EVIDENCIA 47 NTP

Documentación técnica del protocolo NTP y sincronización de relojes

SENDERO FUEL S.A. DE C.V.

Evidencia documental de cumplimiento – Punto 47, Anexo 10 RMF 2026

1. Requisito de cumplimiento

El Punto 47 del Anexo 10 de la Resolución Miscelánea Fiscal 2026 solicita documentación técnica del protocolo NTP o del equipo que implemente este protocolo y que sea utilizado para la sincronización de relojes de los sistemas, redes y servicios de red relacionados con las actividades del monedero electrónico.

Interpretación de SENDERO FUEL
SENDERO FUEL interpreta el requisito como la obligación de demostrar: (i) qué servidor o servicio proporciona la hora de referencia; (ii) qué tecnología/protocolo se utiliza; (iii) qué activos consumen esa referencia; (iv) que existe evidencia de sincronización efectiva; y (v) que el servicio se encuentra protegido para evitar uso o exposición no autorizada.

2. Objetivo

Integrar evidencia suficiente, trazable y técnicamente coherente para demostrar que los activos tecnológicos relacionados con el monedero electrónico mantienen relojes sincronizados mediante NTP, reduciendo discrepancias de fecha y hora que pudieran afectar registros de auditoría, transacciones, correlación de eventos, autenticación, trazabilidad y análisis forense.

3. Alcance

El alcance comprende el servidor central de tiempo SRV-NTP, la infraestructura física alojada en NGX y ASSETEL, los equipos de red de las oficinas administrativas, los servidores virtuales de producción/desarrollo/pruebas, los sistemas de almacenamiento y respaldo, y los componentes que participan en monitoreo y soporte del monedero electrónico.

4. Roles y responsabilidades

Rol	Responsabilidad en el control NTP
Gerente Sendero Fuel – Romina Monserrat Barbosa Apodaca	Supervisar la disponibilidad de recursos y aprobar el expediente de cumplimiento.
Oficial de Seguridad – Axel Martínez Rentería	Validar que la evidencia sea íntegra, consistente y suficiente; revisar excepciones y cambios.
Proveedor TI – ENERFUEL TECH, S. de R.L. de C.V.	Administrar el servicio NTP, configurar clientes, mantener disponibilidad y proporcionar evidencia técnica.
Administradores de infraestructura	Aplicar la configuración de sincronización, monitorear desviaciones y atender incidentes.
Custodio de evidencia	Integrar capturas, registros, inventarios y evidencias de prueba en el expediente correspondiente.

5. Arquitectura de sincronización de tiempo

. En el servidor se utiliza Chrony/chronyd como implementación del protocolo NTP.

Elemento	Identificación	Función	Evidencia esperada
Servidor NTP	SRV-NTP / 10.255.248.40	Fuente de tiempo interna	Servicio chronyd activo, fecha/hora, hostname e IP
Publicación externa	201.174.13.155	Acceso controlado para sedes/segmentos autorizados	NAT/UDP 123 y lista blanca
Fuentes upstream	pool.ntp.org	Referencia externa para SRV-NTP	Archivo chrony.conf y estado de sincronización
Clientes internos	Servidores, red y almacenamiento	Sincronizar reloj contra SRV-NTP	Configuración de cliente + estado Running/Synchronized
Monitoreo/validación	chronyc / w32tm / consola de dispositivo	Confirmar fuente, offset y estado	Captura de tracking/status/sources

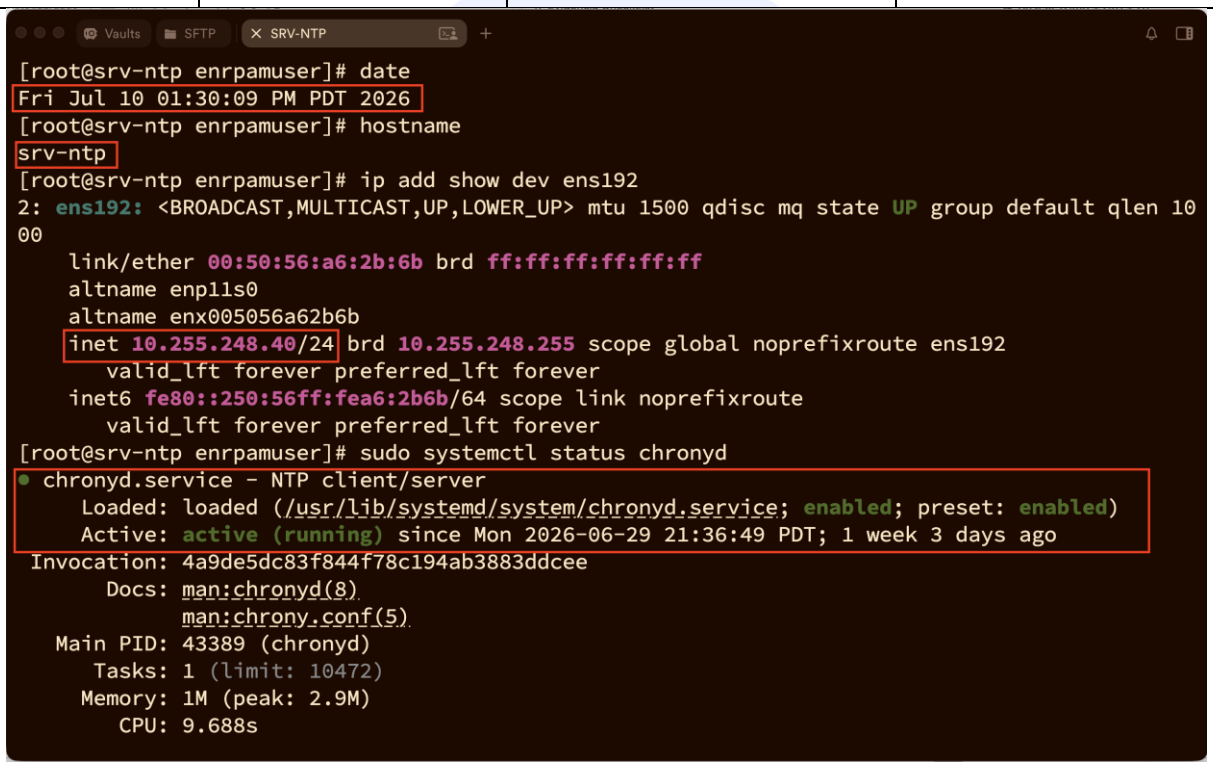


Figura 1. SRV-NTP: fecha, hostname, dirección de red y servicio chronyd en ejecución.

6. Matriz de cobertura por sede y activo

Sede	Activo	IP	Fuente NTP	Tipo
NGX	FW-FTNET-NGX-01	10.20.1.1	10.255.248.40	Firewall
NGX	SW-HP-NGX-01	10.20.1.2	10.255.248.40	Switch
NGX	HST-PRLN-01	10.20.1.4	10.255.248.40	Host virtualización
NGX	HST-PRLN-02	10.20.1.5	10.255.248.40	Host virtualización
NGX	HST-PRLN-03	10.20.1.6	10.255.248.40	Host virtualización
NGX	STR-MSA-01	10.20.1.10	10.255.248.40	Almacenamiento
NGX	VLT-SONCE-01	10.20.1.30	10.255.248.40	Respaldo
ASSETEL	FW-ASSETEL-01	10.30.1.1	201.174.13.155	Firewall
ASSETEL	SW-HP-ASSETEL-01	10.30.1.2	201.174.13.155	Switch
ASSETEL	HST-PRLN-04	10.30.1.13	10.255.248.40	Host virtualización
ASSETEL	HST-PRLN-05	10.30.1.14	10.255.248.40	Host virtualización
ASSETEL	HST-PRLN-06	10.30.1.15	10.255.248.40	Host virtualización
ASSETEL	STR-MSA-02	10.30.1.18	10.255.248.40	Almacenamiento
ASSETEL	VLT-SONCE-02	10.30.1.9 / 10.30.1.19*	10.255.248.40	Respaldo
Oficinas	FW-FG200E-03	10.100.0.1	201.174.13.155	Firewall
Oficinas	SW-ARUBA-2930	10.100.0.14	201.174.13.155	Switch
Oficinas	SRV-NAS	10.100.30.9	10.255.248.40	NAS

8. Evidencia de sincronización – activos físicos NGX

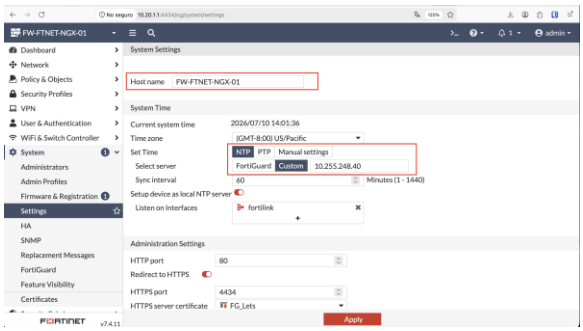


Figura 2. FW-FTNET-NGX-01: configuración NTP hacia 10.255.248.40.

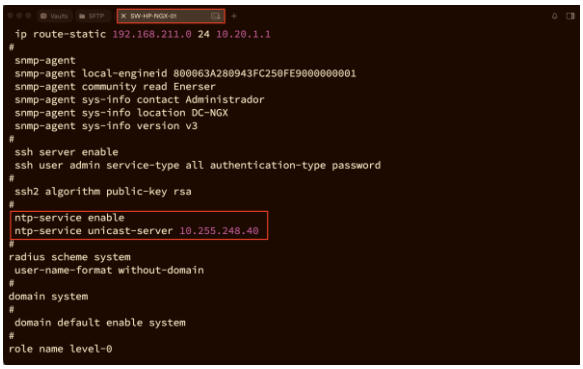


Figura 3. SW-HP-NGX-01: NTP service habilitado contra 10.255.248.40.

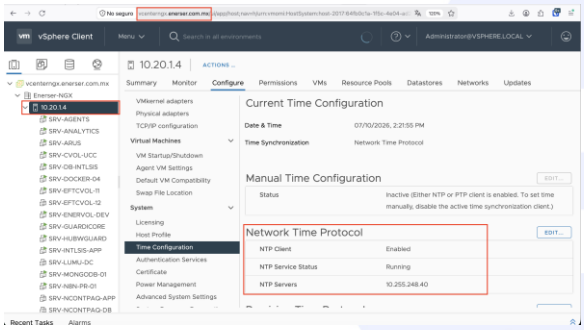


Figura 4. HST-PRLN-01: vCenter muestra NTP client habilitado y servidor 10.255.248.40.

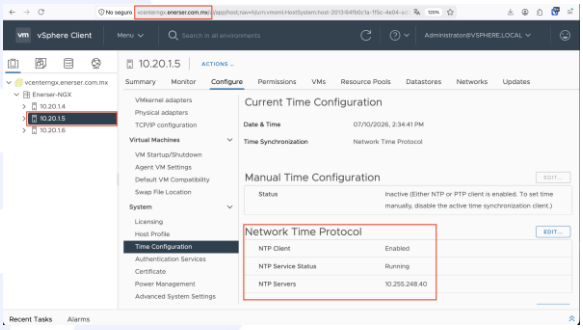


Figura 5. HST-PRLN-02: vCenter muestra NTP client habilitado y servidor 10.255.248.40.

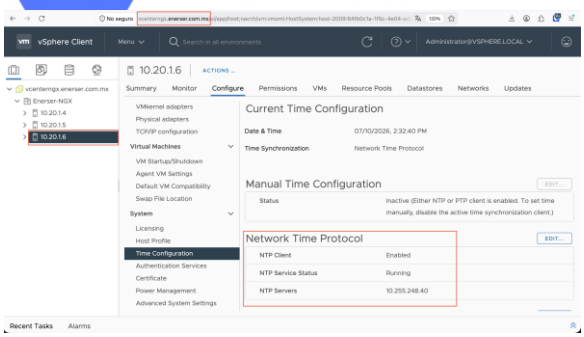


Figura 6. HST-PRLN-03: vCenter muestra servicio NTP y servidor de referencia.

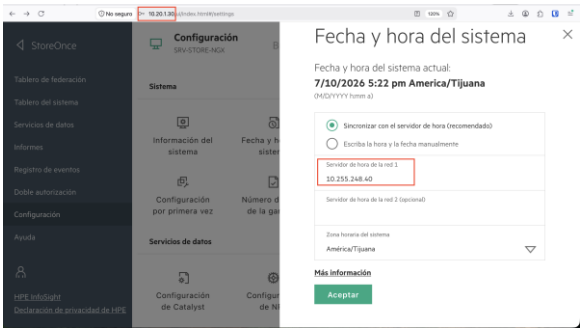


Figura 7. VLT-SONCE-01: StoreOnce sincroniza fecha/hora con 10.255.248.40.

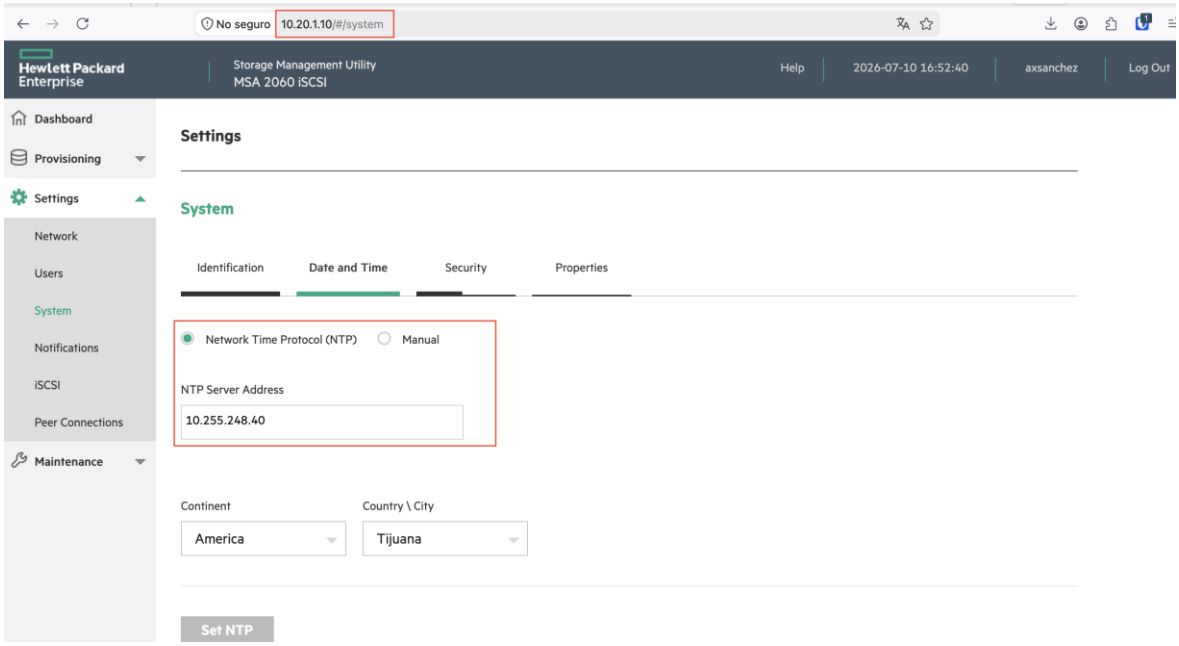


Figura 8. STR-MSA-01: configuración de fecha/hora mediante NTP 10.255.248.40.

8. Evidencia de sincronización – activos físicos ASSETEL

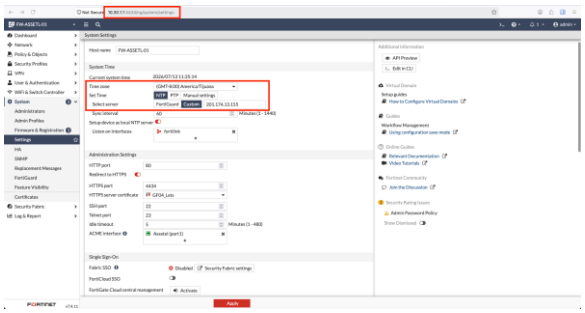


Figura 9. FW-ASSETEL-01: servidor NTP personalizado 201.174.13.155.

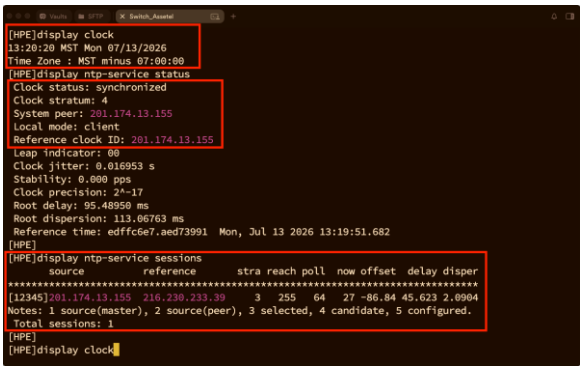


Figura 10. SW-HP-ASSETEL-01: reloj sincronizado y referencia NTP pública.

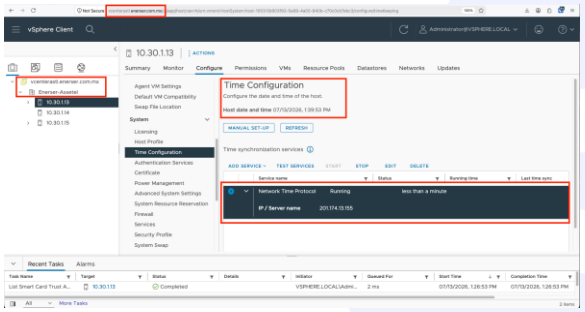


Figura 11. HST-PRLN-04: sincronización de tiempo en vCenter.

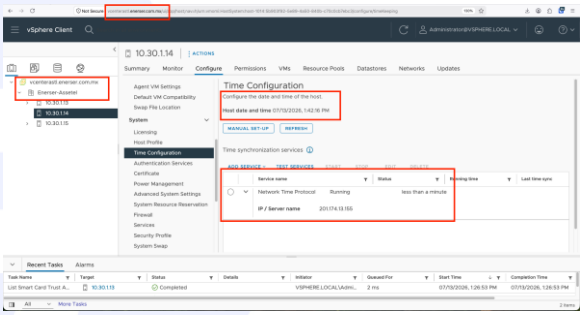


Figura 12. HST-PRLN-05: sincronización de tiempo en vCenter.

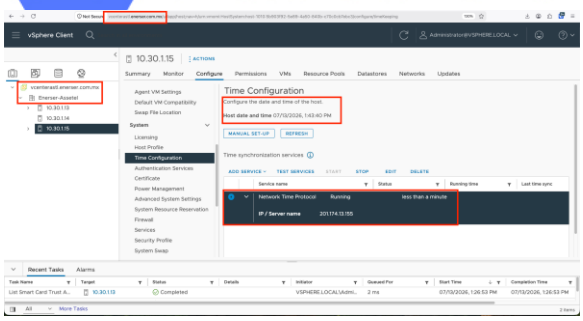


Figura 13. HST-PRLN-06: sincronización de tiempo en vCenter.

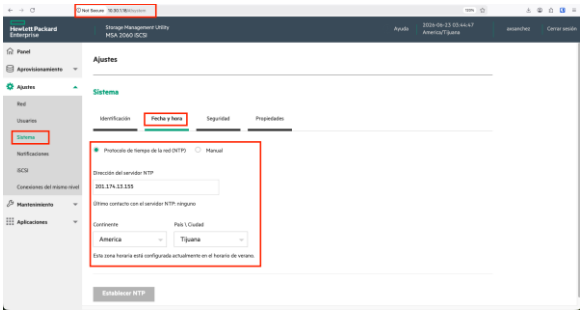


Figura 14. STR-MSA-02: NTP configurado en el sistema de almacenamiento.

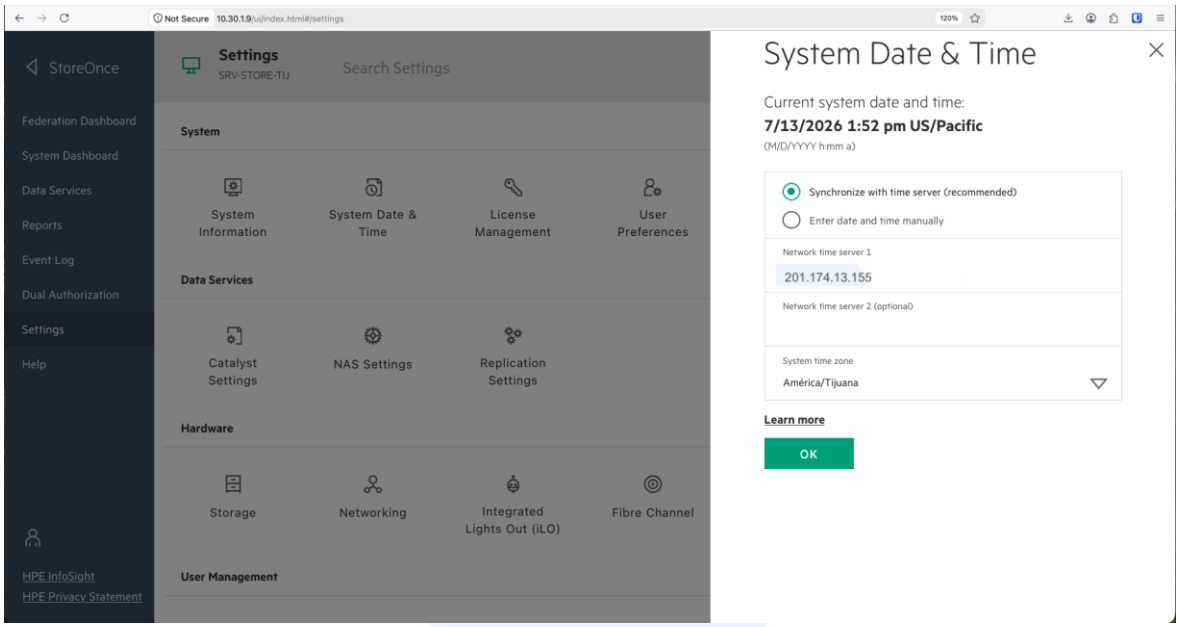


Figura 15. VLT/VTL-SONCE-02: configuración de fecha/hora mediante NTP. Validar IP del activo antes de firma.

9. Evidencia de sincronización – oficinas administrativas

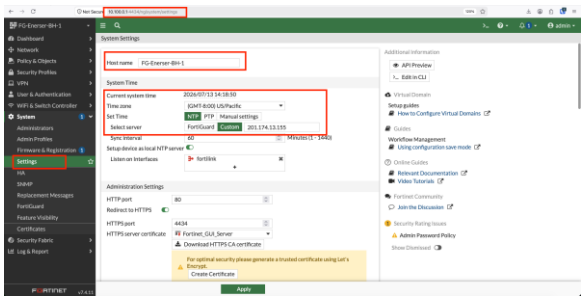


Figura 16. FW-FG200E-03: sincronización contra 201.174.13.155.



Figura 17. SW-ARUBA-2930: configuración NTP con 201.174.13.155.

10. Evidencia de sincronización – servidores virtuales del monedero

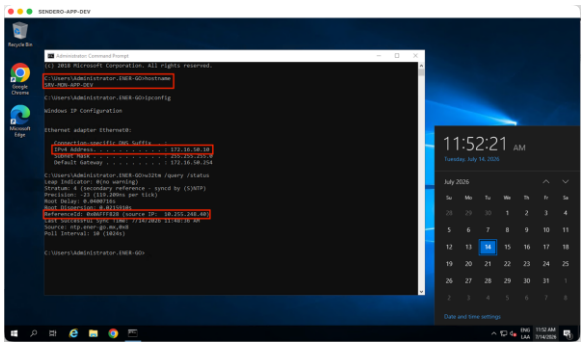


Figura 18. SRV-MON-APP-DV – 172.16.50.10: evidencia de fuente/estado NTP.

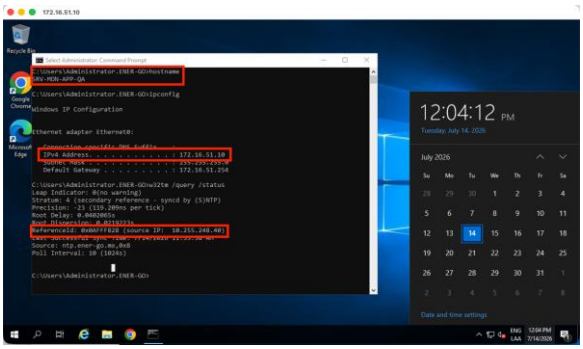


Figura 19. SRV-MON-APP-QA – 172.16.51.10: evidencia de fuente/estado NTP.

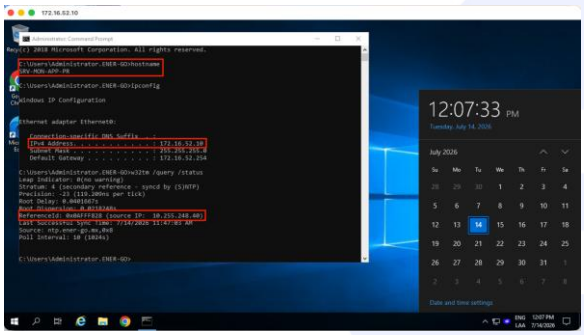


Figura 20. SRV-MON-APP-PR – 172.16.52.10: evidencia de fuente/estado NTP.

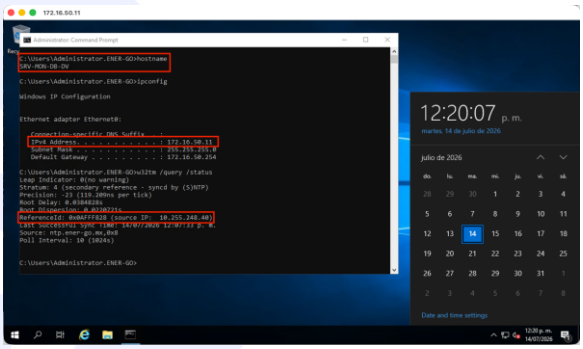


Figura 21. SRV-MON-DB-DV – 172.16.50.11: evidencia de fuente/estado NTP.

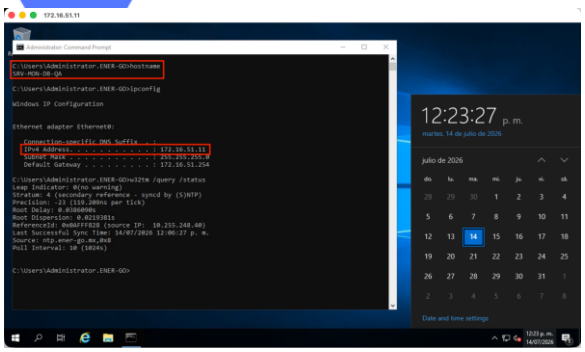


Figura 22. SRV-MON-DB-QA – 172.16.51.11: evidencia de fuente/estado NTP.

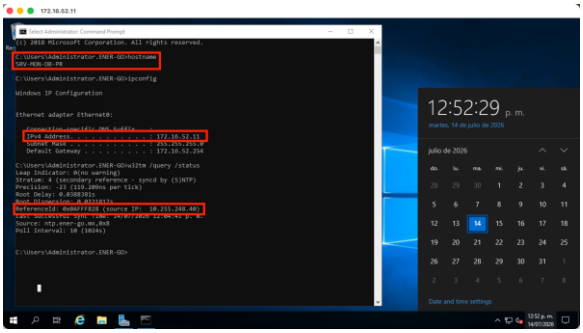


Figura 23. SRV-MON-DB-PR – 172.16.52.11: evidencia de fuente/estado NTP.

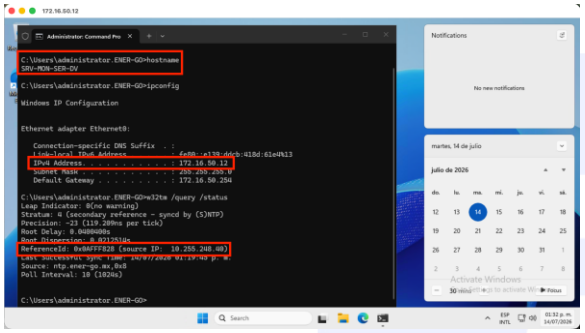


Figura 24. SRV-MON-SER-DV – 172.16.50.12: evidencia de fuente/estado NTP.

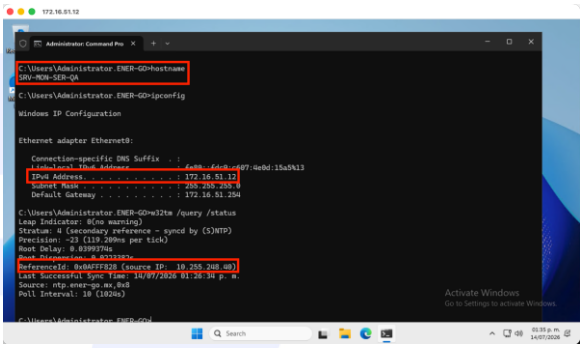


Figura 25. SRV-MON-SER-QA – 172.16.51.12: evidencia de fuente/estado NTP.

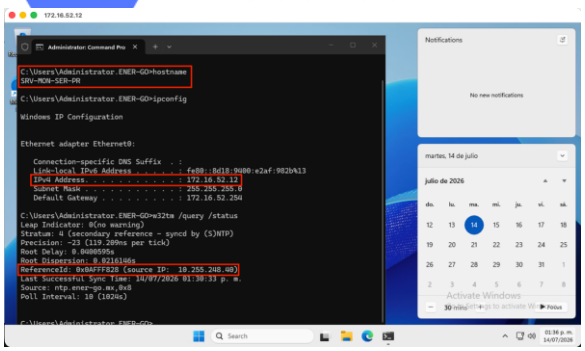


Figura 26. SRV-MON-SER-PR – 172.16.52.12: evidencia de fuente/estado NTP.

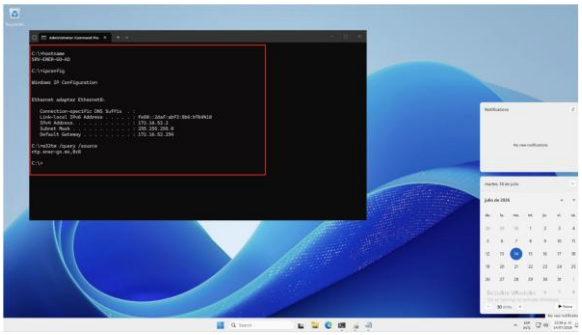


Figura 27. SRV-ENER-GO-AD – 172.16.52.2: evidencia de fuente/estado NTP.

11. Otros activos y escenario de contingencia

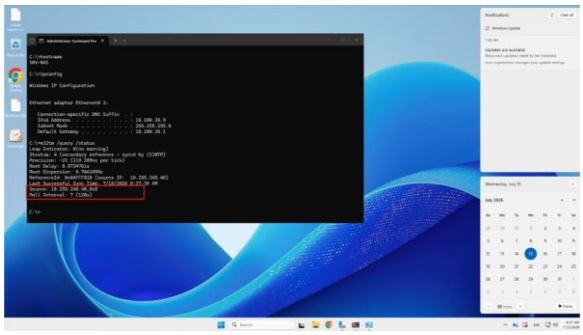


Figura 28. SRV-NAS: sincronización contra 10.255.248.40.

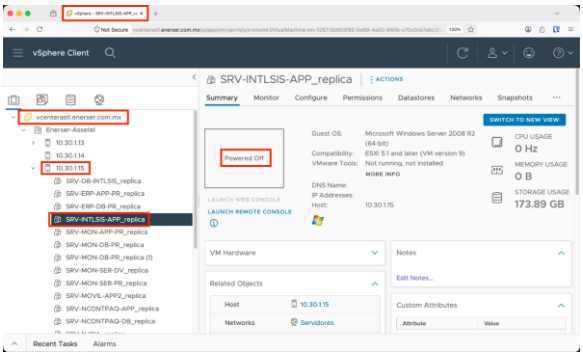


Figura 29. Réplicas en ASSETEL apagadas en operación normal; sincronizan al arrancar durante DRP.

Para las réplicas apagadas no es posible demostrar sincronización permanente mientras permanecen sin ejecución. El criterio de control consiste en que, al activarse durante una prueba o contingencia, el sistema operativo obtenga hora de la fuente NTP configurada y se conserve evidencia del estado posterior al arranque.

12. Documentación técnica de NTP / Chrony

Chrony es la implementación identificada en el documento fuente para proporcionar NTP en SRV-NTP. El servicio principal es chronyd y su administración/consulta puede realizarse mediante chronyc. La evidencia técnica debe demostrar que el demonio está activo, que existe al menos una fuente upstream válida y que los clientes autorizados pueden consultar el servicio.

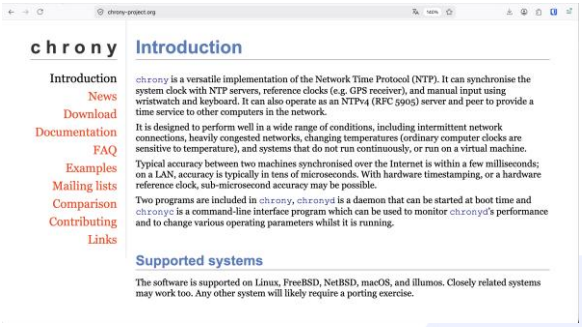


Figura 30. Referencia técnica del proyecto Chrony.

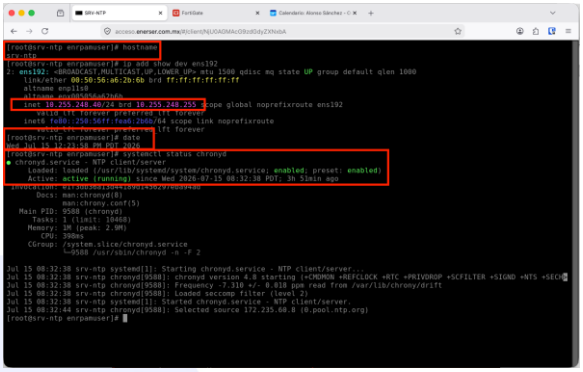


Figura 31. SRV-NTP: chronyd activo como servicio de systemd.

12.1 Configuración del servicio

```
  GNU nano 8.1                          /etc/chrony.conf                          Modified
# These servers were defined in the installation:
pool 1.pool.ntp.org iburst
pool 0.pool.ntp.org iburst
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
# Use NTP servers from DHCP.
sourcedir /run/chrony-dhcp
# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift
# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3
# Enable kernel synchronization of the real-time clock (RTC).
rtcsync
# Allow NTP client access from local network.
allow 192.168.0.0/16
allow 10.255.0.0/16
allow 172.16.0.0/16

# Serve time even if not synchronized to a time source.
local stratum 10

^G Help      ^O Write Out  ^F Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Figura 32. Archivo /etc/chrony.conf: fuentes pool.ntp.org y redes permitidas.

12.2 Evidencia de tráfico NTP

```
[root@srv-ntp enrpamuser]# hostname
srv-ntp
[root@srv-ntp enrpamuser]# ip add show ens192
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:a6:2b:6b brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    altname enx005056a62b6b
    inet 10.255.248.40/24 brd 10.255.248.255 scope global noprefixroute ens192
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea6:2b6b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@srv-ntp enrpamuser]# sudo tcpdump -ni any udp port 123
tcpdump: data link type LINUX_SLL2
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
14:39:56.531787 ens192 In  IP 10.20.1.6.ntp > 10.255.248.40.ntp: NTPv4, Client, length 48
14:39:56.532022 ens192 Out IP 10.255.248.40.ntp > 10.20.1.6.ntp: NTPv4, Server, length 48
14:40:18.793872 ens192 In  IP 10.255.248.254.ntp > 10.255.248.40.ntp: NTPv4, Client, length 48
14:40:18.794207 ens192 Out IP 10.255.248.40.ntp > 10.255.248.254.ntp: NTPv4, Server, length 48
14:40:18.953548 ens192 In  IP 10.20.1.1.61507 > 10.255.248.40.ntp: NTPv4, Client, length 48
14:40:18.953832 ens192 Out IP 10.255.248.40.ntp > 10.20.1.1.61507: NTPv4, Server, length 48
14:40:20.053700 ens192 In  IP 10.20.1.1.35471 > 10.255.248.40.ntp: NTPv4, Client, length 48
14:40:20.054089 ens192 Out IP 10.255.248.40.ntp > 10.20.1.1.35471: NTPv4, Server, length 48
```

Figura 33. Tráfico UDP/123 observado en SRV-NTP con sesiones de clientes del monedero.

12.3 Validación de offset / sincronización

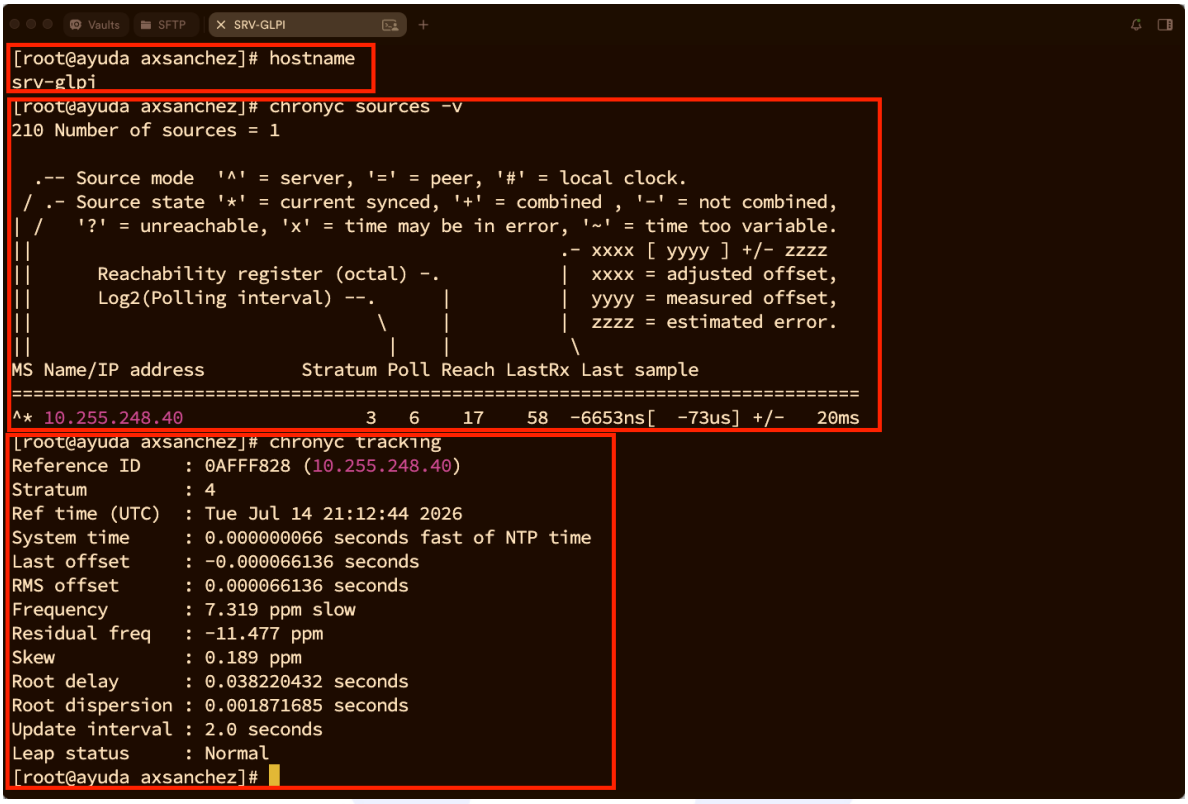


Figura 34. SRV-GLPI: chronyc muestra sincronización contra 10.255.248.40 y una diferencia indicada de 0.000066136 s.

13. Seguridad del servicio NTP

El documento fuente contiene evidencia complementaria de seguridad orientada a reducir la superficie de exposición del servicio y a controlar la administración del servidor de tiempo.

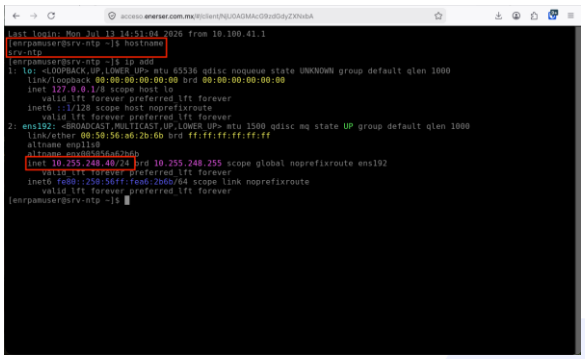


Figura 35. Acceso administrativo a SRV-NTP mediante Apache Guacamole, con sesión controlada.

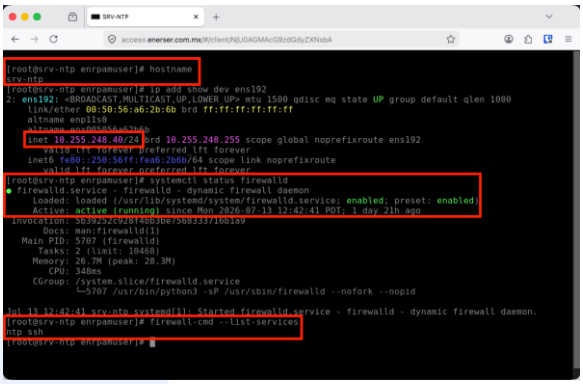


Figura 36. Firewall local de SRV-NTP: servicios permitidos limitados a SSH/NTP según evidencia aportada.

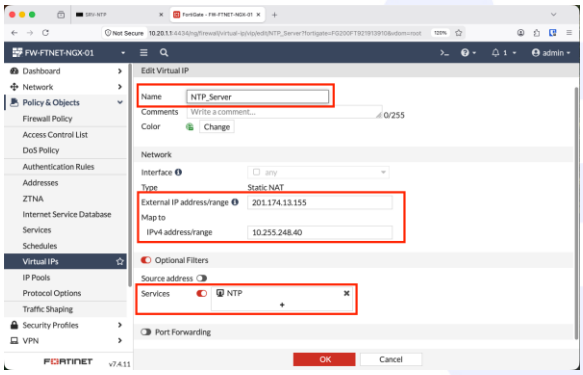


Figura 37. FW-FTNET-NGX-01: NAT/publicación del servicio NTP, limitado al puerto correspondiente.

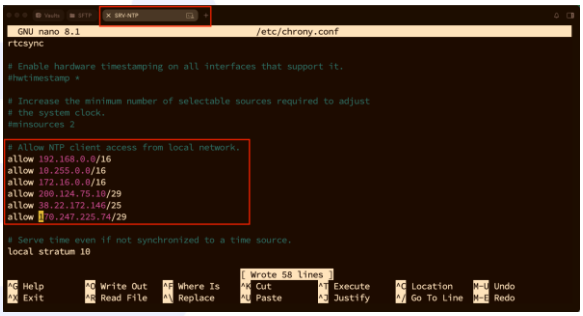


Figura 38. chrony.conf: lista blanca de redes/segmentos autorizados para consulta NTP.

14. Pruebas mínimas de cierre y mantenimiento de evidencia

Para mantener el expediente actualizado y evitar que la evidencia sea únicamente histórica, se recomienda obtener periódicamente una muestra representativa que confirme el estado actual del servicio y de sus clientes.

Componente	Prueba/captura	Qué debe demostrar
SRV-NTP	hostname; ip addr; systemctl status chronyd	Identidad del equipo y servicio activo
SRV-NTP	chronyc sources -v	Fuente upstream seleccionada, reach y estado
SRV-NTP	chronyc tracking	Reference ID, stratum, system time, last offset, RMS offset
Windows crítico	w32tm /query /status y w32tm /query /source	Fuente efectiva y estado de sincronización
Linux crítico	chronyc tracking / timedatectl	Estado synchronized y fuente
Firewall/Switch	pantalla/CLI NTP + clock/status	Servidor configurado y estado de reloj
vCenter/ESXi	Host > Configure > Time Configuration	NTP client enabled/running + server
MSA/StoreOnce	System date/time / NTP settings	Fuente NTP y zona horaria
Red	captura tcpdump UDP/123 o log equivalente	Intercambio NTP entre cliente y servidor
Seguridad	firewall/NAT/allowlist	Solo UDP/123 y orígenes autorizados

15. Observaciones de consistencia a validar antes de firma

Elemento	Situación	Acción de cierre
VLT/VTL-SONCE-02	Inventario: 10.30.1.9 / evidencia NTP: 10.30.1.19	Validar IP real y homologar todos los documentos.
SRV-GLPI	Inventario muestra 10.255.248.326, mientras la evidencia técnica utiliza 10.255.248.26	El valor 10.255.248.326 no es una IPv4 válida; confirmar en inventario y corregir controladamente.
Firewall NGX	Aparecen variantes FW-FNET-NGX-01 y FW-FTNET-NGX-01	Homologar el nombre contra el inventario maestro.
Alias DNS NTP	ntp.enerser.com.mx / ntp.ener-go.mx	Conservar si son endpoints reales; documentar que son alias técnicos usados por SENDERO FUEL.
Réplicas ASSETEL	Activos apagados no muestran sincronización permanente	Agregar evidencia posterior al arranque durante prueba DRP.