Cisco CEE 관찰 가능성 및 Splunk 통합 이해

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

아키텍처 개요

CEE 네임스페이스 워크로드

CEE 설치 및 라이프사이클 관리

- 설치 모드
- CEE 소프트웨어 객체 정의
- 클러스터 및 운영 센터 구성
- 배포 동기화 및 확인

CEE 운영 센터 및 운영 관리

CEE Observability 아키텍처

Splunk 통합: 로그 전송 아키텍처

Splunk HTTP 이벤트 컬렉터 포워딩

- HEC 컨피그레이션 모델
- HEC 트래픽 캡처 및 문제 해결

UDP 5140을 통한 Syslog 전달

- RFC 5424 필드 매핑
- UDP 전송 및 패킷 캡처

경고, SNMP 및 CIMC 관찰 가능성

대량 통계

OpenTelemetry 시스템 게이트웨이

- 시스템 게이트웨이 모델
- 게이트웨이 컨피그레이션 개념
- 원격 엑스포터
- OpenShift OpenTelemetry와 비교

구성 확인

- CEE 동기화 확인
- HEC 및 Syslog를 개별적으로 확인
- Observability 서비스 확인

예상 동작

결정 흐름

결론

관련 콘텐츠

소개

이 문서에서는 Cisco CEE(Common Execution Environment) 아키텍처, 구축, 모니터링, Splunk 통합 및 OpenTelemetry에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 기술에 친숙할 것을 권장합니다.

- CNDP(Cloud Native Deployment Platform), Kubernetes 네임스페이스 및 포드 배치.
- Cisco SMI(Subscriber Microservices Infrastructure) 및 SMI Cluster Manager입니다.
- CEE Ops Center, Prometheus, Grafana, Alertmanager 및 로그 포워딩 구성 요소.
- Splunk HTTP Event Collector(HEC), syslog, tcpdump를 통한 패킷 캡처
- 최신 게이트웨이 통합을 위한 OTLP(OpenTelemetry Protocol) 및 OpenTelemetry Collector.

사용되는 구성 요소

예에는 CEE 및 관련 SMF(Session Management Function) 애플리케이션이 포함된 Kubernetes 기반 Cisco SMI/CNDP 환경이 나와 있습니다. 소프트웨어 정의 예는 CEE 패키지 2026.01.1.08을 나타냅니다. ops Center 예에서는 SMF 리포지토리 식별자 smf-2026.04.m0.i50을 사용합니다. 이는 배치 요구 사항이 아닌 예제 값입니다.

네트워크 엔드포인트, 클러스터 이름 및 네임스페이스 값은 대상 배포에 대해 승인된 값으로 대체해야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco CEE(Common Execution Environment)는 Cisco SMI(Subscriber Microservices Infrastructure)에 포함되어 있습니다. Kubernetes 기반 CNDP 구축에서 Kubernetes 네임스페이스는 플랫폼 서비스, CEE 관찰 가능성 및 Kubernetes 관리 서비스, SMF 애플리케이션 워크로드를 분리합니다. 이 분리를 통해 관리 및 운영 경계를 제공하는 한편, Kubernetes 네트워킹 및 서비스 검색

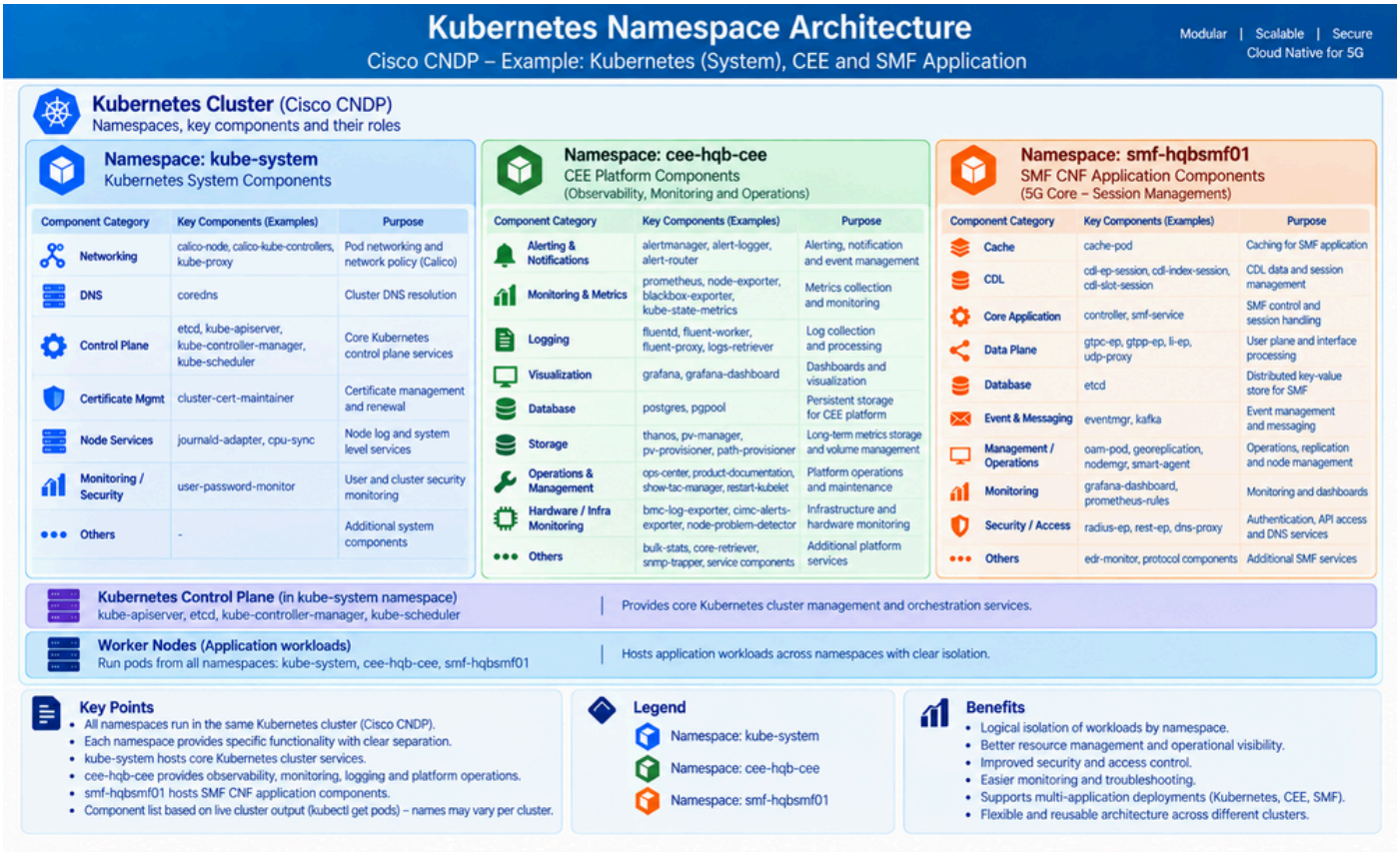
을 통해 허용된 구성 요소 통신을 허용합니다.

이 문서에서는 네임스페이스 아키텍처, CEE 워크로드, CEE 설치 및 라이프사이클 관리, CEE Ops Center, 경고 및 SNMP(Simple Network Management Protocol), Cisco CIMC(Integrated Management Controller) 경고, 로그 전달, 대량 통계, OpenTelemetry 시스템 게이트웨이에 대해 설명합니다.

TCP(Transmission Control Protocol) 포트 8088 및 syslog over UDP(User Datagram Protocol) 포트 5140은 독립적인 수집 메커니즘입니다. 두 경로는 구성, 전송 및 문제 해결 요구 사항이 서로 다르며 공존할 수 있습니다.

아키텍처 개요

CEE 및 관련 애플리케이션 함수는 별도의 Kubernetes 네임스페이스를 사용합니다. 이 아키텍처는 Kubernetes 플랫폼 서비스를 CEE 관찰 및 관리 기능과 SMF 애플리케이션 도메인과 구별합니다.



CEE와 애플리케이션 플랫폼 분리를 보여주는 Cisco SMI 네임스페이스 아키텍처

CEE 네임스페이스는 서비스 수준 아키텍처의 주요 주안점입니다. 다른 네임스페이스는 Kubernetes 플랫폼, 네트워킹 기능 및 SMF 워크로드를 제공합니다.

CEE 네임스페이스 워크로드

CEE 네임스페이스는 모니터링, 경고, 로깅, 대시보드, 통계 및 운영 액세스를 위한 마이크로서비스를 호스팅합니다.

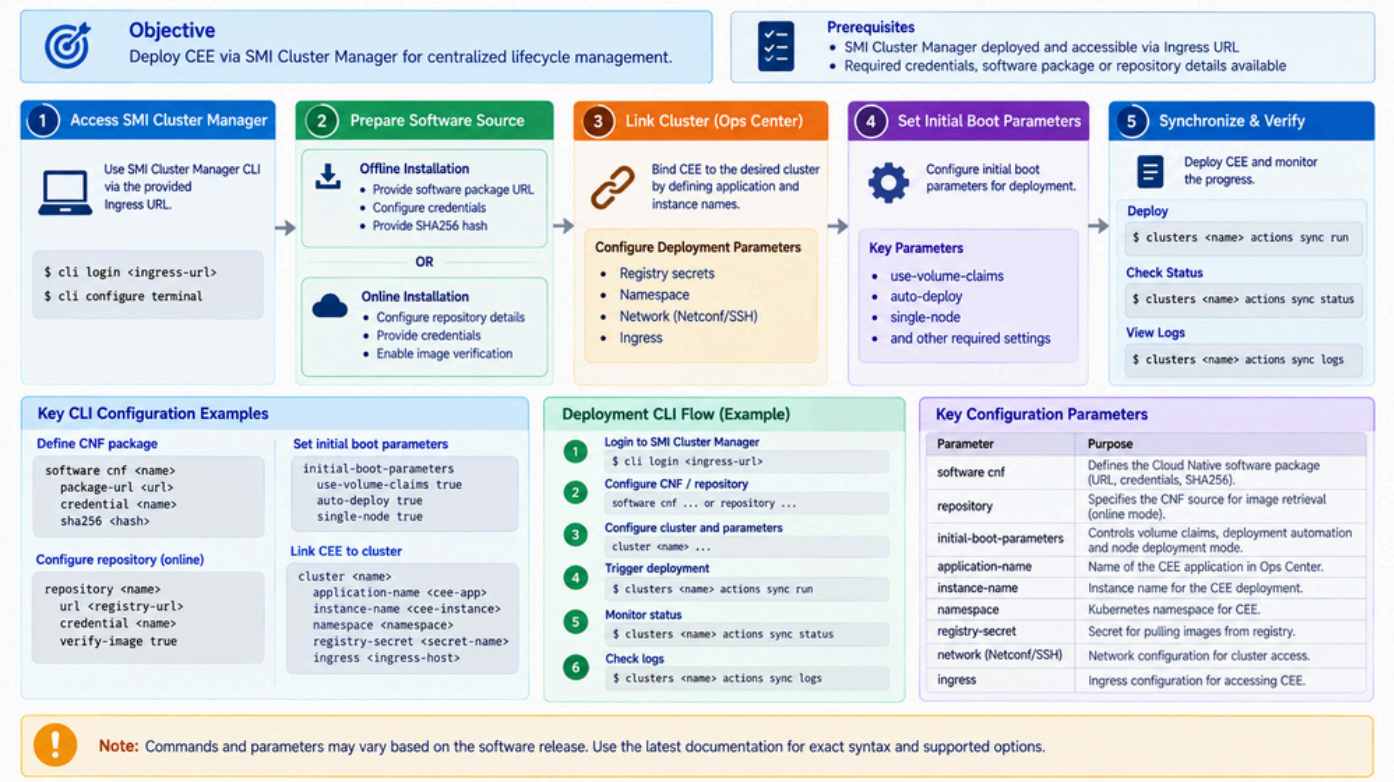


CEE 네임스페이스 마이크로서비스 및 운영 워크로드의 기능

이러한 기능에는 Prometheus 메트릭 수집, Grafana 시각화, Alertmanager 알림 처리, 로그 전달 서비스, 정기적인 대량 통계 생성 등이 포함됩니다. 개별 워크로드는 릴리스 및 구축 컨피그레이션에 따라 달라집니다.

CEE 설치 및 라이프사이클 관리

SMI 클러스터 관리자는 소프트웨어 아티팩트 정의를 대상 클러스터 및 해당 Ops Center 컨피그레이션에서 분리합니다. 이를 통해 소프트웨어 버전 관리 및 반복 가능한 클러스터 동기화를 제어할 수 있습니다.



SMI Cluster Manager CEE 설치 및 소프트웨어 동기화 아키텍처

설치 모드

- 오프라인 설치는 파일 URL 및 Secure Hash Algorithm 256비트(SHA-256) 해시를 통해 로컬 소프트웨어 패키지를 참조할 수 있습니다.
- 클러스터 컨피그레이션은 CEE/SMF 구축을 원하는 클러스터 및 Ops Center 인스턴스와 연결합니다.

CEE 소프트웨어 객체 정의

SMI Cluster Manager 컨피그레이션에서 로컬 CEE 소프트웨어 패키지와 해당 SHA-256 해시를 식별합니다.

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

승인된 패키지의 정확한 SHA-256 값을 사용합니다. 명령의 자리 표시자는 의도적인 것이며 실제 체크섬을 나타내지 않습니다.

클러스터 및 운영 센터 구성

소스 컨피그레이션은 클러스터를 SMF 운영 센터, 로컬 저장소, 관리 엔드포인트 및 구축 설정과 연결합니다. 사이트별 식별자는 자리 표시자로 대체됩니다.

```
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
```

매개변수	예제 구성의 의미
ops-centers smf <smf-ops-center-name>	클러스터를 SMF Ops Center 인스턴스와 연결합니다.
저장소-로컬	구축에 사용할 애플리케이션 리포지토리 및 버전을 지정합니다.
sync-default-repository true	동기화 중에 구성된 기본 리포지토리를 사용합니다.
netconf 포트 2029	NETCONF 관리 연결 포트를 지정합니다.
ssh 포트 2028	SSH(Secure Shell) 관리 연결 포트를 지정합니다.
실제 볼륨 클레임 사용	지속적인 스토리지 요구 사항에 대해 볼륨 클레임을 사용할 수 있습니다.
자동 배포 false	동기화 및 검증이 명시적 제어 하에 유지되도록 자동 구축을 비활성화합니다.
단일 노드 false	단일 노드 모드가 아닌 구축을 지정합니다.

참고: 패키지 및 저장소 식별자는 소스 컨피그레이션의 예입니다. 다른 클러스터에서 사용하기 전에 릴리스 호환성 및 엔드포인트 값을 확인하십시오.

배포 동기화 및 확인

소프트웨어 및 Ops Center 컨피그레이션이 준비된 후 클러스터 동기화 작업을 실행합니다.

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

동기화 상태 및 로그를 검사합니다.

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

동기화가 성공적으로 완료되고 예상 CEE Pod 및 서비스가 구축되었는지 확인합니다.

⚠ 주의: 클러스터 동기화 및 소프트웨어 구축은 실행 환경을 변경할 수 있습니다. 승인된 유지 보수 및 구축 절차에 따라 변경 사항을 적용합니다.

CEE 운영 센터 및 운영 관리

CEE Ops Center는 CEE 서비스를 위한 운영 인터페이스를 제공합니다. 이 워크로드는 클러스터 내의 CEE 기능에 대한 사용자 관리, 인증, 컨피그레이션 및 show 명령을 지원합니다. SMI Cluster Manager는 관리 컨피그레이션을 통해 Ops Center를 대상 구축과 연결합니다.

운영 센터는 관리 플레인에 속합니다. Prometeus, Alertmanager, Fluent Bit/fluent-proxy, HEC, syslog 및 OpenTelemetry는 모니터링 및 텔레메트리 경로에 속합니다. 이러한 업무를 분리하면 트러블슈팅이 간소화됩니다.

CEE Observability 아키텍처

CEE 관찰 기능에는 메트릭, 알림, 로그, CIMC 알림, 대량 통계가 포함됩니다. 이러한 서비스는 서로 관련이 있지만 데이터 경로와 소비자가 다릅니다.

기능	주요 목적	일반 대상 또는 소비자
메트릭	노드, Kubernetes 및 서비스에서 시계열 측정을 수집하고 쿼리합니다.	프로메테우스, 그라파나, 타노스
경고	알림 규칙을 평가하고 알림 이벤트를 라우팅합니다.	알림 관리자, 알림 라우터, 운영 센터 및 외부 수신기.
로그	로그 및 이벤트 레코드를 외부 컬렉터 또는 백엔드에 전달합니다.	Splunk 및 기타 로그 컬렉터
CIMC 알림	모니터링을 위해 Cisco Integrated Management Controller 알림을 내보냅니다.	CEE 메트릭/경고 및 Grafana입니다.
대량 통계	정기적인 통계 스냅샷을 생성합니다.	CSV 스냅샷 및 다운스트림 처리 또는 분석

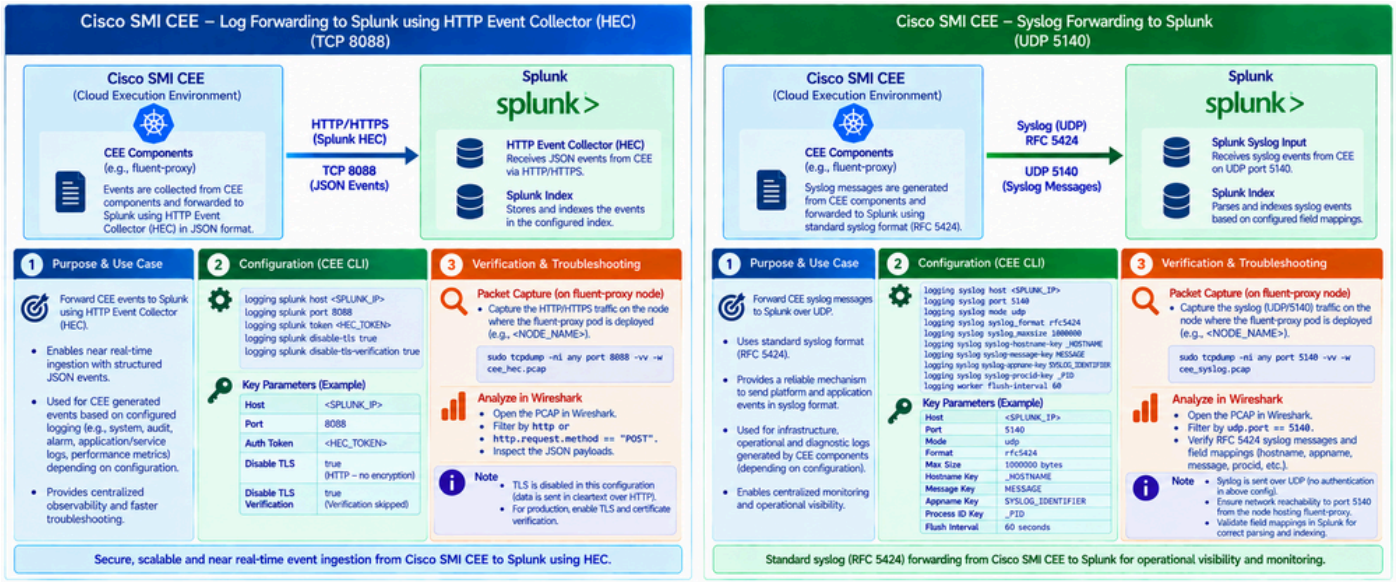
Splunk 통합: 로그 전송 아키텍처

소스에서는 두 개의 CEE-to-Splunk 경로에 대해 설명합니다. 둘 다 Splunk에 이벤트를 전달할 수 있지만 서로 다른 프로토콜과 수집 인터페이스를 사용합니다.

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

각 경로에서 전달하는 이벤트 유형은 CEE 컨피그레이션 및 구현된 전달 파이프라인에 따라 다릅니다. 구성된 2개의 인터페이스에서는 각각이 상호 배타적인 이벤트 카테고리를 전달하는 것을 설정하지 않습니다.

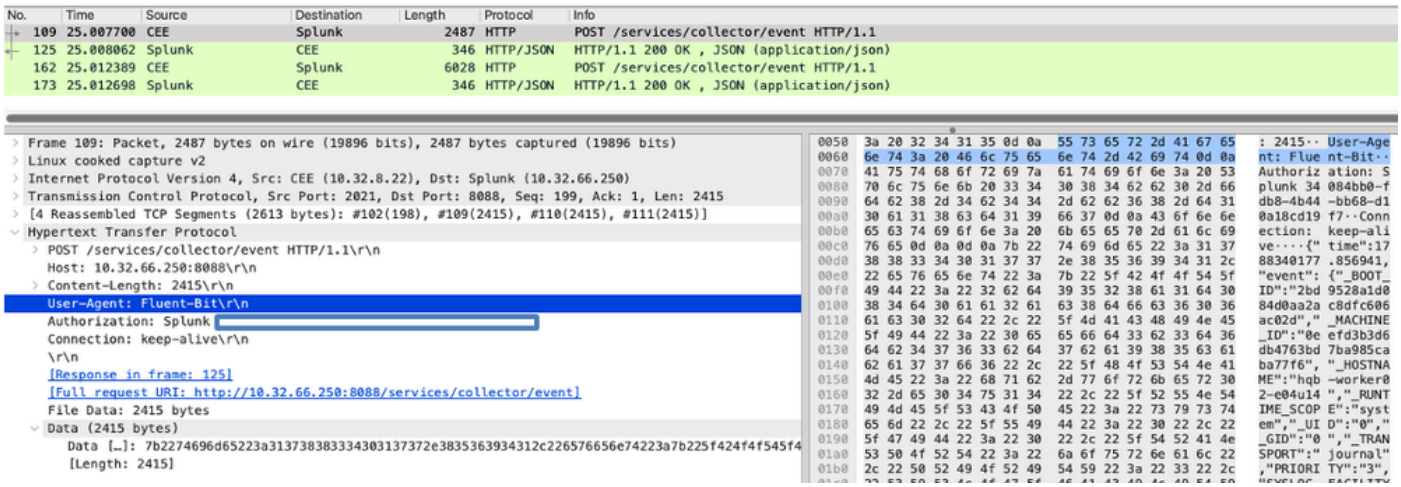
경로를 개별적으로 추적합니다. HEC 전달에 성공하면 syslog 전달이 확인되지 않고, syslog 전달에 성공하면 HEC 전달이 확인되지 않습니다.



CEE Splunk와 별도의 HEC 및 syslog 포워딩 경로 통합

Splunk HTTP 이벤트 컬렉터 포워딩

Splunk HEC는 HTTP 이벤트 제출을 수락하고 HEC 인증 토큰을 사용합니다. CEE는 이 경로에 대해 파일 기반 수집을 요구하지 않고 구성된 HEC 서비스에 직접 이벤트를 전달합니다.



CEE에서 TCP 포트 8088의 Splunk HTTP Event Collector 포워딩 아키텍처에 연결

HEC 컨피그레이션 모델

원래 실습 예에는 CEE Splunk 엔드포인트에 대한 이러한 설정이 포함되어 있습니다. 발췌문은 소스 동작을 기록하며 권장되는 프로덕션 컨피그레이션이 아닙니다.

⚠ 주의: 소스 예에서는 TLS 및 인증서 확인을 모두 비활성화합니다. 이는 텔레메트리 및 HEC 자격 증명을 네트워크 가로채기에 노출합니다. 프로덕션의 경우 TLS 및 인증서 확인을 활성화하고 지원되는 CEE 릴리스 컨피그레이션에 따라 HEC 인증 토큰을 보호합니다.

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

소스 아키텍처에서 CEE 로그/이벤트 생성자는 관련 Fluent 전달 구성 요소를 통해 HEC 목적지로 전달합니다.

```
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 트래픽 캡처 및 문제 해결

Fluent-proxy가 HEC 트래픽을 전달할 때 CEE 네임스페이스에서 Fluent-proxy Pod 및 해당 Kubernetes 작업자 노드를 식별합니다.

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

HEC 트래픽을 전달하는 Kubernetes 노드에서 HEC 포트의 패킷을 캡처합니다.

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

TLS 지원 연결의 경우 패킷 캡처는 전송 설정 및 목적지 세부사항을 표시하지만 일반적으로 HTTP 페이로드를 노출하지는 않습니다. TLS를 비활성화하면 이벤트 내용과 인증 자료가 캡처에 표시될 수 있습니다.

⚠ 주의: 패킷 캡처 및 로그에는 중요한 텔레메트리 및 자격 증명이 포함될 수 있습니다. 수집 및 전송을 권한 있는 지원 워크플로로 제한하고 캡처 파일을 보호합니다.

UDP 5140을 통한 Syslog 전달

두 번째 Splunk 통합 경로는 RFC 5424 형식 지정 및 UDP 포트 5140을 사용하여 syslog 레코드를 전달합니다. 소스 컨피그레이션에서는 필드 매핑, 최대 메시지 크기 및 작업자 플러시 간격도 정의합니다.

```
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 필드 매핑

CEE 소스 필드	Syslog 필드 또는 용도
호스트 이름(_O)	생성된 syslog 레코드에서 시작 호스트를 식별합니다.
메시지	로그 메시지 본문을 전달합니다.
SYSLOG_식별자	syslog 애플리케이션 또는 프로그램 식별자를 제공합니다.
PID(_P)	시작 프로세스 식별자를 전달합니다.

UDP 전송 및 패킷 캡처

UDP는 연결이 없으며 전송 전달 확인 응답이나 재전송을 제공하지 않습니다. 트러블슈팅에서는 패킷 손실, 라우팅, MTU(Maximum Transmission Unit), 프래그먼트화, 수신기 가용성, 큐/속도 동작을 고려해야 합니다.

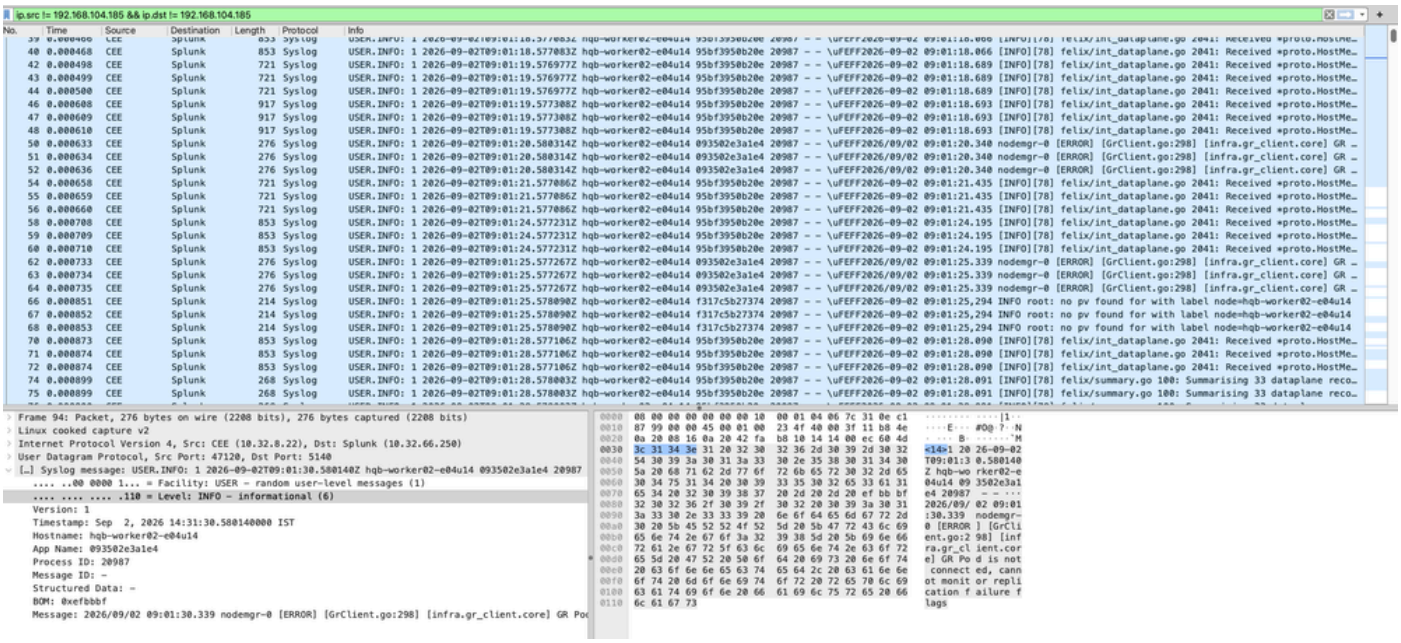
syslog 트래픽을 전달하는 인터페이스 또는 Kubernetes 노드에서 다음을 실행합니다.

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

fluent-proxy가 syslog 트래픽을 전달하는 경우 해당 구성 요소를 호스팅하는 노드가 적절한 패킷 캡처 포인트입니다. 패킷을 수집하기 전에 전달 경로를 확인합니다.



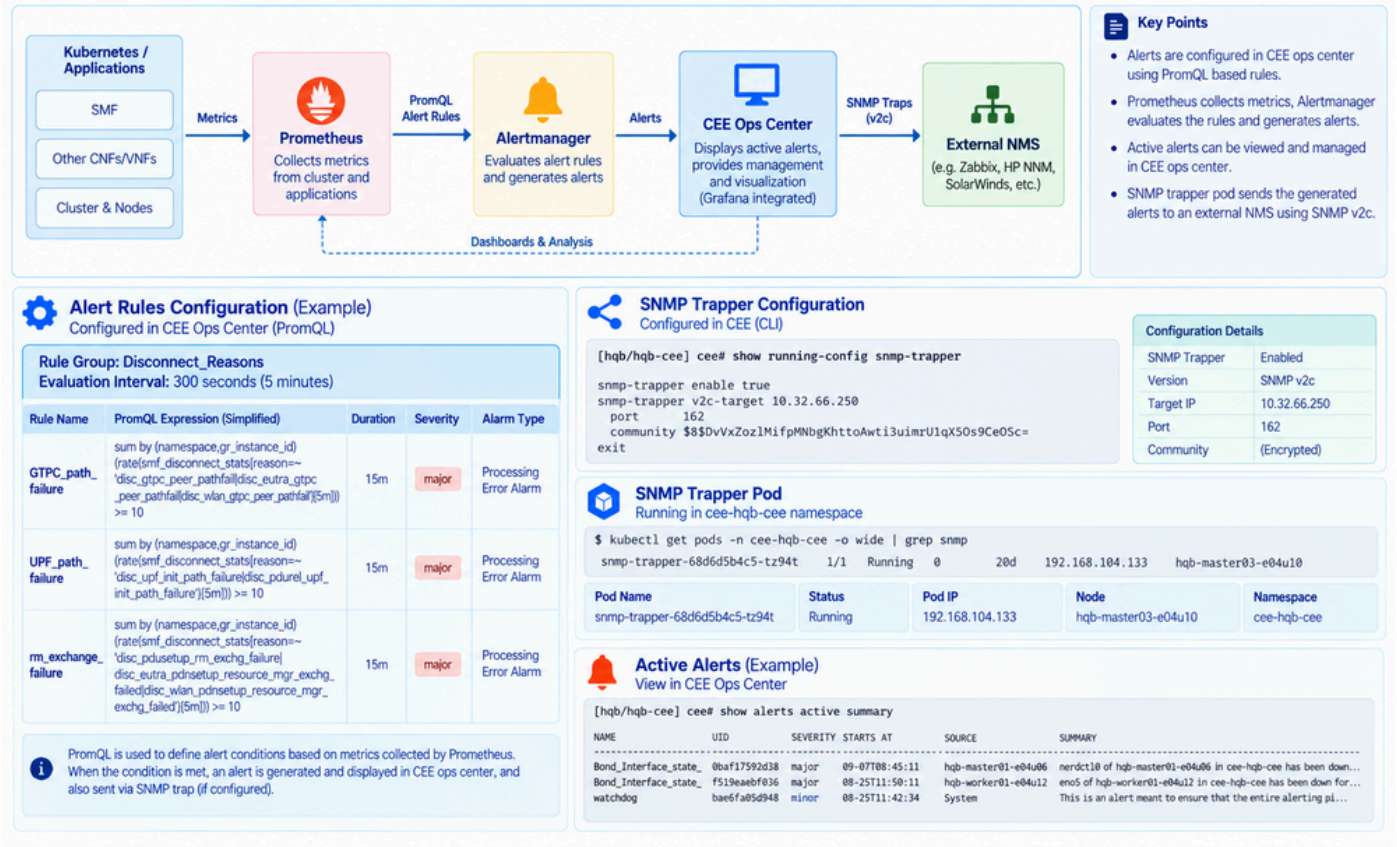
참고: RFC 5424는 선택한 전송과 독립적으로 syslog 메시지 형식을 정의합니다. 소스 시나리오에서는 UDP 5140을 사용합니다. TLS 기반 syslog 전송은 호환되는 발신자 및 수신자 컨피그레이션이 필요한 다른 옵션입니다.



UDP 포트 5140 및 RFC 5424 필드를 사용하여 CEE syslog를 Splunk로 전달

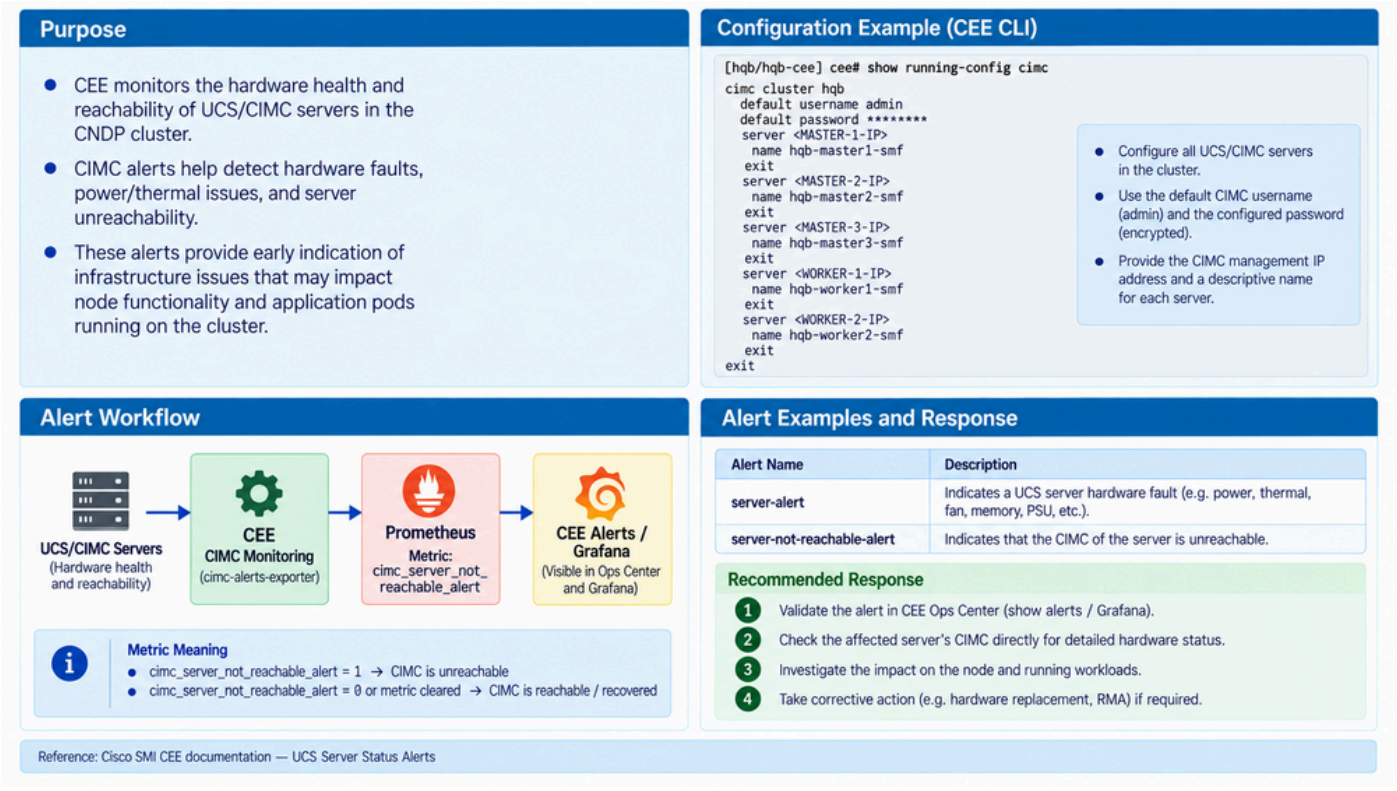
경고, SNMP 및 CIMC 관찰 가능성

CEE 알림은 Prometheus 및 Alertmanager를 사용합니다. Prometheus는 메트릭 및 경고 규칙을 평가합니다. Alertmanager는 수신자에게 알림 이벤트를 라우팅하며, 알림 라우터는 추가 라우팅 지원을 제공합니다. CEE alert-logger는 CEE Ops Center를 통해 검색할 수 있도록 기록 경고 레코드를 제공합니다.



CEE Prometheus 및 Alertmanager 알림 전달 및 SNMP 아키텍처

CIMC 경고 통합은 관련 인프라 모니터링 경로를 제공합니다. cimc-alerts-exporter는 CIMC 알림 정보를 수집하여 Grafana에서 모니터링 및 시각화를 위해 표시합니다.



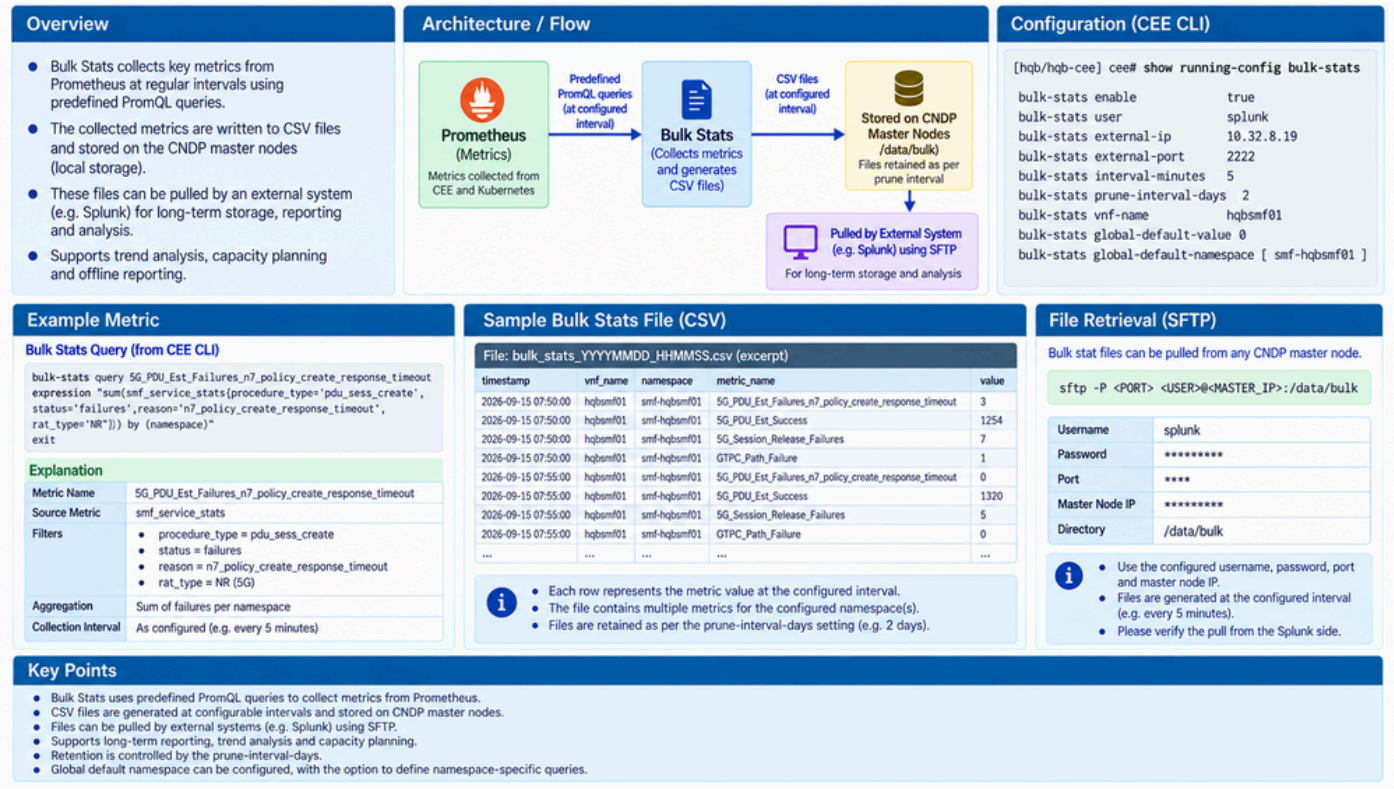
CEE CIMC 경고 내보내기 모니터링 대시보드와 통합

SNMP 통합은 경고 및 관리 인터페이스입니다. Splunk HEC 또는 syslog 전달과 호환되지 않습니다. 프로토콜 및 이벤트 전달 경로는 서로 다릅니다.

관련 MIB(Management Information Base) 참조에는 CISCO-CNEE-MIB.my 및 CISCO-SMI.my가 포함됩니다.

대량 통계

CEE 대량 통계 서비스는 Prometeus를 통해 수집된 통계의 주기적인 CSV(Comma-Separated Values) 스냅샷을 생성합니다. 이러한 스냅샷은 애플리케이션 로그 레코드 스트림이 아니라 통계 스냅샷입니다.



CEE 대량 통계 서비스 프로메테우스 메트릭스에서 정기적인 CSV 스냅샷 생성

대량 통계 출력은 정기적인 보고, 추세 분석 및 다운스트림 데이터 처리를 지원합니다. 구축에서 명시적으로 CSV/통계 데이터를 Splunk로 전달하거나 가져오는 경우에만 Splunk 통합 경로에 포함합니다.

OpenTelemetry 시스템 게이트웨이

최신 Cisco SMI 릴리스는 플랫폼 관리 OpenTelemetry Collector 게이트웨이를 지원합니다. 게이트웨이는 OTLP(OpenTelemetry Protocol)를 통해 애플리케이션에서 텔레메트리를 수신하고 지원되

는 메트릭 및 로그를 로컬 또는 원격 백엔드에 전달합니다.



참고: Cisco SMI Cluster Manager Operations 설명서는 OpenTelemetry 게이트웨이와 릴리스 2026.03.1과의 통합을 식별합니다. 게이트웨이는 원본 예제에 설명된 특정 배포에서 검증되지 않았으므로 이 섹션에서는 해당 환경에서 검증된 작업이 아니라 게시된 구성 모델에 대해 설명합니다.

시스템 게이트웨이 모델

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

게이트웨이 컨피그레이션 개념

OpenTelemetry Collector 게이트웨이를 활성화하고 로컬 메트릭 및 로깅 백엔드를 선택합니다.

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

구축에 외부 서비스 노출이 필요한 경우 컨피그레이션에 외부 IP가 포함될 수 있습니다.

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

선택적 프록시 설정은 게이트웨이 내보내기에 대해 구성됩니다.

```
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
```

로컬 백엔드 옵션은 플랫폼 관리 시스템 게이트웨이가 텔레메트리를 내장형 백엔드에 전송하는 방식을 제어합니다. 외부 IP 노출 및 프록시 설정은 토폴로지 및 보안 요구 사항에 따라 다릅니다.

원격 엑스포터

엑스포터	신호	기술적 사용
도구	로그, 메트릭	gRPC를 통해 OTLP를 수락하는 백엔드에 텔레메트리를 보냅니다.
otlphttp	로그, 메트릭	HTTP를 통해 OTLP를 허용하는 백엔드에 텔레메트리를 보냅니다.
스컹크	로그	로그를 Splunk HEC 엔드포인트로 보냅니다.
신문 잡지	로그	지원되는 노드 저널에 로그를 기록합니다.
디버그	로그, 메트릭	제어된 검증 및 문제 해결 지원.

OpenTelemetry 파이프라인은 수신, 처리 및 내보내기 모델을 따릅니다. 수신자는 원격 분석을 수집합니다. 프로세서 필터 또는 변환 데이터; 내보내기는 선택한 신호를 원격 또는 로컬 백엔드에 전달합니다.

소스는 프록시 동작도 구분합니다. otlp는 컬렉터 인스턴스 프록시 설정을 사용하지만, otlphttp 및 splunkhec는 구축된 릴리스가 해당 컨피그레이션을 표시하는 내보내기 레벨 프록시 재정의를 지원합니다.

OpenShift OpenTelemetry와 비교

Cisco CEE 및 OpenShift는 다음과 같은 공유 아키텍처 패턴을 가지고 있습니다. OpenTelemetry Collector는 계측된 애플리케이션과 관찰 가능한 백엔드 사이에 위치할 수 있습니다. 관리 및 설치 모델은 서로 다릅니다.

개념	CEE OpenTelemetry 시스템 게이트웨이	OpenShift OpenTelemetry 패턴
텔레메트리 소스	OpenTelemetry 지원 CEE 및 애플리케이션 워크로드	OpenTelemetry 지원 OpenShift 워크로드
프로토콜	OTLP	OTLP
컬렉터 역할	플랫폼 관리 시스템 게이트웨이	OpenTelemetry Collector 구축 또는 인스턴스
파이프라인 개념	수신, 처리, 내보내기	수신, 처리, 내보내기
백엔드 유연성	로컬 백엔드 및 지원되는 원격 엑스포터	엑스포터 중심의 백엔드 통합
Splunk 통합	문서화된 CEE 컨피그레이션의 splunkhec exporter	구성된 Splunk HEC 내보내기

이 비교는 아키텍처입니다. 두 플랫폼은 OpenTelemetry를 동일하게 구현한다고 주장되지 않습니

다. OpenShift는 일반적으로 OpenTelemetry Operator/Collector 구축 모델을 사용하는 반면, Cisco SMI 시스템 게이트웨이는 플랫폼 관리형입니다.

소스에서 설명한 OpenShift 참조 아키텍처는 Kubernetes 워크로드에서 텔레메트리를 HEC를 통해 Splunk로 전달하는 컬렉터를 보여줍니다. 샘플 CEE 설치를 위한 검증된 통합이 아닌 컬렉터 기반 모델을 보여줍니다.

구성 확인

CEE 동기화 확인

SMI Cluster Manager 동기화 상태 및 로그를 검토하고 예상 CEE 워크로드가 배포되었는지 확인합니다.

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

HEC 및 Syslog를 개별적으로 확인

HEC 경로가 구성된 TCP 8088 엔드포인트로 이벤트를 전송하고 Splunk에서 이를 수신하는지 확인합니다. syslog 경로가 구성된 리스너에 UDP 5140 레코드를 전송하는지 별도로 확인합니다.

해당 섹션의 패킷 캡처 방법을 사용하고 구성된 컬렉터에서 수신된 이벤트와 패킷 타임스탬프의 상관관계를 분석합니다.

Observability 서비스 확인

메트릭, 경고 라우팅, CIMC 경고 및 대량 통계 스냅샷이 설치된 릴리스에 맞게 작동하는지 확인합니다. OpenTelemetry가 활성화된 경우 지원되는 SMI Cluster Manager 작업 절차를 사용하여 수신기, 파이프라인 및 내보내기 상태를 확인합니다.

예상 동작

구성 요소 또는 경로	예상 결과
SMI 클러스터 관리자	클러스터 동기화가 완료되고 필요한 CEE 서비스가 구축됩니다.

구성 요소 또는 경로	예상 결과
운영 센터	인증된 사용자는 운영 기능 및 지원되는 컨피그레이션/모니터링 명령에 액세스할 수 있습니다.
스플렁크 HEC	이벤트 트래픽은 TCP 포트 8088에서 구성된 HEC 리스너에 도달합니다.
Syslog	RFC 5424 형식의 이벤트는 구성된 UDP 포트 5140 수신기에 도달합니다.
경고 및 CIMC	Alertmanager 및 관련 내보내기는 구성된 경고 정보를 표시합니다.
대량 통계	수집된 통계로부터 정기 CSV 스냅샷이 생성됩니다.
원격 분석 열기	게이트웨이가 구성된 지원되는 릴리스에서 OTLP 신호는 선택된 백엔드/엑스포터 파이프라인을 통해 흐릅니다.

결정 흐름

관찰	다음 확인
동기화 후 CEE 서비스가 없습니다.	클러스터 관리자 동기화 상태, 로그, 소프트웨어 아티팩트 및 운영 센터 매개변수를 검사합니다.
HEC 이벤트가 없습니다.	포워딩 포드/노드를 식별하고 TCP 8088 트래픽, HEC 대상, 인증 및 TLS 컨피그레이션을 확인합니다.
Syslog 이벤트가 없습니다.	UDP 5140 대상, RFC 5424 형식 지정, 패킷 흐름 및 수신기 동작을 확인합니다.
경고 또는 CIMC 데이터가 없습니다.	Prometheus/Alertmanager 라우팅, alert-router 및 cimc-alerts-exporter 작업을 확인합니다.
대량 통계가 누락되었습니다.	대량 통계 서비스 작업, Prometheus 데이터 가용성 및 CSV 스냅샷 생성을 확인합니다.
OpenTelemetry 내보내기가 없습니다.	설치된 릴리스, 게이트웨이 컨피그레이션, 수신기 및 내보내기 상태, 파이프라인 멤버십에 대한 기능 지원을 확인합니다.

결론

CEE는 SMF 애플리케이션 중심의 계층화된 Kubernetes 기반 실행 및 관찰 환경 Kubernetes 네임스페이스 분리는 플랫폼 운영, CEE 서비스 및 애플리케이션 워크로드를 서로 다른 도메인으로 나눕니다. CEE 내에서 모니터링, 알림, 로깅 및 대량 통계는 독립적인 책임이 있는 전문 서비스입니다.

Splunk의 주요 차이점은 TCP 8088을 통한 HEC와 UDP 5140을 통한 syslog입니다. 이는 프로토콜, 컨피그레이션, 문제 해결 절차가 서로 다른 별도의 포워딩 경로입니다. 최신 OpenTelemetry 시스템 게이트웨이는 OTLP 기반 컬렉터 및 내보내기 모델을 추가합니다. OpenShift OpenTelemetry와 유사한 기능은 아키텍처이며, 특정 CEE 릴리스 및 구축에 대한 게이트웨이 운영을 확인해야 합니다.

관련 콘텐츠

- Cisco CEE 컨피그레이션 및 관리 가이드 - 공통 실행 환경
- Cisco CEE 컨피그레이션 및 관리 가이드 - 로깅 명령
- Cisco SMI Cluster Manager Operations - 동기화 및 OpenTelemetry
- RFC 5424 - Syslog 프로토콜

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.