Comprender la capacidad de observación y la integración de Splunk de Cisco CEE

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Descripción general de la arquitectura
- Cargas de trabajo de espacio de nombres CEE
- Instalación de CEE y gestión del ciclo de vida
  - Modos de instalación
  - Definir el artefacto de software CEE
  - Configuración del clúster y el centro de operaciones
  - Sincronizar y verificar la implementación
- Centro de operaciones y gestión operativa de CEE
- Arquitectura CEE Observability
- Integración de Splunk: Arquitectura de transferencia de registro
- Reenvío del recopilador de eventos Splunk HTTP
  - Modelo de configuración de HEC
  - Capturar y solucionar problemas de tráfico HEC
- Reenvío de Syslog sobre UDP 5140
  - Asignación de campos RFC 5424
  - Transporte UDP y captura de paquetes
- Alertas, SNMP y observabilidad CIMC
- Estadísticas masivas
- Gateway del sistema OpenTelemetry
  - Modelo de gateway del sistema
  - Conceptos de configuración de gateway
  - Exportadores remotos
  - Comparar con OpenShift OpenTelemetry
- Verifique la Configuración
  - Verificar sincronización CEE
  - Verifique HEC y Syslog por separado
  - Verificar servicios de observabilidad
- Comportamiento esperado
- Flujo de decisión
- Conclusión
- Contenido relacionado

Introducción

Este documento describe la arquitectura, implementación, supervisión, integración de Splunk y OpenTelemetry de Cisco Common Execution Environment (CEE).

Prerequisites

Requirements

Cisco recomienda estar familiarizado con estas tecnologías:

- Plataforma de implementación nativa en la nube (CNDP), espacios de nombres de Kubernetes y ubicación de grupos de dispositivos.
- Cisco Subscriber Microservices Infrastructure (SMI) y SMI Cluster Manager.
- CEE Ops Center, Prometheus, Grafana, Alertmanager y componentes de reenvío de registros.
- Splunk HTTP Event Collector (HEC), syslog y captura de paquetes con tcpdump.
- OpenTelemetry Protocol (OTLP) y OpenTelemetry Collector para la nueva integración de gateway.

Componentes Utilizados

Los ejemplos muestran un entorno SMI/CNDP de Cisco basado en Kubernetes con CEE y una aplicación asociada Session Management Function (SMF). El ejemplo de definición de software se refiere al paquete CEE 2026.01.1.08; El ejemplo del Centro de Operaciones utiliza un identificador de repositorio SMF smf-2026.04.m0.i50. Estos son valores de ejemplo, no requisitos de despliegue.

Los extremos de red, los nombres de clúster y los valores de espacio de nombres deben reemplazarse por valores aprobados para la implementación de destino.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

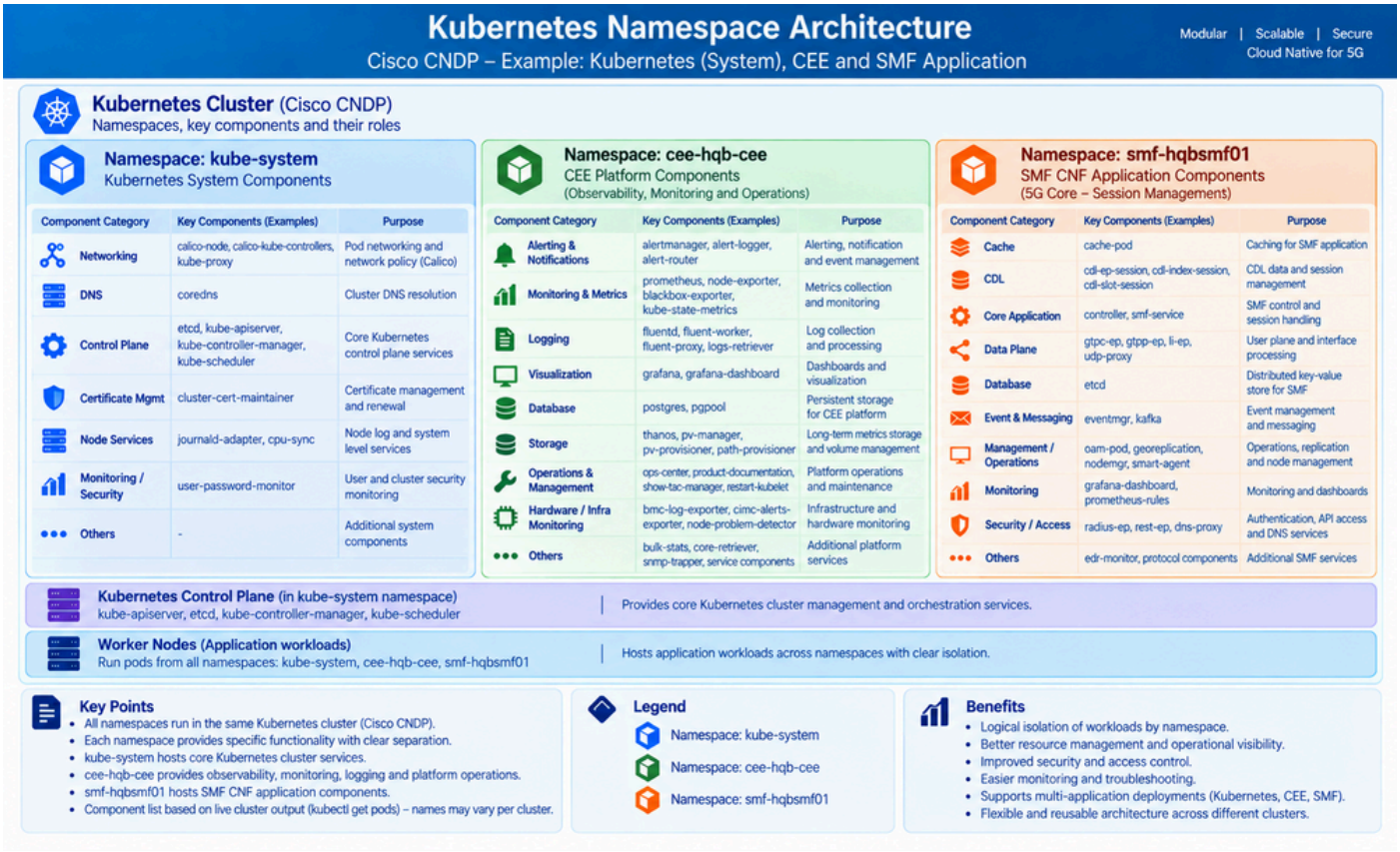
El Entorno de ejecución común (CEE) de Cisco forma parte de la infraestructura de microservicios para abonados de Cisco (SMI). En una implementación de CNDP basada en Kubernetes, los espacios de nombres de Kubernetes separan los servicios de plataforma, los servicios de administración de CEE y observabilidad de Kubernetes, y las cargas de trabajo de aplicaciones SMF. La separación proporciona límites administrativos y operativos, mientras que la red de Kubernetes y la detección de servicios permiten la comunicación de componentes permitida.

Este documento abarca la arquitectura de espacio de nombres, las cargas de trabajo de CEE, la instalación de CEE y la gestión del ciclo de vida, el centro de operaciones de CEE, alertas y el protocolo simple de administración de red (SNMP), alertas de Cisco Integrated Management Controller (CIMC), reenvío de registros, estadísticas masivas y el gateway del sistema OpenTelemetry.

El Splunk HEC en el puerto 8088 del Protocolo de control de transmisión (TCP) y el puerto 5140 del Protocolo de datagramas de usuario (UDP) de syslog over son mecanismos de ingestión independientes. Las dos rutas tienen diferentes requisitos de configuración, transporte y solución de problemas y pueden coexistir.

Descripción general de la arquitectura

CEE y las funciones de aplicación asociadas ocupan espacios de nombres de Kubernetes independientes. La arquitectura diferencia a los servicios de la plataforma Kubernetes de las funciones de observación y gestión de CEE y del dominio de aplicaciones SMF.



Arquitectura de espacio de nombres SMI de Cisco que muestra la separación de CEE y plataformas de aplicaciones

El espacio de nombres CEE es el objetivo principal de la arquitectura de nivel de servicio. Otros espacios de nombres proporcionan la plataforma Kubernetes, funciones de red y cargas de trabajo SMF.

Cargas de trabajo de espacio de nombres CEE

El espacio de nombres CEE aloja microservicios para la supervisión, las alertas, el registro, los paneles, las estadísticas y el acceso operativo.

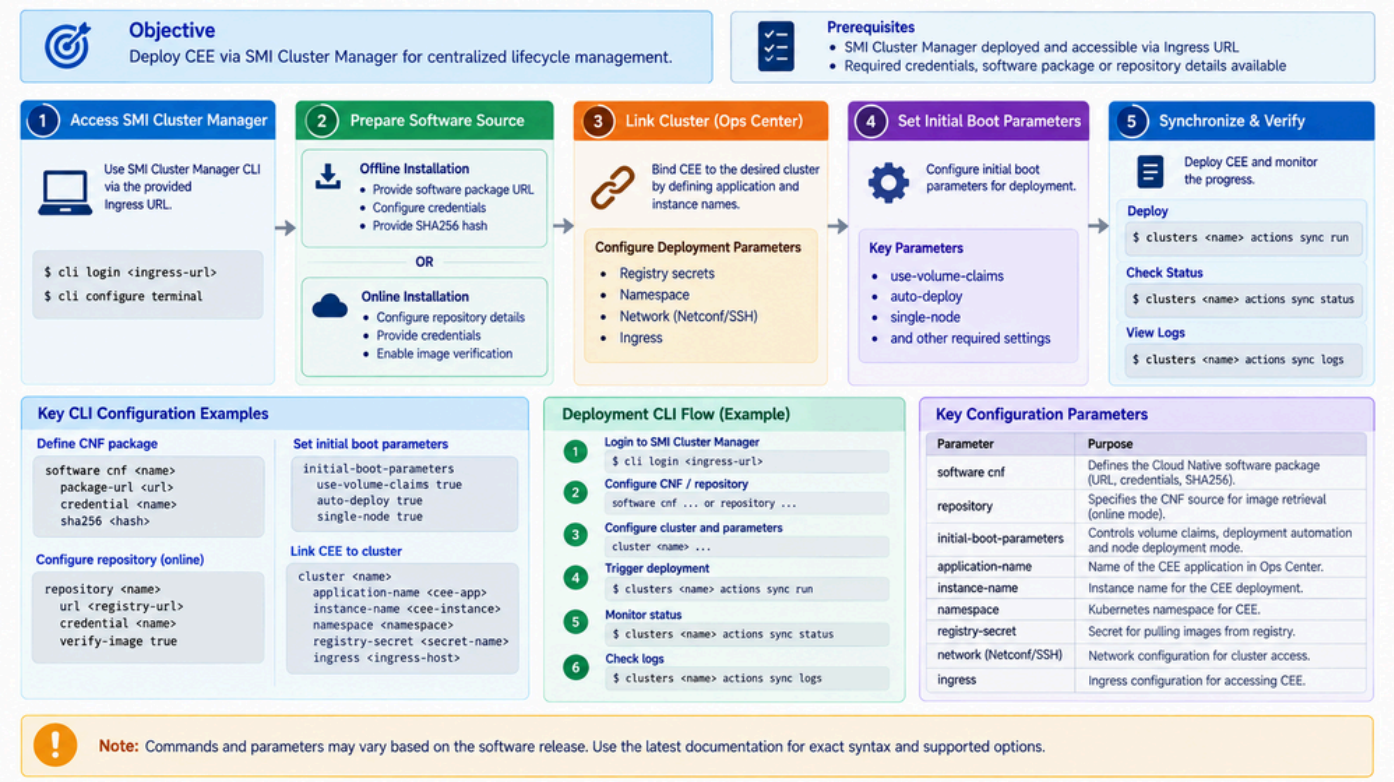


Microservicios de espacio de nombres CEE y las funciones de sus cargas de trabajo operativas

Estas funciones incluyen recopilación de métricas de Prometheus, visualización de Grafana, gestión de alertas de Alertmanager, servicios de reenvío de registros y creación periódica de estadísticas masivas. Las cargas de trabajo individuales varían según la versión y la configuración de implementación.

Instalación de CEE y gestión del ciclo de vida

El Administrador de clústeres SMI separa la definición de artefactos de software del clúster de destino y su configuración del Centro de operaciones. Esto permite controlar las versiones del software y la sincronización repetible del clúster.



Arquitectura de sincronización de software e instalación de SMI Cluster Manager CEE

Modos de instalación

- La instalación sin conexión puede hacer referencia a un paquete de software local a través de una dirección URL de archivo y un hash de algoritmo hash seguro de 256 bits (SHA-256).
- La configuración del clúster asocia la implementación de CEE/SMF con el clúster y la instancia del centro de operaciones previstos.

Definir el artefacto de software CEE

En la configuración de SMI Cluster Manager, identifique el paquete de software CEE local y su hash SHA-256.

```
software cnf cee
  url file:///data/software/images/cee-2026.01.1.08.tar
  sha256 <CEE-SHA256-HASH>
exit
```

Utilice el valor SHA-256 exacto del paquete aprobado. El marcador de posición del comando es intencional y no representa una suma de comprobación real.

Configuración del clúster y el centro de operaciones

La configuración de origen asocia un clúster a un centro de operaciones SMF, un repositorio local, terminales de gestión y configuración de implementación. Los identificadores específicos del sitio se reemplazan por marcadores de posición.

```
clusters <cluster-name>
  ops-centers smf <smf-ops-center-name>
    app-name-override cn
    repository-local smf-2026.04.m0.i50
    sync-default-repository true
    netconf-ip <NETCONF-IP>
    netconf-port 2029
    ssh-ip <SSH-IP>
    ssh-port 2028
    initial-boot-parameters use-volume-claims true
    initial-boot-parameters auto-deploy false
    initial-boot-parameters single-node false
  exit
exit
```

Parámetro	Significado en la configuración de ejemplo
ops-centers smf <smf-ops-center-name>	Asocia el clúster a la instancia del Centro de operaciones SMF.
repository-local	Especifica el repositorio de aplicaciones y la versión para la implementación.
sync-default-repository true	Utiliza el repositorio predeterminado configurado durante la sincronización.
netconf-port 2029	Especifica el puerto de conectividad de administración de NETCONF.
ssh-port 2028	Especifica el puerto de conectividad de administración de Secure Shell (SSH).
use-volume-Claims true	Habilita el uso de notificaciones de volumen para los requisitos de almacenamiento persistente.
auto-deploy false	Deshabilita la implementación automática para que la sincronización y la validación permanezcan bajo control explícito.
single-node false	Especifica una implementación que no está en modo de nodo único.



Nota: Los identificadores de paquete y repositorio son ejemplos de la configuración de origen. Confirme la compatibilidad de versiones y los valores de extremos antes de utilizarlos en un clúster diferente.

Sincronizar y verificar la implementación

Ejecute la acción de sincronización del clúster después de que el software y la configuración del centro de operaciones estén listos.

```
clusters <cluster-name> actions sync run
```

Inspeccione el estado de sincronización y los registros.

```
clusters <cluster-name> actions sync status
clusters <cluster-name> actions sync logs
```

Confirme que la sincronización se complete correctamente y que los dispositivos y servicios CEE esperados estén implementados.

⚠ Precaución: La sincronización de clústeres y la implementación de software pueden cambiar el entorno en ejecución. Aplique los cambios según el procedimiento de mantenimiento y despliegue aprobado.

Centro de operaciones y gestión operativa de CEE

El Centro de operaciones de CEE proporciona la interfaz operativa para los servicios de CEE. La carga de trabajo admite la administración de usuarios, la autenticación, la configuración y los comandos show para las funciones CEE dentro del clúster. El Administrador de clústeres SMI asocia el Centro de operaciones con la implementación de destino a través de la configuración de administración.

El centro de operaciones pertenece al plano de administración. Prometheus, Alertmanager, Fluent Bit/fluent-proxy, HEC, syslog y OpenTelemetry pertenecen a las trayectorias de monitoreo y telemetría. Mantener estas responsabilidades separadas simplifica la resolución de problemas.

Arquitectura CEE Observability

La observabilidad de CEE incluye métricas, alertas, registros, alertas de CIMC y estadísticas masivas. Estos servicios están relacionados, pero las rutas de datos y los consumidores son diferentes.

Función	Objetivo principal	Destino o consumidor típico
Métrica	Recopile y consulte mediciones de series de tiempo de nodos, Kubernetes y servicios.	Prometeo, Grafana y Thanos.
Alertas	Evaluar reglas de alerta y enrutar eventos de alerta.	Alertmanager, alert-router, Ops Center y receptores externos.
Registros	Reenviar registros de eventos y registros de registros a recopiladores o backends externos.	Splunk y otros recopiladores de registro.
Alertas CIMC	Exportar alertas de Cisco Integrated Management Controller para supervisión.	Indicadores/alertas de CEE y Grafana.
Estadísticas masivas	Cree instantáneas estadísticas periódicas.	Instantáneas CSV y procesamiento o análisis descendente.

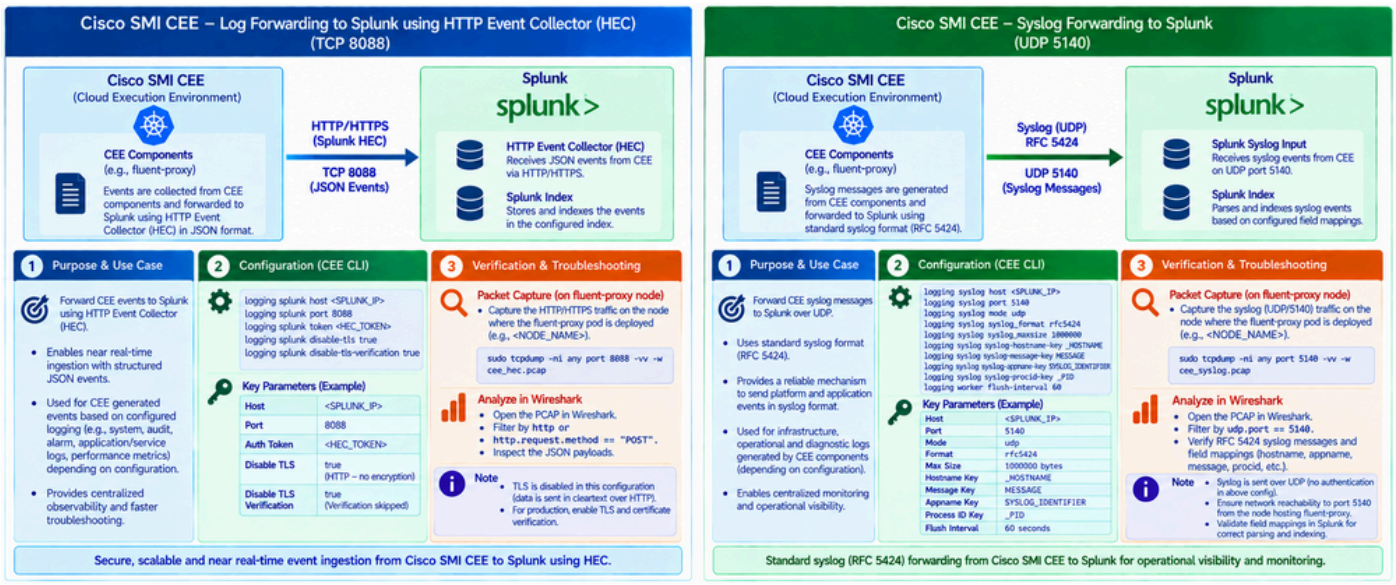
Integración de Splunk: Arquitectura de transferencia de registro

La fuente describe dos trayectorias de CEE a Splunk. Ambos pueden entregar eventos a Splunk, pero utilizan protocolos e interfaces de ingestión distintos.

```
CEE
  |-- logging splunk --> HEC / TCP 8088 --> Splunk HEC input
  |
  +-- logging syslog --> RFC 5424 / UDP 5140 --> Splunk syslog input
```

Los tipos de eventos que transporta cada ruta dependen de la configuración de CEE y de la canalización de reenvío implementada. Dos interfaces configuradas no establecen que cada una lleve una categoría de eventos mutuamente excluyente.

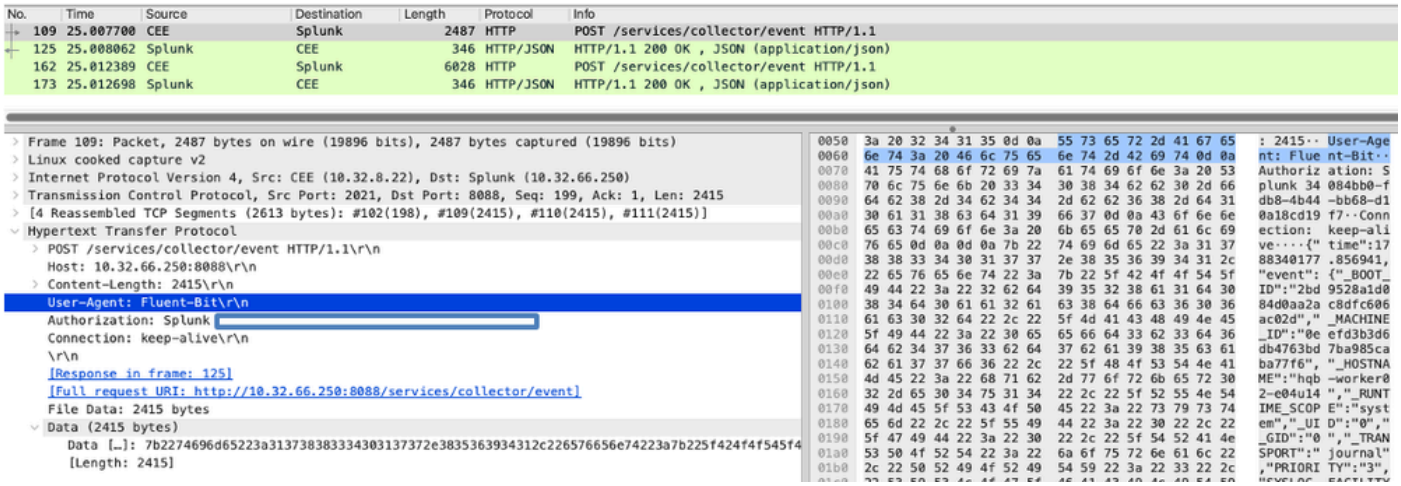
Trace las rutas por separado. La entrega correcta de HEC no confirma la entrega de syslog y la entrega correcta de syslog no confirma la entrega de HEC.



Integración de CEE Splunk con rutas de reenvío HEC y syslog independientes

Reenvío del recopilador de eventos Splunk HTTP

Splunk HEC acepta envíos de eventos HTTP y utiliza un token de autenticación HEC. CEE reenvía los eventos directamente al servicio HEC configurado en lugar de requerir la ingestión basada en archivos para esta ruta.



Arquitectura de reenvío de CEE a Splunk HTTP Event Collector en el puerto TCP 8088

Modelo de configuración de HEC

El ejemplo de laboratorio original contiene estas configuraciones para un punto final de CEE Splunk. El extracto registra el comportamiento de origen y no es una configuración de producción recomendada.

⚠ Precaución: El ejemplo de origen inhabilita la verificación de certificados y TLS. Esto expone la telemetría y las credenciales HEC a la intercepción en la red. Para la producción, habilite la verificación de certificados y TLS, y asegure el token de autenticación HEC de acuerdo con la configuración de la versión de CEE admitida.

```
logging splunk
  <CEE-specific HEC endpoint and authentication parameters>
  disable-tls true
  disable-tls-verification true
```

En la arquitectura de origen, los productores de registros/eventos de CEE envían a través del componente de reenvío Fluent pertinente al destino HEC.

```
CEE log or event source
  |
  v
CEE forwarding service / fluent-proxy
  |
  +-- HTTP(S) HEC over TCP 8088 --> Splunk HEC endpoint
                                      |
                                      v
                                Splunk ingestion tier
                                      |
                                      v
                                Splunk indexing tier
```

Capturar y solucionar problemas de tráfico HEC

Identifique el grupo de dispositivos de proxy fluido y su nodo de trabajo de Kubernetes en el espacio de nombres CEE cuando el proxy fluido transporta el tráfico HEC.

```
kubectl get pods -n <cee-namespace> -o wide | grep fluent-proxy
```

En el nodo Kubernetes que transporta el tráfico HEC, capture paquetes para el puerto HEC.

```
tcpdump -ni any port 8088 -vv -w splunk_hec.pcap
```

Para una conexión con TLS activado, una captura de paquetes revela detalles de establecimiento de transporte y destino, pero normalmente no expone la carga HTTP. Si TLS está desactivado, el contenido del evento y el material de autenticación pueden ser visibles en la captura.

⚠ Precaución: Las capturas y los registros de paquetes pueden contener credenciales y telemetría sensibles. Restrinja la recopilación y la transferencia a flujos de trabajo de asistencia autorizados y proteja los archivos de captura.

Reenvío de Syslog sobre UDP 5140

La segunda ruta de integración de Splunk reenvía los registros de syslog mediante el formato RFC 5424 y el puerto UDP 5140. La configuración de origen también define las asignaciones de campo, el tamaño máximo del mensaje y el intervalo de vaciado del trabajador.

```
logging syslog host <SPLUNK-IP>
logging syslog port 5140
logging syslog mode udp
logging syslog syslog_format rfc5424
logging syslog syslog_maxsize 1000000
logging syslog syslog-hostname-key _HOSTNAME
logging syslog syslog-message-key MESSAGE
logging syslog syslog-appname-key SYSLOG_IDENTIFIER
logging syslog syslog-procid-key _PID
logging worker flush-interval 60
```

Asignación de campos RFC 5424

campo de origen CEE	Campo o propósito de Syslog
_NOMBRE DE HOST	Identifica el host de origen en el registro syslog generado.
MENSAJE	Transporta el cuerpo del mensaje de registro.
SYSLOG_IDENTIFIER	Proporciona la aplicación syslog o el identificador de programa.
_PID	Transporta el identificador de proceso de origen.

Transporte UDP y captura de paquetes

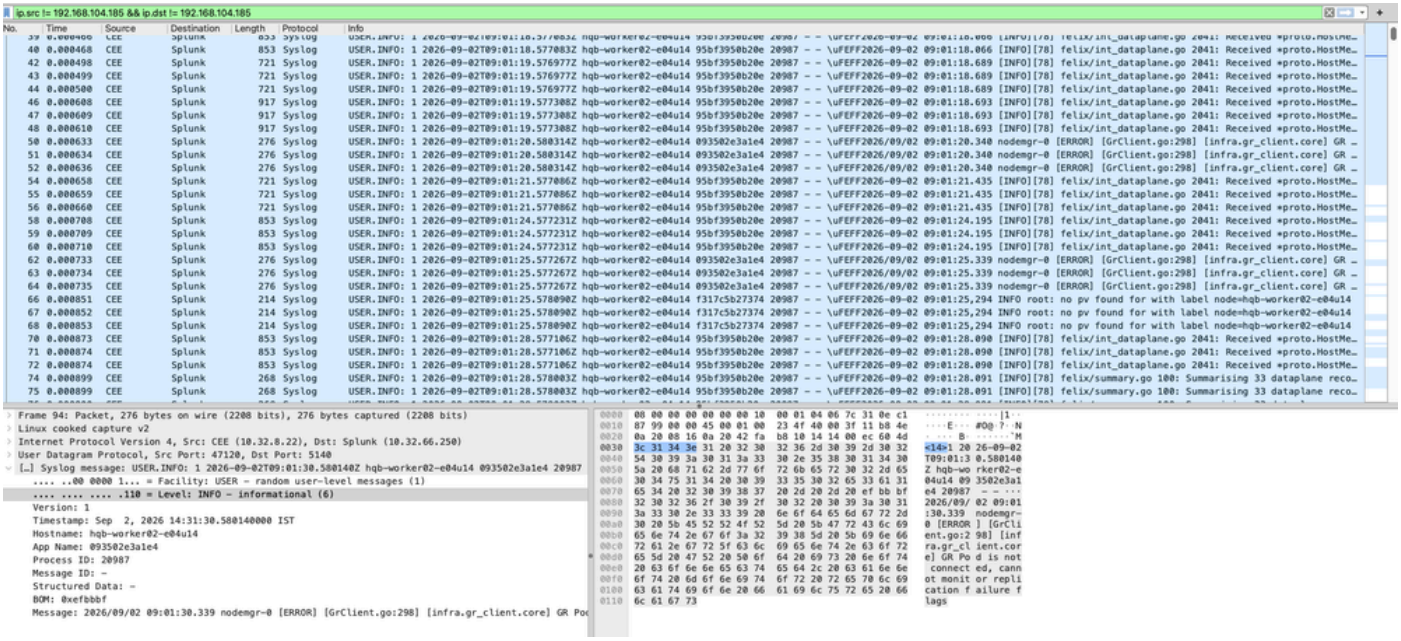
UDP no tiene conexión y no proporciona confirmación de entrega de transporte ni retransmisión. La resolución de problemas debe tener en cuenta la pérdida de paquetes, el routing, la unidad de transmisión máxima (MTU), la fragmentación, la disponibilidad del receptor y el comportamiento de la cola/velocidad.

En la interfaz o el nodo de Kubernetes que transporta el tráfico de syslog, ejecute:

```
tcpdump -ni any udp port 5140 -vv -w splunk_syslog.pcap
```

Si el proxy fluido reenvía el tráfico de syslog, el nodo que aloja ese componente es un punto de captura de paquetes apropiado. Verifique la trayectoria de reenvío antes de recopilar paquetes.

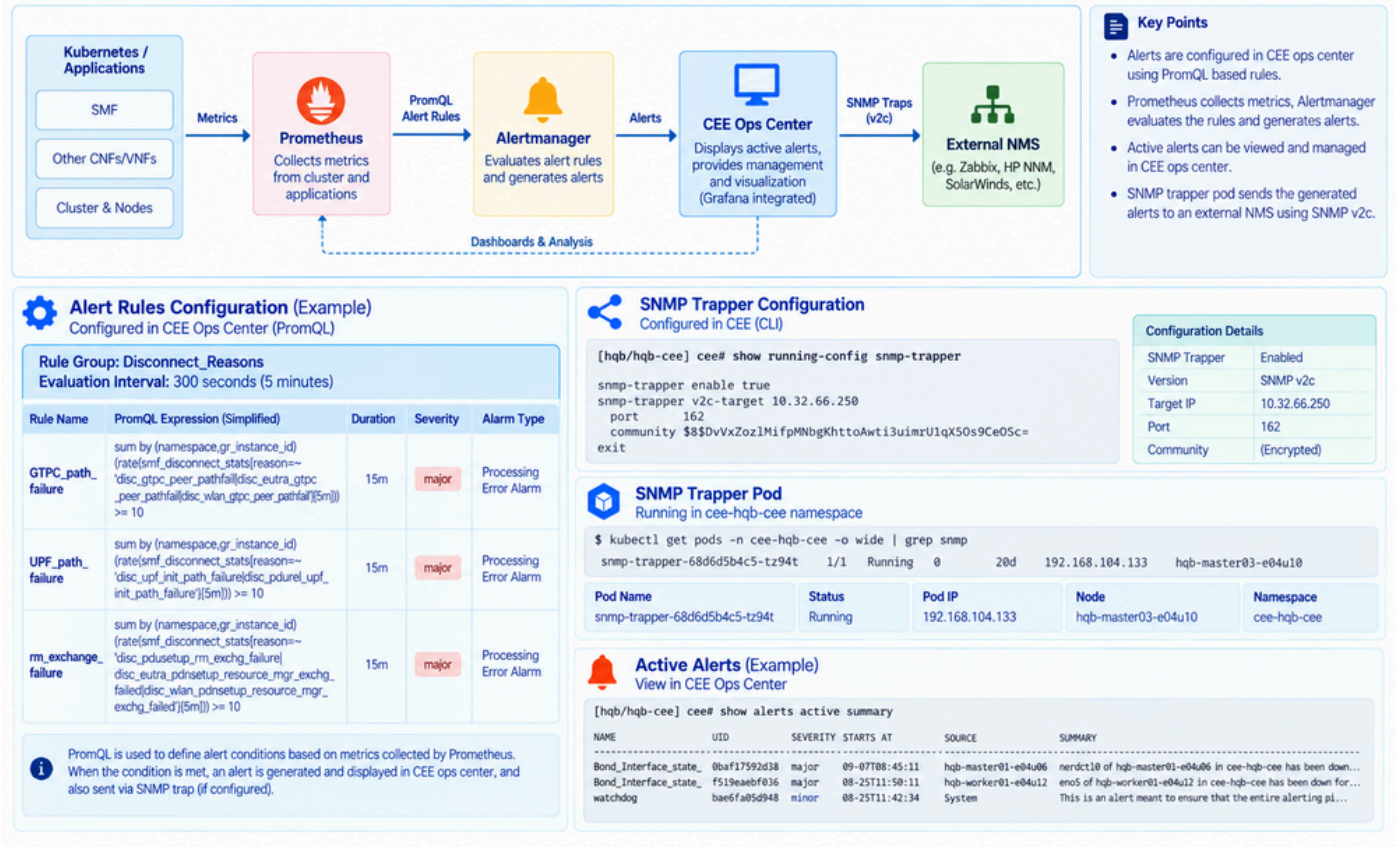
Nota: RFC 5424 define un formato de mensaje syslog independientemente del transporte seleccionado. El escenario de origen utiliza UDP 5140. El transporte de syslog basado en TLS es una opción diferente que requiere una configuración de remitente y receptor compatible.



Reenvío de syslog CEE a Splunk mediante los campos del puerto UDP 5140 y RFC 5424

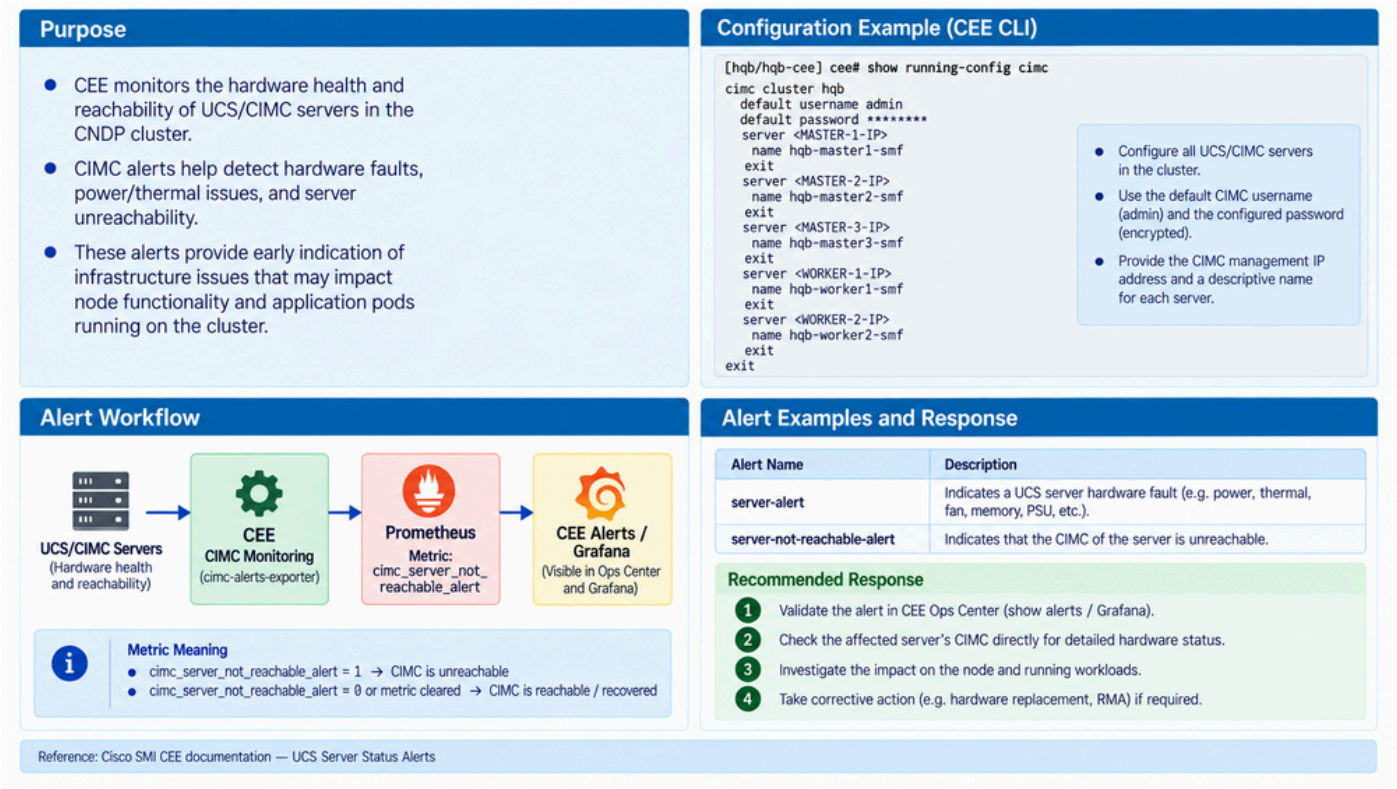
Alertas, SNMP y observabilidad CIMC

Las alertas de CEE utilizan Prometheus y Alertmanager. Prometeo evalúa métricas y reglas de alerta. Alertmanager enruta los eventos de alerta a los receptores, con el router de alerta que proporciona soporte de ruteo adicional. El registrador de alertas de CEE proporciona registros de alertas históricas para su recuperación a través del Centro de Operaciones de CEE.



Reenvío de alertas y arquitectura SNMP de CEE Prometheus y Alertmanager

La integración de alertas CIMC proporciona una ruta de supervisión de la infraestructura relacionada. El cimc-alert-exporter recopila la información de alerta del CIMC y la expone para su monitoreo y visualización en Grafana.

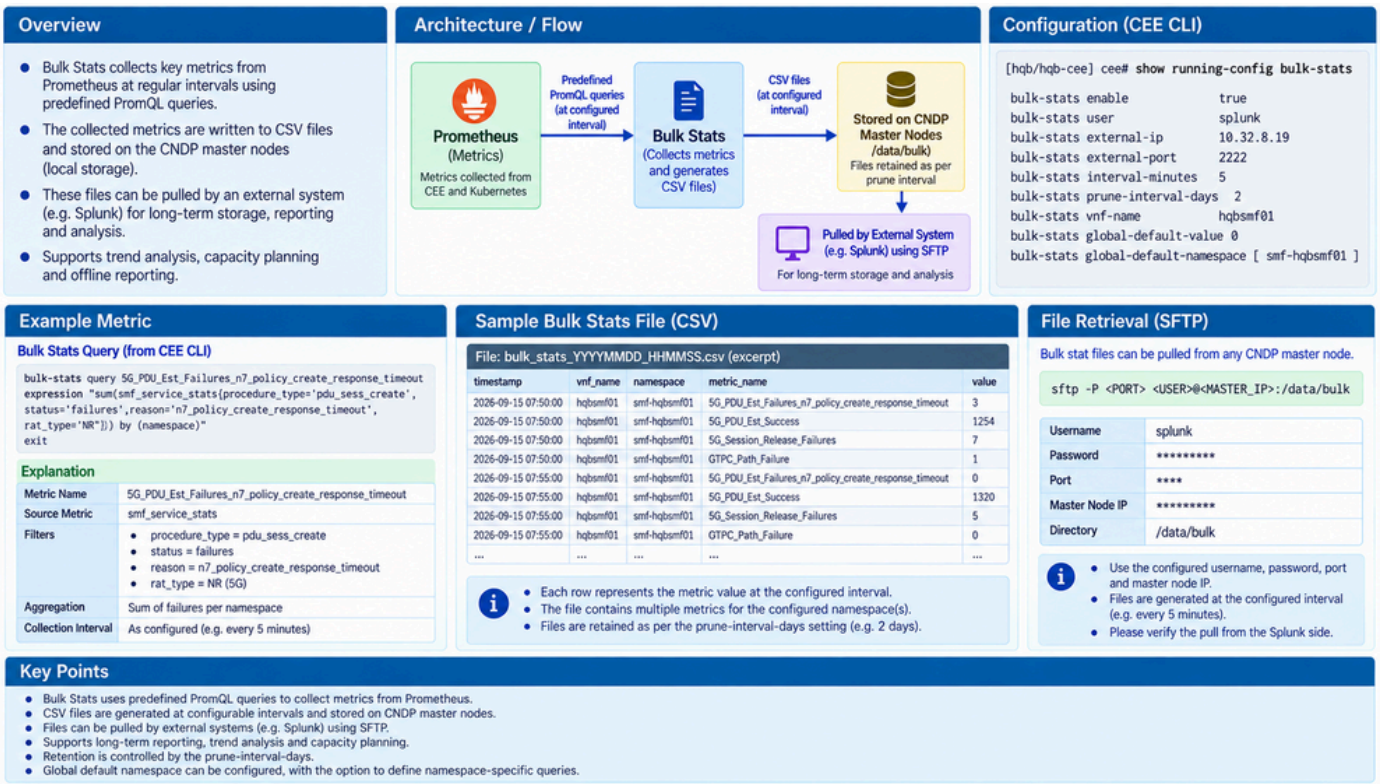


La integración SNMP es una interfaz de alerta y administración; no es intercambiable con Splunk HEC ni con el reenvío de syslog. Las rutas de entrega de protocolos y eventos siguen siendo distintas.

Las referencias relevantes de la Base de información de administración (MIB) incluyen CISCO-CNEE-MIB.my y CISCO-SMI.my.

Estadísticas masivas

El servicio de estadísticas masivas de CEE crea instantáneas periódicas de valores separados por comas (CSV) de las estadísticas recopiladas a través de Prometheus. Se trata de instantáneas estadísticas en lugar de secuencias de registros de registros de aplicaciones.



Servicio de estadísticas masivas de CEE que crea instantáneas CSV periódicas a partir de las métricas de Prometheus

La salida de estadísticas masivas admite informes periódicos, análisis de tendencias y procesamiento de datos descendentes. Incluirlo en una ruta de integración de Splunk solo cuando la implementación reenvíe o importe explícitamente datos CSV/estadísticos a Splunk.

Gateway del sistema OpenTelemetry

Las versiones más recientes de Cisco SMI admiten un gateway de OpenTelemetry Collector gestionado en una plataforma. El gateway recibe telemetría de las aplicaciones a través del protocolo de telemetría abierta (OTLP) y reenvía las métricas y los registros compatibles a los backends locales o remotos.



Nota: La documentación de Cisco SMI Cluster Manager Operations identifica la integración de la puerta de enlace de OpenTelemetry con la versión 2026.03.1. La puerta de enlace no se validó en la implementación específica descrita en el ejemplo de origen, por lo que esta sección describe el modelo de configuración publicado en lugar de la operación verificada en ese entorno.

Modelo de gateway del sistema

```
OpenTelemetry-enabled applications
        |
        | OTLP
        v
CEE OpenTelemetry System Gateway
        |
        +--> Local metrics backend
        +--> Local logging backend
        +--> Remote exporters
                 |
                 +--> OTLP / OTLPHTTP
                 +--> Splunk HEC
                 +--> Other supported destinations
```

Conceptos de configuración de gateway

Active la puerta de enlace de OpenTelemetry Collector y seleccione las métricas locales y los backends de registro.

```
otel-collector gateway enabled
otel-collector gateway system local-backends metrics-enabled true
otel-collector gateway system local-backends logs-enabled true
```

Cuando la implementación requiere la exposición a servicios externos, la configuración puede incluir una IP externa.

```
otel-collector gateway system external-ip <external-ip-address>
```

Los parámetros de proxy opcionales se configuran para los exportadores del gateway.

```
otel-collector gateway system proxy http-proxy http://<proxy-host>:<proxy-port>
otel-collector gateway system proxy https-proxy http://<proxy-host>:<proxy-port>
otel-collector gateway system proxy no-proxy 127.0.0.1,.svc,.cluster.local
```

Las opciones de backend local controlan cómo el gateway del sistema gestionado por la plataforma envía la telemetría a los backends integrados. La configuración de proxy y exposición de IP externa depende de los requisitos de seguridad y topología.

Exportadores remotos

Exportador	Señales	Uso técnico
otlp	Registros, métricas	Enviar telemetría a un servidor que acepte OTLP sobre gRPC.
otlphttp	Registros, métricas	Enviar telemetría a un servidor que acepte OTLP sobre HTTP.
splunkhec	Registros	Envíe registros a un punto final HEC Splunk.
diario	Registros	Escribir registros en el diario de nodos donde se admita.
depurar	Registros, métricas	Compatibilidad con validación controlada y resolución de problemas.

La canalización de OpenTelemetry sigue el modelo de recepción, proceso y exportación. Los receptores ingieren telemetría; los procesadores filtran o transforman los datos; los exportadores envían las señales seleccionadas a los backends remotos o locales.

La fuente también distingue el comportamiento del proxy: otlp utiliza la configuración de proxy de instancia de colector, mientras que otlphttp y splunkhec soportan las invalidaciones de proxy de nivel de exportador donde la versión implementada expone esa configuración.

Comparar con OpenShift OpenTelemetry

Cisco CEE y OpenShift tienen un patrón arquitectónico compartido: un colector de OpenTelemetry puede situarse entre aplicaciones instrumentadas y backends de observabilidad. Sus modelos de gestión e instalación son diferentes.

Concepto	Gateway del sistema CEE OpenTelemetry	patrón OpenShift OpenTelemetry
fuente de telemetría	Cargas de trabajo de aplicaciones y CEE con OpenTelemetry	Cargas de trabajo OpenShift con OpenTelemetry

Concepto	Gateway del sistema CEE OpenTelemetry	patrón OpenShift OpenTelemetry
Protocolo	OTLP	OTLP
Función de recopilador	Gateway del sistema gestionado por la plataforma	Implementación o instancia de OpenTelemetry Collector
Concepto de canalización	Recepción, procesamiento y exportación	Recepción, procesamiento y exportación
Flexibilidad de backend	Backends locales y exportadores remotos admitidos	Integración de back-end impulsada por el exportador
Integración de Splunk	splunkhec exporter en la configuración CEE documentada	Exportador de HEC de Splunk configurado

Esta comparación es arquitectónica. No se afirma que las dos plataformas implementen OpenTelemetry de manera idéntica. OpenShift suele utilizar un modelo de implementación de OpenTelemetry Operator/Collector, mientras que el gateway del sistema Cisco SMI está gestionado por la plataforma.

La arquitectura de referencia de OpenShift descrita en la fuente muestra recopiladores que reenvían telemetría desde cargas de trabajo de Kubernetes hacia Splunk sobre HEC. Ilustra el modelo basado en recopiladores en lugar de una integración verificada para la instalación CEE de ejemplo.

Verifique la Configuración

Verificar sincronización CEE

Revise los registros y el estado de sincronización de SMI Cluster Manager y confirme que se implementan las cargas de trabajo CEE esperadas.

```
clusters <cluster-name> actions sync status
clusters <cluster-name> actions sync logs
```

Verifique HEC y Syslog por separado

Confirme que la trayectoria HEC envía eventos al punto final TCP 8088 configurado y que Splunk los recibe. Confirme por separado que la trayectoria de syslog envía los registros UDP 5140 al receptor configurado.

Utilice los métodos de captura de paquetes en las secciones correspondientes y correlacione las

marcas de tiempo de los paquetes con los eventos recibidos en el colector configurado.

Verificar servicios de observabilidad

Confirme que las métricas, el enrutamiento de alertas, las alertas CIMC y las instantáneas de estadísticas masivas funcionan según lo diseñado para la versión instalada. Si OpenTelemetry está habilitado, verifique el estado del receptor, la canalización y el exportador mediante el procedimiento de operaciones del administrador de clúster SMI admitido.

Comportamiento esperado

Componente o ruta	Resultado esperado
Administrador de clústeres SMI	La sincronización del clúster se completa y se implementan los servicios CEE necesarios.
Centro de operaciones	Los usuarios autorizados pueden acceder a las funciones operativas y a los comandos de configuración/supervisión admitidos.
Splunk HEC	El tráfico del evento llega al receptor HEC configurado en el puerto TCP 8088.
Syslog	Los eventos con formato RFC 5424 llegan al receptor configurado del puerto UDP 5140.
Alertas y CIMC	Alertmanager y los exportadores relacionados exponen la información de alerta configurada.
Estadísticas masivas	Las instantáneas CSV periódicas se generan a partir de las estadísticas recopiladas.
TelemetríaAbierta	En las versiones admitidas con la puerta de enlace configurada, las señales OTLP fluyen a través de la canalización del exportador/servidor seleccionada.

Flujo de decisión

Observación	Próxima comprobación
Los servicios CEE están ausentes después de la sincronización.	Inspeccione el estado de sincronización del Administrador de clústeres, los registros, el artefacto de software y los parámetros del Centro de operaciones.
Faltan eventos de HEC.	Identifique el grupo de dispositivos/nodo de reenvío, verifique el tráfico TCP 8088, el destino HEC, la autenticación y la configuración TLS.
Faltan eventos de Syslog.	Verifique el destino UDP 5140, el formato RFC 5424, el flujo de paquetes y el comportamiento del receptor.
Faltan alertas o datos CIMC.	Verifique el funcionamiento de Prometheus/Alertmanager routing, alert-router y cimc-alert-exporter.
Faltan estadísticas masivas.	Confirme el funcionamiento del servicio de estadísticas masivas,

Observación	Próxima comprobación
	la disponibilidad de datos de Prometheus y la generación de instantáneas de CSV.
Falta la exportación de OpenTelemetry.	Verifique el soporte de funciones para la versión instalada, la configuración de la gateway, el estado del receptor y del exportador y la pertenencia a la canalización.

Conclusión

CEE es un entorno de observabilidad y ejecución basado en niveles de Kubernetes en torno a aplicaciones SMF. La separación del espacio de nombres de Kubernetes divide las operaciones de plataforma, los servicios CEE y las cargas de trabajo de aplicaciones en diferentes dominios. Dentro de CEE, la supervisión, las alertas, el registro y las estadísticas globales son servicios especializados con responsabilidades independientes.

La distinción clave de Splunk es entre HEC sobre TCP 8088 y syslog sobre UDP 5140. Se trata de rutas de reenvío independientes con diferentes protocolos, configuraciones y procedimientos de solución de problemas. La nueva gateway del sistema OpenTelemetry agrega un modelo de colector y exportador basado en OTLP. Su similitud con OpenShift OpenTelemetry es arquitectónica, y se debe verificar el funcionamiento del gateway para la versión e implementación específicas de CEE.

Contenido relacionado

- Guía de configuración y administración de Cisco CEE - Entorno de ejecución común
- Guía de configuración y administración de Cisco CEE - Comandos de registro
- Operaciones de Cisco SMI Cluster Manager - Sincronización y OpenTelemetry
- RFC 5424: protocolo Syslog

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).