Panda SIEMFeeder

Guía de infraestructura Panda SIEMFeeder

Versión: 3.00.00-02

Autor: Panda Security

Fecha: 04/03/2024

panda

pandasecurity.com

Aviso legal.

Marcas registradas.

Información de contacto.

Oficinas centrales:

Panda Security
Calle Santiago de Compostela 12
Bilbao (Bizkaia) 48003 España.
https://www.pandasecurity.com/spain/about/contact/

Acerca de la Guía de infraestructura Panda SIEMFeeder

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

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

Descarga del software Panda Importer

Para obtener el paquete de instalación Panda Importer consulta la url **https://www.pandasecurity.com/es/support/card?id=950031**

Guía de eventos SIEMFeeder

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

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

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

Información técnica sobre módulos y servicios compatibles con Panda SIEMFeeder

Para acceder a la Guía de administración de Advanced Reporting Tools consulta la siguiente URL:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/ADVANCEDREPORTINGTOOL-AETHER-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

https://nexus-documents.cytomic.ai/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 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 1

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 de Panda Security.
- Al personal técnico del proveedor de servicios de seguridad (MSSP) que ha contratado el servicio Panda SIEMFeeder for Partners de Panda Security.

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

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.

Consejo importante de cara a un uso correcto de las opciones de Panda SIEMFeeder o Panda SIEMFeeder for Partners.

Consulta en otro capítulo o punto del manual.

Capítulo 2

Arquitectura Panda SIEMFeeder

Panda SIEMFeeder es el servicio de Panda Security para clientes finales que entrega a la plataforma SIEM instalada toda la información y conocimiento generado por los productos Panda Adaptive Defense. Panda SIEMFeeder facilita al administrador el descubrimiento de amenazas desconocidas, ataques dirigidos y malware avanzado de tipo APT (Advanced Persistent Threats), y amplía 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 principales del servicio Panda SIEMFeeder

El objetivo principal de Panda SIEMFeeder es servir de nexo o unión entre el software de protección instalado en los equipos de la red y el servidor SIEM de la empresa, dentro del siguiente flujo de información general:

- La monitorización permanente de Panda Adaptive Defense envía a la nube de Panda Security la información de telemetría generada por la actividad de las aplicaciones ejecutadas en los equipos del parque informático del cliente.
- Panda SIEMFeeder enriquece esta información con la inteligencia de seguridad generada por Panda Security.

- Panda Importer recupera la información enriquecida desde la infraestructura Azure asignada al cliente, y la envía directamente a su servidor SIEM o a alguna de las plataformas compatibles (Kafka y Syslog) para su posterior explotación.

Enriquecimiento de la actividad monitorizada

Panda Adaptive Defense monitoriza las acciones ejecutadas por los procesos en los equipos. Estas acciones se envían a la plataforma Cloud de Panda Security, 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 Security clasifica todos y cada uno de los procesos que ejecutan sus clientes con una fiabilidad del 99'999%, sin prácticamente falsos positivos ni negativos.

Panda SIEMFeeder reúne la información de los eventos monitorizados por Panda Adaptive Defense y la información de seguridad generada, y crea un único flujo de datos compatible con el servidor SIEM del cliente.

Para sacar partido de Panda SIEMFeeder no se requieren cambios de configuración en los equipos de usuario: el servicio opera dentro de la infraestructura de Panda Security y recibe los datos de forma centralizada desde cada uno de los puestos y servidores que pertenecen a la infraestructura IT del cliente. Estos datos son normalizados, enriquecidos y enviados al SIEM designado de cada organización, para su explotación.

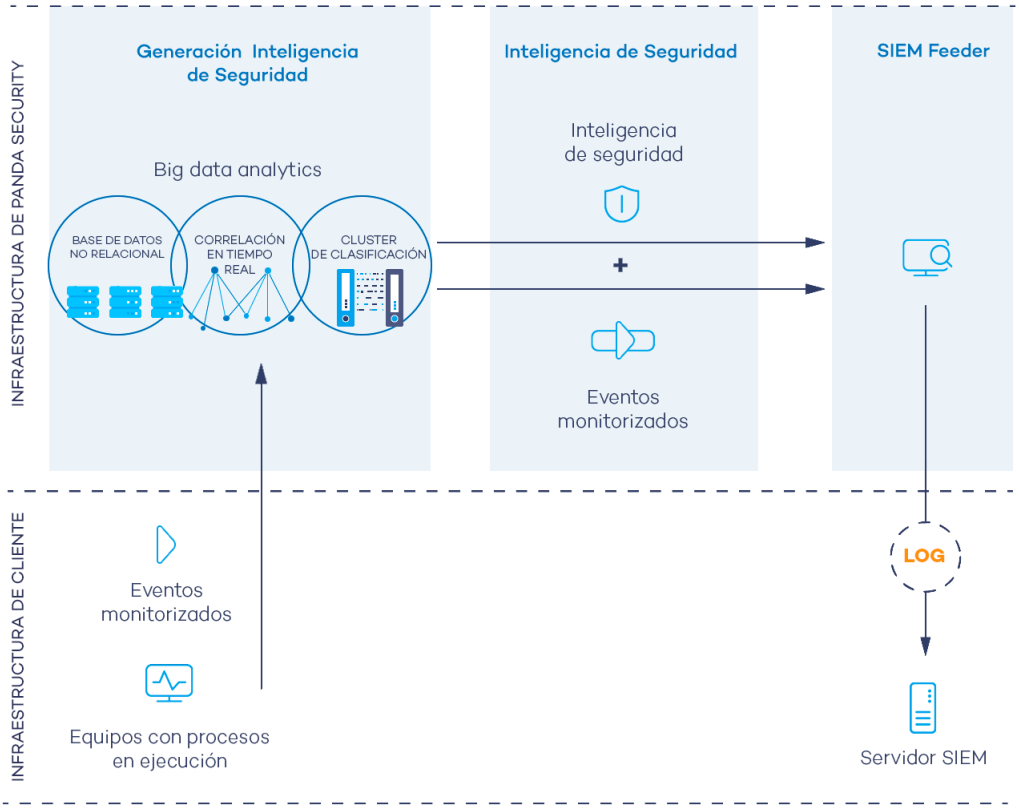

Figura 2.1: Flujo de información generada por Panda Adaptive Defense y Panda SIEMFeeder

Principales beneficios del servicio Panda SIEMFeeder

Panda SIEMFeeder suministra información sobre la actividad de los procesos ejecutados en el parque del cliente al producto SIEM instalado en sus oficinas. Con esta información el administrador es capaz de:

- **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 se facilita la elección de estrategias de resolución y posterior adaptación de las políticas de seguridad de la empresa.
- **Visualizar las acciones ejecutadas por cada proceso**, ya sea goodware malware o temporalmente desconocido, con el objetivo de detectar actividades sospechosas de los programas de reciente aparición. Panda SIEMFeeder recopila indicios que permitan obtener conclusiones acerca de su potencial peligrosidad.
- **Visualizar los accesos de los procesos a la información confidencial de la empresa** para prevenir su extracción o robo. Se muestran 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 ayudar en el diseño de 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 siguiente esquema:

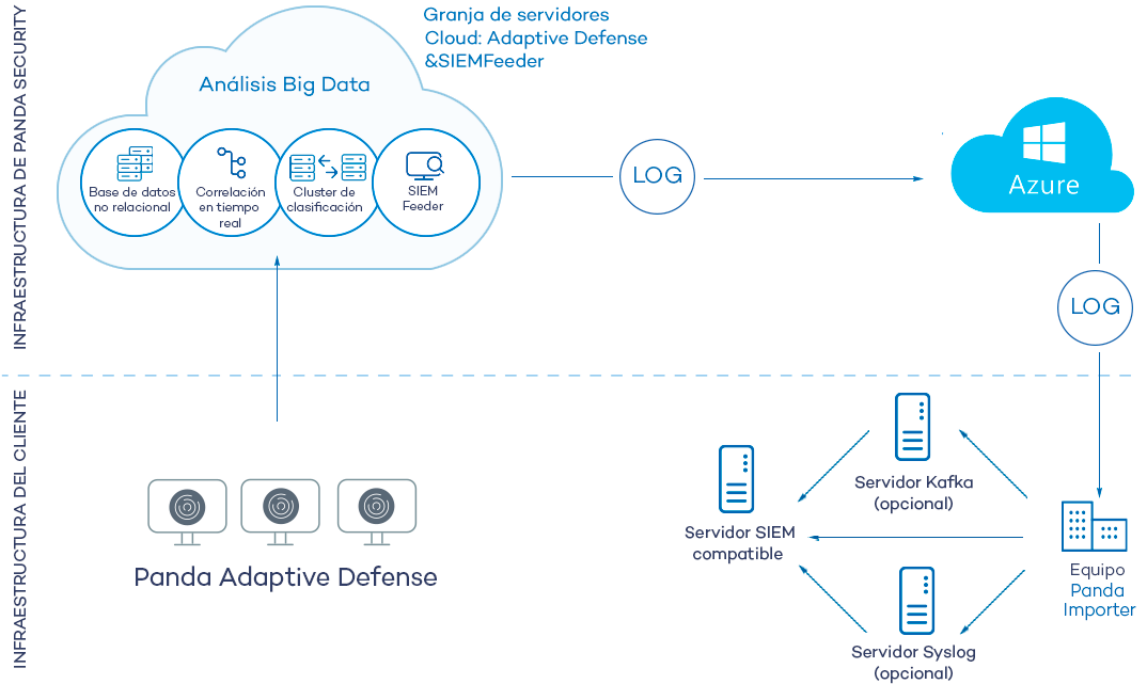

Figura 2.2: Esquema lógico de los módulos que constituyen Panda SIEMFeeder y su relación

En la figura se representan los siguientes elementos:

- Equipos de la red del cliente protegidos con Panda Adaptive Defense sobre Aether, Panda Adaptive Defense 360 sobre Aether, Adaptive Defense Tradicional o Adaptive Defense 360 Tradicional.
- **Nube de Panda Security**: recoge la información de los procesos ejecutados y la utiliza 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 al cliente.
- **Infraestructura Azure**: recibe los logs del servicio Panda SIEMFeeder y los almacena temporalmente a la espera de que el cliente los descargue.
- **Equipo Panda Importer**: equipo en la red del cliente que ejecuta el proceso Panda Importer y comprueba si hay disponibles logs nuevos en la infraestructura Azure para su descarga y almacenamiento.
- **Servidor Kafka (opcional)**: equipo de la red del cliente que gestiona las colas de los logs recibidos por Panda Importer y los envía al servidor SIEM de la empresa.
- **Servidor Syslog (opcional)**: equipo de la red del cliente que recoge los logs recibidos por Panda Importer y los envía al servidor SIEM de la empresa.
- **Servidor SIEM:** se instala en la oficina del cliente y 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 la empresa.

- **Cortafuegos perimetrales y locales:** protegen la salida y entrada de datos entre el equipo Panda Importer y la infraestructura Azure.

Beneficios de la infraestructura Azure

Panda SIEMFeeder genera logs de forma asíncrona con la información recogida de los equipos protegidos, y los almacena temporalmente hasta que el cliente los recupera e integra en su sistema SIEM. Para ello, Panda Security utiliza servicios Cloud alojados en la infraestructura 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. El espacio asignado a cada cliente son 80 Gigabytes y la información se retiene por un máximo de 7 días.
- **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 de Panda Importer se utilizan dos tokens independientes que permiten negociar la clave compartida necesaria para acceder a la plataforma Panda SIEMFeeder y recuperar la información de la red del cliente. Cada token tiene un tiempo de caducidad diferente, lo que garantiza la confidencialidad del acceso a la información.

Para obtener mas información, consulta el "Apéndice II: Arquitectura de seguridad" en la página 55

- **Comunicaciones comprimida**s: los datos enviados se comprimen para minimizar el ancho de banda requerido en las oficinas del cliente.
- **Mecanismo PUSH de entrega**: para facilitar la configuración de los cortafuegos, la dirección de las conexiones con la infraestructura Azure es saliente desde la red del cliente. Una vez establecido el canal de comunicación, Azure envía los logs nuevos disponibles en la plataforma mediante mensajes de tipo PUSH, en lugar de utilizar mecanismos como el "pooling".

Recorrido del flujo de información

Panda Adaptive Defense recoge la actividad de los procesos ejecutados gracias a la monitorización permanente, y envía la información a la nube de Panda Security. Allí se completa con inteligencia de seguridad y se deposita en la infraestructura Azure, donde residirá temporalmente hasta su recogida por parte del cliente suscrito al servicio Panda SIEMFeeder.

El programa Panda Importer se ejecuta en un servidor de la red del cliente, descarga los logs generados y, dependiendo de su configuración, los gestiona de distintas maneras:

- Almacena los logs en una carpeta directamente accesible por el servidor SIEM de la organización, y gestiona el volumen de ficheros guardados para no sobrepasar los límites fijados por el administrador.

- Envía los logs a un servidor de colas Kafka para que el servidor SIEM los recoja al ritmo que le permitan sus recursos.
- Envía los logs a un servidor de Syslog para que el servidor SIEM los recoja al ritmo que le permitan sus recursos disponibles.

El servidor SIEM del cliente importará los logs y los analizará periódicamente para incorporar la información a su repositorio y generar los paneles de control apropiados.

Capítulo 3

Arquitectura Panda SIEMFeeder for Partners

Panda SIEMFeeder for Partners es el servicio de Panda Security que entrega a la plataforma SIEM del proveedor de servicios de seguridad (MSSP) toda la información y el conocimiento generados por los productos Panda Adaptive Defense instalados en los equipos de sus clientes. Panda SIEMFeeder facilita al MSSP el descubrimiento de amenazas desconocidas, ataques dirigidos y malware avanzado de tipo APT (Advanced Persistent Threats) que reside en las infraestructuras IT de sus clientes.

CONTENIDO DEL CAPÍTULO

Objetivos del servicio Panda SIEMFeeder for Partners

El objetivo principal de Panda SIEMFeeder for Partners es servir de nexo o unión entre el software de protección instalado en los equipos de los clientes y el servidor SIEM del MSSP, dentro del siguiente flujo de información general:

- La monitorización permanente de Panda Adaptive Defense envía a la nube de Panda Security la información de telemetría generada por la actividad de las aplicaciones ejecutadas en los equipos de los clientes del MSSP.
- Panda SIEMFeeder for Partners enriquece esta información con la inteligencia de seguridad generada por Panda Security.
- Panda Importer recupera la información enriquecida desde la infraestructura Azure asignada al MSSP, y la envía directamente su servidor SIEM, o a alguna de las plataformas de almacenamiento y gestión de colas compatibles (Kafka y Syslog), para su posterior explotación.

Enriquecimiento de la actividad monitorizada

Panda Adaptive Defense monitoriza las acciones ejecutadas por los procesos en los equipos de los clientes. Estas acciones se envían a la plataforma Cloud de Panda Security, 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 Security clasifica todos y cada uno de los procesos que ejecutan sus clientes con una fiabilidad del 99'999%, sin prácticamente falsos positivos ni negativos.

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 del MSSP.

Para sacar partido de Panda SIEMFeeder for Partners, no se requieren cambios de configuración en los equipos de usuario de sus clientes: el servicio opera dentro de la infraestructura de Panda Security, y recibe los datos de forma centralizada desde cada uno de los puestos y servidores que pertenecen a la infraestructura IT del cliente. Estos datos son normalizados, enriquecidos y enviados al SIEM del MSSP, para su explotación.

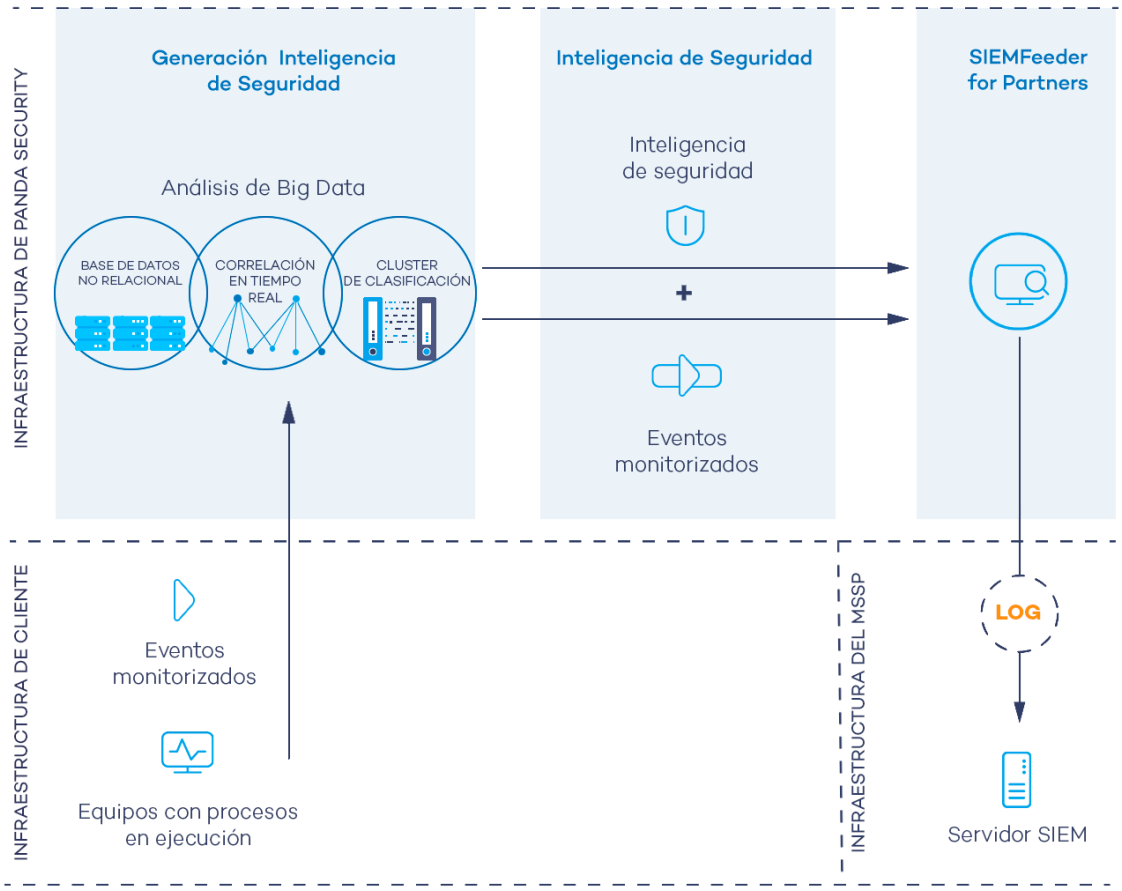

Figura 3.1: Flujo de información generada por Panda Adaptive Defense y Panda SIEMFeeder

Beneficios del servicio Panda SIEMFeeder for Partners

Panda SIEMFeeder for Partners suministra información sobre la actividad de los procesos ejecutados en el parque de los clientes del MSSP. Con esta información el MSSP es capaz de:

- **Visualizar la evolución del estado del malware detectado en la red de sus clientes**, indicando si fue ejecutado o no, el vector de infección y las acciones ejecutadas por el proceso. De esta forma, se facilita la elección de estrategias de resolución y posterior adaptación de las políticas de seguridad de las empresas.
- **Visualizar las acciones ejecutadas por cada proceso**, ya sea goodware, malware o temporalmente desconocido, con el objetivo de detectar actividades sospechosas de los programas de reciente aparición. 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 los clientes** para prevenir su extracción o robo. Se muestran 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 al exterior.
- **Localizar todos los programas ejecutados**, y especialmente aquellos instalados en los equipos de los usuarios que contengan vulnerabilidades conocidas, para ayudar en el diseño de un plan de actualización de software y refinar las políticas de seguridad establecidas en las empresas.
- **Aplicar configuración centralizada a través de Panda Partner Center,** que permite asignar configuraciones para todos los clientes del MSSP de forma simultánea.
- **Instalar el servicio con seguridad y fácilmente** ya que se puede 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, se 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 la infraestructura del MSSP, lo que supone minimizar el ancho de banda y el almacenamiento consumidos.

Arquitectura general

El servicio Panda SIEMFeeder for Partners está formado por los módulos mostrados en el esquema 3.2:

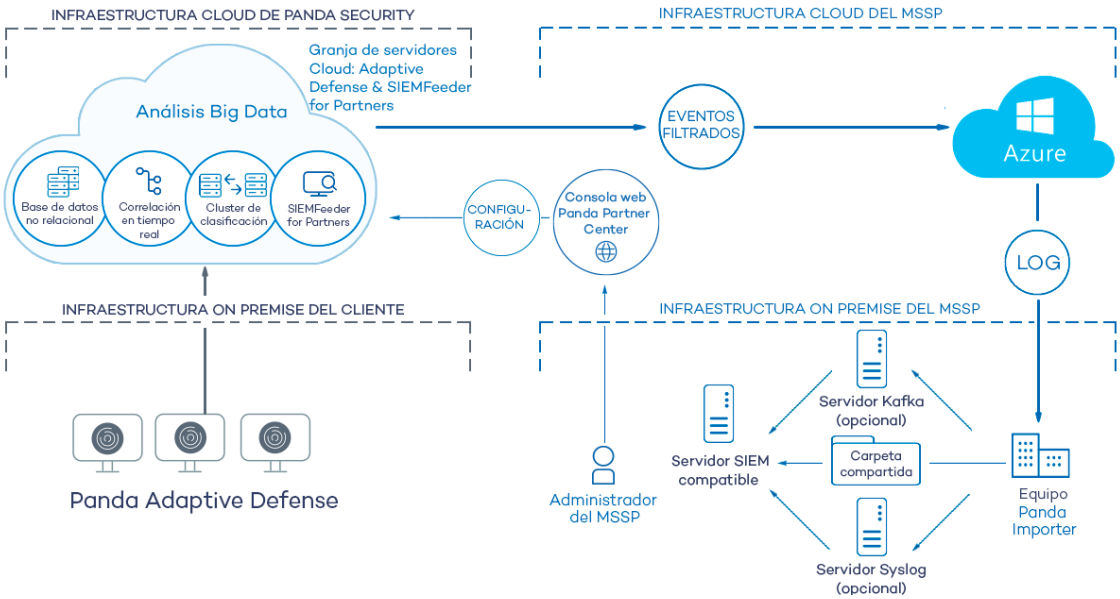

Figura 3.2: Esquema lógico de los módulos que constituyen Panda SIEMFeeder for Partners y su relación

En la figura se representan los siguientes elementos:

- **Equipos de la red del cliente:** protegidos con Panda Adaptive Defense sobre Aether o Panda Adaptive Defense 360 sobre Aether.
- **Nube de Panda Security**: 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 infraestructura Azure asignada al MSSP.
- **Infraestructura Azure del MSSP**: recibe los logs del servicio Panda SIEMFeeder for Partners en la infraestructura cloud asignada al MSSP, 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 y comprueba si hay disponibles logs nuevos en la infraestructura Azure para su descarga y almacenamiento.
- **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 los 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 infraestructura Azure

Panda SIEMFeeder for Partners genera logs de forma asíncrona y los almacena temporalmente hasta que son recuperados e integrados en su sistema SIEM. Para ello, Panda Security utiliza servicios Cloud alojados en la infraestructura 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. El espacio asignado a cada MSSP son 80 Gigabytes y la información se retiene por un máximo de 7 días.
- **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 de Panda Importer se utilizan dos tokens independientes. Su uso permite negociar la clave compartida necesaria para acceder a la plataforma Panda SIEMFeeder for Partners y recuperar la información de los clientes del MSSP. Cada token tiene un tiempo de caducidad diferente, lo que garantiza la confidencialidad del acceso a la información.

Para obtener más información, consulta el "Apéndice II: Arquitectura de seguridad" en la página 55

- **Comunicaciones comprimidas**: los datos enviados se comprimen para minimizar el ancho de banda requerido en las oficinas del MSSP.
- **Mecanismo PUSH de entrega**: para facilitar la configuración de los cortafuegos, la dirección de las conexiones con la infraestructura Azure es saliente desde la red del MSSP. Una vez establecido el canal de comunicación, Azure envía los logs nuevos disponibles en la plataforma mediante mensajes de tipo PUSH, en lugar de utilizar mecanimos como el "pooling".

Operativa general del proveedor de servicios

Para recuperar la información de seguridad generada por los clientes, el proveedor de servicios de seguridad debe interactuar con los elementos mostrados en la figura 3.2. Para ello, es necesario seguir de forma general la siguiente lista de acciones:

- Verifica que la suscripción al servicio Panda SIEMFeeder for Partners continúa vigente en Panda Partner Center. Consulta Gestión de licencias en la Guía de administración Partner Center. Si tu

suscripción ha caducado o no eres cliente de Panda SIEMFeeder for Partners, consulta con el comercial de Panda Security asignado.

- Comprueba la conectividad de todos los elementos mostrados en la figura 3.2, especialmente los relativos a la comunicación entre Panda Importer y Azure. Consulta "**Configuración de los cortafuegos**" en la página 19.
- Revisa los requisitos de despliegue e instalación. Consulta "**Requisitos de despliegue e integración**" en la página 17.
- Instala Panda Importer en tu infraestructura de IT. Consulta "**Instalación y configuración de Panda Importer en sistemas Windows**" en la página 25 o "**Instalación y configuración de Panda Importer en sistemas Linux**" en la página 39.
- Crea una configuración de Panda SIEMFeeder for Partners en Panda Partner Center indicando los grupos de eventos que se enviarán a la infraestructura Azure. Consulta **Configuración SIEMFeeder for Partners** en la **Guía de administración Partner Center**.
- Asocia la configuración recién creada a los clientes. Consulta **Asignar y enviar configuraciones** en la **Guía de administración Partner Center**. 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 "**Guía de administración de Panda Adaptive Defense sobre Aether y Panda Adaptive Defense 360 sobre Aether**" para acceder a la guía de administración del producto contratado por el cliente.

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

Capítulo 4

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, es necesario 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 sobre Aether (compatible con Panda SIEMFeeder y con Panda

SIEMFeeder for Partners)

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

Panda SIEMFeeder

- Para Panda Adaptive Defense sobre Aether o Panda Adaptive Defense 360 sobre Aether, utiliza la dirección de correo electrónico y contraseña de un usuario de la consola que tenga asignado el rol Control total.
- Para Panda Adaptive Defense Tradicional o Panda Adaptive Defense 360 Tradicional utiliza el usuario predeterminado de la consola.
- Una cuenta de correo gestionada por el administrador, que se utilizará para enviar notificaciones sobre el estado del servicio.
- El código de cliente que aparece en el mail de bienvenida enviado al administrador de la red en el momento de aprovisionar el servicio Panda Adaptive Defense.

Panda SIEMFeeder for Partners

- La dirección de correo electrónico y contraseña de un usuario de Panda Adaptive Defense sobre Aether o Panda Adaptive Defense 360 sobre Aether 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

A continuación, se presentan los requisitos necesarios para poder desplegar y utilizar Panda SIEMFeeder y Panda SIEMFeeder for Partners:

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

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

- El programa Panda Importer correctamente configurado. Para más información, consulta "**Instalación y configuración de Panda Importer en sistemas Windows**" en la página **25**.
- 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 infraestructura 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), AmqpWebSockets (puerto 443).

Configuración del servidor proxy

Si Panda Importer accede a la nube de Panda Security 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 del cliente, y del retraso máximo admitido según las necesidades de la organización. 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" en la página 23. 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 de la organización.*

- **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 son aquellos que admitan logs en el 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 datos, es necesario configurar como fuente el sistema elegido para el almacenamiento de datos y mapear correctamente los eventos y campos entregados. Las fuentes disponibles 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 el **Manual de descripción de eventos de Panda SIEMFeeder.**

Características de los ficheros log descargados

- Cada fichero log tiene un tamaño máximo de 256 Kbytes comprimido.
- Los logs se almacenan descomprimidos en la carpeta elegida con un tamaño especificado en la 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 monitorizados en la red (500 Kbytes por equipo y hora).
- Utiliza el valor calculado en el punto anterior para establecer reglas de QoS en el router de la 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 el **Manual de descripción de eventos de Panda SIEMFeeder**.

- 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, quiere decir que Panda SIEMFeeder está 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 el capítulo "**Instalación y configuración de Panda Importer en sistemas Windows**" en la página **25**.
- **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 Security 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 5

Instalación y configuración de Panda Importer en sistemas Windows

Panda Importer es la aplicación encargada de descargar desde la infraestructura Azure los eventos que registran Panda SIEMFeeder y Panda SIEMFeeder for Partners. Estos eventos se almacenan empaquetados en ficheros log y, dependiendo de la configuración elegida, 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 para su correcto funcionamiento, consulta "**Licencias e información necesaria**" en la página 17.

Sistema operativo y librerías necesarias

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

- **.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

Panda Importer se puede ejecutar como un programa de línea de comandos, o en modo desatendido 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 no requiere permisos especiales mas allá del acceso a los recursos que necesite, como por ejemplo acceso de escritura sobre la carpeta configurada como almacenamiento de los logs descargados.

Configuración de los cortafuegos

Para que el equipo Panda Importer pueda descargar los logs desde la infraestructura 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 infraestructura Azure, es necesario completar un proceso de autenticación y autorización que implica la generación de un token. Para mejorar la seguridad de todo el proceso, este token se emite con una fecha de caducidad, y por tanto es necesario que ambos extremos de la comunicación tengan el reloj sincronizado. Por esta razón, es necesario que el equipo que ejecuta Panda Importer tenga en funcionamiento el servicio Hora de Windows u otro servicio equivalente que le permita 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 **53**.

El proceso de instalación y configuración básica de Panda Importer comprende varios pasos a ejecutar en el orden indicado:

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. Configura el método de envío y almacenamiento de los logs recibidos. Consulta "**Configurar el modo de almacenamiento y envío de logs**".
5. Configura el modo en el que se ejecutará Panda Importer: como servicio o desde linea de comandos. Consulta "**Configurar el modo de ejecución**".
6. Indica la plataforma donde residen los productos de seguridad contratados con Panda. Consulta "**Configurar la plataforma a utilizar**".
7. Actualiza el fichero `configuration.json` con la nueva configuración de la instalación. Consulta "**Actualiza el fichero configuration.json**".

Descarga del paquete de instalación

Descarga el paquete .zip de la versión Windows de Panda Importer desde el enlace **https://www.pandasecurity.com/spain/support/card?id=950031** 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 definida por el administrador. Este programa puede ejecutarse como proceso desde la línea de comandos o como servicio (consulta "**Configurar el modo de ejecución**").
- `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

Panda Importer se puede ejecutar varias veces de forma simultánea en un mismo equipo. Cada instancia de Panda Importer requiere un fichero de configuración independiente. Consulta el apartado "**Configurar múltiples instancias**".

Configuración

En este apartado se describe la generación del fichero de configuración necesario para que una única instancia de Panda Importer se ejecute en modo servicio o linea de comandos y se conecte a la infraestructura Azure para descargar los logs. El resto de escenarios toman como base esta configuración.

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

Si el equipo está detrás de un servidor proxy contesta **Y** a la pregunta Is **Event Importer behind a proxy server? [Yes/No]**. En este caso se pide la dirección IP del servidor proxy, y el usuario y la contraseña si se requiere autenticación.

El acceso mediante proxy únicamente se usa para conectar con la infraestructura Azure asignada al cliente o MSSP. Las conexiones a otros recursos internos como el servidor de ficheros, servidor Kafka o servidor Syslog no utilizarán el proxy configurado.

Configurar la plataforma a utilizar

- Determina la plataforma a la que pertenece el producto Panda Adaptive Defense previamente contratado, y contesta a la pregunta **Select your platform: [C]urrent, [L]egacy, or [W]G Endpoint Security:**
  - **C (Current)**: si la cuenta utilizada pertenece a la plataforma Aether.
  - **L (Legacy)**: si la cuenta utilizada pertenece a la plataforma tradicional.
  - **W (Watchguard)**: no aplica para clientes de Panda Security.

Escribir las credenciales de acceso

- Escribe la dirección de correo de la cuenta utilizada para acceder a la consola Panda Adaptive Defense sobre Aether. Para la versión de Panda Adaptive Defense Tradicional, utiliza el usuario predeterminado de la consola.
- 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 internamente para suscribirse al servicio 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 sobre Aether:

- Si tu proveedor de seguridad es Panda Security haz clic en **https://www.pandacloudsecurity.com/PandaLogin/ y escribre** 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 "**Configuración del almacenamiento y reenvío 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 el usuario que inició el proceso de instalación tiene 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 el apartado "**Configurar múltiples instancias**".

Actualiza el fichero configuration.json

Al terminar su ejecución, el asistente de configuración actualizará con la información introducida el fichero `configuration.json` situado en la misma carpeta, y acto seguido Panda Importer comenzará a descargar los logs almacenados en la infraestructura 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 el apartado "**Dimensionamiento del hardware del equipo Panda Importer**" en la página **22**, se recomienda instalar una o varias instancias adicionales del programa y ejecutarlas de forma concurrente.

- Si es necesario que un mismo equipo con Panda Importer descargue logs de más de un cliente simultáneamente, pero no se está 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://www.pandasecurity.com/spain/support/card?id=950031** 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

Si quieres ejecutar varias instancias de Panda Importer en modo servicio, es necesaria su instalación previa en modo linea de comandos y su posterior registro manual como servicio. Para ello, sigue los pasos mostrados a continuación.

- 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**".
- Interrumpe con `control + c` la ejecución de cada instancia en ejecución.
- Si vas a ejecutar Panda Importer como un servicio, es necesario su registro manual. Para ello se requiere dar un nombre distinto a cada instancia con los parámetros `servicename`, `description` y `displayname`. Ejecuta los comandos siguientes como administrador:

```
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
```

- Inicia cada instancia en Panda Importer.

```
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 infraestructura Azure:

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

El método de almacenamiento se elige en el asistente de configuración, cuando se 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]**. Al presionar **Y** 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 equipo que ejecuta Panda Importer o una unidad / recurso remoto compartido por red.
- 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 se enviarán 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, hay que indicar 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, se recomienda 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 así descargado se eliminará de la cola de descarga si al menos una de las localizaciones fue correctamente actualizada; de esta manera es posible que si se producen fallos en la recuperación de logs, las distintas localizaciones terminen el proceso con un número de logs diferente. Para implementar esta característica se utiliza la funcionalidad de "canales". Un canal especifica el tipo de almacenamiento que utilizará Panda Importer y su configuración.

Para configurar Panda Importer sigue los pasos mostrados a continuación:

- Instala Panda Importer tal y como se describe en el apartado "**Configuración**".
- Detén Panda Importer tal y como se describe en el apartado "**Ejecutar y parar**".
- Añade un nuevo canal a la colección ya existente en el fichero `configuration.json`. La sintaxis del parámetro `channels` es la siguiente:

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

- En cada canal se indica el tipo de almacenamiento utilizado 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 se utilizó el registro manual del servicio). 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.

Modificar la configuración

Para regenerar la configuración de Panda Importer sigue los pasos mostrados a continuación:

- Detén el proceso si estaba en ejecución. Consulta "Ejecutar y parar".

- Ejecuta de nuevo el programa `EventsFeederImporter.ConfigAssistant.exe` desde la línea de comandos o mediante doble clic.
- Responde **Y** a la pregunta **Do you want to change the configuration settings? [Yes/No]**
- Escribe la información requerida en el punto "Configurar la plataforma a utilizar".
- Inicia Panda Importer. Consulta "Ejecutar y parar".

Editar manualmente la configuración de Panda Importer

El fichero `configuration.json` se encuentra en la misma carpeta donde reside Panda Importer y contiene sus parámetros de ejecución.

La primera vez que se ejecuta, el programa pedirá cierta información de autenticación que posteriormente volcará en el fichero de configuración. Una vez completado el proceso de instalación y ejecución, podrás modificar el fichero de configuración para afinar algunos de sus parámetros.

Siempre que se modifica el fichero `configuration.json` *es necesario parar y arrancar el proceso Panda Importer para que tenga en cuenta los cambios aplicados al fichero. Consulta "Ejecutar y parar".*

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

Parámetros relacionados con los logs que contienen eventos

Los parámetros que determinan el comportamiento de Panda Importer para generar los ficheros log que contienen los eventos registrados por Panda SIEMFeeder 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).

Parámetros relacionados con el registro de ejecución

Todas las operaciones ejecutadas por Panda Importer se registran en ficheros de tipo 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 53

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 mantendrá 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 6

Instalación y configuración de Panda Importer en sistemas Linux

Panda Importer es la aplicación encargada de descargar desde la infraestructura Azure los eventos que registra Panda SIEMFeeder y Panda SIEMFeeder for Partners. Estos eventos se almacenan empaquetados en ficheros log y, dependiendo de la configuración elegida, 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 para su correcto funcionamiento consulta "Licencias e información necesaria" en la página 17.

Sistema operativo y librerías necesarias

El paquete de descarga contiene todo lo necesario para que Panda Importer pueda funcionar en las distribuciones indicadas a continuación:

- Ubuntu 18.04.4 LTS Desktop (64bits)
- Red Hat Enterprise Linux 7.2 Server (64bits)

Permisos necesarios

Panda Importer se puede ejecutar como un programa de línea de comandos, o como un demonio del sistema.

- En modo demonio se ejecuta bajo una cuenta de usuario, pero serán necesarios permisos de root para que el administrador pueda completar su configuración.
- En modo línea de comandos no requiere permisos especiales más allá del acceso a los recursos que necesite, como por ejemplo acceso de escritura sobre la carpeta configurada como almacenamiento de los logs descargados.

Configuración de los cortafuegos

Para que el equipo Panda Importer pueda descargar los logs desde la infraestructura 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 infraestructura Azure, es necesario completar un proceso de autenticación y autorización que implica la generación de un token. Para mejorar la seguridad de todo el proceso, este token se emite con una fecha de caducidad, y por tanto es necesario que ambos extremos de la comunicación tengan el reloj sincronizado. Por esta razón, es necesario que el equipo que ejecuta Panda Importer tenga en funcionamiento el demonio `ntpd` u otro equivalente que le permita 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 **53**.

El proceso de instalación y configuración básica de Panda Importer comprende varios pasos a ejecutar en el orden indicado:

1. Descarga y descomprime el fichero .gz que contiene el instalador. Consulta "**Descarga del paquete de instalación**".
2. (opcional) 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 "**Configurar el modo de almacenamiento y envío 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://www.pandasecurity.com/spain/support/card?id=950031** y descomprímelo en una carpeta del equipo. El paquete contiene varios ficheros principales:`EventsFeederImporter.Multiplatform.Host`: descarga los ficheros log que contienen los eventos que registrados en los equipos del cliente, y los

almacena en el disco duro del equipo o los reenvía a otro, dependiendo de la configuración definida por el administrador. Este programa puede ejecutarse como proceso desde la línea de comandos o como demonio (consulta "**Configurar Panda Importer como demonio**".

- `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.

Panda Importer se puede ejecutar varias veces de forma simultánea en un mismo equipo. Cada instancia de Panda Importer requiere un fichero de configuración independiente. Consulta el apartado "**Configurar múltiples instancias**".

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

En este apartado se describe la generación del fichero de configuración necesario para que una única instancia de Panda Importer se ejecute en modo linea de comandos y se conecte a la infraestructura Azure para descargar los logs. El resto de escenarios toman como base esta configuración.

Para configurar Panda Importer, es necesario ejecutar el programa `EventsFeederImporter.Multiplatform.ConfigAssistant` 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.

Configurar el método de conexión

Si el equipo está detrás de un servidor proxy contesta **Y** a la pregunta **Is Event Importer behind a proxy server? [Yes/No].** En este caso se pide 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: ":", "/", "?", "#", "[", "]", "@", "!", "$", "&", "'", "(", ")","*", "+",",",";","=","," "

El acceso mediante proxy unicamente se utiliza para conectar con la infraestructura Azure asignada al cliente o MSSP. Las conexiones a otros recursos internos como al servidor de ficheros, servidor Kafka o servidor Syslog no utilizarán el proxy configurado.

Configurar la plataforma a utilizar

- Determina la plataforma a la que pertenece el producto Panda Adaptive Defense previamente contratado, y contesta a la pregunta **Select your platform: [C]urrent, [L]egacy, or [W]G Endpoint Security:**
  - **C (Current)**: si la cuenta utilizada pertenece a la plataforma Aether.
  - **L (Legacy)**: si la cuenta utilizada pertenece a la plataforma tradicional.
  - **W (Watchguard)**: no aplica para clientes de Panda Security.

Escribir las credenciales de acceso

- Escribe la dirección de correo de la cuenta utilizada para acceder a la consola Panda Adaptive Defense sobre Aether. Para la versión de Panda Adaptive Defense Tradicional, utiliza el usuario predeterminado de la consola.
- 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 internamente para suscribirse al servicio 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 sobre Aether:

- Si tu proveedor de seguridad es Panda Security haz clic en **https://www.pandacloudsecurity.com/PandaLogin/ y escribre** 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 "Configuración del almacenamiento y reenvío de logs".

Actualizar el fichero configuration.json

Al terminar su ejecución, el asistente de configuración actualizará con la información introducida el fichero `configuration.json` situado en la misma carpeta, y acto seguido Panda Importer comenzará a descargar los logs almacenados en la infraestructura Azure.

El fichero `configuration.json` contendrá 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:

- Si estás configurando Panda Importer tal como se indica en el apartado "Configuración", una vez terminado el procedimiento, para el proceso siguiendo los pasos indicados a continuación:
  - Abre una nueva linea de comandos y ejecuta el comando `ps ax | grep "EventsFeederImporter.Multiplatform.Host"`.
  - Apunta el PID del proceso y ejecuta el comando kill -9 #PID#
  - Vuelve a la ventana inicial y presiona `control + c`.
- Si Panda Importer ya estaba configurado con anterioridad y se está ejecutando en modo linea de comandos, presiona `control + c`.
- 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`.
- Copia el fichero `siemfeeder.service` al directorio de sistema de la distribución Linux utilizada. Las rutas más frecuente son:
  - `/lib/systemd/system`

- `/usr/lib/systemd/system`

- Ejecuta el comando `sudo systemctl enable siemfeeder` para añadir el script a la secuencia de inicio del sistema.

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 el apartado "**Dimensionamiento del hardware del equipo Panda Importer**" en la página 22, se recomienda instalar una o varias instancias adicionales del programa y ejecutarlas de forma concurrente.
- Si es necesario que un mismo equipo con Panda Importer descargue logs de más de un cliente simultáneamente, pero no se está 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://www.pandasecurity.com/spain/support/card?id=950031** y descomprímelo en una carpeta independiente por cada cliente del que se quiere 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.

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 infraestructura Azure:

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

El método de almacenamiento se elige en el asistente de configuración, cuando se 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]**. Al presionar **Y** 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 equipo que ejecuta Panda Importer o una unidad / recurso remoto compartido por red.
- 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.
- 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 se enviarán 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, hay que indicar 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, se recomienda 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 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.
- 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 así descargado se eliminará de la cola de descarga si al menos una de las localizaciones fue correctamente actualizada; de esta manera es posible que si se producen fallos en la recuperación de logs, las distintas localizaciones terminen el proceso con un número de logs diferente. Para implementar esta característica se utiliza la funcionalidad de "canales". Un canal especifica el tipo de almacenamiento que utilizará Panda Importer y su configuración.

Para configurar Panda Importer sigue los pasos mostrados a continuación:

- Instala Panda Importer tal y como se describe en el apartado "**Configuración**".
- Detén Panda Importer tal y como se describe en el apartado "**Ejecutar y parar**".
- Añade un nuevo canal a la colección ya existente en el fichero `configuration.json`. La sintaxis del parámetro `channels` es la siguiente:

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

- En cada canal se indica el tipo de almacenamiento utilizado 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.
- Si has configurado Panda Importer tal como se indica en el apartado "**Configuración**" y una vez terminado el procedimiento quieres pararlo, sigue los pasos indicados a continuación:
  - Abre una nueva linea de comandos y ejecuta el comando `ps ax | grep "EventsFeederImporter.Multiplatform.Host"`.
  - Apunta el PID del proceso y ejecuta el comando kill -9 #PID#
  - Vuelve a la ventana inicial y presiona `control + c`.
- Para para Panda Importer si ya estaba configurado con anterioridad y se está ejecutando 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

Para modificar la configuración de Panda Importer, sigue los pasos mostrados a continuación:

- Detén el proceso si estaba en ejecución.
  - Si Panda Importer se ejecuta en modo linea de comandos pulsa Control + c.
  - Si Panda Importer se ejecuta en modo demonio ejecuta en una linea de comandos `sudo service siemfeeder stop`
- Ejecuta el programa `EventsFeederImporter.Multiplatform.ConfigAssistant` desde la línea de comandos o mediante doble clic.
- Responde **Y** a la pregunta **Do you want to change the configuration settings? [Yes/No]**
- Completa el asistente de configuración.
- Inicia Panda Importer:
  - Si Panda Importer se ejecutaba en modo linea de comandos haz doble clic en `EventsFeederImporter.Multiplatform.Host` o ejecútalo desde la línea de comandos.
  - Si Panda Importer se ejecutaba en modo demonio ejecuta en una linea de comandos `sudo service siemfeeder start`

Editar manualmente la configuración de Panda Importer

El fichero `configuration.json` se encuentra en la misma carpeta donde reside Panda Importer y contiene sus parámetros de ejecución.

La primera vez que se ejecuta, el programa pedirá cierta información de autenticación que posteriormente volcará en el fichero de configuración. Una vez completado el proceso de instalación y ejecución, podrás modificar el fichero de configuración para afinar algunos de sus parámetros.

Siempre que se modifica el fichero `configuration.json` *es necesario parar y arrancar el proceso Panda Importer para que tenga en cuenta los cambios aplicados al fichero. Consulta "***Ejecutar y parar***".*

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

Parámetros relacionados con los logs que contienen eventos

Los parámetros que determinan el comportamiento de Panda Importer para generar los ficheros log que contienen los eventos registrados por Panda SIEMFeeder 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).

Parámetros relacionados con el registro de ejecución

Todas las operaciones ejecutadas por Panda Importer se registran en ficheros de tipo 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 53

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 mantendrá 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 7

Apéndice I: Solución de problemas

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

Síntoma/Error	Causa	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 SIEMFeeder. Comprueba que la cuenta de correo de acceso a la consola de administración de Panda Adaptive Defense está correctamente introducida en Panda Importer.

Tabla 7.1: Causas probables de fallo y solución

Síntoma/Error	Causa	Solución
unrecognized_client_secret **unsupported_grant_type** **invalid_grant**	La contraseña del cliente no se reconoce.	Comprueba que la cuenta de Aether utilizada para acceder al servicio Panda SIEMFeeder tiene asignado el rol Control total. 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 Security.
temporarily_unavailable **server_error**	Por problemas técnicos el servicio SIEMFeeder esta 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.

Tabla 7.1: Causas probables de fallo y solución

Capítulo 8

Apéndice II: Arquitectura de seguridad

En este capítulo se 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 la solución.

CONTENIDO DEL CAPÍTULO

Esquema general de seguridad AAA

Actores en la arquitectura de seguridad

En la figura 8.1 se muestran los elementos encargados de autenticar al cliente y concederle acceso a los recursos necesarios en la plataforma para descargar los logs con la información del parque IT de la organización.

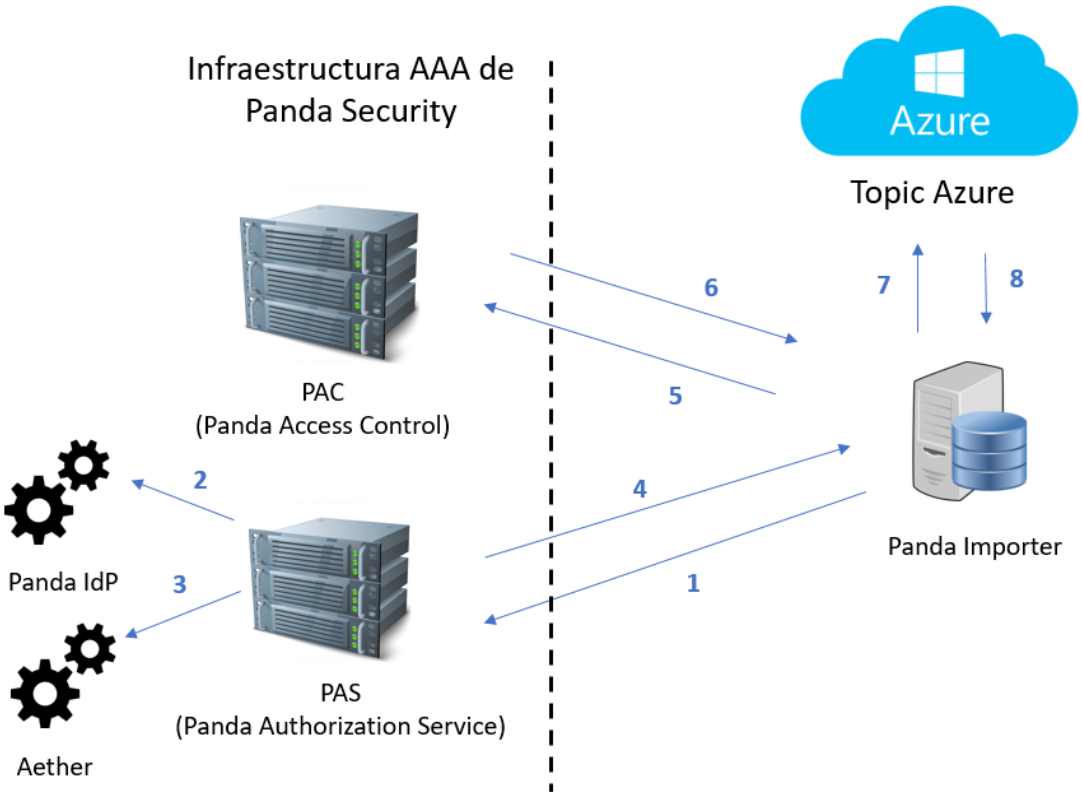

Figura 8.1: Arquitectura general de seguridad AAA

- **Panda Importer**: programa suministrado por Panda Security 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 Security 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.
- **PAC (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.

- **Aether**: 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 será posible acceder a la información publicada en el topic de Azure.

A continuación, se muestra el flujo de mensajes que se intercambian en la primera ejecución de Panda Importer, numerados según la figura 8.1. Este flujo de mensajes es necesario cada vez que el usuario deje de existir en el sistema o deje de tener el rol Control Total asignado en Aether.

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

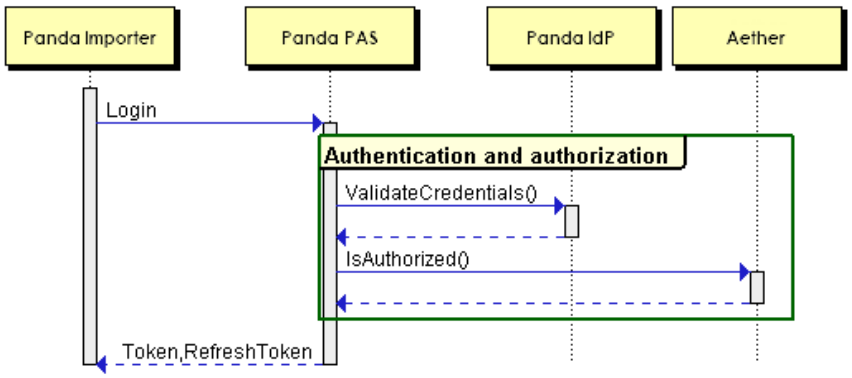

Figura 8.2: Pasos 1 a 4 del flujo de mensajes inicial

4. El servicio PAS genera y entrega un token de acceso y un token de refresco a Panda Importer.
5. **Panda Importer** envía el token de refresco al servicio PAC.
6. **Fase de Acceso**: el servicio PAC genera una SaS key (Shared Access Signature Key).
7. **Acceso al topic**: Panda Importer accede al topic asignado mediante la SaS key.
8. **Panda Importer** recibe los logs del topic suscrito.

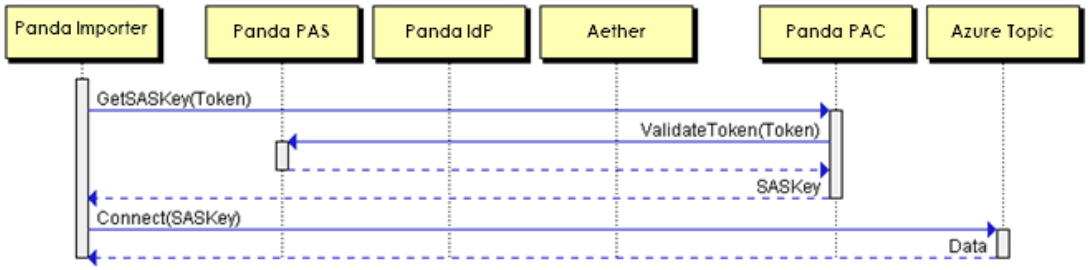

Figura 8.3: Pasos 5 a 8 del flujo de mensajes inicial

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 PAS 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 PAC una nueva SaS key.
3. Con la nueva SaS key, Panda Importer se conecta al topic Azure y continúa recogiendo los logs.

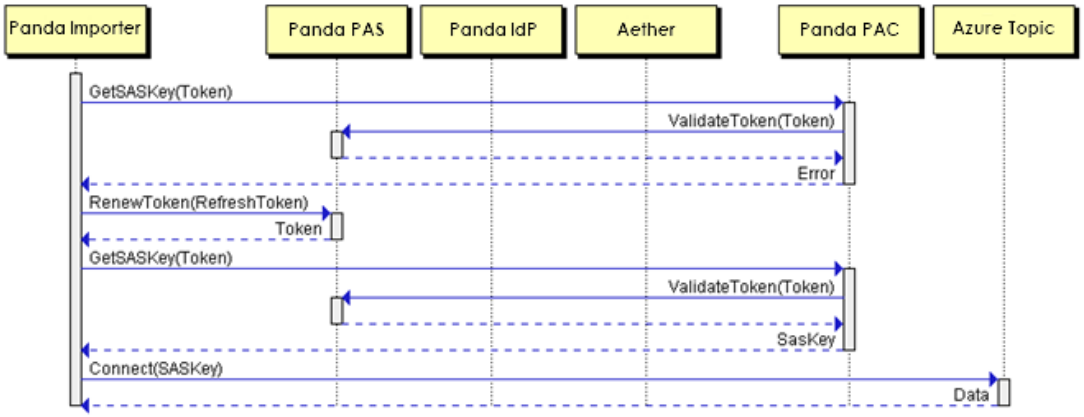

Figura 8.4: Flujo de mensajes cuando caduca el token de refresco

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 PAS**: 14 días
- **Token de acceso del PAS**: 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.