

# Überprüfen der Integrität eines sicheren Workload-Clusters (Tetration)

## Inhalt

---

[Einleitung](#)

[Hintergrundinformationen](#)

[Wann die Integrität des Clusters überprüft werden soll](#)

[Verschiedene Optionen, die Sie zur Überprüfung der Integrität des sicheren Workload-Clusters benötigen](#)

[Cluster-Status](#)

[Servicestatus](#)

[Hawkeye \(Diagramme\)](#)

[Upgrade-Prechecks](#)

---

## Einleitung

In diesem Dokument werden die Schritte zur Überprüfung der Integrität eines sicheren Workload-Clusters beschrieben und die wichtigsten Aspekte herausgestellt, die während der Integritätsprüfung überprüft werden müssen.

## Hintergrundinformationen

Ihr Schwerpunkt liegt in erster Linie auf der Gesundheitskontrolle; Wenn Sie jedoch Probleme oder ungewöhnliches Verhalten feststellen, müssen Sie einen Snapshot erstellen und sich an das Cisco Tetration Solution Support TAC-Team wenden. Das Cluster für sichere Workloads besteht aus Hunderten von Prozessen, die auf mehrere virtuelle Systeme auf mehreren UCS C220-Servern verteilt sind.

Die beiden wichtigsten Tools zur Bewertung der Cluster-Integrität sind die Seiten "Cluster-Status" und "Service-Status", die beide in diesem Dokument erläutert werden. Die Verwendung dieser Seiten ist im Allgemeinen die effektivste Möglichkeit, den allgemeinen Zustand des Clusters zu bestätigen.

## Wann die Integrität des Clusters überprüft werden soll

In den meisten Fällen ist es nicht erforderlich, die Integrität Ihres Clusters zu überprüfen. Es gibt jedoch Situationen, in denen es eine gute Idee ist:

- Wenn Sie etwas Ungewöhnliches oder Unerwartetes in der Benutzeroberfläche (UI) bemerken, basierend auf Ihrer Erfahrung mit der Art und Weise, wie Dinge normalerweise funktionieren. Im Abschnitt Betriebliche Anzeigeparameter finden Sie einige gängige Beispiele.

- Wenn Sie erwarten, dass bestimmte Daten (wie Flow-Daten von Software- oder Hardware-Sensoren) in der Benutzeroberfläche zu sehen, aber es fehlt, obwohl Sie den richtigen Umfang und Zeitraum gewählt haben.
- Vor und nach geplanten Wartungsarbeiten, Upgrades oder größeren Änderungen am Cluster. Es empfiehlt sich, vor und nach diesen Aktivitäten eine Momentaufnahme des Cluster-Zustands zu erstellen. Wenn Sie jemals den TAC-Support kontaktieren müssen, können diese Snapshots helfen, die Änderungen schnell zu identifizieren.

## Verschiedene Optionen, die Sie zur Überprüfung der Integrität des sicheren Workload-Clusters benötigen

### Cluster-Status

Ein Cluster für sichere Workloads besteht je nach Cluster-Typ entweder aus 6 Servern (8 HE) oder 36 Servern (39 HE). Auf der Seite "Cluster Status" (Cluster-Status) werden der Status der Server sowie Informationen zum Bare-Metal-Server angezeigt.



Anmerkung: Benutzer mit Standortadministrator- oder Kundensupportrollen für physische Cluster können auf die Seite "Cluster-Status" zugreifen. Beide Rollen können Aktionen auf der Seite "Cluster Status" (Cluster-Status) anzeigen und ausführen.

Wählen Sie im Navigationsfenster Troubleshoot > Cluster Status aus.

Der Cluster-Status zeigt den Status aller Server im Cisco Secure Workload-Rack an. Ein funktionierender Server kann den Status "Kommissioniert" und "Aktiv" anzeigen, wie hier dargestellt.

**Cluster Status**

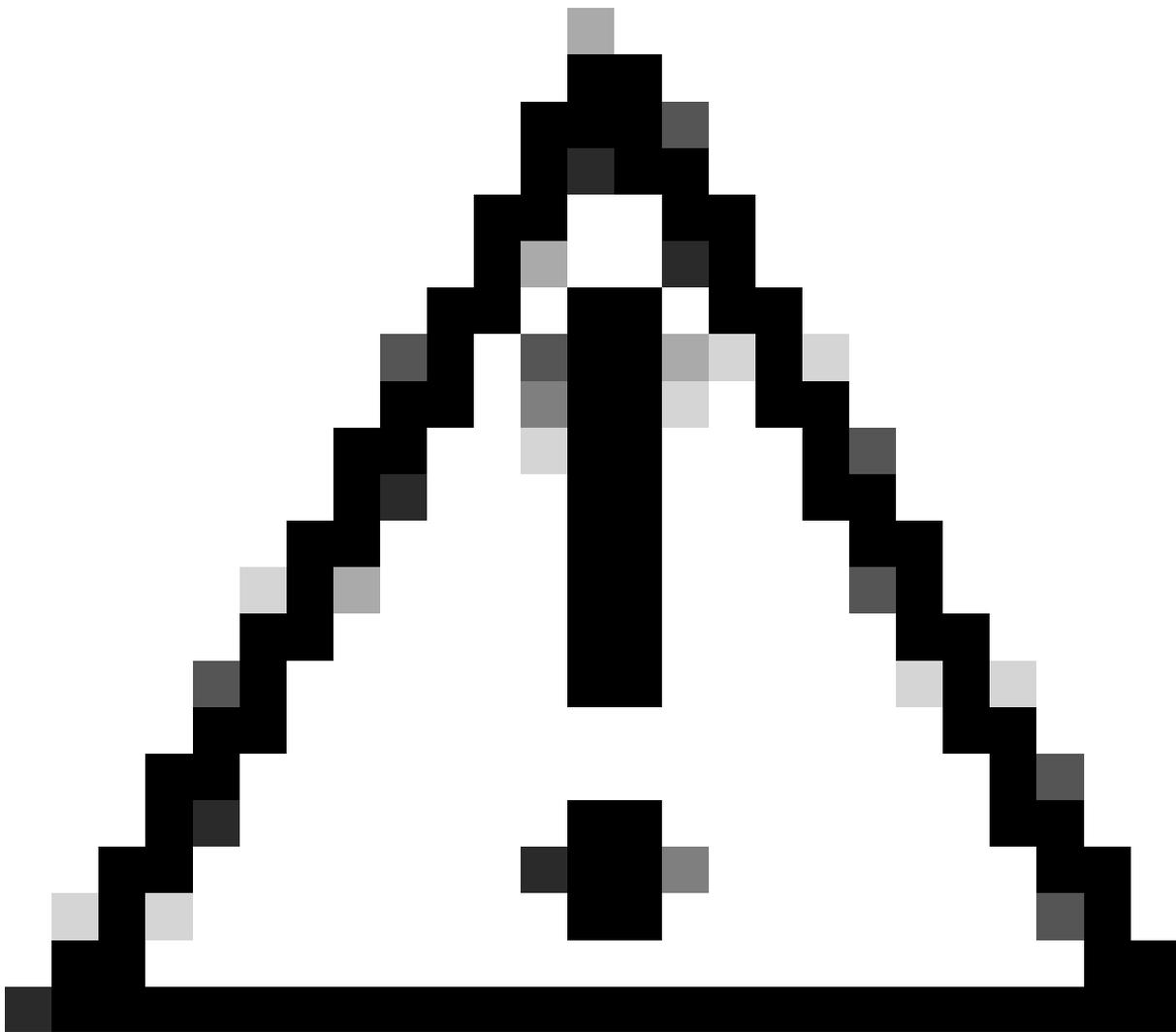
Model: 8RU-M6

CIMC/TOR guest password External Access  Disabled Orchestrator State: IDLE

Displaying 6 nodes (0 selected)

Select action v Apply ↻

State	Status	Switch Port	Serial	Uptime	CIMC Snapshots
Commissioned	Active	Ethernet1/3	WMP272900CQ	1y 7mo 7d 18h 35m 46s	+ ↕
Commissioned	Active	Ethernet1/6	WMP272900EB	10mo 25d 23h 32m 27s	+ ↕
Commissioned	Active	Ethernet1/2	WMP272900E2	10mo 25d 4h 12m 10s	+ ↕
Commissioned	Active	Ethernet1/4	WMP272900DZ	3mo 19d 6h 51s	+ ↕
Commissioned	Active	Ethernet1/1	WMP272900EE	29d 6h 34m 13s	+ ↕
Commissioned	Active	Ethernet1/5	WMP272900CH	27d 23h 5m 53s	+ ↕



Vorsicht: Wenn Sie auf der Cluster-Statusseite einen Knoten feststellen, der als inaktiv markiert ist, erstellen Sie einen CIMC-Snapshot, und erstellen Sie ein TAC-Ticket, einschließlich des Snapshots.

Wenn der Status als Inaktiv angezeigt wird, bedeutet dies in der Regel, dass der Server entweder ausgeschaltet ist oder aufgrund eines Hardware-, Kabel- oder Verbindungsproblems ausfällt.

Wenn Sie auf einen Server in der Liste klicken, werden weitere Details angezeigt, z. B.

- Die virtuellen Systeme (Instanzen), die auf diesem physischen Server ausgeführt werden
- Die private IP-Adresse des Servers im Cluster
- CIMC-IP-Adresse (Management)
- Aktuelle Firmware-Versionen für BIOS, CIMC, VIC-Karte, LOM-Karte und RAID-Controller

**Cluster Status**

Model: 8RU-M6

CIMC/TOR guest password External Access Disabled Orchestrator State: IDLE

Displaying 6 nodes (0 selected)

State	Status	Switch Port	Serial	Uptime	CIMC Snapshots
Commissioned	Active	Ethernet1/3	WMP272900CQ	1y 7mo 7d 18h 49m 3s	+ ↕

**Serial: WMP272900CQ** Switch Port: Ethernet1/3

Private IP: 192.168.1.5  
CIMC IP: 192.168.0.13  
Status: Active  
State: Commissioned  
SW Version: 3.10.1.1  
Hardware: 56 cores, 947G memory, 10 disks, 24.27T space, SSD  
Firmware: View Firmware Upgrade Logs

- BIOS: C220M6.4.2.3a.0.1029220536
- CIMC: 4.2(3b)
- Cisco UCS VIC 1455 Slot 1: 5.2(3a)
- Cisco UCS VIC 1455 Slot 3: 5.2(3a)
- Cisco 12G SAS RAID Controller with 4GB FBWC (16 Drives) Slot MRAID: 52.20.0-4523
- Intel X550 LOM Slot L: 0x800016FD-1.826.0

**Instances**

- collectorDatamover-3
- datanode-3
- druidHistoricalBroker-1
- elasticsearch-1
- enforcementPolicyStore-3
- happobot-1
- hbaseMaster-1
- orchestrator-3
- redis-3
- tsdbBosunGrafana-1
- zookeeper-1

**Disks Status**

- 1 HEALTHY
- 2 HEALTHY
- 3 HEALTHY
- 4 HEALTHY
- 5 HEALTHY
- 6 HEALTHY
- 7 HEALTHY
- 8 HEALTHY
- 9 HEALTHY
- 10 HEALTHY

Commissioned	Active	Ethernet1/6	WMP272900EB	10mo 25d 23h 45m 48s	+ ↕
Commissioned	Active	Ethernet1/2	WMP272900E2	10mo 25d 4h 25m 35s	+ ↕
Commissioned	Active	Ethernet1/4	WMP272900DZ	3mo 19d 6h 14m 17s	+ ↕
Commissioned	Active	Ethernet1/1	WMP272900EE	29d 9h 46m 59s	+ ↕
Commissioned	Active	Ethernet1/5	WMP272900CH	27d 23h 19m 19s	+ ↕

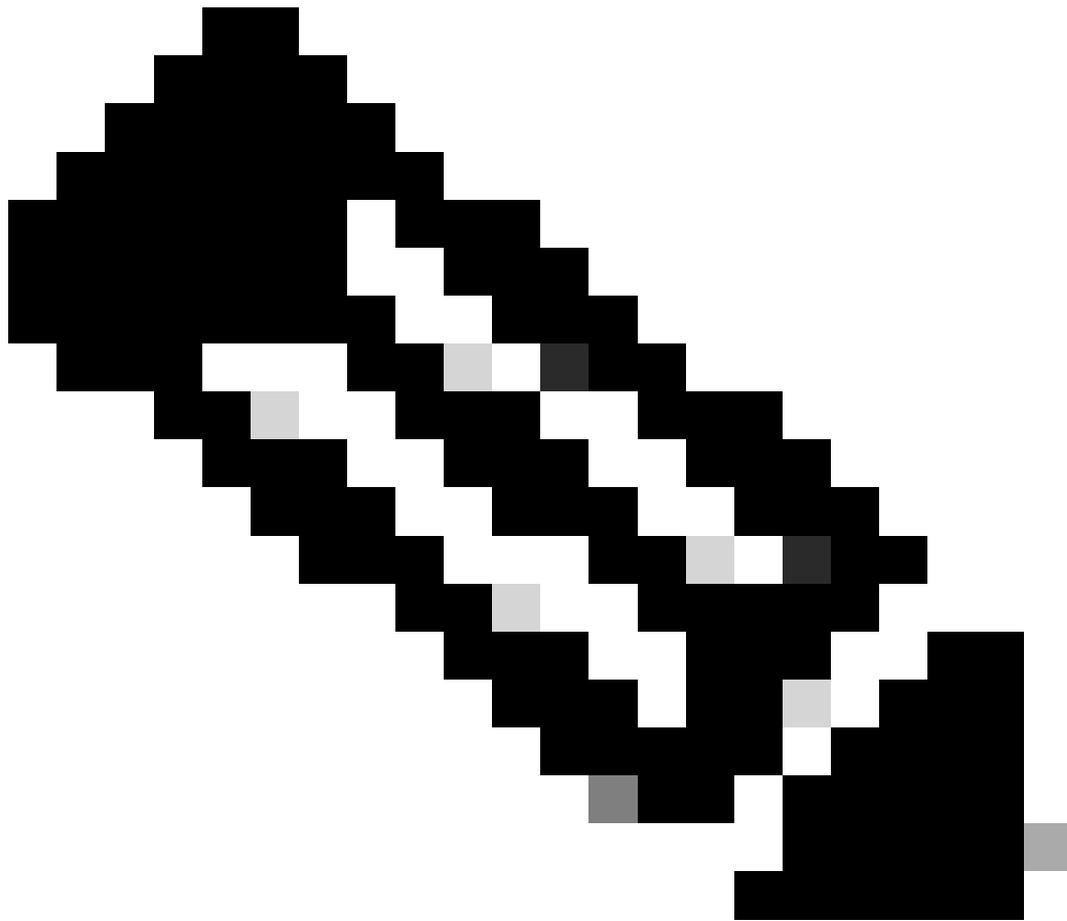
## Servicestatus

Die Seite Service Status (Service-Status) befindet sich im linken Navigationsbereich unter Troubleshoot > Service Status (Fehlerbehebung > Service-Status).

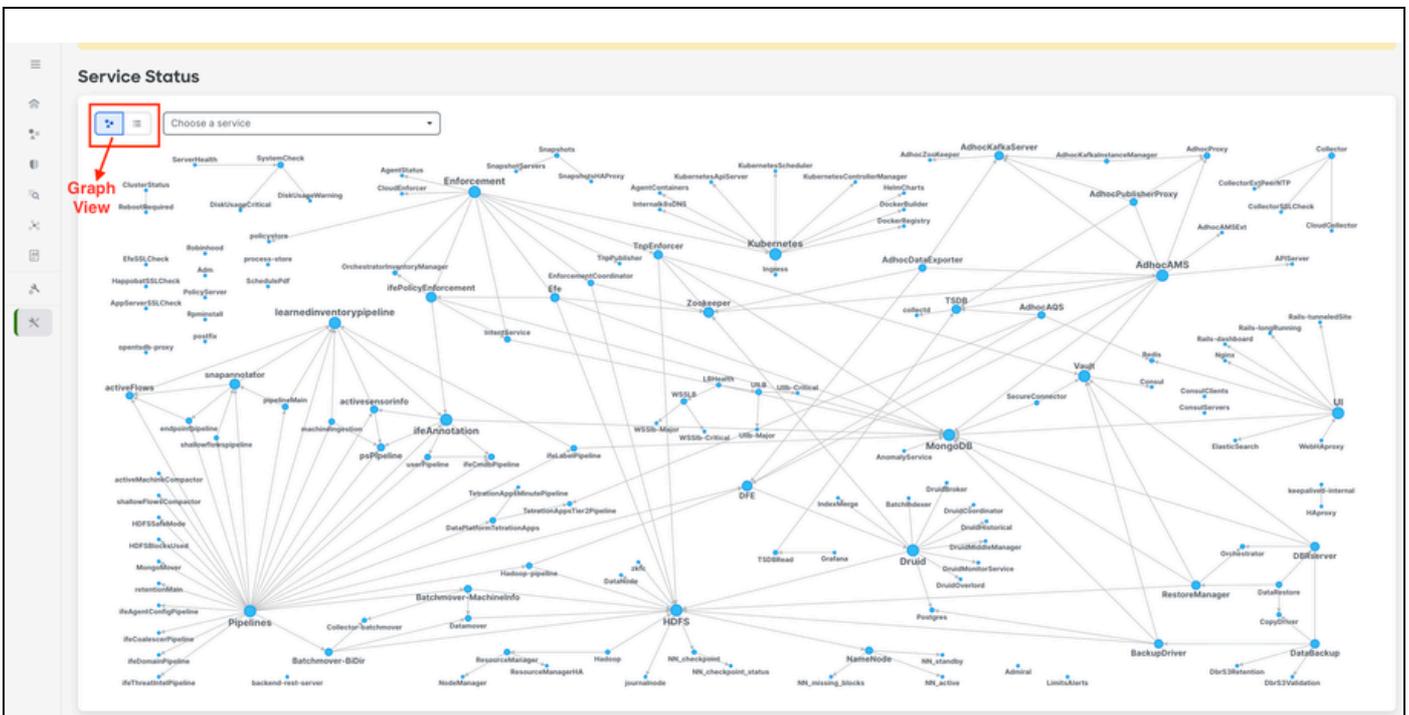
Auf der Seite "Service Status" (Service-Status) werden der Status aller Services angezeigt, die in Ihrem Cisco Secure Workload-Cluster verwendet werden, sowie deren Abhängigkeiten.

Die Diagrammansicht zeigt den Zustand des Diensts an, jeder Knoten im Diagramm zeigt den Zustand des Diensts an, und ein Edge stellt die Abhängigkeit von anderen Diensten dar. Dienste, die nicht ordnungsgemäß funktionieren, werden rot markiert, wenn der Dienst nicht verfügbar ist, und orange, wenn der Dienst heruntergestuft, aber verfügbar ist. Eine grüne Farbe oder eine himmelblaue Farbe weist darauf hin, dass der Service fehlerfrei ist. Weitere Debuginformationen zu diesen Knoten finden Sie in der Strukturansicht mit der Schaltfläche Alle erweitern, um alle untergeordneten Knoten im Abhängigkeitsbaum anzuzeigen. Down zeigt an, dass der Dienst nicht funktioniert, und Ungesund zeigt an, dass der Dienst nicht voll funktionsfähig ist.



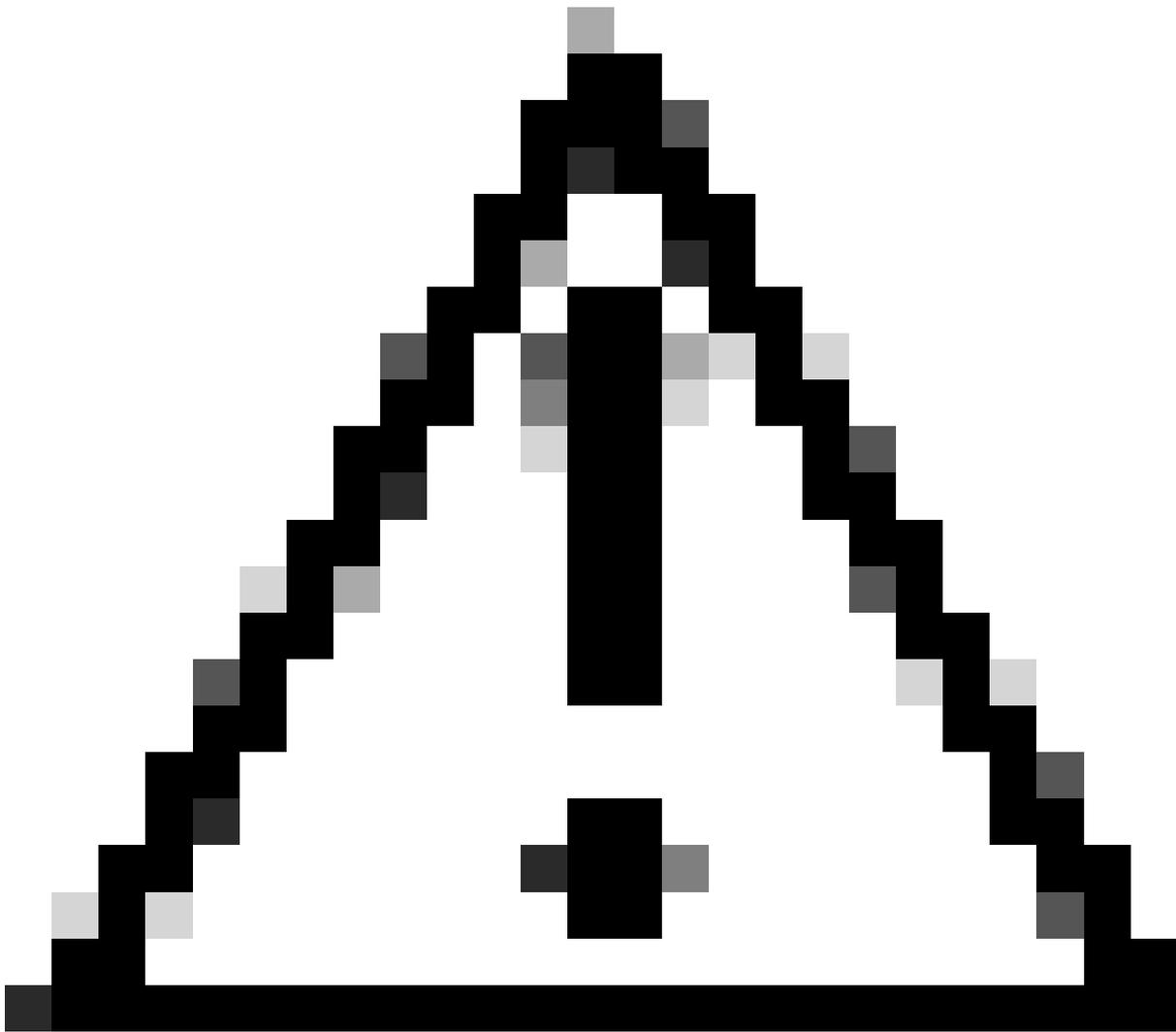


Anmerkung: Ab Patch-Version 3.10.2.11 wird die Service-Statusseite in Himmelblau angezeigt. Eine grüne Farbe oder eine himmelblaue Farbe weist darauf hin, dass der Service fehlerfrei ist.



Standardmäßig werden auf der Seite Service Status (Dienststatus) die Clusterfunktionen und -abhängigkeiten in einer grafischen Ansicht angezeigt. Wenn alle Symbole grün oder himmelblau sind, wird kein Fehler erkannt.

Wenn ein Service in Rot oder Orange angezeigt wird, zeigt die Baumstruktur die Liste der Services an und ermöglicht Ihnen, die Abhängigkeiten des Service sowie weitere Details anzuzeigen, die von der Funktion "Service Status" erkannt wurden. Diese Informationen zu Abhängigkeitsfehlern sollten beim Öffnen eines Tickets beim TAC unbedingt notiert und erfasst werden.



Vorsicht: Wenn Sie feststellen, dass ein Servicefall defekt ist und eine rote Farbe aufweist, wenden Sie sich an das Technical Assistance Center (TAC), um Unterstützung bei der Behebung dieser Probleme zu erhalten. Schnelle Kontaktaufnahme mit dem TAC zur Wiederherstellung der vollen Funktionalität

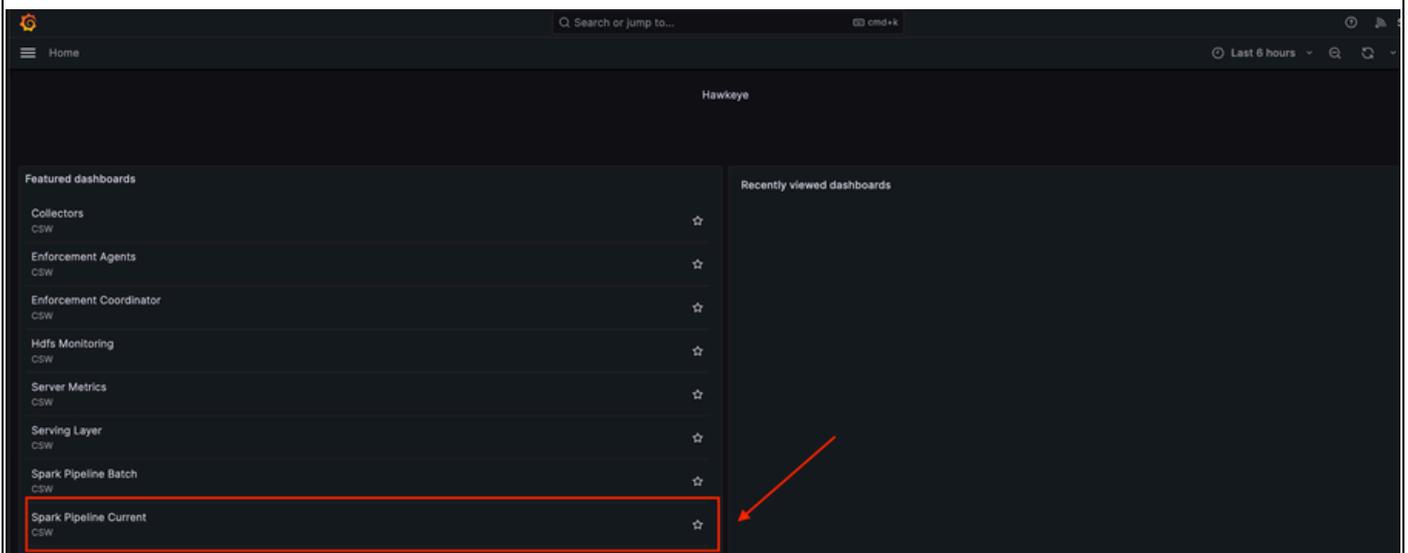
Service	Status	Instances	Details
+ AdhocAQS	Healthy	1 / 1 up	
+ AdhocDataExporter	Healthy	1 / 1 up	
+ AdhocKafkaInstanceManager	Healthy	3 / 3 up	
+ AdhocPublisherProxy	Healthy	1 / 1 up	
Adm	Healthy	3 / 3 up	
Admiral	Healthy	1 / 1 up	
+ AnomalyService	Healthy	1 / 1 up	
AppServerSSLCheck	Healthy	2 / 2 up	
+ ClusterStatus	Healthy	1 / 1 up	
ClusterSwitches	Down	0 / 1 up	Dependencies Failed, URL:http://switchmgr.service.consul:8885/api/v1.0/switchinfo Field:[message][errors] Does not match expectation. Exp:{} Actual:[leaf]: [Interface Ethernet1/41 state value down does not match expected value of up] Please check dependencies!
+ Collector	Healthy	6 / 6 up	
ConsulClients	Healthy	65 / 65 up	
ConsulServers	Healthy	3 / 3 up	
- DataBackup	Down	1 / 1 up	No values found for TSD metric max:dbr.bkpdriver.time_since_cp for at least one dataset None Please check dependencies!
- BackupDriver	Down	0 / 1 up	Dependencies Failed, No values found for TSD metric max:dbr.bkpdriver.health for at least one dataset None Please check dependencies!
+ HDFS	Healthy	2 / 2 up	
MongoDB	Healthy	2 / 2 up	

## Hawkeye (Diagramme)

Hawkeye-Dashboards bieten Einblick in den Status des sicheren Workload-Clusters sowie Metriken und Informationen zur Unterstützung der Fehlerbehebung

Die Seite Hawkeye (Diagramme) befindet sich im linken Navigationsbereich unter Troubleshoot > Hawkeye (Diagramme).

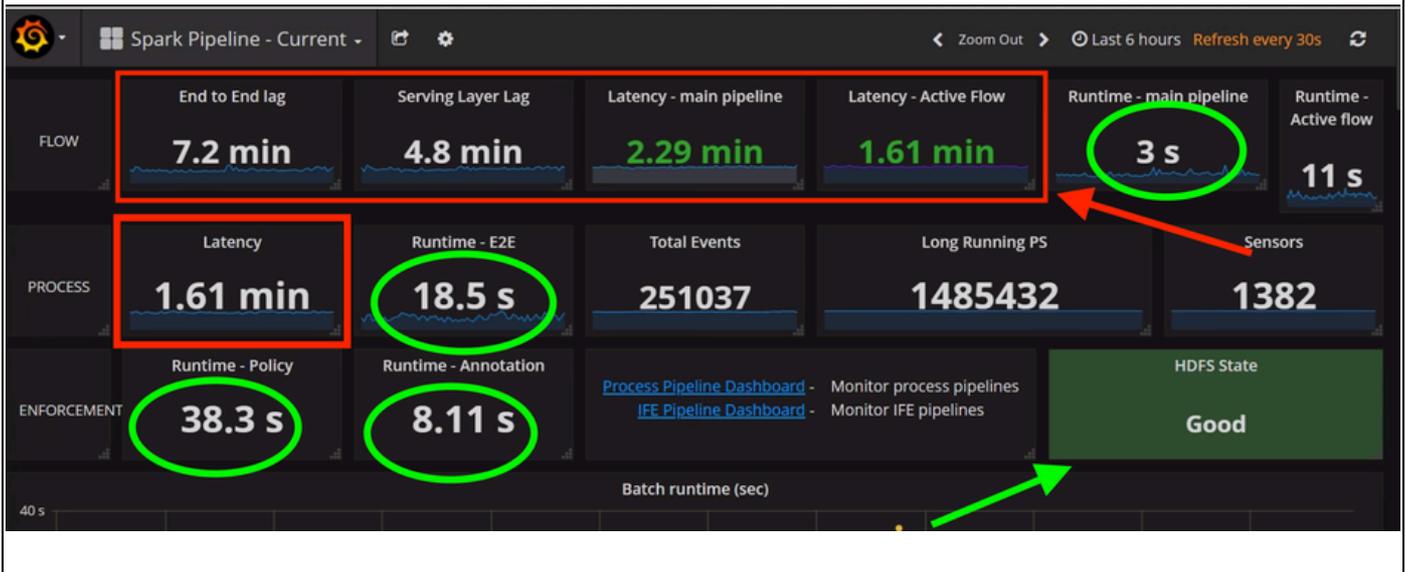
Wenn Sie auf Hawkeye (Diagramme) klicken, wird automatisch eine neue Browserregisterkarte geöffnet, auf der das Hawkeye-Dashboard wie hier dargestellt angezeigt wird.

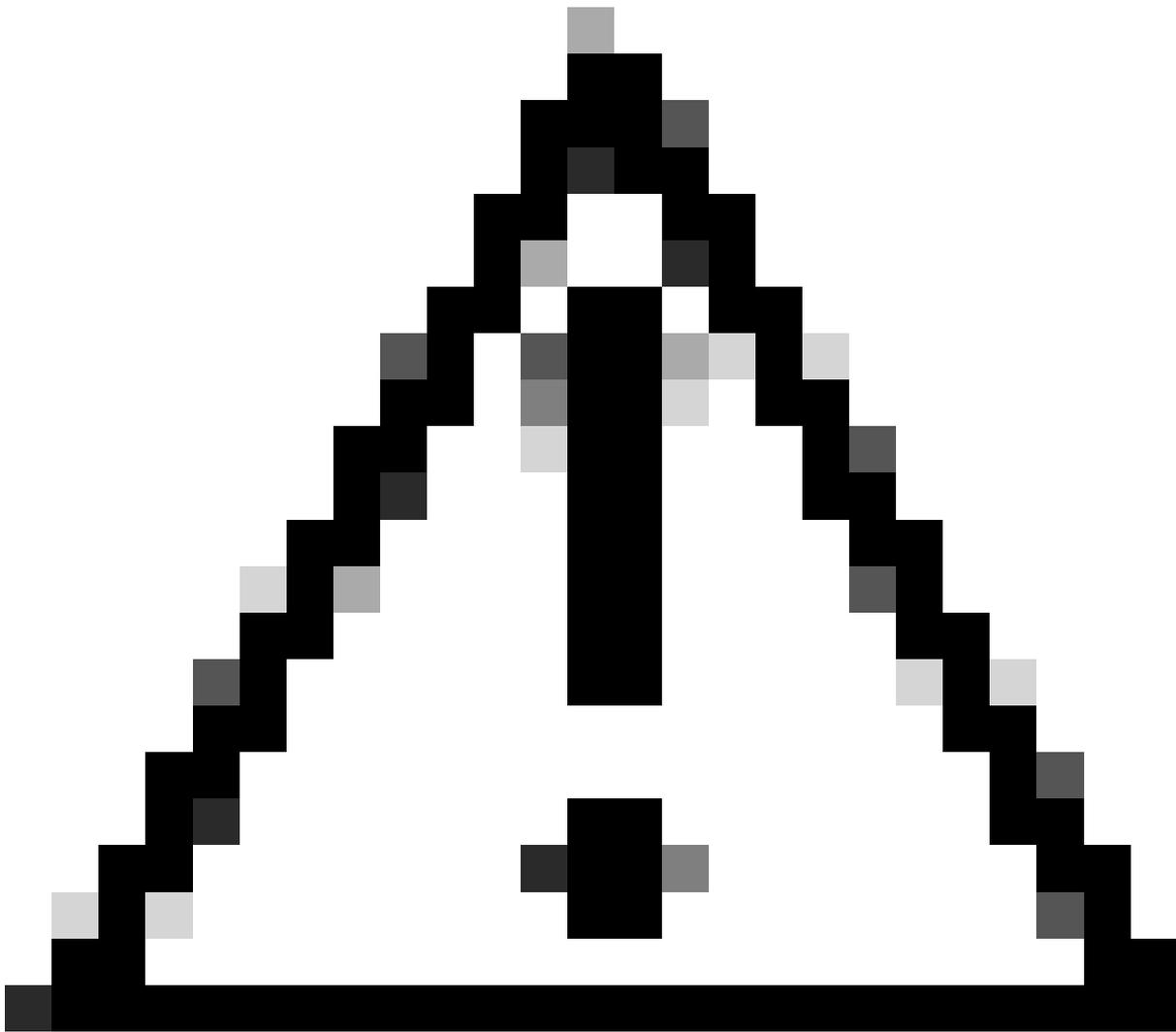


Klicken Sie im Hawkeye-Dashboard auf die Registerkarte Spark Pipeline Current (Spark Pipeline Aktuell), um den Status des sicheren Workload-Clusters zu überwachen.

Überprüfen Sie auf der Seite Spark Pipeline Current (Aktuelle Spark-Pipeline), ob die Werte für End-to-End-Verzögerung, Serving Layer-Verzögerung, Main Pipeline Latency (Hauptpipelinelatenz) und Active Flow Latency (Aktive Flow-Latenz) unter 10 Minuten liegen.

Stellen Sie außerdem sicher, dass die Laufzeitwerte weniger als 1 Minute betragen und in Sekunden angezeigt werden und der HDFS-Status "Good" (Gut) lautet, wie im nächsten Beispiel gezeigt.





Vorsicht: Wenn Sie Latenzwerte (einschließlich End-to-End-Verzögerung oder Verzögerung auf dem Service-Layer) von mehr als 6 Stunden beobachten, ohne eine allmähliche Verringerung festzustellen, wenden Sie sich an das Technical Assistance Center (TAC).

## Upgrade-Prechecks

Verwenden Sie vor und nach Wartungsaufgaben die Upgrade-Vorabprüfung, um Cluster-Zustandsprüfungen auszuführen. Dieser Prozess stellt sicher, dass Services, Konfigurationen und Hardwarekomponenten ordnungsgemäß funktionieren.

1. Navigieren Sie zu Upgrade Precheck.

Navigieren Sie zu TetratationUI, und befolgen Sie die folgenden Schritte:

- Klicken Sie auf Plattform.
- Wählen Sie Upgrade/Neustart/Herunterfahren aus.

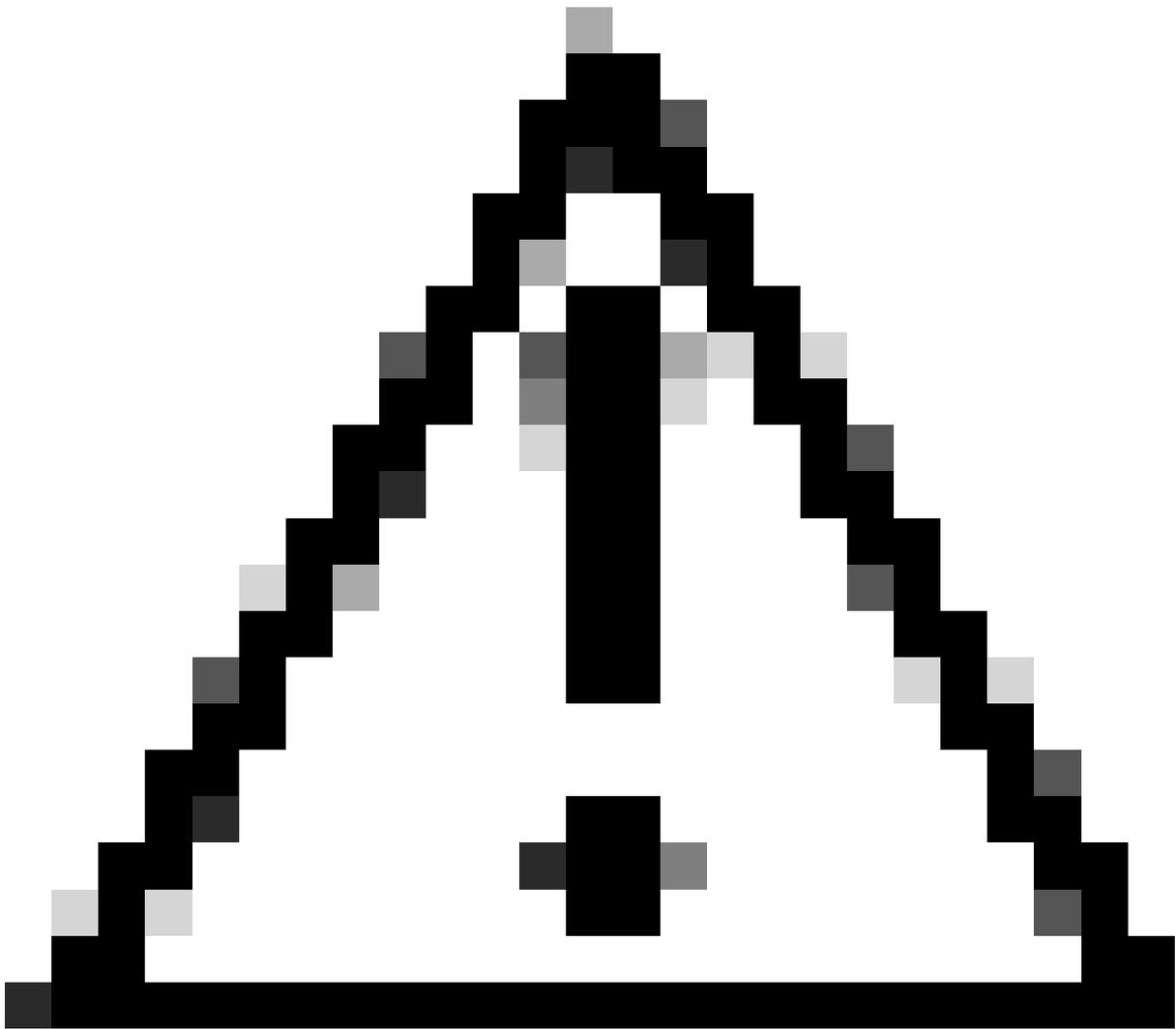
- Klicken Sie auf Upgrade PreCheck starten.

Warten Sie einige Minuten auf die Ausgabe der Upgrade-Vorprüfungen. Wenn alles wie in diesem Bild gezeigt erfolgreich ist, können Sie mit den nächsten Aktionen der Clusterwartungsaktivitäten fortfahren.

The screenshot shows the Cisco Secure Workload interface. A modal dialog box titled "Upgrade Precheck Status" is displayed over the main content. The dialog box contains a table with the following data:

Task	Status	Log
Cluster Health Check	success	Orchestrator
Service Health Check	success	Orchestrator
Secrets Sync Check	success	Orchestrator
Site Linter	success	Orchestrator
Site Checker	success	SiteInfoChecker

The "Status" column is highlighted with a green box, and a green arrow points to the "success" status for the "Cluster Health Check" task. A "Close" button is located in the bottom right corner of the dialog box.



Vorsicht: Wenn die Upgrade-Vorabprüfung nicht erfolgreich war, wenden Sie sich an das Technical Assistance Center (TAC).

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.