Cisco CEEの監視可能性とSplunkの統合について

内容

概要

前提条件

- 要件
- 使用するコンポーネント

背景説明

アーキテクチャ概要

CEE名前空間ワークロード

CEEのインストールとライフサイクル管理

- インストールモード
- CEEソフトウェアアーティファクトの定義
- クラスタとオペレーションセンターの設定
- 同期と展開の確認

CEEオペレーションセンターおよび運用管理

CEE可観測性アーキテクチャ

Splunkの統合：ログ転送アーキテクチャ

Splunk HTTPイベントコレクタの転送

- HEC構成モデル
- HECトラフィックのキャプチャとトラブルシューティング

UDP 5140でのSyslog転送

- RFC 5424フィールドマッピング
- UDPトランスポートおよびパケットキャプチャ

アラート、SNMP、およびCIMCの監視可能性

バルク統計情報

OpenTelemetryシステムゲートウェイ

- システムゲートウェイモデル
- ゲートウェイ設定の概念
- リモートエクスポータ
- OpenShift OpenTelemetryとの比較

設定を検証する

- CEE同期の確認
- HECとsyslogの個別確認
- 監視サービスの検証

予想される動作

決定フロー

結論

関連コンテンツ

概要

このドキュメントでは、Cisco Common Execution Environment(CEE)アーキテクチャ、導入、モニタリング、Splunk統合、およびOpenTelemetryについて説明します。

前提条件

要件

次のテクノロジーに精通していることが推奨されます。

- Cloud Native Deployment Platform(CNDP)、Kubernetes名前空間、ポッド配置。
- Cisco Subscriber Microservices Infrastructure(SMI)およびSMI Cluster Manager
- CEE Ops Center、Prometheus、Grafana、Alertmanager、および口グ転送コンポーネント
- Splunk HTTPイベントコレクタ(HEC)、syslog、およびtcpdumpによるパケットキャプチャ
- OpenTelemetry Protocol(OTLP)およびOpenTelemetry Collectorによる新しいゲートウェイ統合

使用するコンポーネント

この例は、CEEと関連するセッション管理機能(SMF)アプリケーションを使用した、KubernetesベースのCisco SMI/CNDP環境を示しています。ソフトウェア定義の例ではCEEパッケージ2026.01.1.08を参照し、Ops Centerの例ではSMFリポジトリIDとしてsmf-2026.04.m0.i50を使用しています。これらは値の例であり、導入要件ではありません。

ネットワークエンドポイント、クラスタ名、および名前空間の値は、ターゲットの展開で承認された値に置き換える必要があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Common Execution Environment(CEE)は、Cisco Subscriber Microservices Infrastructure(SMI)の一部です。 KubernetesベースのCNDP展開では、Kubernetesネームスペー

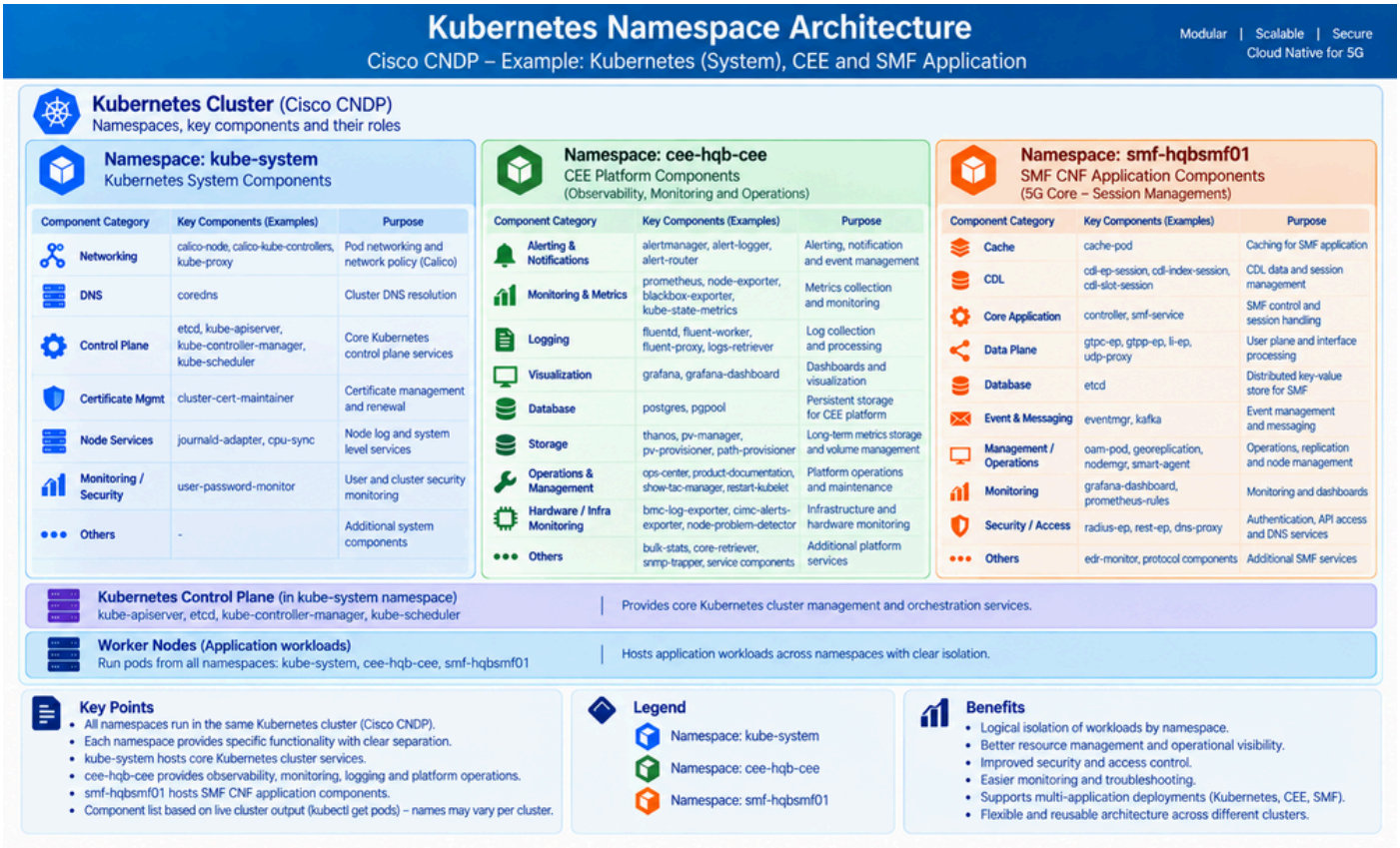
スによって、プラットフォームサービス、CEEの可観測性とKubernetes管理サービス、およびSMFアプリケーションワークロードが分離されます。分離によって管理境界と運用境界が提供され、Kubernetesのネットワーキングとサービス検出によって許可されたコンポーネント通信が可能になります。

このドキュメントでは、名前空間アーキテクチャ、CEEワークロード、CEEインストールとライフサイクル管理、CEE Ops Center、アラートとSimple Network Management Protocol(SNMP)、Cisco Integrated Management Controller(CIMC)アラート、ログ転送、バルク統計、およびOpenTelemetryシステムゲートウェイについて説明します。

伝送制御プロトコル(TCP)ポート8088でのSplunk HECと、ユーザデータグラムプロトコル(UDP)ポート5140でのsyslogは、それぞれ独立した取り込みメカニズムです。この2つのパスは、設定、転送、およびトラブルシューティングの要件が異なり、共存できます。

アーキテクチャ概要

CEEとそれに関連するアプリケーション関数は、別々のKubernetes名前空間を使用します。このアーキテクチャは、Kubernetesプラットフォームサービスを、CEEの可観測性および管理機能、およびSMFアプリケーションドメインと区別するものです。



CEEとアプリケーションプラットフォームの分離を示すCisco SMIネームスペースアーキテクチャ

CEE名前空間は、サービスレベルアーキテクチャの中心となります。その他の名前空間は、Kubernetesプラットフォーム、ネットワーキング関数、およびSMFワークロードを提供します。

CEE名前空間ワークロード

CEE名前空間は、監視、アラート、ロギング、ダッシュボード、統計、および運用アクセスのためのマイクロサービスをホストします。

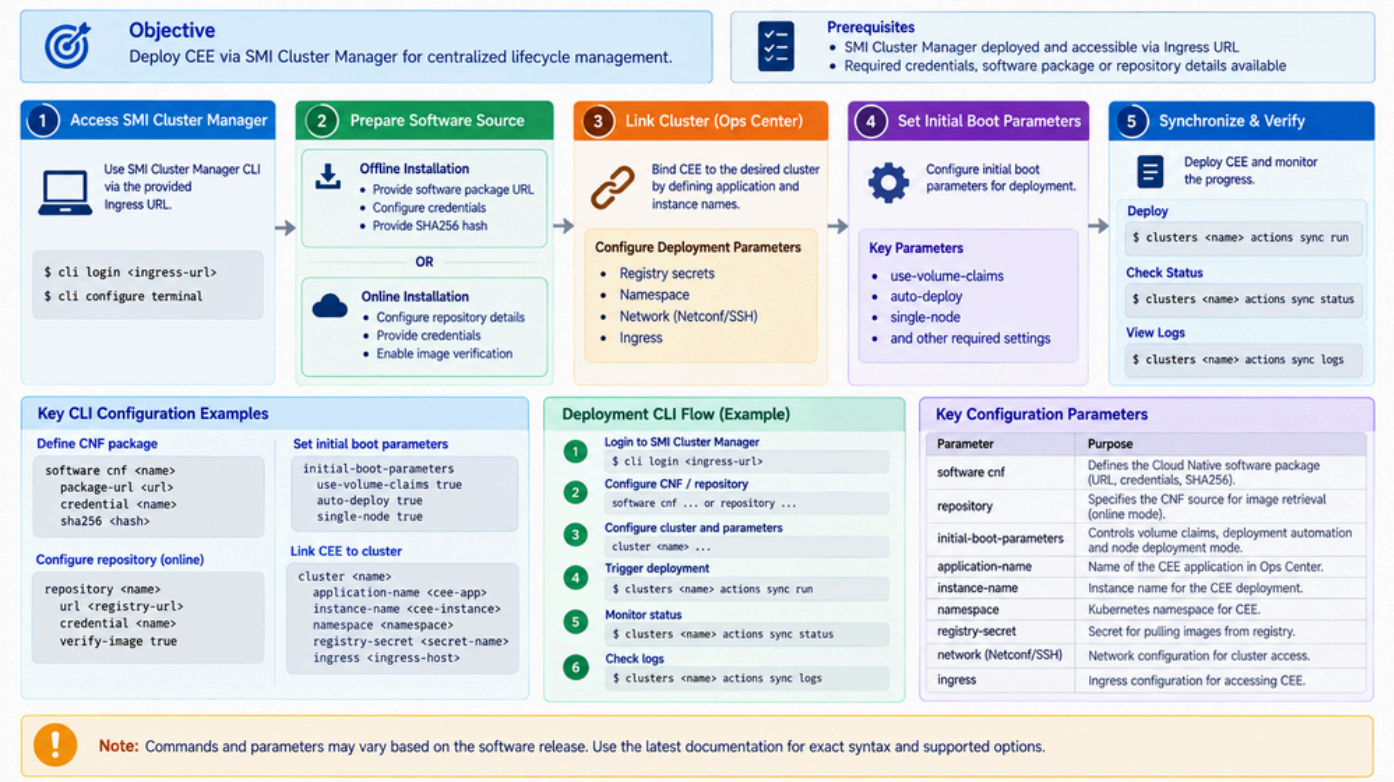


CEE名前空間マイクロサービスとその運用ワークロードの機能

これらの機能には、Prometheusメトリック収集、Grafana可視化、Alertmanagerアラート処理、ログ転送サービス、および定期的なバルク統計の作成が含まれます。個々のワークロードは、リリースおよび導入構成によって異なります。

CEEのインストールとライフサイクル管理

SMIクラスタ・マネージャは、ソフトウェア・アーチファクト定義をターゲット・クラスタおよびそのOpsセンター構成から分離します。これにより、ソフトウェアのバージョン管理と反復可能なクラスタの同期が可能になります。



SMI Cluster Manager CEEのインストールおよびソフトウェア同期アーキテクチャ

インストールモード

- オフラインインストールでは、ファイルURLとSecure Hash Algorithm(SHA)256ビット(SHA-256)ハッシュを使用して、ローカルソフトウェアパッケージを参照できます。
- クラスタ構成は、CEE/SMF展開を目的のクラスタおよびOps Centerインスタンスに関連付けます。

CEEソフトウェアアーティファクトの定義

SMI Cluster Managerの設定で、ローカルCEEソフトウェアパッケージとそのSHA-256ハッシュを特定します。

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

承認されたパッケージの正確なSHA-256値を使用します。このコマンドのプレースホルダは意図的なものであり、実際のチェックサムを表すものではありません。

クラスタとオペレーションセンターの設定

ソース構成は、クラスタをSMFオペレーションセンター、ローカルリポジトリ、管理エンドポイント、および配備設定に関連付けます。サイト固有の識別子は、プレースホルダに置き換えられます。

```
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
```

パラメータ	設定例での意味
ops-centers smf <smf-ops-center-name>	クラスタをSMF Ops Centerインスタンスに関連付けます。
リポジトリローカル	配置するアプリケーションリポジトリとバージョンを指定します。
sync-default-repository真	同期中に設定されたデフォルトのリポジトリを使用します。
netconfポート2029	NETCONF管理接続ポートを指定します。
sshポート2028	セキュアシェル(SSH)管理接続ポートを指定します。
use-volume-claimsが真	永続的なストレージ要件にボリューム要求を使用できます。
auto-deployの誤り	自動展開を無効にして、同期と検証を明示的に制御します。
シングルノードfalse	シングルノードモードでない展開を指定します。



注：パッケージIDとリポジトリIDは、ソース設定の例です。リリースの互換性とエンドポイントの値を確認してから、別のクラスタで使用します。

同期と展開の確認

ソフトウェアとオペレーションセンターの構成の準備が整ったら、クラスター同期アクションを

実行します。

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

同期ステータスとログを調べます。

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

同期が正常に完了し、予想されるCEEポッドとサービスが展開されていることを確認します。

⚠ 注意：クラスタの同期とソフトウェアの導入によって、実行環境が変更される可能性があります。承認されたメンテナンスおよび導入手順に従って変更を適用します。

CEEオペレーションセンターおよび運用管理

CEEオペレーションセンターは、CEEサービスの運用インターフェイスを提供します。このワークロードは、クラスタ内のCEE機能のユーザ管理、認証、設定、およびshowコマンドをサポートします。SMIクラスタ・マネージャは、管理構成を通じてOps Centerをターゲットの導入に関連づけます。

オペレーションセンターは管理プレーンに属しています。Prometheus、Alertmanager、Fluent Bit/fluent-proxy、HEC、syslog、およびOpenTelemetryは、モニタリングおよびテレメトリパスに属しています。これらの責任を分離しておくと、トラブルシューティングが容易になります。

CEE可観測性アーキテクチャ

CEEの監視可能性には、メトリック、アラート、ログ、CIMCアラート、およびバルク統計が含まれます。これらのサービスは関連していますが、データパスとコンシューマは異なります。

機能	主な目的	一般的な宛先またはコンシューマ
メトリック	ノード、Kubernetes、およびサービスから時系列の測定値を収集し、照会します。	Prometheus、Grafana、およびThanos。
アラート	アラートルールとルートアラートイベントを評価します。	Alertmanager、alert-router、Ops Center、および外部レシーバ

機能	主な目的	一般的な宛先またはコンシューマ
ログ	ログおよびイベントレコードを外部のコレクタまたはバックエンドに転送します。	Splunkおよびその他のログコレクタ。
CIMCアラート	モニタリング用にCisco Integrated Management Controller(CIMC)アラートをエクスポートします。	CEEメトリック/アラートおよびGrafana。
バルク統計情報	定期的な統計スナップショットを作成します。	CSVスナップショットおよびダウンストリーム処理または分析

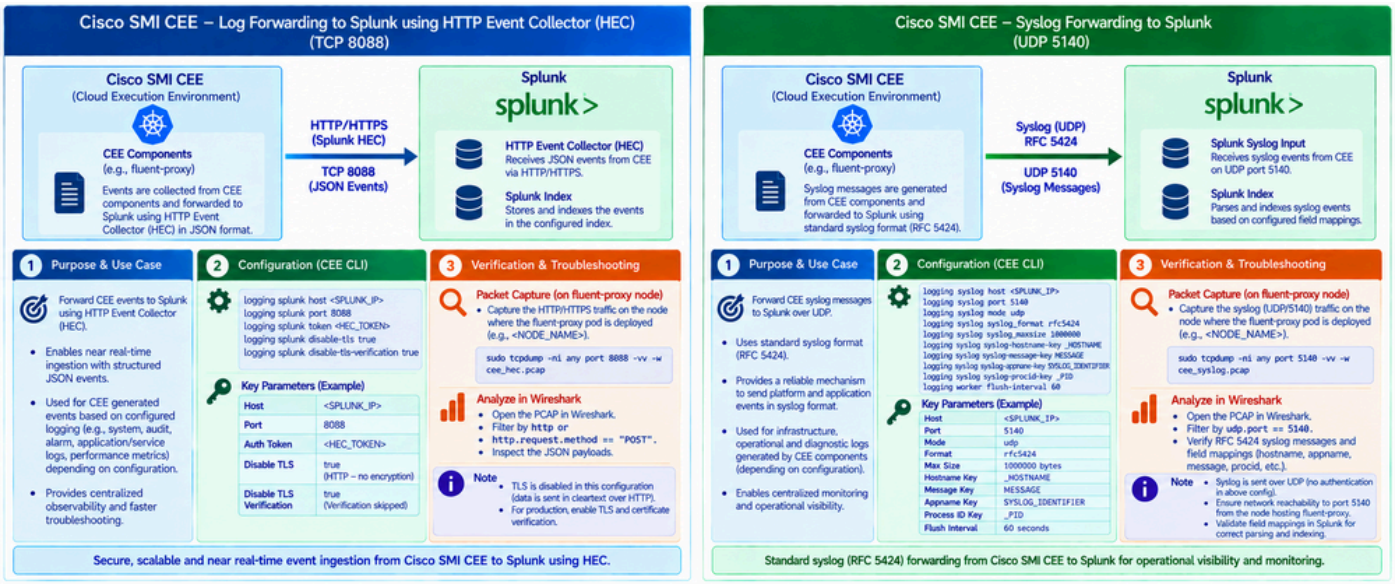
Splunkの統合：ログ転送アーキテクチャ

送信元は、2つのCEE-to-Splunkパスを記述します。どちらもSplunkにイベントを配信できますが、個別のプロトコルと取り込みインターフェイスを使用します。

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

各パスで伝送されるイベントタイプは、CEEの設定と実装された転送パイプラインによって異なります。2つの設定済みインターフェイスは、それぞれが相互に排他的なイベントカテゴリを伝送することを確立しません。

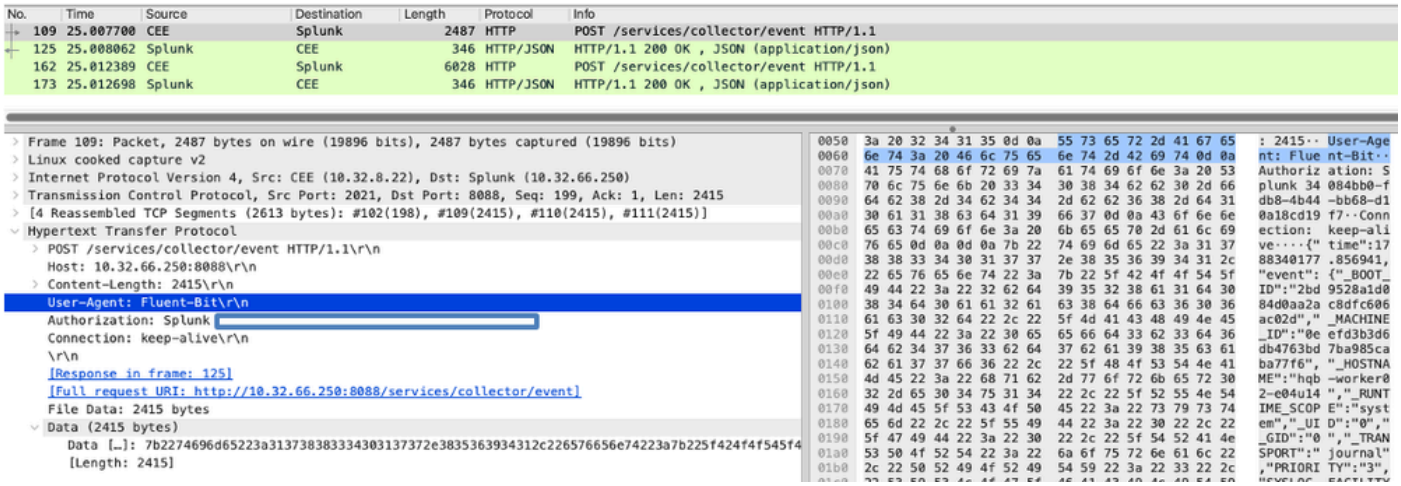
パスを個別にトレースします。HECの配信に成功してもsyslogの配信は確認されず、syslogの配信に成功してもHECの配信は確認されません。



個別のHECおよびsyslog転送パスを使用したCEE Splunkの統合

Splunk HTTPイベントコレクタの転送

Splunk HECはHTTPイベントの送信を受け入れ、HEC認証トークンを使用します。CEEは、このパスに対してファイルベースの取得を要求する代わりに、設定済みのHECサービスにイベントを直接転送します。



TCPポート8088でのCEEからSplunkへのHTTPイベントコレクタの転送アーキテクチャ

HEC構成モデル

元のラボの例には、CEE Splunkエンドポイントの次の設定が含まれています。この抜粋にはソースの動作が記録されており、推奨される実稼働構成ではありません。

⚠ 注意：送信元の例では、TLSと証明書の両方の検証が無効になっています。これにより、テレメトリとHECクレデンシャルがネットワーク上の代行受信に公開されます。実稼働環境では、サポートされているCEEリリースの設定に従って、TLSと証明書の検証を有効にし、HEC認証トークンを保護します。

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

ソースアーキテクチャでは、CEEログ/イベント生成元が、関連するFluent転送コンポーネントを介してHEC宛先に転送します。

```
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トラフィックのキャプチャとトラブルシューティング

fluent-proxyがHECトラフィックを伝送する場合に、CEE名前空間でfluent-proxyポッドとそのKubernetesワーカーノードを特定します。

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

HECトラフィックを伝送するKubernetesノードで、HECポートのパケットをキャプチャします。

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

TLSが有効な接続の場合、パケットキャプチャによってトランスポートの確立と宛先の詳細が明らかになりますが、通常はHTTPペイロードは公開されません。TLSが無効な場合、イベントの内容と認証マテリアルをキャプチャに表示できます。

⚠ 注意：パケットキャプチャおよびログには、機密のテレメトリおよびクレデンシャルが含まれる場合があります。許可されたサポートワークフローへの収集と転送を制限し、キャプチャファイルを保護します。

UDP 5140でのSyslog転送

2つ目のSplunk統合パスは、RFC 5424形式とUDPポート5140を使用してsyslogレコードを転送します。ソース構成では、フィールドマッピング、最大メッセージサイズ、およびワーカーフラッシュ間隔も定義されます。

```
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フィールドマッピング

CEEソースフィールド	Syslogフィールドまたは目的
ホスト名(_H)	生成されたsyslogレコードで発信元ホストを識別します。
メッセージ	ログメッセージ本文を伝送します。
SYSLOG_IDENTIFIER	syslogアプリケーションまたはプログラムの識別子を提供します。
PID(_P)	発信元プロセスIDを伝送します。

UDPトランスポートおよびパケットキャプチャ

UDPはコネクションレス型で、トランスポート配信確認応答も再送信も提供しません。トラブルシューティングでは、パケット損失、ルーティング、最大伝送ユニット(MTU)、フラグメンテーション、受信側のアベイラビリティ、およびキュー/レートの動作を考慮する必要があります。

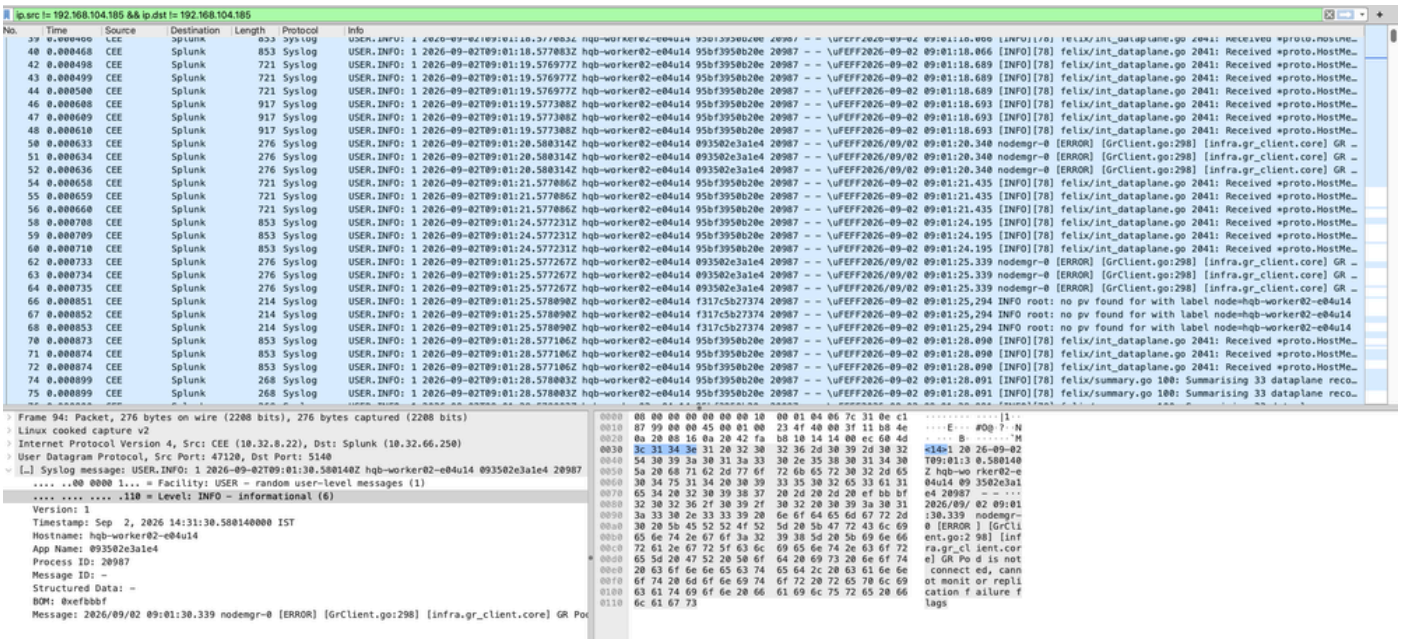
syslogトラフィックを伝送するインターフェイスまたはKubernetesノードで、次のコマンドを実行します。

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

fluent-proxyがsyslogトラフィックを転送する場合、そのコンポーネントをホストしているノードが適切なパケットキャプチャポイントになります。パケットを収集する前に転送パスを確認します。



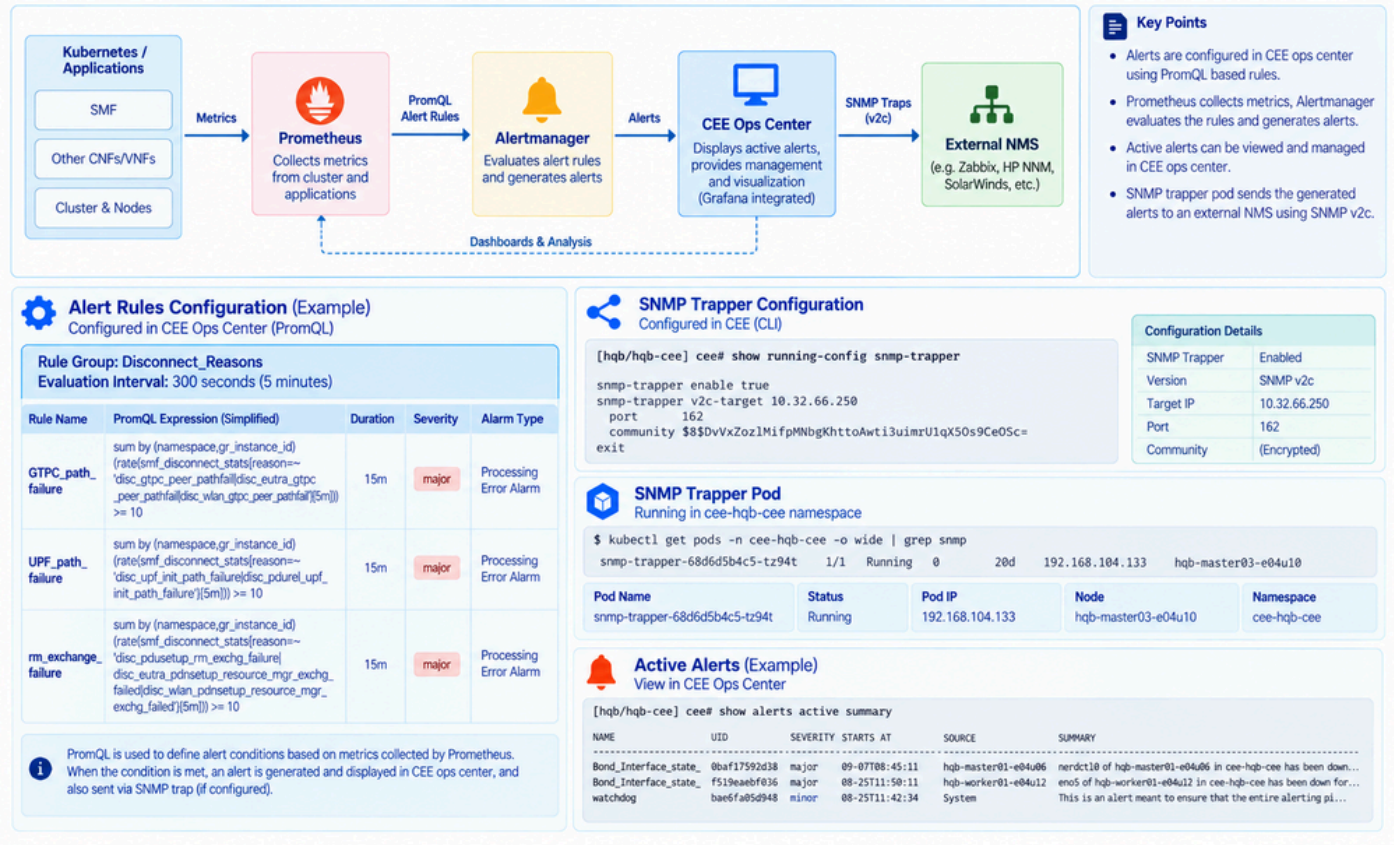
注:RFC 5424では、選択されたトランスポートとは独立してsyslogメッセージの形式が定義されています。送信元シナリオではUDP 5140を使用します。TLSベースのsyslog転送は、互換性のある送信側と受信側の設定を必要とする別のオプションです。



UDPポート5140およびRFC 5424フィールドを使用したSplunkへのCEE syslog転送

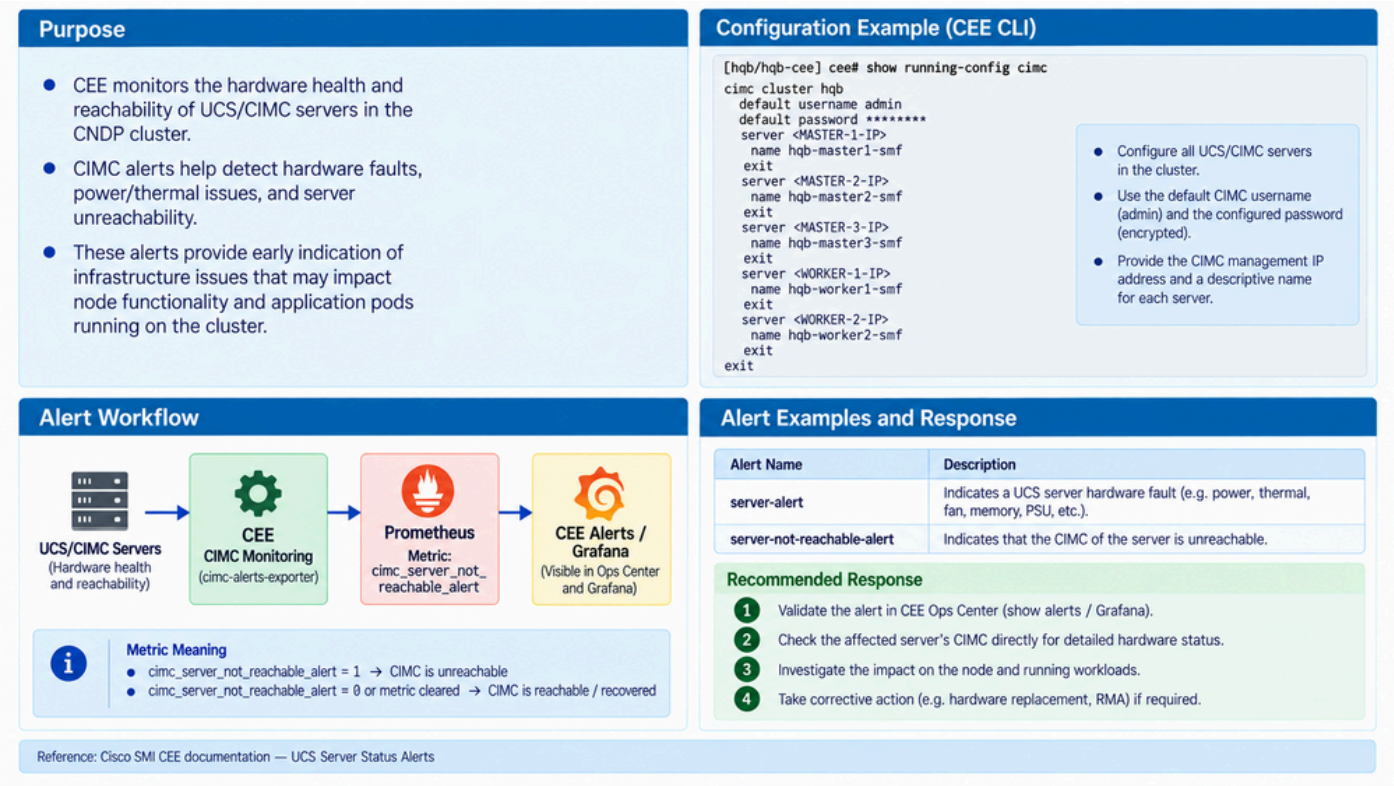
アラート、SNMP、およびCIMCの監視可能性

CEEアラートは、PrometheusとAlertmanagerを使用します。Prometheusは、メトリックとアラートルールを評価します。Alertmanagerは、追加のルーティングサポートを提供するalert-routerを使用して、アラートイベントを受信者にルーティングします。CEEアラートロガーは、CEE Ops Centerを通じて取得できる履歴アラートレコードを提供します。



CEE PrometheusおよびAlertmanagerのアラート転送とSNMPアーキテクチャ

CIMCアラートの統合により、関連するインフラストラクチャモニタリングパスが提供されます。cimc-alerts-exporterは、CIMCアラート情報を収集し、Grafanaでモニタリングおよび可視化するために公開します。

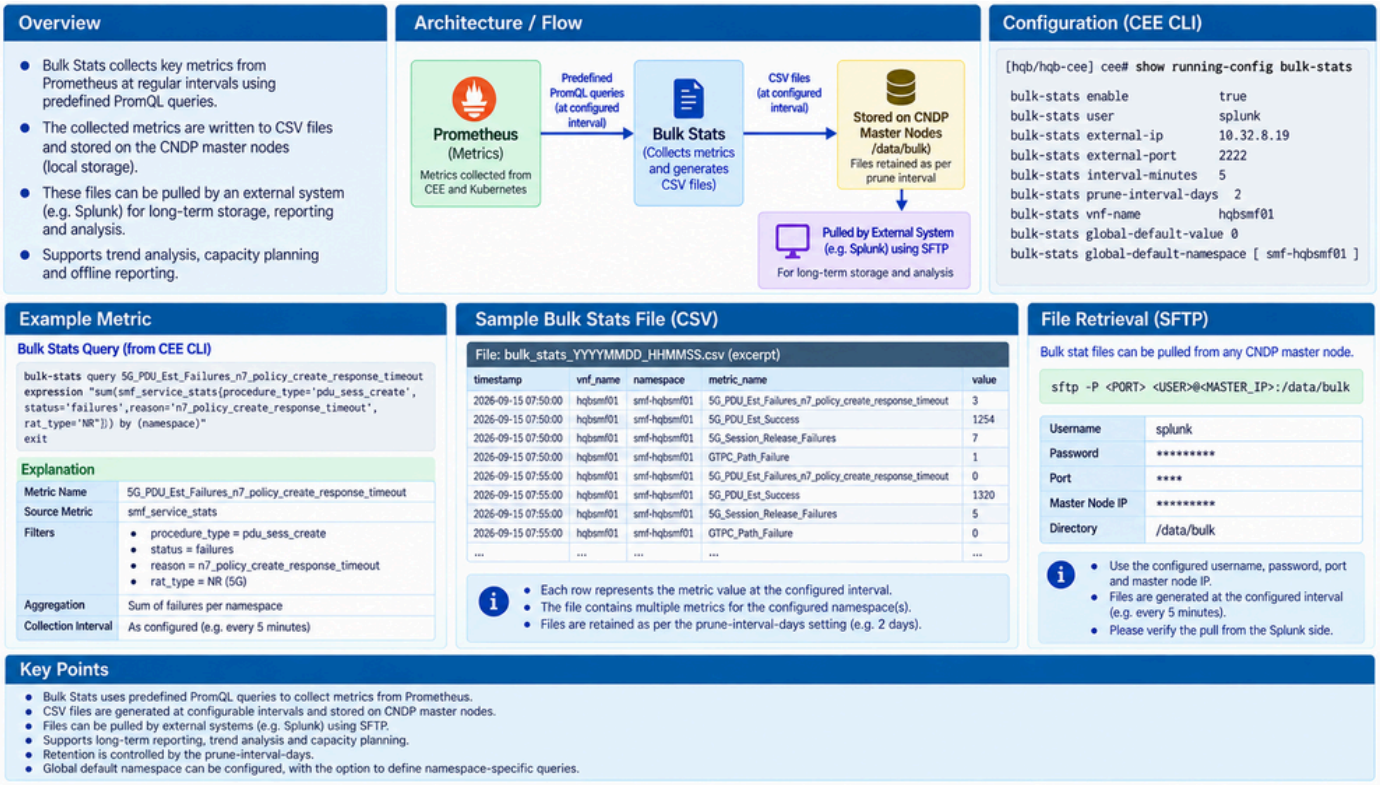


SNMP統合は、アラートおよび管理インターフェイスであり、Splunk HECまたはsyslog転送と交換することはできません。プロトコルとイベント配信パスは異なったままです。

関連するManagement Information Base（MIB；管理情報ベース）の参照には、CISCO-CNEE-MIB.myとCISCO-SMI.myが含まれます。

バルク統計情報

CEE bulk-statsサービスは、Prometheusを通じて収集された統計情報のカンマ区切り値(CSV)スナップショットを定期的に作成します。これらは、アプリケーションログレコードのストリームではなく、統計スナップショットです。



CEE Bulk Statistics ServiceによるPrometheusメトリックからの定期的なCSVスナップショットの作成

バルク統計の出力は、定期的なレポート、傾向分析、およびダウンストリームデータ処理をサポートします。導入でCSV/統計データをSplunkに明示的に転送またはインポートする場合にのみ、Splunk統合パスに含めます。

OpenTelemetryシステムゲートウェイ

新しいCisco SMIリリースは、プラットフォーム管理のOpenTelemetry Collectorゲートウェイをサポートします。ゲートウェイは、OpenTelemetry Protocol(OTLP)を介してアプリケーションからテレメトリを受信し、サポートされているメトリックとログをローカルまたはリモートのバックエンドに転送します。



注:『Cisco SMI Cluster Manager Operations』のドキュメントには、OpenTelemetryゲートウェイとリリース2026.03.1との統合が記載されています。ソースの例で説明されている特定の導入ではゲートウェイが検証されていないため、このセクションでは、その環境での動作の検証ではなく、公開されている設定モデルについて説明します。

システムゲートウェイモデル

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

ゲートウェイ設定の概念

OpenTelemetry Collectorゲートウェイを有効にし、ローカルメトリックとログバックエンドを選択します。

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

導入で外部サービスへのアクセスが必要な場合は、設定に外部IPを含めることができます。

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

ゲートウェイエクスポータには、オプションのプロキシ設定が設定されています。

```
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
```

ローカルバックエンドオプションは、プラットフォーム管理システムゲートウェイが内蔵バックエンドにテレメトリを送信する方法を制御します。外部IPの露出とプロキシ設定は、トポロジとセキュリティ要件によって異なります。

リモートエクスポータ

輸出者	信号	技術的な用途
OTLP	ログ、メトリック	gRPC経由でOTLPを受け入れるバックエンドにテレメトリを送信します。
OTLPHTTP	ログ、メトリック	HTTP経由でOTLPを受け入れるバックエンドにテレメトリを送信します。
スプルンケク	ログ	Splunk HECエンドポイントにログを送信します。
ジャーナード	ログ	サポートされているノードジャーナルにログを書き込みます。
デバッグ	ログ、メトリック	制御された検証とトラブルシューティングをサポートします。

OpenTelemetryパイプラインは、受信、処理、およびエクスポートモデルに従います。レシーバはテレメトリを取り込み、プロセッサはデータをフィルタリングまたは変換し、エクスポータは選択された信号をリモートまたはローカルのバックエンドに配信します。

また、otlpではコレクタインスタンスのプロキシ設定を使用するのに対し、otlphttpとsplunkhecでは、導入されたリリースでプロキシ設定が公開されている場合に、エクスポータレベルでプロキシ設定をオーバーライドできます。

OpenShift OpenTelemetryとの比較

Cisco CEEとOpenShiftは、アーキテクチャパターンを共有しています。OpenTelemetry Collectorは、計測済みアプリケーションと監視可能なバックエンドの間に配置できます。管理モデルと設置モデルが異なります。

概念	CEE OpenTelemetryシステムゲートウェイ	OpenShift OpenTelemetryパターン
テレメトリソース	OpenTelemetry対応CEEおよびアプリケーションワークロード	OpenTelemetry対応OpenShiftワークロード

概念	CEE OpenTelemetryシステムゲートウェイ	OpenShift OpenTelemetryパターン
プロトコル	OTLP	OTLP
コレクタロール	プラットフォーム管理のシステムゲートウェイ	OpenTelemetry Collectorの導入またはインスタンス
パイプラインの概念	受信、処理、エクスポート	受信、処理、エクスポート
バックエンド柔軟性	ローカルバックエンドおよびサポートされるリモートエクスポータ	エクスポータ主導のバックエンド統合
Splunkの統合	文書化されたCEE設定のsplunkhecエクスポータ	Splunk HECエクスポータが設定されている場合

この比較はアーキテクチャ上のものです。この2つのプラットフォームは、OpenTelemetryを同一に実装すると主張するものではありません。OpenShiftは一般的にOpenTelemetry Operator/Collector導入モデルを使用し、Cisco SMIシステムゲートウェイはプラットフォーム管理されます。

ソースで説明されているOpenShiftリファレンスアーキテクチャは、コレクタがKubernetesのワークロードからHEC上のSplunkにテレメトリを転送することを示しています。この図は、サンプルCEEインストールの検証済みの統合ではなく、コレクタベースのモデルを示しています。

設定を検証する

CEE同期の確認

SMI Cluster Managerの同期ステータスとログを確認し、予想されるCEEワークロードが展開されていることを確認します。

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

HECとsyslogの個別確認

HECパスが設定済みのTCP 8088エンドポイントにイベントを送信し、Splunkがそれを受信することを確認します。syslogパスが設定されたリスナーにUDP 5140レコードを送信することを個別に確認します。

対応するセクションのパケットキャプチャ方式を使用して、パケットタイムスタンプを、設定されたコレクタで受信されたイベントに関連付けます。

監視サービスの検証

メトリック、アラートルーティング、CIMCアラート、およびバルク統計スナップショットが、インストールされたリリースに対して設計どおりに動作することを確認します。OpenTelemetryが有効になっている場合は、サポートされているSMI Cluster Managerの操作手順を使用して、受信側、パイプライン、および エクスポータの状態を確認します。

予想される動作

コンポーネントまたはパス	予想される結果
SMIクラスタ・マネージャ	クラスタの同期が完了し、必要なCEEサービスが展開されます。
オペレーションセンター	権限を持つユーザは、運用機能およびサポートされている設定/モニタリングコマンドにアクセスできます。
Splunk HEC	イベントトラフィックは、TCPポート8088で設定されたHECリスナーに到達します。
Syslog	RFC 5424形式のイベントは、設定されているUDPポート5140リスナーに到達します。
アラートとCIMC	Alertmanagerおよび関連するエクスポータは、設定されているアラート情報を公開します。
バルク統計情報	収集された統計情報から定期的なCSVスナップショットが生成されます。
オープンテレメトリ	ゲートウェイが設定されたサポートされているリリースでは、OTLP信号は選択されたバックエンド/エクスポータのパイプラインを通過します。

決定フロー

観察	次のチェック
CEEサービスは同期後に存在しません。	Cluster Managerの同期ステータス、ログ、ソフトウェアアーティファクト、およびOps Centerパラメータを検査します。
HECイベントが見つかりません。	フォワーディングポッド/ノードを特定し、TCP 8088トラフィック、HEC宛先、認証、およびTLS設定を確認します。
syslogイベントが欠落している。	UDP 5140の宛先、RFC 5424のフォーマット、パケットフロー、および受信側の動作を確認します。
アラートまたはCIMCデータが欠落している。	Prometheus/Alertmanagerのルーティング、alert-router、およびcimc-alerts-exporterの動作を確認します。
バルク統計が見つかりません。	bulk-statsサービスの動作、Prometheusデータの可用性、およびCSVスナップショットの生成を確認します。
OpenTelemetryエクスポートがありません。	インストールされたリリースの機能サポート、ゲートウェイの設定、レシーバとエクスポータの状態、およびパイプラインメンバーシップを確認します。

結論

CEEは、SMFアプリケーションを中心としたKubernetesベースの階層型の実行および監視可能性環境です。Kubernetes名前空間の分離により、プラットフォームの運用、CEEサービス、およびアプリケーションワークロードが異なるドメインに分割されます。CEE内では、モニタリング、アラート、ロギング、およびバルク統計は、独立した責任を持つ特殊なサービスです。

Splunkの主な違いは、HEC over TCP 8088とsyslog over UDP 5140の違いです。これらは、異なるプロトコル、設定、およびトラブルシューティング手順を持つ個別の転送パスです。新しいOpenTelemetryシステムゲートウェイでは、OTLPベースのコレクタおよびエクスポータモデルが追加されています。OpenShift OpenTelemetryとの類似点はアーキテクチャ上にあり、特定のCEEリリースおよび導入に対してゲートウェイの動作を検証する必要があります。

関連コンテンツ

- Cisco CEE構成およびアドミニストレーションガイド – 共通実行環境
- Cisco CEE設定およびアドミニストレーションガイド – ロギングコマンド
- Cisco SMI Cluster Managerの操作：同期およびオープンテレメトリ
- RFC 5424 - Syslogプロトコル

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。