Entender a capacidade de observação e integração de Splunk do Cisco CEE

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Visão geral da arquitetura
- Cargas de trabalho de namespace de CEE
- Instalação e gerenciamento do ciclo de vida do CEE
  - Modos de instalação
  - Definir o artefato de software CEE
  - Configurar o Cluster e o Centro de Operações
  - Sincronizar e verificar a implantação
- Centro de operações e gerenciamento operacional do CEE
- Arquitetura de observação CEE
- Integração do Splunk: Arquitetura de transferência de registros
- Encaminhamento do Coletor de Eventos HTTP de Splunk
  - Modelo de configuração HEC
  - Capturar e solucionar problemas de tráfego HEC
- Encaminhamento de Syslog via UDP 5140
  - Mapeamento de campo RFC 5424
  - Transporte UDP e captura de pacotes
- Alertas, SNMP e capacidade de observação do CIMC
- Estatísticas em Massa
- Gateway do sistema OpenTelemetry
  - Modelo de gateway do sistema
  - Conceitos de configuração de gateway
  - Exportadores remotos
  - Compare com OpenShift OpenTelemetry
- Verificar a configuração
  - Verificar sincronização de CEE
  - Verificar HEC e Syslog separadamente
  - Verificar os serviços de observação
- Comportamento esperado
- Fluxo de decisão
- Conclusão
- Conteúdo relacionado

Introdução

Este documento descreve a arquitetura Cisco Common Execution Environment (CEE), implantação, monitoramento, integração Splunk e OpenTelemetry.

Pré-requisitos

Requisitos

A Cisco recomenda familiaridade com estas tecnologias:

- Plataforma de Implantação Nativa em Nuvem (CNDP - Cloud Native Deployment Platform), namespaces Kubernetes e colocação de pods.
- Cisco Subscriber Microservices Infrastructure (SMI) e o SMI Cluster Manager.
- CEE Ops Center, Prometheus, Grafana, Alertmanager e componentes de encaminhamento de registros.
- Coletor de Eventos HTTP (HEC) de Splunk, syslog e captura de pacotes com tcpdump.
- OpenTelemetry Protocol (OTLP) e OpenTelemetry Collector para a integração de gateway mais recente.

Componentes Utilizados

Os exemplos mostram um ambiente Cisco SMI/CNDP baseado no Kubernetes com CEE e uma aplicação Session Management Function (SMF) associada. O exemplo de definição de software refere-se ao pacote CEE 2026.01.1.08; o exemplo do Ops Center usa um identificador de repositório SMF smf-2026.04.m0.i50. Esses são valores de exemplo, não requisitos de disponibilização.

Endpoints de rede, nomes de cluster e valores de namespace devem ser substituídos por valores aprovados para a implantação de destino.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

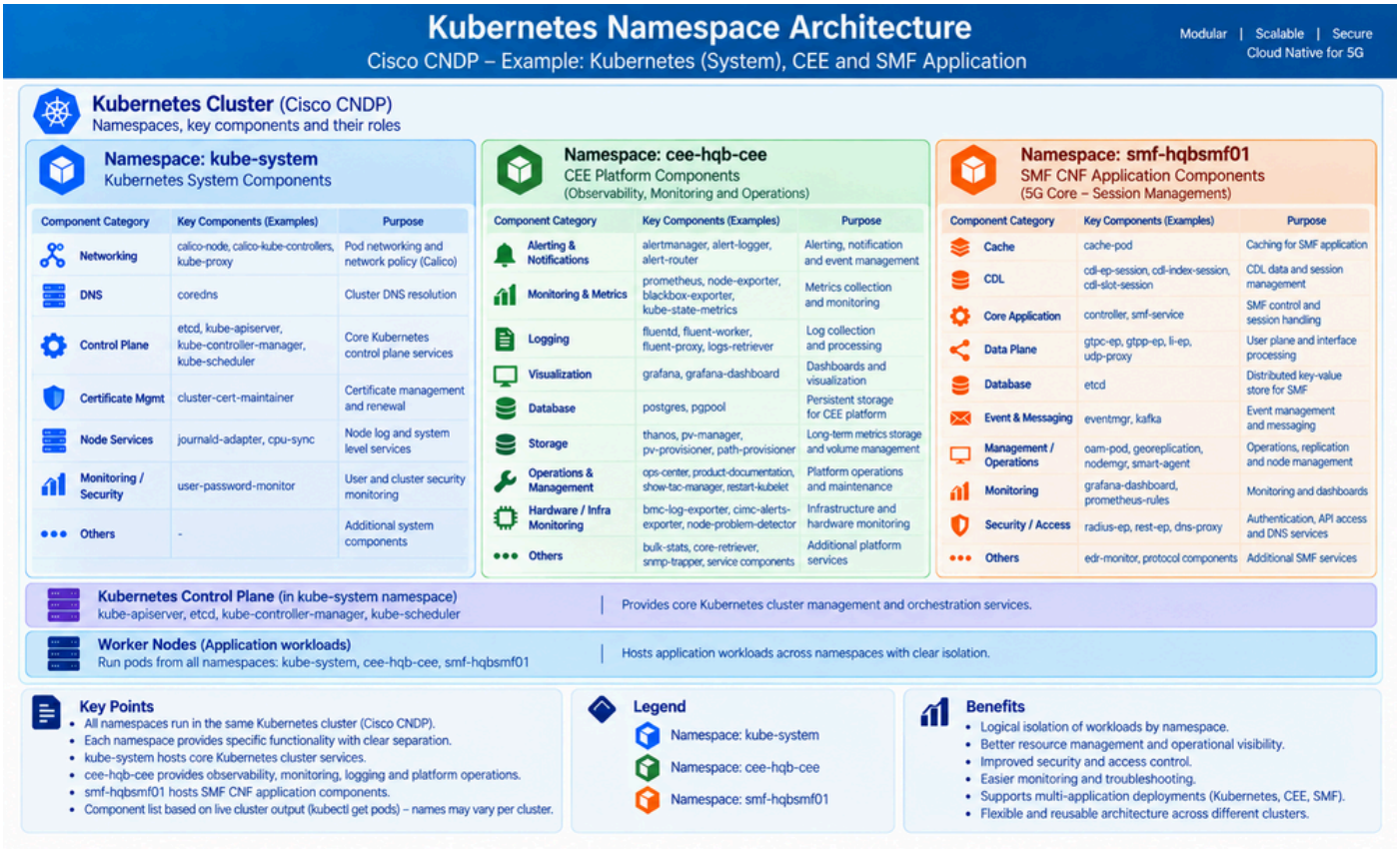
O Cisco Common Execution Environment (CEE) faz parte da Infraestrutura de Microserviços de Assinante (SMI) da Cisco. Em uma implantação de CNDP com base no Kubernetes, o Kubernetes namespace separa serviços de plataforma, observabilidade de CEE e serviços de gerenciamento Kubernetes e cargas de trabalho de aplicativos SMF. A separação fornece limites administrativos e operacionais, enquanto a rede Kubernetes e a descoberta de serviços permitem a comunicação de componentes permitida.

Este documento aborda a arquitetura de namespace, cargas de trabalho CEE, instalação CEE e gerenciamento de ciclo de vida, CEE Ops Center, alertas e Simple Network Management Protocol (SNMP), alertas do Cisco Integrated Management Controller (CIMC), encaminhamento de logs, estatísticas em massa e o gateway do sistema OpenTelemetry.

O Splunk HEC na porta 8088 do Protocolo de Controle de Transmissão (TCP - Transmission Control Protocol) e na porta 5140 do Syslog over User Datagram Protocol (UDP - Protocolo de Datagrama de Usuário) são mecanismos de inclusão independentes. Os dois caminhos têm diferentes requisitos de configuração, transporte e solução de problemas e podem coexistir.

Visão geral da arquitetura

CEE e as funções de aplicativo associadas ocupam espaços de nome Kubernetes separados. A arquitetura diferencia os serviços da plataforma Kubernetes das funções de observabilidade e gerenciamento CEE e do domínio de aplicativos SMF.



Arquitetura de namespace Cisco SMI mostrando separação de plataformas de aplicativos e CEE

O namespace CEE é o foco principal da arquitetura de nível de serviço. Outros namespaces fornecem a plataforma Kubernetes, funções de rede e cargas de trabalho SMF.

Cargas de trabalho de namespace de CEE

O namespace CEE hospeda microsserviços para monitoramento, alertas, registro, painéis, estatísticas e acesso operacional.



alert-logger	Stores and maintains historical alerts that are received from the Alert manager. These alerts are avaiable to user through the CEE ops-center.
alert-router	Provides routing support for the alert manager to pass alerts to its receivers.
alertmanager	Process alerts from Prometheus and route them to its receivers through alert-router. It also provides a list of active alerts in CEE ops-center and Grafana.
blackbox-exporter	Enables Prometheus blackbox probing of endpoints over HTTP, TCP, and ICMP.
bulk-stats	Provides summary of statistics that are collected by Prometheus service and create periodic snapshots of statistics on each node in the form of CSV files.
cee-product-documentation	CEE Product documentation page provides an overview of CEE functions.
cimc-alerts-exporter	Scrapes and exports CIMC alerts to be viewable in Grafana.
core-retriever	Assists in retrieving the core dumps.
documentation	Contains the documentation (metrics and usage).
fluentbit	Collects the logs from journalD or systemd and forwards to the external applications like Splunk or another remote fluent instance.
grafana-dashboard-metrics	Assists in collating Grafana metrics on the dashboard.
fluentbit-listener	Collects the logs from remote fluent instances and forward these logs to external collectors like Splunk.
grafana	Provides visualization tool and host-level dashboards to examine metrics and alerts.
grafana-dashboard-metrics	Supports the internal file server for Grafana dashboards.
kube-state-metrics	Assists in generating metrics about the state of Kubernetes objects: node status, node capacity (CPU and memory), and so on.
loki	Provides support to visualize the logs that are provided by the locally installed fluentBit pods.
logs-retriever	Assists in retrieving Kernel, Kubelet, and Container level logs through output to the JournalD driver.
logs-forwarder	Support pods logs forwarding to external server through Fluent-bit.
metrics-proxy-group	Create tunnels to enable Prometheus to scrape KPIs from the node-exporters on KVM nodes.
node-exporter	Exports the node metrics to Prometheus and to be viewable on the Grafana dashboard in Host details and summary dashboards.
ops-center-cee-ops-center	Supports user management, authentication, configuration, and show commands for CEE features, which run on pods inside the cluster.
path-provisioner	Provisions the local storage volume along with pv-provisioner.
pgpool	Manage the Postgres resource pool for connection, replication, load balance, and so on. Pgpool is a middleware that works between PostgreSQL servers and a PostgreSQL database.
postgres	Supports SQL database with redundancy to store alerts and Grafana dashboards.
prometheus-hi-res	Enables monitoring and alerting for the Kubernetes cluster, both local and remote. It scrapes alerts, metrics, kubernetes resources exported by pods and nodes information.
prometheus-rules	Contains the default alerting rules and recording rules for Prometheus.
prometheus-scrapeconfigs-synch	Synchronizes the Prometheus scrape configuration.
pv-manager	Monitors the state of nodes and manages persistent volume and associated pods.
pv-provisioner	Enables the application pods to automatically provision the persistent volumes.
restart-kubelet	Monitors the pod ready status and resets the kubelet if the state is not-ready even though pod is ready.
show-tac-manager	Supports the Tac-Debug feature to collect coredump, logs, metrics, statistics, and ops-center configuration. It also maintains and provides HTTPS access to files storage in the internal Apache server.
smart-agent-cee-global-ops-center	Manages and enforces the Cisco Smart licensing feature per agreement. The CEE ops-center provides the configuration facility.
thanos-query-hi-res	Runs the Thanos application to support the Prometheus query, data storage, and remote cluster monitoring.

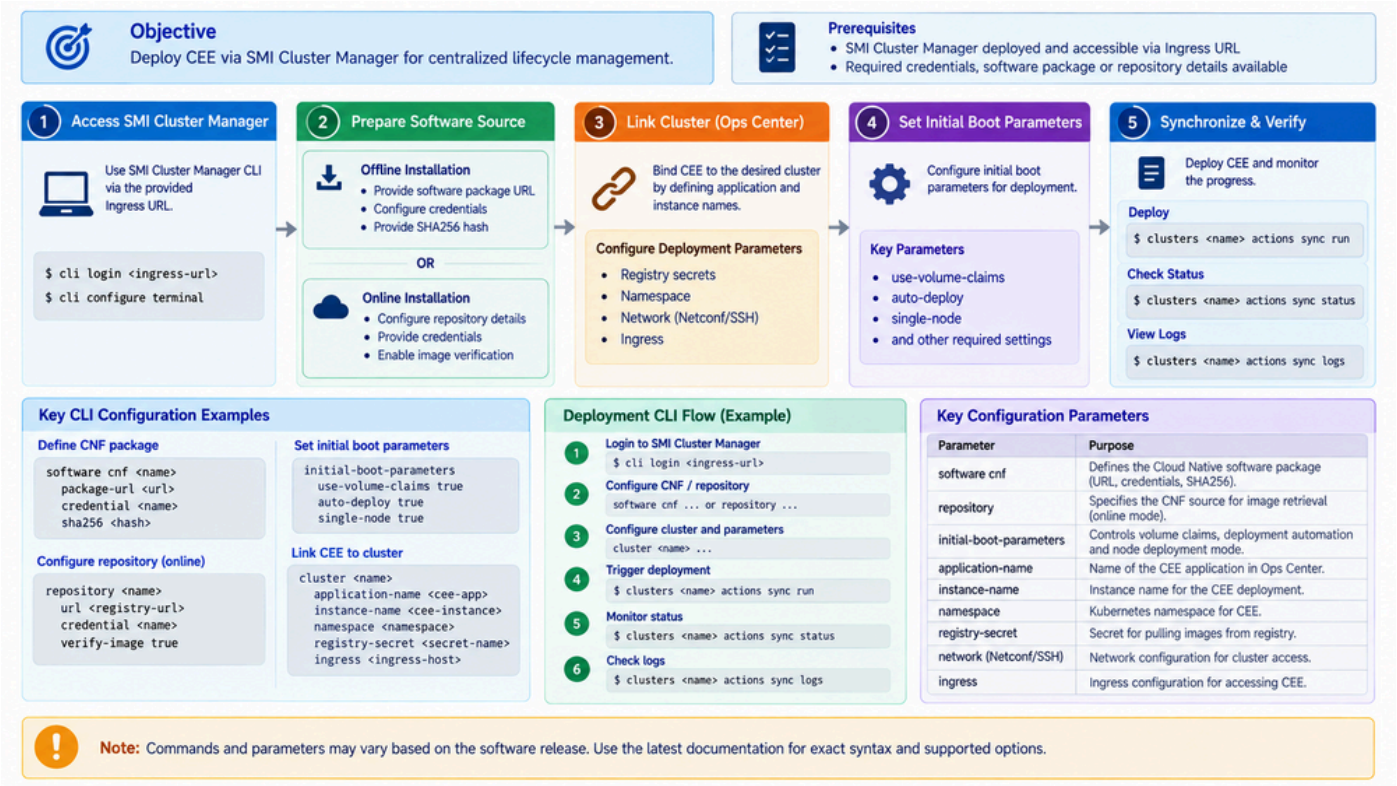
Microsserviços de namespace CEE e as funções de suas cargas de trabalho operacionais

Essas funções incluem coleta de métricas Prometheus, visualização Grafana, tratamento de alertas Alertmanager, serviços de encaminhamento de logs e criação periódica de estatísticas em massa. As cargas de trabalho individuais variam de acordo com a versão e a configuração de implantação.

Instalação e gerenciamento do ciclo de vida do CEE

O Gerenciador de cluster SMI separa a definição de artefato de software do cluster de destino e

sua configuração do Centro de operações. Isso permite o controle de versão de software e a sincronização de cluster repetível.



Instalação do SMI Cluster Manager CEE e arquitetura de sincronização de software

Modos de instalação

- A instalação off-line pode se referir a um pacote de software local por meio de um URL de arquivo e um hash de 256 bits (SHA-256) do Secure Hash Algorithm.
- A configuração do cluster associa a implantação de CEE/SMF ao cluster e à instância do Ops Center desejados.

Definir o artefato de software CEE

Na configuração do SMI Cluster Manager, identifique o pacote de software CEE local e seu hash SHA-256.

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

Use o valor SHA-256 exato do pacote aprovado. O espaço reservado no comando é intencional e não representa um checksum real.

Configurar o Cluster e o Centro de Operações

A configuração de origem associa um cluster a um Centro de Operações SMF, repositório local, endpoints de gerenciamento e configurações de implantação. Os identificadores específicos do site são substituídos por espaços reservados.

```
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
```

Parâmetro	Significado no exemplo de configuração
ops-centers smf <smf-ops-center-name>	Associa o cluster à instância do Centro de Operações SMF.
repositório local	Especifica o repositório e a versão do aplicativo para implantação.
sync-default-repository true	Usa o repositório padrão configurado durante a sincronização.
netconf-port 2029	Especifica a porta de conectividade de gerenciamento NETCONF.
ssh-port 2028	Especifica a porta de conectividade de gerenciamento do Shell Seguro (SSH).
use-volume-claims true	Permite o uso de declarações de volume para requisitos de armazenamento persistentes.
auto-deploy false	Desabilita a implantação automática para que a sincronização e a validação permaneçam sob controle explícito.
single-node false	Especifica uma implantação que não está no modo de nó único.

Note: Os identificadores do pacote e do repositório são exemplos da configuração de origem. Confirme a compatibilidade de versão e os valores de endpoint antes de usá-los em um cluster diferente.

Sincronizar e verificar a implantação

Execute a ação de sincronização de cluster depois que a configuração do software e do Centro de Operações estiver pronta.

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

Inspecione os logs e o status da sincronização.

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

Confirme se a sincronização foi concluída com êxito e se os pods e serviços CEE esperados foram implantados.



Caution: A sincronização do cluster e a implantação de software podem alterar o ambiente em execução. Aplique as alterações de acordo com o procedimento aprovado de manutenção e implantação.

Centro de operações e gerenciamento operacional do CEE

O CEE Ops Center fornece a interface operacional para serviços CEE. A carga de trabalho suporta os comandos de gerenciamento de usuário, autenticação, configuração e show para funções CEE dentro do cluster. O Gerenciador de cluster SMI associa o Centro de operações à implantação de destino por meio da configuração de gerenciamento.

O Centro de Operações pertence ao plano de gerenciamento. Prometheus, Alertmanager, Fluent Bit/fluent-proxy, HEC, syslog e OpenTelemetry pertencem aos caminhos de monitoramento e telemetria. Manter essas responsabilidades separadas simplifica a solução de problemas.

Arquitetura de observação CEE

A capacidade de observação do CEE inclui métricas, alertas, logs, alertas do CIMC e estatísticas em massa. Esses serviços estão relacionados, mas os caminhos de dados e os consumidores

são diferentes.

Função	Finalidade principal	Destino típico ou consumidor
Métrica	Colete e consulte medidas de séries temporais de nós, Kubernetes e serviços.	Prometeu, Grafana e Thanos.
Alertas	Avaliar regras de alerta e eventos de alerta de rota.	Gerenciador de alertas, roteador de alertas, Centro de operações e receptores externos.
Logs	Encaminhar registros de log e eventos para coletores externos ou back-ends.	Splunk e outros coletores de log.
Alertas do CIMC	Exportar alertas do Cisco Integrated Management Controller para monitoramento.	Métricas/alertas de CEE e Grafana.
Estatísticas em massa	Crie instantâneos estatísticos periódicos.	Instantâneos CSV e processamento ou análise de downstream.

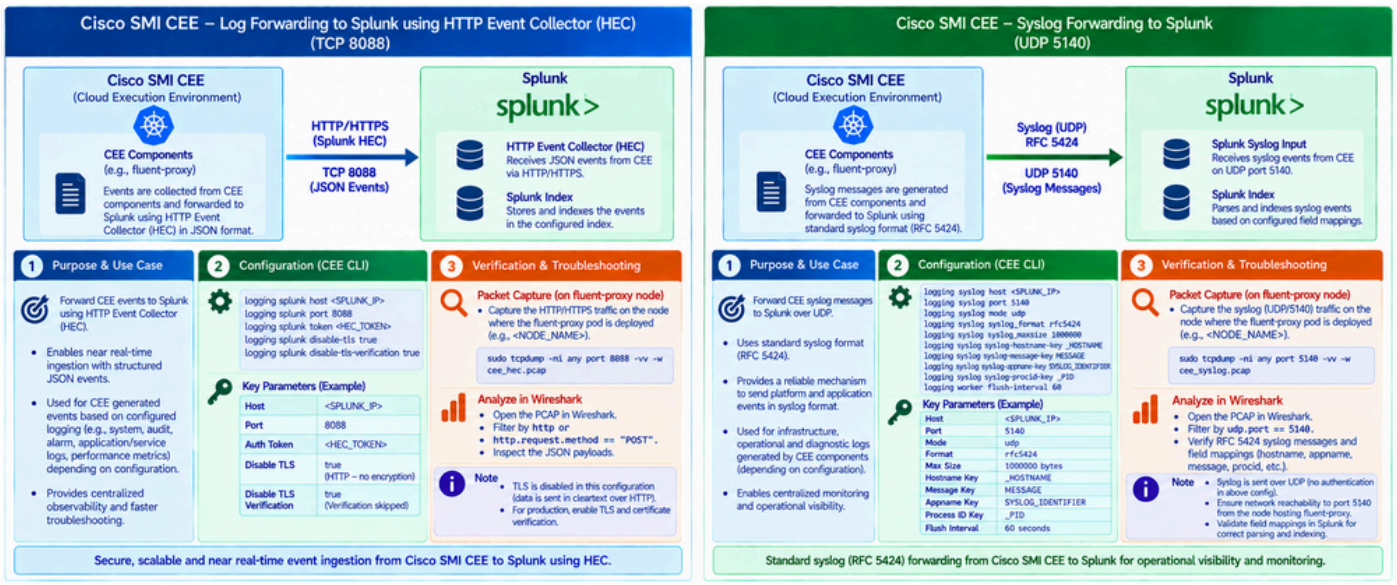
Integração do Splunk: Arquitetura de transferência de registros

A origem descreve dois caminhos CEE-to-Splunk. Ambos podem entregar eventos ao Splunk, mas usam protocolos e interfaces de inclusão distintos.

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

Os tipos de evento transportados por cada caminho dependem da configuração CEE e do pipeline de encaminhamento implementado. Duas interfaces configuradas não estabelecem que cada uma transporta uma categoria de eventos mutuamente exclusivos.

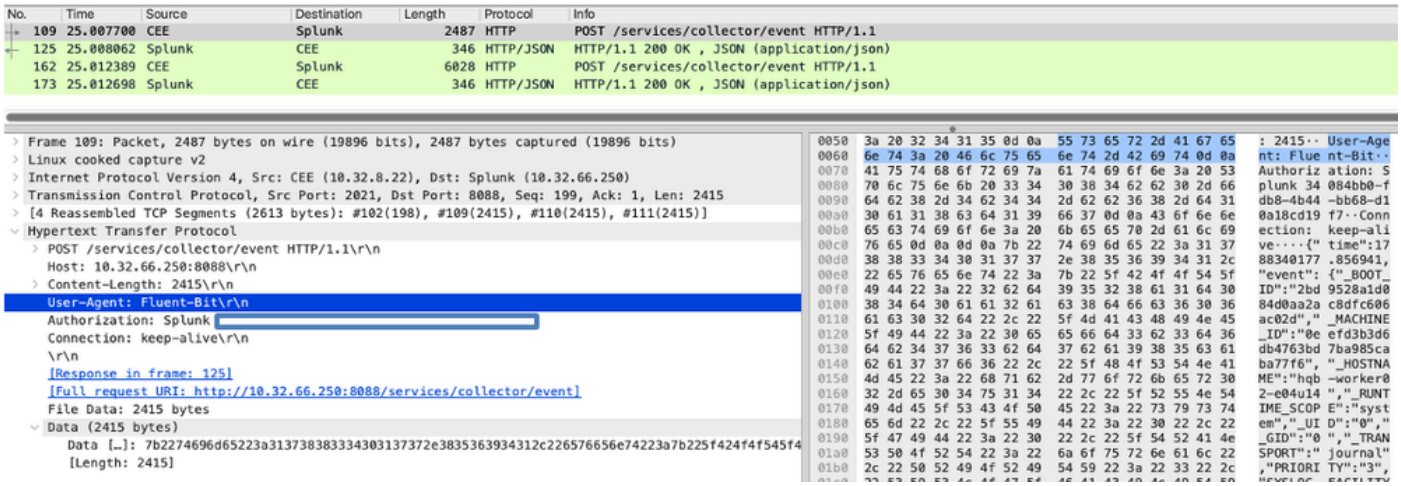
Rastreie os caminhos separadamente. A entrega de HEC bem-sucedida não confirma a entrega de syslog e a entrega de syslog bem-sucedida não confirma a entrega de HEC.



Integração de CEE Splunk com caminhos separados de encaminhamento de HEC e syslog

Encaminhamento do Coletor de Eventos HTTP de Splunk

O Splunk HEC aceita envios de eventos HTTP e usa um token de autenticação HEC. O CEE encaminha eventos diretamente para o serviço HEC configurado, em vez de exigir a inclusão baseada em arquivos para esse caminho.



Arquitetura de encaminhamento CEE para Splunk HTTP Event Collector na porta TCP 8088

Modelo de configuração HEC

O exemplo original do laboratório contém essas configurações para um endpoint CEE Splunk. O trecho registra o comportamento de origem e não é uma configuração de produção recomendada.

⚠

> Caution: O exemplo de origem desabilita a verificação de certificado e TLS. Isso expõe a telemetria e as credenciais HEC à interceptação na rede. Para produção, habilite a verificação de TLS e certificado e proteja o token de autenticação HEC de acordo com a configuração de versão CEE suportada.

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

Na arquitetura de origem, os produtores de log/evento CEE encaminham através do componente de encaminhamento Fluent relevante para o 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 e solucionar problemas de tráfego HEC

Identifique o pod fluent-proxy e seu nó de operador Kubernetes no namespace CEE quando fluent-proxy transporta o tráfego HEC.

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

No nó Kubernetes que transporta o tráfego HEC, capture pacotes para a porta HEC.

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

Para uma conexão habilitada para TLS, uma captura de pacote revela detalhes do estabelecimento e do destino do transporte, mas normalmente não expõe o payload HTTP. Se o TLS estiver desativado, o conteúdo do evento e o material de autenticação poderão ser visíveis na captura.

⚠ Caution: Capturas de pacotes e registros podem conter telemetria e credenciais confidenciais. Restringir a coleta e a transferência para fluxos de trabalho de suporte autorizados e proteger arquivos de captura.

Encaminhamento de Syslog via UDP 5140

O segundo caminho de integração Splunk encaminha registros de syslog usando a formatação RFC 5424 e a porta UDP 5140. A configuração de origem também define os mapeamentos de campo, o tamanho máximo da mensagem e o intervalo de liberação do trabalhador.

```
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
```

Mapeamento de campo RFC 5424

campo de origem CEE	Campo ou propósito do Syslog
_NOME DO HOST	Identifica o host de origem no registro de syslog gerado.
MENSAGEM	Carrega o corpo da mensagem de log.
IDENTIFICADOR_SYSLOG	Fornece o aplicativo syslog ou o identificador do programa.
_PID	Transporta o identificador do processo de origem.

Transporte UDP e captura de pacotes

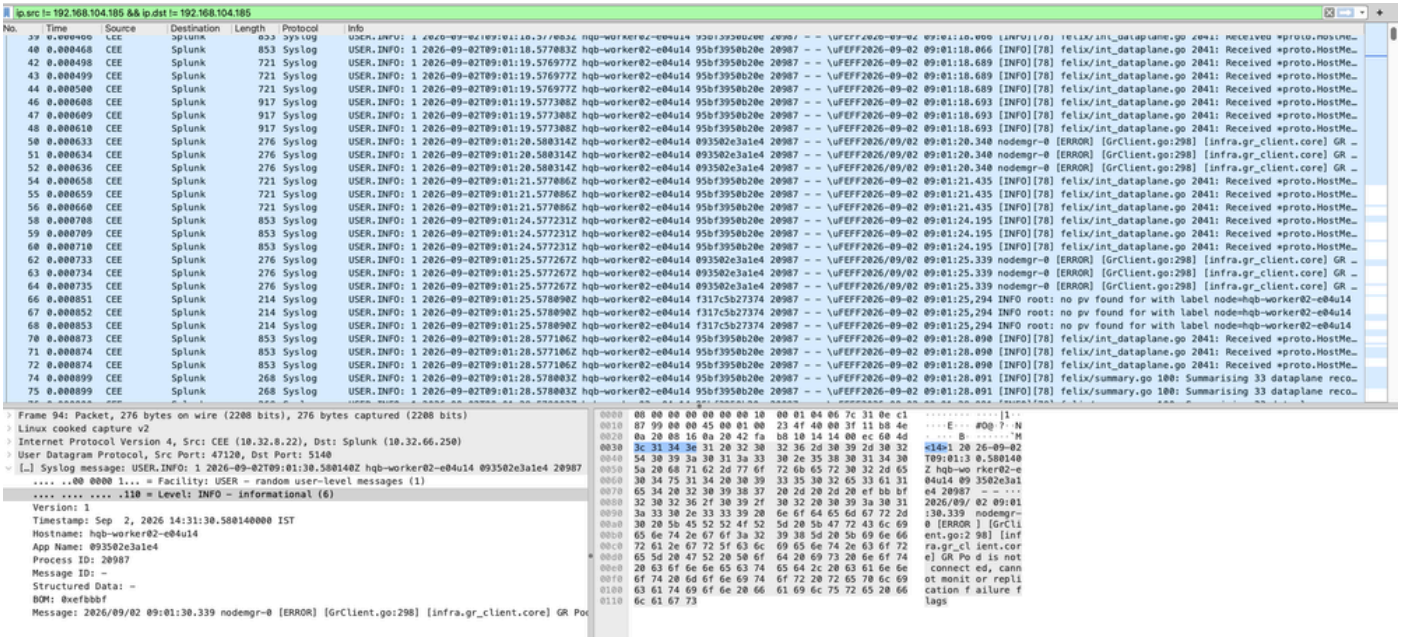
O UDP é sem conexão e não fornece confirmação de entrega de transporte nem retransmissão. A identificação e solução de problemas deve levar em conta a perda de pacotes, o roteamento, a unidade máxima de transmissão (MTU), a fragmentação, a disponibilidade do receptor e o comportamento de fila/taxa.

Na interface ou no nó Kubernetes que transporta o tráfego syslog, execute:

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

Se o proxy fluente encaminhar o tráfego de syslog, o nó que hospeda esse componente será um ponto de captura de pacotes apropriado. Verifique o caminho de encaminhamento antes de coletar pacotes.

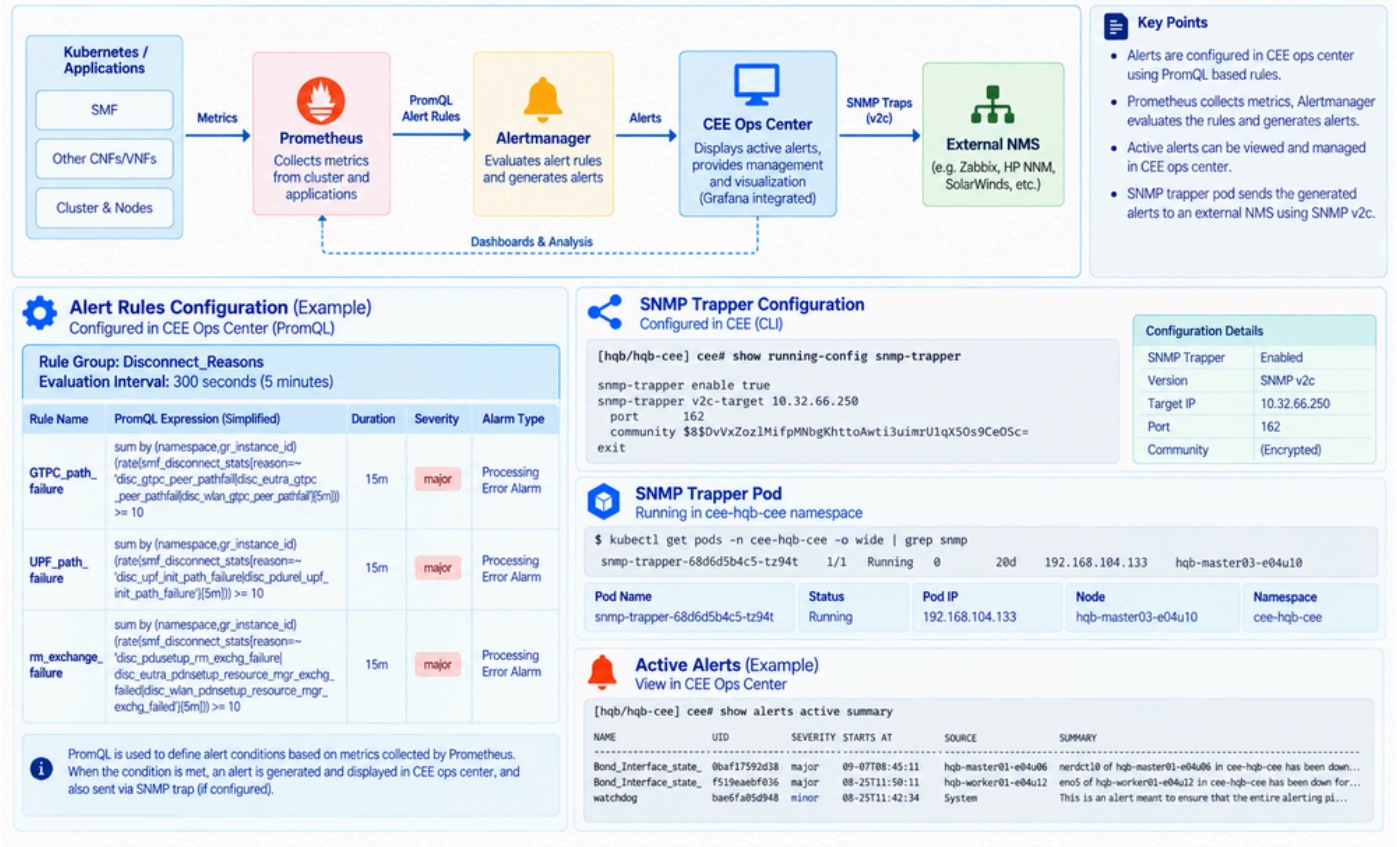
Note: O RFC 5424 define um formato de mensagem de syslog independentemente do transporte selecionado. O cenário de origem usa UDP 5140. O transporte de syslog baseado em TLS é uma opção diferente que requer uma configuração de remetente e receptor compatível.



Encaminhamento de syslog CEE para Splunk usando campos de porta UDP 5140 e RFC 5424

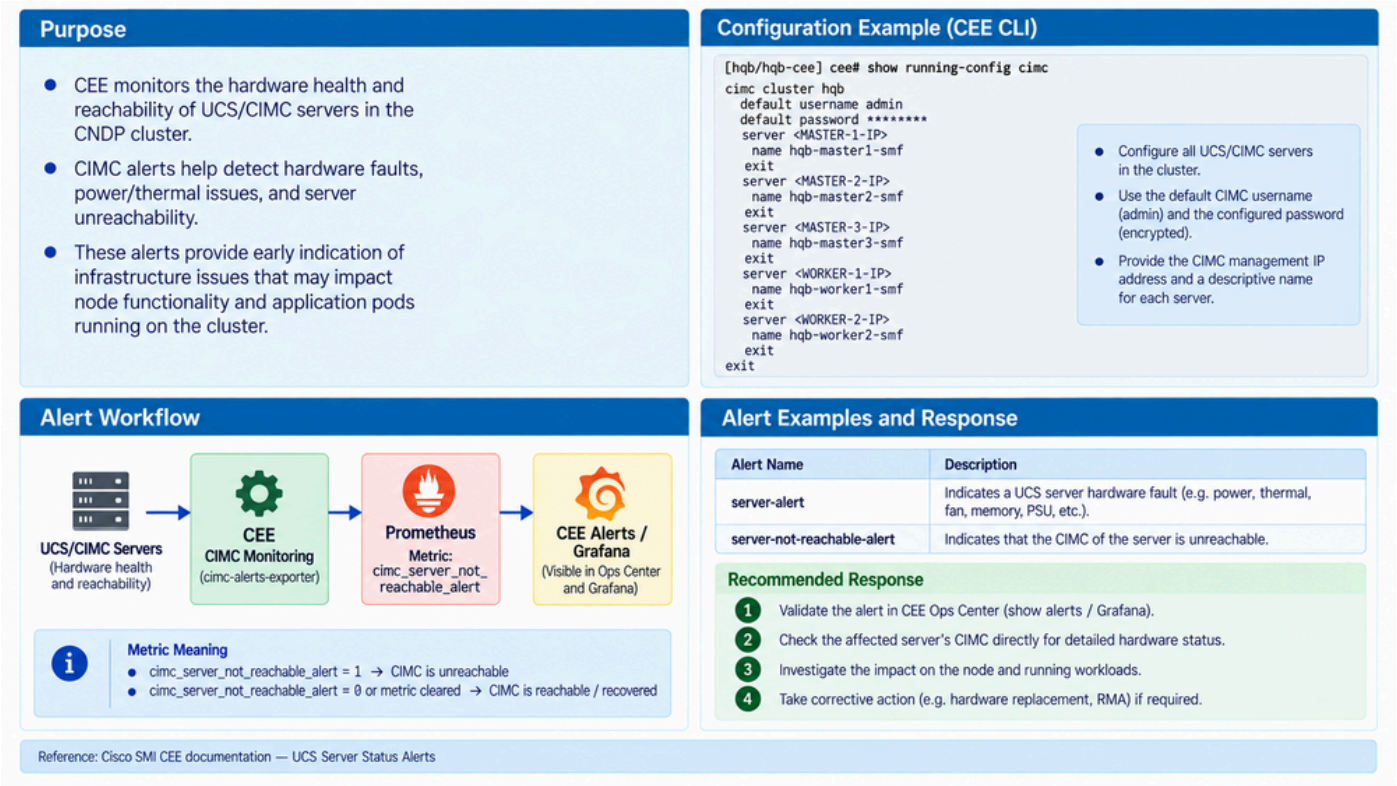
Alertas, SNMP e capacidade de observação do CIMC

Os alertas CEE usam Prometheus e Alertmanager. Prometheus avalia métricas e regras de alerta. O Alertmanager roteia eventos de alerta para os receptores, com o roteador de alerta fornecendo suporte de roteamento adicional. O CEE alert-logger fornece registros de alertas históricos para recuperação através do CEE Ops Center.



Encaminhamento de alertas CEE Prometheus e Alertmanager e arquitetura SNMP

A integração de alertas do CIMC fornece um caminho de monitoramento de infraestrutura relacionado. O cimc-alerts-export coleta informações de alertas do CIMC e as expõe para monitoramento e visualização no Grafana.

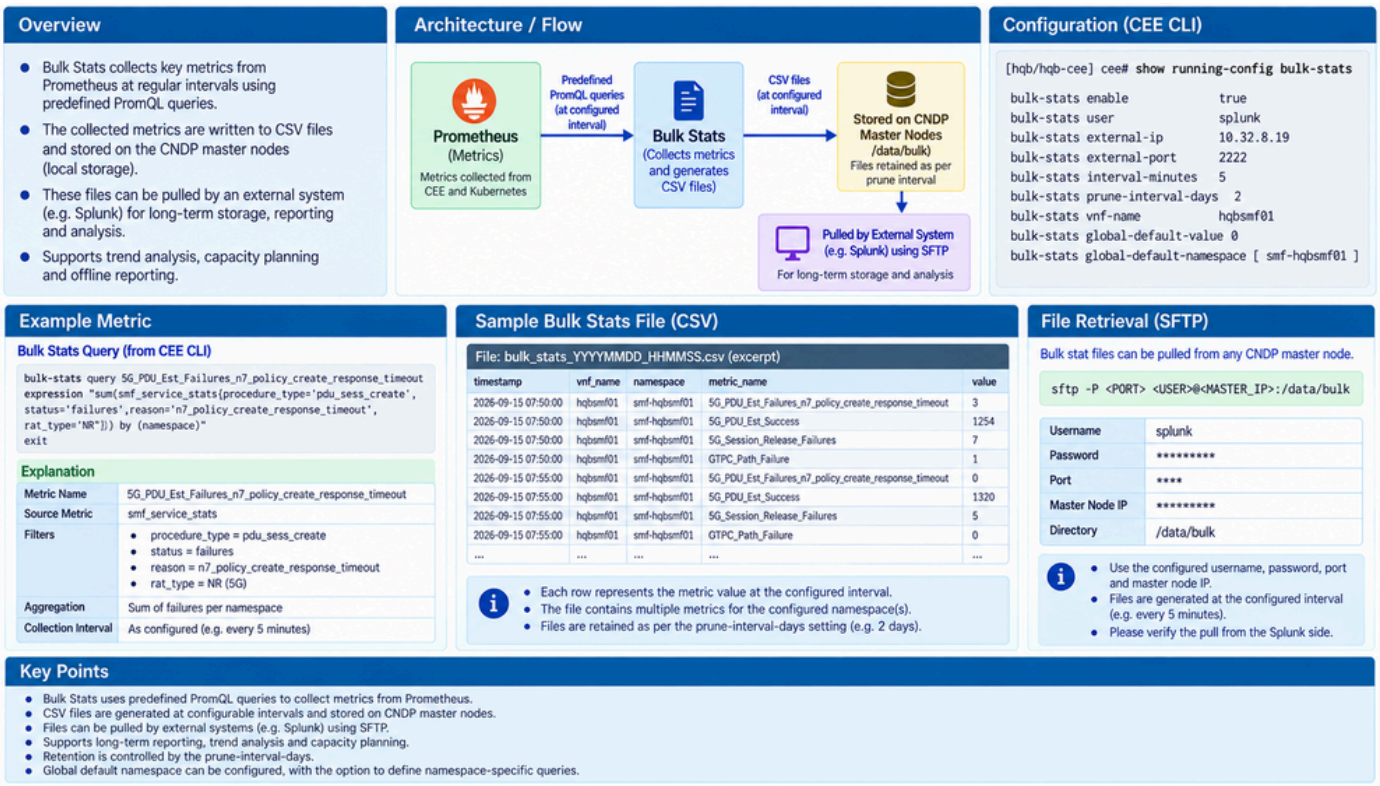


A integração SNMP é uma interface de gerenciamento e alerta; não é intercambiável com Splunk HEC ou encaminhamento de syslog. O protocolo e os caminhos de entrega de eventos permanecem distintos.

As referências relevantes à Base de Informações de Gerenciamento (MIB - Management Information Base) incluem CISCO-CNEE-MIB.my e CISCO-SMI.my.

Estatísticas em Massa

O serviço CEE bulk-stats cria instantâneos periódicos CSV (Comma-Separated Values) de estatísticas coletadas através do Prometheus. Esses são instantâneos estatísticos, e não fluxos de registros de log de aplicativo.



Serviço de estatísticas em massa CEE criando instantâneos CSV periódicos a partir das métricas de Prometheus

A saída de estatísticas em massa suporta relatórios periódicos, análise de tendências e processamento de dados downstream. Inclua-o em um caminho de integração de Splunk somente quando a implantação encaminhar ou importar explicitamente dados CSV/estatísticas para Splunk.

Gateway do sistema OpenTelemetry

As versões mais recentes do Cisco SMI oferecem suporte a um gateway OpenTelemetry Collector gerenciado por plataforma. O gateway recebe telemetria de aplicativos por meio do protocolo OTLP (OpenTelemetry Protocol) e encaminha métricas e registros suportados para back-ends locais ou remotos.



Note: A documentação do Cisco SMI Cluster Manager Operations identifica a integração do gateway OpenTelemetry com a versão 2026.03.1. O gateway não foi validado na implantação específica descrita pelo exemplo da origem, portanto, esta seção descreve o modelo de configuração publicado em vez da operação verificada nesse ambiente.

Modelo de gateway do 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
```

Conceitos de configuração de gateway

Habilite o gateway do OpenTelemetry Collector e selecione as métricas locais e os back-ends de registro.

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

Quando a implantação exigir exposição de serviço externo, a configuração poderá incluir um IP externo.

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

As configurações de proxy opcionais são definidas para os exportadores de 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
```

As opções de back-end local controlam como o gateway do sistema gerenciado pela plataforma envia telemetria para back-ends internos. A exposição a IP externo e as configurações de proxy dependem dos requisitos de topologia e segurança.

Exportadores remotos

Exportador	Sinais	Uso técnico
otlp	Logs, métricas	Enviar telemetria para um back-end que aceite OTLP por gRPC.
otlphttp	Logs, métricas	Enviar telemetria para um back-end que aceite OTLP sobre HTTP.
splunkhec	Logs	Enviar logs para um ponto de extremidade de HEC de Splunk.
journald	Logs	Grave logs no diário de nós onde houver suporte.
debug	Logs, métricas	Suporte a validação e solução de problemas controlados.

O pipeline OpenTelemetry segue o modelo de recebimento, processamento e exportação. Receptores ingerem telemetria; processadores filtram ou transformam dados; os exportadores enviam os sinais selecionados para back-ends remotos ou locais.

A origem também distingue o comportamento de proxy: o otlp usa configurações de proxy da instância do coletor, enquanto o otlphttp e o splunkhec suportam substituições de proxy no nível do exportador onde a versão implantada expõe essa configuração.

Compare com OpenShift OpenTelemetry

O Cisco CEE e o OpenShift têm um padrão de arquitetura compartilhado: um OpenTelemetry Collector pode ficar entre aplicações instrumentadas e back-ends de observabilidade. Seus modelos de gerenciamento e instalação são diferentes.

Conceito	Gateway de sistema CEE OpenTelemetry	Padrão OpenTelemetry OpenShift
Fonte de telemetria	CEE e cargas de trabalho de aplicativos habilitados para OpenTelemetry	Cargas de trabalho do OpenShift habilitadas para OpenTelemetry
Protocolo	OTLP	OTLP

Conceito	Gateway de sistema CEE OpenTelemetry	Padrão OpenTelemetry OpenShift
Função do coletor	Gateway de sistema gerenciado por plataforma	Implantação ou instância do OpenTelemetry Collector
Conceito de pipeline	Receber, processar, exportar	Receber, processar, exportar
Flexibilidade de back-end	Infraestruturas locais e exportadores remotos suportadosName	Integração de back-end orientada por exportador
Integração de Splunk	exportador splunkhec na configuração CEE documentada	Exportador Splunk HEC onde configurado

Essa comparação é arquitetônica. As duas plataformas não são reivindicadas para implementar OpenTelemetry de forma idêntica. O OpenShift geralmente usa um modelo de implantação OpenTelemetry Operator/Collector, enquanto o gateway do sistema Cisco SMI é gerenciado por plataforma.

A arquitetura de referência do OpenShift discutida na fonte mostra coletores encaminhando telemetria das cargas de trabalho do Kubernetes para o Splunk sobre HEC. Ele ilustra o modelo baseado em coletor em vez de uma integração verificada para a instalação CEE de amostra.

Verificar a configuração

Verificar sincronização de CEE

Revise o status e os registros de sincronização do SMI Cluster Manager e confirme se as cargas de trabalho CEE esperadas estão implantadas.

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

Verificar HEC e Syslog separadamente

Confirme se o caminho HEC envia eventos ao ponto final TCP 8088 configurado e se o Splunk os recebe. Confirme separadamente que o caminho do syslog envia registros UDP 5140 para o ouvinte configurado.

Use os métodos de captura de pacotes nas seções correspondentes e correlacione os carimbos de data/hora dos pacotes com os eventos recebidos no coletor configurado.

Verificar os serviços de observação

Confirme se as métricas, o roteamento de alertas, os alertas do CIMC e os instantâneos de estatísticas em massa operam conforme designado para a versão instalada. Se OpenTelemetry estiver habilitado, verifique a integridade do receptor, do pipeline e do exportador usando o procedimento de operações do SMI Cluster Manager com suporte.

Comportamento esperado

Componente ou caminho	Resultado esperado
Gerenciador de cluster SMI	A sincronização do cluster é concluída e os serviços CEE necessários são implantados.
Centro de Operações	Os usuários autorizados podem acessar funções operacionais e comandos de configuração/monitoramento suportados.
HEC de Splunk	O tráfego de eventos atinge o ouvinte HEC configurado na porta TCP 8088.
Syslog	Os eventos formatados pelo RFC 5424 alcançam o ouvinte da porta UDP 5140 configurada.
Alertas e CIMC	O Alertmanager e os exportadores relacionados expõem as informações de alerta configuradas.
Estatísticas em massa	Instantâneos CSV periódicos são gerados a partir de estatísticas coletadas.
TelemetriaAberta	Nas versões suportadas com o gateway configurado, os sinais OTLP fluem pelo pipeline back-end/exportador selecionado.

Fluxo de decisão

Observação	Próxima verificação
Os serviços CEE estão ausentes após a sincronização.	Inspecione o status da sincronização do Cluster Manager, logs, artefatos de software e parâmetros do Centro de Operações.
Os eventos HEC estão ausentes.	Identifique o pod/nó de encaminhamento, verifique o tráfego TCP 8088, o destino HEC, a autenticação e a configuração TLS.
Eventos de syslog ausentes.	Verifique o destino UDP 5140, a formatação RFC 5424, o fluxo de pacotes e o comportamento do receptor.
Alertas ou dados do CIMC estão ausentes.	Verifique o roteamento Prometheus/Alertmanager, o roteador de alerta e a operação cimc-alerts-export.
Estatísticas em massa ausentes.	Confirme a operação do serviço bulk-stats, a disponibilidade de dados do Prometheus e a geração de instantâneos CSV.
A exportação de OpenTelemetry está	Verifique o suporte de recursos para a versão instalada, a configuração de gateway, o estado do receptor e do exportador e a

Observação	Próxima verificação
ausente.	associação de pipeline.

Conclusão

CEE é um ambiente de execução e observabilidade em camadas baseado no Kubernetes em torno de aplicativos SMF. A separação de namespace do Kubernetes divide as operações da plataforma, os serviços CEE e as cargas de trabalho do aplicativo em domínios diferentes. Na CEE, monitoramento, alertas, registro e estatísticas em massa são serviços especializados com responsabilidades independentes.

A principal distinção de Splunk é entre HEC sobre TCP 8088 e syslog sobre UDP 5140. Esses são caminhos de encaminhamento separados com diferentes protocolos, configurações e procedimentos de solução de problemas. O gateway de sistema OpenTelemetry mais recente adiciona um modelo de coletor e exportador baseado em OTLP. Sua semelhança com o OpenShift OpenTelemetry é arquitetônica, e a operação do gateway deve ser verificada para a versão e a implantação específicas do CEE.

Conteúdo relacionado

- Guia de configuração e administração do Cisco CEE - Common Execution Environment
- Guia de configuração e administração do Cisco CEE - Comandos de registro
- Operações do Cisco SMI Cluster Manager - Sincronização e telemetria aberta
- RFC 5424 - O protocolo Syslog

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.