Cisco CEE Observability en Splunk Integration begrijpen

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Overzicht architectuur

CEE-naamruimte-werklasten

CEE Installatie en Lifecycle Management

- Installatiemodi
- Het CEE Software Artefact definiëren
- Het cluster en het Ops-centrum configureren
- De implementatie synchroniseren en verifiëren

CEE Ops Center en Operationeel Management

CEE Observability Architecture

Splunk-integratie: logoverdrachtarchitectuur

Splunk HTTP Event Collector Forwarding

- HEC-configuratiemodel
- HEC-verkeer vastleggen en oplossen

Syslog Forwarding via UDP 5140

- RFC 5424 Field Mapping
- UDP Transport en Packet Capture

Waarschuwingen, SNMP en CIMC-observatie

bulkstatistieken

OpenTelemetry System Gateway

- Systeemgatewaymodel
- Configuratieconcepten gateway
- Exporteurs op afstand
- Vergelijk met OpenShift

De configuratie verifiëren

- CEE-synchronisatie verifiëren
- HEC en Syslog afzonderlijk controleren
- Waarnemingsdiensten verifiëren

verwacht gedrag

beslissingsstroom

Conclusie

Gerelateerde inhoud

Inleiding

In dit document worden de Cisco Common Execution Environment (CEE)-architectuur, implementatie, bewaking, Splunk-integratie en OpenTelemetry beschreven.

Voorwaarden

Vereisten

Cisco raadt aan om deze technologieën te leren kennen:

- Cloud Native Deployment Platform (CNDP), Kubernetes-naamruimten en pod-plaatsing.
- Cisco Subscriber Microservices Infrastructure (SMI) en de SMI Cluster Manager.
- CEE Ops Center, Prometheus, Grafana, AlertManager en log-forwarding componenten.
- Splunk HTTP Event Collector (HEC), syslog en packet capture met tcpdump.
- OpenTelemetry Protocol (OTLP) en de OpenTelemetry Collector voor de nieuwere gateway-integratie.

Gebruikte componenten

De voorbeelden tonen een op Kubernetes gebaseerde Cisco SMI/CNDP-omgeving met CEE en een bijbehorende Session Management Function (SMF)-toepassing. Het voorbeeld van de softwaredefinitie verwijst naar het CEE-pakket 2026.01.1.08; het voorbeeld van het Ops Center gebruikt een SMF-identificatiecode van de opslagplaats smf-2026.04.m0.i50. Dit zijn voorbeeldwaarden, geen implementatievereisten.

Netwerkeindpunten, clusternamen en naamruimtewaarden moeten worden vervangen door waarden die zijn goedgekeurd voor de doelimplementatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Common Execution Environment (CEE) maakt deel uit van Cisco Subscriber Microservices

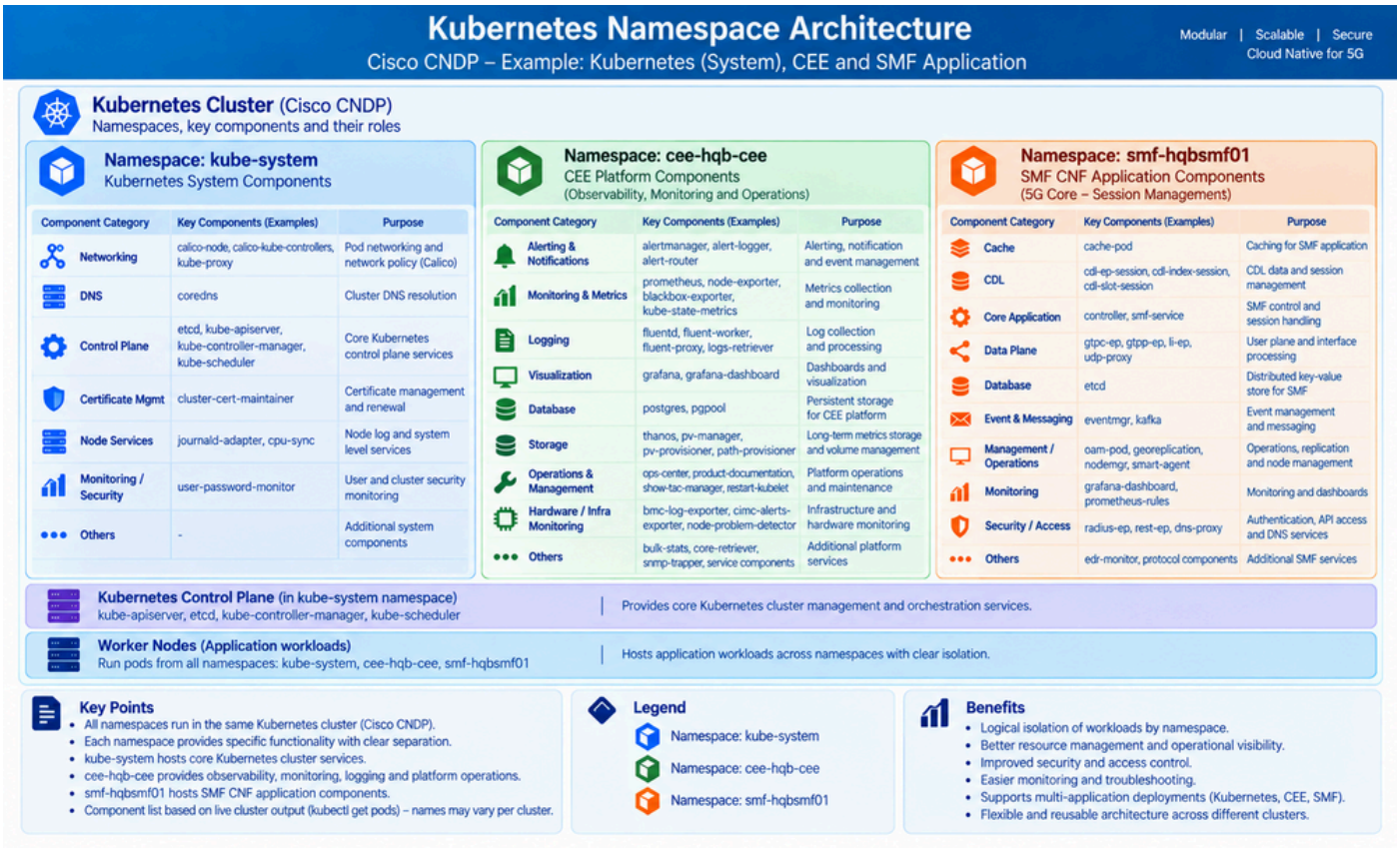
Infrastructure (SMI). In een op Kubernetes gebaseerde CNDP-implementatie biedt Kubernetes namespaces voor afzonderlijke platformservices, CEE-observabiliteits- en Kubernetes-beheerservices en SMF-toepassingsworkloads. De scheiding biedt administratieve en operationele grenzen, terwijl Kubernetes-netwerken en servicedetectie toegestane componentcommunicatie mogelijk maken.

Dit document behandelt naamruimtearchitectuur, CEE-werklasten, CEE-installatie en levenscyclusbeheer, CEE Ops Center, waarschuwingen en Simple Network Management Protocol (SNMP), Cisco Integrated Management Controller (CIMC) -waarschuwingen, logforwarding, bulkstatistieken en de OpenTelemetry-systeemgateway.

Splunk HEC op Transmission Control Protocol (TCP) poort 8088 en syslog over User Datagram Protocol (UDP) poort 5140 zijn onafhankelijke inslikmechanismen. De twee paden hebben verschillende configuratie-, transport- en probleemoplossingsvereisten en kunnen naast elkaar bestaan.

Overzicht architectuur

CEE en de bijbehorende toepassingsfuncties bezetten afzonderlijke Kubernetes-naamruimten. De architectuur onderscheidt Kubernetes-platformdiensten van CEE-observatie- en beheerfuncties en van het SMF-toepassingsdomein.



Cisco SMI-naamruimtearchitectuur die CEE en scheiding van toepassingsplatforms toont

De CEE-naamruimte is de belangrijkste focus van de architectuur op serviceniveau. Andere naamruimten bieden het Kubernetes-platform, netwerkfuncties en SMF-werklasten.

CEE-naamruimte-werklasten

De CEE namespace host microservices voor monitoring, alarmering, logging, dashboards, statistieken en operationele toegang.



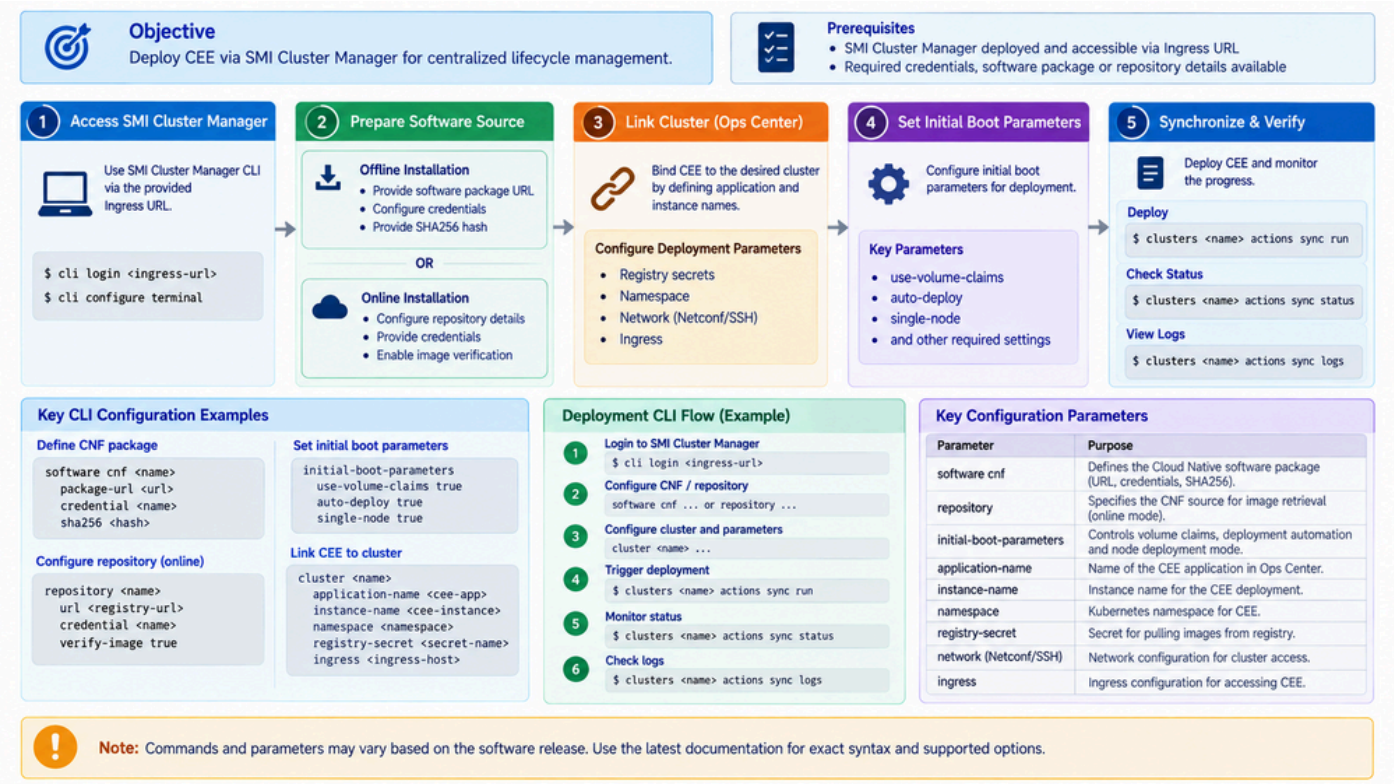
CEE namespace microservices en de functies van de operationele werklasten

Deze functies omvatten de verzameling van Prometheus-statistieken, Grafana-visualisatie, AlertManager-alarmafhandeling, logforwarding-services en het maken van periodieke bulkstatistieken. Individuele werkbelastingen verschillen per release- en implementatieconfiguratie.

CEE Installatie en Lifecycle Management

De SMI Cluster Manager scheidt de definitie van het softwarearepunt van het doelcluster en de

configuratie van het Ops Center. Dit maakt gecontroleerde softwareversie en herhaalbare clustersynchronisatie mogelijk.



Installatie- en softwaresynchronisatiearchitectuur voor SMI Cluster Manager CEE

Installatiemodi

- Offline installatie kan verwijzen naar een lokaal softwarepakket via een bestand URL en een Secure Hash Algorithm 256-bit (SHA-256) hash.
- Clusterconfiguratie koppelt de CEE/SMF-implementatie aan de beoogde cluster- en Ops Center-installatie.

Het CEE Software Artefact definiëren

Identificeer in de configuratie van SMI Cluster Manager het lokale CEE-softwarepakket en de SHA-256-hash.

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

Gebruik de exacte SHA-256-waarde uit de goedgekeurde verpakking. De plaatsaanduiding in de opdracht is opzettelijk en vertegenwoordigt geen werkelijke controlesom.

Het cluster en het Ops-centrum configureren

De bronconfiguratie koppelt een cluster aan een SMF Ops Center, lokale repository, beheereindpunten en implementatie-instellingen. Locatiespecifieke identificatiemiddelen worden vervangen door plaatsaanduidingen.

```
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	Betekenis in de voorbeeldconfiguratie
OPS-Centers SMF <SMF-OPS-Center-Name>	Koppelt het cluster aan de instantie SMF Ops Center.
lokaal in de repository	Hiermee geeft u de toepassingsrepository en de versie voor implementatie op.
sync-default-repository true	Maakt gebruik van de geconfigureerde standaard repository tijdens synchronisatie.
NetConf-poort 2029	Hiermee geeft u de connectiviteitspoort voor NETCONF-beheer op.
SSH-poort 2028	Hiermee geeft u de connectiviteitspoort voor SSH-beheer (Secure Shell) op.
use-volume-claims true	Maakt het gebruik van volumeclaims voor permanente opslagvereisten mogelijk.
Vals automatisch implementeren	Schakelt automatische implementatie uit, zodat synchronisatie en validatie onder expliciete controle blijven.
single-node false	Hiermee geeft u een implementatie op die zich niet in de modus voor één knooppunt bevindt.



Opmerking: De pakketidentificatie en de identificatiecode van de repository zijn

voorbeelden uit de bronconfiguratie. Bevestig de compatibiliteit van de release en de eindpuntwaarden voordat u deze in een ander cluster gebruikt.

De implementatie synchroniseren en verifiëren

Voer de clustersynchronisatieactie uit nadat de software en de Ops Center-configuratie gereed zijn.

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

Controleer de synchronisatiestatus en logs.

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

Bevestig dat de synchronisatie met succes is voltooid en dat de verwachte CEE-pods en -services zijn geïmplementeerd.

⚠ Waarschuwing: clustersynchronisatie en software-implementatie kunnen de actieve omgeving wijzigen. Breng wijzigingen aan volgens de goedgekeurde onderhouds- en implementatieprocedure.

CEE Ops Center en Operationeel Management

CEE Ops Center biedt de operationele interface voor CEE-diensten. De werkbelasting ondersteunt gebruikersbeheer, verificatie, configuratie en weergaveopdrachten voor CEE-functies binnen het cluster. De SMI Cluster Manager koppelt het Ops Center aan de doelimplementatie via de beheerconfiguratie.

Ops Center behoort tot het managementvliegtuig. Prometheus, AlertManager, Fluent Bit/fluent-proxy, HEC, syslog en OpenTelemetry behoren tot de monitoring- en telemetriepaden. Het gescheiden houden van deze verantwoordelijkheden vereenvoudigt het oplossen van problemen.

CEE Observability Architecture

CEE observabiliteit omvat metrics, waarschuwingen, logs, CIMC waarschuwingen, en bulk statistieken. Deze diensten zijn gerelateerd, maar de gegevenspaden en consumenten zijn verschillend.

functie	Primair doel	Typische bestemming of consument
metriek	Tijdreeksmetingen verzamelen en opvragen van knooppunten, Kubernetes en services.	Prometheus, Grafana en Thanos.
Dringende berichten	Waarschuwingsregels en routewaarschuwingen evalueren.	AlertManager, alert-router, Ops Center en externe ontvangers.
Logboeken	Logbestanden en gebeurtenisrecords doorsturen naar externe verzamelaars of back-ends.	Splunk en andere houtverzamelaars.
CIMC-waarschuwingen	Waarschuwingen voor Cisco Integrated Management Controller exporteren voor bewaking.	CEE metrics/alerting en Grafana.
Bulkstatistieken	Maak periodieke statistische momentopnamen.	CSV-momentopnamen en downstreamverwerking of -analyse.

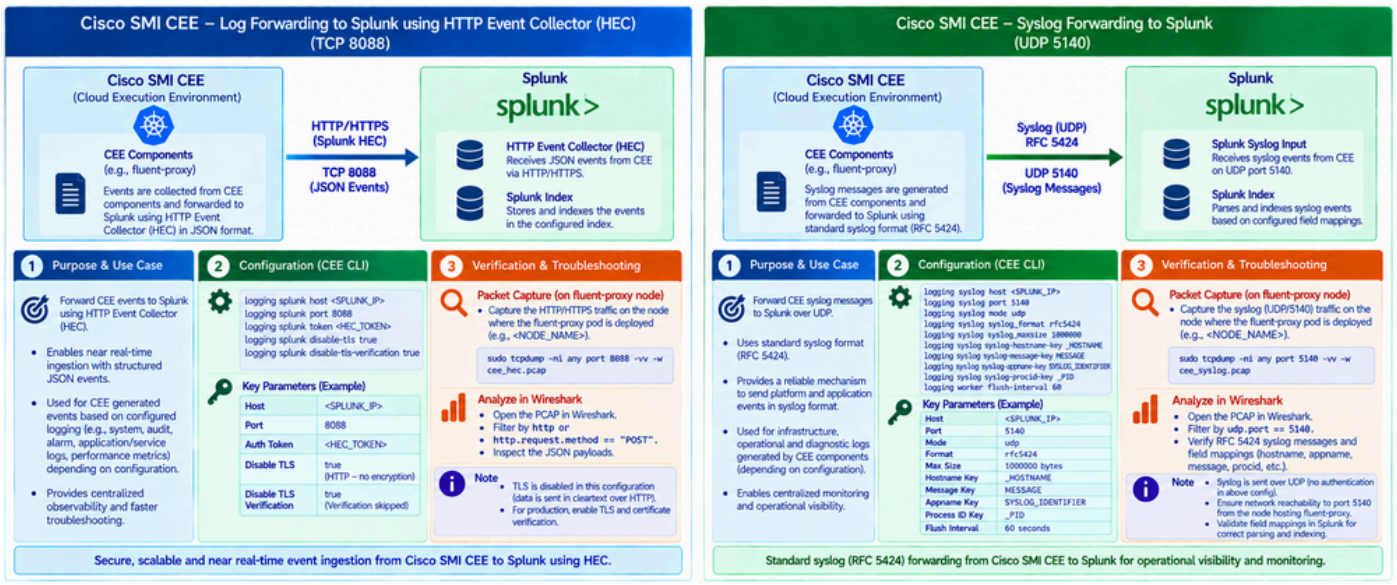
Splunk-integratie: logoverdrachtarchitectuur

De bron beschrijft twee CEE-naar-Splunk paden. Beide kunnen gebeurtenissen leveren aan Splunk, maar ze gebruiken verschillende protocollen en inname-interfaces.

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

De gebeurtenistypen die door elk pad worden uitgevoerd, zijn afhankelijk van de CEE-configuratie en de geïmplementeerde doorstuurpijplijn. Twee geconfigureerde interfaces stellen niet vast dat elk een elkaar uitsluitende categorie gebeurtenissen bevat.

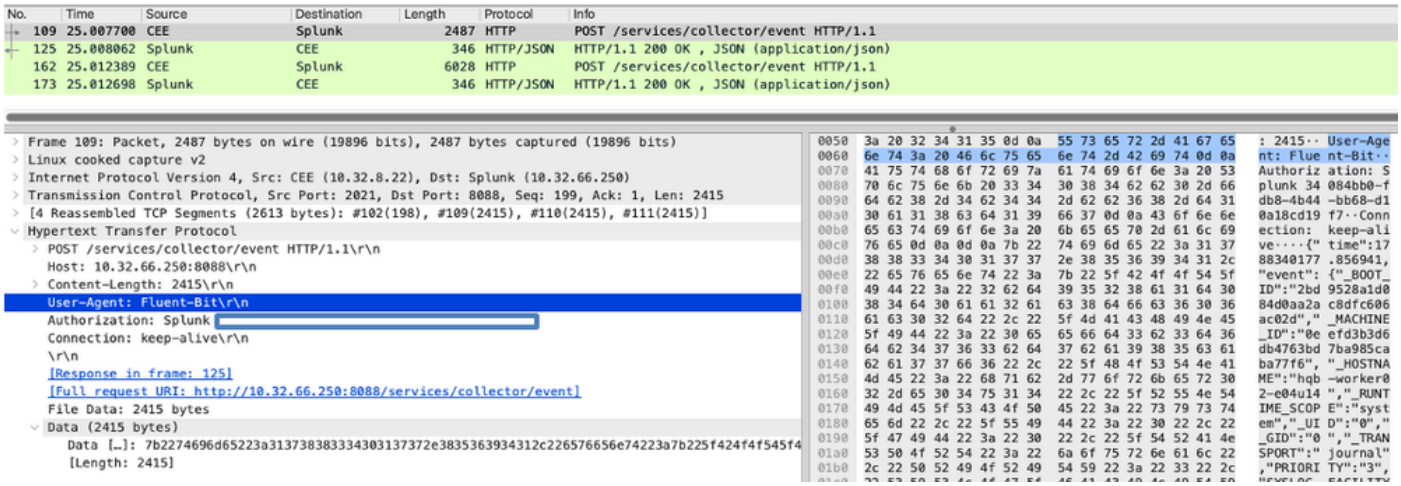
Traceer de paden afzonderlijk. Succesvolle HEC-levering bevestigt de syslog-levering niet en succesvolle syslog-levering bevestigt de HEC-levering niet.



CEE Splunk-integratie met afzonderlijke HEC- en syslog-doorstuurpaden

Splunk HTTP Event Collector Forwarding

Splunk HEC accepteert HTTP-gebeurtenisinzendingen en gebruikt een HEC-verificatietoken. CEE stuurt gebeurtenissen rechtstreeks door naar de geconfigureerde HEC-service in plaats van bestandsgebaseerde inname voor dit pad te vereisen.



CEE naar Splunk HTTP Event Collector doorstuurarchitectuur op TCP-poort 8088

HEC-configuratiemodel

Het oorspronkelijke labvoorbeeld bevat deze instellingen voor een CEE Splunk-eindpunt. Het uittreksel registreert het brongedrag en is geen aanbevolen productieconfiguratie.

⚠

> Waarschuwing: In het bronvoorbeeld wordt zowel TLS- als certificaatverificatie uitgeschakeld. Dit stelt telemetrie en HEC-referenties bloot aan onderschepping op het netwerk. Schakel voor productie TLS- en certificaatverificatie in en beveilig het HEC-verificatietoken volgens de ondersteunde CEE-vrijgaveconfiguratie.

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

In de bronarchitectuur sturen CEE-log-/evenementenproducenten via de relevante Fluent-doorstuurcomponent door naar de HEC-bestemming.

```
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
```

HEC-verkeer vastleggen en oplossen

Identificeer de fluent-proxy-pod en de Kubernetes-werknemersknooppunt in de CEE-naamruimte wanneer fluent-proxy het HEC-verkeer vervoert.

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

Op de Kubernetes-node die het HEC-verkeer vervoert, vangen pakketten voor de HEC-poort.

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

Voor een TLS-compatibele verbinding onthult een pakketopname de gegevens van de transportinstelling en de bestemming, maar wordt de HTTP-payload normaal gesproken niet zichtbaar. Als TLS is uitgeschakeld, kunnen de inhoud van de gebeurtenis en het verificatiemateriaal zichtbaar zijn in de opname.

⚠ Let op: pakketopnamen en logs kunnen gevoelige telemetrie en referenties bevatten. Verzameling en overdracht beperken tot geautoriseerde ondersteuningsworkflows en opnamebestanden beveiligen.

Syslog Forwarding via UDP 5140

Het tweede Splunk-integratiepad stuurt syslog-records door met RFC 5424-opmaak en UDP-poort 5140. De bronconfiguratie definieert ook veldtoewijzingen, de maximale berichtgrootte en het spoelinterval van de werknemer.

```
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 Field Mapping

CEE-bronveld	Sysloogveld of -doel
_HOSTNAAM	Identificeert de oorspronkelijke host in het gegenereerde syslog-record.
BOODSCHAP	Draagt de log-message body.
SYSLOG_IDENTIFIER	Biedt de syslog-toepassing of programma-id.
_PID	De oorspronkelijke proces-ID wordt meegenomen.

UDP Transport en Packet Capture

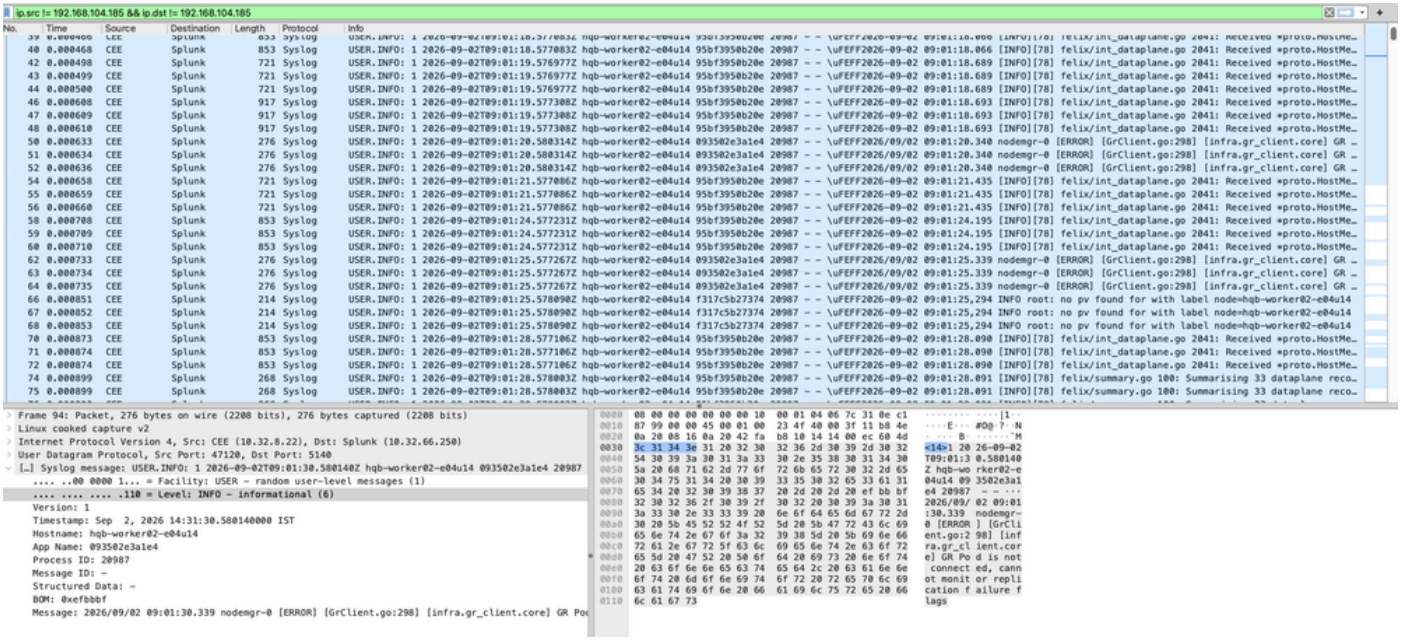
UDP is verbindingsloos en biedt geen bevestiging van de levering van het transport of hertransmissie. Bij het oplossen van problemen moet rekening worden gehouden met pakketverlies, routering, maximale transmissieeenheid (MTU), fragmentatie, beschikbaarheid van de ontvanger en wachtrijgedrag.

Voer op de interface of de Kubernetes-node die het syslog-verkeer vervoert:

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

Als fluent-proxy het syslog-verkeer doorstuurt, is de node die die component host een geschikt pakketopnamepunt. Controleer het doorstuurpad voordat u pakketten verzamelt.

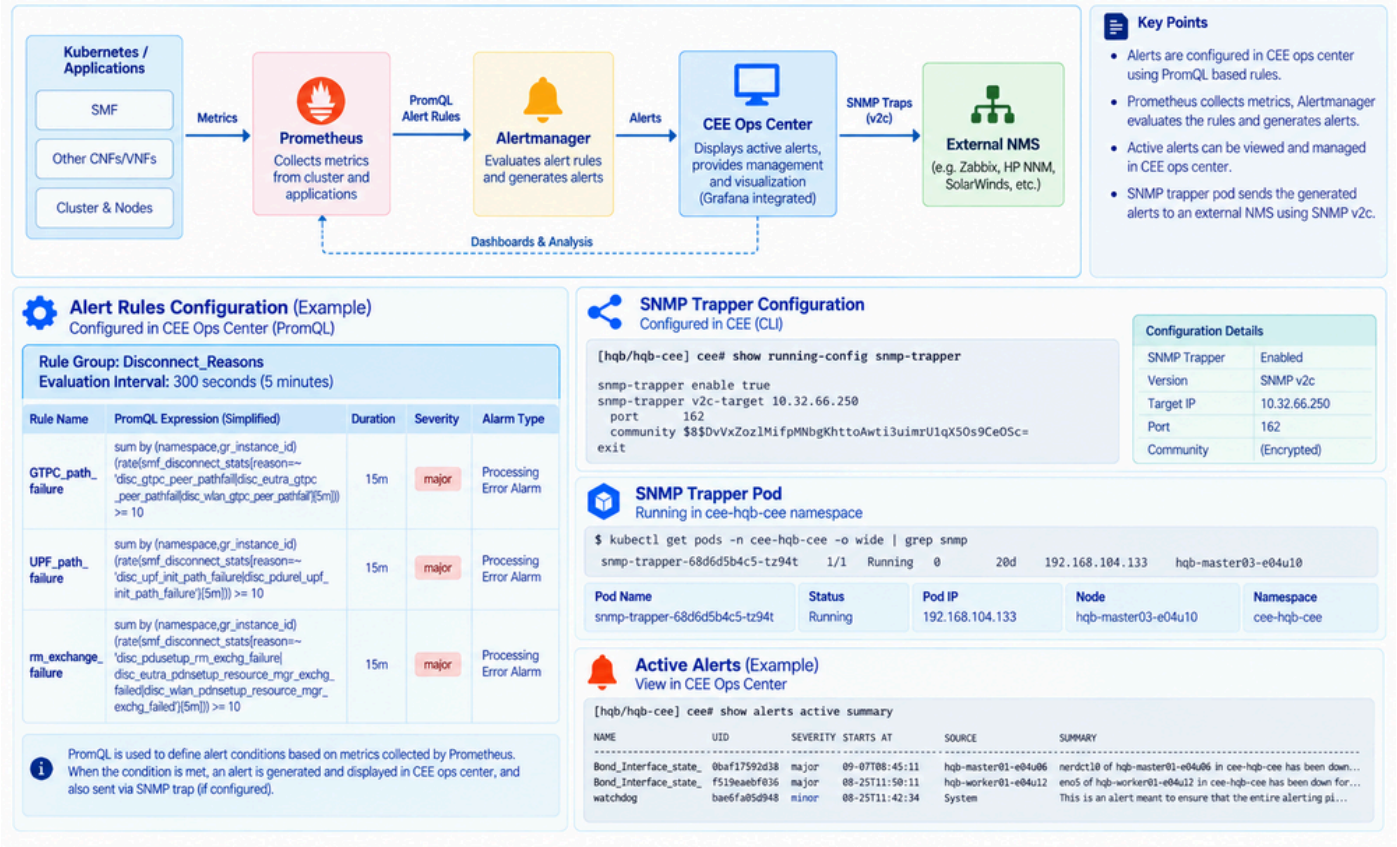
Opmerking: RFC 5424 definieert een syslog-berichtformaat onafhankelijk van het geselecteerde transport. Het bronscenario maakt gebruik van UDP 5140. TLS-gebaseerd syslog transport is een andere optie die compatibele afzender en ontvanger configuratie vereist.



CEE-syslog doorsturen naar Splunk met behulp van UDP-poort 5140 en RFC 5424-velden

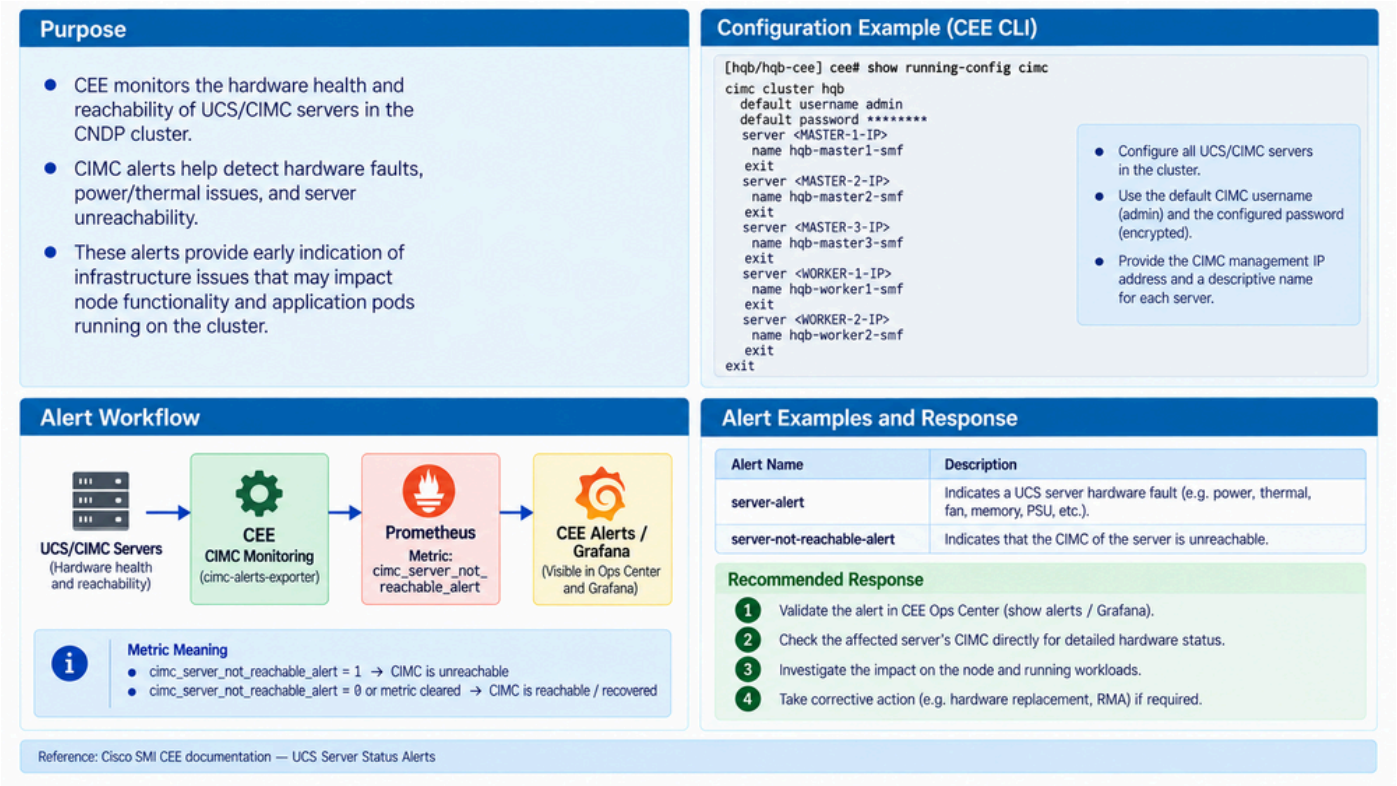
Waarschuwingen, SNMP en CIMC-observatie

CEE Alerting maakt gebruik van Prometheus en Alertmanager. Prometheus evalueert metrics en waarschuwingsregels. AlertManager routeert waarschuwingsgebeurtenissen naar ontvangers, met een waarschuwingsrouter die extra routeringsondersteuning biedt. CEE alert-logger biedt historische waarschuwingsrecords voor ophalen via CEE Ops Center.



CEE Prometheus en AlertManager alert forwarding en SNMP architectuur

De integratie van CIMC-waarschuwingen biedt een gerelateerd monitoringpad voor de infrastructuur. De cimc-alerts-exporter verzamelt CIMC-waarschuwingsinformatie en stelt deze bloot voor monitoring en visualisatie in Grafana.

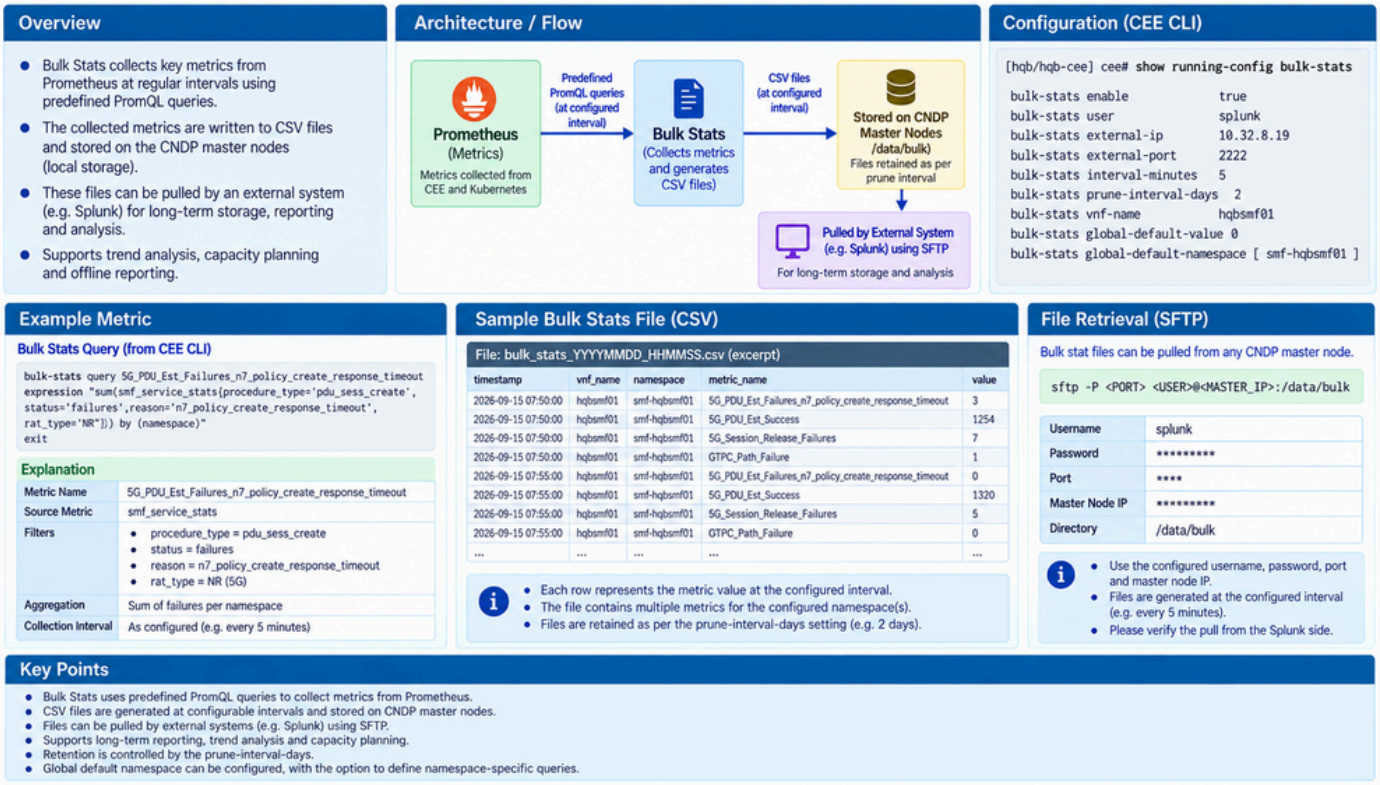


SNMP-integratie is een waarschuwings- en beheerinterface; deze is niet uitwisselbaar met Splunk HEC of syslog forwarding. Het protocol en de gebeurtenisafleveringstrajecten blijven verschillend.

Relevante Management Information Base (MIB) referenties zijn CISCO-CNEE-MIB.my en CISCO-SMI.my.

bulkstatistieken

De CEE bulk-stats service maakt periodieke Comma-Separated Values (CSV) momentopnamen van statistieken verzameld via Prometheus. Dit zijn statistische momentopnamen in plaats van streams van logbestanden van toepassingen.



CEE bulkstatistiekdienst die periodieke CSV-momentopnamen maakt van Prometheus-statistieken

Bulk-output statistieken ondersteunen periodieke rapportage, trendanalyse en downstream gegevensverwerking. Neem het alleen op in een Splunk-integratiepad wanneer de implementatie expliciet CSV/statistische gegevens doorstuurt of importeert naar Splunk.

OpenTelemetry System Gateway

Nieuwere Cisco SMI releases ondersteunen een platform-managed OpenTelemetry Collector gateway. De gateway ontvangt telemetrie van toepassingen via het OpenTelemetry Protocol (OTLP) en stuurt ondersteunde statistieken en logs door naar lokale of externe backends.



Opmerking: in de documentatie van Cisco SMI Cluster Manager Operations wordt de integratie van de OpenTelemetry-gateway geïdentificeerd met versie 2026.03.1. De gateway is niet gevalideerd in de specifieke implementatie die in het bronvoorbeeld wordt beschreven, dus in dit gedeelte wordt het gepubliceerde configuratiemodel beschreven in plaats van de geverifieerde werking in die omgeving.

Systeemgatewaymodel

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

Configuratieconcepten gateway

Schakel de OpenTelemetry Collector-gateway in en selecteer de lokale statistieken en logboekback-ends.

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

Wanneer voor de implementatie externe serviceblootstelling vereist is, kan de configuratie een extern IP-adres bevatten.

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

Optionele proxy-instellingen worden geconfigureerd voor de gateway-exporteurs.

```
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
```

De lokale back-endopties bepalen hoe de platformbeheerde systeemgateway telemetrie naar ingebouwde back-ends verzendt. Externe IP-belichting en proxy-instellingen zijn afhankelijk van de topologie en beveiligingsvereisten.

Exporteurs op afstand

exporteur	seinen	Technisch gebruik
OTLP	Logboeken, statistieken	Stuur telemetrie naar een backend die OTLP via gRPC accepteert.
otlphttp	Logboeken, statistieken	Stuur telemetrie naar een backend die OTLP via HTTP accepteert.
afgestompt	Logboeken	Logs verzenden naar een Splunk HEC-eindpunt.
dagboek	Logboeken	Schrijf logboeken naar het node-journaal waar dit wordt ondersteund.
debuggen	Logboeken, statistieken	Ondersteuning voor gecontroleerde validatie en probleemoplossing.

De OpenTelemetry-pijplijn volgt het ontvangst-, proces- en exportmodel. Ontvangers nemen telemetrie in; processors filteren of transformeren gegevens; exporteurs leveren de geselecteerde signalen aan externe of lokale backends.

De bron onderscheidt ook proxygedrag: otlp maakt gebruik van collector-instance proxy-instellingen, terwijl otlphttp en splunkhec ondersteuning bieden voor proxy-instellingen op exportniveau waar de geïmplementeerde release die configuratie blootlegt.

Vergelijk met OpenShift

Cisco CEE en OpenShift hebben een gedeeld architectonisch patroon: een OpenTelemetry Collector kan tussen geïnstrumenteerde toepassingen en observabiliteitsbackends zitten. De beheer- en installatiemodellen zijn verschillend.

concept	CEE OpenTelemetry system gateway	OpenShift OpenTelemetry-patroon
telemetriebron	OpenTelemetry-enabled CEE en applicatiewerkbelastingen	OpenShift-werklasten met OpenTelemetry
Protocol	OTLP	OTLP

concept	CEE OpenTelemetry system gateway	OpenShift OpenTelemetry-patroon
Collectorrol	Platform-managed system gateway	Implementatie of installatie van OpenTelemetry Collector
Pijpleidingconcept	Ontvangen, verwerken, exporteren	Ontvangen, verwerken, exporteren
Flexibiliteit van backend	Lokale backends en ondersteunde externe exporteurs	Exportergestuurde backendintegratie
Splunk-integratie	splunkhec-exporteur in de gedocumenteerde CEE-configuratie	Splunk HEC-exporteur indien geconfigureerd

Deze vergelijking is architectonisch. Er wordt niet beweerd dat de twee platforms OpenTelemetry op dezelfde manier implementeren. OpenShift gebruikt meestal een OpenTelemetry Operator/Collector-implementatiemodel, terwijl de Cisco SMI-systeemgateway platformbeheerd is.

De OpenShift-referentiearchitectuur die in de bron wordt besproken, toont verzamelaars die telemetrie van Kubernetes-werklasten doorsturen naar Splunk over HEC. Het illustreert het collector-based model in plaats van een geverifieerde integratie voor de steekproef CEE installatie.

De configuratie verifiëren

CEE-synchronisatie verifiëren

Controleer de synchronisatiestatus en logbestanden van SMI Cluster Manager en bevestig dat de verwachte CEE-werklasten zijn geïmplementeerd.

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

HEC en Syslog afzonderlijk controleren

Bevestig dat het HEC-pad gebeurtenissen naar het geconfigureerde TCP 8088-eindpunt verzendt en dat Splunk ze ontvangt. Bevestig afzonderlijk dat het syslog-pad UDP 5140-records naar de geconfigureerde listener verzendt.

Gebruik de pakketopnamemethoden in de corresponderende secties en correleer pakkettijdstempels met gebeurtenissen die zijn ontvangen op de geconfigureerde collector.

Waarnemingsdiensten verifiëren

Bevestig dat statistieken, waarschuwingsroutering, CIMC-waarschuwingen en momentopnamen met bulkstatistieken werken zoals ontworpen voor de geïnstalleerde release. Als OpenTelemetry is ingeschakeld, controleert u de status van de ontvanger, pijpleiding en exporteur met behulp van de ondersteunde procedure voor de werking van SMI Cluster Manager.

verwacht gedrag

Component of pad	Verwacht resultaat
SMI-clusterbeheer	Clustersynchronisatie is voltooid en de vereiste CEE-services zijn geïmplementeerd.
OPS-centrum	Geautoriseerde gebruikers hebben toegang tot operationele functies en ondersteunde configuratie-/bewakingsopdrachten.
Splunk HEC	Het gebeurtenisverkeer bereikt de geconfigureerde HEC-listener op TCP-poort 8088.
Syslog	RFC 5424-geformatteerde gebeurtenissen bereiken de geconfigureerde UDP-poort 5140 listener.
Waarschuwingen en CIMC	Waarschuwingsmanager en gerelateerde exporteurs stellen de geconfigureerde waarschuwingsinformatie bloot.
Bulkstatistieken	Periodieke CSV-momentopnamen worden gegenereerd uit verzamelde statistieken.
open telemetrie	In ondersteunde releases waarbij de gateway is geconfigureerd, stromen OTLP-signalen door de geselecteerde backend/exporter-pijplijn.

beslissingsstroom

waarneming	Volgende controle
CEE-services ontbreken na synchronisatie.	Inspecteer de synchronisatiestatus van Cluster Manager, logboeken, softwareareartefacten en Ops Center-parameters.
HEC-gebeurtenissen ontbreken.	Identificeer de doorstuurpod/node, verifieer TCP 8088-verkeer, HEC-bestemming, verificatie en TLS-configuratie.
Syslog-gebeurtenissen ontbreken.	Controleer de bestemming van de UDP 5140, de RFC 5424-opmaak, de pakketstroom en het gedrag van de ontvanger.
Er ontbreken waarschuwingen of CIMC-gegevens.	Controleer Prometheus/AlertManager-routering, waarschuwingsrouter en cimc-waarschuwingen-exporterbewerking.
Bulkstatistieken ontbreken.	Bevestig de werking van de bulkstatusservice, de beschikbaarheid van Prometheus-gegevens en het genereren van CSV-momentopnamen.
De export van OpenTelemetry ontbreekt.	Verifieer de ondersteuning voor de geïnstalleerde versie, de gatewayconfiguratie, de status van de ontvanger en de exporteur en het lidmaatschap van de pijpleiding.

Conclusie

CEE is een gelaagde Kubernetes-gebaseerde uitvoerings- en observatieomgeving rond SMF-toepassingen. Kubernetes-naamruimtescheiding verdeelt platformactiviteiten, CEE-services en toepassingswerklasten in verschillende domeinen. Binnen CEE zijn monitoring, alarmering, logging en bulkstatistieken gespecialiseerde diensten met onafhankelijke verantwoordelijkheden.

Het belangrijkste Splunk-onderscheid is tussen HEC over TCP 8088 en syslog over UDP 5140. Dit zijn afzonderlijke doorstuurpaden met verschillende protocollen, configuraties en procedures voor het oplossen van problemen. De nieuwere OpenTelemetry-systeemgateway voegt een op OTLP gebaseerd collector- en exportmodel toe. De gelijkenis met OpenShift is architectonisch en de gateway-werking moet worden geverifieerd voor de specifieke CEE-release en -implementatie.

Gerelateerde inhoud

- Cisco CEE Configuratie- en beheergids - Gemeenschappelijke uitvoeringsomgeving
- Cisco CEE Configuratie- en beheergids - Logboekopdrachten
- Cisco SMI Cluster Manager Operations - Synchronisatie en OpenTelemetry
- RFC 5424 — The Syslog Protocol

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.