EVIDENCIA 46 LOGS

Registros de actividades de sistemas de información, sistemas operativos y activos relacionados con el monedero electrónico

SENDERO FUEL S.A. DE C.V.

Evidencia documental de cumplimiento – Punto 46, Anexo 10 RMF 2026

1. Requisito de cumplimiento

El Punto 46 del Anexo 10 de la Resolución Miscelánea Fiscal 2026 requiere documentación que permita identificar los registros de actividades de los sistemas de información, sistemas operativos y cualquier otro activo relacionado con el monedero electrónico. Los registros deben contener, como mínimo:

- a) Identificador del usuario que realiza la actividad.
- b) Descripción de la actividad realizada.
- c) Origen de la conexión al sistema.
- d) Resultado de la actividad efectuada.
- e) Todos los registros deben ser generados como solo lectura para todos los usuarios.
- f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada.

Nota especial sobre cuentas privilegiadas
El propio requisito exige registros de actividades independientes para administradores y cuentas privilegiadas. Dichos registros deben conservarse como solo lectura y no deben ser accesibles por los propios administradores o cuentas privilegiadas cuya actividad se registra.

2. Objetivo

Demostrar que SENDERO FUEL registra y conserva trazabilidad suficiente sobre actividades relevantes ejecutadas en la aplicación del monedero, servidores, bases de datos, equipos de red, almacenamiento y demás infraestructura relacionada, mediante un esquema de centralización en Wazuh (SIEM) y registros transaccionales propios de las aplicaciones y plataformas.

3. Alcance

El alcance incluye los activos tecnológicos vinculados con el monedero electrónico de combustibles en el centro de datos principal NGX, el centro de datos secundario ASSETEL y la infraestructura operativa de oficina que genera eventos relevantes. Se consideran registros de aplicación, sistema operativo, base de datos, equipos de red, firewalls, hosts de virtualización, almacenamiento y repositorios de respaldo.

4. Arquitectura de registro y centralización

Wazuh como repositorio central/SIEM, usado para concentrar registros de servidores mediante agentes y eventos de dispositivos que no admiten agente mediante Syslog. El servidor de referencia es SRV-WAZUH, identificado con la dirección 10.255.248.15.

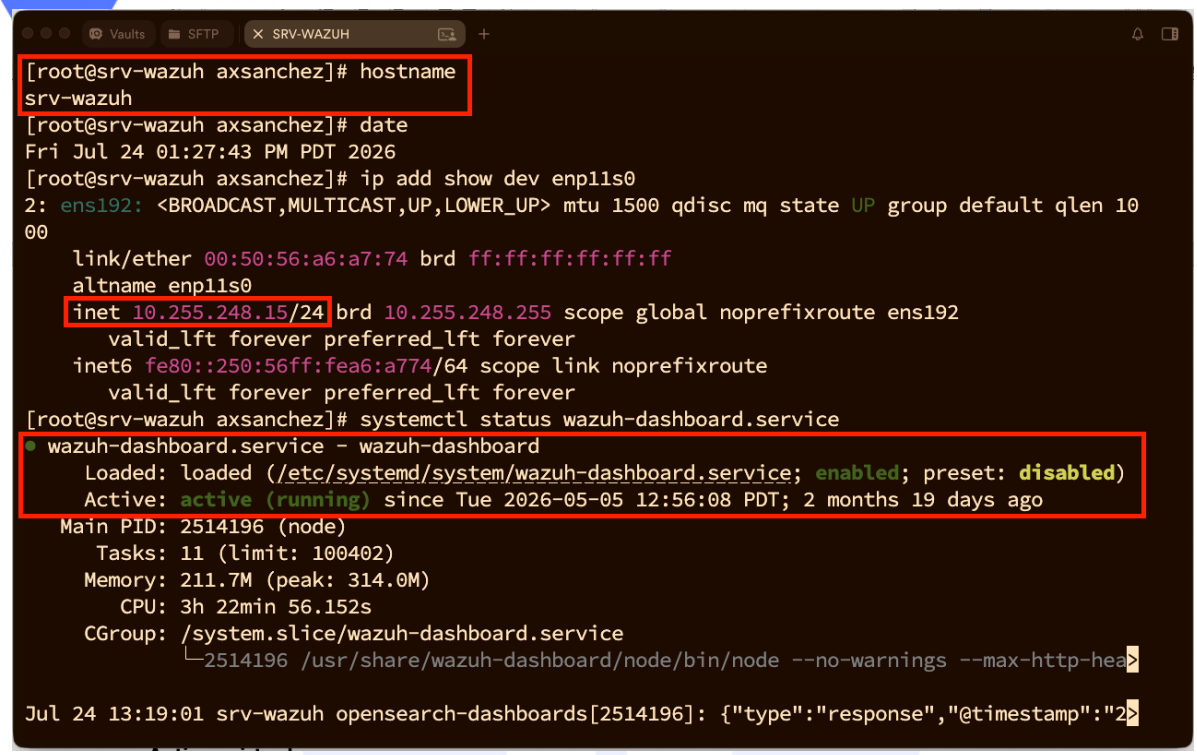


Figura 1. SRV-WAZUH: identificación del servidor y evidencia del servicio wazuh-dashboard.service en ejecución.

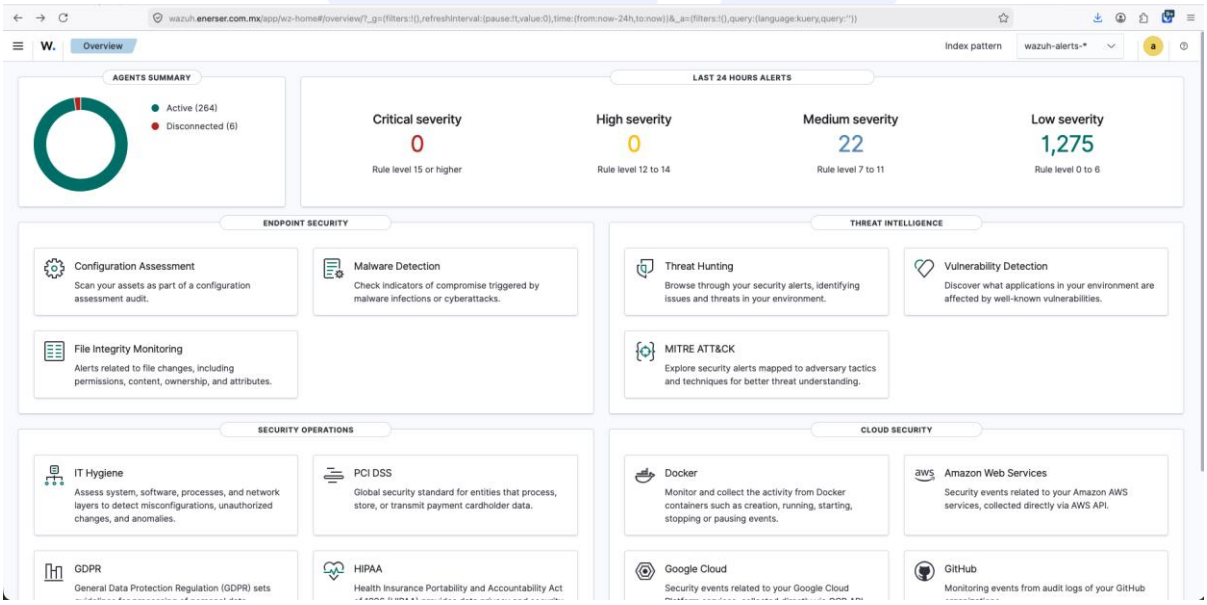


Figura 2. Dashboard web de Wazuh utilizado para la administración y consulta centralizada de eventos.

5. Inventario base y activos sujetos a registro

Nombre	Descripción	Dirección IP	Tipo de registro / fuente
SRV-ENERGO-AD	Directorio Activo	172.16.52.2	Wazuh agent
SRV-MON-APP-DV	Aplicaion de Monedero Desarrollo	172.16.50.10	Wazuh agent
SRV-MON-APP-PR	Aplicaion de monedero produccion	172.16.52.10	Wazuh agent
SRV-MON-APP-QA	Aplicación de monedero pruebas	172.16.51.10	Wazuh agent
SRV-MON-DB-DV	Base de datos de monedero desarrollo	172.16.50.11	Wazuh agent
SRV-MON-DB-PR	Base de datos de monedero produccion	172.16.52.11	Wazuh agent
SRV-MON-DB-QA	Base de datos de monedero pruebas	172.16.51.11	Wazuh agent
SRV-MON-SER-DV	Servicios de backend desallo	172.16.50.12	Wazuh agent
SRV-MON-SER-PR	Servicios de backend produccion	172.16.52.12	Wazuh agent
SRV-MON-SER-QA	Servicios de backend pruebas	172.16.51.12	Wazuh agent
SRV-NTP	Servidor de tiempo	10.255.248.40	Wazuh agent
SRV-GLPI	Servidor de Tickets	10.255.248.326	Wazuh agent
SW-HP-NGX-01	Switch Core, interconecta todos los dispositivos del centro de datos	10.20.1.2	Syslog / registro de plataforma
FW-FTNET-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	10.20.1.1	Syslog / registro de plataforma
SW-HP-ASSTEL-01	Switch Core, interconecta todos los dispositivos del centro de datos	10.30.1.2	Syslog / registro de plataforma
FW-ASSETEL-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	10.30.1.1	Syslog / registro de plataforma
SW-ARUBA-2930	Switch Core, interconecta todos los dispositivos del centro de datos	10.100.0.14	Syslog / registro de plataforma
FW-FG200f-03	Firewall perimetral,	10.100.0.1	Syslog / registro de plataforma
HST-PRLN-01	Host de virtualizacion VMWare	10.20.1.4	Syslog / registro de plataforma
HST-PRLN-02	Host de virtualizacion VMWare	10.20.1.5	Syslog / registro de plataforma
HST-PRLN-03	Host de virtualizacion VMWare	10.20.1.6	Syslog / registro de plataforma
STR-MSA-01	Dispositivo de Almacenamiento de para las VM de VMWare	10.20.1.10	Syslog / registro de plataforma
VLT-SONCE-01	Almacenameinto inmutable de respaldos	10.20.1.30	Syslog / registro de plataforma
HST-PRLN-04	Host de virtualizacion VMWare	10.30.1.13	Syslog / registro de plataforma
HST-PRLN-05	Host de virtualizacion VMWare	10.30.1.14	Syslog / registro de plataforma
HST-PRLN-06	Host de virtualizacion VMWare	10.30.1.15	Syslog / registro de plataforma
STR-MSA-02	Dispositivo de Almacenamiento para las VM de VMWare	10.30.1.18	Syslog / registro de plataforma
VLT-SONCE-02	Almacenameinto inmutable de respaldos	10.30.1.9	Syslog / registro de plataforma

SRV-NAS-APP	Almancenamiento de red.	10.100.30.9	Syslog / registro de plataforma

Nota: la columna “Tipo de registro / fuente” se utiliza como clasificación operativa para ordenar el expediente. La existencia efectiva de la configuración se acredita en las capturas posteriores.

6.1 Activos en espera (stand-by) en ASSETEL

Los activos identificados con sufijo “-ASS” permanecen apagados y son sobrescritos mediante réplicas; por ello, no generan registros mientras se encuentran inactivos. Al activarse como parte del plan de recuperación, deberán comenzar a generar y remitir registros al SIEM.

Activo	Descripción	IP indicada en fuente
SRV-ENERGO-AD-ASS	Directorio Activo	172.16.52.2
SRV-MON-APP-DV-ASS	Aplicaion de Monedero Desarrollo	172.16.50.10
SRV-MON-APP-PR-ASS	Aplicaion de monedero produccion	172.16.52.10
SRV-MON-APP-QA-ASS	Aplicación de monedero pruebas	172.16.51.10
SRV-MON-DB-DV-ASS	Base de datos de monedero desarrollo	172.16.50.11
SRV-MON-DB-PR-ASS	Base de datos de monedero produccion	172.16.52.11
SRV-MON-DB-QA-ASS	Base de datos de monedero pruebas	172.16.51.11
SRV-MON-SER-DV-ASS	Servicios de backend desallo	172.16.50.12
SRV-MON-SER-PR-ASS	Servicios de backend produccion	172.16.52.12
SRV-MON-SER-QA-ASS	Servicios de backend pruebas	172.16.51.12

6. Evidencia de cobertura de servidores y endpoints

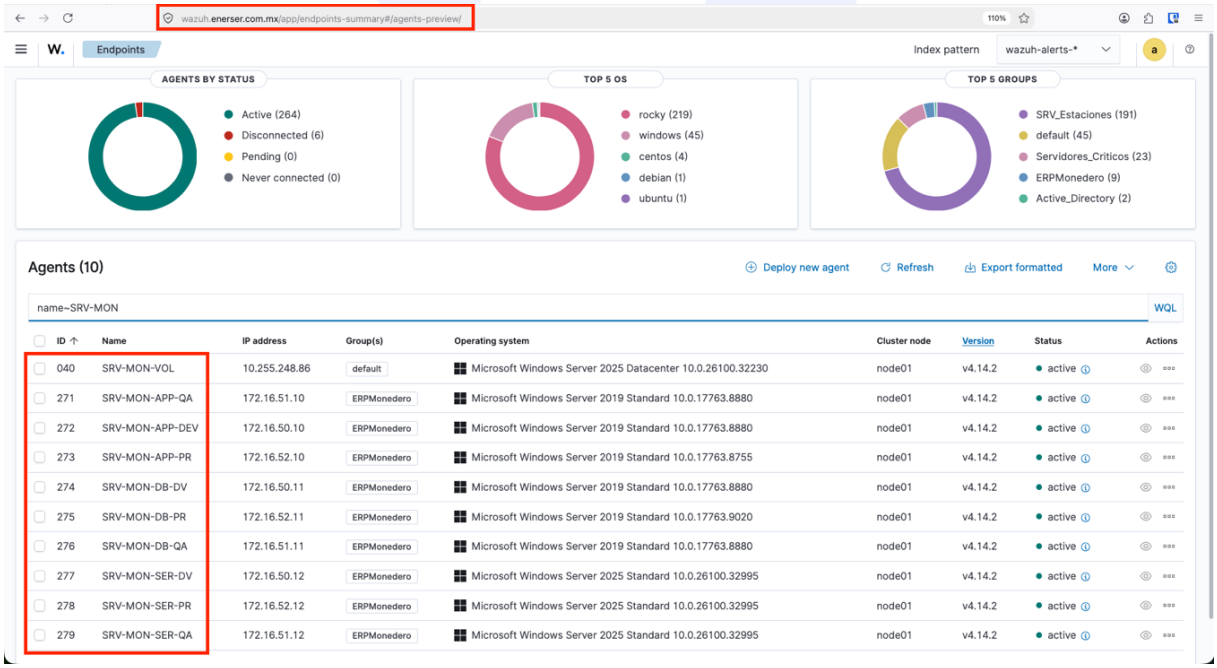


Figura 3. Lista de endpoints en Wazuh filtrada por servidores del monedero (“SRV-MON”), con IP y estado del agente.

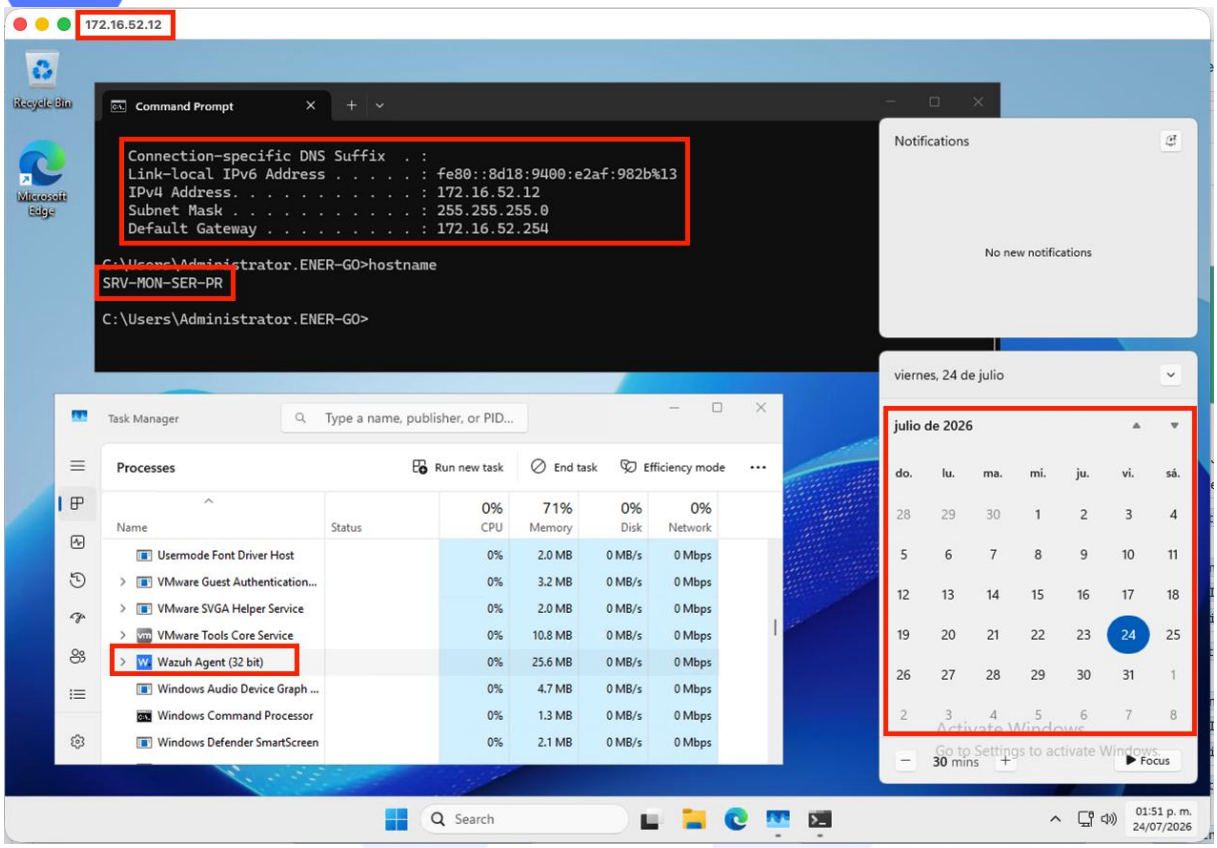
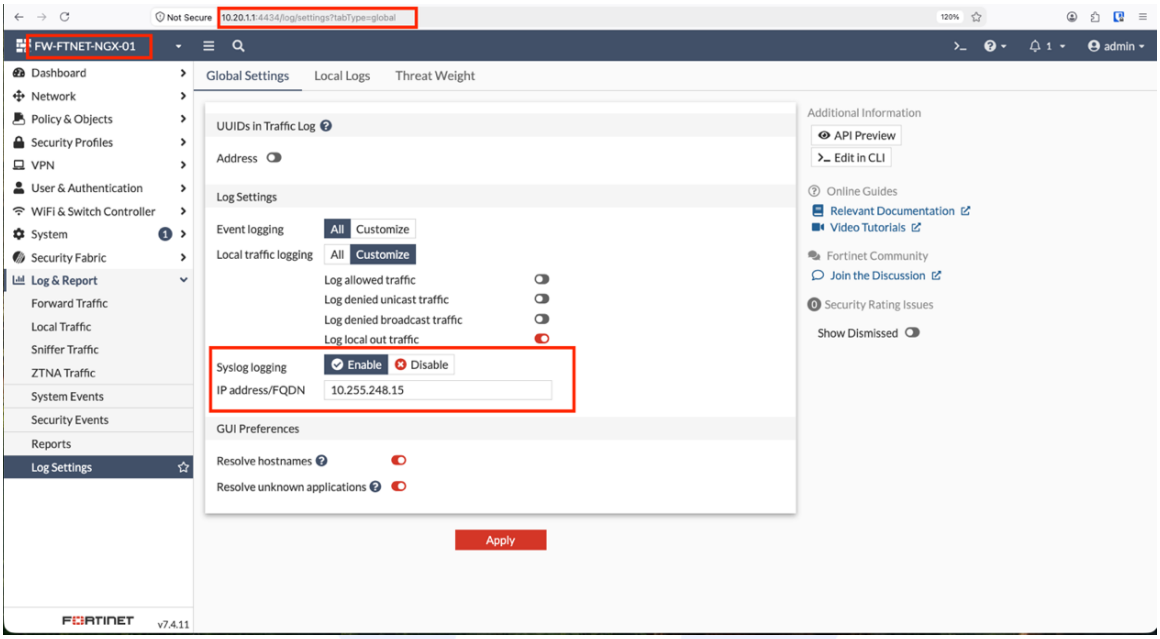


Figura 4. Servidor SRV-MON-SER-PR mostrando el agente de Wazuh en ejecución.

7. Evidencia de envío de logs por equipos de red, seguridad y almacenamiento

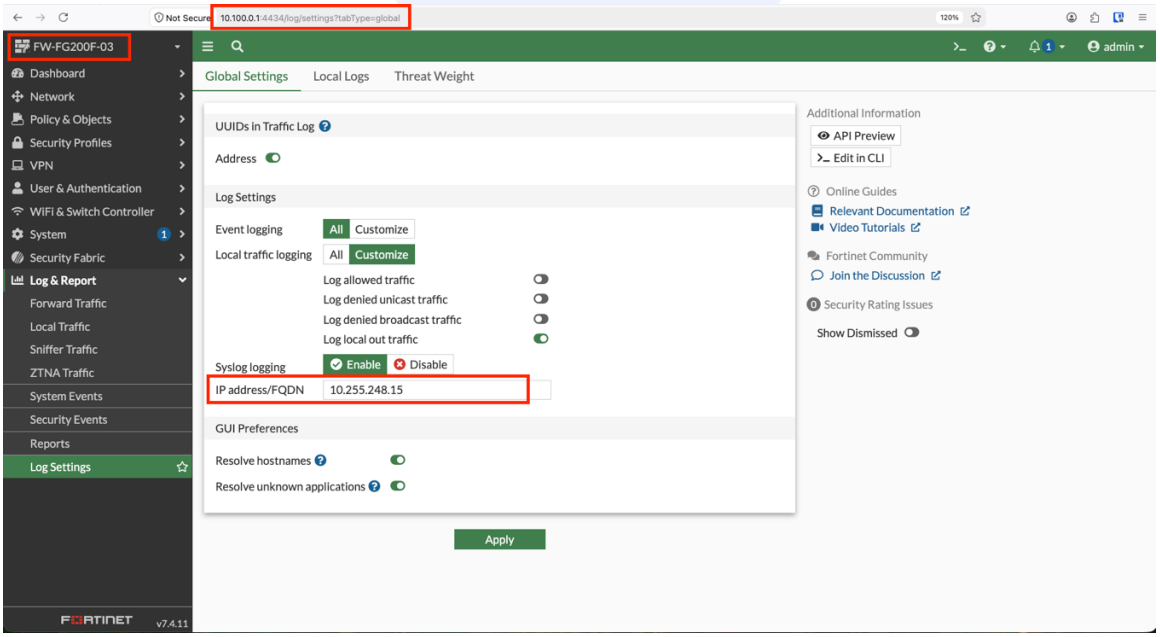
Para activos que no utilizan agente, la evidencia fuente muestra configuración de envío Syslog hacia el servidor SRV-WAZUH.

7.1 Firewall NGX – FW-FTNET-NGX-01



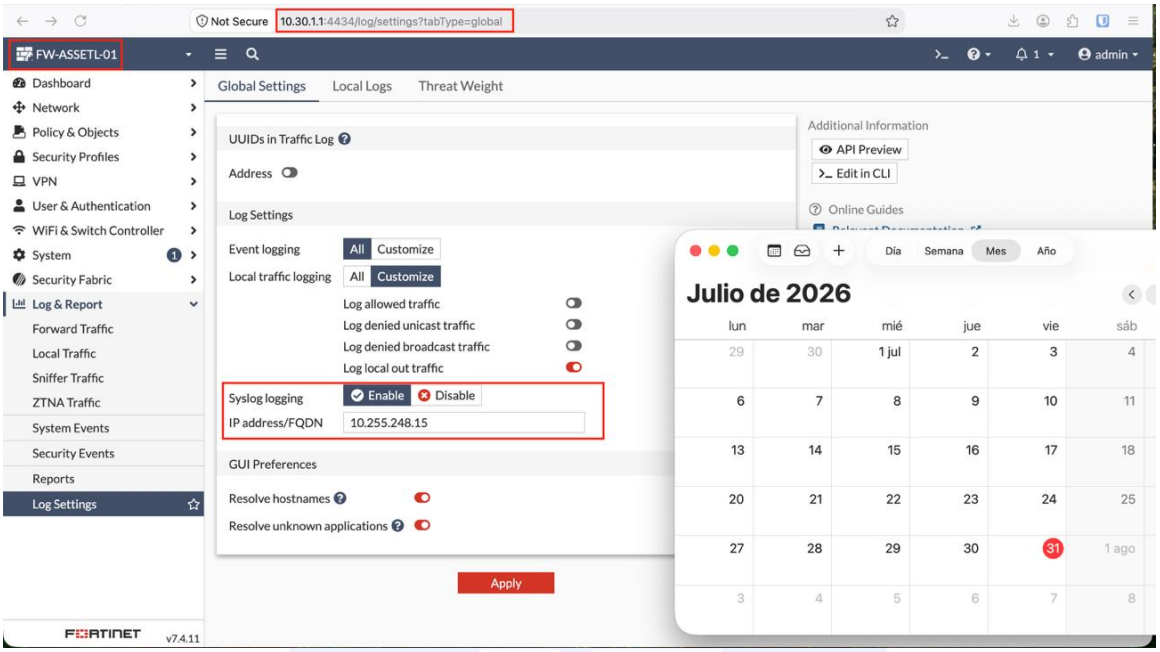
Configuración Syslog del firewall del centro de datos NGX hacia SRV-WAZUH.

7.2 Firewall de oficina – FW-FG200F-03



Configuración Syslog del firewall de oficina hacia SRV-WAZUH.

7.3 Firewall ASSETEL – FW-ASSETEL-NGX-01



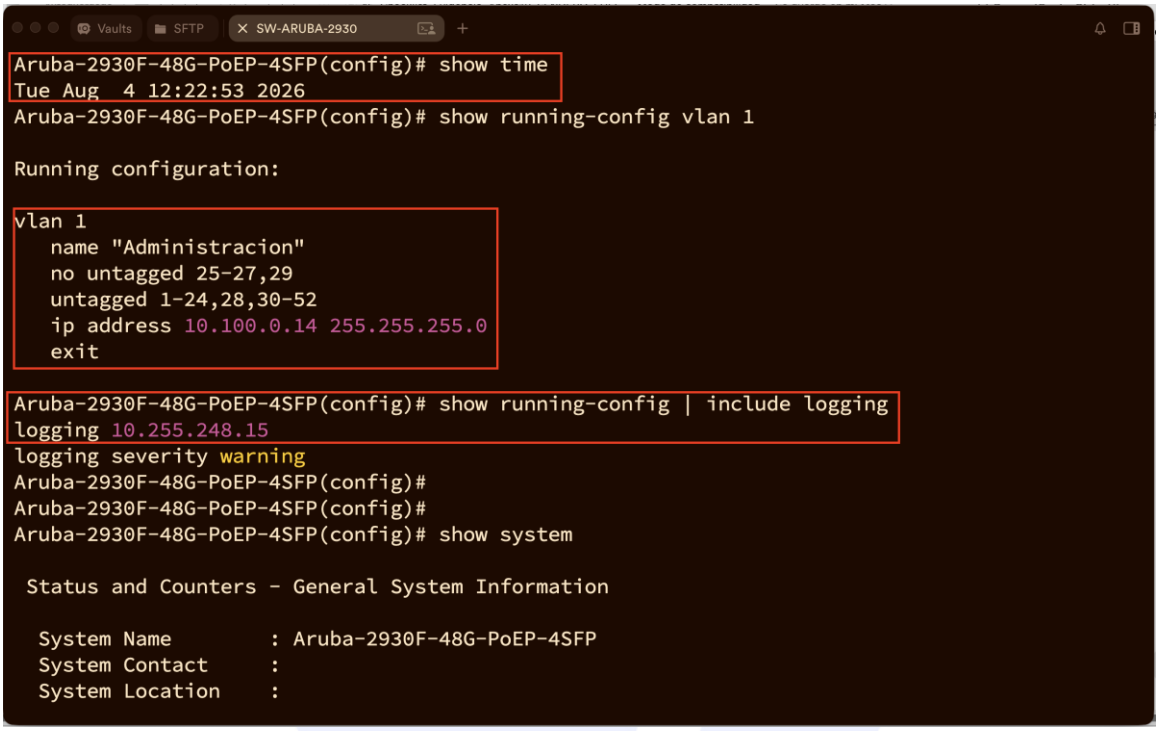
Configuración Syslog del firewall del centro de datos ASSETEL hacia SRV-WAZUH.

7.4 Switch NGX – SW-HP-NGX-01

```
[HPE]display clock
13:16:22 MST Fri 07/31/2026
Time Zone : MST minus 07:00:00
[HPE]display ip interface brief
*down: administratively down
(s): spoofing
Interface                   Physical Protocol IP Address      Description
M-GE0/0/0                   down     down     unassigned      M-Gigabit...
Vlan1                       up       up       10.20.1.2       Vlan-inte...
Vlan11                      up       up       10.255.248.254  Vlan-inte...
Vlan21                      up       up       10.20.10.254    Vlan-inte...
Vlan50                      up       up       172.16.50.254   Vlan-inte...
Vlan51                      up       up       172.16.51.254   Vlan-inte...
Vlan52                      up       up       172.16.52.254   Vlan-inte...
[HPE]display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    10.255.248.15,
    port number: 514, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512
    Current messages 512, dropped messages 0, overwritten messages 1616
Log file: Enabled
```

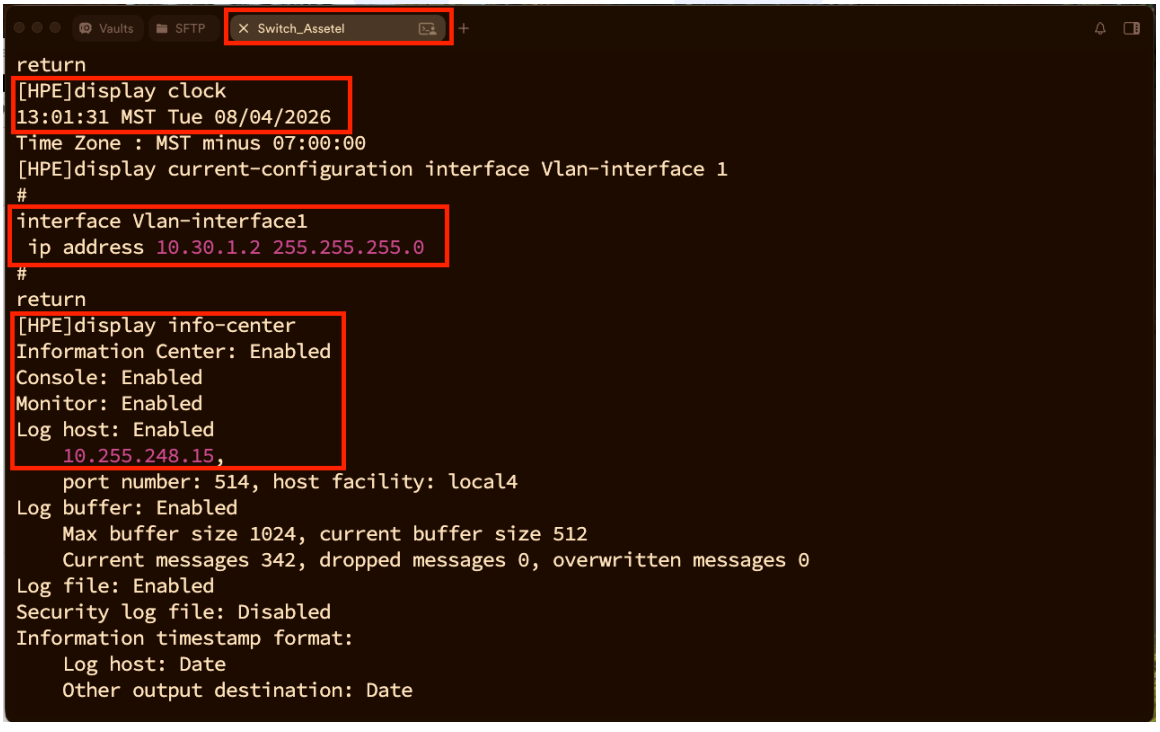
Configuración de log host/Syslog del switch NGX.

7.5 Switch de oficina – SW-ARUBA-2930



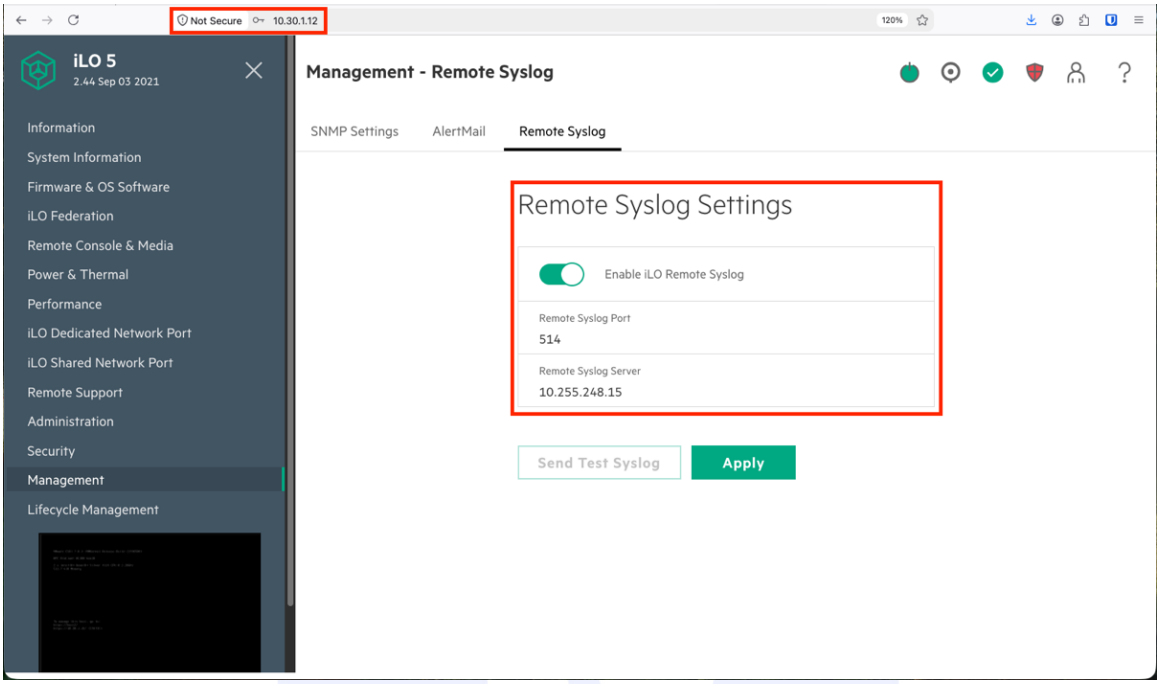
Configuración de logging/Syslog del switch Aruba de oficina.

7.6 Switch ASSETEL – SW-HP-ASSTEL-01



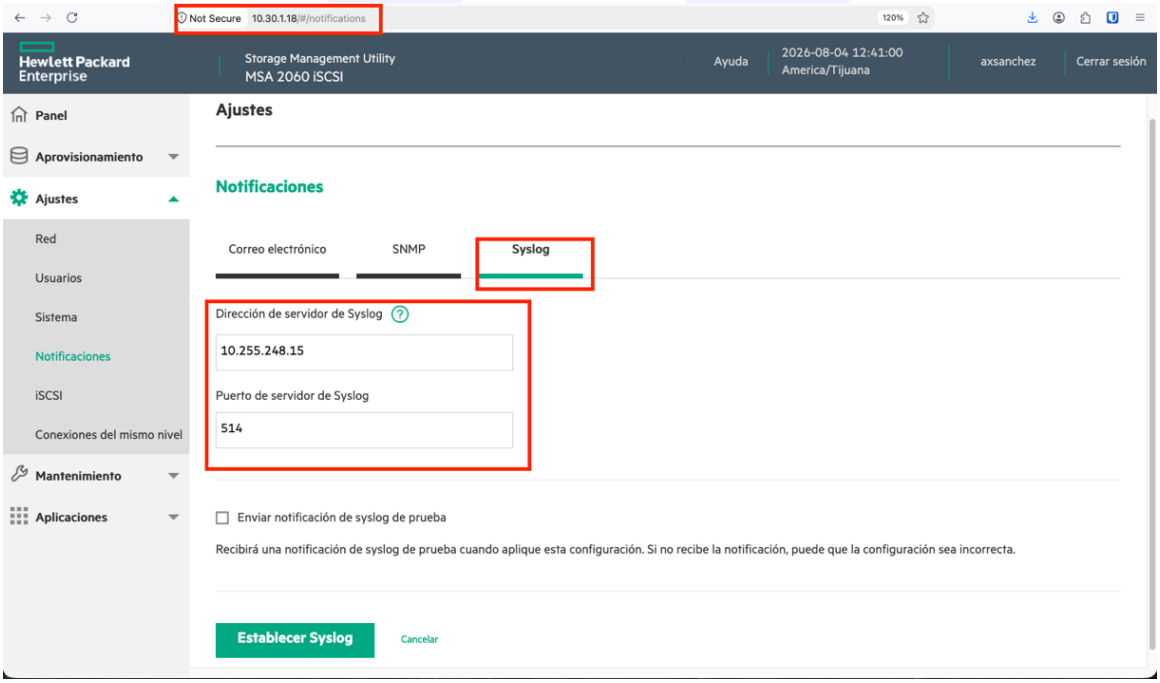
Configuración de logging/Syslog del switch del centro de datos ASSETEL.

7.7 Host de virtualización ASSETEL – HST-PRLN-04



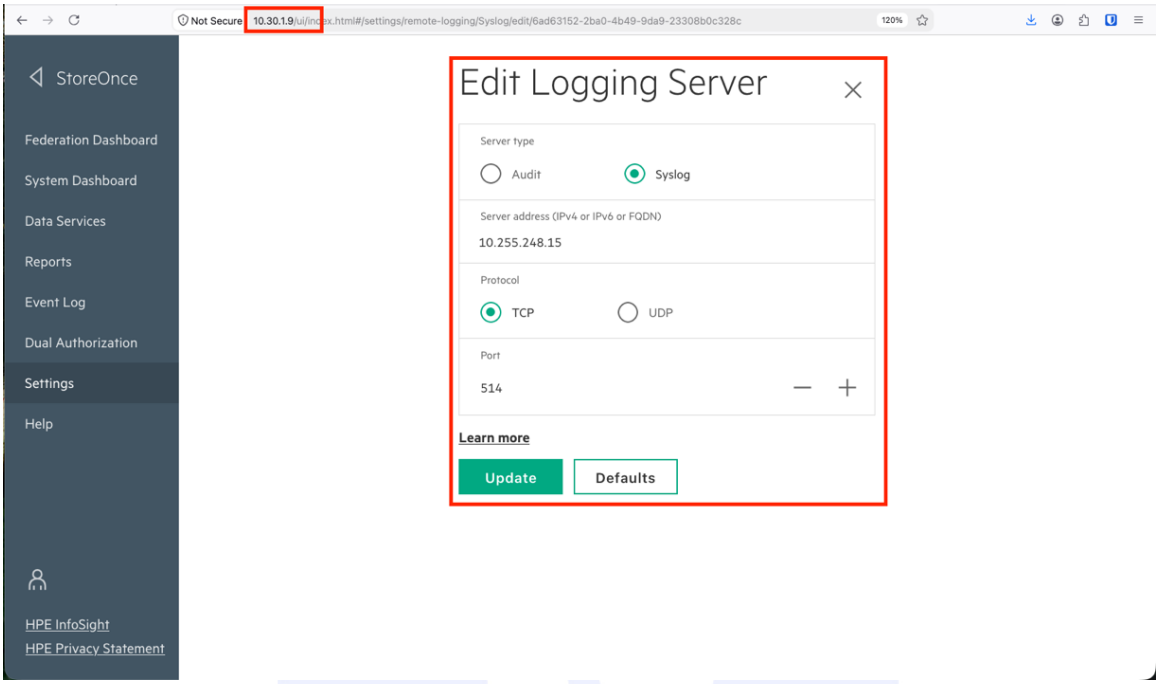
HPE iLO Remote Syslog habilitado.

7.8 Almacenamiento ASSETEL – STR-MSA-02



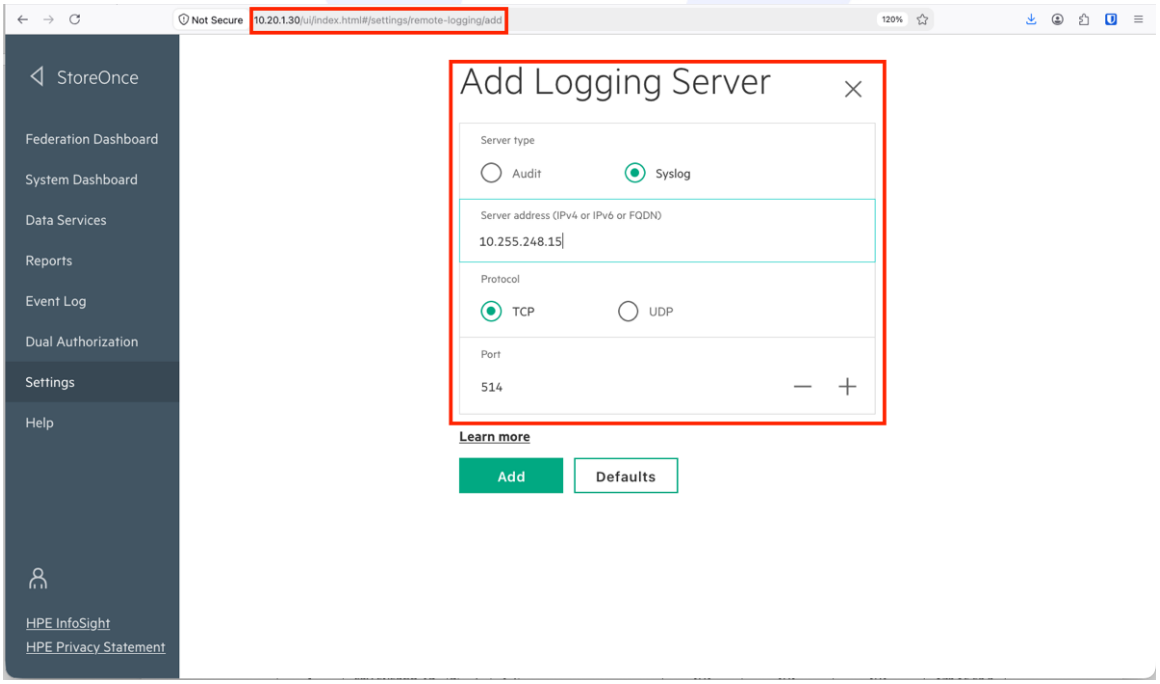
Configuración de Syslog en HPE MSA.

7.9 StoreOnce ASSETEL – VLT-SONCE-02



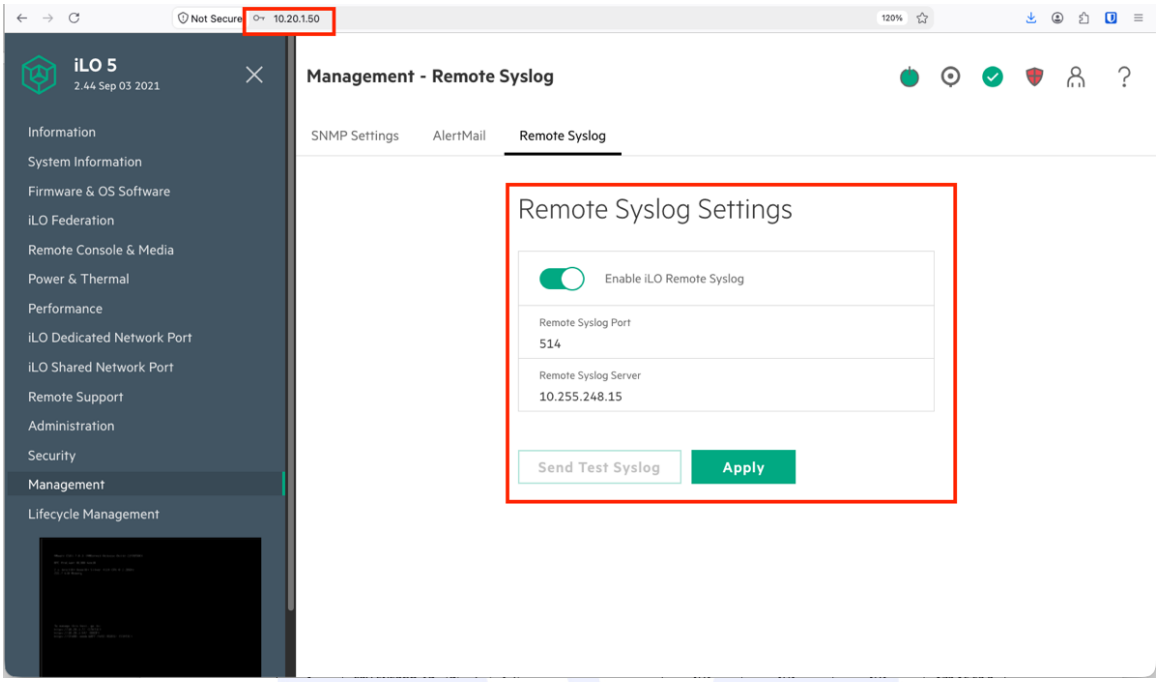
Servidor de logging configurado en HPE StoreOnce.

7.10 StoreOnce NGX – VLT-SONCE-01



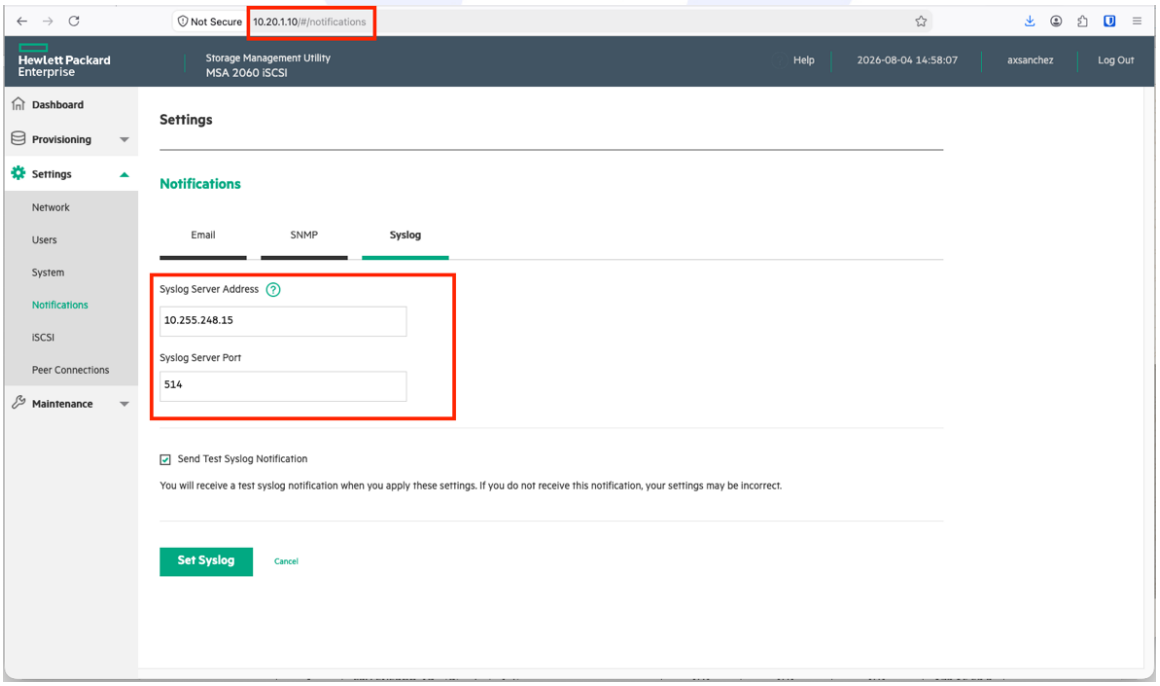
Servidor de logging configurado en HPE StoreOnce.

7.11 Host de virtualización NGX – HST-PRLN-01



HPE iLO Remote Syslog habilitado.

7.12 Almacenamiento NGX – STR-MSA-01



Configuración de Syslog en HPE MSA.

8. Evidencia de logs transaccionales

8.1 Software / bitácora funcional

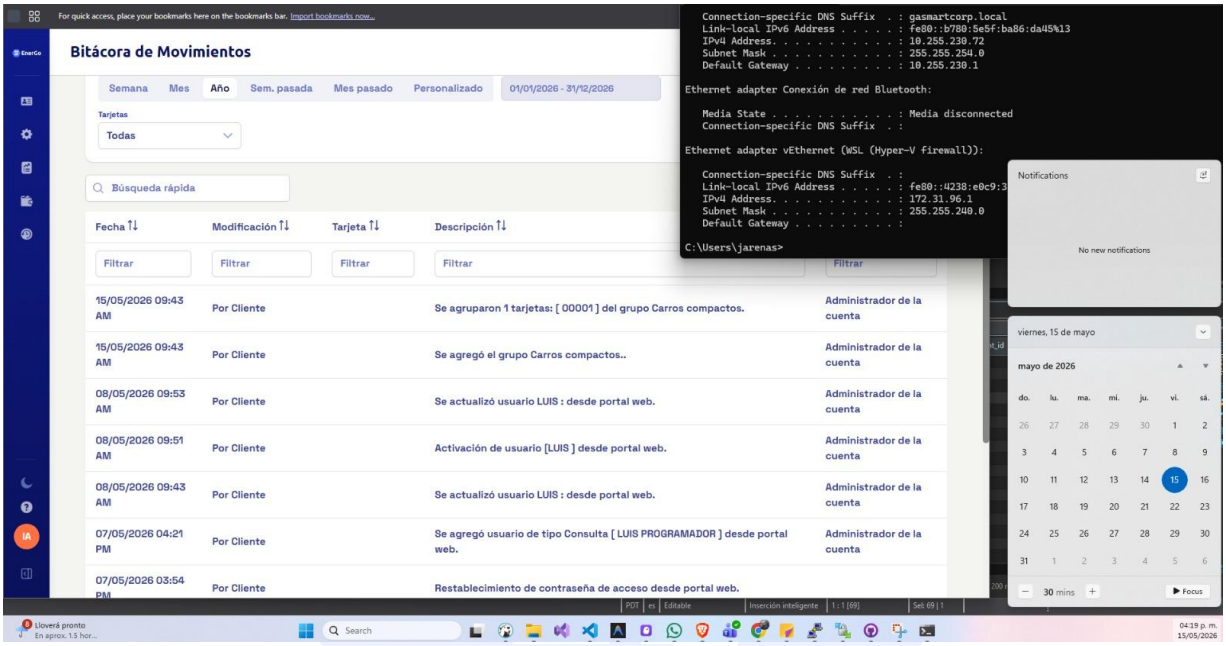


Figura 17. Bitácora de movimientos de la aplicación: ejemplo de registro funcional de operaciones realizadas por usuarios.

8.2 Servidor / bitácora de aplicación

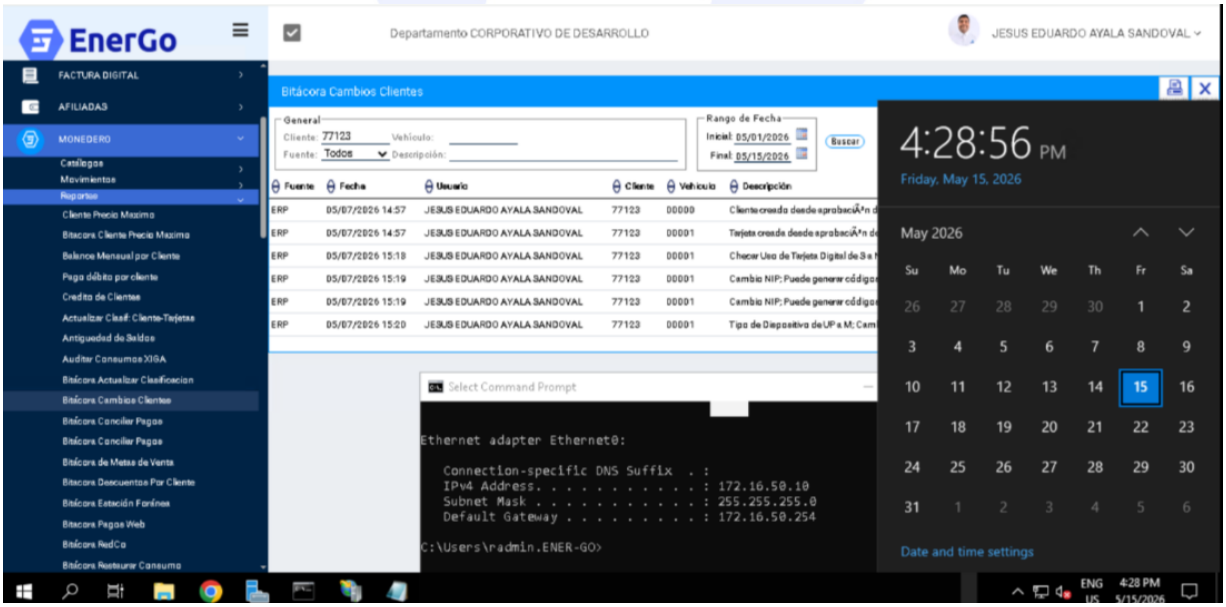


Figura 18. Vista de bitácora en servidor de aplicación con contexto del equipo y fecha/hora.

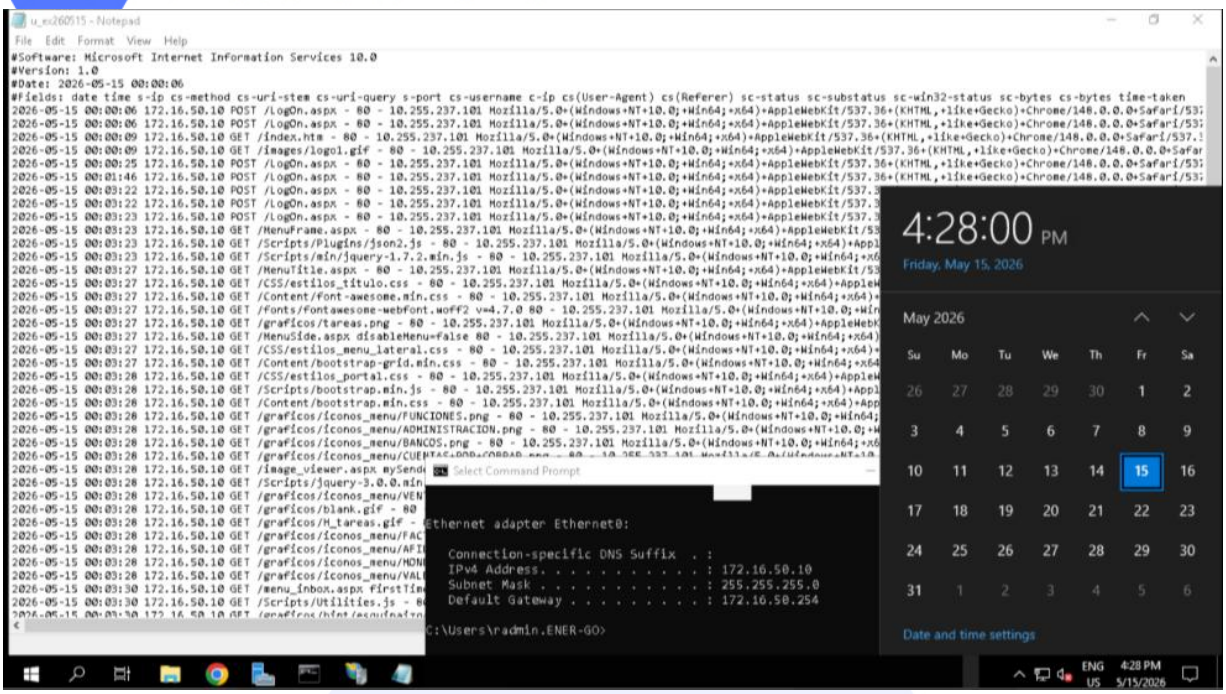


Figura 19. Registro técnico del servidor con eventos de aplicación/servicio y contexto temporal.

8.3 Base de datos

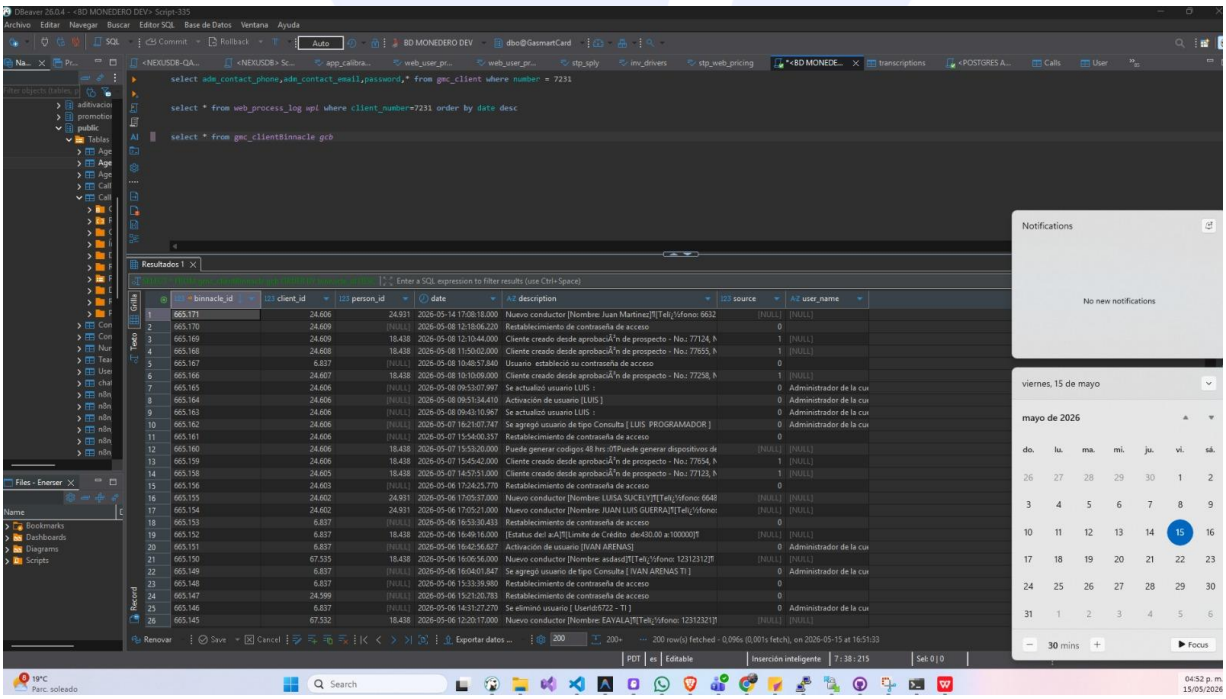


Figura 20. Consulta de registros en base de datos, utilizada como evidencia de persistencia y trazabilidad de eventos transac cionales.

9. Campos mínimos del registro y mapeo de evidencia

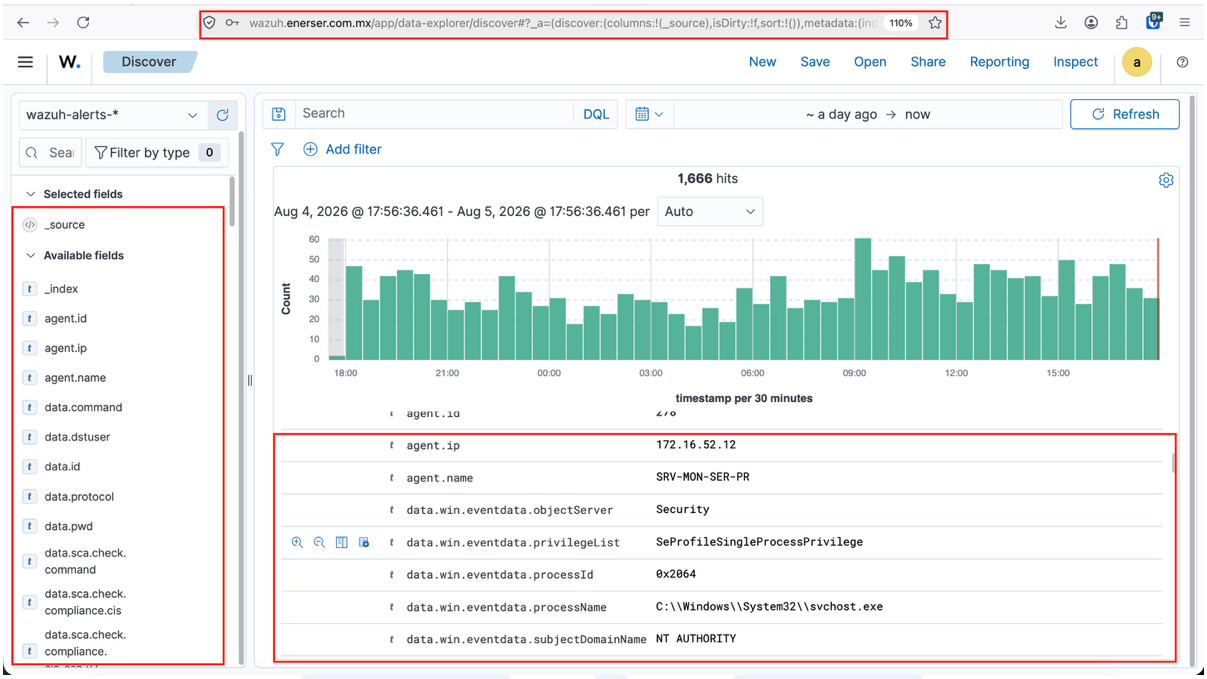


Figura 21. Wazuh Discover: ejemplo de campos disponibles por evento para identificar agente/origen, servidor, archivo, acción y demás atributos.

10. Protección, solo lectura y segregación de funciones

La evidencia proporcionada muestra controles de consulta centralizada, roles y segregación de permisos en Wazuh. Estos controles se relacionan directamente con los incisos e) y f) del Punto 46.

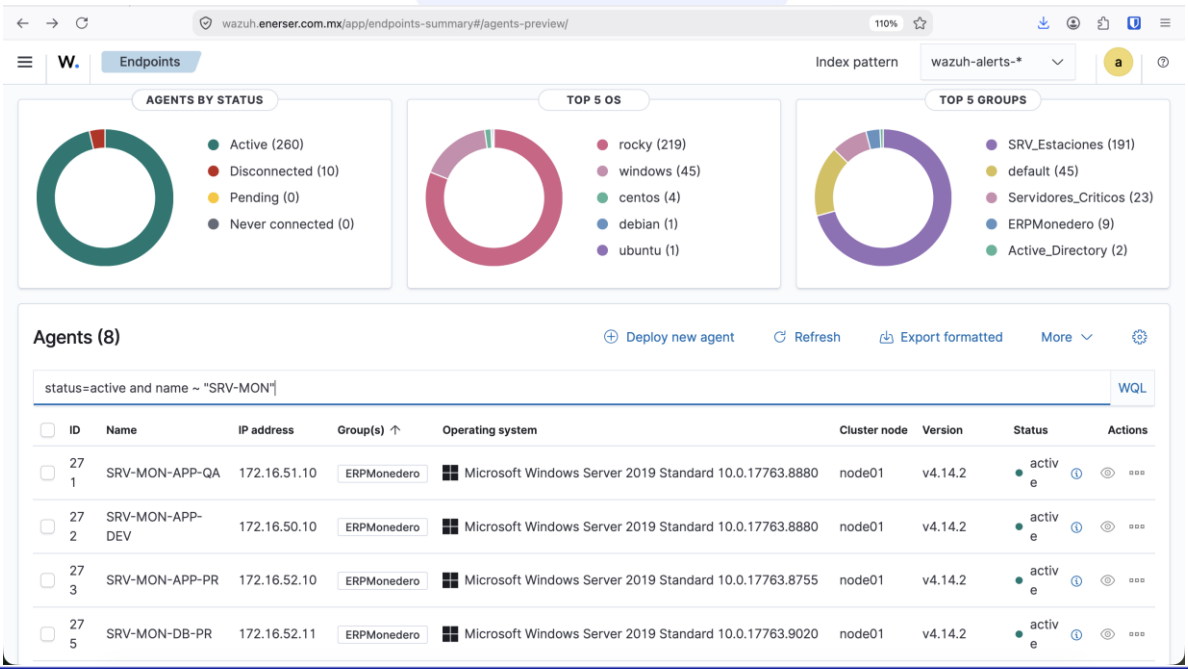


Figura 22. Repositorio central Wazuh con endpoints del monedero registrados.

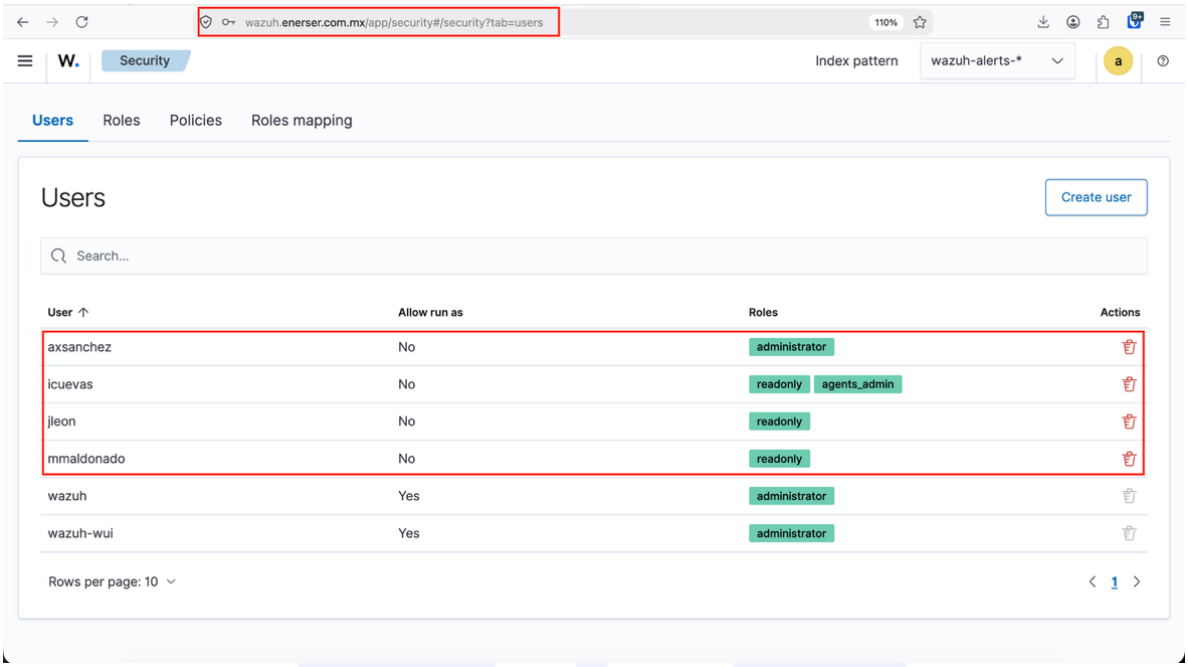


Figura 23. Usuarios analistas y configuración orientada a consulta/solo lectura.

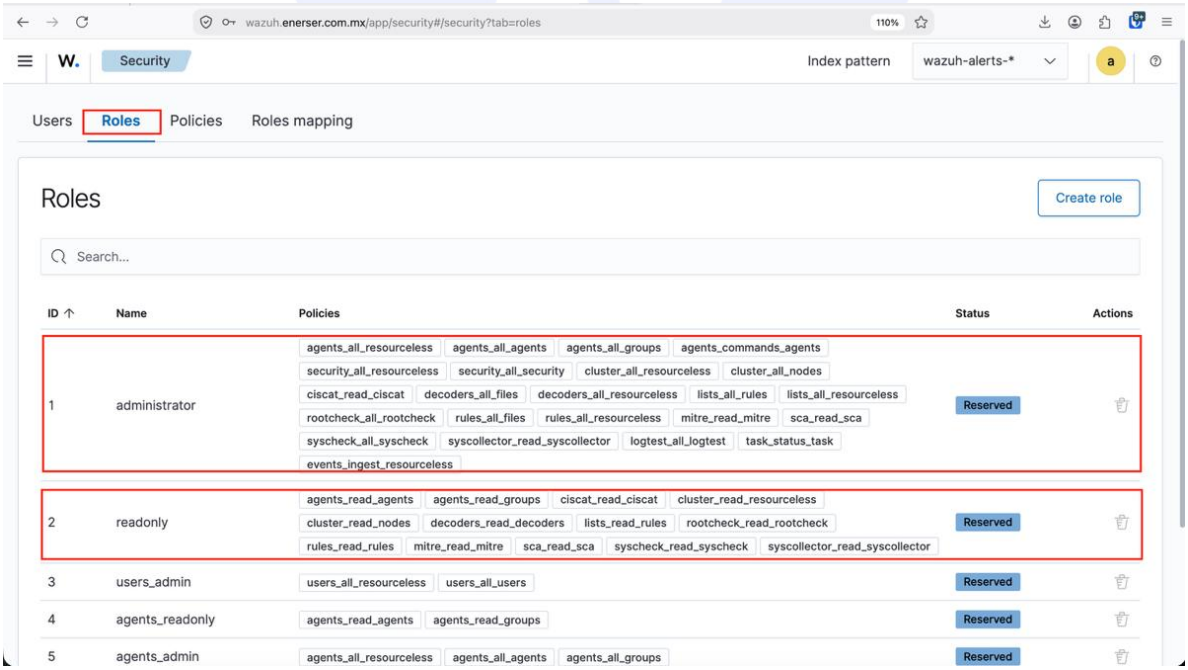


Figura 24. Roles de Wazuh para separar atribuciones administrativas y de auditoría.

10.1 Controles contra pérdida o destrucción

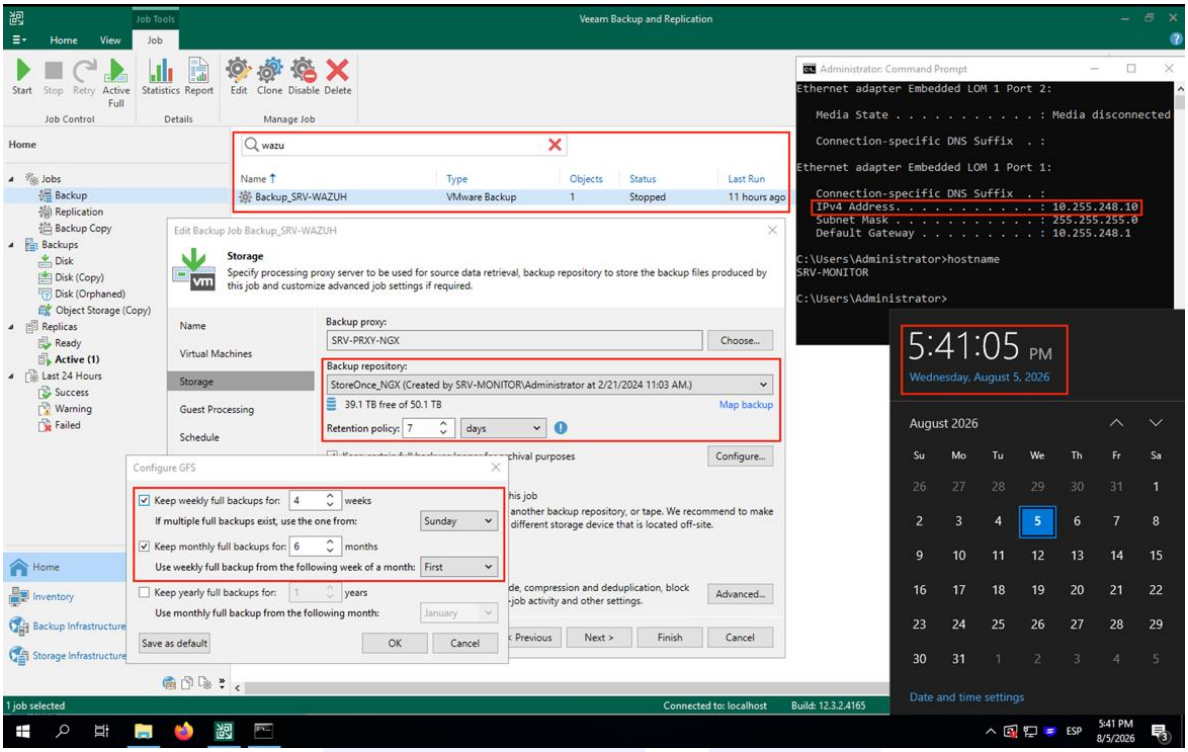


Figura 25. Configuración de respaldo del servidor SRV-WAZUH mediante Veeam, con retención e inmutabilidad según evidencia proporcionada.

10.2 Controles contra distribución no autorizada

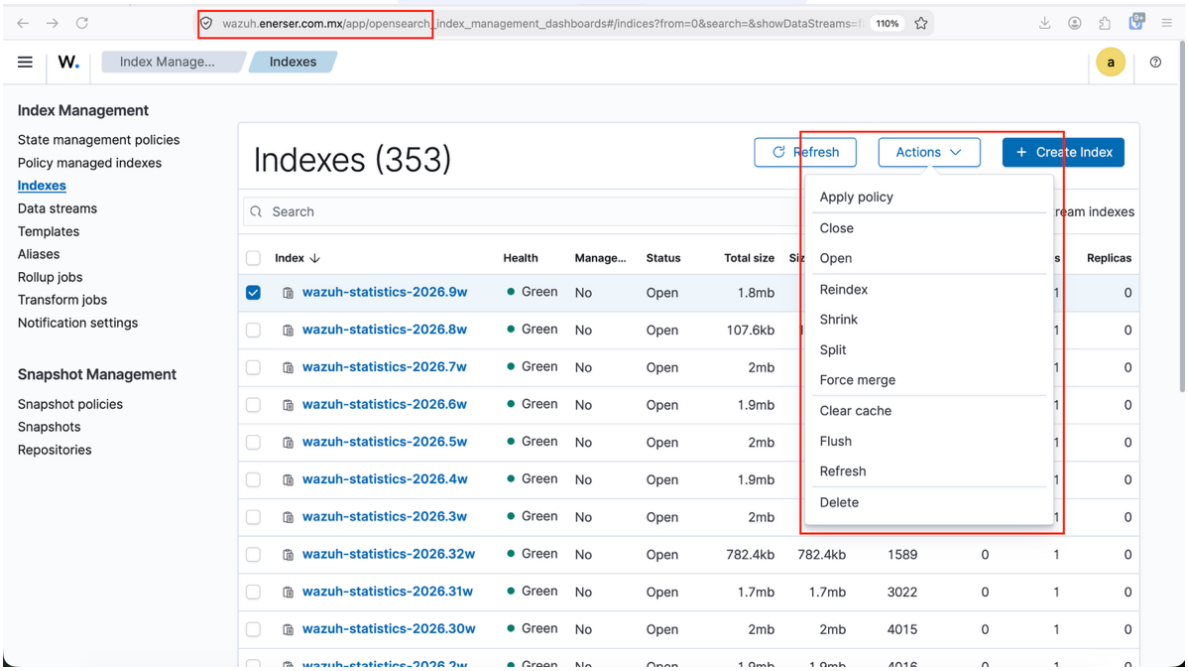


Figura 26. Gestión de índices en Wazuh/OpenSearch utilizada como evidencia del control de administración y ausencia de exportación directa desde la vista mostrada.

11. Control especial de administradores y cuentas privilegiadas

