# Comprendere l'osservabilità Cisco CEE e l'integrazione Splunk

## Sommario


- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Premesse
- Panoramica dell'architettura
- Carichi di lavoro spazio dei nomi CEE
- Installazione CEE e gestione del ciclo di vita
  - Modalità di installazione
  - Definizione dell'artifact software CEE
  - Configurare il cluster e il centro operativo
  - Sincronizzare e verificare la distribuzione
- Gestione operativa e centro operativo CEE
- Architettura di osservabilità CEE
- Integrazione Splunk: Architettura di trasferimento dei log
- Inoltro agente di raccolta eventi HTTP Splunk
  - Modello di configurazione HEC
  - Acquisizione e risoluzione dei problemi relativi al traffico HEC
- Syslog Forwarding su UDP 5140
  - RFC 5424 - Mappatura campi
  - Trasporto UDP e acquisizione pacchetti
- Osservabilità di avvisi, SNMP e CIMC
- Statistiche in blocco
- OpenTelemetry System Gateway
  - Modello Gateway di sistema
  - Nozioni base sulla configurazione del gateway
  - Esportatori remoti
  - Confronta con OpenShift OpenTelemetry
- Verifica della configurazione
  - Verifica sincronizzazione CEE
  - Verifica separata di HEC e syslog
  - Verifica servizi di osservabilità
- Comportamento previsto
- Flusso decisionale
- Conclusioni
- Contenuto correlato

# Introduzione

Questo documento descrive l'architettura Cisco Common Execution Environment (CEE), l'implementazione, il monitoraggio, l'integrazione di Splunk e OpenTelemetry.

# Prerequisiti

## Requisiti

Cisco consiglia di familiarizzare con queste tecnologie:

- Cloud Native Deployment Platform (CNDP), spazi dei nomi Kubernetes e posizionamento dei pod.
- Cisco Subscriber Microservices Infrastructure (SMI) e SMI Cluster Manager.
- Componenti di CEE Ops Center, Prometheus, Grafana, Alertmanager e log-forwarding.
- HEC (Splunk HTTP Event Collector), syslog e acquisizione pacchetti con tcpdump.
- OpenTelemetry Protocol (OTLP) e OpenTelemetry Collector per l'integrazione del gateway più recente.

## Componenti usati

Gli esempi mostrano un ambiente Cisco SMI/CNDP basato su Kubernetes con CEE e un'applicazione SMF (Session Management Function) associata. L'esempio di definizione del software si riferisce al pacchetto CEE 2026.01.1.08; nell'esempio di Ops Center viene utilizzato un identificativo del repository SMF smf-2026.04.m0.i50. Si tratta di valori di esempio, non di requisiti di distribuzione.

Gli endpoint di rete, i nomi di cluster e i valori dello spazio dei nomi devono essere sostituiti con valori approvati per la distribuzione di destinazione.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

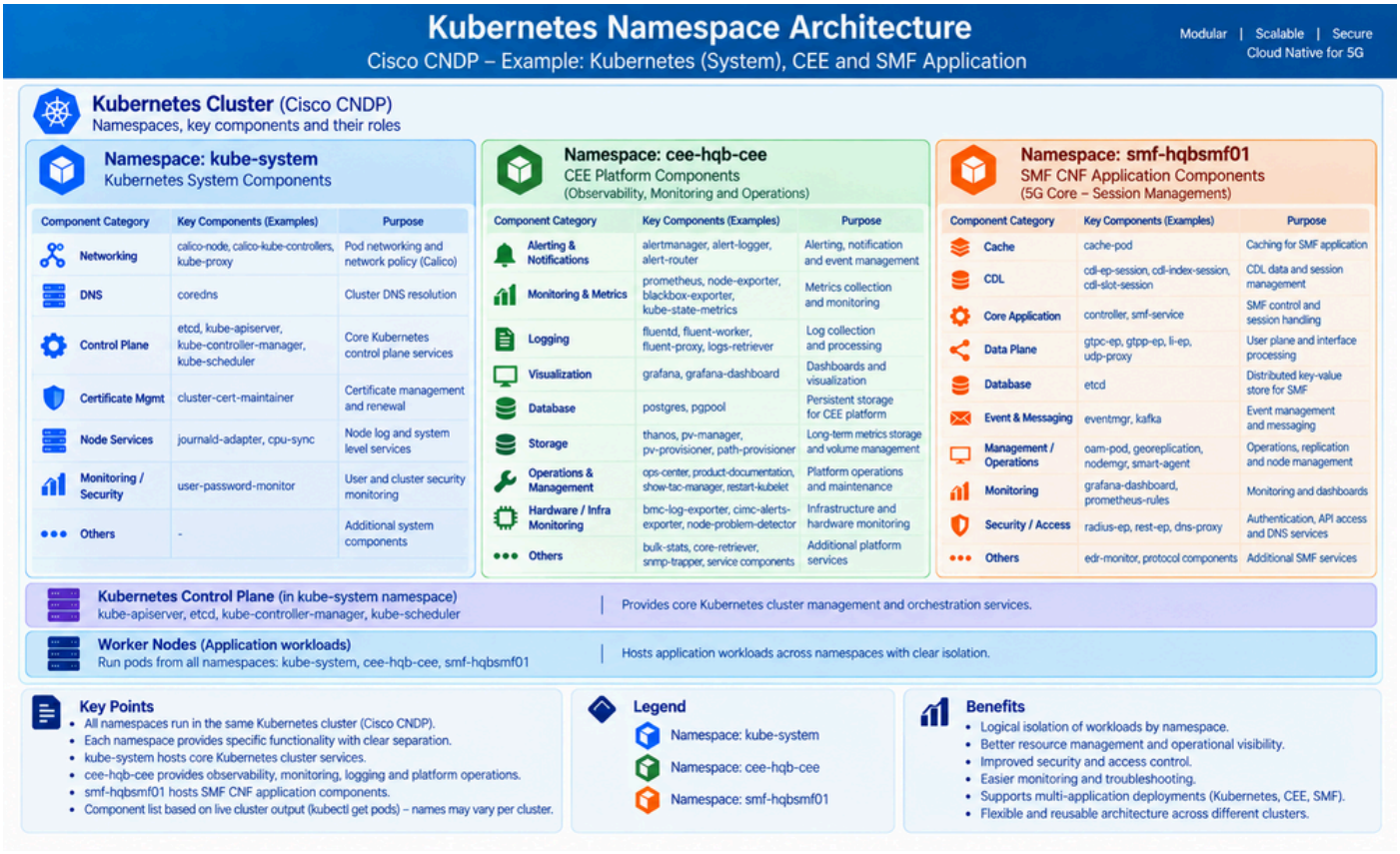
Cisco Common Execution Environment (CEE) fa parte di Cisco Subscriber Microservices Infrastructure (SMI). In un'implementazione CNDP basata su Kubernetes, gli spazi dei nomi Kubernetes prevedono servizi di piattaforma separati, servizi di osservabilità CEE e gestione Kubernetes e carichi di lavoro delle applicazioni SMF. La separazione fornisce i confini amministrativi e operativi mentre le reti Kubernetes e il discovery dei servizi consentono la comunicazione consentita dei componenti.

Questo documento descrive l'architettura dello spazio dei nomi, i carichi di lavoro CEE, l'installazione e la gestione del ciclo di vita CEE, il centro operativo CEE, gli avvisi e il protocollo SNMP (Simple Network Management Protocol), gli avvisi di Cisco Integrated Management Controller (CIMC), l'inoltro dei log, le statistiche di massa e il gateway di sistema OpenTelemetry.

La porta 8088 Splunk HEC sul protocollo TCP (Transmission Control Protocol) e la porta 5140 syslog over User Datagram Protocol (UDP) sono meccanismi di acquisizione indipendenti. I due percorsi hanno requisiti di configurazione, trasporto e risoluzione dei problemi diversi e possono coesistere.

## Panoramica dell'architettura

CEE e le funzioni applicative associate occupano spazi dei nomi Kubernetes separati. L'architettura differenzia i servizi della piattaforma Kubernetes dalle funzioni di osservabilità e gestione CEE e dal dominio dell'applicazione SMF.



Architettura dello spazio dei nomi Cisco SMI che mostra la separazione tra CEE e piattaforma applicativa

Lo spazio dei nomi CEE è l'elemento principale dell'architettura dei livelli di servizio. Altri namespace forniscono la piattaforma Kubernetes, le funzioni di rete e i carichi di lavoro SMF.

## Carichi di lavoro spazio dei nomi CEE

Lo spazio dei nomi CEE ospita microservizi per il monitoraggio, gli avvisi, la registrazione, i dashboard, le statistiche e l'accesso operativo.



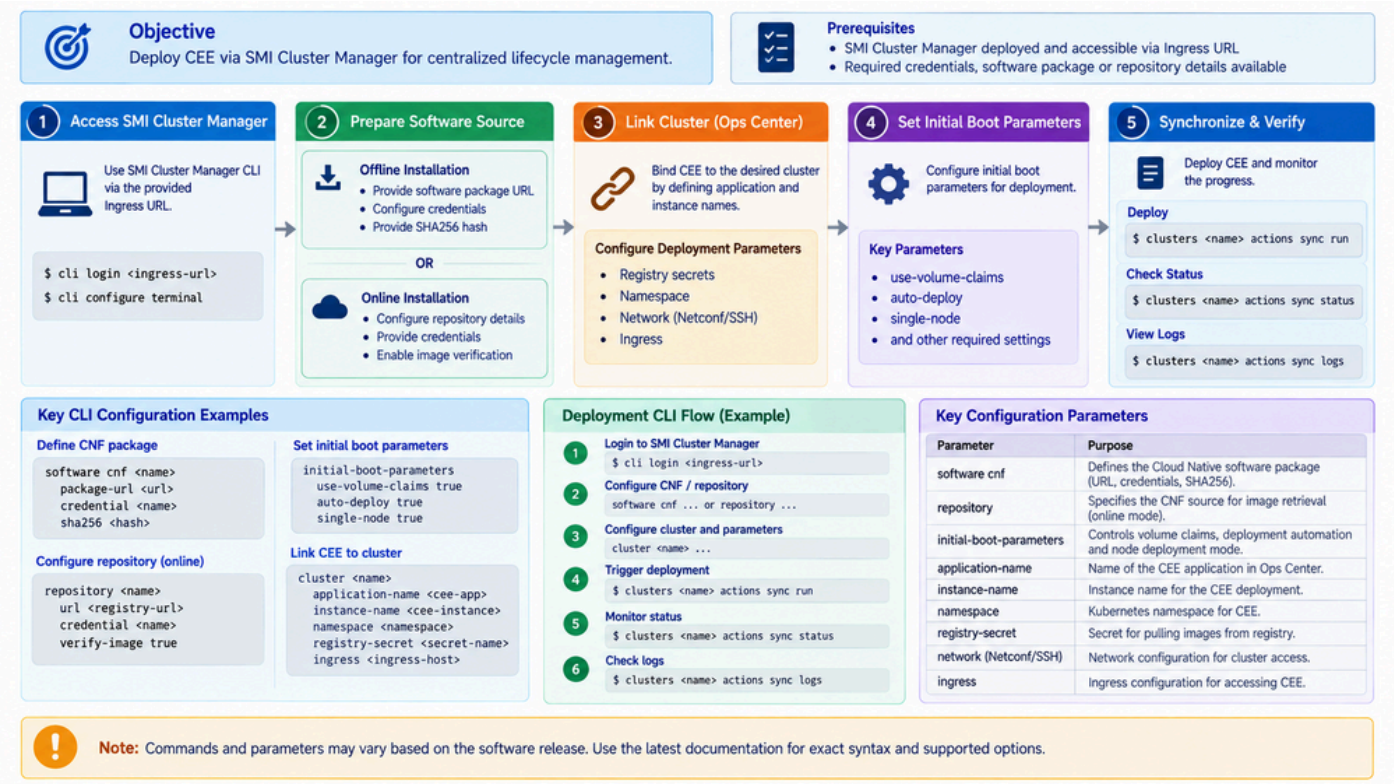

Microservizi dello spazio dei nomi CEE e funzioni dei relativi carichi di lavoro operativi

Queste funzioni includono la raccolta di metriche Prometheus, la visualizzazione Grafana, la gestione degli avvisi Alertmanager, i servizi di inoltro log e la creazione periodica di statistiche di massa. I singoli carichi di lavoro variano in base alla release e alla configurazione di distribuzione.

## Installazione CEE e gestione del ciclo di vita

Gestione cluster SMI separa la definizione dell'artifact software dal cluster di destinazione e dalla relativa configurazione di Centro operativo. Ciò consente il controllo delle versioni del software e la

sincronizzazione ripetibile del cluster.




Installazione CEE di SMI Cluster Manager e architettura di sincronizzazione software

## Modalità di installazione

- L'installazione offline può fare riferimento a un pacchetto software locale tramite un URL di file e un hash SHA-256-bit (Secure Hash Algorithm).
- La configurazione del cluster associa la distribuzione CEE/SMF al cluster e all'istanza di Ops Center previsti.

## Definizione dell'artifact software CEE

Nella configurazione di SMI Cluster Manager, identificare il pacchetto software CEE locale e il relativo hash SHA-256.

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

Utilizzare il valore esatto SHA-256 del pacchetto approvato. Il segnaposto nel comando è

intenzionale e non rappresenta un checksum effettivo.

## Configurare il cluster e il centro operativo

La configurazione di origine associa un cluster a un centro operativo SMF, al repository locale, agli endpoint di gestione e alle impostazioni di distribuzione. Gli identificatori specifici del sito vengono sostituiti con segnaposto.

```
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
```

| Parametro | Significato nella configurazione di esempio |
|---|---|
| ops-center smf <smf-ops-center-name> | Associa il cluster all'istanza di SMF Ops Center. |
| locale del repository | Specifica il repository dell'applicazione e la versione per la distribuzione. |
| sync-default-repository true | Utilizza il repository predefinito configurato durante la sincronizzazione. |
| netconf-port 2029 | Specifica la porta di connettività di gestione NETCONF. |
| ssh-port 2028 | Specifica la porta di connettività di gestione Secure Shell (SSH). |
| use-volume-claim true | Consente l'utilizzo di attestazioni di volume per i requisiti di archiviazione persistente. |
| distribuzione automatica false | Disabilita la distribuzione automatica in modo che la sincronizzazione e la convalida rimangano sotto il controllo esplicito. |
| false a nodo singolo | Specifica una distribuzione che non è in modalità nodo singolo. |



Nota: Gli identificatori di package e repository sono esempi della configurazione di origine. Confermare la compatibilità della versione e i valori degli endpoint prima di utilizzarli in un cluster diverso.

### Sincronizzare e verificare la distribuzione

Eseguire l'azione di sincronizzazione del cluster quando il software e la configurazione di Ops Center sono pronti.

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

Esaminare lo stato della sincronizzazione e i registri.

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

Confermare che la sincronizzazione sia stata completata correttamente e che siano stati distribuiti i servizi e i pod CEE previsti.

---



Attenzione: La sincronizzazione dei cluster e la distribuzione del software possono modificare l'ambiente in esecuzione. Applicare le modifiche in base alla procedura di manutenzione e installazione approvata.

---

## Gestione operativa e centro operativo CEE

CEE Ops Center fornisce l'interfaccia operativa per i servizi CEE. Il carico di lavoro supporta la gestione degli utenti, l'autenticazione, la configurazione e i comandi show per le funzioni CEE all'interno del cluster. Gestione cluster SMI associa il centro operativo alla distribuzione di destinazione tramite la configurazione di gestione.

Il centro operativo appartiene al piano di gestione. Prometeo, Alertmanager, Fluent Bit/fluent-proxy, HEC, syslog e OpenTelemetry appartengono ai percorsi di monitoraggio e telemetria. Mantenere separate queste responsabilità semplifica la risoluzione dei problemi.

## Architettura di osservabilità CEE

L'osservabilità CEE include metriche, avvisi, registri, avvisi CIMC e statistiche di massa. Questi servizi sono correlati, ma i percorsi dei dati e i consumatori sono diversi.

| Funzione | Scopo principale | Destinazione o consumatore tipico |
|---|---|---|
| Metriche | Raccogliere ed eseguire query sulle misure delle serie temporali da nodi, Kubernetes e servizi. | Prometeo, Grafana e Thanos. |
| Avvisi | Valutare le regole di avviso e instradare gli eventi di avviso. | Alertmanager, alert-router, Ops Center e ricevitori esterni. |
| Log | Inoltra i record di log ed eventi agli agenti di raccolta esterni o ai back-end. | Splunk e altri agenti di raccolta log. |
| allarmi CIMC | Esportare gli avvisi di Cisco Integrated Management Controller per il monitoraggio. | Metrics/alerting e Grafana per CEE. |
| Statistiche in blocco | Creare snapshot statistici periodici. | Snapshot CSV ed elaborazione o analisi a valle. |

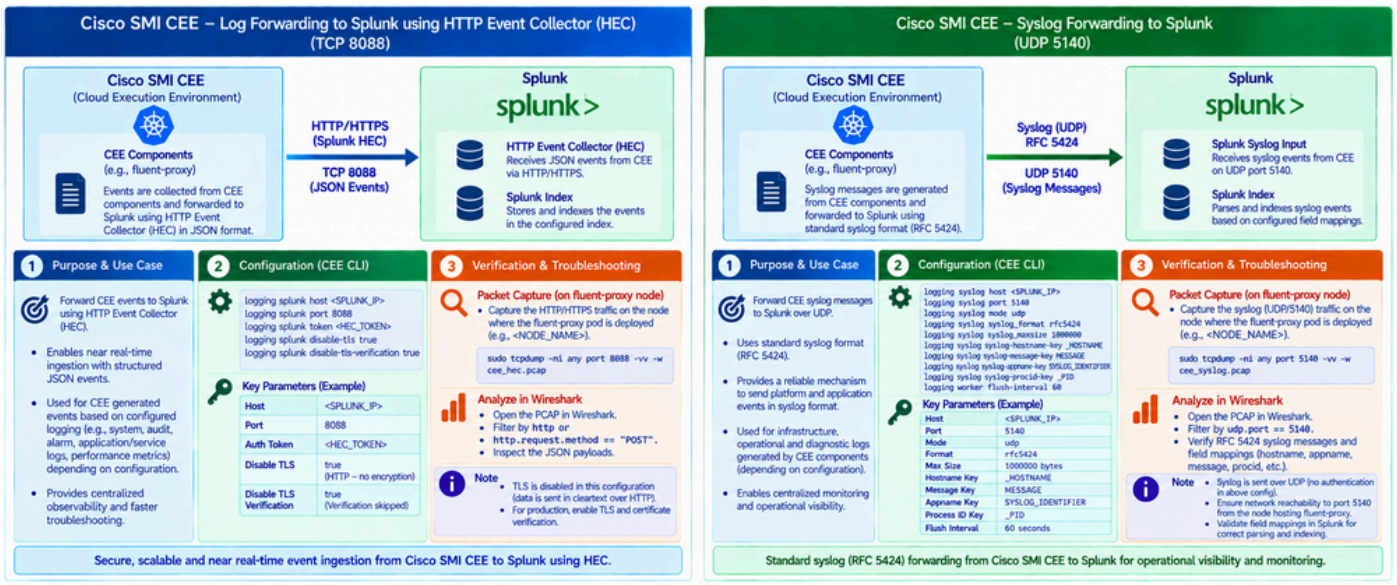
# Integrazione Splunk: Architettura di trasferimento dei log

L'origine descrive due percorsi da CEE a Splunk. Entrambi possono inviare eventi a Splunk, ma utilizzano protocolli e interfacce di acquisizione distinti.

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

I tipi di evento trasportati da ogni percorso dipendono dalla configurazione CEE e dalla pipeline di inoltro implementata. Due interfacce configurate non stabiliscono che ognuna di esse presenti una categoria di eventi che si escludono a vicenda.

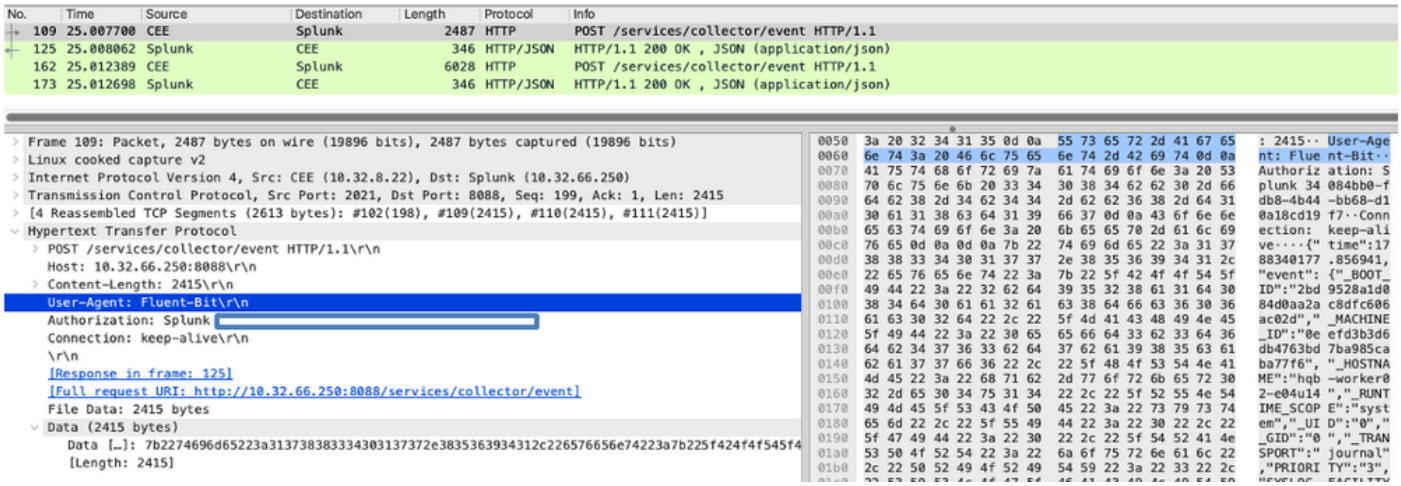
Tracciare i percorsi separatamente. Se il recapito HEC riesce, il recapito non conferma il recapito del syslog e il recapito riuscito del syslog non conferma il recapito dell'HEC.




Integrazione CEE Splunk con percorsi di inoltro HEC e syslog separati

# Inoltro agente di raccolta eventi HTTP Splunk

Splunk HEC accetta l'invio di eventi HTTP e utilizza un token di autenticazione HEC. Il protocollo CEE inoltra gli eventi direttamente al servizio HEC configurato, anziché richiedere l'acquisizione basata su file per questo percorso.




Architettura di inoltro da CEE a Splunk HTTP Event Collector sulla porta TCP 8088

## Modello di configurazione HEC

L'esempio di esercitazione originale contiene queste impostazioni per un endpoint Splunk CEE. Il brano registra il comportamento di origine e non è una configurazione di produzione consigliata.

⚠

Attenzione: Nell'esempio di origine vengono disattivati sia TLS che la verifica dei certificati. Questo espone la telemetria e le credenziali HEC all'intercettazione sulla rete. Per la produzione, abilitare TLS e la verifica dei certificati e proteggere il token di autenticazione HEC in base alla configurazione CEE supportata.

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

Nell'architettura di origine, i produttori di log/eventi CEE inoltrano il componente di inoltro fluente alla destinazione 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
```

## Acquisizione e risoluzione dei problemi relativi al traffico HEC

Identificare il pod fluent-proxy e il relativo nodo di lavoro Kubernetes nello spazio dei nomi CEE quando fluent-proxy trasporta il traffico HEC.

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

Sul nodo Kubernetes che trasporta il traffico HEC, catturare i pacchetti per la porta HEC.

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

Per una connessione abilitata per TLS, l'acquisizione di un pacchetto rivela i dettagli sulla destinazione e sull'istituzione del trasporto, ma in genere non espone il payload HTTP. Se TLS è disattivato, il contenuto degli eventi e il materiale di autenticazione possono essere visualizzati nell'acquisizione.

---

⚠ Attenzione: Le acquisizioni e i log dei pacchetti possono contenere dati di telemetria e credenziali riservate. Limitare la raccolta e il trasferimento ai workflow di supporto autorizzati e proteggere i file di acquisizione.

---

# Syslog Forwarding su UDP 5140

Il secondo percorso di integrazione Splunk inoltra i record syslog utilizzando la formattazione RFC 5424 e la porta UDP 5140. La configurazione di origine definisce inoltre i mapping dei campi, le dimensioni massime dei messaggi e l'intervallo di scaricamento del worker.

```
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
```

## RFC 5424 - Mappatura campi

| Campo origine CEE | Scopo o campo Syslog |
|---|---|
| _NOME HOST | Identifica l'host di origine nel record syslog generato. |
| MESSAGGIO | Trasporta il corpo del messaggio di log. |
| IDENTIFICATORE_SYSLOG | Fornisce l'identificatore dell'applicazione o del programma syslog. |
| _PID | Trasporta l'identificativo del processo di origine. |

## Trasporto UDP e acquisizione pacchetti

UDP è privo di connessione e non fornisce né conferma della consegna del trasporto né ritrasmissione. La risoluzione dei problemi deve tenere conto della perdita di pacchetti, del routing, dell'MTU (Maximum Transmission Unit), della frammentazione, della disponibilità del ricevitore e del comportamento di coda/velocità.

Sull'interfaccia o sul nodo Kubernetes che trasmette il traffico syslog, eseguire:

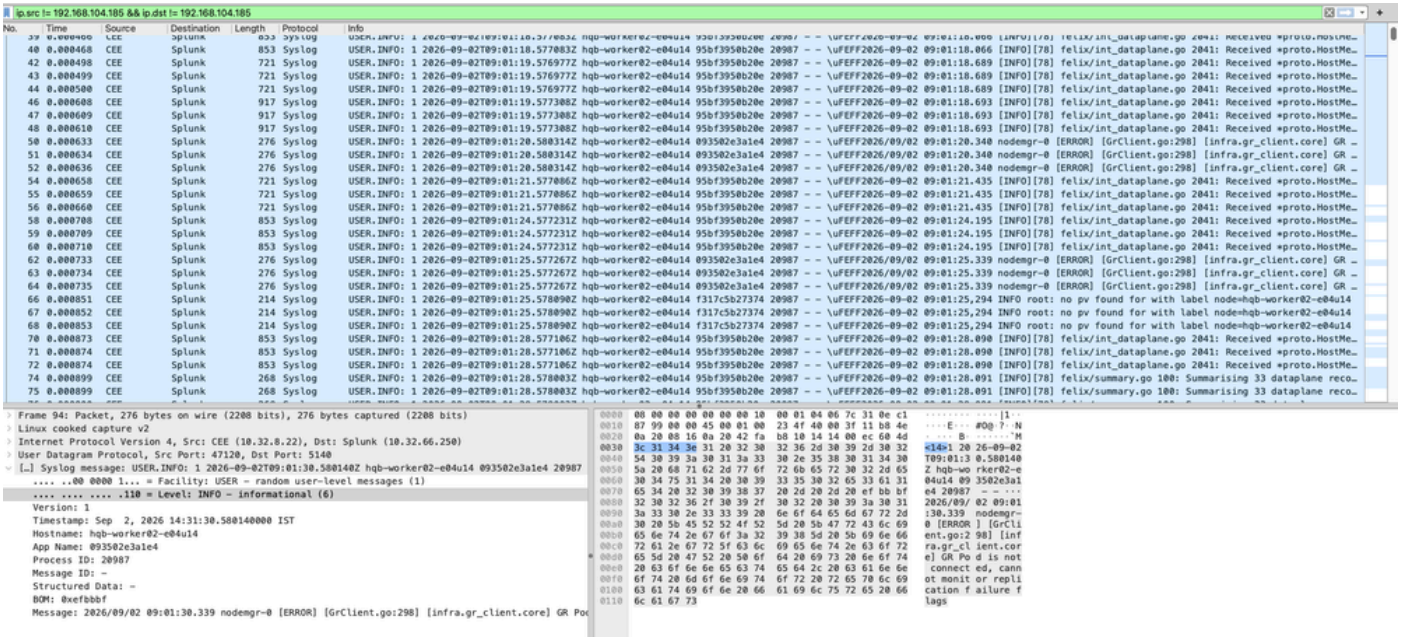
```
tcpdump -ni any udp port 5140 -vv -w splunk_syslog.pcap
```

Se il proxy fluent inoltra il traffico syslog, il nodo che ospita il componente è un punto di acquisizione del pacchetto appropriato. Verificare il percorso di inoltro prima di raccogliere i pacchetti.

---

Nota: La RFC 5424 definisce un formato di messaggio syslog indipendente dal trasporto selezionato. Nello scenario di origine viene utilizzato UDP 5140. Il trasporto syslog basato su TLS è un'opzione diversa che richiede una configurazione compatibile del mittente e del destinatario.

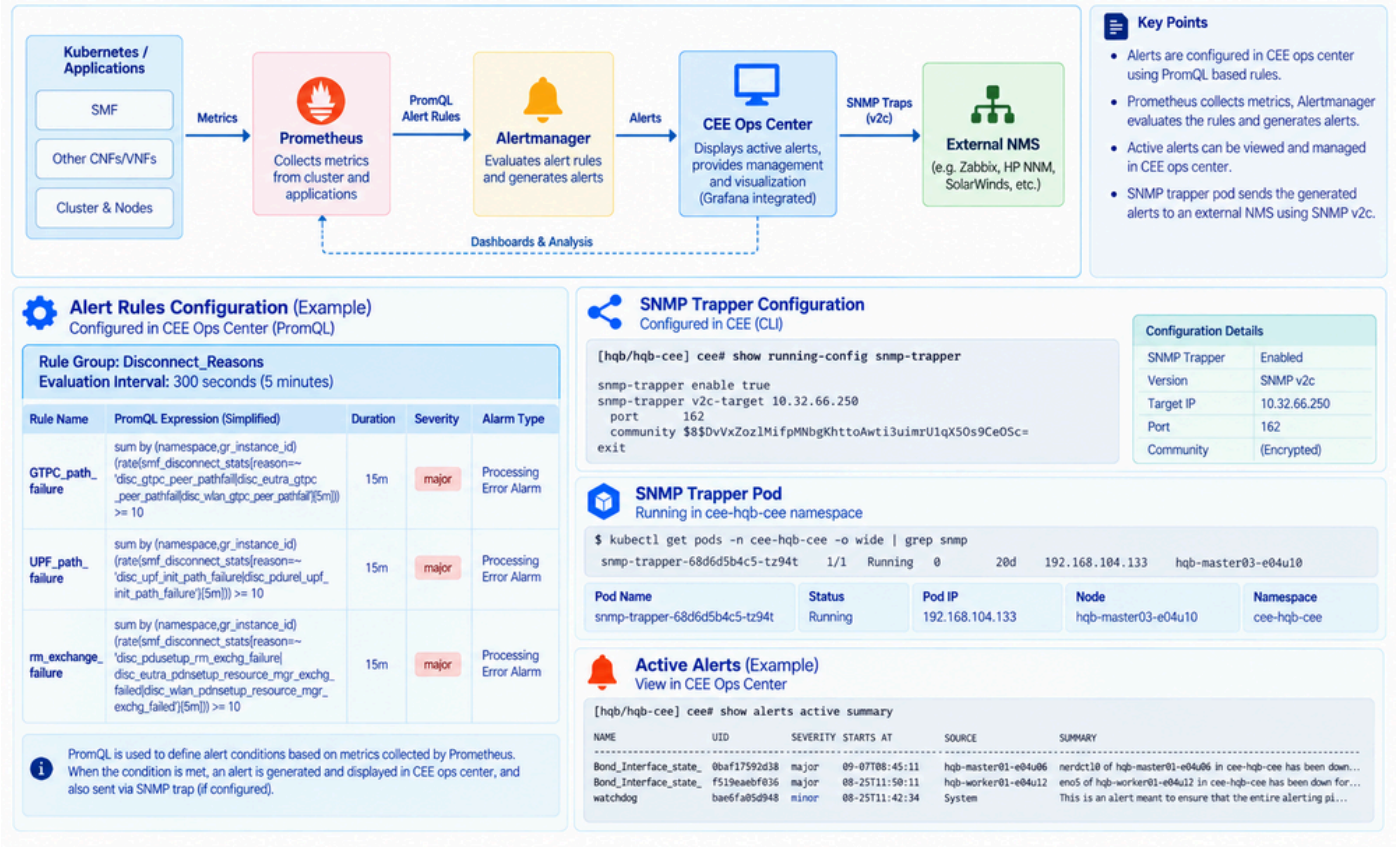
---




CEE syslog forwarding su Splunk con campi della porta UDP 5140 e RFC 5424

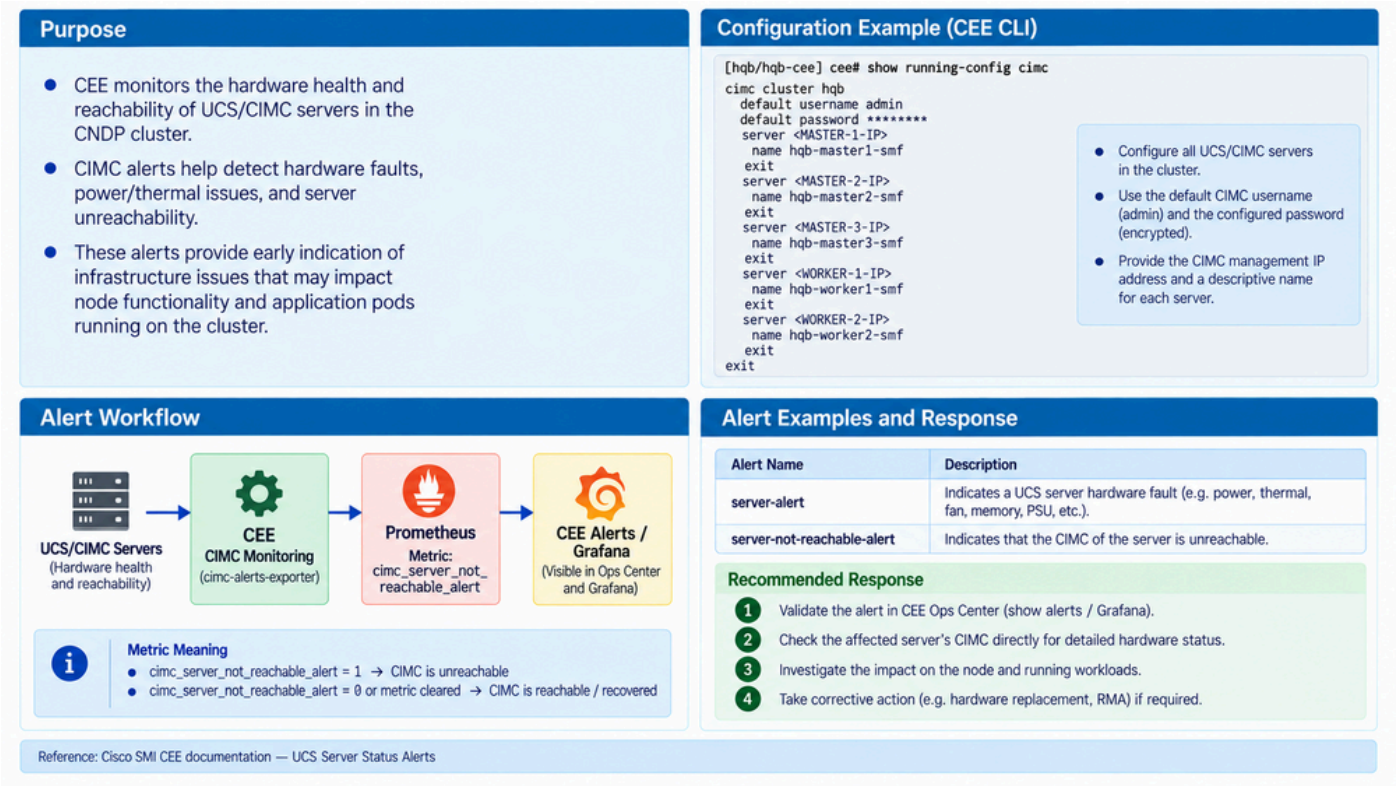
# Osservabilità di avvisi, SNMP e CIMC

Gli avvisi CEE utilizzano Prometheus e Alertmanager. Prometheus valuta le metriche e le regole di avviso. Alertmanager instrada gli eventi di allarme ai ricevitori, con alert-router che fornisce ulteriore supporto di routing. L'alert logger CEE fornisce record cronologici degli alert per il recupero tramite il Centro operativo CEE.




Architettura SNMP e inoltro avvisi CEE Prometheus e Alertmanager

L'integrazione degli avvisi CIMC fornisce un percorso di monitoraggio dell'infrastruttura correlato. Il cimc-alert-export raccoglie le informazioni sugli alert CIMC e le espone per il monitoraggio e la visualizzazione in Grafana.

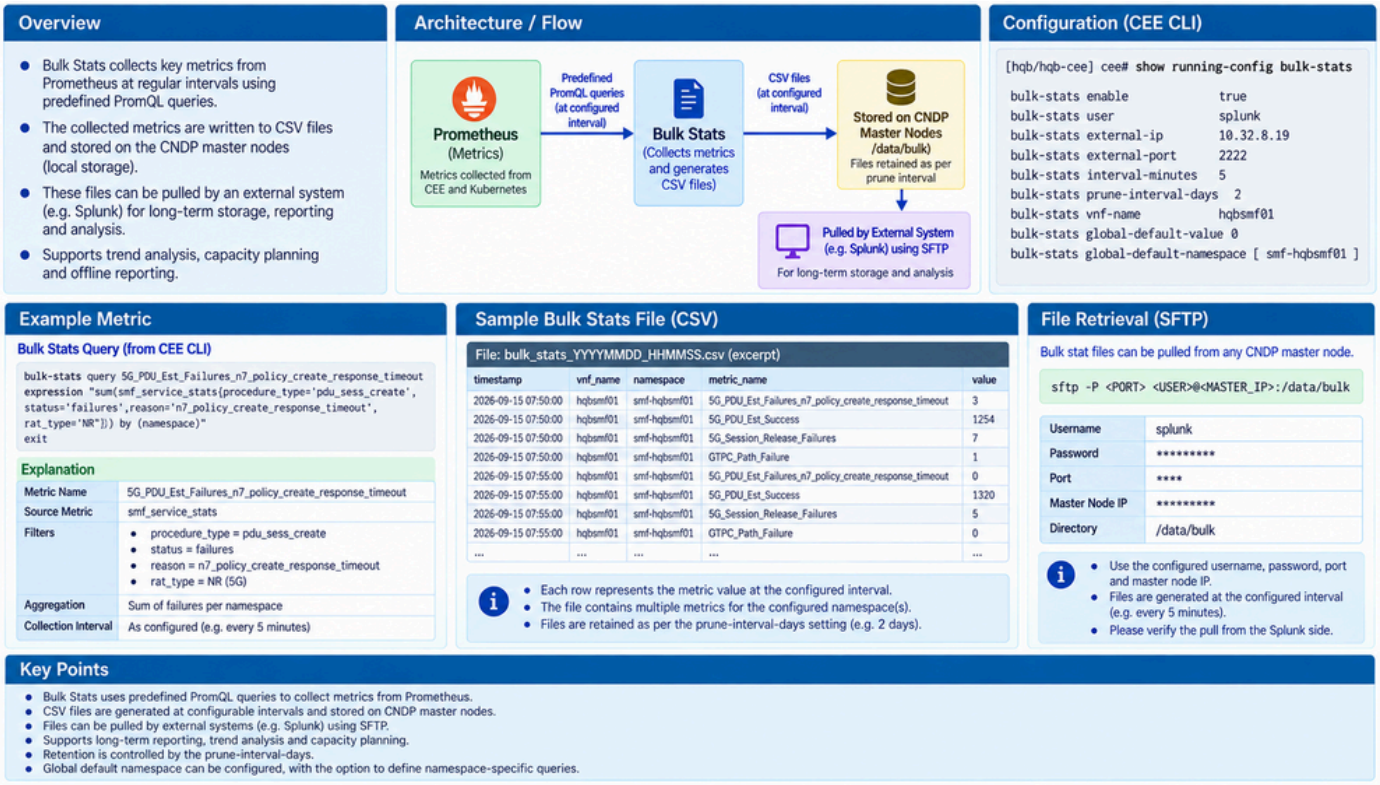


L'integrazione SNMP è un'interfaccia di gestione degli allarmi; non è intercambiabile con l'inoltro Splunk HEC o syslog. Il protocollo e i percorsi di recapito degli eventi rimangono distinti.

I riferimenti MIB (Management Information Base) pertinenti includono CISCO-CNEE-MIB.my e CISCO-SMI.my.

## Statistiche in blocco

Il servizio di statistiche cumulative CEE crea periodicamente snapshot CSV (Comma-Separated Values) delle statistiche raccolte tramite Prometheus. Si tratta di snapshot statistici anziché di flussi di record di log delle applicazioni.




Servizio statistiche di massa CEE per la creazione di snapshot CSV periodiche dalle metriche di Prometheus

L'output di tipo Bulk-statistics supporta la creazione di report periodici, l'analisi delle tendenze e l'elaborazione dei dati a valle. Includerlo in un percorso di integrazione Splunk solo quando la distribuzione inoltra o importa esplicitamente i dati CSV/statistici in Splunk.

## OpenTelemetry System Gateway

Le versioni più recenti di Cisco SMI supportano un gateway OpenTelemetry Collector gestito da piattaforma. Il gateway riceve la telemetria dalle applicazioni tramite il protocollo OTLP (OpenTelemetry Protocol) e inoltra le metriche e i log supportati ai back-end locali o remoti.

---



Nota: La documentazione relativa alle operazioni di Cisco SMI Cluster Manager identifica l'integrazione del gateway OpenTelemetry con la versione 2026.03.1. Il gateway non è stato convalidato nella distribuzione specifica descritta dall'esempio di origine, quindi in questa sezione viene descritto il modello di configurazione pubblicato anziché il funzionamento verificato in tale ambiente.

---

## Modello Gateway di 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
```

## Nozioni base sulla configurazione del gateway

Abilitare il gateway di OpenTelemetry Collector e selezionare le metriche locali e i back-end di log.

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

Se l'installazione richiede l'esposizione del servizio esterno, la configurazione può includere un indirizzo IP esterno.

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

Per gli esportatori del gateway sono configurate impostazioni proxy facoltative.

```
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
```

Le opzioni di back-end locale controllano il modo in cui il gateway di sistema gestito dalla piattaforma invia la telemetria ai back-end integrati. L'esposizione IP esterna e le impostazioni proxy dipendono dalla topologia e dai requisiti di sicurezza.

## Esportatori remoti

| Esportatore | Segnali | Uso tecnico |
|---|---|---|
| alto | Registri, metriche | Invia la telemetria a un back-end che accetta OTLP su gRPC. |
| otlphttp | Registri, metriche | Invia la telemetria a un back-end che accetta OTLP su HTTP. |
| splunkhec | Log | Invia i registri a un endpoint HEC Splunk. |
| diario | Log | Scrivere i log nel journal dei nodi, se supportato. |
| debug | Registri, metriche | Supportare la convalida controllata e la risoluzione dei problemi. |

La pipeline OpenTelemetry segue il modello di ricezione, elaborazione ed esportazione. I ricevitori ricevono la telemetria; i processori filtrano o trasformano i dati; inviano i segnali selezionati a back-end remoti o locali.

L'origine distingue anche il comportamento proxy: otlp utilizza le impostazioni del proxy dell'istanza del collector, mentre otlphttp e splunkhec supportano le impostazioni del proxy a livello di export che sostituiscono la release distribuita per esporre tale configurazione.

## Confronta con OpenShift OpenTelemetry

Cisco CEE e OpenShift hanno un modello di architettura condiviso: un OpenTelemetry Collector può essere posizionato tra applicazioni instrumentate e back-end di osservabilità. I modelli di gestione e installazione sono diversi.

| Concetto | Gateway di sistema OpenTelemetry CEE | OpenShift Motivo OpenTelemetry |
|---|---|---|
| Origine telemetria | Carichi di lavoro CEE e applicazioni abilitati per OpenTelemetry | Carichi di lavoro OpenShift abilitati per Telemetria |
| Protocollo | OTLP | OTLP |
| Ruolo agente di raccolta | Gateway di sistema gestito da piattaforma | Distribuzione o istanza di OpenTelemetry Collector |
| Concetto di tubazione | Ricezione, elaborazione ed esportazione | Ricezione, elaborazione ed esportazione |

| Concetto | Gateway di sistema OpenTelemetry CEE | OpenShift Motivo OpenTelemetry |
|---|---|---|
| Flessibilità back-end | Back-end locali ed esportatori remoti supportati | Integrazione back-end basata su esportazione |
| Integrazione con Splunk | splunkhec export nella configurazione CEE documentata | Esportatore HEC Splunk se configurato |

Questo confronto è architettonico. Non si pretende che le due piattaforme implementino OpenTelemetry in modo identico. OpenShift in genere utilizza un modello di distribuzione OpenTelemetry Operator/Collector, mentre il gateway di sistema Cisco SMI è gestito tramite piattaforma.

L'architettura di riferimento OpenShift discussa nella fonte mostra i collettori che inoltrano la telemetria dai carichi di lavoro Kubernetes verso Splunk over HEC. Illustra il modello basato su collector piuttosto che un'integrazione verificata per l'installazione CEE di esempio.

# Verifica della configurazione

## Verifica sincronizzazione CEE

Esaminare i registri e lo stato di sincronizzazione di Gestione cluster SMI e verificare che siano stati distribuiti i carichi di lavoro CEE previsti.

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

## Verifica separata di HEC e syslog

Confermare che il percorso HEC invii gli eventi all'endpoint TCP 8088 configurato e che lo Splunk li riceva. Confermare separatamente che il percorso syslog invia i record UDP 5140 al listener configurato.

Utilizzare i metodi di acquisizione dei pacchetti nelle sezioni corrispondenti e correlare i timestamp dei pacchetti agli eventi ricevuti dall'agente di raccolta configurato.

## Verifica servizi di osservabilità

Verificare che le metriche, il routing degli avvisi, gli avvisi CIMC e gli snapshot di statistiche globali funzionino come previsto per la release installata. Se OpenTelemetry è abilitato, verificare

l'integrità del ricevitore, della pipeline e dell'utilità di esportazione utilizzando la procedura operativa supportata di Gestione cluster SMI.

## Comportamento previsto

| Componente o percorso | Risultato previsto |
|---|---|
| Gestione cluster SMI | La sincronizzazione del cluster è stata completata e i servizi CEE richiesti sono stati distribuiti. |
| Centro operativo | Gli utenti autorizzati possono accedere alle funzioni operative e ai comandi di configurazione/monitoraggio supportati. |
| HEC Splunk | Il traffico di eventi raggiunge il listener HEC configurato sulla porta TCP 8088. |
| Syslog | Gli eventi formattati con RFC 5424 raggiungono il listener della porta UDP 5140 configurato. |
| Avvisi e CIMC | Alertmanager ed esportatori correlati espongono le informazioni sugli avvisi configurate. |
| Statistiche in blocco | Gli snapshot CSV periodici vengono generati dalle statistiche raccolte. |
| TelemetriaAperta | Nelle versioni supportate con il gateway configurato, i segnali OTLP passano attraverso la pipeline back-end/esportazione selezionata. |

## Flusso decisionale

| Osservazione | Controllo successivo |
|---|---|
| I servizi CEE sono assenti dopo la sincronizzazione. | Esaminare lo stato di sincronizzazione di Cluster Manager, i log, gli elementi software e i parametri di Ops Center. |
| Eventi HEC mancanti. | Identificare il pod/nodo di inoltro, verificare il traffico TCP 808, la destinazione HEC, l'autenticazione e la configurazione TLS. |
| Eventi syslog mancanti. | Verificare la destinazione UDP 5140, la formattazione RFC 5424, il flusso del pacchetto e il comportamento del destinatario. |
| Avvisi o dati CIMC mancanti. | Verificare le operazioni di routing tra Prometeo e Alertmanager, alert-router e cimc-alert-export. |
| Statistiche di massa mancanti. | Confermare l'operazione del servizio bulk-stats, la disponibilità dei dati Prometheus e la generazione di snapshot CSV. |
| Esportazione OpenTelemetry mancante. | Verificare il supporto delle funzionalità per la versione installata, la configurazione del gateway, lo stato del ricevitore e dell'esportatore e l'appartenenza alla pipeline. |

## Conclusioni

CEE è un ambiente di esecuzione e di osservazione su più livelli basato su Kubernetes relativo

alle applicazioni SMF. La separazione dei namespace di Kubernetes divide le operazioni di piattaforma, i servizi CEE e i carichi di lavoro delle applicazioni in domini diversi. All'interno di CEE, il monitoraggio, gli allarmi, il logging e le statistiche di massa sono servizi specializzati con responsabilità indipendenti.

La distinzione chiave per lo splunk è tra HEC su TCP 8088 e syslog su UDP 5140. Si tratta di percorsi di inoltro separati con protocolli, configurazioni e procedure di risoluzione dei problemi diversi. Il nuovo gateway di sistema OpenTelemetry aggiunge un modello di esportazione e raccoglitore basato su OTLP. La sua somiglianza con OpenShift OpenTelemetry è di architettura e il funzionamento del gateway deve essere verificato per la release e la distribuzione CEE specifica.

## Contenuto correlato

- Guida alla configurazione e amministrazione di Cisco CEE - Common Execution Environment
- Guida alla configurazione e amministrazione di Cisco CEE - Comandi di registrazione
- Operazioni Cisco SMI Cluster Manager - Sincronizzazione e OpenTelemetry
- RFC 5424 - Protocollo Syslog

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).