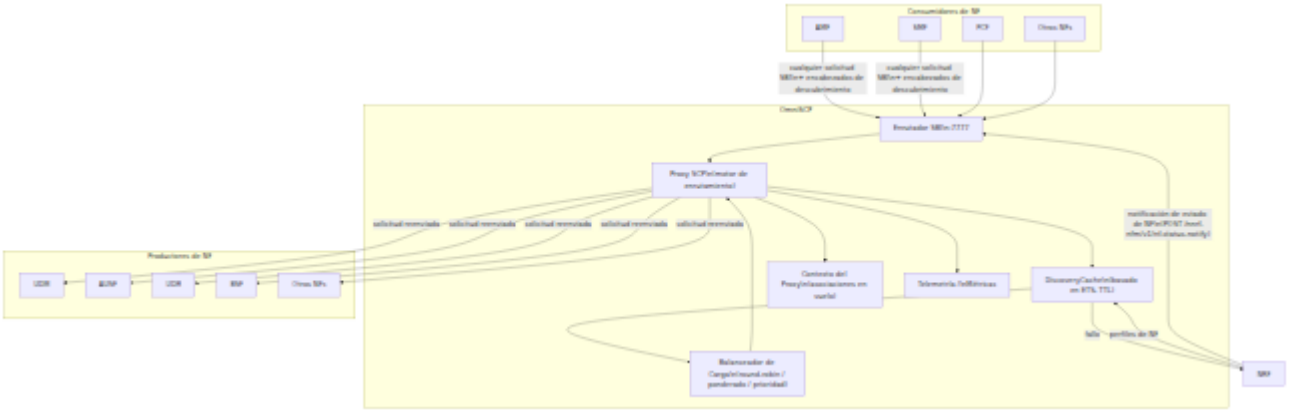
Guía de Operaciones de OmniSCP

Tabla de Contenidos

1. Descripción del Componente
2. Referencias de Rol y Especificación 3GPP
3. Puntos Finales SBI
4. Referencia de Configuración
5. Procedimientos Clave
6. Observabilidad
7. Limitaciones Conocidas
8. Solución de Problemas

Descripción del Componente

OmniSCP implementa la función de red Proxy de Comunicación de Servicio (SCP) definida en 3GPP TS 29.500 y TS 23.501. El SCP actúa como un proxy inverso HTTP entre consumidores de NF y productores de NF en la Arquitectura Basada en Servicios 5G (SBA). Proporciona descubrimiento NRF delegado, balanceo de carga entre instancias de productores de NF, reintentos en caso de fallo y almacenamiento en caché de resultados de descubrimiento NRF.



Modos de Enrutamiento

El SCP soporta tres modos de enrutamiento, evaluados en orden de prioridad en cada solicitud entrante:

1. **Reenvío directo** — El encabezado `3gpp-Sbi-Target-apiRoot` está presente. La solicitud se reenvía directamente a la URI base especificada sin búsqueda de NRF.
2. **Descubrimiento delegado** — Los encabezados `3gpp-Sbi-Discovery-target-nf-type` y `3gpp-Sbi-Discovery-service-names` están presentes. El SCP consulta el NRF (o accede a la caché) y selecciona una instancia mediante la estrategia de balanceo de carga configurada.
3. **Inferencia basada en la ruta** — No hay encabezados de enrutamiento presentes. El SCP infiere el tipo de NF objetivo del prefijo de la ruta (por ejemplo, `/nudm-` → UDM) y realiza un descubrimiento delegado.

Referencias de Rol y Especificación 3GPP

Elemento	Referencia
Definición de NF SCP	3GPP TS 23.501 Sección 7.3
Modelo de comunicación indirecta SCP	3GPP TS 29.500 Sección 6.10
Encabezados 3gpp-Sbi-Discovery-*	3GPP TS 29.500 Sección 6.10.3
Encabezado 3gpp-Sbi-Target-apiRoot	3GPP TS 29.500 Sección 6.10.3.2
Encabezado 3gpp-Sbi-Producer-Id	3GPP TS 29.500 Sección 6.10.3.3
Balanceo de carga SCP	3GPP TS 29.500 Sección 6.10.4
Servicio de descubrimiento de NF	3GPP TS 29.510 Sección 6.2
Notificación de estado de NF NRF	3GPP TS 29.510 Sección 6.3
Marco común SBI	3GPP TS 29.500

Puntos Finales SBI

OmniSCP opera como un proxy transparente. Solo hay un punto final manejado localmente; todas las demás rutas son enviadas al productor de NF apropiado.

Método	Ruta	Manejada Localmente	Descripción
`POST`	`/nnrf-nfm/v1/nf-status-notify`	Sí	Recibe notificaciones de cambio de estado de NF de NRF. En eventos `NF_DEREGISTERED` o `NF_PROFILE_CHANGED`, invalida toda la caché de descubrimiento. Devuelve 204 No Content.
`*`	`/*` (todas las demás rutas)	No — proxy	Cualquier método y ruta que no coincida con lo anterior se envía al productor de NF resuelto de acuerdo con el modo de enrutamiento activo.

Respuestas de Error del Proxy

Cuando el SCP no puede completar una operación de proxy, devuelve un cuerpo `ProblemDetails` según TS 29.500.

Estado HTTP	Causa	Condición
400 Bad Request	`MANDATORY_IE_MISSING`	No hay información de enrutamiento disponible: sin `3gpp-Sbi-Target-apiRoot`, sin encabezados de descubrimiento, y la ruta no puede ser mapeada a un servicio conocido.
502 Bad Gateway	`TARGET_NF_NOT_REACHABLE`	Todas las instancias de productores de NF seleccionadas devolvieron errores 5xx o errores de conexión después de reintentos, o no se pudo resolver ninguna URI SBI para una instancia descubierta.
504 Gateway Timeout	`NF_DISCOVERY_FAILURE`	El descubrimiento NRF devolvió cero instancias de NF para el servicio solicitado.
500 Internal Server Error	`SYSTEM_FAILURE`	Error interno inesperado en el proxy SCP.

Encabezados 3gpp-Sbi Consumidos

Encabezado	Descripción
`3gpp-Sbi-Target-apiRoot`	Objetivo de enrutamiento directo. Eliminado antes del reenvío.
`3gpp-Sbi-Discovery-target-nf-type`	Tipo de NF a descubrir (por ejemplo, `UDM`). Usado para descubrimiento delegado. Eliminado antes del reenvío.
`3gpp-Sbi-Discovery-service-names`	Lista de nombres de servicio separados por comas. El primer valor se usa como el principal. Eliminado antes del reenvío.
`3gpp-Sbi-Discovery-requester-nf-type`	Tipo de NF solicitante para el alcance de consulta NRF. Eliminado antes del reenvío.
`3gpp-Sbi-Discovery-target-plmn-list`	Lista de PLMN objetivo. Pasado al descubrimiento NRF. Eliminado antes del reenvío.
`3gpp-Sbi-Discovery-requester-snssai-list`	Lista de S-NSSAI solicitante. Pasada al descubrimiento NRF. Eliminada antes del reenvío.
`3gpp-Sbi-Discovery-nf-set-id`	Filtro de ID de conjunto de NF para el descubrimiento. Eliminado antes del reenvío.
`3gpp-Sbi-Discovery-target-nf-instance-id`	ID de instancia de NF específico a objetivo. Eliminado antes del reenvío.
`3gpp-Sbi-Discovery-requester-nf-instance-id`	ID de instancia solicitante. Eliminado antes del reenvío.

Encabezados 3gpp-Sbi Producidos

Encabezado	Descripción
`3gpp-Sbi-Producer-Id`	Agregado a cada respuesta enrutada. Contiene el `nfInstanceId` del productor de NF que manejó la solicitud, permitiendo la vinculación de consumidor a productor según TS 29.500 Sección 6.10.3.3.

Referencia de Configuración

Todos los parámetros se establecen a través del entorno de la aplicación (típicamente `config/runtime.exs`).

```
config :omniscp,
  sbi_scheme:            "http",
  sbi_addr:              "127.0.0.200",
  sbi_port:              7777,
  nrf_uri:               "http://127.0.0.10:7777",
  mcc:                   "999",
  mnc:                   "70",
  heartbeat_interval:    10_000,
  discovery_cache_ttl:   60_000,
  lb_strategy:           :round_robin,
  max_retries:           1,
  upstream_timeout:      5_000
```

Tabla de Parámetros

Parámetro	Predeterminado	Tipo	Descripc
`sbi_scheme`	`"http"`	string	Esquema de transporte p oyente SBI.
`sbi_addr`	`"127.0.0.200"`	string	Dirección IP que se vincu servidor HT Los consum de NF deber enrutar el tr SBI a esta dirección.
`sbi_port`	`7777`	integer	Puerto TCP que escucha servidor HT
`nrf_uri`	`"http://127.0.0.10:7777"`	string	URI base de Usado para registro de l latido y con de descubrimie de NF en no de los consumidor
`mcc`	`"999"`	string	Código de P Móvil. Inclui el perfil de N registrado c NRF.

Parámetro	Predeterminado	Tipo	Descripc
`mnc`	`"70"`	string	Código de R Móvil. Inclui el perfil de I registrado c NRF.
`heartbeat_interval`	`10_000`	integer (ms)	Intervalo en solicitudes d latido NRF.
`discovery_cache_ttl`	`60_000`	integer (ms)	Tiempo de v para las ent de caché de descubrimie NRF, indexa por `{target_nf_ service_nam` Las entrada expiradas se eliminan de perezosa en búsqueda y una tarea de limpieza en segundo pla cada 30 segundos. Aumentar p implementa estables; disminuir cu los perfiles c cambian co frecuencia.

Parámetro	Predeterminado	Tipo	Descripc
`lb_strategy`	`:round_robin`	atom	Estrategia d balanceo de para la sele de producto NF. Valores válidos: `:round_rob` `:weighted`, `:priority`. sección de Balanceo de Carga para semántica.
`max_retries`	`1`	integer	Número má de intentos reintento cu un producto NF devuelve un error de conexión. U valor de `1` significa un intento orig más un rein Establecer e para deshab reintentos.
`upstream_timeout`	`5_000`	integer (ms)	Tiempo de e para solicitu HTTP ascen a productor NF (tiempo espera de

Parámetro	Predeterminado	Tipo	Descripc
			recepción). solicitudes c excedan est tiempo de e se tratan co fallos y pue desencaden reintento.

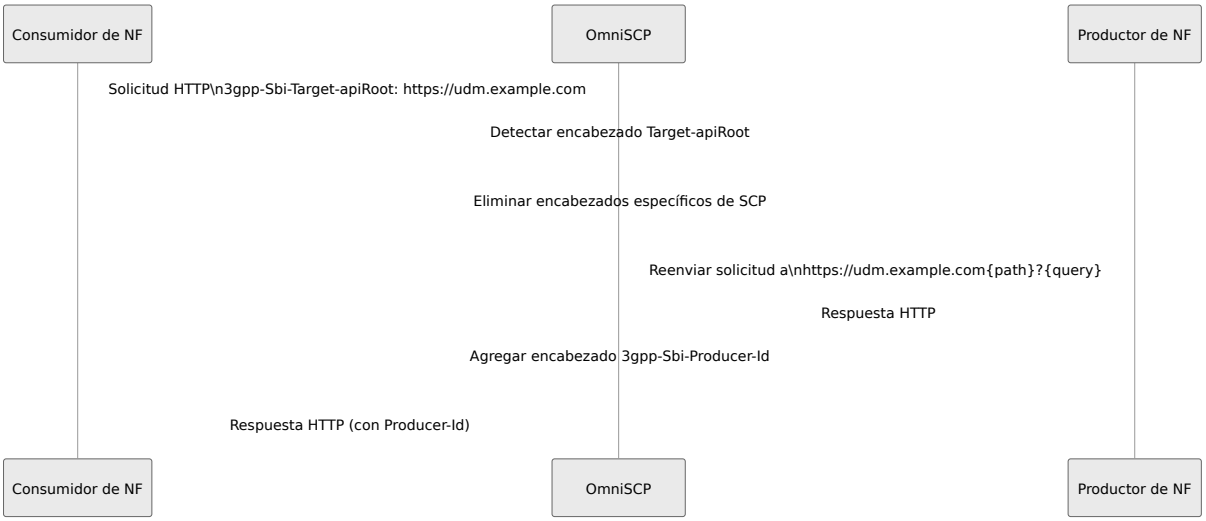
Estrategias de Balanceo de Carga

Estrategia	Descripción
`:round_robin`	Cicla a través de instancias saludables en orden. El estado se mantiene por cada par `{nf_type, service_name}`. Esta es la estrategia predeterminada y recomendada para implementaciones uniformes de NF.
`:weighted`	Selecciona la instancia con la puntuación más baja de `load - capacity`. Utiliza los campos `load` y `capacity` del perfil de NF de NRF. Prefiere instancias con alta capacidad y baja carga actual.
`:priority`	Selecciona la instancia con el valor de `priority` más bajo (mayor prioridad). Útil para implementaciones activas/en espera.

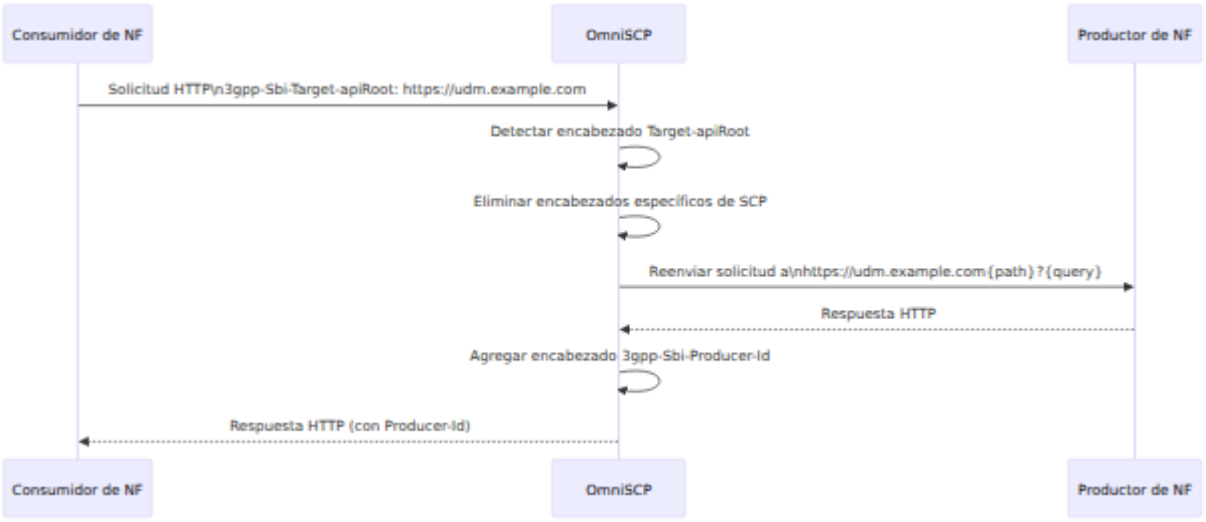
Una instancia se marca como no saludable después de 3 fallos consecutivos y se recupera automáticamente después de un período de enfriamiento de 30 segundos. Cuando todas las instancias están no saludables, el balanceador de carga vuelve a la lista completa de instancias.

Procedimientos Clave

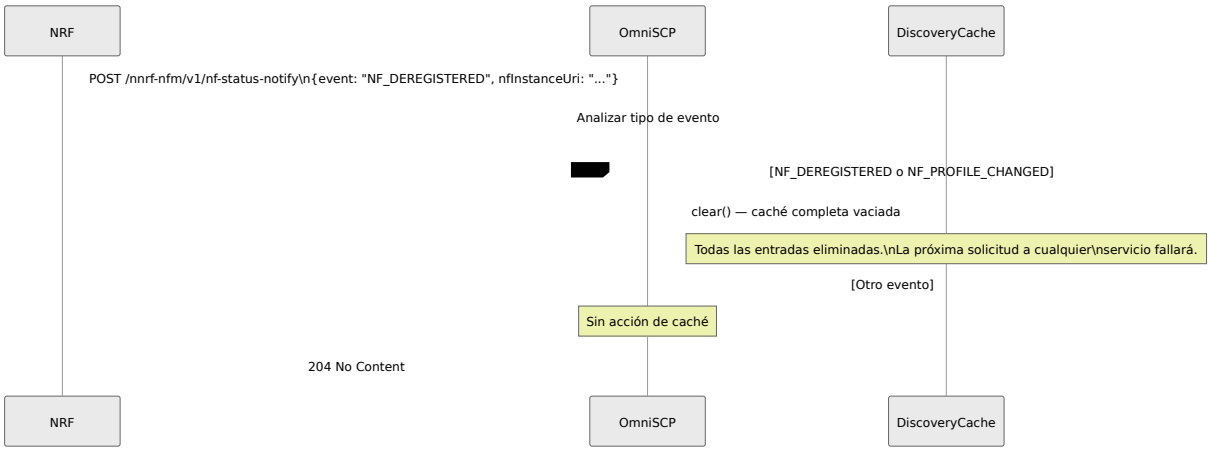
Reenvío Directo (Modo 1)



Descubrimiento Delegado y Reenvío (Modo 2)



Notificación de Estado de NRF (Invalidación de Caché)



Inferencia de Servicio Basada en la Ruta (Modo 3)

Cuando no hay encabezados de enrutamiento presentes, el SCP extrae el nombre del servicio del prefijo de la ruta de la solicitud y lo mapea a un tipo de NF utilizando la siguiente tabla incorporada:

Prefijo de Ruta	Tipo de NF
`nudm-`	UDM
`nausf-`	AUSF
`namf-`	AMF
`nsmf-`	SMF
`npcf-`	PCF
`nudr-`	UDR
`nnssf-`	NSSF
`nbsf-`	BSF
`nnrf-`	NRF

Nota: los prefijos `nchf-`, `nnef-` y `naf-` no están en el mapa incorporado (limitación SCP-L1). Las solicitudes a servicios CHF, NEF o AF requieren encabezados de descubrimiento explícitos al usar el modo 3.

Observabilidad

Eventos de Telemetría

Evento	Medidas	Etiquetas	Descripción
`[:omniscp, :proxy, :requests]`	`count`, `duration_ms`	`target_nf_type`, `result`	Resultado del proxy por solicitud
`[:omniscp, :proxy, :result]`	`count`, `duration_ms`	`target_nf_type`, `result`	Mismo evento utilizado para histograma de distribución
`[:omniscp, :discovery, :cache]`	`hits`, `misses`	`target_nf_type`, `service_name`	Acertar/fallo de caché por servicio
`[:omniscp, :cache, :hit]`	`count`	—	Contador agregado de aciertos de caché
`[:omniscp, :cache, :miss]`	`count`	—	Contador agregado de fallos de caché
`[:omniscp, :associations, :active]`	`count`	—	Medida: asociaciones de proxy activas
`[:omni5g, :nrf, :registration]`	`status`	`nf_type`	Estado de registro de NRF (1=registrado, 0=no)

Valores de etiqueta de resultado: `success` (2xx/3xx), `client_error` (4xx), `server_error` (5xx), `error` (conexión/tiempo de espera).

Métricas de Prometheus

Métricas del Proxy SCP

Métrica	Tipo	Etiquetas
`omni_scp.proxy.requests.count`	contador	`target_nf_type`, `result`
`omni_scp.proxy.requests.duration_ms`	resumen	`target_nf_type`
`omni_scp.proxy_requests.total`	contador	`target_nf_type`, `result`
`omni_scp.proxy_request.duration_ms`	distribución	`target_nf_type`
`omni_scp.active_associations.count`	medidor	--

Métricas de Caché

Métrica	Tipo	Etiquetas	Descri
`omni_scp.discovery.cache.hits`	contador	`target_nf_type`, `service_name`	Aciertos caché p servicio
`omni_scp.discovery.cache.misses`	contador	`target_nf_type`, `service_name`	Fallos d caché p servicio
`omni_scp.cache_hits.total`	contador	--	Contad agrega aciertos caché
`omni_scp.cache_misses.total`	contador	--	Contad agrega fallos d caché

Métricas de NRF

Métrica	Tipo	Etiquetas	Descripción
`omni_scp.nrf.registration.status`	medidor	`nf_type`	Estado de registro de NRF (1=registrado 0=no)

Métricas de la VM BEAM

Métrica	Tipo	Descripción
`beam.memory.total`	medidor	Memoria total de BEAM en bytes
`beam.memory.processes`	medidor	Memoria utilizada por procesos Erlang
`beam.memory.processes_used`	medidor	Memoria realmente utilizada por procesos
`beam.memory.system`	medidor	Memoria del sistema
`beam.memory.atom`	medidor	Memoria total de átomos
`beam.memory.atom_used`	medidor	Memoria de átomos utilizada
`beam.memory.binary`	medidor	Memoria binaria
`beam.memory.code`	medidor	Memoria de código
`beam.memory.ets`	medidor	Memoria de tablas ETS
`beam.processes.count`	medidor	Número de procesos Erlang
`beam.ports.count`	medidor	Número de puertos Erlang
`beam.atom.count`	medidor	Número de átomos
`beam.vm.uptime`	medidor	Tiempo de actividad de la VM en segundos

Patrones de Registro

Nivel	Patrón	Significado
`info`	`Recibida notificación de estado de NRF`	Notificación de estado de NF recibida
`info`	`Notificación de NRF: event=<E> nf=<URI>`	Evento de notificación analizado
`debug`	`Reenvío directo de SCP: <METHOD> <URL>`	Reenvío del modo 1
`debug`	`Reenvío delegado de SCP: <METHOD> <URL> (intento <N>)`	Intento de reenvío del modo 2/3
`warning`	`SCP reintentando después de <STATUS> de <ID>...`	Reintento desencadenado por 5xx
`warning`	`SCP reintentando después de error de <ID>...`	Reintento desencadenado por error de conexión
`warning`	`SCP no puede determinar objetivo para <METHOD> <PATH>`	Ruta del modo 3 no en el mapa de servicios
`warning`	`El descubrimiento de NRF no devolvió instancias para <NF>/<SVC>`	El descubrimiento devolvió una lista vacía
`warning`	`Todas las instancias de NF no saludables, volviendo a la lista completa`	Recaída de salud del LB
`error`	`Fallo en el descubrimiento de NRF: ...`	Error de consulta de NRF

Nivel	Patrón	Significado
`error`	`Error de proxy SCP: ...`	Fallo inesperado del proxy
`info`	`Instancia de NF &lt;ID> recuperada después del período de enfriamiento`	Salud de la instancia restaurada

Limitaciones Conocidas

ID	Severidad	Descripción
~~SCP-H4~~	~~Alto~~	~~La deconstrucción de ECIES SUCI no está implementada.~~ **RESUELTO.** La deconstrucción de los perfiles ECIES A (X25519) y B (secp256r1) ahora está implementada en `Omni5gEx.Crypto.SUPI` según el Anexo C de TS 33.501. OmniUDM realiza la deconstrucción antes de la búsqueda de UDR utilizando claves privadas de la red doméstica configuradas a través de `hnet_key_dir`. El SCP no necesita deconstruir SUCIs en el modelo de comunicación directa estándar.
SCP-M1	Medio	El control de sobrecarga no está implementado. El encabezado `3gpp-Sbi-Oci` (Información de Control de Sobrecarga) no se genera ni se consume. En escenarios de sobrecarga, el SCP continuará reenviando solicitudes sin reducir la carga o presionar a los consumidores.
SCP-M2	Medio	La indicación de control de carga no está implementada. El encabezado `3gpp-Sbi-Lci` (Información de Control de Carga) no se genera. Los consumidores no pueden usar OmniSCP para obtener pistas de carga de NF para sus propias decisiones de control de carga.
SCP-L1	Bajo	El mapa de inferencia de servicio basado en la ruta (Modo 3) carece de entradas de prefijo `nchf-` (CHF), `nnef-` (NEF) y `naf-` (AF). Las solicitudes a estos servicios sin encabezados de descubrimiento explícitos recibirán un 400 Bad Request con causa `MANDATORY_IE_MISSING`. Solución alternativa: configurar a los consumidores para que envíen

ID	Severidad	Descripción
		encabezados `3gpp-Sbi-Discovery-*` para estos servicios.
SCP-L3	Bajo	Las notificaciones de estado de NRF con el evento `NF_DEREGISTERED` o `NF_PROFILE_CHANGED` borran toda la caché de descubrimiento en lugar de solo la entrada afectada `{nf_type, service_name}`. En implementaciones con cambios frecuentes en los perfiles de NF, esto provoca una ráfaga de consultas de redescubrimiento de NRF.

Solución de Problemas

400 Bad Request — MANDATORY_IE_MISSING

El SCP no pudo determinar un objetivo de enrutamiento. Verifique:

1. ¿Está el consumidor enviando `3gpp-Sbi-Target-apiRoot` o ambos `3gpp-Sbi-Discovery-target-nf-type` y `3gpp-Sbi-Discovery-service-names`?
2. Si se basa en la inferencia basada en la ruta (Modo 3), ¿aparece el prefijo de la ruta en el mapa de servicios incorporado? Tenga en cuenta que `nchf-`, `nnef-` y `naf-` están ausentes (SCP-L1). Agregue encabezados explícitos para esos servicios.

504 Gateway Timeout — NF_DISCOVERY_FAILURE

NRF no devolvió instancias de NF. Verifique:

1. ¿Es el NRF accesible desde OmniSCP? Verifique `nrf_uri` y la conectividad de red.
2. ¿Está el tipo de NF objetivo registrado en el NRF? Consulte directamente al NRF: `GET {nrf_uri}/nnrf-disc/v1/nf-instances?target-nf-`

`type=<TYPE>`.

3. Verifique si una notificación de estado de NRF acaba de borrar la caché (evento `NF_DEREGISTERED`) y el NF no se ha re-registrado.

502 Bad Gateway — TARGET_NF_NOT_REACHABLE

Todas las instancias de productores de NF fallaron. Verifique:

1. ¿Están los productores de NF en ejecución y son accesibles en las direcciones SBI reportadas en sus perfiles de NRF?
2. Verifique `upstream_timeout`. Si los productores de NF tardan en responder, aumente este valor.
3. Revise `max_retries`. Si se establece en `0`, un solo fallo se convierte en un 502 inmediato.
4. Verifique el estado de salud del balanceador de carga en los registros: busque `Instancia de NF <ID> marcada como no saludable después de N fallos`.

Caché de descubrimiento causando enrutamiento obsoleto

Si los productores de NF cambian de dirección o se reinician sin una desregistración adecuada de NRF, la caché puede contener URIs SBI obsoletas hasta que expire el TTL. Opciones:

1. Reduzca `discovery_cache_ttl` para limitar la ventana de obsolescencia.
2. Asegúrese de que los productores de NF se desregistren del NRF al apagarse; esto desencadena una notificación de estado de NRF que borra la caché de OmniSCP.
3. Un reinicio del proceso de OmniSCP borra todo el estado de la caché.

Alta latencia del proxy

1. Verifique el histograma `omni_scp.proxy_request.duration_ms` para la distribución de latencia.

2. Compare la tasa de aciertos de caché (`omni_scp.cache_hits.total` vs `omni_scp.cache_misses.total`). Una alta tasa de fallos significa consultas frecuentes a NRF. Aumente `discovery_cache_ttl`.
3. Verifique `upstream_timeout` — las solicitudes que superan el tiempo de espera añaden toda la duración del tiempo de espera a la latencia antes de desencadenar un reintento.

Registro de NRF no mantenido

Verifique la métrica `omni_scp.nrf.registration.status`. Si muestra 0:

1. Verifique que `nrf_uri` sea correcto y que el NRF sea accesible.
2. Verifique que `mcc` y `mnc` coincidan con la configuración de PLMN del NRF.
3. Busque errores de registro de NRF en los registros de la aplicación al inicio.