

Überprüfen der Integrität eines Tetration Analytics-Clusters

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Wann wird der Status des Clusters überprüft?](#)

[Verschiedene Möglichkeiten zur Überprüfung des Betriebsstatus eines Tetration-Clusters](#)

[Betriebliche Anzeigeparameter](#)

[Cluster-Status](#)

[Servicestatus](#)

[Bosun-Warnungen](#)

[Snapshot erstellen und TAC-Ticket öffnen](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie der Zustand eines Tetration Analytics-Clusters überprüft wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Anmeldung bei einem Cluster
- Grundlegende Benutzeroberfläche

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Version 2.2.1.x
- 39-HE-Tetration Analytics-Cluster

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ein Tetration-Cluster besteht aus Hunderten von Prozessen (Programmen), die auf mehreren VMs [virtuelle Systeme] auf mehreren UCS C220-M4 Servern ausgeführt werden. Es stehen mehrere Dienste und Funktionen zur Verfügung, um die Vorgänge des Clusters zu überwachen und den Administrator zu benachrichtigen, wenn der Cluster möglicherweise nicht voll funktionsfähig ist.

Dieses Dokument bietet eine Übersicht über die Funktionen, die bei der Überprüfung der Integrität des Clusters überprüft werden müssen. Während der Umfang dieses Dokuments die Überprüfung der Integrität umfasst, sollten Maßnahmen ergriffen werden, um Probleme zu beheben, die scheinbar nicht ordnungsgemäß funktionieren, eine Momentaufnahme erstellen und beim Cisco Tetration Solution Support TAC-Team ein Ticket erstellen.

Zwei gängige Tools zur Überprüfung der Integrität des Clusters sind die Seiten **Cluster-Status** und **Dienststatus**, die in diesem Dokument zusammen mit einigen anderen Systemtools behandelt werden. Obwohl **kritische** E-Mail-Warnmeldungen von Bosun häufig einer der ersten Hinweise für einen Administrator sind, dass im Cluster möglicherweise etwas vorkommt, wird die Überprüfung der Integrität des Clusters in der Regel am besten über die Seiten **Cluster-Status** und **Dienststatus** durchgeführt.

Während Boson-Warnungen syslog-ähnliche Funktionen bieten, wurden in einigen Tetration-Versionen einige kritische Bosun-Warnungen in einem normalerweise funktionierenden Cluster ausgelöst. Eine Suche über das [Bug Search Tool](#) für **Tetration** mit dem Metric-Schlüsselwort cisco.com hilft bei der Identifizierung möglicher Probleme für eine bestimmte Metrik.

Wann wird der Status des Clusters überprüft?

Normalerweise muss der Administrator des Clusters die Funktionalität des Clusters nicht überprüfen. Es gibt jedoch gewisse Zeiten, in denen dies notwendig sein kann. Hier einige Beispiele:

1. Wenn der Benutzer ein unerwartetes Verhalten in der Benutzeroberfläche (user interface, UI) erkennt. Dies beruht zum Teil auf den Kenntnissen und Erfahrungen des Benutzers, wie der Cluster funktionieren soll, aber einige Beispiele sind in diesem Abschnitt **Betriebliche Anzeigeparameter** dargestellt.
2. Wenn erwartet wird, dass einige Daten angezeigt werden, aber nicht in der Benutzeroberfläche angezeigt werden. Zum Beispiel fließen Daten von einem Software- oder Hardware-Agent (Sensor), wenn der richtige Bereich und der richtige Zeitraum angezeigt werden, in dem Daten angezeigt werden sollen.
3. Vor und nach einem geplanten Service, Upgrade oder größeren Aktionen des Clusters. Es ist empfehlenswert, einen Snapshot vor und einen weiteren Snapshot nach Wartungsarbeiten zu sammeln und diesen für den Fall verfügbar zu machen, dass ein TAC-Ticket geöffnet wird. Dadurch kann das TAC das Problem isolieren, indem es nach Änderungen sucht, die

während der Wartung vorgenommen wurden.

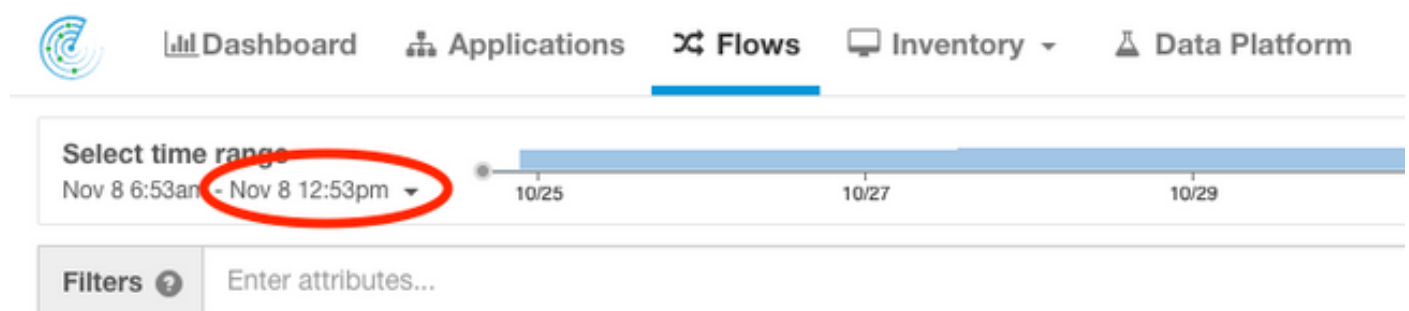
Hinweis: Einige Serviceunterbrechungen sind für einen bestimmten Zeitraum unmittelbar nach der Systemwartung im Cluster normal. Der Zeitraum kann im Beispiel eines Serveraustauschs bis zu 24 Stunden betragen, wenn ein Datode-VM auf diesem Server ausgeführt wird. Normale Systemredundanz im Cluster reduziert in der Regel die negativen Auswirkungen eines Serveraustauschs.

Verschiedene Möglichkeiten zur Überprüfung des Betriebsstatus eines Tetration-Clusters

Betriebliche Anzeigeparameter

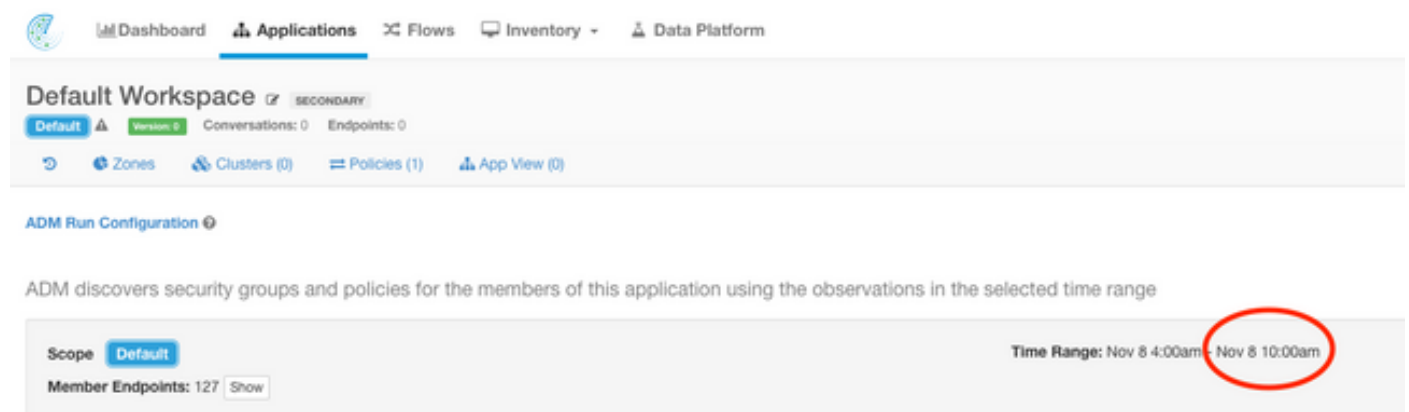
Ein Administrator, der über Kenntnisse und Erfahrung im Betrieb des Clusters verfügt, kann erkennen, wie der normale Betrieb des Clusters in seiner Umgebung aussieht. Dies sind einige Beispiele für die Vorgehensweise bei der Überprüfung, ob der Cluster normal arbeitet.

Beispiel 1: Die aktuellste verfügbare Flow-Zeit ist innerhalb von 10 Minuten nach der aktuellen Zeit verfügbar.



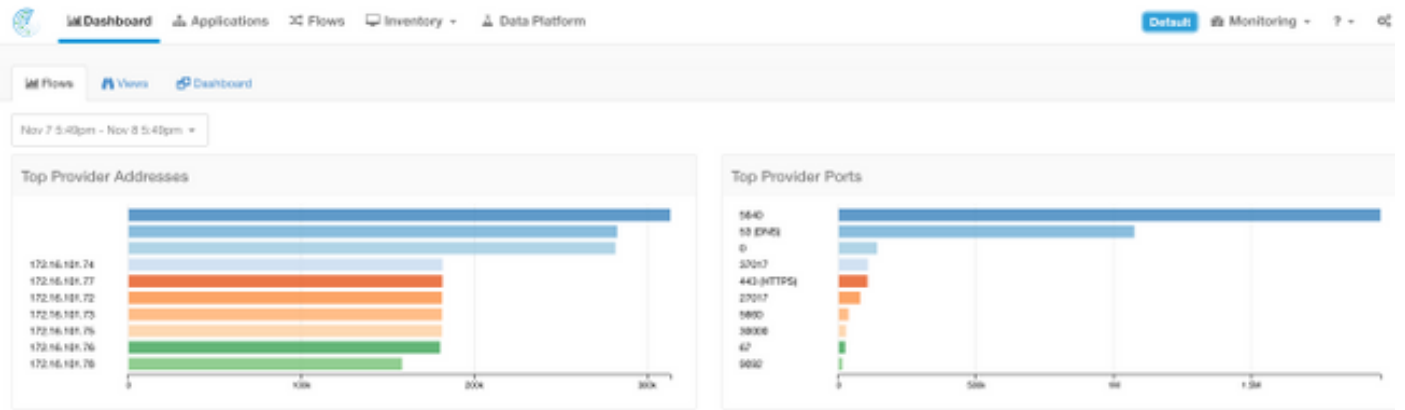
The screenshot shows the Tetration dashboard with the 'Flows' tab selected. The navigation bar includes 'Dashboard', 'Applications', 'Flows', 'Inventory', and 'Data Platform'. Below the navigation bar, there is a 'Select time range' dropdown menu highlighted with a red circle, displaying the selected range 'Nov 8 6:53am - Nov 8 12:53pm'. A timeline below the dropdown shows dates 10/25, 10/27, and 10/29. Below the timeline is a 'Filters' section with a search input 'Enter attributes...'.

Beispiel 2: Die neueste verfügbare Anwendungs-Workspace-Zeit ist innerhalb von 10 Stunden nach der aktuellen Zeit verfügbar:



The screenshot shows the Tetration dashboard with the 'Applications' tab selected. The 'Default Workspace' section is visible, showing 'Default' as the selected workspace. Below this, there are navigation options for 'Zones', 'Clusters (0)', 'Policies (1)', and 'App View (0)'. The 'ADM Run Configuration' section is also visible, with a description: 'ADM discovers security groups and policies for the members of this application using the observations in the selected time range'. At the bottom, there is a 'Scope' dropdown set to 'Default' and a 'Time Range' dropdown highlighted with a red circle, showing the selected range 'Nov 8 4:00am - Nov 8 10:00am'. Below the 'Time Range' dropdown, it says 'Member Endpoints: 127' with a 'Show' button.

Beispiel 3: Dashboard-Inhalte werden gefüllt.

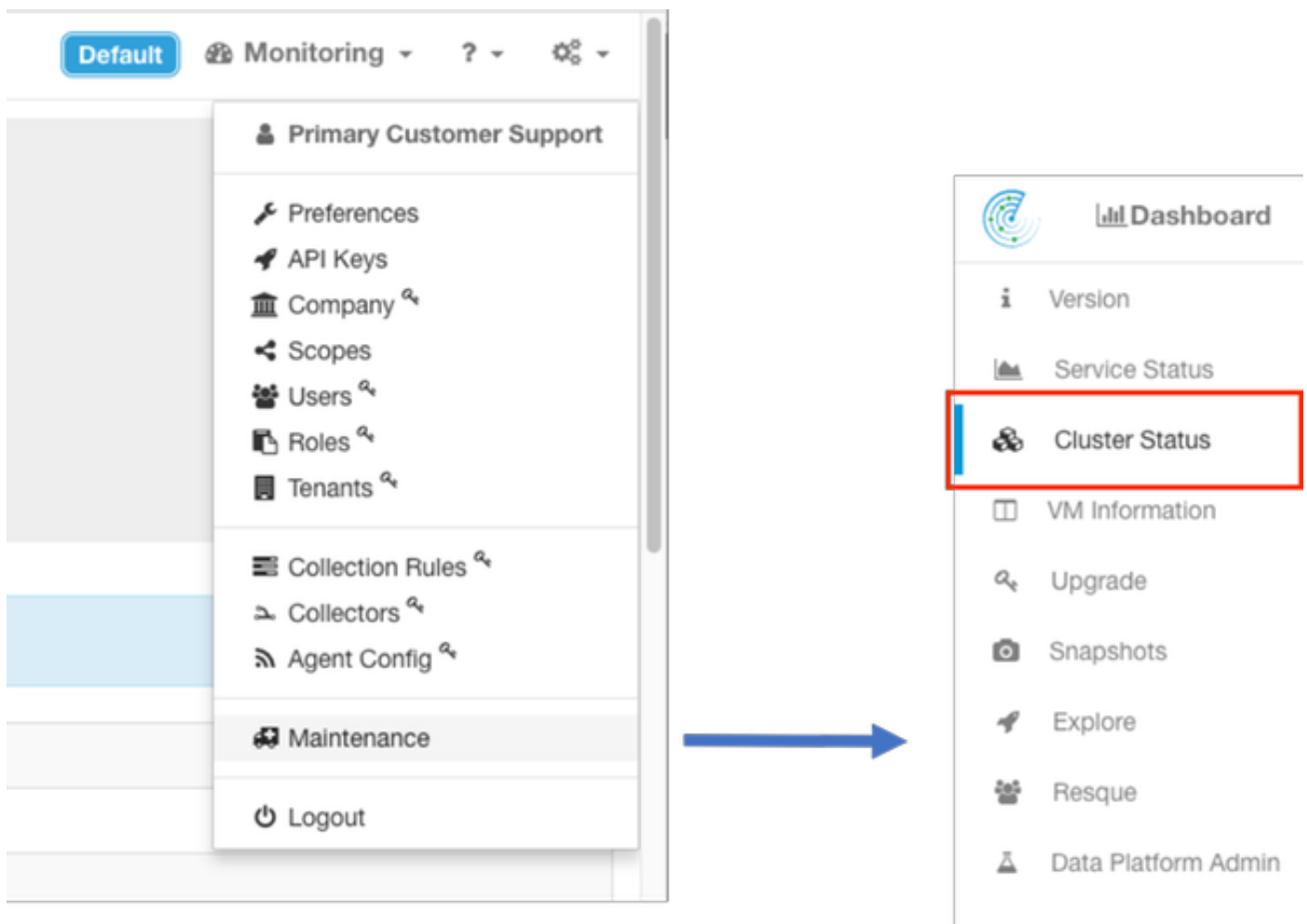


Cluster-Status

Ein Tetration Analytics-Cluster besteht je nach Cluster-Typ aus entweder 6 (8 HE) oder 36 (39 HE) Servern. Die Seite "Cluster Status" (Cluster-Status) zeigt den Status der Server sowie weitere Bare-Metal-Serverinformationen an.

Die Seite Cluster Status (Clusterstatus) befindet sich im Menü Maintenance (Wartung), das über das Dropdown-Menü Settings (Einstellungen > **Maintenance (Einstellungen > Wartung)** verfügbar ist. Cluster-Status in der linken Spalte.)

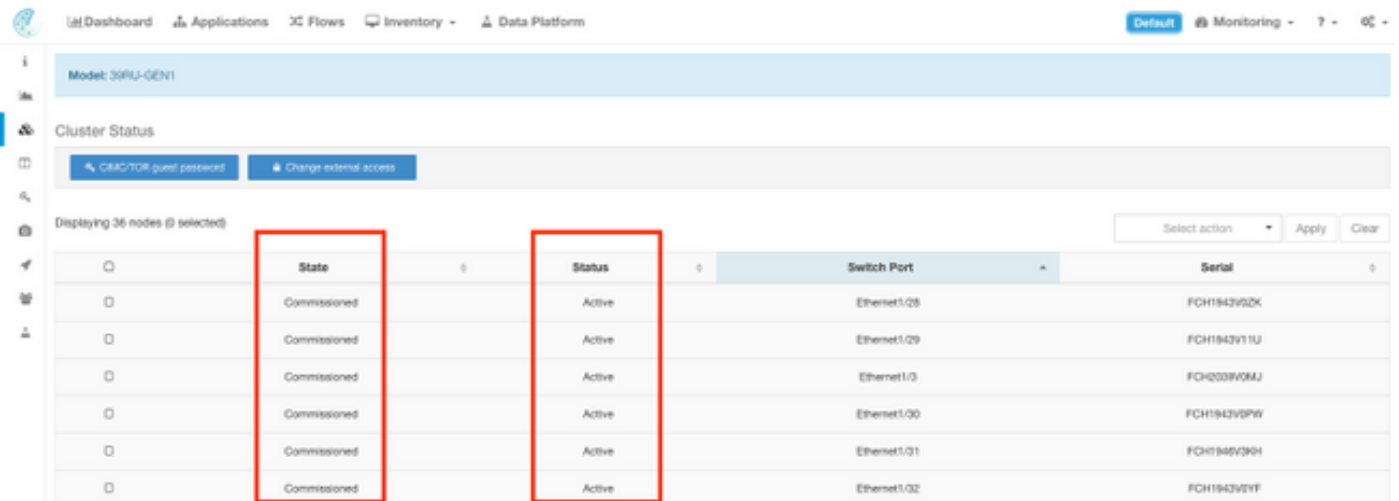
Hinweis: Nur das Symbol wird angezeigt, bis Sie auf die linke Spalte klicken.



Die Seite "Clusterstatus" in einem Cluster zeigt eine Liste aller Server im Cluster an. Ein

funktionierender Server sollte einen **Zustand** von **beauftragen** und einen **Status** von **aktiv** anzeigen, wie hier gezeigt.

Hinweis: Image wird auf die ersten 6 von 36 Servern (39-HE-Cluster) abgeschnitten.

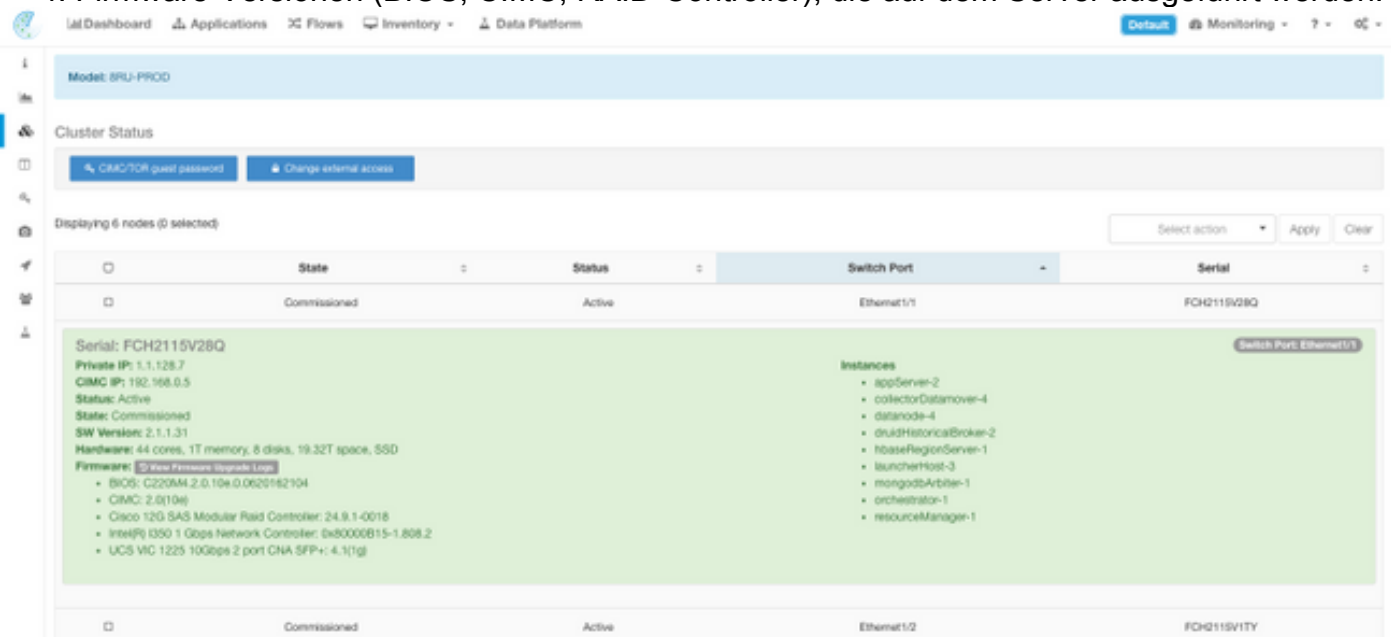


State	Status	Switch Port	Serial
Commissioned	Active	Ethernet1/28	FCH1943V52K
Commissioned	Active	Ethernet1/29	FCH1943V11U
Commissioned	Active	Ethernet1/0	FCH203RVMU
Commissioned	Active	Ethernet1/30	FCH1943V8PW
Commissioned	Active	Ethernet1/01	FCH1945V3GH
Commissioned	Active	Ethernet1/02	FCH1943V5VF

Wenn der Status "Inaktiv" anzeigt, bezieht sich dies in der Regel auf einen Server, der nicht eingeschaltet ist oder möglicherweise Kabel- oder Verbindungsprobleme aufweist.

Wenn Sie auf einen Server in der Liste klicken, werden zusätzliche Informationen zu diesem bestimmten Server angezeigt, darunter:

1. Instanzen (virtuelle Systeme), die auf dem Bare-Metal-Server ausgeführt werden.
2. Private IP-Adresse innerhalb des Clusters.
3. CIMC-IP-Adresse im Cluster.
4. Firmware-Versionen (BIOS, CIMC, RAID-Controller), die auf dem Server ausgeführt werden.



State	Status	Switch Port	Serial
Commissioned	Active	Ethernet1/1	FCH2115V28Q

Serial: FCH2115V28Q

Private IP: 1.1.128.7
CIMC IP: 192.168.0.5
Status: Active
State: Commissioned
SW Version: 2.1.1.31
Hardware: 44 cores, 1T memory, 6 disks, 19.32T space, SSD
Firmware: [View Firmware Details](#)

- BIOS: C220AM.2.0.10e.0.0620162104
- CIMC: 2.0(10e)
- Cisco 12G SAS Modular Raid Controller: 24.9.1-0018
- Intel(R) i350 1 Gbps Network Controller: 0x80000B15-1.808.2
- UCS VIC 1225 10Gbps 2 port CNA SFP+: 4.1(1g)

Instances

- appServer-2
- collectorData mover-4
- datanode-4
- druidHistoricalBroker-2
- hbaseRegionServer-1
- launcherHost-3
- mongodbArbiter-1
- orchestrator-1
- resourceManager-1

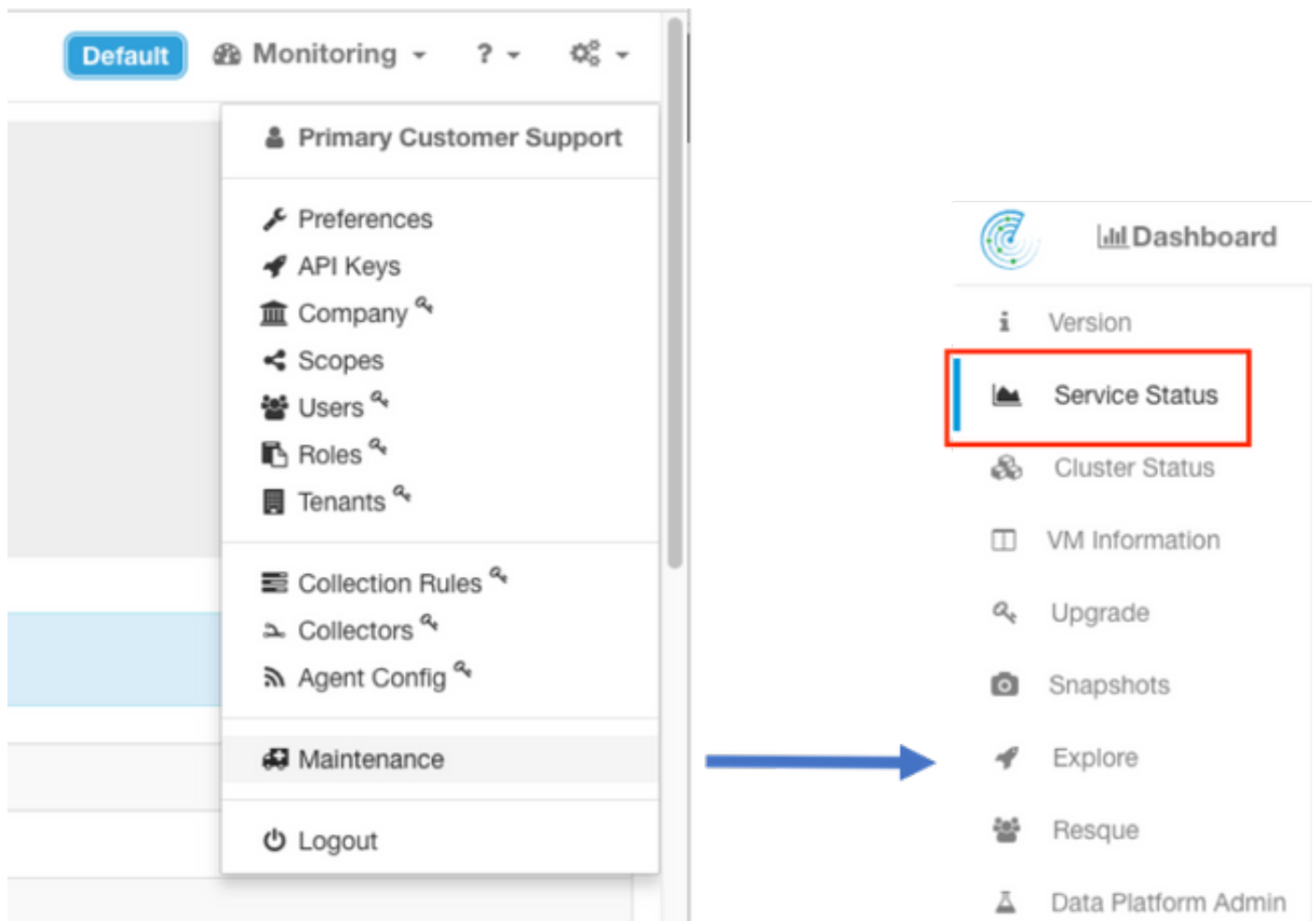
Commissioned	Active	Ethernet1/2	FCH2115V1TY
--------------	--------	-------------	-------------

Servicestatus

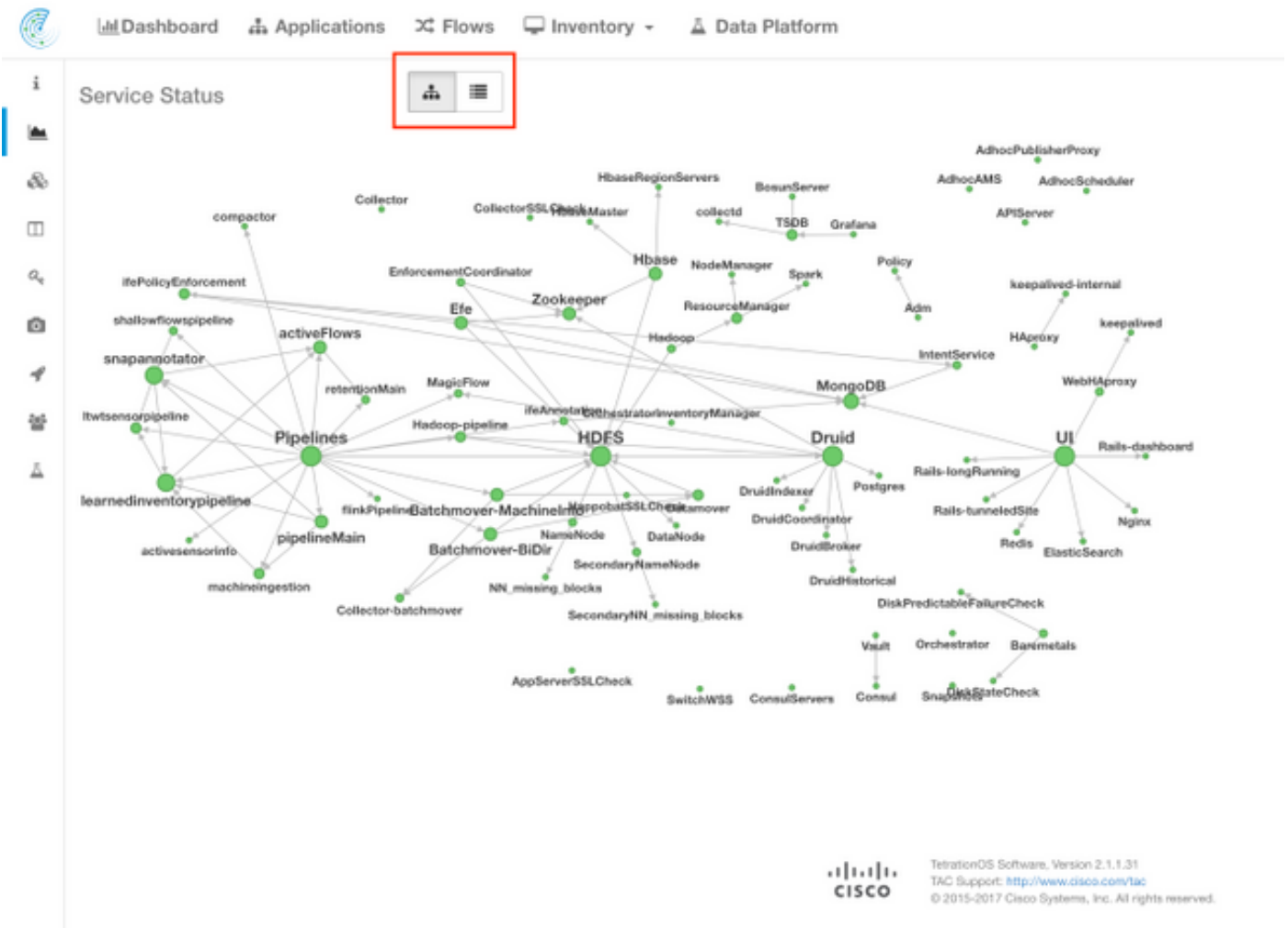
Die ServiceStatus Seite zeigt alle Dienstdie im Cisco Tetricon Analytics-Cluster mit ihren Abhängigkeiten und ihrem Status verwendet werden Status.

Die Seite Service Status (Dienststatus) befindet sich im Menü Maintenance (Wartung), das über das Dropdown-Menü Settings (Einstellungen) verfügbar ist. (**Einstellungen > Wartung;** Dienststatus in der linken Spalte.)

Hinweis: Nur das Symbol wird angezeigt, bis Sie auf die linke Spalte klicken.



Standardmäßig zeigt die Seite "Dienststatus" die Clusterfunktionen und -abhängigkeiten in einer grafischen Ansicht an. Wenn alle Symbole grün leuchten, wird kein Fehler erkannt.



Wenn ein Dienst rot oder orange angezeigt wird, wird in der Strukturansicht eine Liste mit Diensten angezeigt, in der Sie detaillierte Informationen zu den Abhängigkeiten des Dienstes sowie zu anderen Details finden können, die von der Funktion Dienststatus erkannt wurden. Diese Informationen zu Abhängigkeitsfehlern sind besonders wichtig, wenn Sie beim TAC ein Ticket erstellen.

So sieht die Listenansicht beispielsweise aus, wenn eines der virtuellen HDFS DataNode-Systeme im Cluster ausgefallen ist.

Hinweis: Die Redundanz, die im Tetratron-Cluster vorgesehen ist, hat möglicherweise keine nennenswerten Auswirkungen auf den Cluster.

Service	Status	Instances	Details
SwitchWSS	Healthy	2 / 2 up	
Hadoop	Down	1 / 1 up	Please check dependencies!
HDFS	Down	1 / 2 up	Dependencies Failed, Dependencies Failed, URL:http://namenode.namenode.service.consul:50070/jmx?gry=Hadoop: Field [beans]name-->Hadoop.service.Namenode.name-FSNamesystemState[NumDeadDataNodes] Does not match expectation, Exp:0 Actual:1 Please check dependencies!
DataNode	Down	23 / 24 up	Dependencies Failed, URL:http://namenode.namenode.service.consul:50070/jmx?gry=Hadoop: Field [beans]name-->Hadoop.service.Namenode.name-FSNamesystemState[NumDeadDataNodes] Does not match expectation, Exp:0 Actual:1 Please check dependencies!

Hinweis: Bestimmte Dienste können nach der Durchführung der Wartung zu einem

funktionierenden Zustand zurückkehren. Beispielsweise kann es bis zu 24 Stunden dauern, bis ein Server, auf dem eine Instanz des virtuellen DataNode-Systems ausgeführt wird und der für die RMA-Wartung außer Betrieb genommen und wieder außer Betrieb genommen wird, bevor das erkannte Problem behoben wird.

Obwohl Details zum Service-Status darauf hinweisen, was im Falle eines aufgedeckten Problems passieren könnte, wird empfohlen, ein TAC-Ticket zu eröffnen, wenn Fragen zur Bedeutung und/oder zu möglichen Gegenmaßnahmen bestehen.

Bosun-Warnungen

Bosun ist ein Open-Source-Überwachungs- und Alerting-System, das im Tetration Analytics-Cluster verwendet wird, um verschiedene Metriken der Dienste (ein Programm, das beim Booten beginnt) zu überwachen, die im Cluster ausgeführt werden. Wenn ein Dienst normal ausgeführt wird, werden seine Metriken in openTSDB eingetragen. Das Bosun Programm untersucht die Kennzahlen eines Service in openTSDB und wendet die Bosun-Regeln an, um zu bestimmen, ob die aktuellen Kennzahlen benachrichtigt werden. Bosun-Warnungen werden lokal auf der Cluster-Benutzeroberfläche unter **Monitoring > Sentinel [Alerts]** angezeigt.

Bosun sendet E-Mail (an die Konfigurations-Site_bosun_email des Clusters), um den Clusteradministrator über einen potenziellen **kritischen** Zustand zu informieren, wenn ein Grenzwert für diese Kennzahl überschritten wird. Bosun generiert drei Arten von E-Mails:

Kritisch: Wenn eine Kennzahl für eine Bosun-Warnungs-Regel den konfigurierten Grenzwert überschreitet

Normal: Folge einer "kritischen" E-Mail, sobald die Kennzahl unter den Schwellenwert fällt

Zusammenfassung: Wird in der Regel alle 6 Stunden gesendet und enthält eine Zusammenfassung der Warnungen im 6-Stunden-Fenster.

Beispiele für E-Mail-Warnungen:

Critical (für intentservice.checkMissingIntentService-Metrik) :

(critical)(bosun)(pan): intentservice.checkMissingIntentService 6:50 AM
To:

Status: **Critical**
[View Incident](#) | [Ack](#) | [Close](#) | [History](#) | Silence: [1h](#) [2h](#) [4h](#) [8h](#) [12h](#) [24h](#)
Last published data point: 1961 seconds ago
Threshold: 1800 seconds
Description: "Intent service is losing heartbeat. Check if intent service is up. Without intent service, users cannot access and modify intents."
Tags

Normal:

(normal)(bosun)(pan): intentservice.checkMissingIntentService 6:52 AM
To:

Status: **Normal**
[View Incident](#) | [Ack](#) | [Close](#) | [History](#) | Silence: [1h](#) [2h](#) [4h](#) [8h](#) [12h](#) [24h](#)
Last published data point: 581 seconds ago
Threshold: 1800 seconds
Description: "Intent service is losing heartbeat. Check if intent service is up. Without intent service, users cannot access and modify intents."
Tags

Zusammenfassung:

(Summary)(bosun)(pan): summary

To:

2017-10-26 00:42:07.260409693 +0000 UTC

This alert is executed every 6h. It summarizes alerts in the last 6h.

Summary of alerts in critical state in the last 6h, ordered by percentage

These are alerts that has **at least** one instance in critical state.

<code>bosun.checkErrorsIsHigh</code>
<code>magicflow.numberOfServerHostForMagicFlowsLow</code>
<code>intentservice.checkMissingIntentService</code>

Summary of alerts in error state in the last 6h.

Note: Alerts in error state means either it has syntax errors (unlikely) or required metrics never show up in OpenTSDB (very likely).

Alert

Die kritischen Warnmeldungen enthalten Informationen darüber, welche Kennzahlen, wann, welcher Grenzwert, welcher gemessene Datenpunkt und eine Problembeschreibung enthalten. Beispielsweise kann die Warnung generiert werden, wenn der Dienst fehlerhaft funktioniert und seine Kennzahlen nicht mehr für openTSDB bereitstellt. Die Bedeutung und die potenziellen Auswirkungen der Bosun-kritischen Warnung erfordern möglicherweise, dass ein TAC-Fall geöffnet wird, um den Kontext besser zu verstehen und die Bedeutung der Warnung zu erklären.

Snapshot erstellen und TAC-Ticket öffnen

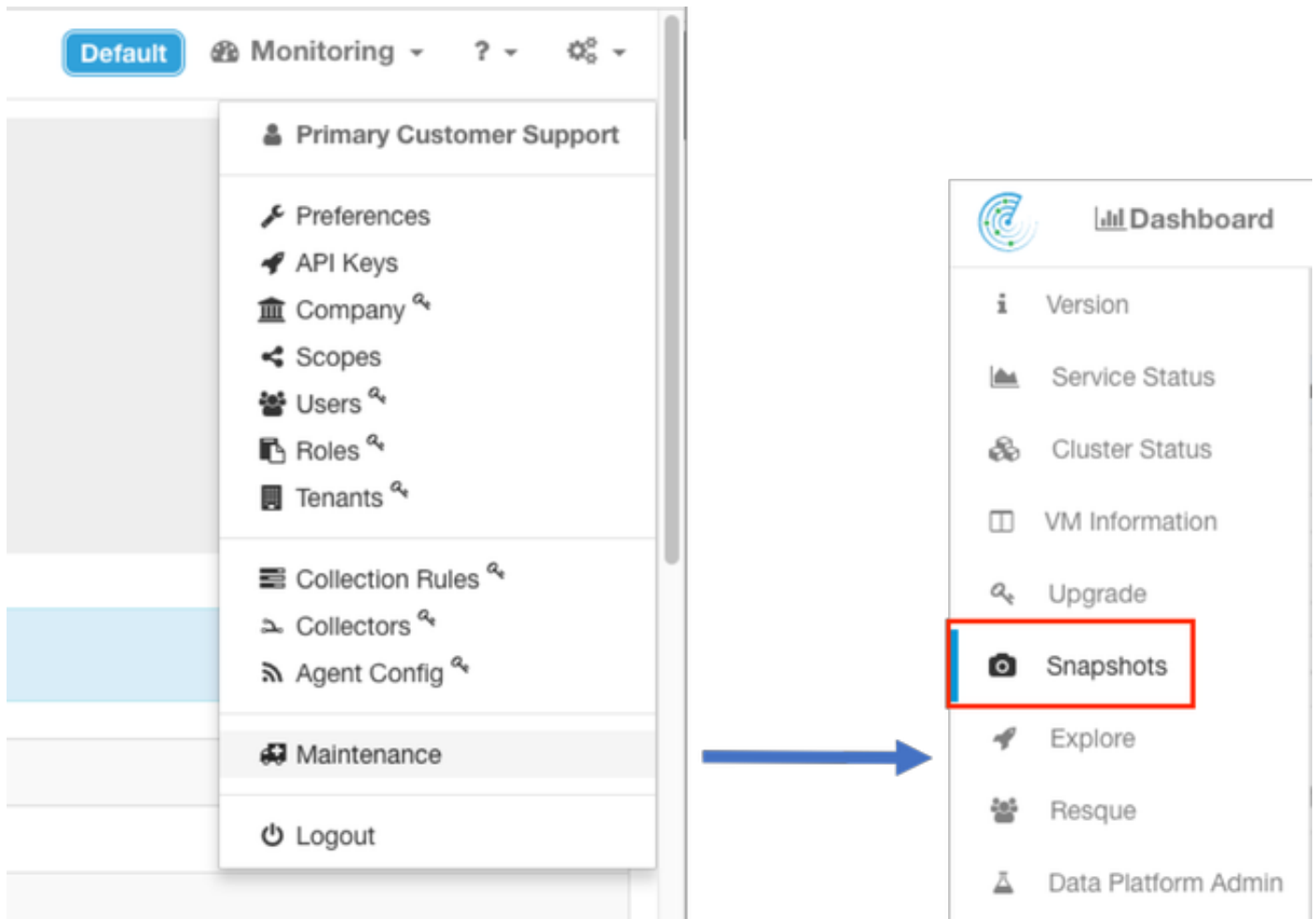
Das Cisco Tetration Solution Team ist auf Tetration Analytics-Kunden spezialisiert und unterstützt diese. Eine der gängigsten Aufgaben, die TAC bei der Fehlerbehebung am meisten unterstützen, ist eine Snapshot-Sammlung von Protokollen aus dem Cluster. Manchmal reichen nur die in den Snapshot-Protokolldateien enthaltenen Informationen aus, um das Problem zu verstehen. Ist dies nicht der Fall, stellt ein Snapshot in vielen Fällen den Ausgangspunkt für die Fehlerbehebung dar.

Ein Snapshot in einem Tetration-Cluster ähnelt dem Technologiesupport in anderen Cisco Produkten. Es handelt sich um komprimierte Tarball-Dateien oder Protokolldateien von allen Servern und virtuellen Systemen, die Folgendes umfassen:

- Protokolle
- Bundesstaat der Hadoop/YARN-Anwendung und Protokolle
- Warnmeldungsverlauf
- Zahlreiche TSDB-Statistiken

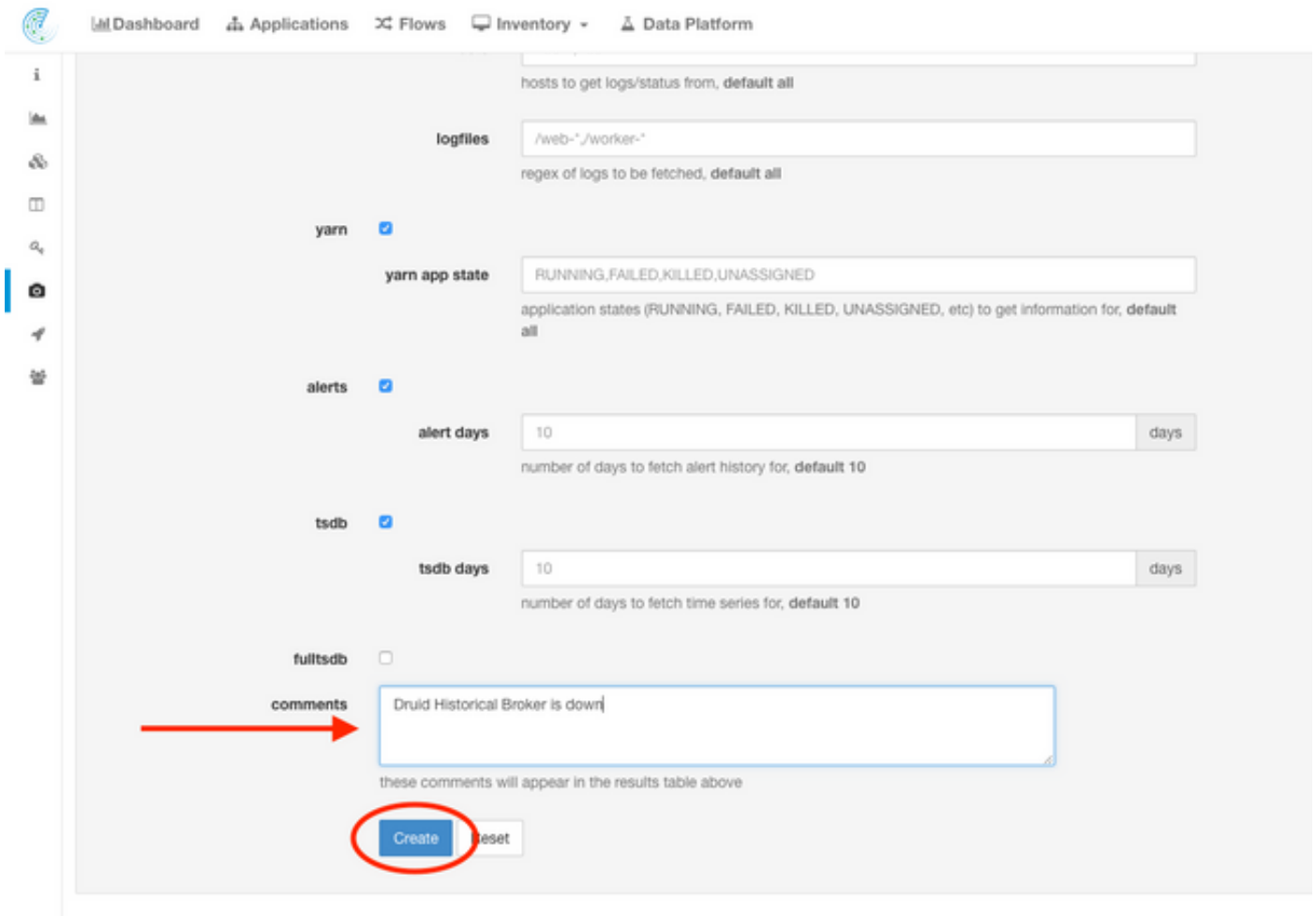
Die Snapshot-Seite befindet sich im Menü Maintenance (Wartung), das über das Einstellungs-Pulldown-Menü verfügbar ist. (**Einstellungen > Wartung**; Snapshots in der linken Spalte).

Hinweis: Nur das Symbol wird angezeigt, bis Sie auf die linke Spalte klicken.



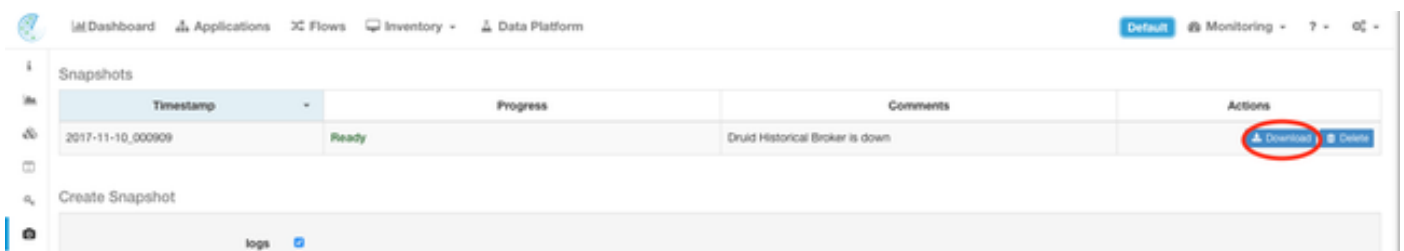
Die Snapshot-Seite bietet verschiedene Optionen zur Auswahl, aber wenn Sie nicht von einem TAC-Techniker angewiesen werden, können die Standardwerte zum Erfassen des Snapshots verwendet werden.

Ein wichtiger Bereich, der geändert werden muss, sind **Kommentare**. Kommentare sollten Informationen bereitstellen, um anzugeben, warum der Snapshot erfasst wurde, wenn mehrere Snapshots vom Cluster gesammelt wurden, und der hinzugefügte Kommentar auch im Snapshot während der Analyse durch das Cisco TAC verfügbar ist.



Wenn auf die Schaltfläche **Erstellen** geklickt wird, beginnt der Snapshot-Prozess. Es kann jeweils nur ein Snapshot erstellt werden. Der Vorgang kann einige Minuten in Anspruch nehmen. Eine Statusanzeige für die Snapshot-Sammlung wird oben auf der Snapshot-Seite angezeigt.

Der Snapshot kann dann auf das lokale System des Benutzers heruntergeladen werden, wenn Sie auf den entsprechenden Download-Link auf der Snapshot-Seite geklickt haben, wie im Bild gezeigt:



Hinweis: Die Snapshot-Datei kann eine Größe von bis zu mehreren hundert Megabyte haben. Diese Datei kann dann in das offene TAC-Ticket hochgeladen werden.

Zugehörige Informationen

- [Unterstützung für Cisco Tetration Analytics](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)