فهم إمكانية مراقبة Cisco CEE وتكامل Splunk

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

نظرة عامة على البنية

مجموعة المستشعر المجمعة (CEE) لشبكة الإنترنت المستخدمة لجمع المعلومات

تثبيت شبكة الإنترنت المستخدمة لمجموعة المستشعر المجمعة (CEE) لأجهزة التوجيه

أوضاع التثبيت

تدفق برنامج CEE

نظرة عامة على النظام المجموعة و OPS

التشفير والمصادقة

تكوين شبكة الإنترنت المستخدمة لمجموعة المستشعر المجمعة (CEE) والموجهات مركز العمليات

تكوين CEE البيانات للمراقبة

تسجيل الدخول إلى Splunk: تكوين

إعداد مجموعة أحداث Splunk HTTP

تكوين HEC

استكشاف أخطاء رمز حالة HEC والصمامات

إعداد توجيه Syslog عبر UDP 5140

تعيين الحقول وفقا لمعيار RFC 5424

تكوين UDP وتجاوز النقل

مراقبة البنية التحتية و SNMP و CIMC

خصائص الجرم

نظرة عامة على بوابة OpenTelemetry

تكوين بوابة النظام

مفاهيم تكوين البوابة

المصدر عن بعد

مقارنة OpenShift OpenTelemetry

التحقق من التكوين

التحقق من صحة CEE

تصفية syslog و netflow للتحقق من الحقل العلوي

التحقق من صحة إدخال المقاييس

الأخطاء الشائعة

التدفق المرتجع

المرتجع

الخاتمة

المقدمة

يصف هذه المستندات بنية بيئة التنفيذ المشترك (CEE) من Cisco والنشر والمراقبة وتكامل Splunk وقياس OpenTele.

المتطلبات الأساسية

المتطلبات

توصي Cisco بالألفة مع هذه التقنيات:

- النظام الأساسي للنشر الأصلي للسحابة (CNDP) ومساحات أسماء Kubernetes وموضع Pod.
- البنية الأساسية للخدمات الدقيقة للمشترك (SMI) من Cisco ومدير مجموعة SMI.
- مكونات مركز عمليات شبكة إيثرنت المحسنة المجمعة (CEE) وبروميثيوس وغرافانا وبرنامج AlertManager وإعادة توجيه السجلات.
- مجمع أحداث HTTP (HEC)، و syslog، والتقاط الحزمة باستخدام tcpdump.
- برتوكول OpenTeleEmetry (OTLP) ومجمع OpenTeleEmetry لتكامل العبارة الأحدث.

المكونات المستخدمة

تظهر الأمثلة بيئة Cisco SMI/CNDP المستندة إلى Kubernetes مع CEE وتطبيق وظيفة إدارة الجلسات المرتبط (SMF). يشير مثال تعريف البرنامج إلى حزمة تقنية شبكة إيثرنت المحسنة المجمعة 2026.01.1.08؛ يستخدم المثال الخاص بمركز العمليات معرف مستودع SMF SMF-2026.04.m0.i50. هذه هي قيم الأمثلة، وليست متطلبات النشر.

يجب إستبدال نقاط نهاية الشبكة أو أسماء نظام المجموعة وقيم مساحة الاسم بالقيم المعتمدة للنشر الهدف.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تعد بيئة التنفيذ المشترك (CEE) من Cisco جزءا من البنية الأساسية للخدمات الدقيقة للمشترك (SMI) من Cisco. في عملية نشر قائمة على Kubernetes لأسماء مراكز البيانات،

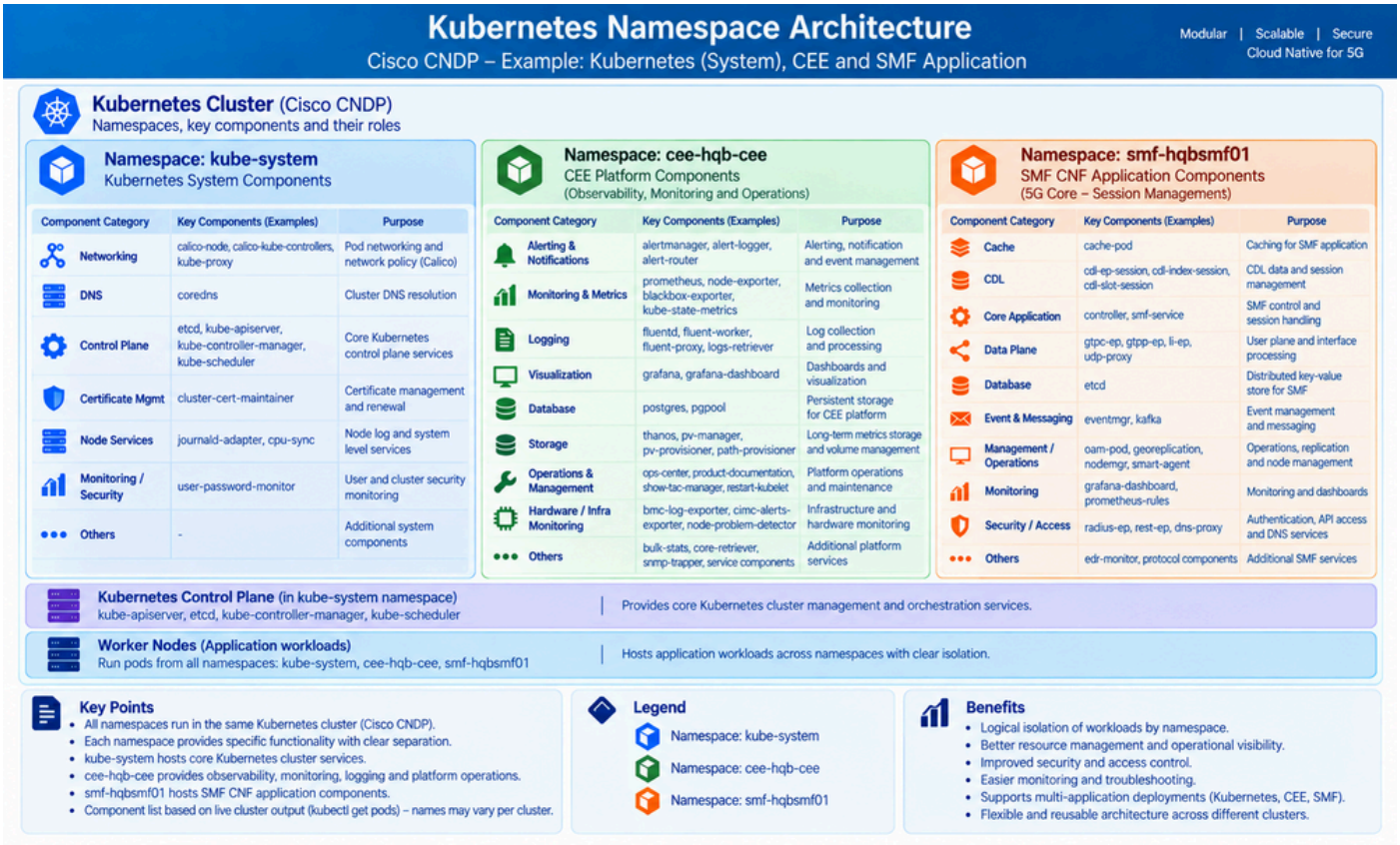
تشمل Kubernetes خدمات منفصلة للنظام الأساسي وإمكانية الملاحظة عبر شبكة إيثرنت المحسنة المجمعة وخدمات إدارة Kubernetes وأحمال عمل تطبيقات الشركات صغيرة ومتوسطة الحجم. يوفر الفصل حدود إدارية وتشغيلية بينما تسمح شبكات Kubernetes واكتشاف الخدمات باتصال المكونات المسموح به.

ويغطي هذا المستند بنية مساحة الاسم وحمولات عمل تقنية شبكة إيثرنت المحسنة المجمعة (CEE) وتثبيت شبكة إيثرنت المحسنة المجمعة (CEE) وإدارة دورة الحياة ومركز عمليات شبكة إيثرنت المحسنة المجمعة (CEE) والتنبيهات وبروتوكول إدارة الشبكة البسيط (SNMP) وتنبيهات وحدة التحكم في الإدارة المتكاملة (CIMC) من Cisco وإعادة توجيه السجل والإحصاءات المجمعة وبوابة نظام OpenTeleEmetry.

Splunk HEC على الإرسال تحكم بروتوكول (TCP) ميناء 8088 و syslog عبر المستعمل مخطط بيانات بروتوكول (UDP) ميناء 5140 هي آليات إستيعاب مستقلة. يحتوي المساران على متطلبات مختلفة للتكوين والنقل واستكشاف الأخطاء وإصلاحها ويمكن أن يتعايشا معا.

نظرة عامة على البنية

يشغل مركز تقنية شبكة إيثرنت المحسنة المجمعة (CEE) ووظائف التطبيق المرتبطة به مساحات أسماء منفصلة من Kubernetes. تعمل البنية على التمييز بين خدمات النظام الأساسي ل Kubernetes ووظائف المراقبة والإدارة الخاصة ب CEE ومن مجال تطبيق SMF.



بنية مساحة اسم Cisco SMI التي تظهر الفصل بين تقنية شبكة إيثرنت المحسنة المجمعة (CEE) والنظام الأساسي

مساحة اسم تقنية شبكة إيثرنت المحسنة المجمعة (CEE) هي التركيز الرئيسي لبنية مستوى الخدمة. توفر مساحات الأسماء الأخرى منصة Kubernetes ووظائف الشبكة وأحمال عمل SMF.

حمولات عمل مساحة اسم تقنية شبكة إيثرنت المحسنة المجمعة (CEE)

وتستضيف مساحة اسم تقنية شبكة إيثرنت المحسنة المجمعة (CEE) خدمات صغيرة للمراقبة والتنبيه والتسجيل ولوحات المعلومات والإحصاءات والوصول التشغيلي.

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.

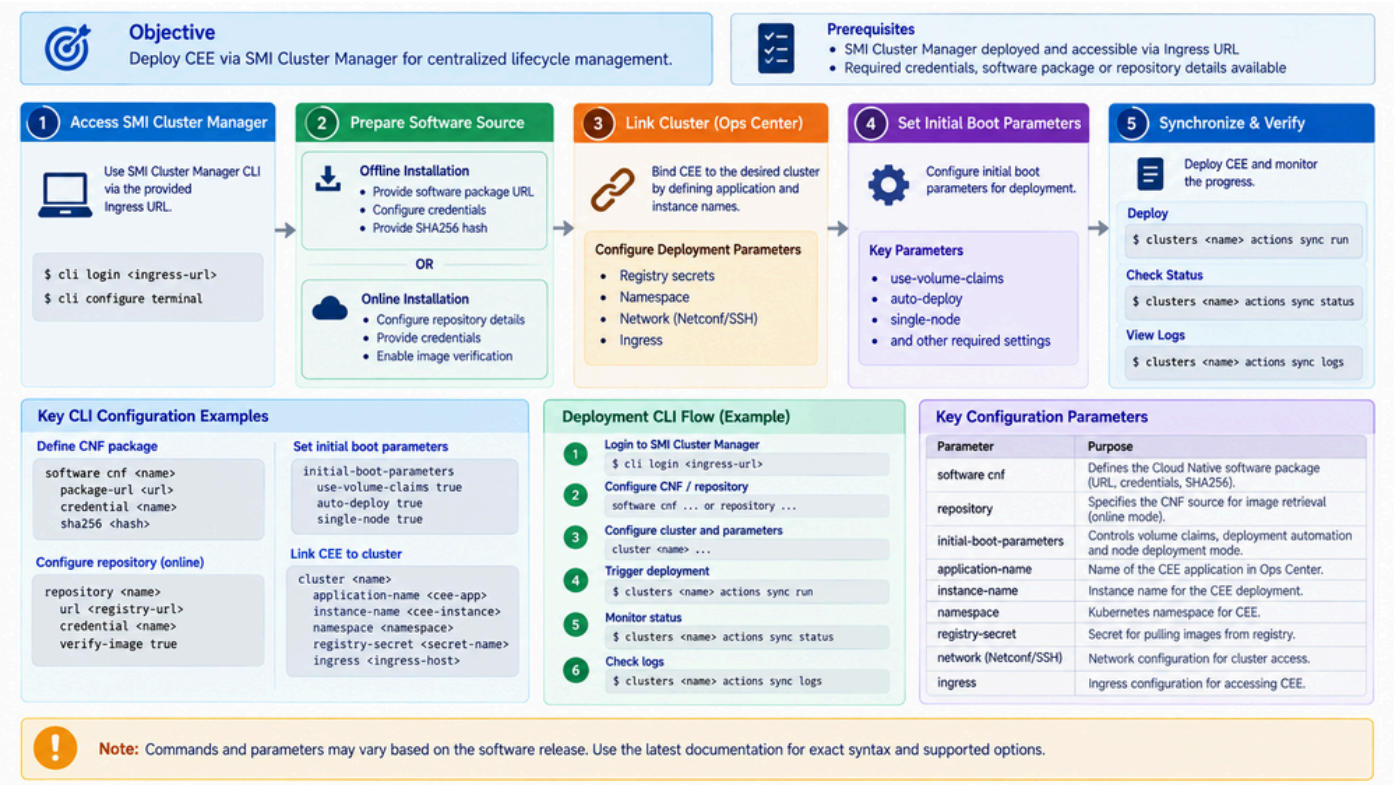
loki	Provides support to visualize the logs that are provided by the locally installed fluentBit pods.
logs-retriever	Assists in retrieving Kernel, Kubelet, and Container level logs through output to the JournalD driver.
logs-forwarder	Support pods logs forwarding to external server through Fluent-bit.
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.

الخدمات الدقيقة لمساحة الاسم الخاصة ب CEE ووظائف أحمال العمل التشغيلية الخاصة بها

وتتضمن هذه الوظائف مجموعة مقاييس بروميثيوس، وعرض مرئيات غرافانا، والتعامل مع تنبيه AlertManager، وخدمات إعادة توجيه السجلات، وإنشاء إحصائيات مجمعة دورية. تختلف أحمال العمل الفردية باختلاف تهيئة الإصدار والنشر.

تثبيت شبكة إيثرنت المحسنة المجمعة (CEE) وإدارة دورة الحياة

يفصل "مدير قطاعات SMI" تعريف منتجات البرامج عن المجموعة الهدف وتكوين مركز عمليات التشغيل الخاص بها. وهذا يتيح إمكانية إصدار البرامج المتحكم بها ومزامنة نظام المجموعة القابلة للتكرار.



تركيب SMI Cluster Manager وبنية تزامن البرامج

أوضاع التثبيت

- يمكن أن يشير التثبيت دون اتصال إلى حزمة برامج محلية من خلال عنوان URL للملف وخوارزمية التجزئة الآمنة 256 بت (SHA-256).
- يقوم تكوين المجموعة بإقران عملية نشر CEE/SMF بنظام المجموعة المخصصة ومثيل مركز عمليات التشغيل.

تحديد منتج برنامج CEE

في تكوين "مدير مجموعة SMI"، حدد حزمة برامج CEE المحلية ومهايئ SHA-256 الخاص بها.

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

أستخدم القيمة SHA-256 الدقيقة من الحزمة المعتمدة. العنصر النائب في الأمر مقصود
.والي يمثل المجموع الاختباري الفعلي

تكوين مركز نظام المجموعة و OPS

يقوم تكوين المصدر بإقران مجموعة مع مركز عمليات SMF، ومستودع محلي، ونقاط نهاية
.إدارة، وإعدادات نشر. يتم إستبدال المعرفات الخاصة بالموقع بالمواضع المؤقتة

```
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
```

باراماتر	يعني في مثال تشكيل
SMF <smf-ops-center-name>	إقران المجموعة بمثيل مركز عمليات SMF.
المستودع المحلي	تحديد مستودع التطبيق وإصداره للنشر.
المستودع - المزامنة الافتراضي صحيح	يستخدم المستودع الافتراضي الذي تم تكوينه أثناء المزامنة.
netconf-port 2029	تحديد منفذ اتصال إدارة NETCONF.
ssh-port 2028	تحديد منفذ اتصال إدارة طبقة الأمان (SSH).
عدد مرات الاستخدام الفعلية	تمكين إستخدام مطالبات الحجم لتلبية متطلبات التخزين الثابتة.
نشر تلقائي خاطئ	تعطيل النشر التلقائي بحيث تبقى المزامنة والتحقق من الصحة تحت التحكم الصريح.
عقدة واحدة خاطئة	يحدد عملية نشر ليست في وضع العقدة المفردة.

ملاحظة: الحزمة ومعرفات المستودع هي أمثلة من تكوين المصدر. تأكيد توافق
.الإصدار وقيم نقاط النهاية قبل إستخدامها في نظام مجموعة مختلف

مزامنة النشر والتحقق منه

قم بتشغيل إجراء مزامنة نظام المجموعة بعد جاهزية تكوين البرنامج و Ops Center.

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

فحص حالة المزامنة والسجلات.

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

تأكد من اكتمال عملية المزامنة بنجاح ومن نشر وحدات التزويد بالطاقة (CEE) والخدمات المتوقعة.

⚠ تحذير: يمكن لمزامنة نظام المجموعة ونشر البرامج تغيير البيئة قيد التشغيل. تطبيق التغييرات وقفا لإجراءات الصيانة والنشر المعتمدة.

مركز عمليات شبكة إيثرنت المحسنة المجمعة (CEE) والإدارة التشغيلية

يوفر مركز عمليات شبكة إيثرنت المحسنة المجمعة (CEE) الواجهة التشغيلية لخدمات شبكة إيثرنت المحسنة المجمعة (CEE). يدعم حمل العمل إدارة المستخدم والمصادقة والتكوين وأوامر العرض لوظائف شبكة إيثرنت المحسنة المجمعة داخل نظام المجموعة. من خلال برطب مركز عمليات التشغيل بعملية النشر الهدف "SMI تاعاطق ريدم" يقوم بتكوين الإدارة.

ينتمي مركز OPS إلى مستوى الإدارة. ينتمي كل من Prometheus و AlertManager و Fluent Bit/Fluent Proxy و HEC و Syslog و OpenTeleEmetry إلى مسارين المرافقين والقياس عن بعد. إن الحفاظ على هذه المسؤوليات منفصلة يسهل عملية أستكشاف المشكلات وحلها.

بنية CEE القابلة للملاحظة

تتضمن إمكانية الملاحظة عبر شبكة إيثرنت المحسنة المجمعة (CEE) المقاييس والتنبيه والسجلات وتنبيهات CIMC والإحصاءات المجمعة. وهذه الخدمات مرتبطة ببعضها البعض، ولكن مسارات البيانات والمستهلكين مختلفون.

الوظيفة	الغرض الأساسي	الوجهة النموذجية أو المستهلك النموذجي
المقاييس	تجميع قياسات السلاسل الزمنية والاستعلام عنها من العقد	برومیثیوس، غرافانا، وثانوس.

الوظيفة	الغرض الأساسي	الوجهة النموذجية أو المستهلك النموذجي
	Kubernetes والخدمات.	
التنبيهات	تقييم قواعد التنبيه وأحداث التنبيه المسار.	مركز موجه التنبيه و AlertManager عمليات التشغيل وأجهزة الاستقبال الخارجية.
السجلات	إعادة توجيه سجلات السجل والحدث إلى أدوات التجميع وأو الأجهزة الخلفية الخارجية.	أداة تجميع السجلات (SPLUNK) وغيرها من أدوات تجميع السجلات.
تنبيهات CIMC	تصدير تنبيهات عنصر التحكم في Cisco من الإدارة المتكاملة للمراقبة.	Grafana و CEE تنبيهات/قياسات.
إحصائيات جرمية	إنشاء لقطات إحصائية دورية.	لقطات CSV ومعالجة أو تحليل البيانات في الخادم.

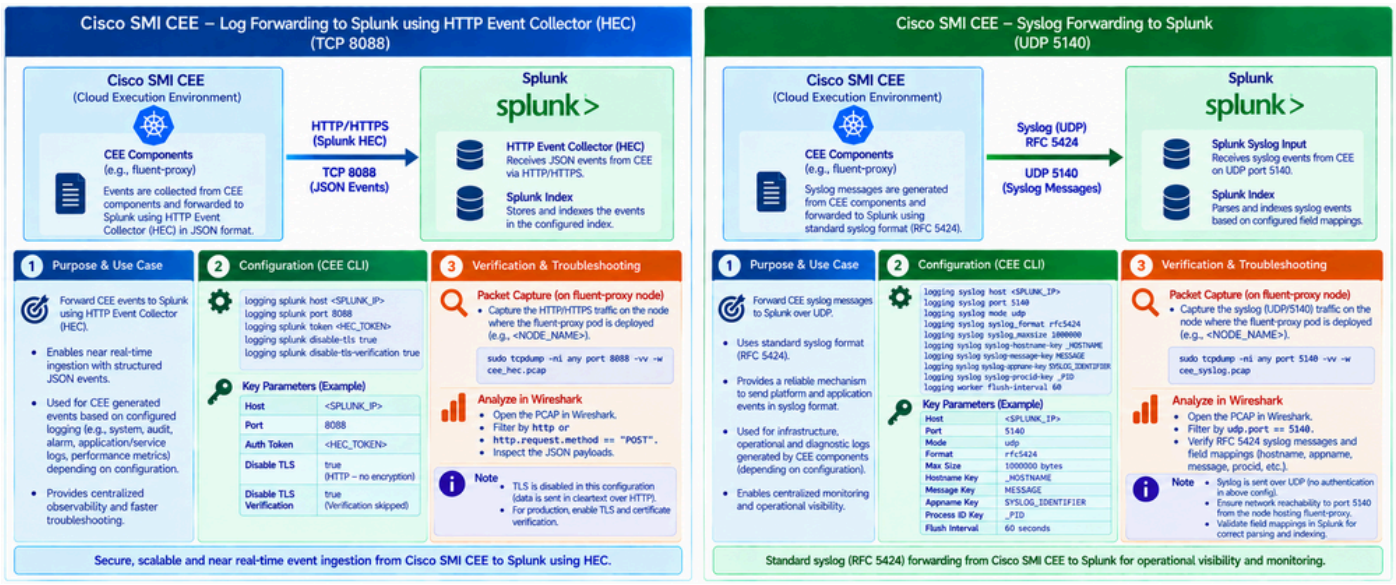
تكامل SPLUNK: بنية نقل السجل

يصف المصدر مسارين من CEE إلى Splunk. يمكن لكل الطرازين توصيل أحداث إلى SPLUNK، لكنهما يستخدمان بروتوكولات مميزة وواجهات اتصال.

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

تعتمد أنواع الأحداث التي يتم نقلها بواسطة كل مسار على تكوين تقنية شبكة إيثرنت المحسنة المجمعة (CEE) وتوصيل إعادة التوجيه الذي تم تنفيذه. لا تقوم واجهات تم تكوينهما على تحديد أن كل واحدة منها تحمل فئة أحداث حصرية بشكل متبادل.

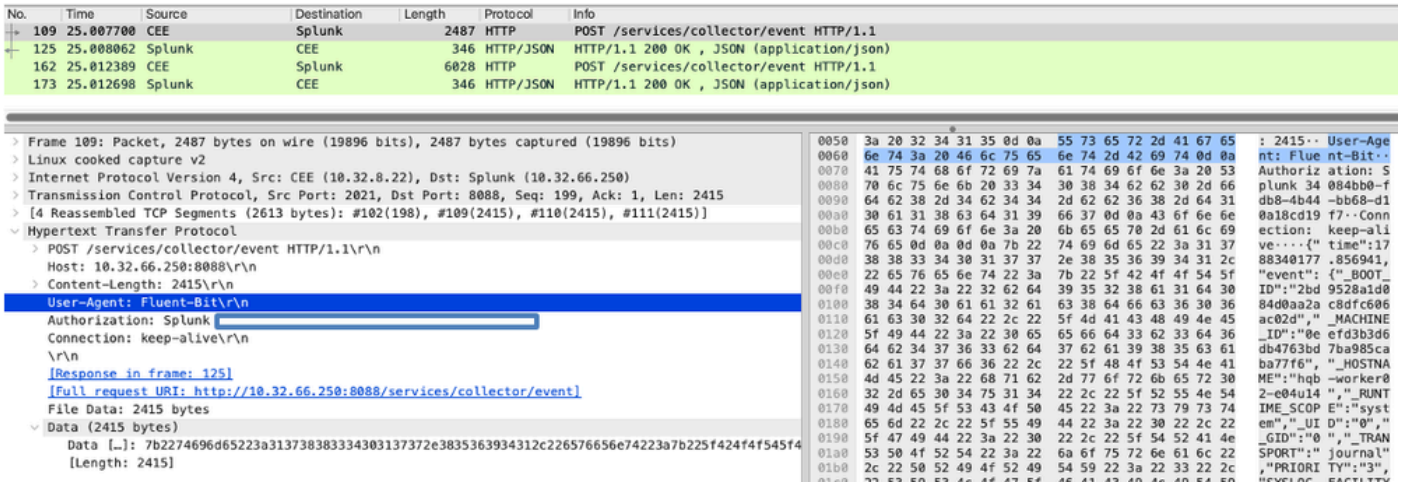
تتبع المسارات بشكل منفصل. تأكيد التسليم الناجح للجنة العليا للانتخابات HEC. تسليم syslog لـ syslog، وتأكيد التسليم الناجح



دمج شبكة إيثرنت المحسنة المجمعة (CEE) مع مسارات إعادة توجيه منفصلة خاصة بـ HEC و syslog

إعادة توجيه مجمع أحداث Splunk HTTP

تقبل Splunk CTP عمليات إرسال حدث HTTP وتستخدم رمز مصادقة خاص بـ HEC. يقوم مركز أوروبا الوسطى والشرقية بإعادة توجيه الأحداث مباشرة إلى خدمة اللجنة العليا للانتخابات التي تم تكوينها بدلاً من الحاجة إلى معالجة قائمة على الملفات لهذا المسار.



بنية إعادة توجيه مجمع أحداث HTTP الخاصة بـ CEE إلى Splunk على منفذ TCP 8088

نموذج تكوين HEC

يحتوي مثال المختبر الأصلي على هذه الإعدادات لنقطة نهاية انقسام CEE. يسجل المقتطف سلوك المصدر وهو ليس تكوين إنتاج موصى به.



تحذير: يعجز المثال المصدر كل من TLS والتحقق من الترخيص. ويكشف هذا عن بيانات تتبع الاستخدام ومسوغات اللجنة العليا للانتخابات للاعتراض على الشبكة. للإنتاج، قم بتمكين TLS والتحقق من الشهادة أو منت رمز مصادقة HEC المدعوم. إصدار CEE المميز وقفا لتكوين.

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

في بنية المصدر، يقوم منتجو سجلات/أحداث شبكة إيثرنت المحسنة المجمعة بتقديم عنصر إعادة التوجيه السريع ذي الصلة إلى وجهة اللجنة العليا للانتخابات.

```
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
```

التقاط حركة مرور HEC واستكشاف أخطائها وإصلاحها

تعرف على Pod الوكيل الذي يدعم تقنية Fluent وعقدة العامل Kubernetes الخاصة بها في مساحة اسم شبكة إيثرنت المحسنة المجمعة عندما يقوم الوكيل الذي يدعم تقنية Fluent بنقل بيانات اللجنة العليا للانتخابات.

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

على عقدة Kubernetes التي تحمل حركة مرور اللجنة العليا للانتخابات، قم بالاستيلاء على الحزم الخاصة بميناء CTO.

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

ال اتصال TLS مم كن، ي كشف ال تقاط حزمة عن تفاصيل إنشاء ال نفق وال ولوجة ول كن ه
ي عرض عادة حمولة HTTP. إذا تم تعطيل TLS، ي مكن أن تكون محتويات الحدث ومواد المصادقة
مرئية في ال ال تقاط.

⚠
تحذير: ي مكن أن تحتوي عمليات ال تقاط الحزم وال سجلات على بيانات اعتماد وقيا س
بيانات اعتماد حساسة عن بعد. تقييد الت جميع وال نقل إلى عمليات سير عمل الدعم
ال معتمدة وحماية ملفات ال ال تقاط.

إعادة توجيه Syslog عبر UDP 5140

ي رسل م سار تكامل Splunk ال ثاني سجلات syslog باستخدام تنسيق RFC 5424 ومنفذ UDP
5140. كما يحدد تكوين المصدر تعييينات الحقول والحد الأقصى لحجم الرسالة والفترة
الزمنية لتدفق العامل.

```
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
```

تعيين الحقل وفقا لمعيار RFC 5424

حقل مصدر CEE	حقل Syslog أو الغرض
_اسم المضيف	تعريف المضيف الأصلي في سجل syslog الذي تم إنشاؤه.
الرسالة	حمل نص رسالة السجل.
syslog_identifier	يوفر تطبيق syslog أو معرف البرنامج.
_PID	حمل معرف العملية الأصلي.

نقل UDP والتقاط الحزم

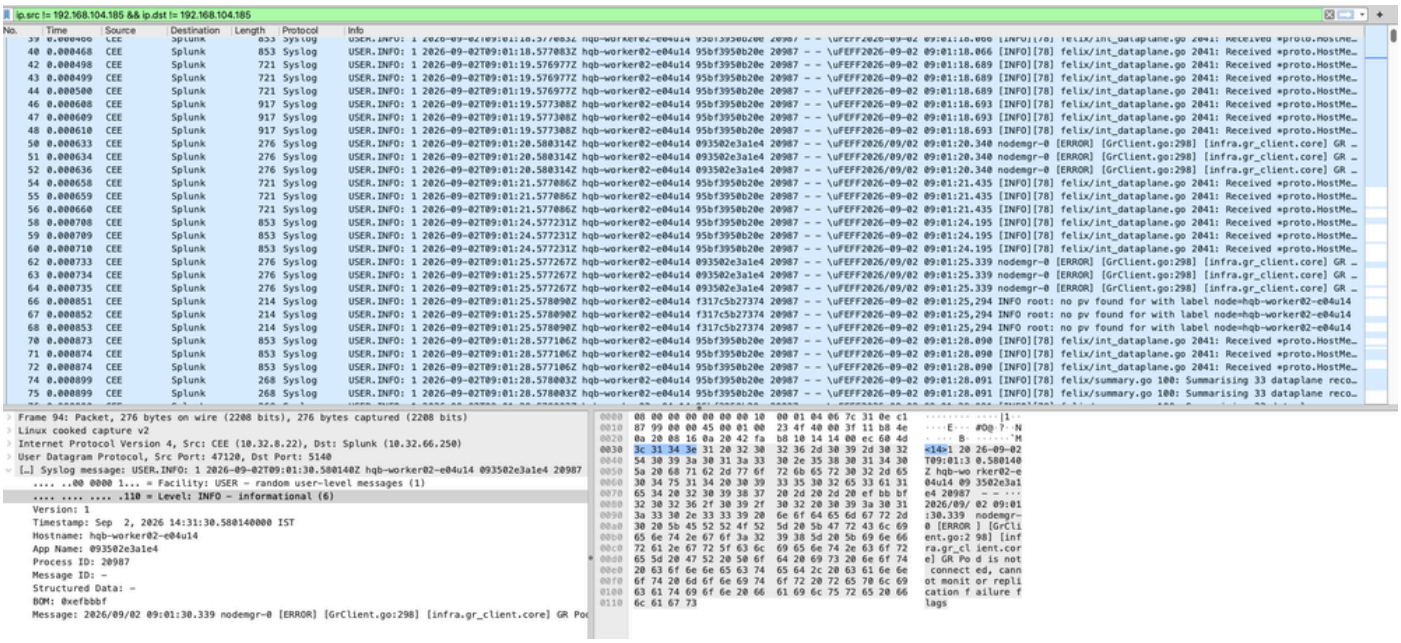
UDP غير متصل والي قدم إقرار تسليم النقل أو إعادة الإرسال. يجب أن يغطي أستكشاف
الأخطاء وإصلاحها فقدان الحزم والتوجيه ووحدة الإرسال القصوى (MTU) والتجزئة وتوفر جهاز
الاستقبال وسلوك قائمة الانتظار/المعدل.

على القرص أو Kubernetes عقدة أن يحمل ال syslog حركة مرور، يركض:

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

إذا قام وكيل تدفق البيانات بإعادة توجيه حركة مرور syslog، فإن العقدة المضيفة لهذا المكون هي نقطة التقاط حزمة مناسبة. تحقق من مسار إعادة التوجيه قبل تجميع الحزم.

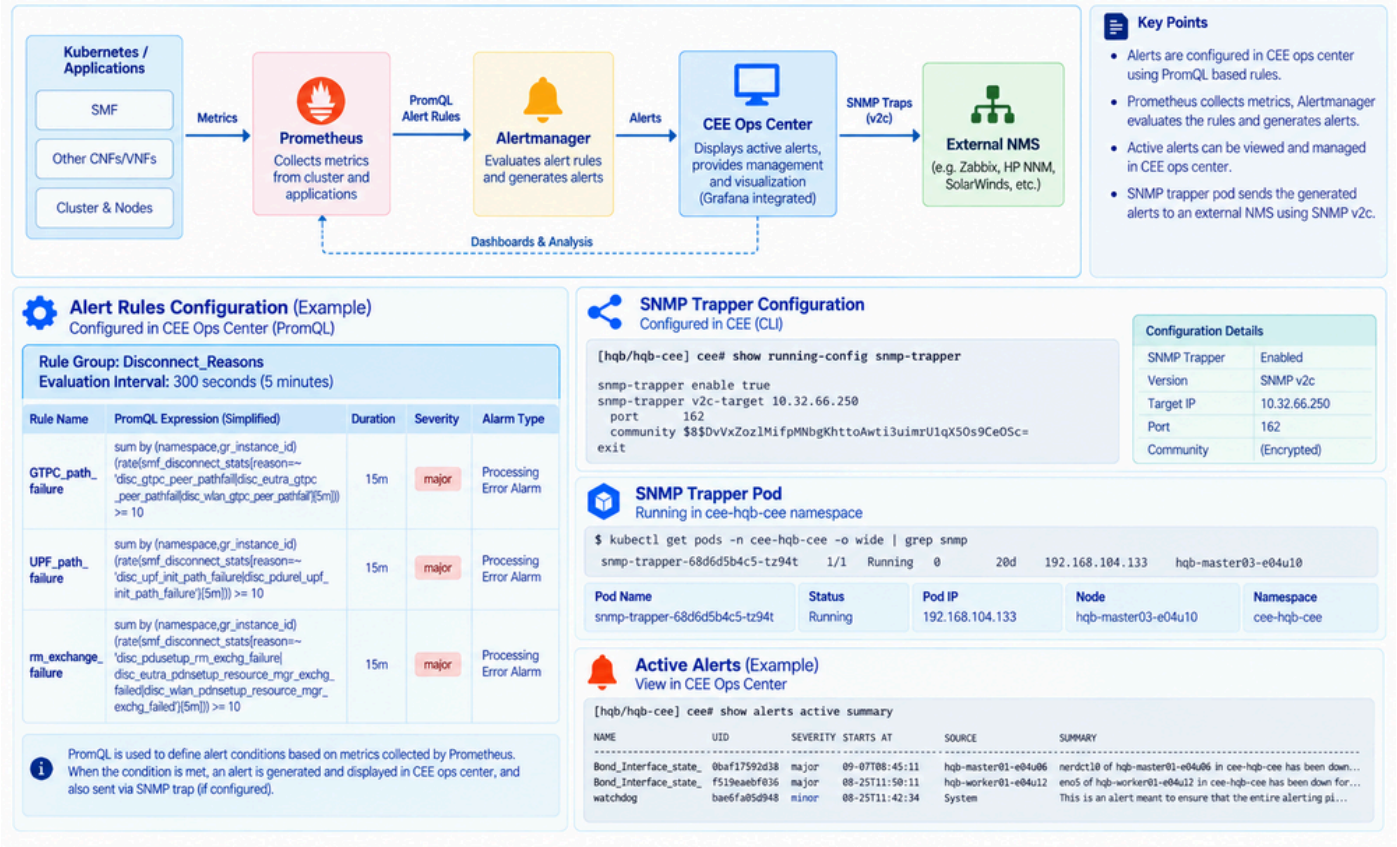
ملاحظة: يحدد RFC 5424 تنسيق رسالة syslog بشكل مستقل عن النقل المحدد. يستخدم سيناريو المصدر UDP 5140. يعد نقل syslog المستند إلى TLS خيارا مختلفا يتطلب تكوين المرسل والمستلم المتوافق.



إعادة توجيه بروتوكول Syslog من CEE إلى Splunk باستخدام حقلي UDP Port 5140 و RFC 5424

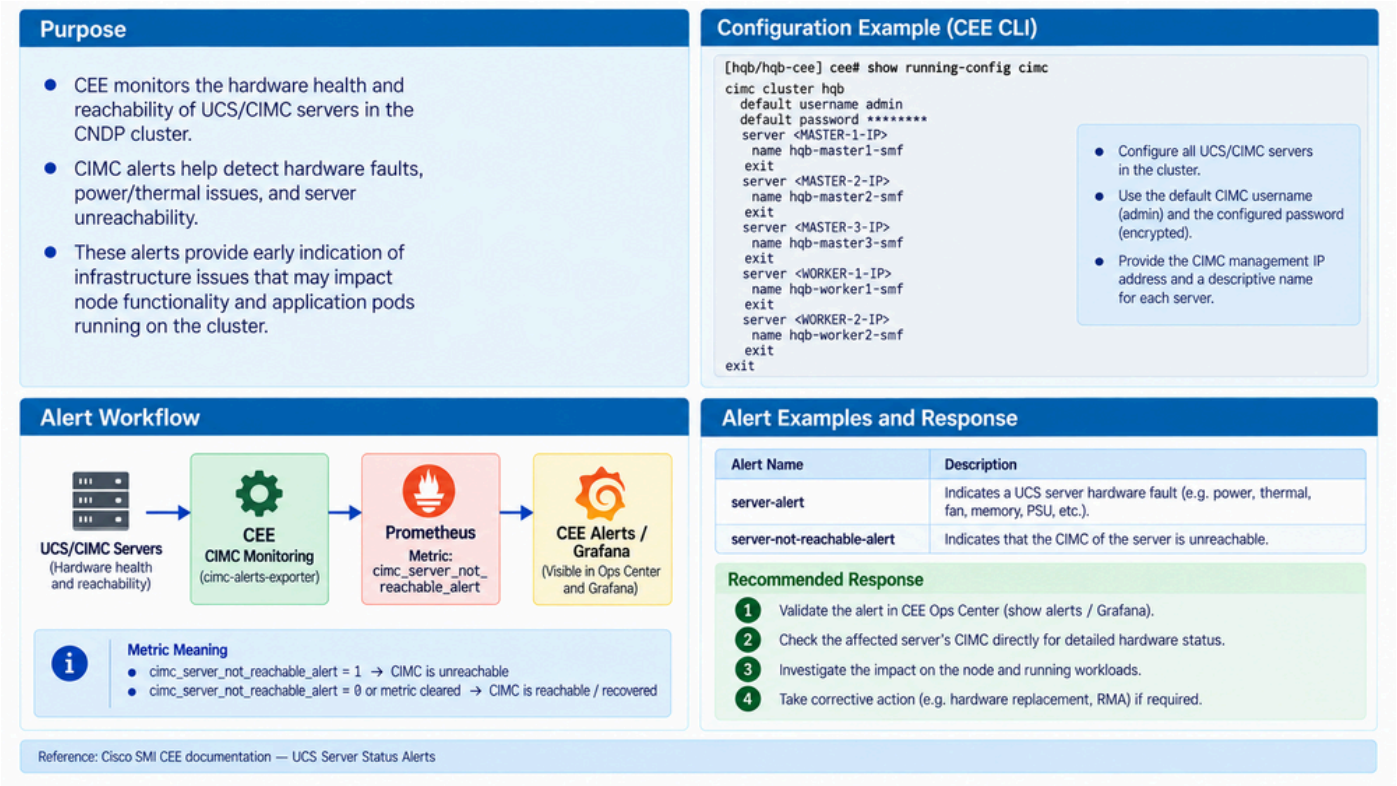
التنبيهات و SNMP و CIMC وإمكانية الملاحظة

دعم قواعد وسياسات AlertManager. يقيم بروميثيوس و AlertManager يستخدم تنبيه CEE بروميثيوس، مع توفير موجه التنبيه. يقوم AlertManager بتوجيه أحداث التنبيه إلى أجهزة الاستقبال، سجلات تنبيه تاريخية التنبيه لدعم توجيه إضافي. يوفر مسجل التنبيه لـ CEE للاسترداد من خلال مركز عمليات CEE.



إعادة توجيه تنبيه CEE Prometheus و AlertManager وبنية SNMP

يوفر دمج تنبيه CIMC مسار مراقبة للبنية الأساسية ذي صلة. ويقوم مصدر تنبيهات CIMC بجمع معلومات التنبيه الخاصة بلجنة إدارة الاتصالات البحرية الدولية وتعرضها للرصد والتصوير المرئي في غرافانا.

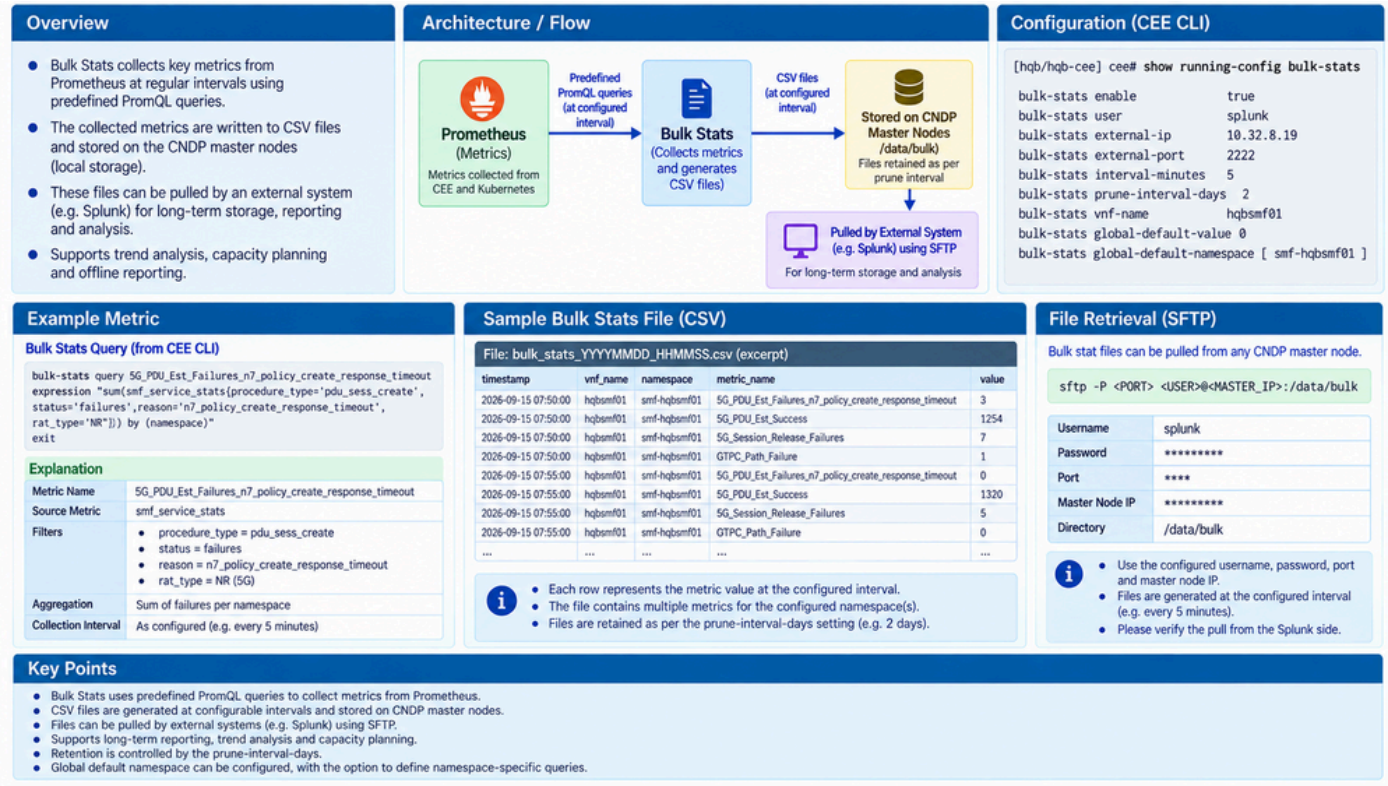


تكامل SNMP وهو واجهة إدارة وتنبيه؛ ولا يمكن إستبدالها بإعادة توجيه Splunk HEC أو syslog. ويظل البروتوكول ومسارات تسليم الأحداث متميزين.

تتضمن مراجع قاعدة معلومات الإدارة ذات الصلة Cisco-CNEE-MIB.my وCisco-SMI.my.

إحصائيات جرمية

تقوم خدمة الحالات المجمعة ل CEE بإنشاء لقطات دورية للقيم المنفصلة عن فاصلة (CSV) للإحصائيات التي تم تجميعها من خلال Prometheus. وهي لقطات إحصائية بدلا من عمليات دفق لسجلات سجل التطبيقات.



خدمة إحصائيات حجم تقنية شبكة إيثرنت المحسنة المجمعة (CEE) التي تقوم بإنشاء لقطات CSV دورية من مقاييس Prometheus

يدعم إخراج الإحصاءات المجمعة التقارير الدورية، وتحليل الاتجاهات، ومعالجة البيانات اللاحقة. قم بتضمينه في مسار تكامل Splunk فقط عندما يقوم النشر بإعادة توجيه بيانات CSV/statistics إلى Splunk بشكل صريح أو إستيرادها.

بوابة نظام OpenTelemetry

تدعم إصدارات Cisco SMI الأحدث بوابة مجمع بيانات OpenTeleRate المدارة عبر النظام الأساسي. تتلقى البوابة بيانات تتبع الاستخدام من التطبيقات من خلال بروتوكول OpenTeleEmetry (OTLP) وإعادة توجيه المقاييس والسجلات المدعومة إلى الإصدارات الخلفية المحلية أو البعيدة.

ملاحظة: تحدد وثائق عمليات مدير مجموعة Cisco SMI الكامل عبارة OpenTeleEmetry مع الإصدار 2026.03.1. لم يتم التحقق من صحة البوابة في النشر المحدد الموضح بواسطة المثال المصدر، لذلك يصف هذا القسم نموذج التكوين المنشور بدلا من العملية التي تم التحقق منها في تلك البيئة.

نموذج بوابة النظام

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

مفاهيم تكوين البوابة

قم بتمكين بوابة مجمع OpenTeleEmetry وحدد المقاييس المحلية والنهايات الخلفية للتسجيل.

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

حيث يتطلب النشر تعرض الخدمة الخارجية، يمكن أن يتضمن التكوين عنوان IP خارجي.

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

.يتم تكوين إعدادات الوكيل الاختيارية لمصدري البوابة

```
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
```

تتحكم خيارات الخلفية المحلية في كيفية إرسال بوابة النظام المدارة من قبل النظام الأساسي بيانات تتبع إلى المحولات الخلفية المدمجة. يعتمد التعرض لبروتوكول (IP) الإنترنت الخارجي وإعدادات الوكيل على متطلبات المخطط والأمان.

المصدرون عن بعد

مصدر	الإشارة	إستخدام فني
أوتل	السجلات، المقاييس	قم بإرسال بيانات تتبع إلى جهة خلفية تقبل OTLP عبر gRPC.
otlphttp	السجلات، المقاييس	قم بإرسال تتبع بيانات إلى نهاية خلفية تقبل OTLP عبر HTTP.
سبونكيتو	السجلات	إرسال السجلات إلى نقطة نهاية Splunk HEC.
صحفي	السجلات	كتابة السجلات إلى دفتر يومية العقد حيث يتم دعمها.
تصحيح الأخطاء	السجلات، المقاييس	دعم التحقق من الصحة واستكشاف الأخطاء وإصلاحها الذي يتم التحكم به.

يتبع سير عمل OpenTeleEmetry نموذج الاستلام والمعالجة والتصدير. أجهزة إستقبال المصدرون؛ يقوم المعالجات بتصفية البيانات أو تحويلها؛ يقوم التتبع الاحتكاك؛ بتسليم الإشارات المحددة إلى طرفيات خلفية بعيدة أو محلية.

يدعم، في حين يميز المصدر أيضا سلوك الوكيل: يستخدم OTLP إعدادات وكيل مثيل مجمع وsplunkhec عمليات إستبدال وكيل على مستوى المصدر حيث يعرض الإصدار OTLPHTTP المنشور هذا التكوين.

قارن مع OpenShift OpenTelemetry

أن OpenTeleEmetry يمكن لمجمع: مشترك بنية مطمن OpenShift و Cisco CEE يكون لكل من المحولات الخلفية التي يمكن ملاحظتها. يقع بين التطبيقات المزودة بمعدات وبين المحولات الخلفية التي يمكن ملاحظتها. وتختلف نماذج الإدارة والتركيب الخاصة بها.

مفهوم	CEE ل OpenTelemetry مظان ةبوابة	مطمن OpenShift OpenTelemetry
مصدر بيانات تتبع الاستخدام	CEE ب حومالات العمل الخاصة OpenTelemetry ل ةنمكمل تاقيبطتلاو	ةنمكمل OpenShift لمحامل عم OpenTeleEmetry ب
البروتوكول	OTLP	OTLP
دور مجمع	مظان النظام المدارة عبر بوابة	عمجم ليثم وأ رشن

مفهوم	CEE ل OpenTelemetry مظان ةبواب	نمط OpenShift OpenTelemetry
	الأساسي	OpenTeleEmetry
مفهوم خط الأنابيب	ريدصتو ةجلاعمو مالتسإ	إستلام ومعالجة وتصدير
مرونة النسخ الاحتياطي	دعب نع نيردصملاو ةيلحملا تاظهيرا نيعوملدا	دنتسملا يف لخلدا لماكتلا ىلإ ردصملا
رطشلا لماكتلا	اب ورو أ ل دو ةقثوملا ةيقرشلاو ىطسولا ردصملا يف تشكيلة ةيحولا ردصملا	تم ثيح ردصملا Splunk HEC نيوكت

هذه المقارنة مع مايكروسوفت Azure Monitor توضح أن النظامين الأساسيين ينفذان OpenTeleEmetry بشكل مماثل. يستخدم OpenShift بشكل عام عامل تشغيل/نموذج نشر مجمع بيانات OpenTele، بينما تتم إدارة وكلاء النظام الأساسي بواسطة Cisco SMI.

تظهر بنية مرجع OpenShift التي تمت مناقشتها في المصدر أدوات التجميع التي تقوم بإعادة توجيه بيانات تتبع الاستخدام من أحمال عمل Kubernetes نحو Splunk عبر CTLoS. وهو يوضح النموذج المستند إلى المجمع بدلا من الدمج الذي تم التحقق منه لتثبيت نموذج CEE.

التحقق من التكوين

التحقق من مزامنة CEE

تأكد من نشر أحمال عمل "شبكة إيثرنت" و"تسجيلاته" و"مدير مجموعة SMI" بحالة مزامنة "راجع المحسنة المجمعة" المتوقعة.

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

التحقق من اللجنة العليا للانتخابات و syslog بشكل منفصل

تأكد من أن مسار CTCP يرسل الأحداث إلى نقطة نهاية TCP 8088 التي تم تكوينها وأن مسار syslog يرسل سجلات UDP 5140 إلى عزوم. تأكد بشكل منفصل من أن Splunk يستلمها.

أستخدم أسلوب التقاط الحزمة في الأقسام المقابلة وربط الطوابع الزمنية للحزمة بالأحداث المستلمة في مجمع البيانات الذي تم تكوينه.

التحقق من خدمات إمكانية الملاحظة

لعمل تأكد من أن القياسات وتوجيه التنبيه وتنبيهات CIMC ولقطات الإحصائيات المجمعة تعمل كما هي مصممة للإصدار الذي تم تثبيته. إذا تم تمكين OpenTeleEmetry، فتحقق من صحة مجموعة SMI جاهز الاستقبال وخطوط الأنابيب والمصدر باستخدام إجراء عمليات إدارة المجموعة.

السلوك المتوقع

المكون أو المسار	النتيجة المتوقعة
مدير نظام مجموعة SMI	يتم إكمال مزامنة نظام المجموعة ويتم نشر خدمات CEE المطلوبة.
مركز العمليات	يستطيع المستخدمون المعتمدون الوصول إلى وظائف التشغيل وأوامر التكوين/المراقبة المدعومة.
سبونك	تصل حركة مرور الأحداث إلى وحدة إصغاء CTCP التي تم تكوينها على منفذ TCP 8088.
Syslog	تصل الأحداث المنسقة وفقا لمعيار RFC 5424 إلى وحدة إصغاء منفذ UDP 5140 التي تم تكوينها.
التنبيهات و CIMC	يعرض AlertManager والمصدرين ذوي الصلة معلومات التنبيه التي تم تكوينها.
إحصائيات جرمية	يتم إنشاء لقطات CSV دورية من الإحصائيات المجمعة.
OpenTelemetry	في الإصدارات المدعومة مع البوابة التي تم تكوينها، تتدفق إشارات OTLP من خلال خط أنابيب الخلفية/المصدر المحدد.

تدفق القرار

رصد	الشيك التالي
خدمات CEE غير موجودة بعد المزامنة.	فحص حالة مزامنة "مدير نظام المجموعة" والسجلات وفتحات البرامج ومعلمات مركز العمليات.
أحداث Syslog مفقودة.	تحقق من وجود UDP 5140، وتنسيق RFC 5424، وتدفق الحزم، وسلوك جاهز الاستقبال.
تنبيهات أو بيانات CIMC مفقودة.	تحقق من توجيه Prometheus/AlertManager وموجه التنبيه وعملية مصدر تنبيهات CIMC.
الإحصاءات المجمعة مفقودة.	تأكيد عملية خدمة الحالات المجمعة وتوفر بيانات CSV وإنشاء لقطة Prometheus.
تصدير OpenTeleEmetry مفقود.	تحقق من دعم الميزات للإصدار الذي تم تثبيته وتكوين البوابة والمتلقي والدولة المصدر وعضوية خط الأنابيب.

القرار

تقنية شبكة إيثرنت المحسنة المجمعة (CEE) هي بيئة تنفيذ ومالحظة قائمة على

طبقات من Kubernetes ترتكز على تطبيقات الشركات صغيرة ومتوسطة الحجم (SMF). يقسم فصل مساحة اسم Kubernetes عمليات النظام الأساسي وخدمات شبكة إيثرنت المحسنة المجمعة وحمولات عمل التطبيقات إلى مجالات مختلفة. في شبكة إيثرنت المحسنة المجمعة، تعد عمليات المراقبة والتنبيه والتسجيل والإحصاءات المجمعة خدمات متخصصة ذات مسؤوليات مستقلة.

الفرق الأساسي بين اللجنة العليا للانتخابات على TCP 8088 و syslog عبر UDP 5140. وهذه هي مسارات إعادة توجيه منفصلة تشتمل على بروتوكولات وتكوينات وإجراءات أستكشاف الأخطاء وإصلاحها مختلفة. تضيف بوابة نظام OpenTeleEmetry الأحدث نموذج مجمع ومصدر يستند إلى OTLP. تعد التشابه بينها وبين OpenShift OpenTelemetry معمارية، ويجب التحقق من تشغيل البوابة لإصدار CEE المحدد ونشره.

المحتوى ذي الصلة

- [دليل تكوين وادارة تقنية شبكة إيثرنت المحسنة المجمعة من Cisco - بيئة التنفيذ المشتركة]
- [دليل تكوين وادارة تقنية شبكة إيثرنت المحسنة المجمعة من Cisco - أوامر التسجيل]
- [عمليات مدير مجموعة SMI من Cisco - المزامنة وقياس OpenTele]
- [بروتوكول Syslog - المعيار RFC 5424]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).