Analyse der Cisco CEE-Beobachtbarkeit und Splunk-Integration

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Architekturübersicht
- CEE-Namespace-Workloads
- CEE Installation und Lifecycle Management
  - Installationsmodi
  - Definieren des CEE-Software-Artefakts
  - Konfigurieren des Clusters und des Betriebscenters
  - Synchronisieren und Überprüfen der Bereitstellung
- CEE Ops Center und Betriebsmanagement
- CEE-Beobachtbarkeitsarchitektur
- Splunk-Integration: Log-Transfer-Architektur
- Splunk-HTTP-Ereignis-Collector-Weiterleitung
  - HEC-Konfigurationsmodell
  - Erfassung und Fehlerbehebung von HEC-Datenverkehr
- Syslog-Weiterleitung über UDP 5140
  - RFC 5424 - Feldzuordnung
  - UDP-Transport und Paketerfassung
- Warnmeldungen, SNMP und CIMC-Beobachtbarkeit
- Massenstatistiken
- OpenTelemetry System-Gateway
  - System-Gateway-Modell
  - Gateway-Konfigurationskonzepte
  - Remote-Exporteure
  - Vergleich mit OpenShift OpenTelemetry
- Überprüfen der Konfiguration
  - CEE-Synchronisierung überprüfen
  - Separate Überprüfung von HEC und Syslog
  - Services zur Beobachtbarkeit überprüfen
- Erwartetes Verhalten
- Entscheidungsablauf
- Schlussfolgerung
- Verwandte Inhalte

Einleitung

In diesem Dokument werden die Cisco Common Execution Environment (CEE)-Architektur, die Bereitstellung, die Überwachung, die Splunk-Integration und OpenTelemetry beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit diesen Technologien vertraut zu machen:

- Cloud Native Deployment Platform (CNDP), Kubernetes-Namespaces und POD-Platzierung.
- Cisco Subscriber Microservices Infrastructure (SMI) und der SMI Cluster Manager.
- CEE Ops Center, Prometheus, Grafana, Alertmanager und Logforward-Komponenten.
- Splunk HTTP Event Collector (HEC), Syslog und Paketerfassung mit tcpdump.
- OpenTelemetry Protocol (OTLP) und OpenTelemetry Collector für die neuere Gateway-Integration.

Verwendete Komponenten

Die Beispiele zeigen eine Kubernetes-basierte Cisco SMI/CNDP-Umgebung mit CEE und einer zugehörigen Session Management Function (SMF)-Anwendung. Das Beispiel der Softwaredefinition bezieht sich auf das CEE-Paket 2026.01.1.08. Im Beispiel "Ops Center" wird ein SMF-Repository-Bezeichner smf-2026.04.m0.i50 verwendet. Dies sind Beispielwerte, keine Bereitstellungsanforderungen.

Netzwerkendpunkte, Clusternamen und Namespacewerte müssen durch Werte ersetzt werden, die für die Zielbereitstellung genehmigt wurden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Common Execution Environment (CEE) ist Teil der Cisco Subscriber Microservices

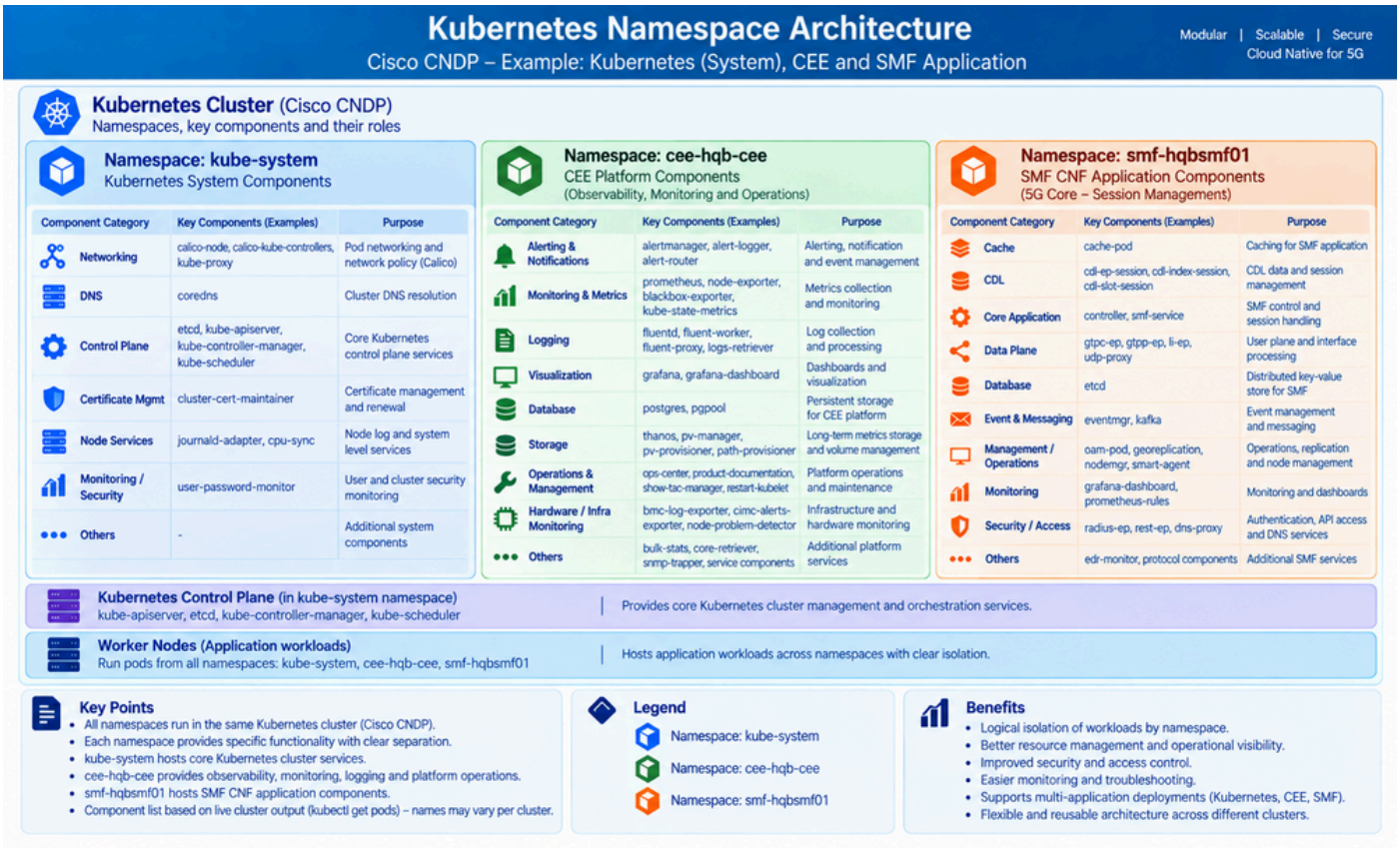
Infrastructure (SMI). In einer Kubernetes-basierten CNDP-Bereitstellung benennt Kubernetes separate Plattform-Services, CEE-Observability- und Kubernetes-Management-Services sowie SMF-Anwendungs-Workloads. Die Trennung schafft administrative und betriebliche Grenzen, während Kubernetes-Netzwerk und die Service-Erkennung eine zulässige Komponentenkommunikation ermöglichen.

Dieses Dokument behandelt die Namespace-Architektur, CEE-Workloads, CEE-Installation und -Lifecycle-Management, CEE Ops Center, Warnungen und SNMP (Simple Network Management Protocol), Cisco Integrated Management Controller (CIMC)-Warnungen, Protokollweiterleitung, Massenstatistiken und das OpenTelemetry-System-Gateway.

Splunk HEC auf dem Transmission Control Protocol (TCP)-Port 8088 und Syslog über dem User Datagram Protocol (UDP)-Port 5140 sind unabhängige Übernahmemechanismen. Die beiden Pfade haben unterschiedliche Konfigurations-, Transport- und Fehlerbehebungsanforderungen und können gleichzeitig genutzt werden.

Architekturübersicht

CEE und die zugehörigen Anwendungsfunktionen belegen separate Kubernetes-Namespaces. Die Architektur unterscheidet Kubernetes-Plattform-Services von CEE-Observability- und Management-Funktionen und von der SMF-Anwendungsdomäne.



Cisco SMI-Namespace-Architektur mit CEE- und Anwendungsplattformtrennung

Der CEE-Namespace ist der Schwerpunkt der Service-Level-Architektur. Andere Namespaces stellen die Kubernetes-Plattform, Netzwerkfunktionen und SMF-Workloads bereit.

CEE-Namespace-Workloads

Der CEE-Namespace hostet Mikroservices für Überwachung, Warnmeldungen, Protokollierung, Dashboards, Statistiken und betrieblichen Zugriff.



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.

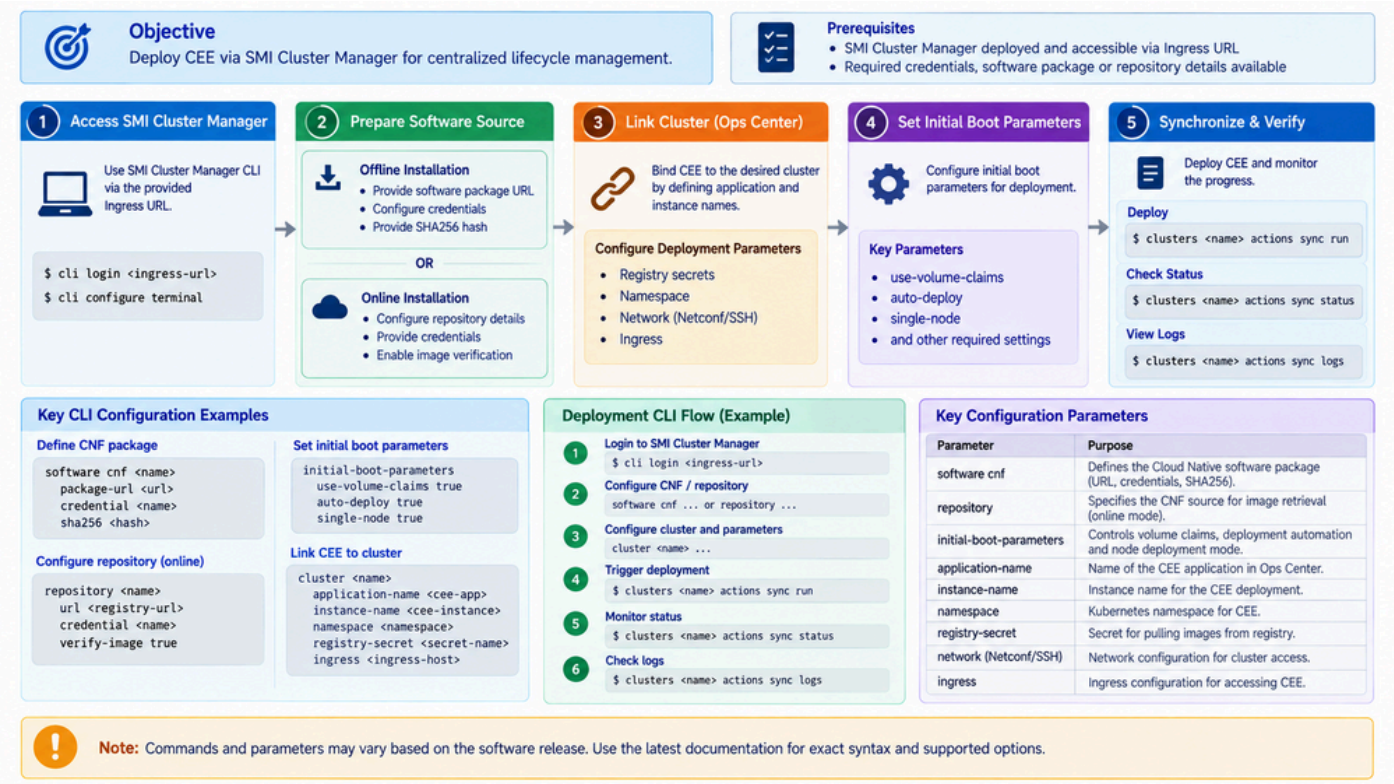
CEE-Namespace-Mikroservices und die Funktionen seiner betrieblichen Workloads

Zu diesen Funktionen gehören die Prometheus-Metriksammlung, die Grafana-Visualisierung, die Handhabung von Warnmeldungen durch den Alertmanager, Log-Forwarding-Services und die Erstellung regelmäßiger Massenstatistiken. Die einzelnen Workloads variieren je nach Version und Bereitstellungskonfiguration.

CEE Installation und Lifecycle Management

Der SMI-Cluster-Manager trennt die Definition des Software-Artefakts vom Ziel-Cluster und

dessen Operations Center-Konfiguration. Dies ermöglicht eine kontrollierte Softwareversionierung und wiederholbare Cluster-Synchronisierung.



SMI Cluster Manager CEE-Installations- und Software-Synchronisierungsarchitektur

Installationsmodi

- Bei der Offline-Installation kann über eine Datei-URL und einen Secure Hash Algorithm 256-Bit (SHA-256) Hash auf ein lokales Softwarepaket verwiesen werden.
- Die Cluster-Konfiguration verknüpft die CEE/SMF-Bereitstellung mit dem beabsichtigten Cluster und der Operations Center-Instanz.

Definieren des CEE-Software-Artefakts

Identifizieren Sie in der SMI Cluster Manager-Konfiguration das lokale CEE-Softwarepaket und seinen SHA-256-Hash.

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

Verwenden Sie den exakten SHA-256-Wert aus dem genehmigten Paket. Der Platzhalter im Befehl ist beabsichtigt und stellt keine tatsächliche Prüfsumme dar.

Konfigurieren des Clusters und des Betriebscenters

Die Quellkonfiguration verknüpft einen Cluster mit einem SMF Operations Center, einem lokalen Repository, Management-Endpunkten und Bereitstellungseinstellungen. Site-spezifische Bezeichner werden durch Platzhalter ersetzt.

```
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
```

Parameter	Bedeutung in der Beispielkonfiguration
ops-centers smf <smf-ops-center-name>	Ordnet den Cluster der Instanz des SMF-Betriebszentrums zu.
Repository-lokal	Gibt das Anwendungsrepository und die Version für die Bereitstellung an.
sync-default-repository true	Verwendet das konfigurierte Standard-Repository während der Synchronisierung.
netconf-port 2029	Gibt den NETCONF-Verwaltungs-Verbindungsport an.
SSH-Port 2028	Gibt den SSH-Management-Verbindungsport (Secure Shell) an.
Verwendung-Volumen-Angabe wahr	Ermöglicht die Verwendung von Volume-Ansprüchen für dauerhafte Speicheranforderungen.
Automatische Bereitstellung von false	Deaktiviert die automatische Bereitstellung, sodass die Synchronisierung und Validierung unter expliziter Kontrolle bleiben.
Single-Node-Falsch	Gibt eine Bereitstellung an, die sich nicht im Einzelknotenmodus befindet.



Anmerkung: Die Paket- und Repository-IDs sind Beispiele aus der Quellkonfiguration. Überprüfen Sie die Versionskompatibilität und die Endpunktwerte, bevor Sie sie in einem anderen Cluster verwenden.

Synchronisieren und Überprüfen der Bereitstellung

Führen Sie die Cluster-Synchronisierungsaktion aus, nachdem die Software- und Operations Center-Konfiguration fertig sind.

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

Überprüfen des Synchronisierungsstatus und der Protokolle

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

Bestätigen Sie, dass die Synchronisierung erfolgreich abgeschlossen wurde und dass die erwarteten CEE-PODs und -Services bereitgestellt wurden.



Vorsicht: Die Cluster-Synchronisierung und die Softwarebereitstellung können die aktuelle Umgebung verändern. Wenden Sie die Änderungen entsprechend dem genehmigten Wartungs- und Bereitstellungsverfahren an.

CEE Ops Center und Betriebsmanagement

Das CEE Ops Center stellt die operative Schnittstelle für CEE-Services bereit. Der Workload unterstützt Benutzerverwaltung, Authentifizierung, Konfiguration und Anzeigebefehle für CEE-Funktionen im Cluster. Der SMI-Cluster-Manager ordnet das Operations Center der Zielbereitstellung über die Verwaltungskonfiguration zu.

Operations Center gehört zur Managementebene. Zu den Überwachungs- und Telemetriepfaden gehören Prometheus, Alertmanager, Fluent Bit/fluent-proxy, HEC, syslog und OpenTelemetry. Eine Trennung dieser Aufgaben vereinfacht die Fehlerbehebung.

CEE-Beobachtbarkeitsarchitektur

Die CEE-Observabilität umfasst Metriken, Warnungen, Protokolle, CIMC-Warnungen und Massenstatistiken. Diese Services sind miteinander verknüpft, die Datenpfade und die

Verbraucher unterscheiden sich jedoch voneinander.

Funktion	Primärer Zweck	Typisches Ziel oder Verbraucher
Metriken	Erfassung und Abfrage von Zeitreihenmessungen von Knoten, Kubernetes und Services.	Prometheus, Grafana und Thanos.
Warnungen	Auswerten von Warnungsregeln und Weiterleiten von Warnungsereignissen	Warnungs-Manager, Warnungs-Router, Betriebszentrum und externe Empfänger.
Protokolle	Leiten Sie Protokolle und Ereignisdatensätze an externe Collectors oder Backends weiter.	Splunk und andere Protokollsammler.
CIMC-Warnungen	Exportieren Sie Cisco Integrated Management Controller-Warnungen zur Überwachung.	CEE Metriken/Alerting und Grafana.
Massenstatistiken	Erstellen Sie regelmäßige statistische Snapshots.	CSV-Snapshots und Downstream-Verarbeitung oder -Analyse.

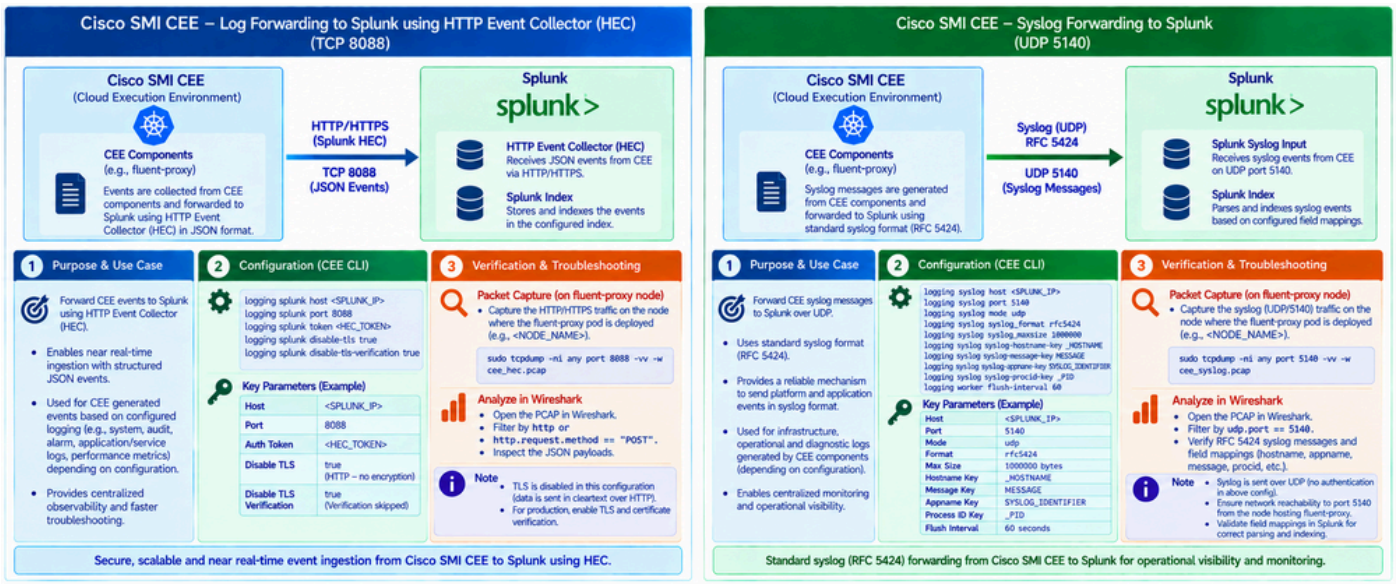
Splunk-Integration: Log-Transfer-Architektur

Die Quelle beschreibt zwei CEE-zu-Splunk-Pfade. Beide können Ereignisse an Splunk senden, verwenden jedoch unterschiedliche Protokolle und Erfassungsschnittstellen.

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

Die für die einzelnen Pfade verwendeten Ereignistypen hängen von der CEE-Konfiguration und der implementierten Weiterleitungspipeline ab. Zwei konfigurierte Schnittstellen stellen nicht sicher, dass jede eine sich gegenseitig ausschließende Ereigniskategorie enthält.

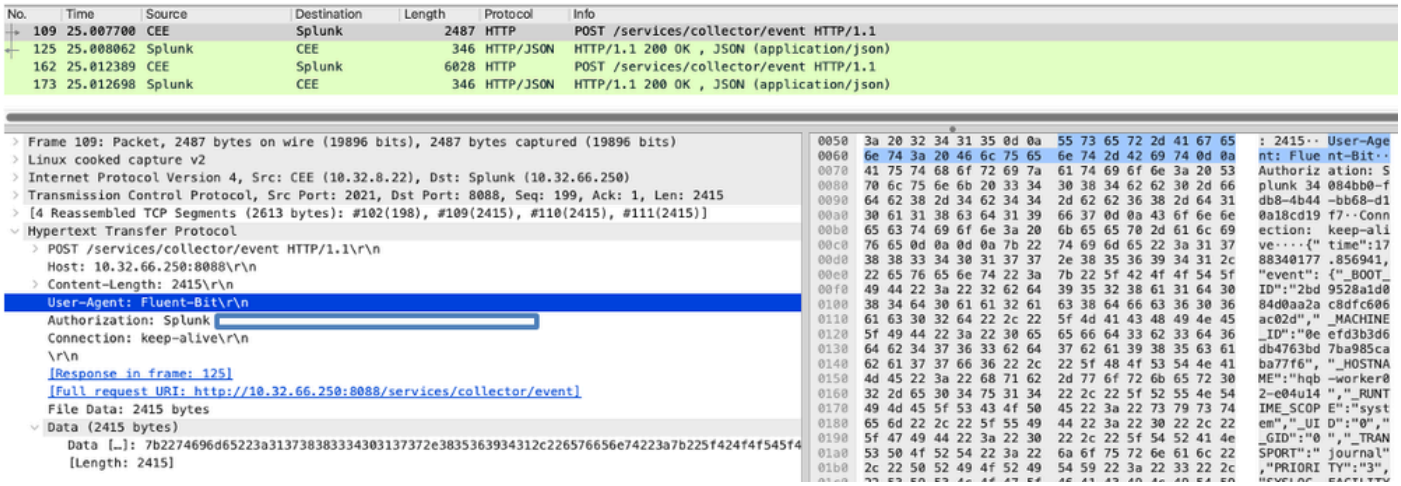
Verfolgen Sie die Pfade separat. Bei einer erfolgreichen HEC-Bereitstellung wird die Syslog-Bereitstellung nicht bestätigt, während bei einer erfolgreichen Syslog-Bereitstellung die HEC-Bereitstellung nicht bestätigt wird.



CEE Splunk-Integration mit separaten HEC- und Syslog-Weiterleitungspfaden

Splunk-HTTP-Ereignis-Collector-Weiterleitung

Splunk HEC akzeptiert HTTP-Ereigniseinreichungen und verwendet ein HEC-Authentifizierungstoken. CEE leitet Ereignisse direkt an den konfigurierten HEC-Service weiter, anstatt eine dateibasierte Erfassung für diesen Pfad zu erfordern.



CEE an Splunk HTTP Event Collector-Weiterleitungsarchitektur auf TCP-Port 8088

HEC-Konfigurationsmodell

Das ursprüngliche Lab-Beispiel enthält diese Einstellungen für einen CEE-Splunk-Endpunkt. Der Auszug zeichnet das Quellverhalten auf und stellt keine empfohlene Produktionskonfiguration dar.

⚠

Vorsicht: Im Quellbeispiel werden sowohl die TLS- als auch die Zertifikatsüberprüfung deaktiviert. Dies ermöglicht das Abfangen von Telemetrie- und HEC-Anmeldeinformationen im Netzwerk. Aktivieren Sie für die Produktion die TLS- und Zertifikatsverifizierung, und sichern Sie das HEC-Authentifizierungstoken entsprechend der unterstützten CEE-Freigabekonfiguration.

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

In der Quellarchitektur leiten CEE-Log-/Event-Produzenten durch die jeweilige Fluent-Weiterleitungskomponente an das HEC-Ziel weiter.

```
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
```

Erfassung und Fehlerbehebung von HEC-Datenverkehr

Identifizieren Sie den fluent-proxy pod und dessen Kubernetes-Workerknoten im CEE-Namespace, wenn fluent-proxy den HEC-Datenverkehr überträgt.

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

Erfassen Sie auf dem Kubernetes-Knoten, der den HEC-Datenverkehr überträgt, die Pakete für den HEC-Port.

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

Bei einer TLS-fähigen Verbindung werden bei einer Paketerfassung Details zum Transportaufbau und -ziel aufgedeckt, aber normalerweise nicht die HTTP-Nutzlast. Wenn TLS deaktiviert ist, können Ereignisinhalte und Authentifizierungsmaterial in der Erfassung angezeigt werden.

⚠ Vorsicht: Paketerfassungen und -protokolle können vertrauliche Telemetriedaten und Anmeldeinformationen enthalten. Beschränken Sie die Erfassung und Übertragung auf autorisierte Support-Workflows, und schützen Sie Erfassungsdateien.

Syslog-Weiterleitung über UDP 5140

Der zweite Splunk-Integrationspfad leitet Syslog-Datensätze unter Verwendung der RFC 5424-Formatierung und des UDP-Ports 5140 weiter. Die Quellkonfiguration definiert außerdem Feldzuordnungen, die maximale Nachrichtengröße und das Arbeitsleerungsintervall.

```
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 - Feldzuordnung

CEE-Quellfeld	Syslog-Feld oder Zweck
_HOSTNAME	Identifiziert den ursprünglichen Host im generierten Syslog-Datensatz.
MELDUNG	Enthält den Text der Protokollmeldung.
SYSLOG_IDENTIFIER	Stellt die Syslog-Anwendungs- oder Programm-ID bereit.
_PID	Enthält die Kennung des Ursprungsprozesses.

UDP-Transport und Paketerfassung

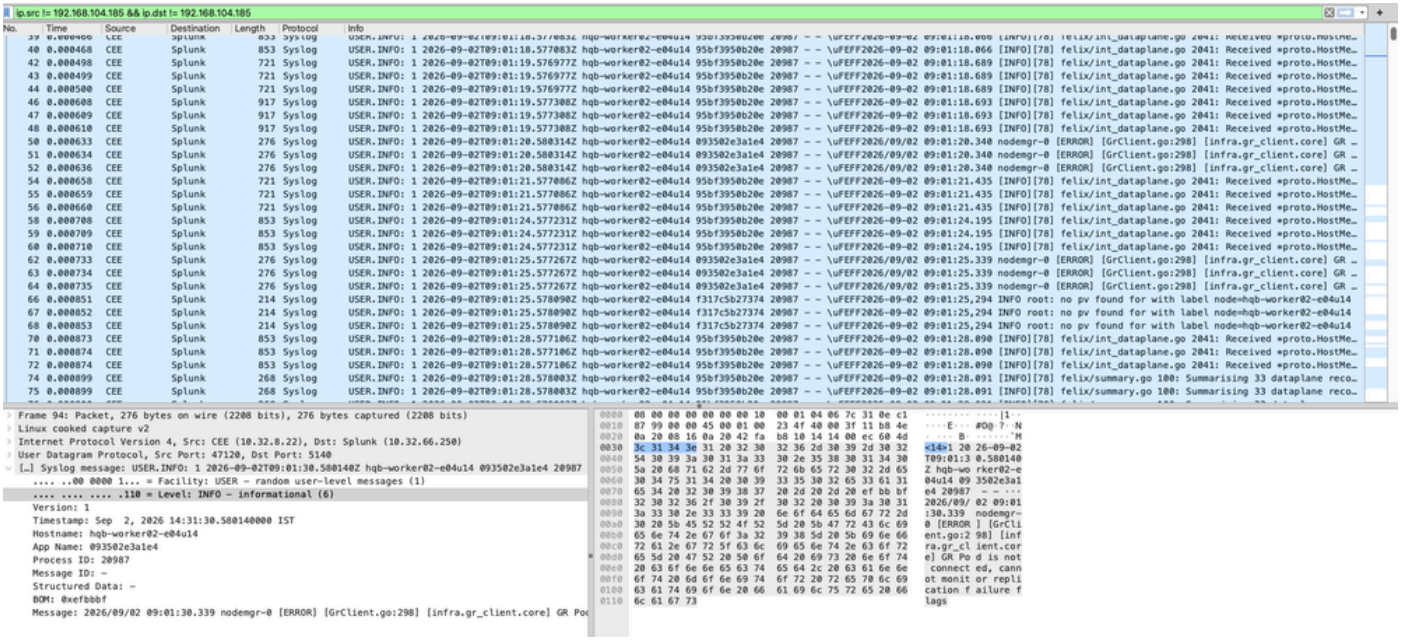
UDP ist verbindungslos und bietet weder eine Empfangsbestätigung noch eine erneute Übertragung. Bei der Fehlerbehebung müssen Paketverluste, Routing, MTU (Maximum Transmission Unit), Fragmentierung, Empfängerverfügbarkeit und Warteschlangen-/Ratenverhalten berücksichtigt werden.

Führen Sie auf der Schnittstelle oder dem Kubernetes-Knoten, der den Syslog-Datenverkehr überträgt, Folgendes aus:

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

Wenn der fluent-proxy den Syslog-Datenverkehr weiterleitet, ist der Knoten, der diese Komponente hostet, ein geeigneter Paketerfassungspunkt. Überprüfen Sie den Weiterleitungspfad, bevor Sie Pakete sammeln.

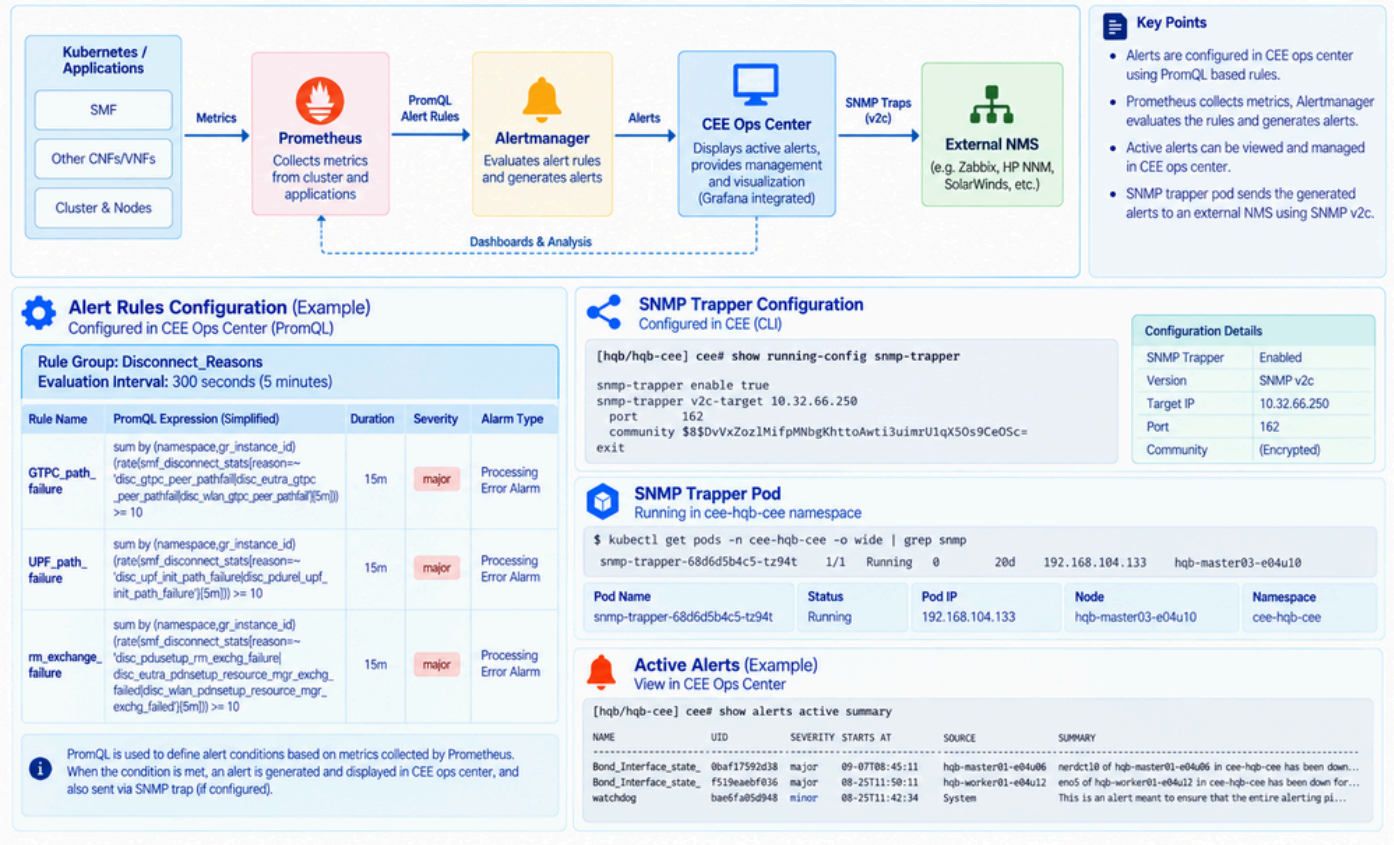
Anmerkung: RFC 5424 definiert ein Syslog-Nachrichtenformat unabhängig vom ausgewählten Transport. Im Quellszenario wird UDP 5140 verwendet. TLS-basierter Syslog-Transport ist eine andere Option, für die eine kompatible Absender- und Empfängerkonfiguration erforderlich ist.



CEE-Syslog-Weiterleitung an Splunk mit UDP-Port 5140 und RFC 5424-Feldern

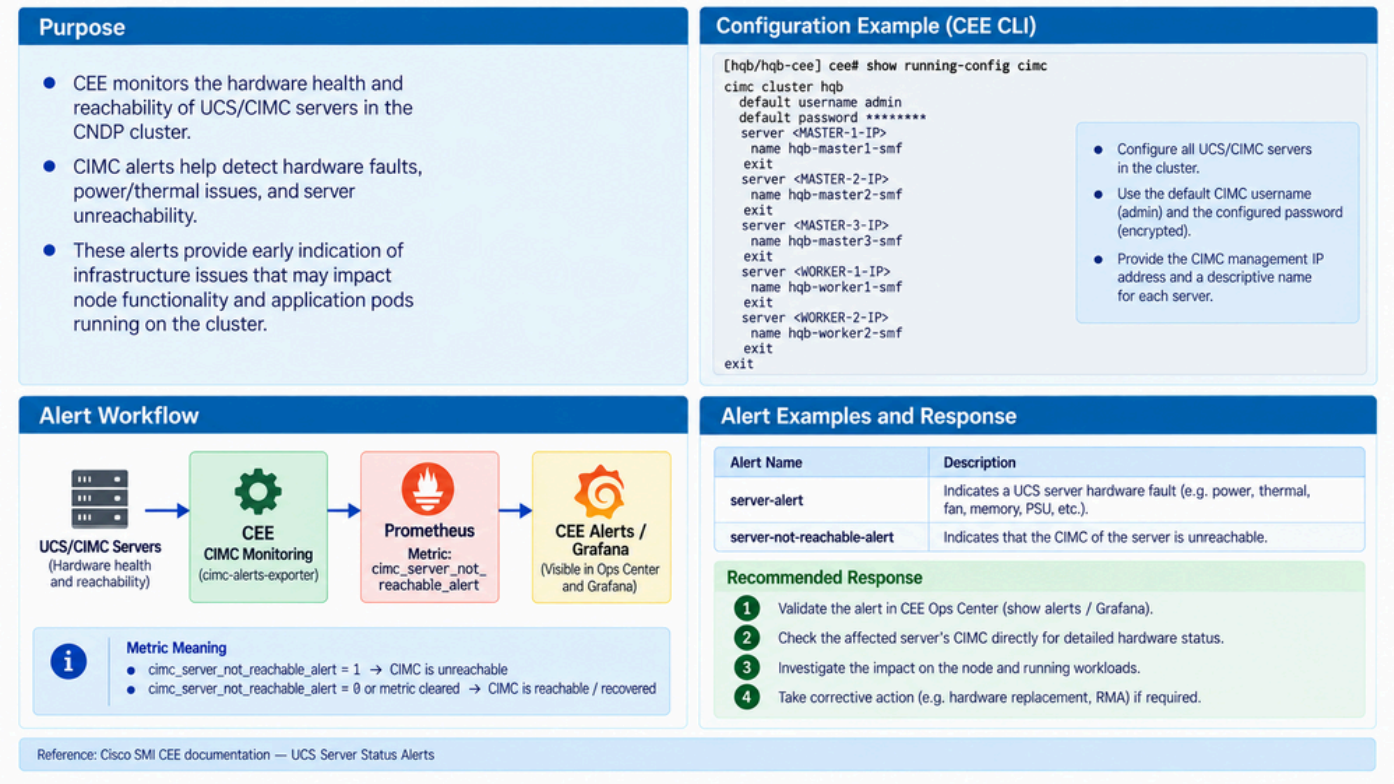
Warnmeldungen, SNMP und CIMC-Beobachtbarkeit

CEE-Warnmeldungen verwenden Prometheus und Alertmanager. Prometheus bewertet Metriken und Warnungsregeln. Der Warnungs-Manager leitet Warnungsereignisse an Empfänger weiter, wobei der Warnungs-Router zusätzliche Routing-Unterstützung bereitstellt. Der CEE Alert-Logger stellt historische Datensätze bereit, die über das CEE Ops Center abgerufen werden können.



CEE Prometheus und Alertmanager Warnweiterleitung und SNMP-Architektur

Die CIMC-Warnmeldungsintegration stellt einen entsprechenden Pfad zur Infrastrukturüberwachung bereit. Der cimc-alerts-Exporter sammelt CIMC-Alarminformationen und macht diese für die Überwachung und Visualisierung in Grafana verfügbar.

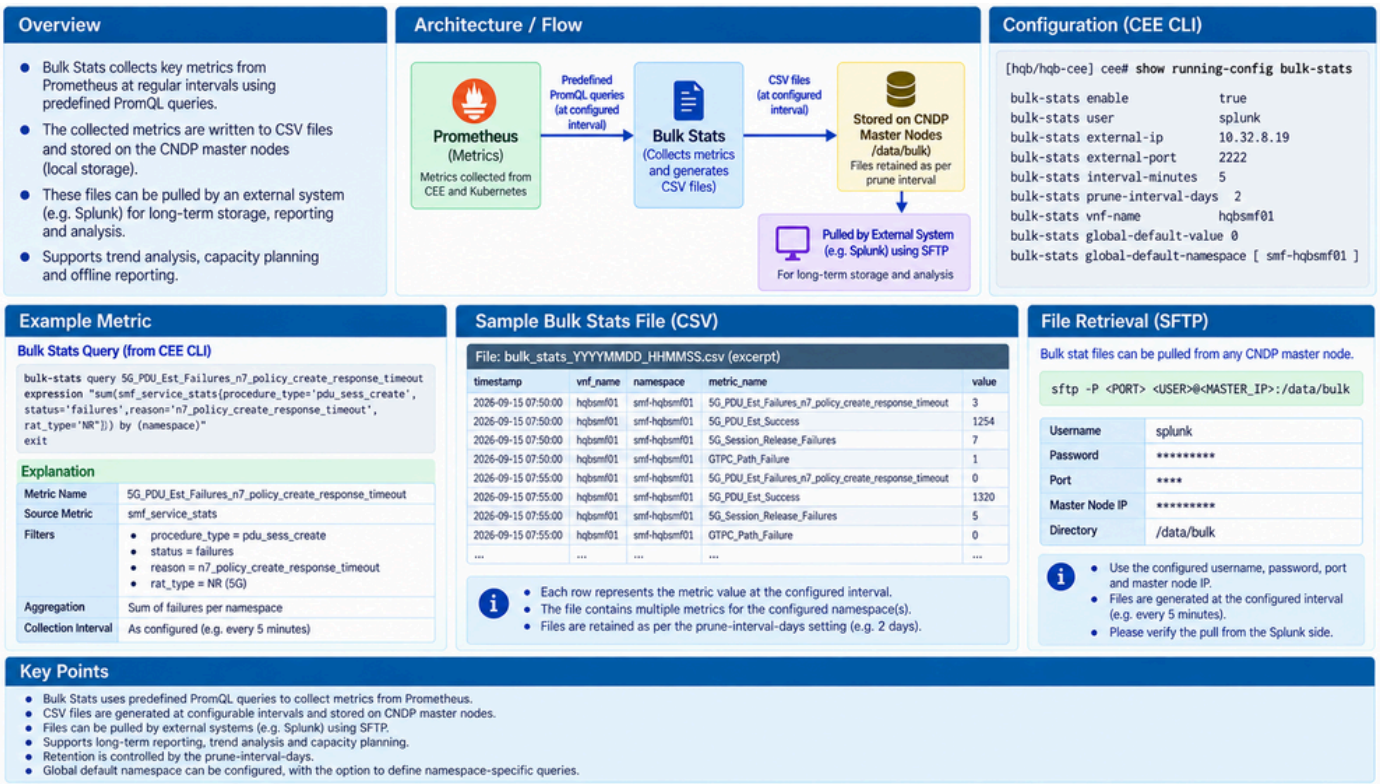


SNMP-Integration ist eine Alarm- und Verwaltungsschnittstelle. sie ist weder mit Splunk-HEC noch mit Syslog-Weiterleitung austauschbar. Das Protokoll und der Pfad für die Ereignisbereitstellung bleiben voneinander getrennt.

Zu den relevanten Referenzmaterialien für die Management Information Base (MIB) gehören CISCO-CNEE-MIB.my und CISCO-SMI.my.

Massenstatistiken

Der CEE Bulk-Stats-Service erstellt regelmäßig CSV-Snapshots (Comma-Separated Values) der durch Prometheus gesammelten Statistiken. Dies sind statistische Snapshots und keine Datenströme von Anwendungsprotokolldatensätzen.



CEE Bulk Statistics Service, der regelmäßige CSV-Snapshots aus Prometheus-Metriken erstellt

Bulk-Statistikausgabe unterstützt regelmäßige Berichte, Trendanalysen und nachgeschaltete Datenverarbeitung. Integrieren Sie sie nur dann in einem Splunk-Integrationspfad, wenn die Bereitstellung CSV-/Statistikdaten explizit an Splunk weiterleitet oder importiert.

OpenTelemetry System-Gateway

Neuere Cisco SMI-Versionen unterstützen ein plattformverwaltetes OpenTelemetry Collector-Gateway. Das Gateway empfängt Telemetriedaten von Anwendungen über das OpenTelemetry Protocol (OTLP) und leitet die unterstützten Metriken und Protokolle an lokale oder entfernte Backends weiter.



Anmerkung: Die Betriebsdokumentation von Cisco SMI Cluster Manager identifiziert die OpenTelemetry Gateway-Integration mit Version 2026.03.1. Das Gateway wurde in der im Quellbeispiel beschriebenen spezifischen Bereitstellung nicht validiert. Daher wird in diesem Abschnitt das veröffentlichte Konfigurationsmodell und nicht der verifizierte Betrieb in dieser Umgebung beschrieben.

System-Gateway-Modell

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

Gateway-Konfigurationskonzepte

Aktivieren Sie das OpenTelemetry Collector-Gateway, und wählen Sie die lokalen Metriken und Protokollierungs-Backends aus.

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

Wenn für die Bereitstellung eine externe Service-Anbindung erforderlich ist, kann die Konfiguration eine externe IP-Adresse beinhalten.

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

Für die Gateway-Exporteure werden optionale Proxy-Einstellungen konfiguriert.

```
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
```

Die Optionen für das lokale Backend steuern, wie das plattformverwaltete System-Gateway Telemetrie an integrierte Backends sendet. Die externe IP-Belichtung und die Proxy-Einstellungen hängen von der Topologie und den Sicherheitsanforderungen ab.

Remote-Exporteure

Exporteur	Signale	Technische Verwendung
totlp	Protokolle, Metriken	Senden Sie Telemetriedaten an ein Backend, das OTLP über gRPC akzeptiert.
Otlphttp	Protokolle, Metriken	Senden Sie Telemetriedaten an ein Backend, das OTLP über HTTP akzeptiert.
plunkhec	Protokolle	Senden von Protokollen an einen Splunk-HEC-Endpunkt
Zeitschrift	Protokolle	Protokolle in das Knotenjournal schreiben, sofern unterstützt.
Fehlersuche	Protokolle, Metriken	Unterstützt eine kontrollierte Validierung und Fehlerbehebung

Die OpenTelemetry-Pipeline folgt dem Empfangs-, Prozess- und Exportmodell. Empfänger empfangen Telemetrie; Prozessoren filtern oder transformieren Daten; Exporteure liefern die ausgewählten Signale an entfernte oder lokale Backends.

Die Quelle unterscheidet auch das Proxy-Verhalten: otlp verwendet die Einstellungen für den Collector-Instanz-Proxy, während otlphttp und splunkhec den Export-Level-Proxy überschreiben, wenn die bereitgestellte Version diese Konfiguration verfügbar macht.

Vergleich mit OpenShift OpenTelemetry

Cisco CEE und OpenShift verfügen über ein gemeinsames Architekturmuster: Ein OpenTelemetry Collector kann zwischen instrumentierten Anwendungen und Beobachtbarkeits-Backends sitzen. Ihre Verwaltungs- und Installationsmodelle sind unterschiedlich.

Konzept	CEE OpenTelemetry System Gateway	OpenShift OpenTelemetry-Muster
Telemetriequelle	OpenTelemetrie-fähige CEE- und Anwendungs-Workloads	OpenTelemetrie-fähige OpenShift-Workloads
Protokolle	OTLP	OTLP

Konzept	CEE OpenTelemetry System Gateway	OpenShift OpenTelemetry-Muster
Collector-Rolle	Plattform-verwaltetes System-Gateway	OpenTelemetry Collector-Bereitstellung oder -Instanz
Pipeline-Konzept	Empfangen, verarbeiten, exportieren	Empfangen, verarbeiten, exportieren
Backend-Flexibilität	Lokale Backends und unterstützte Remote-Exporteure	Exportergesteuerte Backend-Integration
Splunk-Integration	splunkhec-Exporteur in dokumentierter CEE-Konfiguration	Splunk-HEC-Exporteur (konfiguriert)

Dieser Vergleich basiert auf der Architektur. Die beiden Plattformen sollen OpenTelemetry nicht identisch implementieren. OpenShift verwendet in der Regel ein OpenTelemetry Operator/Collector-Bereitstellungsmodell, während das Cisco SMI-System-Gateway plattformverwaltet wird.

Die im Quelltext besprochene OpenShift-Referenzarchitektur zeigt, wie Collectors Telemetrie von Kubernetes-Workloads an Splunk über HEC weiterleiten. Es zeigt das kollektorbasierte Modell anstelle einer verifizierten Integration für die Beispiel-CEE-Installation.

Überprüfen der Konfiguration

CEE-Synchronisierung überprüfen

Überprüfen Sie den SMI Cluster Manager-Synchronisierungsstatus und die Protokolle, und bestätigen Sie, dass die erwarteten CEE-Workloads bereitgestellt wurden.

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

Separate Überprüfung von HEC und Syslog

Bestätigen Sie, dass der HEC-Pfad Ereignisse an den konfigurierten TCP 8088-Endpunkt sendet und dass Splunk diese empfängt. Separat bestätigen, dass der Syslog-Pfad UDP 5140-Datensätze an den konfigurierten Listener sendet.

Verwenden Sie die Paketerfassungsmethoden in den entsprechenden Abschnitten, und korrelieren Sie die Paket-Zeitstempel mit Ereignissen, die am konfigurierten Collector empfangen wurden.

Services zur Beobachtbarkeit überprüfen

Vergewissern Sie sich, dass Metriken, Alert-Routing, CIMC-Warnungen und Bulk-Statistics-Snapshots wie für die installierte Version vorgesehen funktionieren. Wenn OpenTelemetry aktiviert ist, überprüfen Sie die Integrität von Empfänger, Pipeline und Exporteur mithilfe des unterstützten SMI Cluster Manager-Verfahrens.

Erwartetes Verhalten

Komponente oder Pfad	Erwartetes Ergebnis
SMI-Cluster-Manager	Die Cluster-Synchronisierung ist abgeschlossen, und die erforderlichen CEE-Services werden bereitgestellt.
Betriebszentrum	Autorisierte Benutzer können auf Betriebsfunktionen und unterstützte Konfigurations-/Überwachungsbefehle zugreifen.
Splunk HEC	Der Ereignisverkehr erreicht den konfigurierten HEC-Listener auf dem TCP-Port 8088.
Syslog	Ereignisse im RFC 5424-Format erreichen den konfigurierten UDP-Port 5140-Listener.
Warnungen und CIMC	AlertManager und zugehörige Exporteure machen die konfigurierten Warnmeldungsinformationen verfügbar.
Massenstatistiken	Regelmäßige CSV-Snapshots werden aus den erfassten Statistiken erstellt.
OffeneTelemetrie	In unterstützten Versionen, für die das Gateway konfiguriert ist, durchlaufen die OTLP-Signale die ausgewählte Back-End-/Export-Pipeline.

Entscheidungsablauf

Beobachtung	Nächste Prüfung
CEE-Dienste fehlen nach der Synchronisierung.	Überprüfen Sie den Cluster Manager-Synchronisierungsstatus, Protokolle, Software-Artefakte und die Parameter des Betriebscenters.
HEC-Ereignisse fehlen.	Ermitteln Sie den weiterleitenden POD/Knoten, überprüfen Sie den TCP-8088-Datenverkehr, das HEC-Ziel, die Authentifizierung und die TLS-Konfiguration.
Syslog-Ereignisse fehlen.	Überprüfen des UDP 5140-Ziels, der RFC 5424-Formatierung, des Paketflusses und des Empfängerverhaltens
Warnungen oder CIMC-Daten fehlen.	Prüfen Sie den Betrieb von Prometheus/Alertmanager Routing, Alert-Router und cimc-alerts-export.
Massenstatistiken fehlen.	Bestätigen Sie den Bulk-Stats-Service, die Verfügbarkeit der Prometheus-Daten und die Generierung von CSV-Snapshots.
OpenTelemetry-Export fehlt.	Überprüfen der Funktionsunterstützung für die installierte Version, die Gateway-Konfiguration, den Empfänger- und Exporterstatus und die Pipeline-Mitgliedschaft

Schlussfolgerung

CEE ist eine mehrschichtige Kubernetes-basierte Ausführungs- und Beobachtungsumgebung für SMF-Anwendungen. Durch die Aufteilung des Kubernetes-Namespace werden Plattformabläufe, CEE-Services und Anwendungs-Workloads in verschiedene Domänen unterteilt. In CEE sind Überwachung, Alarmierung, Protokollierung und Massenstatistiken spezialisierte Services mit unabhängigen Verantwortlichkeiten.

Die wichtigste Splunk-Unterscheidung betrifft HEC über TCP 8088 und Syslog über UDP 5140. Hierbei handelt es sich um separate Weiterleitungspfade mit unterschiedlichen Protokollen, Konfigurationen und Fehlerbehebungsverfahren. Das neuere OpenTelemetry System-Gateway fügt ein OTLP-basiertes Collector- und Exporter-Modell hinzu. Die Architektur ähnelt OpenShift OpenTelemetry, und der Gateway-Betrieb muss für die spezifische CEE-Version und -Bereitstellung überprüft werden.

Verwandte Inhalte

- Cisco CEE Konfigurations- und Administrationsleitfaden - Allgemeine Ausführungsumgebung
- Cisco CEE Konfigurations- und Administrationsleitfaden - Protokollbefehle
- Cisco SMI Cluster Manager Operations - Synchronisierung und OpenTelemetry
- RFC 5424 - The Syslog Protocol

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.