puedes ejecutar Panda Importer como un programa de línea de comandos o como servicio de Windows.

- En modo servicio, Panda Importer se ejecuta bajo la cuenta `local system` y necesita permisos de administración para instalarse correctamente.
- En modo línea de comandos Panda Importer solo requiere permisos para acceder a los recursos de almacenamiento que necesite, como por ejemplo acceso de escritura sobre la carpeta que has configurado para almacenar los logs descargados.

Configuración de los cortafuegos

Para que el equipo Panda Importer descargue los logs desde la plataforma Azure, todos los cortafuegos intermedios deberán permitir el tráfico de red con las siguientes características:

- Acceso a la URL **https://auth.pandasecurity.com**.
- Acceso a la URL **https://storage.accesscontrolmngr.pandasecurity.com**.
- Acceso a la URL **sb://pac100siemfeeder.servicebus.windows.net**.
- **Origen de la comunicación**: equipo Panda Importer.
- **Destino de la comunicación**: infraestructura Azure.
- **Tipo de conexión**: saliente desde la red del cliente.
- **Protocolo nivel 3 (transporte)**: TLS 1.2.

- **Protocolo nivel 4 (aplicación)**: HTTPS (puerto 443), Amqp (puertos 5671 y 5672), Amqp WebSockets (puerto 443).

Servidor NTP

Para descargar los logs almacenados en la plataforma Azure, es necesario completar un proceso de autenticación y autorización que implica la generación de un token. Este token se emite con una fecha de caducidad, por lo que ambos extremos de la comunicación tienen que tener el reloj sincronizado. Panda Importer utiliza el servicio Hora de Windows u otro servicio equivalente para recuperar la hora de un servidor NTP. Para obtener más información, consulta **https://docs.microsoft.com/es- es/windows- server/networking/windows- time- service/accurate-time**.

Instalación y configuración

> *Para obtener más información sobre el origen de los errores encontrados en el proceso de instalación, consulta **Apéndice I: Solución de problemas** en la página **61**.*

Para instalar y configurar Panda Importer:

1. Descarga y descomprime el fichero `.zip` que contiene el instalador. Consulta **Descarga del paquete de instalación**.
2. Indica el método de conexión soportado por la infraestructura IT que alojará el equipo Panda Importer: directa o mediante proxy corporativo. Consulta **Configurar el método de conexión**.
3. Escribe las credenciales de la cuenta utilizada para acceder al servicio. Consulta **Escribir las credenciales de acceso**.
4. Indica la plataforma donde residen los productos de seguridad contratados con Panda. Consulta **Configurar la plataforma a utilizar**.
5. Configura el método de envío y almacenamiento de los logs recibidos. Consulta **Configurar el modo de almacenamiento y envío de logs**.
6. Actualiza el fichero `configuration.json` con la nueva configuración de la instalación. Consulta **Actualiza el fichero configuration.json**.
7. Configura el modo en el que se ejecutará Panda Importer: como servicio o desde linea de comandos. Consulta **Configurar el modo de ejecución**.

Descarga del paquete de instalación

Descarga el paquete `.zip` de la versión Windows de Panda Importer desde el enlace **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA** y descomprímelo en una carpeta del equipo. El paquete contiene varios ficheros principales:

- `EventsFeederImporter.Host.exe`: descarga los ficheros log que contienen los eventos registrados en los equipos del cliente, y los almacena en el disco duro del equipo o los reenvía a otro, dependiendo de la configuración que has definido.
- `EventsFeederImporter.ConfigAssistant.exe`: muestra el asistente de configuración que recoge los parámetros necesarios para configurar Panda Importer.
- `Configuration.json`: contiene la configuración del programa. Todos los datos de carácter personal se almacenan ofuscados para evitar filtraciones de seguridad

Configuración

En este apartado se describe la generación del fichero de configuración necesario para ejecutar una única instancia de Panda Importer en modo servicio o linea de comandos y conectar con la plataforma Azure para descargar los logs.

Para configurar Panda Importer es necesario ejecutar el programa `EventsFeederImporter.ConfigAssistant.exe` en modo linea de comandos y responder "**Yes**" a la pregunta **Do you want to change the configuration settings? [Yes/No]**. De esta forma, se genera un nuevo fichero de configuración que invalida el existente y se lanza el asistente de configuración.

Para instalar Panda Importer como servicio es necesario ejecutar `EventsFeederImporter.ConfigAssistant.exe` con permisos de administrador. Haz clic en el fichero con el botón derecho del ratón y selecciona Ejecutar como administrador.

Configurar el método de conexión

Panda Importer utiliza el acceso mediante proxy para conectar con la plataforma Azure. Las conexiones a otros recursos internos como al servidor de ficheros, servidor Kafka o servidor Syslog no utilizan el proxy configurado.

Si Panda Importer está detrás de un servidor proxy:

- Contesta **Y** a la pregunta **Is Event Importer behind a proxy server? [Yes/No]**.
- Escribe la dirección IP del servidor proxy, y el usuario y la contraseña si se requiere autenticación.

> *La contraseña debe ser una cadena de caracteres alfanuméricos, espacios y símbolos excepto los indicados a continuación: ":", "/", "?", "#", "[", "]", "@", "!", "$", "&", "'", "(", ")","*", "+",",",";","=",","*

Configurar la plataforma a utilizar

Selecciona la plataforma de seguridad a la que pertenece el producto Panda Adaptive Defense que protege a los equipos de usuario, y contesta a la pregunta **Select your platform: [C]urrent or [W]G Endpoint Security**:

- **C (Current)**: si la cuenta utilizada pertenece a la plataforma de seguridad Panda.
- **W (Watchguard)**: si la cuenta utilizada pertenece a la plataforma de seguridad WatchGuard.

Escribir las credenciales de acceso

- Escribe la dirección de correo de la cuenta utilizada para acceder a la consola Panda Adaptive Defense.
- Escribe la contraseña. Si la cuenta tiene activado el servicio 2FA, escribe el código OTP de 6 dígitos inmediatamente después de la contraseña, sin dejar espacios en blanco.
- Escribe el identificador del cliente incluido en el correo de bienvenida. Una vez hecho, Panda Importer generará un nuevo token de acceso que utilizará para acceder a la plataforma Azure y descargar los logs generados.

Para determinar si la cuenta de acceso tiene el servicio 2FA activado, accede a la consola de administración de Panda Adaptive Defense:

- Si tu proveedor de seguridad es Panda Security haz clic en **https://www.pandacloudsecurity.com/PandaLogin/** y escribe tus credenciales. Se mostrará la consola de administración.
- Si tu proveedor de seguridad es WatchGuard:
    - Accede a la URL **https://www.watchguard.com/** y haz clic en el botón **Log in** situado en la esquina superior derecha de la pantalla.
    - Escribe tus credenciales de WatchGuard. Se mostrará la ventana **Support Center**.
    - Haz clic en el menú superior **My watchguard**. Se mostrará un menú desplegable.

- Haz clic en la opción **Manage Panda Products**. Se abrirá una ventana con todos los servicios contratados.
- Haz clic en el panel asociado al nombre de producto. Se mostrará la consola de administración.

- Haz clic en el nombre de la cuenta, situado en la esquina superior derecha. Se mostrará un menú desplegable.
- Haz clic en **Configurar mi perfil**. Se abrirá la ventana **Panda Cuenta** donde se indica si el servicio 2FA está activado o no.

Para obtener más información sobre cómo activar 2FA, consulta ***http://documents.managedprotection.pandasecurity.com/Help/PandaCloud/es-es/#t=001.htm***

Configurar el modo de almacenamiento y envío de logs

Para elegir el método de envío y almacenamiento de los logs descargados, consulta el apartado **Configurar el modo de almacenamiento y envío de logs**.

Configurar el modo de ejecución

Panda Importer se puede ejecutar como servicio o en modo linea de comandos. Responde **Y** o **N** a la pregunta **Do you want to register Event importer as a Windows service? [Yes/No]**:

- **Y**: para instalar el programa como servicio. Panda Importer se instalará automáticamente como servicio solo si iniciaste el proceso de instalación con permisos de administrador.

*Utiliza la opción (**Y**) solo en el caso de que vayas a instalar y ejecutar una única instancia Panda Importer como servicio en el equipo. En el resto de casos, elige siempre (**N**). Consulta el apartado **Configurar múltiples instancias**.*

- **N**: para ejecutar una o varias instancias desde la linea de comandos o para ejecutar varias instancias del programa como servicio. Consulta **Configurar múltiples instancias**.

Actualiza el fichero `configuration.json`

Al terminar la ejecución del asistente de configuración, Panda Importer actualizará el fichero `configuration.json` situado en la misma carpeta, y comenzará a descargar los logs almacenados en la plataforma Azure.

El fichero `configuration.json` contiene los siguientes datos:

- Información relativa al cliente del cual se descargarán los logs.
- Información del método de envío y almacenamiento de logs descargados.
- Información sobre el modo de ejecución (línea de comandos o servicio).

Configurar múltiples instancias

Es necesario configurar varias instancias de Panda Importer en los casos siguientes:

- Si el equipo que ejecuta el programa Panda Importer presenta los síntomas de falta de recursos descritos en **Dimensionamiento del equipo Panda Importer** en la página **29**, es recomendable que instales una o varias instancias adicionales del programa y ejecútalas de forma concurrente.
- Si necesitas que un mismo equipo con Panda Importer instalado descargue logs de más de un cliente simultáneamente, pero no estás utilizando Panda SIEMFeeder for Partners.

> ⚠ *Para descargar logs de varios clientes y centralizar todas las descargas en una única instancia de Panda Importer, utiliza Panda SIEMFeeder for Partners. Consulta* ***Arquitectura*** *en la página* ***20****.*

Múltiples instancias en modo linea de comandos

- Descarga la última versión de Panda Importer desde el enlace **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA** y descomprímelo en una carpeta independiente por cada cliente a recuperar los logs.
- Para instalarlo en modo línea de comandos, configura cada aplicación de forma independiente, siguiendo los pasos mostrados en el apartado **Configuración**.
- Ejecuta cada aplicación de forma independiente.

Múltiples instancias en modo servicio

> ⚠ *Ejecuta este procedimiento con permisos de administrador.*

Si quieres ejecutar varias instancias de Panda Importer en modo servicio, primero es necesario instalar el programa en modo linea de comandos y después registrarlo como servicio:

- En este ejemplo se utilizarán las carpetas `c:\users\customer1 y c:\users\customer2.`
- Sigue los pasos del apartado **Múltiples instancias en modo linea de comandos**.

- Presiona `control + c` para interrumpir la ejecución de cada instancia.
- Para registrar Panda Importer como un servicio da un nombre distinto a cada instancia con los parámetros `servicename`, `description` y `displayname`:

```
PS C:\> cd c:\users\customer1
PS C:\users\customer1> EventsFeederImporter.Host.exe install
-servicename:ServiceCustomer1
-description: ServiceCustomer1
-displayname: ServiceCustomer1
PS C:\> cd c:\users\customer2
PS C:\users\customer2> EventsFeederImporter.Host.exe install
-servicename:ServiceCustomer2
-description: ServiceCustomer2
-displayname: ServiceCustomer2
```

- Para iniciar cada instancia:

```
PS C:\> cd c:\users\customer1
PS C:\users\customer1> EventsFeederImporter.Host.exe start
-servicename:ServiceCustomer1
PS C:\> cd c:\users\customer2
PS C:\users\customer2> EventsFeederImporter.Host.exe start
-servicename:ServiceCustomer2
```

Configuración del almacenamiento y reenvío de logs

Panda Importer incorpora varios métodos de almacenamiento y reenvío de logs en función de la arquitectura de red, recursos disponibles y volumen de información recibida de la plataforma Azure:

- Almacenamiento en una carpeta local o remota
- Envío a un servidor Kafka
- Envío a un servidor Syslog

Para elegir el método de almacenamiento presiona **Y** cuando Panda Importer te muestra la pregunta **Event Importer enables you to send received events simultaneously to various channels. Do you want to change the current channel settings? [Yes/No]** en el asistente de configuración. Se borrarán las configuraciones de almacenamiento y reenvío preexistentes si las hubiera y se generará una nueva.

Almacenamiento de logs en una carpeta local o remota

- Crea previamente la carpeta donde se almacenarán los logs. Esta carpeta puede ser local en el equipo que ejecuta Panda Importer o una unidad o recurso remoto compartido.
- Si ejecutas varias instancias de Panda Importer, crea una carpeta independiente para cada una de ellas. De no hacerse así, es posible que se pierdan logs en el proceso de recogida y almacenamiento.
- Presiona **F** en respuesta a la pregunta **Select where you want to deliver received events: [F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Escribe la ruta completa de la carpeta para cada instancia de Panda Importer.
- Escribe la extensión de los ficheros donde se volcarán los eventos recibidos de Panda Importer.
- Para finalizar la configuración del método de almacenamiento contesta **N** a la pregunta **Do you want to configure another delivery channel? [Yes/No]**.

Envío de logs a un servidor Kafka

- Presiona **K** en respuesta a la pregunta **Select where you want to deliver received events: [F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Escribe la dirección IP o el nombre del dominio del servidor Kafka y el puerto de escucha separado por ":".
- Escribe el nombre de la cola / topic donde Panda Importer enviará los logs en el servidor Kafka.
- Escribe el protocolo de comunicación que Panda Importer utilizará para enviar los logs al servidor Kafka:
    - **[N]one**: presiona **N** para configurar el envío de logs sin cifrar.
    - **[S]SL**: presiona **S** para configurar el envío de logs mediante cifrado SSL.
    - **S[A]SL_SSL**: presiona **A** para configurar el envío de logs mediante cifrado SASL/SSL.
    - **SASL_PLAIN [T]TEXT**: presiona **T** para configurar el envío de logs mediante cifrado SASL/PLAIN.

- Dependiendo de si el protocolo de comunicación elegido cifra o no los datos, indica la ruta del fichero con el certificado de la CA configurada en el servidor Kafka.
- Para finalizar la configuración del método de envío, contesta **N** a la pregunta **Do you want to configure another delivery channel? [Yes/No]**.

Envío a un servidor Syslog

- Presiona **S** en respuesta a la pregunta **Select where you want to deliver received events: [F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Selecciona el formato configurado en el servidor de Syslog para recibir los logs: **RFC[5]424** o **RFC[3]164**.
- Escribe la dirección IP o el nombre del dominio del servidor Syslog y el puerto de escucha separado por ":".
- Selecciona el protocolo de transporte configurado en el servidor de Syslog para recibir los logs: **[T]CP** o **[U]DP**.

Para asegurar la recepción en el servidor Syslog de todos los logs enviados por Panda Importer , es recomendable configurar el uso del protocolo de transporte TCP en ambos extremos. De lo contrario, en situaciones se sobrecarga es posible que el protocolo UDP descarte logs sin previo aviso.

- Elige el protocolo seguro para cifrar la comunicación entre el servidor de Syslog y Panda Importer: **[N]one** o **TLS 1.[2]**.
- Selecciona el delimitador de final de mensaje configurado en el servidor de Syslog para recibir los logs: **[C]R**, **[L]F**, **C[R]LF**.

Si el protocolo de transporte elegido es UDP no se utiliza delimitador.
Si el protocolo de transporte elegido es TCP y TLS se utiliza siempre el delimitador Null.

- Si el protocolo de comunicación elegido cifra los datos, indica el lugar donde se encuentra el certificado de la CA configurada en el servidor Syslog:
    - **[F]ile**: el certificado de la CA se encuentra en un fichero independiente
    - **[C]ert Store**: el certificado de la CA se encuentra en el almacén de certificados local del equipo donde se ejecuta Panda Importer, en la rama Certificados de usuarios de confianza.

- Para finalizar la configuración del método de envío, contesta **N** a la pregunta **Do you want to configure another delivery channel? [Yes/No]**.

Copia de logs descargados en diferentes localizaciones

Panda Importer permite descargar logs en varias localizaciones de forma simultánea. Cada log descargado se elimina de la cola de descarga en la infraestructura Azure si al menos se actualiza una de las localizaciones configurada.

> *Si se producen fallos en la recuperación de logs, las distintas localizaciones configuradas podrán contener un número de logs diferente.*

Para implementar esta característica Panda Importer utiliza la funcionalidad de "canales". Un canal especifica el tipo de almacenamiento que utilizará Panda Importer y su configuración.

Para configurar Panda Importer:

1. Instala Panda Importer tal y como se describe en el apartado **Configuración**.
2. Detén Panda Importer tal y como se describe en el apartado **Ejecutar y parar**.
3. Añade un nuevo canal a la colección ya existente en el fichero `configuration.json`:

```
"Channels": [{ parámetros del canal 1} , {parámetros del canal 2},
…]
```

4. Indica en cada canal el tipo de almacenamiento que utilizarás para almacenar los logs y su configuración asociada.

A modo de ejemplo se muestra una configuración de Panda Importer con dos canales; el primero de ellos dejará los logs en la carpeta `Log1`, y el segundo en la carpeta `Log2`:

```
"Channels": [{
"Type": "LocalDisk",
"Name": "LD1",
"Configuration": {
"fullPath":
"D:\\\\SIEMFeeder\\\\EventFeederImporter 1.0.3 Pro\\\\Log1",
"filesSplitFormat": "1m",
```

```
"filesSizeLimitInBytes": 102400,
"directoryMaxSizeInMb": 1024
}
}, {
"Type": "LocalDisk",
"Name": "LD2",
"Configuration";{
"fullPath:
"D:\\\\SIEMFeeder\\\\EventFeederImporter 1.0.3 Pro\\\\Log2",
"fileSplitFormat":"1m",
"filesSizeLimitInBytes": 102400,
"directoryMaxSizeInMb": 1024
}
},]
```

Ejecutar y parar

En modo línea de comandos

- Para iniciar Panda Importer, haz doble clic en el fichero `EventsFeederImporter.Host.exe` o ejecútalo desde la línea de comandos.
- Para parar Panda Importer, presiona `Control + c` en la ventana de comandos.

En modo servicio

- El servicio se configura de forma automática para iniciarse con el sistema operativo. Para ejecutar Panda Importer tras una parada manual, accede al snap-in Servicios de la consola MMC del sistema operativo y localiza el servicio `EventsFeederImporter` (nombre por defecto utilizado por el asistente de instalación y si no has registrado el servicio de forma manual). Selecciona Iniciar con el botón de la derecha.
- Para parar Panda Importer accede al snap-in Servicios de la consola MMC del sistema operativo y localiza el servicio `EventsFeederImporter`. Selecciona Detener con el botón de la derecha.

Capítulo 7

Instalación y configuración de Panda Importer en sistemas Linux

Panda Importer es la aplicación encargada de descargar desde la plataforma Azure los eventos que registra Panda Adaptive Defense y Panda Adaptive Defense 360. Estos eventos se almacenan empaquetados en ficheros log y, dependiendo de la configuración que elijas, Panda Importer los descomprime y los deposita en una carpeta (local o remota), o los envía a un servidor compatible (Kafka o Syslog).

Contenido del capítulo

Requisitos de instalación

Información necesaria

Para conocer la información requerida por Panda Importer consulta **Licencias e información necesaria** en la página **25**.

Sistema operativo y librerías necesarias

Aunque Panda Importer es compatible con todas las plataformas Linux que soportan el framework .NET 8.0, Panda Security certifica y da soporte a las distribuciones siguientes :

- Ubuntu 24.04 LTS
- Red Hat Enterprise Linux 9.5

El paquete de instalación contiene todos los recursos necesarios para el funcionamiento de Panda SIEMFeeder.

Para conocer las distribuciones compatibles con el framework .NET 8.0 consulta **.NET 8.0 - Supported OS versions.**

Permisos necesarios

Puedes ejecutar Panda Importer como un programa de línea de comandos, o como un demonio del sistema:

- En modo demonio Panda Importer se ejecuta bajo una cuenta de usuario, pero necesitarás permisos de `root` para completar su configuración.
- En modo línea de comandos Panda Importer solo requiere permisos a los recursos de almacenamiento que necesite, como por ejemplo acceso de escritura sobre la carpeta que has configurado para almacenar los logs descargados.

Configuración de los cortafuegos

Para que Panda Importer descargue los logs desde la plataforma Azure, todos los cortafuegos intermedios deberán permitir el tráfico de red con las siguientes características:

- Acceso a la url **https://auth.pandasecurity.com**.
- Acceso a la url **https://storage.accesscontrolmngr.pandasecurity.com**.
- Acceso a la url **sb://pac100siemfeeder.servicebus.windows.net**.
- **Origen de la comunicación**: equipo Panda Importer.
- **Destino de la comunicación**: infraestructura Azure.
- **Tipo de conexión**: saliente desde la red del cliente.

- **Protocolo nivel 3 (transporte)**: TLS 1.2.
- **Protocolo nivel 4 (aplicación)**: HTTPS (puerto 443), Amqp (puertos 5671 y 5672), Amqp WebSockets (puerto 443).

Servidor NTP

Para descargar los logs almacenados en la plataforma Azure, es necesario completar un proceso de autenticación y autorización que implica la generación de un token. Este token se emite con una fecha de caducidad, por lo que ambos extremos de la comunicación tienen que tener el reloj sincronizado. Panda Importer utiliza el demonio `ntpd` u otro equivalente para recuperar la hora de un servidor NTP. Para obtener más información, consulta **https://www.ntppool.org/es/use.html**.

Instalación y configuración

> *Para obtener más información sobre el origen de los errores encontrados en el proceso de instalación, consulta **Apéndice I: Solución de problemas** en la página **61**.*

Para instalar y configurar Panda Importer :

1. Descarga y descomprime el fichero `.gz` que contiene el instalador. Consulta **Descarga del paquete de instalación**.
2. Modifica si es necesario el atributo de ejecución de los ficheros.
3. Indica el método de conexión soportado por la infraestructura IT que alojará el equipo Panda Importer: directa o mediante proxy corporativo. Consulta **Configurar el método de conexión**.
4. Escribe las credenciales de la cuenta utilizada para acceder al servicio. Consulta **Escribir las credenciales de acceso**.
5. Indica la plataforma donde residen los productos de seguridad contratados con Panda. Consulta **Configurar la plataforma a utilizar**.
6. Configura el método de envío y almacenamiento de los logs recibidos. Consulta **Configuración del almacenamiento y reenvío de logs**.
7. Actualiza el fichero `configuration.json` con la nueva configuración de la instalación. Consulta **Actualizar el fichero configuration.json**.
8. (opcional) Configura Panda Importer para ejecutarse como demonio. Consulta **Configurar Panda Importer como demonio**.

Descarga del paquete de instalación

Descarga el paquete `.gz` de la versión Linux de Panda Importer desde el enlace **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA** y descomprímelo en una carpeta del equipo. El paquete `EventsFeederImporter x.x Pro.zip` contiene varios ficheros principales:

- `EventsFeederImporter.Multiplatform.Host`: descarga los ficheros log que contienen los eventos registrados en los equipos de los usuarios, y los almacena en el disco duro del equipo o los reenvía a otro, dependiendo de la configuración que has definido.
- `EventsFeederImporter.Multiplatform.ConfigAssistant`: muestra el asistente de configuración que recoge los parámetros necesarios para configurar Panda Importer.
- `Configuration.json`: contiene la configuración del programa. Todos los datos de carácter personal se almacenan ofuscados para evitar filtraciones de seguridad.

Modifica el atributo de ejecución de los ficheros

Para que un sistema Linux pueda ejecutar un programa, es necesario que el bit de ejecución del fichero esté activado. Ejecuta desde una linea de comandos:

```
$ sudo chmod a+x /#_SAMPLEFOLDER_
SiemFeeder#/EventsFeederImporter.Multiplatform.Host

$ sudo chmod a+x /#_SAMPLEFOLDER_
SiemFeeder#/EventsFeederImporter.Multiplatform.ConfigAssistant
```

La variable `/#_SAMPLEFOLDER_SiemFeeder#/` contiene la ruta completa de la carpeta donde reside el paquete descomprimido.

Configuración

Este apartado describe cómo puedes generar el fichero de configuración para ejecutar una única instancia de Panda Importer en modo linea de comandos y conectar con la plataforma Azure para descargar los logs.

Para configurar Panda Importer, ejecuta el programa `EventsFeederImporter.Multiplatform.ConfigAssistant` y responde **Yes** a la pregunta **Do you want to change the configuration settings? [Yes/No]**. Se generará un nuevo fichero de configuración que invalidará el existente, y se lanzará el asistente de configuración.

Configurar el método de conexión

Panda Importer utiliza el acceso mediante proxy para conectar con la plataforma Azure. Las conexiones a otros recursos internos como al servidor de ficheros, servidor Kafka o servidor Syslog no utilizan el proxy configurado.

Si Panda Importer está detrás de un servidor proxy:

- Contesta **Y** a la pregunta **Is Event Importer behind a proxy server? [Yes/No]**.
- Escribe la dirección IP del servidor proxy, y el usuario y la contraseña si se requiere autenticación.

La contraseña debe ser una cadena de caracteres alfanuméricos, espacios y símbolos excepto los indicados a continuación: ":", "/", "?", "#", "[", "]", "@", "!", "$", "&", "'", "(", ")","", "+",",",";","=","%"*

Configurar la plataforma a utilizar

Selecciona la plataforma de seguridad a la que pertenece el producto Panda Adaptive Defenseque protege a los equipos de usuario, y contesta a la pregunta **Select your platform: [C]urrent or [W]G Endpoint Security**:

- **C (Current)**: si la cuenta utilizada pertenece a la plataforma de seguridad Panda.
- **W (Watchguard)**: si la cuenta utilizada pertenece a la plataforma WatchGuard.

Escribir las credenciales de acceso

- Escribe la dirección de correo de la cuenta utilizada para acceder a la consola Panda Adaptive Defense.
- Escribe la contraseña. Si la cuenta tiene activado el servicio 2FA, escribe el código OTP de 6 dígitos inmediatamente después de la contraseña, sin dejar espacios en blanco.
- Escribe el identificador del cliente incluido en el correo de bienvenida. Una vez hecho, Panda Importer generará un nuevo token de acceso que utilizará para acceder a la plataforma Azure y descargar los logs generados.

Para determinar si la cuenta de acceso tiene el servicio 2FA activado, accede a la consola de administración de Panda Adaptive Defense:

- Si tu proveedor de seguridad es Panda Security haz clic en **https://www.pandacloudsecurity.com/PandaLogin/** y escribe tus credenciales. Se abrirá la consola de administración.
- Si tu proveedor de seguridad es WatchGuard:
    - Accede a la URL **https://www.watchguard.com/** y haz clic en el botón **Log in** situado en la esquina superior derecha de la pantalla.
    - Escribe tus credenciales de WatchGuard. Se mostrará la ventana **Support Center**.
    - Haz clic en el menú superior **My watchguard**. Se mostrará un menú desplegable.
    - Haz clic en la opción **Manage Panda Products**. Se abrirá una ventana con todos los servicios contratados.
    - Haz clic en el panel asociado al nombre de producto. Se mostrará la consola de administración.
- Haz clic en el nombre de la cuenta, situado en la esquina superior derecha. Se mostrará un menú desplegable.
- Haz clic en **Configurar mi perfil**. Se abrirá la ventana Panda Cuenta donde se indica si el servicio 2FA está activado o no.

Para obtener más información sobre cómo activar 2FA, consulta ***http://documents.managedprotection.pandasecurity.com/Help/PandaCloud/es-es/#t=001.htm***

Configurar el modo de almacenamiento y envío de logs

Para elegir el método de envío y almacenamiento de los logs descargados, consulta el apartado **Configuración del almacenamiento y reenvío de logs**.

Actualizar el fichero configuration.json

Después de configurar el modo de almacenamiento y envío de logs, Panda Importer actualizará el fichero `configuration.json` situado en la misma carpeta, con los siguientes datos:

- Información relativa al cliente del cual se descargarán los logs.
- Información del método de envío y almacenamiento de logs descargados.
- Información sobre el modo de ejecución (línea de comandos o demonio).

Configurar Panda Importer como demonio

Panda Importer puede ejecutarse de forma automática como proceso en segundo plano al iniciar el sistema, sin mostrar mensajes por pantalla:

- Contesta **N** a la pregunta **Do you want to start the Event Importer process? (This is not necessary when Event Importer runs as a daemon.)**.
- Edita el fichero `Siemfeeder.service` incluido en el paquete `.gz` y cambia la linea que comienza por `ExecStart` por la ruta completa donde reside el programa `EventsFeederImporter.Multiplatform.Host`. Por ejemplo:

```
ExecStart="/home/panda/Desktop/SIEMFeeder 3.10
Linux/EventsFeederImporter.Multiplatform.Host"
```

- Copia el fichero `siemfeeder.service` al directorio de sistema de la distribución Linux utilizada. Las rutas más frecuente son:
  - En Ubuntu: `/lib/systemd/system`
  - En Red Hat: `/usr/lib/systemd/system`
- Si el equipo tiene Security-Enhanced Linux (SELinux) habilitado y tiene instalada una distribución Red Hat Enterprise, utiliza el script `selinux-checks.sh` para configurar el entorno de ejecución:
  - Para dar permisos de ejecución al script, ejecuta el comando `chmod +x selinux-checks.sh`.
  - Ejecuta el comando `sudo #_PATH_#/selinux-checks.sh`. Comprueba que no hay espacios en blanco en la ruta donde esta el script.
- Ejecuta el comando `sudo systemctl enable siemfeeder` para añadir el script a la secuencia de inicio del sistema.
- Para iniciar Panda SIEMFeeder consulta **Ejecutar y parar**.

Configurar múltiples instancias

Es necesario configurar varias instancias de Panda Importer en los casos siguientes:

- Si el equipo que ejecuta el programa Panda Importer presenta los síntomas de falta de recursos descritos en **Dimensionamiento del hardware del equipo Panda Importer** en la página **30**, es recomendable instalar una o varias instancias adicionales del programa y ejecutarlas de forma concurrente.
- Si necesitas que un mismo equipo con Panda Importer instalado descargue logs de más de un cliente simultáneamente, pero no estás utilizando Panda SIEMFeeder for Partners.

Para descargar logs de varios clientes y centralizar todas las descargas en una única instancia de Panda Importer, utiliza Panda SIEMFeeder for Partners. Consulta ***Arquitectura Panda SIEMFeeder for Partners*** *en la página* ***17***.

Múltiples instancias en modo linea de comandos

- Descarga la última versión de Panda Importer desde el enlace **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA** y descomprímelo en una carpeta independiente por cada cliente del que se quieras descargar logs.
- Para instalar Panda Importer en modo línea de comandos, configura cada aplicación de forma independiente siguiendo los pasos mostrados en el apartado **Configuración**.
- Ejecuta cada aplicación de forma independiente.

Configuración del almacenamiento y reenvío de logs

Panda Importer soporta varios métodos de almacenamiento y reenvío de logs en función de la arquitectura de red, recursos disponibles y volumen de información almacenada de la plataforma Azure:

- Almacenamiento en una carpeta local o remota
- Envío a un servidor Kafka
- Envío a un servidor Syslog

Para elegir el método de almacenamiento presiona **Y** cuando Panda Importer te muestra la pregunta **Event Importer enables you to send received events simultaneously to various channels. Do you want to change the current channel settings? [Yes/No]** en el asistente de configuración. Se borrarán las configuraciones de almacenamiento y reenvío preexistentes si las hubiera y se generará una nueva.

Almacenamiento de logs en una carpeta local o remota

Comprueba que Panda SIEMFeeder tiene permisos de escritura en la carpeta local o remota donde descargará los ficheros log.

- Crea previamente la carpeta donde se almacenarán los logs. Esta carpeta puede ser local en el equipo que ejecuta Panda Importer o una unidad o recurso remoto compartido.
- Si ejecutas varias instancias de Panda Importer, crea una carpeta independiente para cada una de ellas. De no hacerse así, es posible que se pierdan logs en el proceso de recogida y almacenamiento.
- Presiona **F** en respuesta a la pregunta **Select where you want to deliver received events: [F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Escribe la ruta completa de la carpeta para cada instancia de Panda Importer.
- Escribe la extensión de los ficheros donde se volcarán los eventos recibidos de Panda Importer.
- Para finalizar la configuración del método de almacenamiento contesta **N** a la pregunta **Do you want to configure another delivery channel? [Yes/No]**.

Envío de logs a un servidor Kafka

- Presiona **K** en respuesta a la pregunta **Select where you want to deliver received events: [F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Escribe la dirección IP o el nombre del dominio del servidor Kafka y el puerto de escucha separado por ":".
- Escribe el nombre de la cola / topic a donde Panda Importer enviará los logs en el servidor Kafka.
- Escribe el protocolo de comunicación que Panda Importer utilizará para enviar los logs al servidor Kafka:
    - **[N]one**: presiona **N** para configurar el envío de logs sin cifrar.
    - **[S]SL**: presiona **S** para configurar el envío de logs mediante cifrado SSL.
    - **S[A]SL_SSL**: presiona **A** para configurar el envío de logs mediante cifrado SASL/SSL.
    - **SASL_PLAIN [T]TEXT**: presiona **T** para configurar el envío de logs mediante cifrado SASL/PLAIN.
- Dependiendo de si el protocolo de comunicación elegido cifra o no los datos, escibe la ruta del fichero con el certificado de la CA configurada en el servidor Kafka.
- Para finalizar la configuración del método de envío contesta **N** a la pregunta **Do you want to configure another delivery channel? [Yes/No]**.

Envío a un servidor Syslog

- Presiona **S** en respuesta a la pregunta **Select where you want to deliver received events: [F]ile on disk, [K]afka topic/queue, or [S]yslog server**.

- Selecciona el formato configurado en el servidor de Syslog para recibir los logs: **RFC[5]424 o RFC[3]164**.
- Escribe la dirección IP o el nombre del dominio del servidor Syslog y el puerto de escucha separado por ":".
- Selecciona el protocolo de transporte configurado en el servidor de Syslog para recibir los logs: **[T]CP** o **[U]DP**.

Para asegurar la recepción en el servidor Syslog de todos los logs enviados por Panda SIEMFeeder, elige el protocolo de transporte TCP en ambos extremos. De lo contrario, en situaciones se sobrecarga es posible que el protocolo UDP descarte logs sin previo aviso.

- Elige el protocolo seguro para cifrar la comunicación entre el servidor de Syslog y Panda Importer (TLS 1.2 solo admite el protocolo de transporte TCP): **[N]one** o **TLS 1.[2]**.
- Selecciona el delimitador de final mensaje configurado en el servidor de Syslog para recibir los logs: **[C]R**, **[L]F**, **C[R]LF**.

Si el protocolo de transporte elegido es UDP, Panda SIEMFeeder no utiliza delimitador. Si el protocolo de transporte elegido es TCP, Panda SIEMFeeder utiliza el delimitador elegido.

- Si el protocolo de comunicación elegido cifra los datos, escribe el lugar donde se encuentra el certificado de la CA configurada en el servidor Syslog.
- Para finalizar la configuración del método de envío contesta **N** a la pregunta **Do you want to configure another delivery channel? [Yes/No]**.

Copia de logs descargados en diferentes localizaciones

Panda Importer permite descargar logs en varias localizaciones de forma simultánea. Cada log descargado se elimina de la cola de descarga en la infraestructura Azure si al menos se actualiza una de las localizaciones configurada.

Si se producen fallos en la recuperación de logs, las distintas localizaciones configuradas podrán contener un número de logs diferente.

Para implementar esta característica Panda Importer utiliza la funcionalidad de "canales". Un canal especifica el tipo de almacenamiento que utilizará Panda Importer y su configuración.

Para configurar Panda Importer :

1. Instala Panda Importer tal y como se describe en el apartado **Configuración**.
2. Detén Panda Importer tal y como se describe en el apartado **Ejecutar y parar**.
3. Añade un nuevo canal a la colección ya existente en el fichero `configuration.json`:

```
"Channels": [{ parámetros del canal 1} , {parámetros del canal 2},
…]
```

4. Indica en cada canal el tipo de almacenamiento que utilizarás para almacenar los logs y su configuración asociada.

A modo de ejemplo se muestra una configuración de Panda Importer con dos canales, el primero de ellos dejará los logs en la carpeta `Log1` y el segundo en la carpeta `Log2`:

```
"Channels": [{
"Type": "LocalDisk",
"Name": "LD1",
"Configuration": {
"fullPath":
"D:\\\\SIEMFeeder\\\\EventFeederImporter 1.0.3 Pro\\\\Log1",
"filesSplitFormat": "1m",
"filesSizeLimitInBytes": 102400,
"directoryMaxSizeInMb": 1024
}
}, {
"Type": "LocalDisk",
"Name": "LD2",
"Configuration";{
"fullPath:
```

```
"D:\\\\SIEMFeeder\\\\EventFeederImporter 1.0.3 Pro\\\\Log2",
"fileSplitFormat":"1m",
"filesSizeLimitInBytes": 102400,
"directoryMaxSizeInMb": 1024
}
},]
```

Ejecutar y parar

En modo línea de comandos

- Para iniciar Panda Importer haz doble clic en `EventsFeederImporter.Multiplatform.Host` o ejecútalo desde la línea de comandos.
- Para parar Panda Importer ejecutándose en modo linea de comandos, presiona `control + c`.

En modo demonio

- Para iniciar Panda Importer ejecuta desde la linea de comandos `sudo service siemfeeder start`
- Para parar Panda Importer ejecuta desde la linea de comandos `sudo service siemfeeder stop`
- Para obtener el estado de ejecución de Panda Importer ejecuta desde la linea de comandos `systemctl status siemfeeder.service`

Modificar la configuración de Panda SIEMFeeder

Panda SIEMFeeder almacena los parámetros de ejecución configurados en el fichero `configuration.json`. Este fichero se encuentra en la misma carpeta donde reside Panda Importer .

Una vez completado el proceso de instalación y ejecución, puedes volver a generar el fichero de configuración para cambiar algunos de sus parámetros, o modificarlo manualmente.

Regenerar el fichero de configuración con el asistente

- Para el proceso si estaba en ejecución. Consulta **Ejecutar y parar** en la página **44** en Windows o **Ejecutar y parar** en la página **56** en Linux.
- Ejecuta desde la línea de comandos o mediante doble clic el programa `EventsFeederImporter.ConfigAssistant.exe` en Windows o `EventsFeederImporter.Multiplatform.ConfigAssistant` en Linux.
- Responde **Y** a la pregunta **Do you want to change the configuration settings? [Yes/No]**
- Completa el asistente de configuración.
- Inicia Panda Importer. Consulta **Ejecutar y parar** en la página **44** en Windows o **Ejecutar y parar** en la página **56** en Linux.

Modificar manualmente la configuración de Panda SIEMFeeder

El fichero `configuration.json` sigue la sintaxis json.

- Para la ejecución de Panda SIEMFeeder. Consulta **Ejecutar y parar** en la página **44** en Windows o **Ejecutar y parar** en la página **56** en Linux.
- Abre el fichero `configuration.json` con un editor de texto.

- Para una referencia de los parámetros soportados, consulta **Parámetros relacionados con la descarga de logs con eventos** en la página **58** y **Parámetros relacionados con el registro de ejecución** en la página **59**
- Inicia la ejecución de Panda SIEMFeeder. Consulta **Ejecutar y parar** en la página **44** en Windows o **Ejecutar y parar** en la página **56** en Linux.

Parámetros relacionados con la descarga de logs con eventos

Los parámetros que determinan el comportamiento de Panda Importer para generar los ficheros log que contienen los eventos registrados son:

- **fullPath**: ruta absoluta a la carpeta donde se descargarán los ficheros de logs.
- **fileSizeLimitInBytes**: tamaño máximo que podrá alcanzar cada fichero de logs.
- **directoryMaxSizeInMb**: tamaño máximo que podrá alcanzar la carpeta que almacena los ficheros de logs. Una vez alcanzado este tamaño se borrará el 10% de los ficheros más antiguos.
- **FileSplitFormat**: intervalo de rotación de los ficheros log. El nombre del fichero contiene el año (yyyy), mes (MM), día (dd), hora(HH) y minuto (mm) del momento en la que se creó.
    - "**1h**" o vacío: formato yyyyMMdd-HH. Genera un fichero cada hora.
    - "**1m**": formato yyyyMMdd-HHmm. Genera un fichero cada minuto.
    - "**5m**": formato yyyyMMdd-HHmm. Genera un fichero cada 5 minutos.
    - "**10m**": formato yyyyMMdd-HHmm. Se genera un fichero cada 10 minutos.
    - "**15m**": formato yyyyMMdd-HHmm. Se genera un fichero cada 15 minutos.
    - "**30m**": formato yyyyMMdd-HHmm. Se genera un fichero cada 30 minutos.
- **Channels**: indica las características del canal utilizado para descargar los ficheros de logs.
- **Type**: tipo de almacenamiento utilizado en el canal.
- **Name**: nombre del canal.
- **Configuration**: configuración del canal (**fullPath**, **fileSplitFormat**, **fileSizeLimitInBytes**, **directoryMaxSizeInMb**).
- **MessageFormat**: formato del mensaje enviado al servidor Syslog:
    - **0**: RFC5424
    - **1**: RFC3164
- **MessageDelimiter**: carácter separador de los mensajes enviados al servidor Syslog:
    - **13**: CR
    - **10**: LF
    - **1310**: CRLF

- **IterationCount**: contador interno de mensajes utilizado para establecer una pausa en el envío de mensajes a Syslog.
- **IterationMs**: pausa medida en milisegundos que se establece cuando se han enviado **IterationCount** mensajes al servidor Syslog.
- **MaxBufferSize**: tamaño máximo del mensaje medido en bytes que se envía al servidor Syslog.

Parámetros relacionados con el registro de ejecución

Todas las operaciones ejecutadas por Panda Importer se registran en ficheros de texto almacenados en la carpeta `Log`, localizada en la misma carpeta que contiene el programa.

Para una descripción de los errores que puede generar Panda Importer, consulta ***Apéndice I: Solución de problemas** en la página **61***

Los parámetros que determinan el comportamiento de Panda Importer para generar el fichero log que contienen el registro de todas sus acciones ejecutadas son:

- **LogsPath**: ruta absoluta o relativa y nombre del fichero. Es necesario escapar el carácter `\` duplicando su aparición. Por ejemplo `.\\log\\log.txt`.
- **LogFileSizeLimitKBytes**: rota el fichero de logs cuando llega a un determinado tamaño en Kbytes, añadiendo el sufijo "-NúmeroDeSecuencia". Por ejemplo `log-3.txt`.
- **LogRetainedFileCountLimit**: indica el número de ficheros que Panda Importer mantiene en el dispositivo de almacenamiento. Cuando llega al número indicado en este parámetro, Panda Importer borrará el fichero más antiguo.
- **Interval**: intervalo de rotación de los ficheros de log:
    - **0**: sin rotado. El sufijo es nulo, de forma que el nombre coincide con el definido en el parámetro **LogsPath**.
    - **1**: el fichero se rota cada año. El sufijo para el nombre definido en **LogsPath** es NombrelogAño(YYYY). Por ejemplo `log2021.txt`.
    - **2**: el fichero se rota cada mes. El sufijo para el nombre definido en **LogsPath** es NombrelogAñoMes(YYYYMM). Por ejemplo `log202107.txt`
    - **3**: el fichero se rota cada día. El sufijo para el nombre definido en **LogsPath** es NombrelogAñoMesDia(YYYYMMDDhh). Por ejemplo `log20210722.txt`
    - **4**: el fichero se rota cada hora. El sufijo para el nombre definido en **LogsPath** es NombrelogAñoMesDiaHora(YYYYMMDDhh). Por ejemplo `log2021072210.txt`

- **5**: el fichero se rota cada minuto. El sufijo para el nombre definido en **LogsPath** es NombrelogAñoMesDiaHoraMinuto (YYYYMMDDhhmm). Por ejemplo `log202107221055.txt`

Capítulo 8

Apéndice I: Solución de problemas

A continuación, se enumeran las causas más probables de fallo y su posible solución:

Sintoma / error	Causas	Solución
Error de inicialización de .NET Framework.	Panda Importer no encuentra el Framework 4.6.1 o superior en el equipo del administrador.	Comprueba que el Framework 4.6.1 está instalado. Consulta la página **https://www.microsoft.com/es-es/download/details.aspx?id=49981** para su descarga.
invalid_redirect_uri **unrecognized_client_id** **unsupported_scope**	No se reconoce el identificador de cliente.	Comprueba que el cliente está correctamente registrado en el servicio Panda SIEMFeeder. Comprueba que la cuenta de correo de acceso a la consola de administración de Panda Adaptive Defense está correctamente introducida en Panda Importer.
unrecognized_client_secret **unsupported_grant_type**	La contraseña del cliente no se reconoce.	Comprueba que la cuenta de Panda utilizada para acceder al servicio Panda SIEMFeeder tiene asignado el rol Control total.

Sintoma / error	Causas	Solución
invalid_grant		Ejecuta Panda Importer y contesta **Y** a la pregunta **Do you want to change the configuration settings?** para volver a introducir la contraseña. Comprueba que el equipo donde se ejecuta Panda Importer tiene la hora sincronizada mediante NTP o un servicio equivalente. Comprueba que el servicio Hora de Windows está en funcionamiento.
unauthorized_client **unsupported_response_type** **invalid_scope** **access_denied** **invalid_request**	La información de autenticación es correcta, pero hay un problema con la descarga de datos.	Consulta al departamento de soporte de Panda.
temporarily_unavailable **server_error**	Por problemas técnicos el servicio Panda SIEMFeeder está temporalmente fuera de servicio	Ejecuta Panda Importer pasados unos minutos. Consulta la cuenta de correo utilizada para dar de alta el servicio. Si el error no es temporal se enviará un correo al administrador explicando los motivos de la parada y las alternativas disponibles.

Causas probables de fallo y solución

Capítulo 9

Apéndice II: Arquitectura de seguridad

Este capítulo trata la arquitectura de seguridad de Panda SIEMFeeder referente a los mecanismos AAA (Autorización, Autenticación y Acceso) y a la encriptación de las comunicaciones entre el software Panda Importer y el resto de elementos que forman el servicio.

Contenido del capítulo

Esquema general de seguridad AAA

Actores en la arquitectura de seguridad

La figura muestra los elementos que autentican al cliente y le conceden acceso a los recursos necesarios en la plataforma Azure para descargar los logs con la información de la monitorización del parque IT.

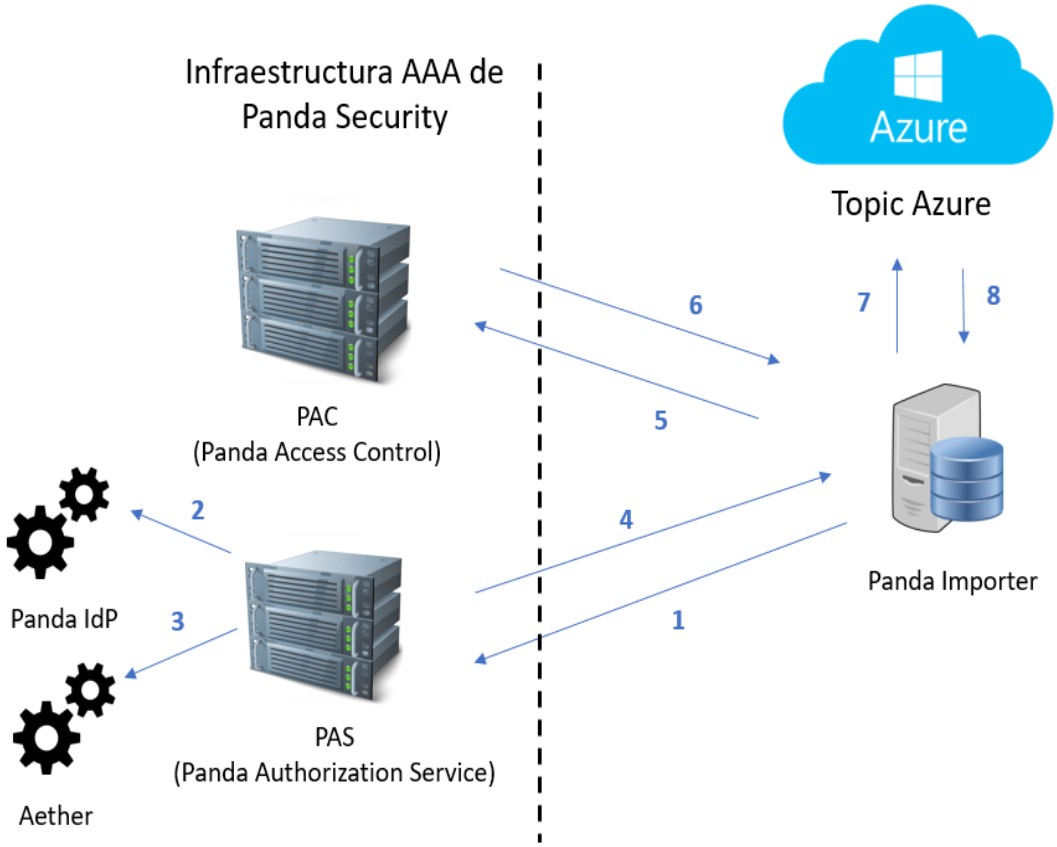

Figura 9.1: Arquitectura general de seguridad AAA

- **Panda Importer**: programa suministrado por Panda encargado de recoger los logs almacenados en la plataforma Azure.
- **Topic Azure**: recurso de tipo cola generado en la plataforma Azure, que almacena los logs recibidos desde Panda con la información de la monitorización de la infraestructura IT del cliente.
- **PAS (Panda Authorization Service)**: servicio que autentica y autoriza el acceso al topic Azure. Recibe de Panda Importer las credenciales asignadas al cliente en el proceso de contratación del servicio y le devuelve un token de acceso y un token de refresco.
- **CAC (Panda Access Control)**: servicio que permite el acceso de Panda Importer al topic de Azure provisionado para el cliente. Recibe de Panda Importer el token de refresco y devuelve una SaS key (Shared Access Signature Key).
- **Panda IdP (Identity Provider)**: servicio encargado de autenticar las credenciales enviadas.
- **Panda**: servicio encargado de autorizar el acceso al Panda SIEMFeeder.

Flujo de mensajes inicial

El flujo de mensajes inicial configura el acceso seguro al servicio Panda SIEMFeeder y es imprescindible que el equipo Panda Importer complete con éxito este procedimiento, o por el contrario no podrá acceder a la información publicada en el topic de Azure.

La figura muestra el flujo de mensajes que se intercambian en la primera ejecución de Panda Importer. Este flujo de mensajes es necesario cada vez que el usuario deja de existir en el sistema o deja de tener el rol Control Total asignado en la consola de su producto de seguridad Panda.

1. Panda Importer envía las credenciales (cuenta de correo y contraseña) asignadas al cliente.
2. Fase Autenticación: el servicio CAS conecta con el servicio Panda IdP para validar las credenciales.
3. Fase de Autorización: el servicio CAS conecta con el servicio Panda para comprobar que el cliente tiene acceso al servicio Panda SIEMFeeder.

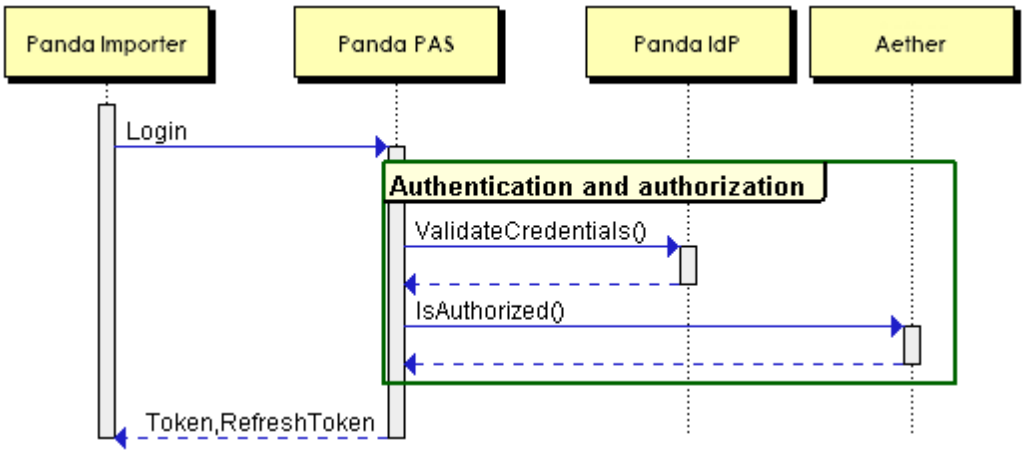

Figura 9.2: Pasos 1 a 4 del flujo de mensajes inicial

1. El servicio CAS genera y entrega un token de acceso y un token de refresco a Panda Importer.
2. Panda Importer envía el token de refresco al servicio CAC.
3. Fase de Acceso: el servicio CAC genera una SaS key (Shared Access Signature Key).
4. Acceso al topic: Panda Importer accede al topic asignado mediante la SaS key.
5. Panda Importer recibe los logs del topic suscrito.

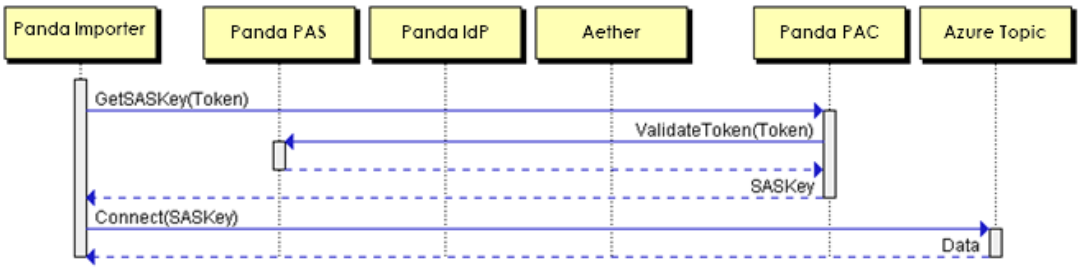

Figura 9.3: Pasos 5 a 8 del flujo de mensajes inicial

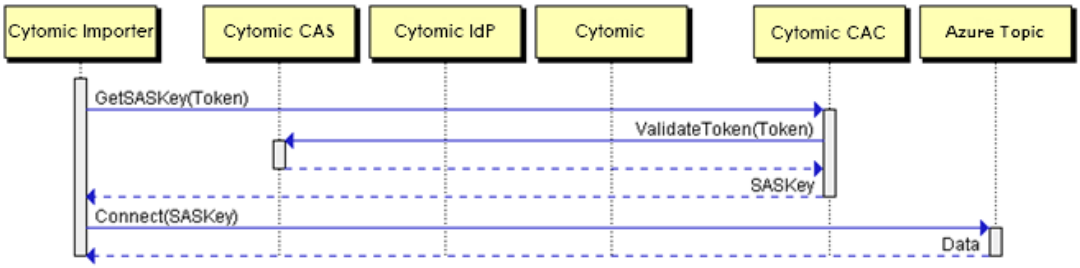

Figura 9.4: Pasos 5 a 8 del flujo de mensajes inicial

Flujo de mensajes sucesivos

Panda Importer utiliza el token de refresco para obtener la SaS key y tanto el token como la SaS key tienen una duración limitada por seguridad. Cuando expira el token de refresco, Panda Importer genera el flujo de mensajes alternativo mostrado a continuación:

1. Panda Importer pide al servicio CAS un nuevo token de refresco. Para ello envía el token de acceso asignado en el flujo inicial mostrado anteriormente.
2. Con el nuevo token de refresco, Panda Importer pide al servicio CAC una nueva SaS key.
3. Con la nueva SaS key, Panda Importer se conecta al topic Azure y continúa recogiendo los logs.

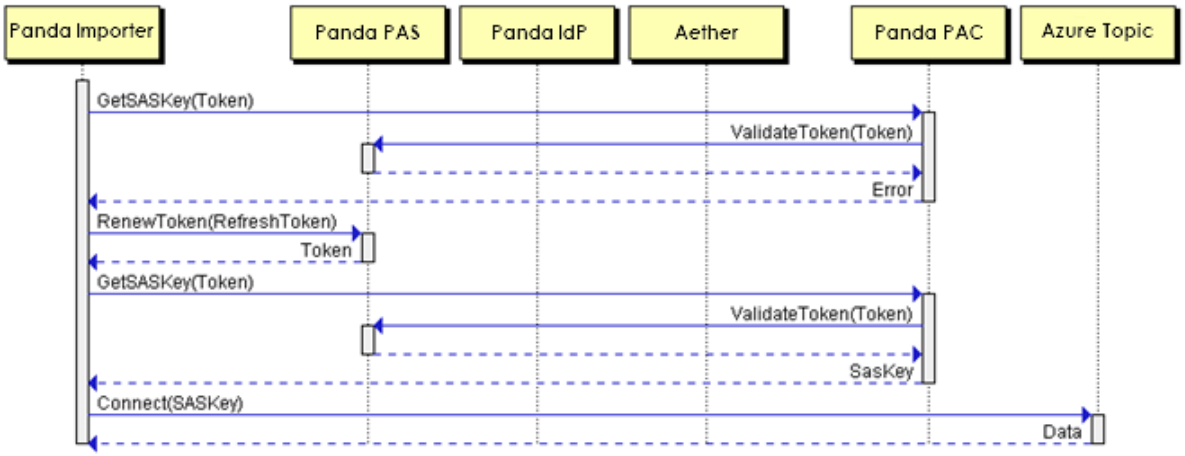

Figura 9.5: Flujo de mensajes cuando caduca el token de refresco

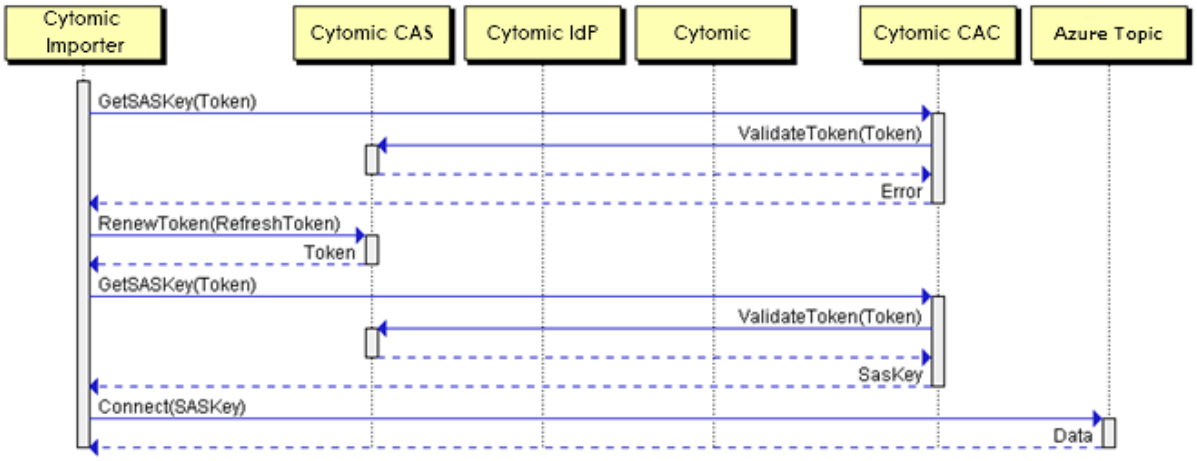

Figura 9.6: Flujo de mensajes cuando caduca el token de refresco

Características de las comunicaciones

Encriptación de las comunicaciones AAA

Las comunicaciones establecidas para la petición y envío de tokens están encriptadas con el protocolo https SSL SHA256 - G3.

Duración de los tokens asignados por Panda SIEMFeeder

- Token de refresco del CAS: 14 días
- Token de acceso del CAS: 20 minutos
- SAS key: 1 día

Panda Importer utiliza el token de refresco para acceder al topic Azure. Una vez caducado, se generará un nuevo token de acceso con los datos de la cuenta introducidos en el programa Panda Importer, y con él un nuevo token de refresco para continuar accediendo al topic Azure.

Si la cuenta utilizada en la configuración del servicio ya no se encuentra disponible o ya no tiene asignada el rol Control total, el cliente podrá seguir accediendo al servicio en tanto en cuando no expire el token de refresco (como máximo 14 días), momento en el cual será incapaz de regenerar un nuevo token de refresco y el acceso será cancelado.

Encriptación de las comunicaciones para la descarga de logs

Las comunicaciones establecidas para descarga de logs están encriptadas con el protocolo TLS/SSL y SASL.

Glosario

C

Consola Web

Herramienta de gestión del servicio de seguridad avanzada Panda SIEMFeeder, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador puede desplegar el software de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección. También permite utilizar herramientas de análisis forense que establecen el alcance de los problemas de seguridad.

D

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio (PDC) o Directorio Activo (AD).

E

Evento

Acción relevante ejecutada por un proceso en el equipo del usuario y monitorizada porPanda SIEMFeeder. Los eventos se envían a la nube de Panda en tiempo real como parte del flujo de telemetría. Allí, los analistas, threat hunters y los procesos automáticos de Machine Learning los analizan en su contexto para determinar si son susceptibles de pertenecer a la cadena CKC de un ataque informático. Consulta "CKC (Cyber Kill Chain)".

F

Firewall

También conocido como cortafuegos, es una tecnología que bloquea el tráfico de red que coincide con patrones definidos por el administrador mediante reglas. De esta manera se limita o impide la comunicación de ciertas aplicaciones que se ejecutan en los equipos, restringiéndose la superficie de exposición del equipo.

FQDN (Fully Qualified Domain Name)

Es un nombre de dominio que especifica la localización de forma precisa y sin ambiguedades dentro del árbol de jerarquía del sistema de nombres DNS. El FQDN especifica todos los niveles del dominio incluyendo el nivel superior y la zona raiz (root).

I

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

M

Machine learning

Es una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas para capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos.

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

P

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Software que hace de intermediario de las comunicaciones establecidas entre dos equipos, un cliente situado en una red interna (por ejemplo, una intranet) y un servidor en una extranet o en internet.

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

R

Red de confianza

Redes desplegadas en locales privados, tales como oficinas y domicilios. Los equipos conectados son generalmente visibles por sus vecinos y no es necesario establecer limitaciones al compartir archivos, recursos y directorios.

Red pública

Redes desplegadas en locales abiertos al público como cafeterías, aeropuertos, etc. Debido a su naturaleza publica se recomienda establecer límites en el nivel de visibilidad de los equipos que se conectan

a este tipo de redes ellas, y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

S

Servicio Panda SIEMFeeder

Modulo compatible con Panda SIEMFeeder que envía al servidor SIEM de la empresa toda la telemetría generada por los procesos ejecutado en los equipos de usuario y servidores.

SIEM (Security Information and Event Management)

Software que ofrece almacenamiento y análisis en tiempo real de las alertas generadas por los dispositivos de red.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

SYN

Bandera (flag) en el campo TOS (Type Of Service) de los paquetes TCP que los identifican como paquetes de inicio de conexión.

T

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0.

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

U

UDP (User Datagram Protocol)

Protocolo del nivel de transporte dentro de la pila de protocolos de Internet, no confiable y no orientado a la conexión para el envío y recepción de paquetes IP.

Usuario (consola)

Recurso formado por un conjunto de información que Panda SIEMFeeder utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Personal de la empresa que utiliza equipos informáticos para desarrollar su trabajo.