Comprendre l'observabilité et l'intégration Splunk de Cisco CEE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Présentation de l'architecture
- Charges de travail des espaces de noms CEE
- Installation CEE et gestion du cycle de vie
  - Modes d'installation
  - Définition de l'artefact logiciel CEE
  - Configuration du cluster et du centre des opérations
  - Synchronisation et vérification du déploiement
- Centre d'opérations CEE et gestion opérationnelle
- Architecture d'observabilité CEE
- Intégration de Splunk : Architecture de transfert de journal
- Transfert du collecteur d'événements HTTP Splunk
  - Modèle de configuration HEC
  - Capturer et dépanner le trafic HEC
- Transfert Syslog sur UDP 5140
  - Mappage de champ RFC 5424
  - Transport UDP et capture de paquets
- Alertes, SNMP et observabilité CIMC
- Statistiques groupées
- Passerelle système OpenTelemetry
  - Modèle de passerelle système
  - Concepts de configuration de passerelle
  - Exportateurs distants
  - Comparer avec OpenShift OpenTelemetry
- Vérification de la configuration
  - Vérification de la synchronisation CEE
  - Vérifier HEC et Syslog séparément
  - Vérifier les services Observability
- Comportement attendu
- Flux de décision
- Conclusion
- Autres informations utiles

Introduction

Ce document décrit l'architecture, le déploiement, la surveillance, l'intégration Splunk et OpenTelemetry de Cisco Common Execution Environment (CEE).

Conditions préalables

Exigences

Cisco recommande de se familiariser avec ces technologies :

- Cloud Native Deployment Platform (CNDP), espaces de noms Kubernetes et emplacement des pod.
- Cisco Subscriber Microservices Infrastructure (SMI) et SMI Cluster Manager.
- CEE Ops Center, Prometheus, Grafana, Alertmanager et composants de transfert de journal.
- Splunk HTTP Event Collector (HEC), syslog et capture de paquets avec tcpdump.
- OpenTelemetry Protocol (OTLP) et OpenTelemetry Collector pour la nouvelle intégration de la passerelle.

Composants utilisés

Les exemples montrent un environnement Cisco SMI/CNDP basé sur Kubernetes avec CEE et une application SMF (Session Management Function) associée. L'exemple de définition logicielle fait référence au package CEE 2026.01.1.08 ; l'exemple d'Ops Center utilise un identificateur de référentiel SMF smf-2026.04.m0.i50. Il s'agit de valeurs d'exemple et non de conditions de déploiement.

Les points de terminaison réseau, les noms de cluster et les valeurs d'espace de noms doivent être remplacés par des valeurs approuvées pour le déploiement cible.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

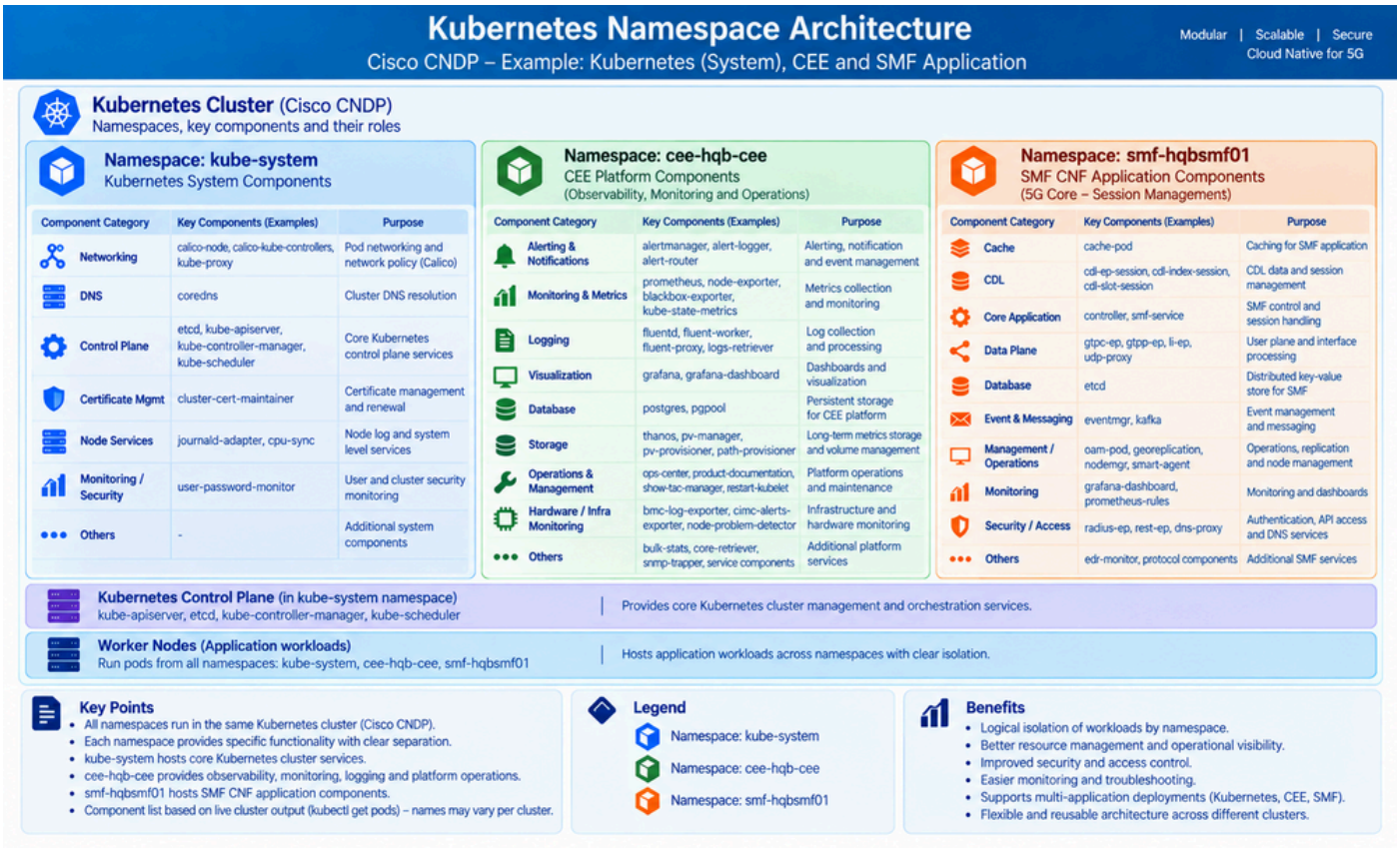
Cisco Common Execution Environment (CEE) fait partie de Cisco Subscriber Microservices Infrastructure (SMI). Dans un déploiement CNDP basé sur Kubernetes, les espaces de noms Kubernetes séparent les services de plate-forme, les services d'observabilité CEE et de gestion Kubernetes, et les charges de travail d'application SMF. La séparation fournit des limites administratives et opérationnelles tandis que la mise en réseau et la découverte de services Kubernetes permettent la communication de composants autorisés.

Ce document couvre l'architecture d'espace de noms, les charges de travail CEE, l'installation CEE et la gestion du cycle de vie, le centre d'opérations CEE, les alertes et le protocole SNMP (Simple Network Management Protocol), les alertes Cisco Integrated Management Controller (CIMC), le transfert de journaux, les statistiques en bloc et la passerelle système OpenTelemetry.

Splunk HEC sur le port TCP (Transmission Control Protocol) 8088 et syslog sur le port UDP (User Datagram Protocol) 5140 sont des mécanismes d'ingestion indépendants. Les deux chemins ont des exigences de configuration, de transport et de dépannage différentes et peuvent coexister.

Présentation de l'architecture

CEE et les fonctions d'application associées occupent des espaces de noms Kubernetes distincts. L'architecture différencie les services de la plate-forme Kubernetes des fonctions d'observation et de gestion CEE et du domaine d'application SMF.



Architecture d'espace de noms Cisco SMI montrant la séparation CEE et plate-forme applicative

L'espace de noms CEE est le principal objet de l'architecture de niveau de service. D'autres espaces de noms fournissent la plate-forme Kubernetes, les fonctions réseau et les charges de travail SMF.

Charges de travail des espaces de noms CEE

L'espace de noms CEE héberge des microservices pour la surveillance, les alertes, la journalisation, les tableaux de bord, les statistiques et l'accès opérationnel.

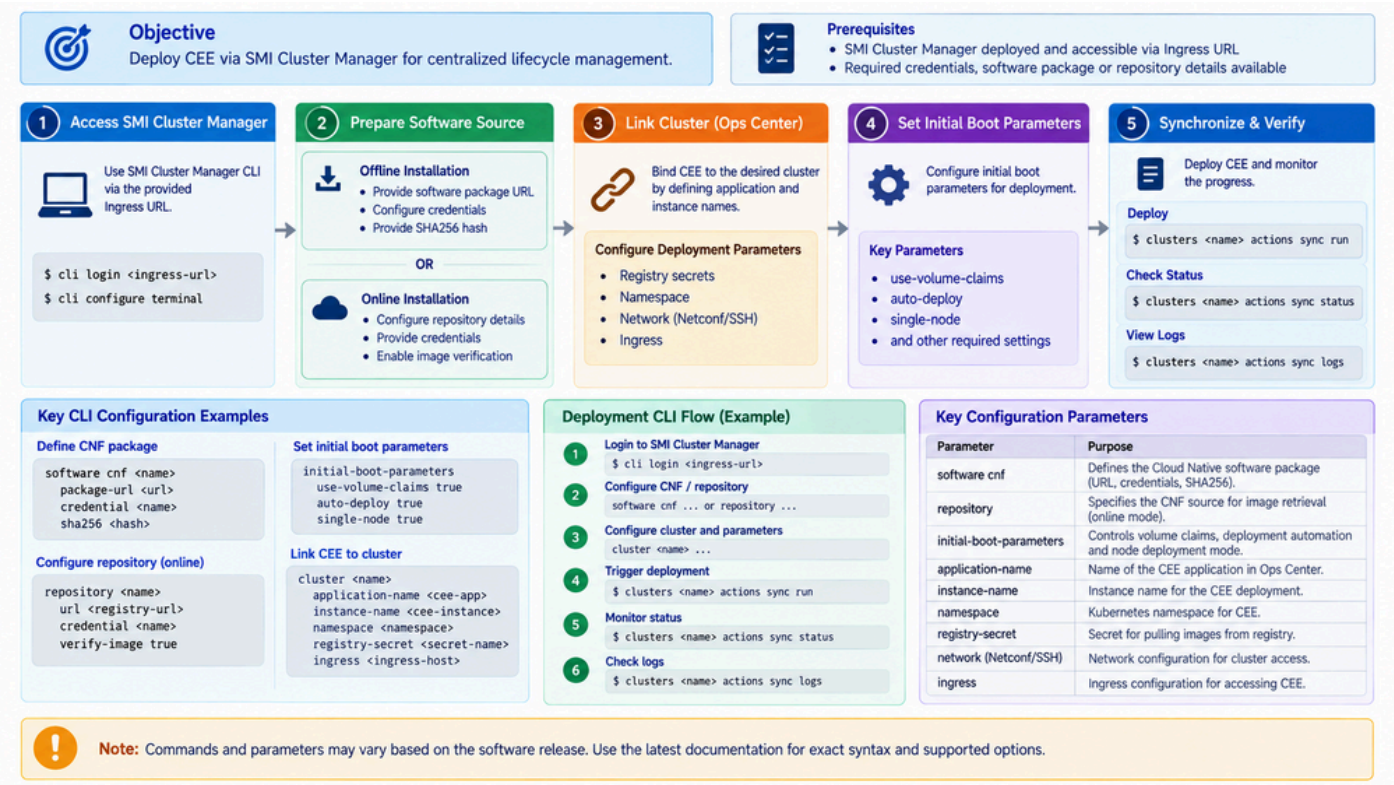


Microservices d'espace de noms CEE et fonctions de ses charges de travail opérationnelles

Ces fonctions incluent la collecte des mesures Prometheus, la visualisation Grafana, la gestion des alertes Alertmanager, les services de transfert de journal et la création périodique de statistiques en masse. Les charges de travail varient selon la version et la configuration du déploiement.

Installation CEE et gestion du cycle de vie

SMI Cluster Manager sépare la définition d'artefact logiciel du cluster cible et de sa configuration Ops Center. Cela permet le contrôle des versions logicielles et la synchronisation répétable des clusters.



Installation de SMI Cluster Manager CEE et architecture de synchronisation logicielle

Modes d'installation

- L'installation hors ligne peut faire référence à un package logiciel local via une URL de fichier et un hachage SHA-256 (Secure Hash Algorithm 256-bit).
- La configuration de cluster associe le déploiement CEE/SMF à la grappe et à l'instance Ops Center prévues.

Définition de l'artefact logiciel CEE

Dans la configuration de SMI Cluster Manager, identifiez le package logiciel CEE local et son hachage SHA-256.

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

Utilisez la valeur SHA-256 exacte du colis approuvé. L'espace réservé dans la commande est intentionnel et ne représente pas une somme de contrôle réelle.

Configuration du cluster et du centre des opérations

La configuration source associe un cluster à un centre d'opérations SMF, un référentiel local, des terminaux de gestion et des paramètres de déploiement. Les identificateurs propres au site sont remplacés par des espaces réservés.

```
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
```

Paramètre	Signification dans l'exemple de configuration
ops-centers smf <smf-ops-center-name>	Associe le cluster à l'instance SMF Ops Center.
référentiel-local	Spécifie le référentiel et la version de l'application à déployer.
sync-default-repository true	Utilise le référentiel par défaut configuré lors de la synchronisation.
netconf-port 2029	Spécifie le port de connectivité de gestion NETCONF.
ssh-port 2028	Spécifie le port de connectivité de gestion SSH (Secure Shell).
use-volume-claims true	Permet l'utilisation de revendications de volume pour les besoins de stockage persistants.
auto-deploy false	Désactive le déploiement automatique afin que la synchronisation et la validation restent sous contrôle explicite.
faux noeud unique	Spécifie un déploiement qui n'est pas en mode noeud unique.



Remarque : Les identificateurs de package et de référentiel sont des exemples de la configuration source. Vérifiez la compatibilité des versions et les valeurs des points de terminaison avant de les utiliser dans un cluster différent.

Synchronisation et vérification du déploiement

Exécutez l'action de synchronisation du cluster une fois que la configuration du logiciel et du centre d'opérations est prête.

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

Inspectez l'état et les journaux de synchronisation.

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

Vérifiez que la synchronisation s'est terminée correctement et que les pods et services CEE attendus sont déployés.



Mise en garde : La synchronisation de cluster et le déploiement de logiciels peuvent modifier l'environnement en cours d'exécution. Appliquer les modifications conformément à la procédure de maintenance et de déploiement approuvée.

Centre d'opérations CEE et gestion opérationnelle

Le Centre d'opérations CEE fournit l'interface opérationnelle pour les services CEE. La charge de travail prend en charge la gestion des utilisateurs, l'authentification, la configuration et les commandes show pour les fonctions CEE au sein du cluster. SMI Cluster Manager associe le centre d'opérations au déploiement cible via la configuration de gestion.

Ops Center appartient au plan de gestion. Prometheus, Alertmanager, Fluent Bit/fluent-proxy, HEC, syslog et OpenTelemetry appartiennent aux chemins de surveillance et de télémétrie. La séparation de ces responsabilités simplifie le dépannage.

Architecture d'observabilité CEE

L'observabilité CEE inclut des mesures, des alertes, des journaux, des alertes CIMC et des statistiques groupées. Ces services sont liés, mais les chemins de données et les consommateurs sont différents.

Fonction	Objectif principal	Destination ou consommateur type
Indicateurs	Collecter et interroger des mesures de séries chronologiques à partir de noeuds, de réseaux Kuber et de services.	Prométhée, Grafana et Thanos.
Alertes	Évaluation des règles d'alerte et routage des événements d'alerte	Alertmanager, alert-router, Ops Center et récepteurs externes.
Journaux	Transférer les enregistrements de journaux et d'événements vers des collecteurs externes ou des serveurs principaux.	Splunk et autres collecteurs de journaux.
Alertes CIMC	Exporter les alertes du contrôleur de gestion intégré Cisco pour la surveillance.	Mesures/alertes CEE et Grafana.
Statistiques groupées	Créez des instantanés statistiques périodiques.	Instantanés CSV et traitement ou analyse en aval.

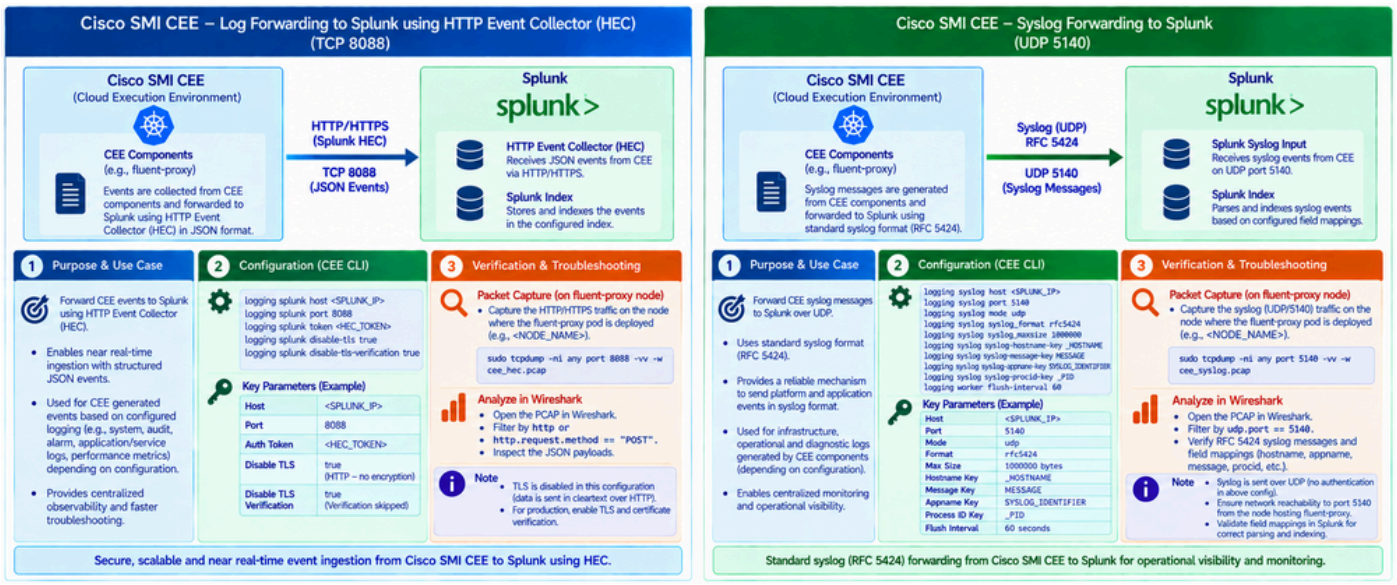
Intégration de Splunk : Architecture de transfert de journal

La source décrit deux chemins CEE vers Splunk. Les deux peuvent transmettre des événements au Splunk, mais ils utilisent des protocoles et des interfaces de réception distincts.

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

Les types d'événements transportés par chaque chemin dépendent de la configuration CEE et du pipeline de transfert mis en oeuvre. Deux interfaces configurées n’établissent pas que chacune porte une catégorie d’événements mutuellement exclusifs.

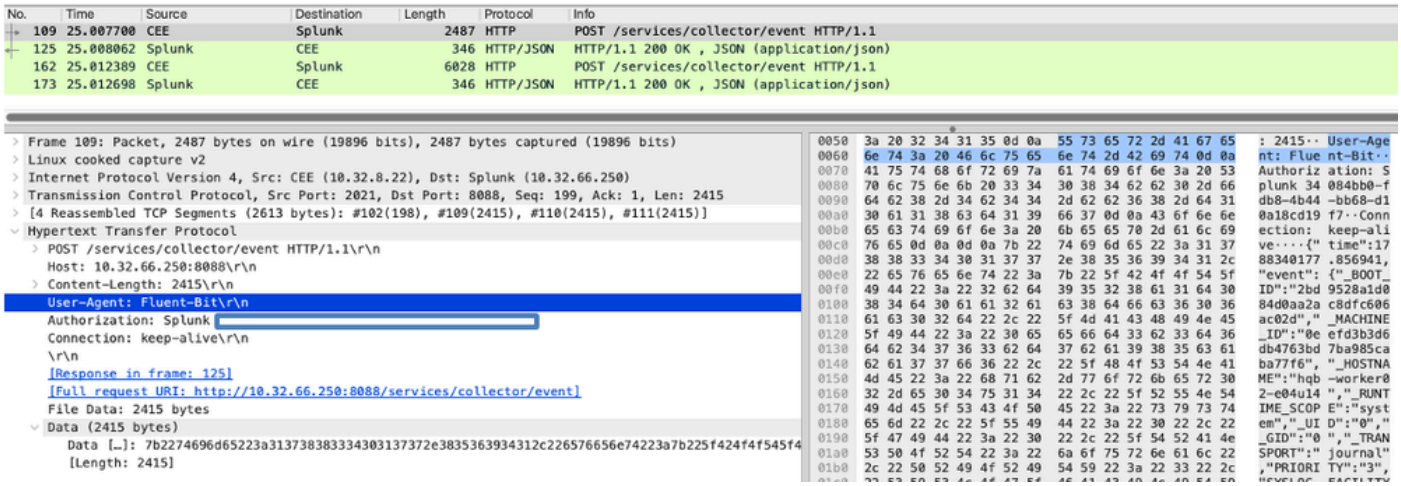
Suivez les chemins séparément. Une livraison HEC réussie ne confirme pas la livraison Syslog, et une livraison Syslog réussie ne confirme pas la livraison HEC.



Intégration Splunk CEE avec chemins de transfert HEC et Syslog séparés

Transfert du collecteur d'événements HTTP Splunk

Splunk HEC accepte les envois d'événements HTTP et utilise un jeton d'authentification HEC. CEE transfère les événements directement au service HEC configuré au lieu d'exiger une réception basée sur des fichiers pour ce chemin.



Architecture de transfert du collecteur d'événements HTTP CEE vers Splunk sur le port TCP 8088

Modèle de configuration HEC

L’exemple de TP d’origine contient ces paramètres pour un point de terminaison CEE Splunk. L'extrait enregistre le comportement de la source et n'est pas une configuration de production recommandée.

⚠ Mise en garde : L'exemple source désactive à la fois TLS et la vérification de certificat. Cela expose la télémétrie et les informations d'identification HEC à une interception sur le réseau. Pour la production, activez TLS et la vérification de certificat et sécurisez le jeton d'authentification HEC conformément à la configuration de version CEE prise en charge.

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

Dans l'architecture source, les producteurs d'événements/journaux CEE transfèrent le composant de transfert Fluent approprié vers la destination 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
```

Capturer et dépanner le trafic HEC

Identifiez le pod fluent-proxy et son noeud de travail Kubernetes dans l'espace de noms CEE lorsque fluent-proxy transporte le trafic HEC.

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

Sur le noeud Kubernetes qui transporte le trafic HEC, capturez les paquets pour le port HEC.

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

Pour une connexion TLS, une capture de paquet révèle les détails de l'établissement du transport et de la destination, mais n'expose normalement pas la charge utile HTTP. Si TLS est désactivé, le contenu des événements et le matériel d'authentification peuvent être visibles dans la capture.

⚠ Mise en garde : Les captures de paquets et les journaux peuvent contenir des informations de télémétrie et d'identification sensibles. Limitez la collecte et le transfert aux workflows de support autorisés et protégez les fichiers de capture.

Transfert Syslog sur UDP 5140

Le deuxième chemin d'intégration Splunk transfère les enregistrements Syslog à l'aide du formatage RFC 5424 et du port UDP 5140. La configuration source définit également les mappages de champs, la taille maximale des messages et l'intervalle de vidage du convertisseur.

```
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
```

Mappage de champ RFC 5424

champ source CEE	Champ ou objectif Syslog
_NOM D'HÔTE	Identifie l'hôte d'origine dans l'enregistrement syslog généré.
MESSAGE	Transporte le corps du message de journalisation.
IDENTIFICATEUR_SYSLOG	Fournit l'identificateur de l'application ou du programme Syslog.
_PID	Transporte l'identificateur du processus d'origine.

Transport UDP et capture de paquets

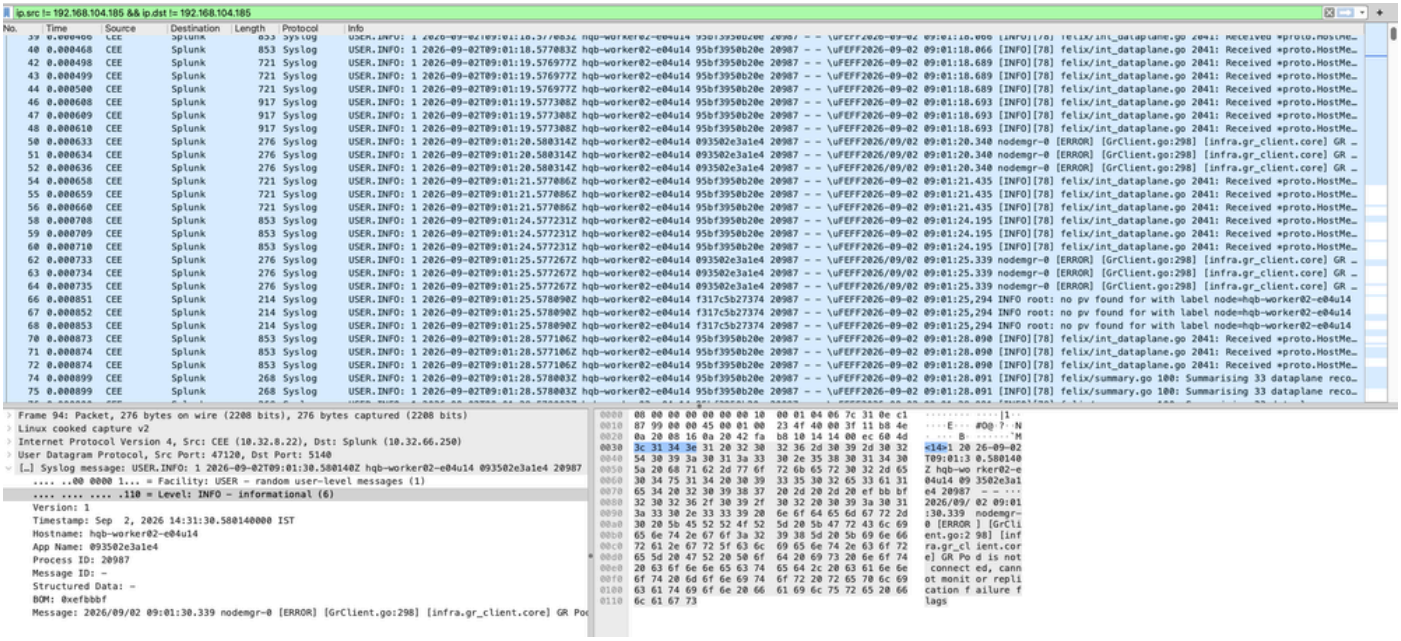
Le protocole UDP est non orienté connexion et ne fournit ni accusé de réception ni retransmission. Le dépannage doit tenir compte de la perte de paquets, du routage, de l'unité de transmission maximale (MTU), de la fragmentation, de la disponibilité du récepteur et du comportement de la file d'attente/du débit.

Sur l'interface ou le noeud Kubernetes qui transporte le trafic syslog, exécutez :

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

Si fluent-proxy transfère le trafic syslog, le noeud hébergeant ce composant est un point de capture de paquets approprié. Vérifiez le chemin de transfert avant de collecter les paquets.

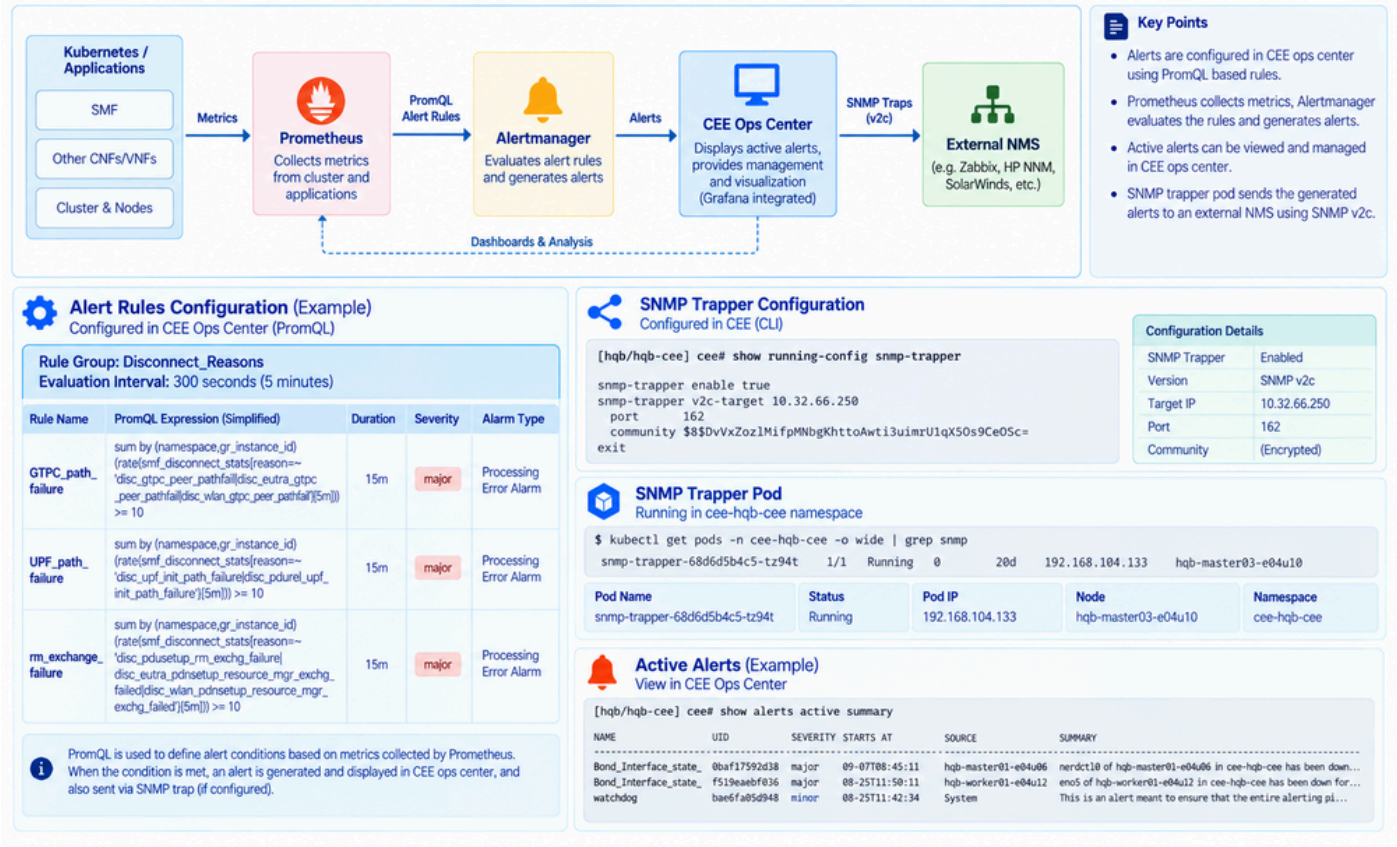
Remarque : Le document RFC 5424 définit un format de message Syslog indépendamment du transport sélectionné. Le scénario source utilise UDP 5140. Le transport syslog basé sur TLS est une option différente qui nécessite une configuration d'expéditeur et de récepteur compatible.



Transfert Syslog CEE vers Splunk à l'aide des champs UDP port 5140 et RFC 5424

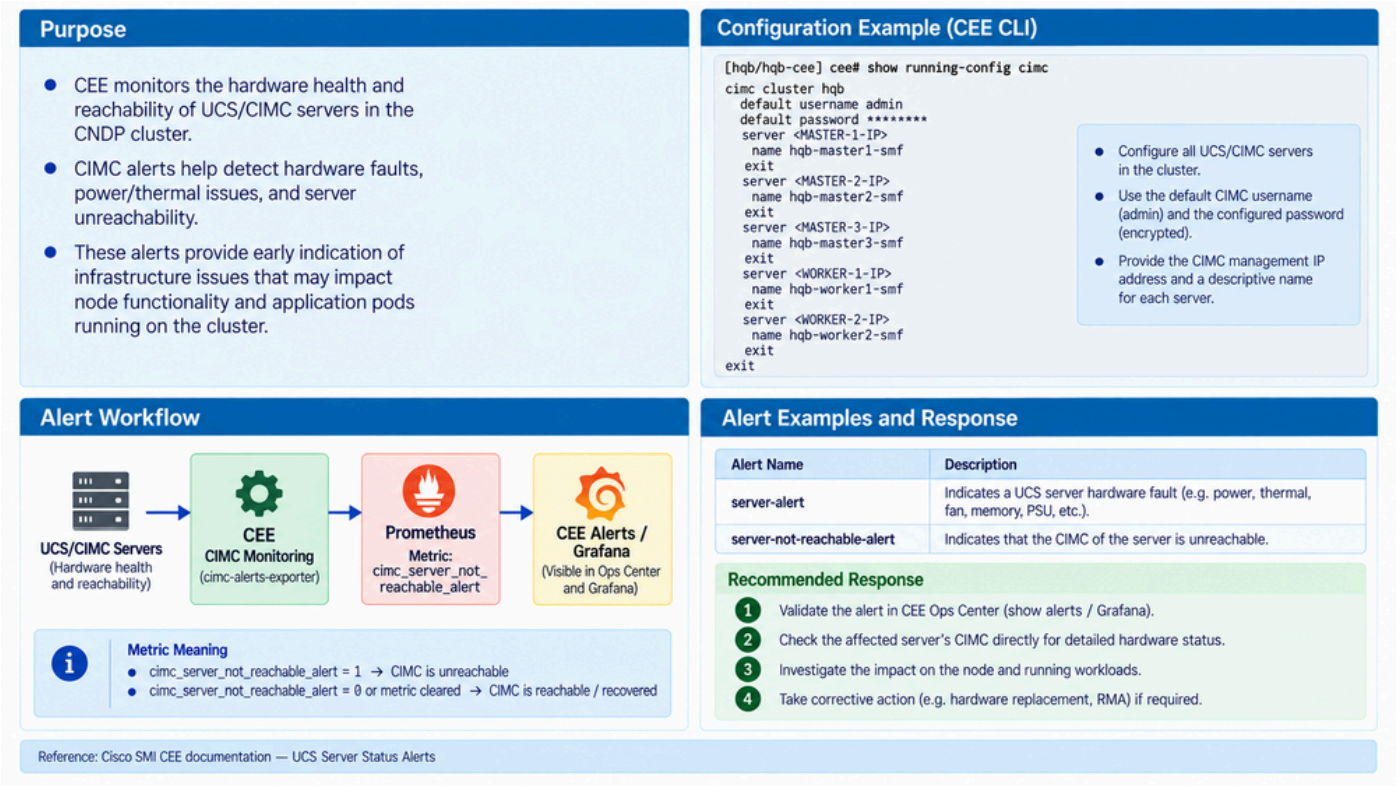
Alertes, SNMP et observabilité CIMC

Les alertes CEE utilisent Prometheus et Alertmanager. Prometheus évalue les mesures et les règles d'alerte. Alertmanager achemine les événements d'alerte vers les destinataires, avec alert-router fournissant une prise en charge de routage supplémentaire. CEE alert-logger fournit des enregistrements d'alertes historiques pour la récupération via le centre d'opérations CEE.



CEE Prometheus et Alertmanager - Transfert d'alertes et architecture SNMP

L'intégration des alertes CIMC fournit un chemin de surveillance de l'infrastructure connexe. Le cimc-alerts-exporter recueille des informations d'alerte CIMC et les expose à des fins de surveillance et de visualisation à Grafana.

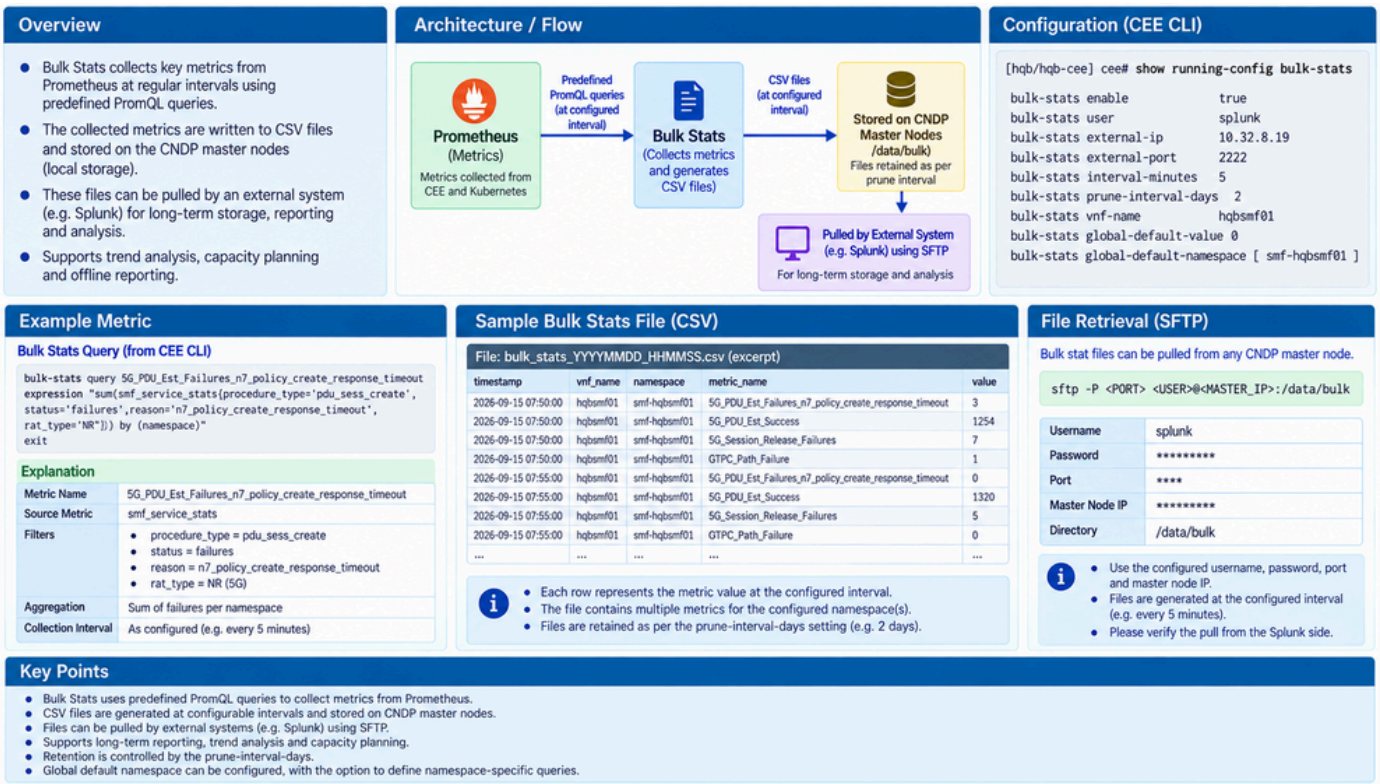


L'intégration SNMP est une interface d'alerte et de gestion ; il n'est interchangeable ni avec Splunk HEC ni avec le transfert syslog. Le protocole et les chemins d'acheminement des événements restent distincts.

Les références MIB (Management Information Base) pertinentes incluent CISCO-CNEE-MIB.my et CISCO-SMI.my.

Statistiques groupées

Le service CEE bulk-stats crée des instantanés CSV (Comma-Separated Values) périodiques des statistiques collectées via Prometheus. Il s'agit d'instantanés statistiques plutôt que de flux d'enregistrements du journal des applications.



Service de statistiques groupées CEE, création de snapshots CSV périodiques à partir des métriques Prometheus

La sortie de statistiques groupées prend en charge les rapports périodiques, l'analyse des tendances et le traitement des données en aval. Incluez-le dans un chemin d'intégration Splunk uniquement lorsque le déploiement transfère ou importe explicitement des données CSV/statistiques vers Splunk.

Passerelle système OpenTelemetry

Les versions plus récentes de Cisco SMI prennent en charge une passerelle OpenTelemetry Collector gérée par plate-forme. La passerelle reçoit la télémétrie des applications via le protocole OpenTelemetry Protocol (OTLP) et transfère les métriques et les journaux pris en charge vers les serveurs principaux locaux ou distants.



Remarque : La documentation relative aux opérations de Cisco SMI Cluster Manager identifie l'intégration de la passerelle OpenTelemetry avec la version 2026.03.1. La passerelle n'a pas été validée dans le déploiement spécifique décrit par l'exemple source, de sorte que cette section décrit le modèle de configuration publié plutôt que le fonctionnement vérifié dans cet environnement.

Modèle de passerelle système

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

Concepts de configuration de passerelle

Activez la passerelle OpenTelemetry Collector et sélectionnez les mesures locales et les moteurs de journalisation.

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

Lorsque le déploiement nécessite une exposition au service externe, la configuration peut inclure

une adresse IP externe.

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

Des paramètres de proxy facultatifs sont configurés pour les exportateurs de passerelle.

```
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
```

Les options de back-end local contrôlent la manière dont la passerelle système gérée par la plate-forme envoie la télémétrie aux back-ends intégrés. Les paramètres d'exposition IP externe et de proxy dépendent de la topologie et des exigences de sécurité.

Exportateurs distants

Exportation	Signaux	Utilisation technique
saut	Journaux, mesures	Envoyer la télémétrie à un serveur principal qui accepte OTLP sur gRPC.
otlphttp	Journaux, mesures	Envoyez des données de télémétrie à un serveur principal qui accepte le protocole OTLP sur HTTP.
éclat	Journaux	Envoi de journaux à un point de terminaison Splunk HEC.
journal	Journaux	Écrire les journaux dans le journal de noeud si pris en charge.
déboguer	Journaux, mesures	Prise en charge de la validation et du dépannage contrôlés.

Le pipeline OpenTelemetry suit le modèle de réception, de traitement et d'exportation. Les récepteurs ingèrent la télémétrie ; les processeurs filtrent ou transforment les données ; les exportateurs transmettent les signaux sélectionnés aux systèmes principaux distants ou locaux.

La source distingue également le comportement du proxy : otlp utilise des paramètres de proxy d'instance de collecteur, tandis que otlphttp et splunkhec prennent en charge les remplacements de proxy au niveau de l'exportateur lorsque la version déployée expose cette configuration.

Comparer avec OpenShift OpenTelemetry

Cisco CEE et OpenShift ont un modèle d'architecture commun : un collecteur OpenTelemetry peut se placer entre des applications instrumentées et des systèmes d'observation. Leurs modèles de gestion et d'installation sont différents.

Concept	Passerelle système CEE OpenTelemetry	Modèle OpenShift OpenTelemetry
Source de télémétrie	Charges de travail CEE et d'application compatibles OpenTelemetry	Charges de travail OpenShift compatibles avec OpenTelemetry
Protocol	OTLP	OTLP
Rôle du collecteur	Passerelle système gérée par plate-forme	Déploiement ou instance OpenTelemetry Collector
Concept de pipeline	Réception, traitement, exportation	Réception, traitement, exportation
Flexibilité du back-end	Moteurs de traitement locaux et exportateurs distants pris en charge	Intégration back-end axée sur les exportateurs
Intégration Splunk	splunkhec exportateur dans la configuration CEE documentée	Exportateur Splunk HEC configuré

Cette comparaison est architecturale. Les deux plates-formes ne sont pas censées implémenter OpenTelemetry de manière identique. OpenShift utilise généralement un modèle de déploiement OpenTelemetry Operator/Collector, tandis que la passerelle système Cisco SMI est gérée par plate-forme.

L'architecture de référence OpenShift décrite dans la source montre des collecteurs qui transfèrent la télémétrie depuis les charges de travail Kubernetes vers Splunk via HEC. Il illustre le modèle basé sur le collecteur plutôt qu'une intégration vérifiée pour l'exemple d'installation CEE.

Vérification de la configuration

Vérification de la synchronisation CEE

Vérifiez l'état et les journaux de synchronisation de SMI Cluster Manager et confirmez que les charges de travail CEE attendues sont déployées.

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

Vérifier HEC et Syslog séparément

Vérifiez que le chemin HEC envoie des événements au point d'extrémité TCP 8088 configuré et que le Splunk les reçoit. Confirmez séparément que le chemin syslog envoie des enregistrements UDP 5140 à l'écouteur configuré.

Utilisez les méthodes de capture de paquets dans les sections correspondantes et mettez en

corrélation les horodatages de paquets avec les événements reçus au niveau du collecteur configuré.

Vérifier les services Observability

Vérifiez que les mesures, le routage des alertes, les alertes CIMC et les instantanés de statistiques en masse fonctionnent comme prévu pour la version installée. Si OpenTelemetry est activé, vérifiez l'état du récepteur, du pipeline et de l'exportateur à l'aide de la procédure d'exploitation SMI Cluster Manager prise en charge.

Comportement attendu

Composant ou chemin	Résultat attendu
Gestionnaire de cluster SMI	La synchronisation du cluster est terminée et les services CEE requis sont déployés.
Centre des opérations	Les utilisateurs autorisés peuvent accéder aux fonctions opérationnelles et aux commandes de configuration/surveillance prises en charge.
Splunk HEC	Le trafic des événements atteint l'écouteur HEC configuré sur le port TCP 8088.
Syslog	Les événements au format RFC 5424 atteignent l'écouteur du port UDP 5140 configuré.
Alertes et CIMC	Alertmanager et les exportateurs associés exposent les informations d'alerte configurées.
Statistiques groupées	Des instantanés CSV périodiques sont générés à partir des statistiques collectées.
TélémétrieOuverte	Dans les versions prises en charge avec la passerelle configurée, les signaux OTLP circulent dans le pipeline principal/exportateur sélectionné.

Flux de décision

Observation	Vérification suivante
Les services CEE sont absents après la synchronisation.	Inspectez l'état de synchronisation, les journaux, l'artefact logiciel et les paramètres Ops Center de Cluster Manager.
Les événements HEC sont manquants.	Identifiez le pod/noeud de transfert, vérifiez le trafic TCP 8088, la destination HEC, l'authentification et la configuration TLS.
Les événements Syslog sont manquants.	Vérifiez la destination UDP 5140, le formatage RFC 5424, le flux de paquets et le comportement du récepteur.
Des alertes ou des données CIMC sont manquantes.	Cochez les options de routage Prometheus/Alertmanager, alert-router et cimc-alerts-exporter.
Des statistiques en masse	Confirmez le fonctionnement du service de statistiques en masse, la

Observation	Vérification suivante
sont manquantes.	disponibilité des données Prometheus et la génération de clichés CSV.
L'exportation OpenTelemetry est manquante.	Vérifiez la prise en charge des fonctionnalités pour la version installée, la configuration de la passerelle, l'état du récepteur et de l'exportateur et l'appartenance au pipeline.

Conclusion

CEE est un environnement d'observation et d'exécution basé sur Kubernetes en couches autour des applications SMF. La séparation des espaces de noms Kubernetes divise les opérations de plate-forme, les services CEE et les charges de travail d'application en différents domaines. Au sein de CEE, la surveillance, les alertes, la journalisation et les statistiques groupées sont des services spécialisés ayant des responsabilités indépendantes.

La principale distinction Splunk est entre HEC sur TCP 8088 et syslog sur UDP 5140. Il s’agit de chemins de transfert distincts avec différents protocoles, configurations et procédures de dépannage. La nouvelle passerelle système OpenTelemetry ajoute un collecteur basé sur OTLP et un modèle d'exportateur. Sa similitude avec OpenShift OpenTelemetry est architecturale, et le fonctionnement de la passerelle doit être vérifié pour la version et le déploiement CEE spécifiques.

Autres informations utiles

- Guide de configuration et d'administration de Cisco CEE - Common Execution Environment
- Guide de configuration et d'administration de Cisco CEE - Commandes de journalisation
- Opérations de Cisco SMI Cluster Manager - Synchronisation et OpenTelemetry
- RFC 5424 - Protocole Syslog

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.