Cisco Telemetry Broker

Hardware-Appliance-Installations- und Konfigurationshandbuch 2.0.1

Inhalt

Einführung

Übersicht

In diesem Handbuch wird die Installation des Cisco Telemetry Broker TB2300 erläutert. Diese Anleitung beschreibt auch die Montage und Installation der Cisco Telemetry Broker-Hardware. Beachten Sie, dass Cisco Telemetry Broker in diesem Dokument manchmal als CTB bezeichnet wird.

> ⚠ Lesen Sie vor der Installation des Broker-Knotens TB2300 die das Dokument zu gesetzlichen Auflagen und Sicherheitshinweisen.

Matrix zu unterstützten Hardware- und Softwareversionen

Appliance	Plattform	Gen.	v2.0
Broker-Knoten TB2300	UCSC-C220	M6	●

Diese Legende erleichtert das Verständnis der Matrix zu unterstützten Hardware- und Softwareversionen.

Symbol	Beschreibung
●	Auf dieser Hardware volle Leistung
○	Unterstützt, aber Leistung nicht optimal
x	Nicht unterstützt

Zielgruppe

Dieses Handbuch richtet sich an die Person, die für die Installation der Cisco Telemetry Broker-Hardware verantwortlich ist. Wir gehen davon aus, dass Sie bereits über Grundkenntnisse in der Installation von Netzwerkgeräten verfügen.

Wenn Sie es vorziehen, mit einem unserer Installationsfachleute zusammenzuarbeiten, wenden Sie sich bitte an Ihren Cisco Partner vor Ort oder an den Cisco Support.

Installieren von virtuellen Broker-Knoten

Wenn Sie virtuelle Broker-Knoten installieren möchten, befolgen Sie die Anweisungen aus dem Bereitstellungs- und Konfigurationshandbuch für die Cisco Telemetry Broker Virtual Appliance.

Terminologie

In diesem Handbuch wird manchmal der Begriff „**Appliance**“ für den Broker-Knoten TB2300 verwendet.

Ein „**Hochverfügbarkeits-Cluster**“ ist eine Gruppe von Broker-Knoten, die von einem Manager-Knoten verwaltet werden.

Häufige Abkürzungen

Die folgenden Abkürzungen werden in diesem Handbuch verwendet:

Abkürzung	Beschreibung
CIMC	Cisco Integrated Management Controller
DNS	Domain Name Server/Service
FTP	File Transfer Protocol
Gbit/s	Gigabit pro Sekunde
GB	Gigabyte
HTTPS	Hypertext Transfer Protocol (Secure)
Mbit/s	Megabit pro Sekunde
NAT	Network Address Translation
NIC	Netzwerkkarte
NTP	Network Time Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer

Abkürzung	Beschreibung
SSH	Secure Shell
TAP	Test Access Port
UDPD	UDP Director
USV	Unterbrechungsfreie Stromversorgung
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine

Konzepte und Architektur

Cisco Telemetry Broker ermöglicht das Erfassen von Netzwerktelemetrie aus vielen Eingängen, das Transformieren des Telemetrieformats und das Weiterleiten dieser Telemetrie an eines oder mehrere Ziele. In der folgenden Tabelle finden Sie Beispiele.

> Derzeit ist die einzige Hardware-Appliance für Cisco Telemetry Broker ein Broker-Knoten (TB2300). Dieser muss für die Bereitstellung mit einem VM-Manager-Knoten gekoppelt werden.
>
> Sie können eine Kombination aus virtuellen und physischen Broker-Knoten bereitstellen, aber auch ausschließlich virtuelle oder ausschließlich physische Broker-Knoten.
>
> Es gibt keine erforderliche Installationsreihenfolge für Broker-Knoten, selbst wenn Sie eine Kombination aus virtuellen und physischen Broker-Knoten bereitstellen.

Sie können folgende Telemetriedaten erfassen:	**Diese Telemetrie können Sie an eines oder alle der folgenden Ziele weiterleiten:**
• Lokale Netzwerktelemetrie, einschließlich NetFlow, Syslog und IPFIX • Cloud-basierte Telemetrieeingaben wie Flow-Protokolle von Amazon Web Services (AWS) Virtual Private Cloud (VPC)	• Analyseplattformen wie Cisco Secure Network Analytics oder Cisco Secure Cloud Analytics • Netzwerkmanagement- und Automatisierungsplattformen wie Cisco DNA Center • Security Information and Event Management(SIEM)-Plattformen

Um dies zu erreichen, müssen Sie einen oder mehrere Cisco Telemetry Broker-Knoten bereitstellen, die Telemetrie erfassen und an die konfigurierten Ziele weiterleiten.

Cisco Telemetry Broker ist sofort einsatzbereit und unterstützt von Anfang an die folgenden Transformationen:

Format der erfassten Daten	Format der weitergeleiteten Daten
VPC-Flow-Protokolle	IPFIX
Flow-Protokolle der Microsoft Network Security Group (NSG)	IPFIX
IPFIX, NetFlow v5, NetFlow v9	JSON (nur bei SCA-Zielen)

Ihre Broker-Knoten werden alle von einem Cisco Telemetry Broker-Manager verwaltet. Sie können sich beim Web-Interface dieses Managers anmelden und verschiedene Konfigurationsaufgaben durchführen, z. B. die Verwaltung der Broker-Knoten, das Einrichten der Weiterleitungsregeln, das Erstellen von Benutzern und das Überprüfen der Nutzung im Dashboard.

Implementierungsanforderungen

Bevor Sie beginnen, lesen Sie diesen Leitfaden, um den Prozess sowie die Vorbereitung, den Zeitaufwand und die Ressourcen zu verstehen, die Sie für die Planung der Installation benötigen.

Matrix der unterstützten Hardware- und Softwareversionen

In der Matrix zu unterstützten Hardware- und Softwareversionen erfahren Sie mehr zum Thema Kompatibilität. Die Matrix ist in diesem Handbuch im Kapitel **Einführung** dokumentiert.

Spezifikationen

Laden Sie das Datenblatt für den Broker-Knoten TB2300 herunter, den Sie installieren möchten.

Cisco Integrated Management Controller (CIMC)

Nachdem Sie Ihre Appliances installiert haben, stellen Sie sicher, dass Sie den Cisco Integrated Management Controller (CIMC) konfigurieren, um den Zugriff auf die Serverkonfiguration und eine virtuelle Serverkonsole zu ermöglichen. Sie können den CIMC auch zum Monitoring der Hardwareintegrität verwenden.

- **Anweisungen:** Beachten Sie die Informationen unter **Verbinden mit CIMC** und befolgen Sie die Anweisungen im Konfigurationsleitfaden für die GUI des Integrated Management Controllers der Cisco UCS C-Series.
- **Standardkennwort:** Melden Sie sich bei der Erstkonfiguration beim CIMC als Administrator an und geben Sie **password** in das Kennwortfeld ein.
- **Kennwortanforderungen:** Ändern Sie nach der Anmeldung das Standardkennwort, um die Sicherheit Ihres Netzwerks zu gewährleisten.

Migrieren der Konfiguration zu einem neuen System

Führen Sie die folgenden Prozesse aus, um die CTB-Konfigurationsregeln, die Sie im Cisco Telemetry Broker Manager eingerichtet haben, zu sichern und wiederherzustellen.

- UDPD-Kunden können ihre vorhandene UDPD-Konfiguration zu Cisco Telemetry Broker migrieren. Weitere Informationen finden Sie im Benutzerhandbuch für Cisco Telemetry Broker im Abschnitt zum Importieren und Exportieren der UDP Director-Konfiguration.

Sichern der CTB-Konfigurationsregeln

Führen Sie den folgenden Befehl auf dem CTB-Manager-Knoten aus:

```
$ sudo ctb-backup-config -v -f ctb_config.json
```

Wenn dieser Prozess abgeschlossen ist, werden die Konfigurationsregeln in der Datei unter „~/.ctb_config.json“ gesichert. Danach können Sie die Konfigurationsregeln an einen anderen Speicherort kopieren.

- VPC-/NSG-Flow-Protokollregeln werden nicht gesichert. Daher müssen Sie diese Regeln bei der Migration zu einem neuen System neu erstellen.
- Sie können Ihre CTB-Konfigurationsregeln nur innerhalb derselben Version sichern und wiederherstellen. Wenn Sie dies versionsübergreifend versuchen, kann der Prozess fehlschlagen.

Wiederherstellen der CTB-Konfigurationsregeln

> ⚠ Schließen Sie zunächst `ctb-install --init` auf dem Manager-Knoten ab und führen Sie anschließend `ctb-restore-config` aus. Wenn Sie ein GUI-Anmeldekonto manuell erstellen, wird es durch die Kontoinformationen aus `ctb-restore-config` überschrieben.

Führen Sie diese Schritte aus:

1. Melden Sie sich als *Installationsbenutzer* ab.
2. Kopieren Sie die Datei **ctb-config.json** von einem vorhandenen System.
3. Melden Sie sich beim neuen System als *admin* an.
4. Führen Sie den folgenden Befehl auf dem CTB-Manager-Knoten aus:

```
$ sudo ctb-restore-config -v -f ctb_config.json
```

Die Eingaben, die Sie Cisco Telemetry Broker aufgrund der Wiederherstellung hinzufügen, werden keinem Knoten oder Cluster zugewiesen. Sie müssen sie nach Bedarf zuweisen.

1. Konfigurieren Ihrer Firewall für die Kommunikation

Damit die Appliances richtig kommunizieren können, sollten Sie das Netzwerk so konfigurieren, dass Firewalls oder Zugriffskontrolllisten die erforderlichen Verbindungen nicht blockieren. Verwenden Sie die Informationen in diesem Abschnitt, um Ihr Netzwerk so zu konfigurieren, dass die Appliances über das Netzwerk kommunizieren können.

Öffnen der Kommunikations-Ports

Die folgende Tabelle enthält Details zu allen Netzwerkverbindungen zu und von Ihren Cisco Telemetry Broker-Appliances. Um sicherzustellen, dass Ihr Netzwerk diese Verbindungen zulässt, müssen Sie die geltenden Zugriffskontrollen ändern (z. B. Ihre Firewall).

Client	Server	Port	Beschreibung
Benutzer	Broker-Knoten und Manager-Knoten	22/TCP	SSH-Zugriff auf die Konsole
Manager	Externes Internet	443/TCP	HTTPS für sichere externe Kommunikation, z. B. Smart Licensing und Software-Updates
Manager	Kunden-Syslog-Server	Vom Kunden definierter Port	Syslog-Telemetrie für Cisco Telemetry Broker-Benachrichtigungen
Manager	Kunden-SMTP-Server	Vom Kunden definierter Port	SMTP-Telemetrie für Cisco Telemetry Broker-Benachrichtigungen
Jeder Broker-Knoten	Manager	443/TCP	HTTPS für sichere Managementverbindungen

Jeder Broker-Knoten	Externes Internet	443/TCP	HTTPS zum Abrufen von VPC-/NSG-Flow-Protokollen aus AWS S3- bzw. Azure SAS-Speicher-Buckets HTTPS für Broker-Knoten, um den Zugriff auf den SCA-Server zu sichern und Dateien in den SCA S3-Bucket hochzuladen
Benutzer	Manager	443/TCP	HTTPS für sicheren Zugriff auf das Web-Interface
Broker-Knoten und Manager-Knoten	Kunden-DNS-Server	53/UDP	DNS-Telemetrie
Jeder *Hardware*-Broker-Knoten	Kunden-NTP-Server	123	NTP-Daten für die Zeitsynchronisierung

Darüber hinaus müssen Sie Ports basierend auf dem an einen Broker-Knoten gesendeten Telemetrietyp und dem von einem Broker-Knoten an ein Ziel gesendeten Telemetrietyp öffnen. Die folgende Tabelle enthält Details zu gängigen Ports für verschiedene Telemetrietypen:

Port	**Beschreibung**
514/UDP	syslog
2055/UDP	NetFlow v5, NetFlow v9
4739/UDP	IPFIX
6343/UDP	sFlow

2. Installationswarnungen und Richtlinien

Installationswarnungen

Lesen Sie vor dem Installieren von Cisco Telemetry Broker-Appliances das Dokument zu gesetzlichen Auflagen und Sicherheitshinweisen.

Beachten Sie die folgenden Warnhinweise:

Anweisung 1071 – Definition der Warnhinweise

WICHTIGE SICHERHEITSANWEISUNGEN

Dieses Warnsymbol weist auf eine Gefahr hin. Sie befinden sich möglicherweise in einer Situation, in der es zu körperlichen Verletzungen kommen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung von Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE ANWEISUNGEN SICHER AUF.

Anweisung 1004 – Installationsanweisungen

Lesen Sie die Installationshinweise, bevor Sie das System nutzen, installieren oder an die Stromversorgung anschließen.

Anweisung 12 – Warnhinweis zum Trennen der Stromversorgung

Bevor Sie an einem Chassis oder in der Nähe von Netzteilen arbeiten, ziehen Sie von AC-Geräten das Netzkabel ab, oder trennen Sie bei DC-Geräten die Stromversorgung am Leitungsschutzschalter.

Anweisung 43 – Warnhinweis zum Ablegen von Schmuck

Bevor Sie an Geräten arbeiten, die mit Stromleitungen verbunden sind, legen Sie Ihren Schmuck ab (einschließlich Ringe, Halsketten und Uhren). Metallobjekte erhitzen sich bei der Verbindung mit Strom und Masse und können schwere Verbrennungen verursachen, oder das Metall kann mit den Terminals verschmelzen.

Anweisung 94 – Warnhinweis zu Armbändern

Tragen Sie bei diesem Verfahren Erdungsarmbänder, um Schäden an der Karte durch elektrostatische Entladungen zu vermeiden. Berühren Sie die Backplane nicht mit der Hand oder einem Metallwerkzeug, da Sie sonst einen Stromschlag bekommen können.

Anweisung 1045 – Kurzschlusssicherung

Dieses Produkt muss im Rahmen der Gebäudeinstallation mit einer Kurzschlusssicherung (Überstromschutz) versehen sein. Installieren Sie es nur in Übereinstimmung mit den nationalen und lokalen Verkabelungsvorschriften.

Anweisung 1021 – SELV-Schaltkreise

Zur Vermeidung von Stromschlägen sollten Sie keine Sicherheitskleinspannungs-Schaltkreise (SELV) an Telefonnetz-Schaltkreise (TNV) anschließen. LAN-Ports verfügen über SELV-Schaltkreise, WAN-Ports über TNV-Schaltkreise. In manchen Fällen verwenden sowohl LAN- als auch WAN-Ports RJ-45-Steckverbinder. Gehen Sie beim Anschluss von Kabeln vorsichtig vor.

Anweisung 1024 – Erdungsleiter

Dieses Gerät muss geerdet sein. Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an die zuständige Inspektionsbehörde oder eine/n ElektrikerIn.

Anweisung 1040 – Entsorgung des Produkts

Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.

Anweisung 19 – Warnung TN-Stromversorgung

Das Gerät ist mit TN-Stromversorgungssystemen kompatibel.

Installationsrichtlinien

Beachten Sie die folgenden Warnhinweise:

Anweisung 1047 – Schutz vor Überhitzung

Um das System vor Überhitzung zu schützen, vermeiden Sie dessen Verwendung in Bereichen, in denen die Umgebungstemperatur außerhalb des folgenden Bereichs liegt: 5 bis 35 °C.

Anweisung 1019 – Primäre Ausschaltvorrichtung

Die Stecker-Steckdosen-Kombination muss jederzeit zugänglich sein, da sie zum Ausschalten des Geräts dient.

Anweisung 1005 – Leitungsschutzschalter

Dieses Produkt ist für Gebäude mit Kurzschlusssicherung (Überstromschutz) gedacht. Stellen Sie sicher, dass der Nennwert der Schutzvorrichtung folgende Werte nicht überschreitet: USA 120 V, 15 A (EU: 250 V, 16 A)

Anweisung 1074 – Übereinstimmung mit örtlichen und nationalen elektrischen Richtlinien und Bestimmungen

Die Installation des Geräts muss in Übereinstimmung mit den örtlichen und nationalen elektrischen Richtlinien und Bestimmungen erfolgen.

Anweisung 371 – Netzkabel und Netzteil

Nutzen Sie für die Installation des Produkts die mitgelieferten oder vorge-

sehenen Verbindungskabel/Netzkabel/AC-Adapter/Batterien. Die Nutzung anderer Kabel oder Adapter kann Funktionsstörungen oder einen Brand verursachen. Das (japanische) Gesetz zur Sicherheit von Elektrogeräten und elektrischem Material verbietet die Nutzung von zertifizierten Kabeln (bei denen im Code „UL“ steht) für andere elektrische Geräte, als die von Cisco festgelegten Produkte. Diese müssen stattdessen das PSE-Zeichen auf dem Kabel aufweisen.

Anweisung 1073 – Keine vom Benutzer zu wartenden Teile

Innen befinden sich keine vom Benutzer zu wartenden Teile. Nicht öffnen.

Beachten Sie bei der Installation des Chassis die folgenden Richtlinien:

- Stellen Sie sicher, dass um das Chassis herum genügend Platz für Wartungsarbeiten und für eine ausreichende Belüftung bleibt. Der Luftstrom im Chassis fließt von vorne nach hinten.

Um einen einwandfreien Luftstrom zu gewährleisten, muss Ihr Chassis mit Gleitschienen-Sätzen montiert werden. Das Übereinanderstapeln der Einheiten oder das Stapeln ohne Verwendung der Gleitschienen-Sätze blockiert die Lüftungsöffnungen auf dem Chassis, was zu Überhitzung, höheren Lüfterdrehzahlen und einem höheren Stromverbrauch führen kann. Wir empfehlen Ihnen, Ihr Chassis beim Einbau in das Rack auf Gleitschienen zu montieren, da diese Schienen den erforderlichen Mindestabstand zwischen den Chassis gewährleisten. Bei der Montage mit Gleitschienen-Sätzen ist kein zusätzlicher Abstand zwischen den Chassis erforderlich.

- Stellen Sie sicher, dass die Klimaanlage das Chassis auf einer Temperatur von 5 bis 35 °C halten kann.
- Stellen Sie sicher, dass der Schrank oder das Rack den Rack-Anforderungen entspricht.
- Stellen Sie sicher, dass die Stromversorgung am Standort die im Datenblatt Ihrer Appliance aufgeführten Stromversorgungsbedingungen erfüllt. Sie können eine USV zum Schutz vor Stromausfällen verwenden (falls verfügbar).

Vermeiden Sie USV-Modelle mit Ferroresonanztechnologie. Diese USV-Modelle können bei der Verwendung mit solchen Systemen, die aufgrund von stoßartigen Datenverkehrsmustern erhebliche Schwankungen im Stromverbrauch aufweisen können, instabil werden.

Sicherheitshinweise

Beachten Sie zu Ihrer eigenen Sicherheit und zum Schutz des Chassis die folgenden Informationen. Darin werden möglicherweise nicht alle potenziell gefährlichen Situationen in Ihrer Arbeitsumgebung abgedeckt. Seien Sie daher wachsam, und lassen Sie stets Vorsicht walten.

Beachten Sie die folgenden Sicherheitsrichtlinien:

- Halten Sie den Bereich vor, während und nach der Installation sauber und staubfrei.
- Legen Sie Ihre Werkzeuge nicht in Gangflächen ab, wo Sie oder andere darüber stolpern könnten.
- Tragen Sie keine losen Kleidungsstücke oder Schmuck, wie Ohrringe, Armbänder oder Halsketten, die sich im Chassis verfangen könnten.
- Tragen Sie bei Arbeiten unter Bedingungen, die möglicherweise die Augen gefährden, eine Schutzbrille.
- Unterlassen Sie alles, was eine Gefahr für Personen darstellen kann oder die Sicherheit des Geräts beeinträchtigt.
- Versuchen Sie niemals, ein Objekt anzuheben, das für eine Person allein zu schwer ist.

Sicherheit bei Arbeiten mit Elektrizität

> ⚠ Bevor Sie an einem Chassis arbeiten, stellen Sie sicher, dass das Netzkabel abgezogen ist.

Befolgen Sie bei Arbeiten an mit elektrischem Strom betriebenen Geräten diese Richtlinien:

- Arbeiten Sie nicht allein, wenn an Ihrem Arbeitsplatz potenziell gefährliche Bedingungen vorhanden sind.
- Nehmen Sie niemals an, dass die Stromversorgung getrennt ist. Überprüfen Sie dies stets.
- Suchen Sie sorgfältig nach möglichen Gefahren in Ihrem Arbeitsbereich, z. B. feuchten Böden, nicht geerdeten Verlängerungskabeln, durchgescheuerten Netzkabeln und fehlenden Schutzerdungen.
- Bei einem elektrischen Unfall:
    - Seien Sie vorsichtig, und werden Sie nicht selbst zum Opfer.
    - Trennen Sie die Stromversorgung des Systems.

    - Wenn möglich, bitten Sie eine andere Person, den Rettungsdienst zu rufen. Versuchen Sie andernfalls, den Zustand des Opfers einzuschätzen, und holen Sie dann Hilfe.
    - Bestimmen Sie, ob die Person Mund-zu-Mund-Beatmung oder eine Herzmassage benötigt; ergreifen Sie dann die geeigneten Maßnahmen.
- Verwenden Sie das Chassis mit der angegebenen Spannung und wie im Benutzerhandbuch angegeben.

Vermeidung von Schäden durch ESD

ESD tritt auf, wenn elektronische Komponenten nicht ordnungsgemäß genutzt werden. Dadurch können Geräte und elektrische Schaltkreise beschädigt werden und einen temporären oder vollständigen Ausfall Ihrer Geräte verursachen.

Beachten Sie immer die Vorgehensweisen zur Vermeidung von Schäden durch elektrostatische Entladung, wenn Sie Komponenten ausbauen und ersetzen. Stellen Sie sicher, dass das Chassis geerdet ist. Verwenden Sie immer ein antistatisches Armband und stellen Sie guten Hautkontakt sicher. Verbinden Sie die Erdungsklemme mit einer unlackierten Fläche am Chassis-Rahmen, um ESD-Spannungen sicher zu erden. Zum zuverlässigen Schutz vor Beschädigungen durch ESD und vor Stromschlägen müssen das Armband und der Leiter wirksam funktionieren. Wenn kein Armband verfügbar ist, erden Sie sich durch Berühren des Metallteils am Chassis.

Überprüfen Sie zu Ihrem Schutz regelmäßig den Widerstandswert des antistatischen Armbands. Er sollte zwischen einem und 10 Megohm liegen.

Standortumgebung

Planen Sie das Layout des Standorts und die Positionen der Geräte sorgfältig, um Geräteausfälle zu vermeiden und die Wahrscheinlichkeit umgebungsbedingter Systemabschaltungen zu verringern. Sollte es bei Ihren derzeitigen Geräten zu Systemabschaltungen oder ungewöhnlich hohen Fehlerraten kommen, können Sie mithilfe dieser Empfehlungen die Ursache der Ausfälle lokalisieren und künftige Probleme vermeiden.

Überlegungen zur Stromversorgung

Beachten Sie bei der Installation des Chassis Folgendes:

- Vergewissern Sie sich vor der Installation des Chassis, dass die Stromversorgung am Standort frei von Spitzen und Störungen ist. Installieren Sie bei Bedarf ein Netzschutzgerät, um ein angemessenes Spannungs- und Stromniveau in der Eingangsspannung der Appliance sicherzustellen.

- Installieren Sie eine geeignete Erdung für den Standort, um Schäden durch Blitzschlag und Stromanstiege zu vermeiden.
- Der Betriebsbereich des Chassis kann nicht durch den Benutzer festgelegt werden. Entnehmen Sie die korrekten Eingangsstromanforderungen der Appliance dem Etikett auf dem Chassis.
- Es stehen verschiedene Arten von Wechselstrom-Netzkabel für die Appliance zur Verfügung. Vergewissern Sie sich, dass Ihnen das korrekte Kabel für Ihren Standort vorliegt.
- Falls Sie doppelte redundante (1+1) Netzteile verwenden, empfehlen wir Ihnen die Nutzung unabhängiger Stromkreise für jedes der Netzteile.
- Installieren Sie, falls möglich, eine unterbrechungsfreie Stromversorgung für Ihren Standort.

Überlegungen zur Rack-Konfiguration

Beachten Sie beim Planen der Rack-Konfiguration die folgenden Punkte:

- Wenn Sie ein Chassis in einem offenen Rack montieren, stellen Sie sicher, dass der Rack-Rahmen die Ein- und Auslassöffnungen nicht blockiert.
- Stellen Sie sicher, dass geschlossene Racks ausreichend belüftet werden. Stellen Sie sicher, dass das Rack nicht zu voll ist, da jedes Chassis Wärme erzeugt. Ein geschlossenes Rack sollte seitliche Luftschlitze und einen Lüfter haben, um Kühlluft zur Verfügung zu stellen.
- In einem geschlossenen Rack mit einem Lüfter oben kann die von Geräten im unteren Bereich des Racks erzeugte Wärme in die Einlassöffnungen der darüber-liegenden Einheiten gezogen werden. Stellen Sie sicher, dass Einheiten im unteren Bereich des Racks ausreichend belüftet werden.
- Leitbleche können dazu beitragen, Abluft von der Ansaugluft zu trennen, was auch die Kühlluftzirkulation durch das Chassis verbessert. Die beste Platzierung der Leitbleche hängt von den Luftstrommustern im Rack ab. Probieren Sie verschiedene Varianten aus, um die beste Position für die Leitbleche zu finden.

3. Montage Ihrer Appliances

Sie können Cisco Telemetry Broker-Appliances direkt in einem Standard-19"-Rack oder -Schrank, einem anderen geeigneten Schrank oder auf einer ebenen Fläche montieren. Wenn Sie eine Appliance in einem Rack oder Schrank montieren, befolgen Sie die Anweisungen zu den Gleitschienen-Sätzen. Bei der Bestimmung des Aufstellungsortes einer Appliance ist auf folgenden Abstand zur Vorder- und Rückseite zu achten:

- Die Anzeigen auf der Vorderseite sind gut ablesbar.
- Der Zugang zu den Ports an der Rückseite ist für eine problemlose Verkabelung ausreichend.
- Der Netzanschluss an der Rückseite befindet sich in Reichweite einer konditionierten Wechselstromquelle.
- Der Luftstrom rund um die Appliance und durch die Lüfter ist unbeschränkt.

Im Lieferumfang der Appliance enthaltene Hardware

Die folgende Hardware ist im Lieferumfang der Cisco Telemetry Broker-Appliances enthalten:

- Wechselstromkabel
- Zugangsschlüssel (für Frontplatte)
- Gleitschienen-Satz für die Rackmontage oder Montagelaschen für kleinere Appliances

Zusätzlich erforderliche Hardware

Sie müssen die folgende zusätzlich erforderliche Hardware bereitstellen:

- Befestigungsschraube für ein Standard-19“-Rack
- Unterbrechungsfreie Stromversorgung (USV) für den Broker-Knoten TB2300, den Sie installieren
- Um lokal zu konfigurieren (optional), verwenden Sie eine der folgenden Methoden:
    - Laptop mit einem Videokabel und einem USB-Kabel (für die Tastatur)
    - Videomonitor mit einem Videokabel und Tastatur mit einem USB-Kabel

4. Verbinden Ihrer Appliances mit dem Netzwerk

1. Spezifikationen prüfen

Verwenden Sie das gleiche Verfahren, um jeden Broker-Knoten TB2300 mit dem Netzwerk zu verbinden. Der einzige Unterschied für den Anschluss ist die Art von Appliance, die Sie haben.

- **Datenblätter:** Detaillierte Informationen finden Sie in den Cisco Telemetry Broker -Datenblättern.
- **UCS-Plattform:** Der Cisco Telemetry Broker TB2300 verwendet die UCS-Plattform UCSC-C225-M6SX.

> ⚠ Aktualisieren Sie das Appliance-BIOS nicht, da dies zu Problemen mit der Appliance-Funktionalität führen kann.

2. Verbinden Ihrer Appliance mit dem Netzwerk

So verbinden Sie Ihre Appliance mit Ihrem Netzwerk:

1. Verbinden Sie ein Ethernet-Kabel mit dem Management-Port, wie im Datenblatt beschrieben.
2. Verbinden Sie ein Ethernet-Kabel mit dem Telemetrie-Port, wie im Datenblatt beschrieben.
    - Stellen Sie sicher, dass der Managementport mit dem Management-Netzwerk und der Telemetrie-Port mit dem Telemetrie-Netzwerk verbunden ist. Weitere Informationen finden Sie im nächsten Abschnitt, Ermitteln der Netzwerkkonfiguration.
3. Verbinden Sie das jeweils andere Ende der Ethernetkabel mit dem Switch/den Switches Ihres Netzwerks.
4. Verbinden Sie die Netzkabel mit dem Netzteil. Einige Appliances verfügen über zwei Stromanschlüsse: Netzteil 1 und Netzteil 2.

Ermitteln der Netzwerkkonfiguration

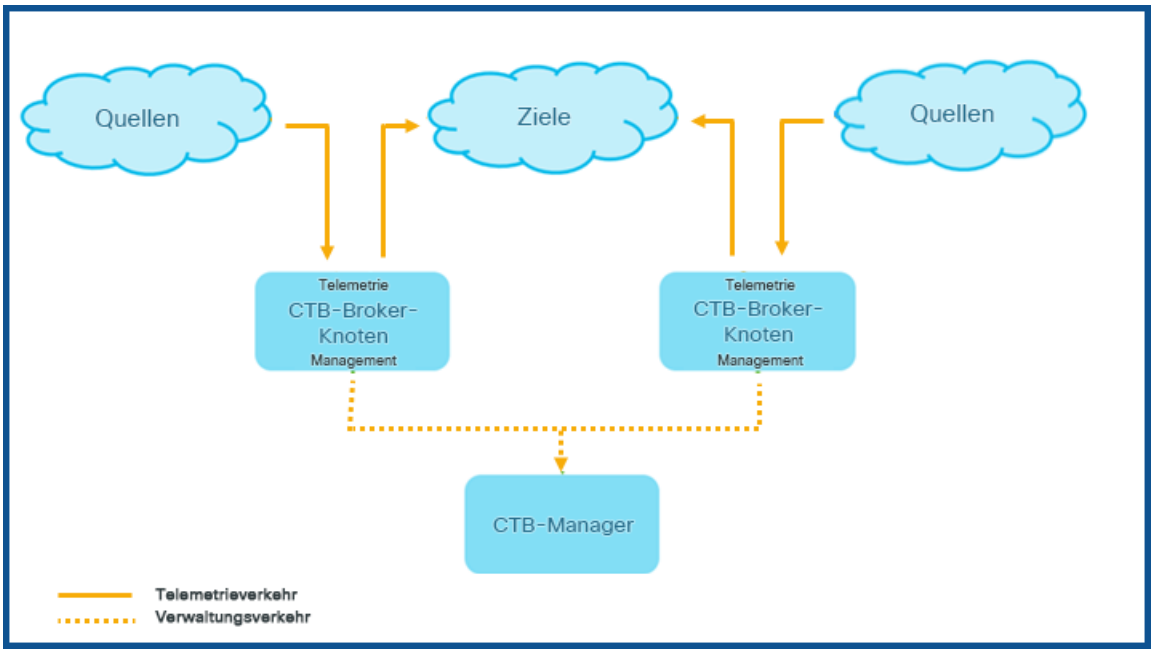
Cisco Telemetry Broker unterstützt Setups mit mehreren Knoten, wobei ein einzelner Cisco Telemetry Broker-Manager mehrere Broker-Knoten verwalten kann. Da Cisco Telemetry Broker jeden Broker-Knoten mit allen Zielen und Regeln aktualisiert, müssen Sie Ihre Konfiguration sorgfältig planen, um die unten aufgeführten gängigen Probleme zu vermeiden.

- Sie können Broker-Knoten in verschiedenen Telemetriesegmenten bereitstellen, in denen die Telemetrieschnittstellen der einzelnen Broker-Knoten möglicherweise nicht über das Netzwerk zugänglich sind. Gehen Sie bei der Erstellung der Regeln mit besonderer Sorgfalt vor, damit Pakete eines Exporters, die einen bestimmten Knoten erreichen, nicht an Ziele weitergeleitet werden, auf die von diesem Knoten aus nicht zugegriffen werden kann. Daher müssen Sie Regeln erstellen, die Exporter ausschließen, die dieses Routing-Problem verursachen könnten. Beispielsweise dürfen Sie keine Standardregeln verwenden, da diese mit allen Eingaben übereinstimmen.
- Möglicherweise sind nicht alle Ziele für jeden Broker-Knoten relevant. Mit der Funktion zum Prüfen der Zielerreichbarkeit können jedoch die Broker-Knoten widersprüchliche Informationen an den Manager melden, da jeder Broker-Knoten versucht, die Zugänglichkeit für jedes Ziel zu ermitteln. Wenn die Möglichkeit besteht, dass einige Broker-Knoten keine Verbindung zu bestimmten Zielen herstellen können, deaktivieren Sie die Option zum Prüfen der Zielerreichbarkeit für diese Ziele.

Wenn Sie von UDP Director zu Cisco Telemetry Broker migrieren, müssen Sie vor der Bereitstellung des Manager-Knotens und der Broker-Knoten planen, wie Sie den Manager-Knoten und die Broker-Knoten mit dem Netzwerk verbinden, da sich die Konfigurationen von Cisco Telemetry Broker und UDP Director unterscheiden.

Cisco Telemetry Broker unterscheidet zwischen Telemetrieverkehr und Verwaltungsverkehr. Der Broker-Knoten verfügt über zwei Schnittstellen: die Telemetrie-Netzwerkschnittstelle und die Management-Netzwerkschnittstelle. Der Manager-Knoten verfügt nur über die Management-Netzwerkschnittstelle. Das folgende Diagramm zeigt, wie der Manager-Knoten und die Broker-Knoten logisch bereitgestellt werden.

> Beachten Sie, dass die Beispiele bei diesem Thema typische Bereitstellungsszenarien darstellen. Wenden Sie sich an Ihre NetzwerkadministratorInnen, um zu erfahren, wie Sie eine erweiterte Bereitstellung (z. B. mit VLANs) einrichten.



Cisco Telemetry Broker empfängt Verwaltungsverkehr *nur* über die Management-Netzwerkschnittstelle. Diese Schnittstelle wird für die gesamte Kommunikation zwischen dem Broker- und dem Manager-Knoten verwendet. Telemetrieverkehr wird hauptsächlich über die Telemetrie-Netzwerkschnittstelle des Broker-Knotens vermittelt. Die einzige Ausnahme bildet das Abrufen von AWS VPC-Flow-Protokollen oder Azure NSG-Flow-Protokollen durch Cisco Telemetry Broker oder das Senden von Telemetrie-daten an SCA durch Cisco Telemetry Broker. Beides erfolgt über die Management-Netzwerkschnittstelle des Broker-Knotens.

Sie können den Manager-Knoten an einer beliebigen Stelle im Netzwerk in einem beliebigen Subnetz platzieren. Es muss jedoch eine TCP-Netzwerkverbindung über Port 443 mit den Broker-Knoten gegeben sein.

Sie können für den Broker-Knoten einen der folgenden Bereitstellungsmodi verwenden:

1. Die Telemetrie-Subnetze und die Management-Subnetze sind identisch. In diesem Modus gehören die Telemetrie-Netzwerkschnittstelle und die Management-Netzwerkschnittstelle auf dem Broker-Knoten zum selben Subnetz. Weitere Informationen finden Sie im nächsten Abschnitt, Schnittstellen gehören zum selben Subnetz.
2. Da sich die Telemetrie-Subnetze und die Management-Subnetze unterscheiden, belässt der Broker-Knoten seine Telemetrie-Netzwerkschnittstelle und seine Management-Netzwerkschnittstelle in zwei separaten Subnetzen. Weitere Informationen finden Sie im übernächsten Abschnitt, Schnittstellen gehören zu unterschiedlichen Subnetzen.

Die Bereitstellung separater Pfade für Telemetrieverkehr und Managementverkehr bietet die folgenden Vorteile:

- Getrennte Pfade erhöhen die Leistung, insbesondere wenn sich die Leistung der Schnittstellen-Leitungsrate nähert, da der Datenverkehr keine Ressourcen gemeinsam nutzen muss.
- Die Trennung von Management- und Telemetrieverkehr ist für eine Netzwerkkonfiguration schlichtweg sinnvoll.

Schnittstellen gehören zum selben Subnetz

Dieser Bereitstellungsmodus ist dem von UDP Director sehr ähnlich. Die Management-Netzwerkschnittstelle und die Telemetrie-Netzwerkschnittstelle sind identisch. Der einzige Unterschied bei diesem ersten Bereitstellungsmodus ist, dass Sie separate IP-Adressen für die Broker-Knoten-Schnittstellen benötigen.

Sie können dies erreichen, indem Sie die Telemetrie-Netzwerkschnittstelle des Broker-Knotens und die Management-Netzwerkschnittstelle mit demselben Subnetz verbinden.

Schnittstellen gehören zu unterschiedlichen Subnetzen

In diesem Bereitstellungsmodus befinden sich die Telemetrie-Netzwerkschnittstelle und die Management-Netzwerkschnittstelle in unterschiedlichen Subnetzen.

5. Verbinden mit Ihrer Appliance

In diesem Abschnitt wird beschrieben, wie Sie eine Verbindung zur Appliance für die Systemkonfiguration herstellen.

Wählen Sie Ihr Verbindungsverfahren aus:

- **Anschluss einer Tastatur und eines Monitors**
- **Anschluss eines seriellen Kabels oder einer seriellen Konsole**
- **Verbinden mit CIMC (für Remote-Zugriff erforderlich)** Nutzen Sie dieses Verbindungsverfahren, um eine Verbindung mit der Appliance für den Remote-Zugriff herzustellen.

Anschluss einer Tastatur und eines Monitors

Gehen Sie wie folgt vor, um die IP-Adresse lokal zu konfigurieren:

1. Stecken Sie das Netzkabel in die Appliance.
2. Drücken Sie den Netzschalter, um die Appliance einzuschalten. Warten Sie, bis der Boot-Vorgang abgeschlossen ist. Unterbrechen Sie den Boot-Vorgang nicht.

> Möglicherweise müssen Sie die Frontplatte entfernen, um die Strom-versorgung herzustellen.
>
> Bei einigen Modellen schalten sich die Lüfter der Stromversorgung ein, während das System nicht eingeschaltet ist. Überprüfen Sie, ob die LED auf der Frontplatte leuchtet.
>
> Achten Sie darauf, die Appliance an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Das Netzteil benötigt Strom; andernfalls zeigt das System einen Fehler an.

3. Schließen Sie die Tastatur an:

    - Wenn Sie eine Standardtastatur haben, schließen Sie sie an den Standard-Tastaturanschluss an.
    - Wenn Sie eine USB-Tastatur besitzen, schließen Sie diese an einen USB-Anschluss an.

4. Schließen Sie das Videokabel an den Videoanschluss an. Die Anmeldeaufforderung wird angezeigt.
5. Weiter mit dem nächsten Kapitel, **6. Konfigurieren Ihres Cisco Telemetry Broker-Systems**.

Anschluss eines seriellen Kabels oder einer seriellen Konsole

Sie können die Appliance mit einem seriellen Kabel oder einer seriellen Konsole, wie z. B. einem Laptop mit Terminal-Emulator, verbinden. Wir verwenden in den Anweisungen einen Laptop als Beispiel.

1. Schließen Sie Ihren Laptop mit einer der folgenden Methoden an die Appliance an:

   - Schließen Sie ein RS232-Kabel vom seriellen Port (DB9) Ihres Laptops an den Konsolen-Port der Appliance an.
   - Verbinden Sie ein Crossover-Kabel vom Ethernet-Port Ihres Laptops mit dem Management-Port der Appliance.

2. Stecken Sie das Netzkabel in die Appliance.
3. Drücken Sie den Netzschalter, um die Appliance einzuschalten. Warten Sie, bis der Boot-Vorgang abgeschlossen ist. Unterbrechen Sie den Boot-Vorgang nicht.

   Möglicherweise müssen Sie die Frontplatte entfernen, um die Stromversorgung herzustellen.

   Bei einigen Modellen schalten sich die Lüfter der Stromversorgung ein, während das System nicht eingeschaltet ist. Überprüfen Sie, ob die LED auf der Frontplatte leuchtet. Achten Sie darauf, die Appliance an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Das Netzteil benötigt Strom; andernfalls zeigt das System einen Fehler an.

4. Stellen Sie auf dem Laptop eine Verbindung zur Appliance her.

   Sie können jeden verfügbaren Terminal-Emulator verwenden, um mit der Appliance zu kommunizieren.

5. Verwenden Sie die folgenden Einstellungen:

    - BPS: 115200
    - Datenbits: 8
    - Stoppbit: 1
    - Parität: Keine
    - Flusskontrolle: keine

    Der Anmeldebildschirm und die Anmeldeaufforderung werden angezeigt.

6. Weiter mit dem nächsten Kapitel, **6. Konfigurieren Ihres Cisco Telemetry Broker-Systems**.

Verbinden mit CIMC (für Remote-Zugriff erforderlich)

Der Cisco Integrated Management Controller (CIMC) ermöglicht den Zugriff auf die Serverkonfiguration und eine virtuelle Serverkonsole sowie das Monitoring des Hardwarezustands.

1. Befolgen Sie die Anweisungen im Konfigurationsleitfaden für die GUI des Integrated Management Controllers der Cisco UCS C-Series.
2. Melden Sie sich bei CIMC als Administrator an und geben Sie **password** in das Kennwortfeld ein.
3. Ändern Sie das Standardkennwort, um die Sicherheit Ihres Netzwerks zu gewährleisten.
4. Weiter mit dem nächsten Kapitel, **6. Konfigurieren Ihres Cisco Telemetry Broker-Systems**.

6. Konfigurieren Ihres Cisco Telemetry Broker-Systems

Wenn Sie die Installation Ihrer Hardware-Appliances abgeschlossen haben, können Sie Cisco Telemetry Broker in einem gemanagten System konfigurieren.

Browseranforderungen

Cisco Telemetry Broker unterstützt die folgenden Browser (getestet mit dem neuesten Rapid Release und einer Auflösung von 1.024 x 768 px):

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Systemkonfigurationsanforderungen

Stellen Sie sicher, dass Sie über CIMC Zugriff auf die Appliance-Konsole haben.

Verwenden Sie die folgende Tabelle, um die erforderlichen Informationen für die Konfiguration aller Broker-Knoten TB2300 bereitzulegen.

Konfigurationsanforderungen	Details
IP-Adresse	Weisen Sie dem Management-Port eine routbare IP-Adresse zu.
Netmask (Netzmaske)	Richten Sie das Subnetz für die ausgewählte IP-Adresse ein.
Gateway	Verweisen Sie auf die Gateway-IP-Adresse Ihres Subnetzes.

Host-Name	Für jeden Broker-Knoten TB2300 ist ein eindeutiger Hostname erforderlich. Eine Appliance kann nicht mit demselben Hostnamen wie ein anderer Broker-Knoten konfiguriert werden. Stellen Sie außerdem sicher, dass jeder Broker-Knoten-Hostname die Internet-standardanforderungen für Internethosts erfüllt.
DNS-Server	Interner DNS-Server zur Namensauflösung
NTP-Server	Interner Zeitserver für die Synchronisierung zwischen Servern. Für jeden Broker-Knoten TB2300 ist mindestens 1 NTP-Server erforderlich.

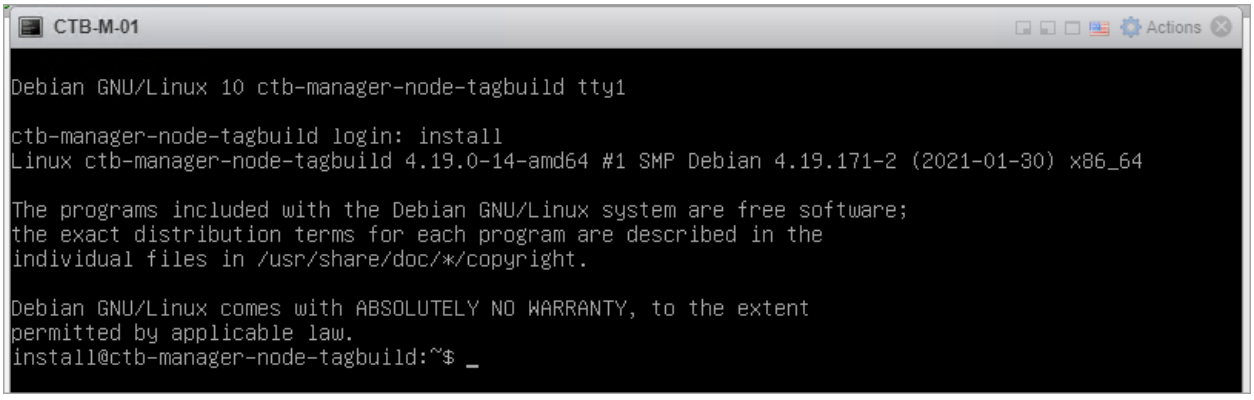
Installieren des Broker-Knotens

Gehen Sie wie nachfolgend beschrieben vor.

> Derzeit ist die einzige Hardware-Appliance für Cisco Telemetry Broker ein Broker-Knoten (TB2300). Dieser muss für die Bereitstellung mit einem VM-Manager-Knoten gekoppelt werden.

1. Anmelden als Installationsbenutzer

Klicken Sie in der CIMC-Konsole auf **vKVM starten**.



2. Ausführen des Befehls „sudo ctb-install --init“

1. Führen Sie den Befehl `sudo ctb-install --init` aus.
2. Geben Sie folgende Informationen ein:

- Kennwort für den **admin**-Benutzer

  Das Kennwort muss die folgenden Anforderungen erfüllen:

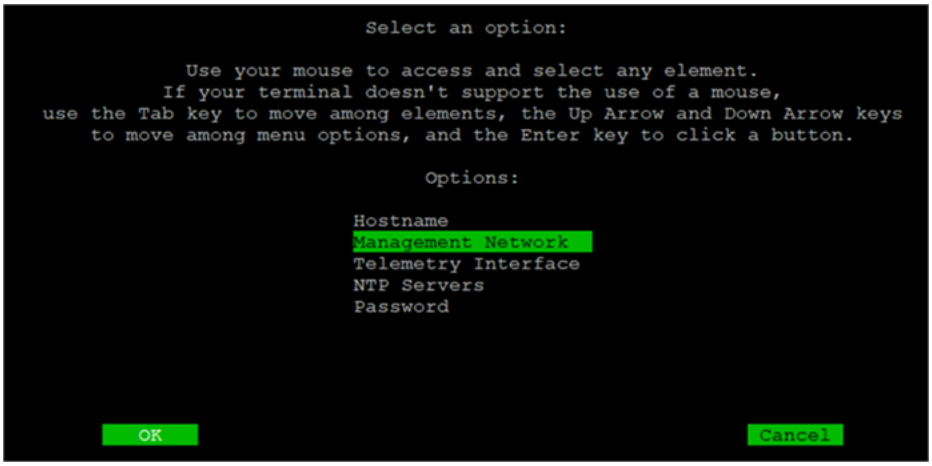
  - Muss mindestens acht Zeichen umfassen
  - Muss mindestens einen Kleinbuchstaben enthalten
  - Muss mindestens einen Großbuchstaben enthalten
  - Muss mindestens eine Ziffer enthalten
  - Muss mindestens eines der folgenden Sonderzeichen enthalten: @ # $ % ^ & * ! + ?
  - Darf kein gängiges Wort und keine typische Abfolge sein
  - Darf nicht mit identifizierenden Attributen des Benutzers (wie dem Benutzernamen) übereinstimmen
- Hostname (max. 255 Zeichen, nur Buchstaben und Ziffern)
- Sie können einen oder beide der folgenden IP-Adressparameter eingeben:
  - IPv4-Adresse, Subnetzmaske und Standardgateway für die Management-Netzwerkschnittstelle
  - IPv6-Adresse, Subnetzmaske und Standardgateway für die Management-Netzwerkschnittstelle
- Gültige DNS-Nameserver-IP-Adresse, die über den Broker-Knoten erreichbar ist (eine oder zwei)
- Gültige NTP-IP-Adresse, die über den Broker-Knoten erreichbar ist

(Optional) Ändern eines einzelnen Parameters

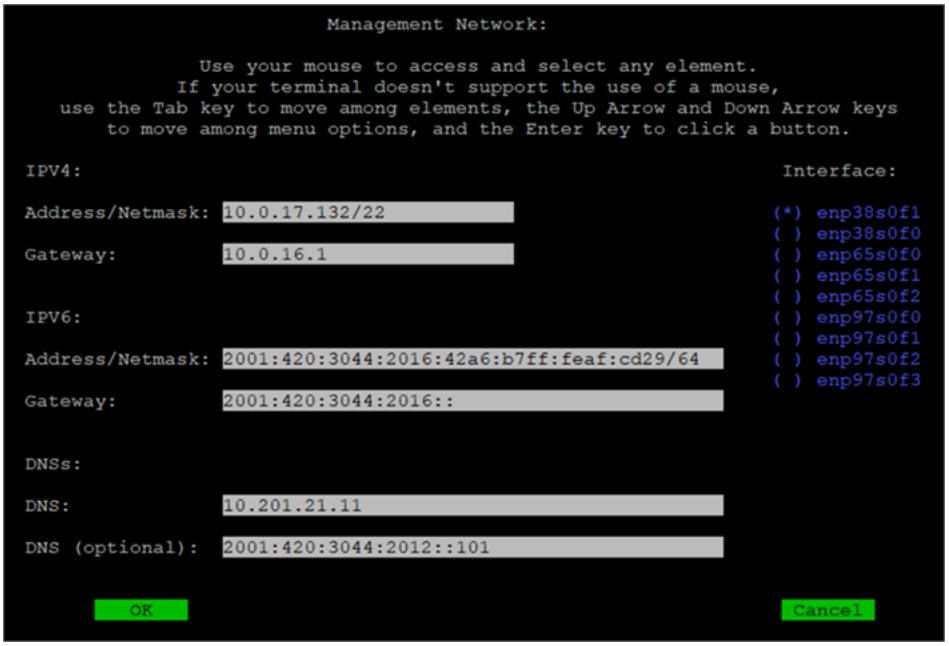
Um einzelne Parameter zu ändern, führen Sie den Befehl `sudo ctb-install --config` aus.

Ändern der Management-Netzwerkschnittstelle

1. Wenn Sie die Management-Netzwerkschnittstelle ändern möchten, wählen Sie im Hauptfenster das **Management-Netzwerk** aus:

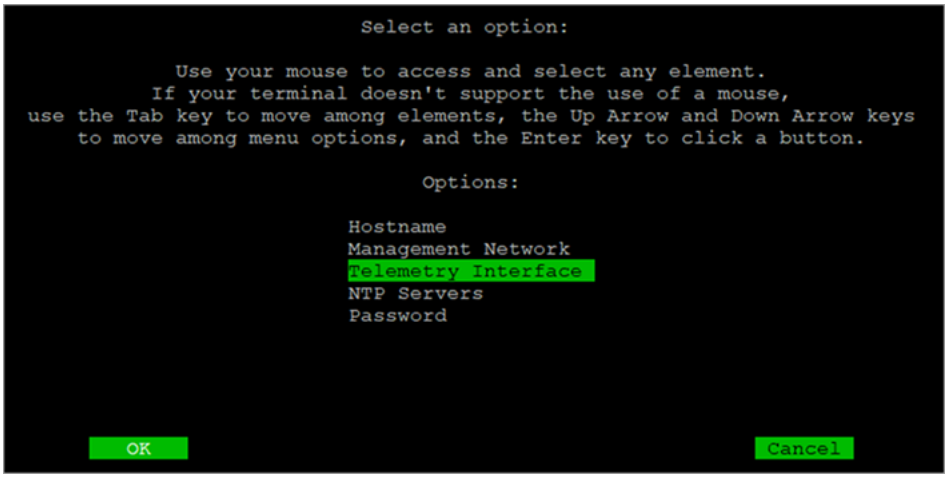


2. Nehmen Sie anschließend im sich öffnenden Fenster für das Management-Netzwerk alle erforderlichen Änderungen an den Einstellungen des Management-Netzwerks vor. Sie können auch eine neue Management-Netzwerkschnittstelle auswählen. Welcher Schnittstellenname für eine bestimmte Port-Nummer zu wählen ist, können Sie der Tabelle zur Zuordnung von Port-Nummern und Schnittstellennamen am Ende dieses Abschnitts entnehmen.



Ändern der Telemetrie-Netzwerkschnittstelle

1. Wenn Sie die Telemetrie-Netzwerkschnittstelle ändern möchten, wählen Sie im Hauptfenster die **Telemetrieschnittstelle** aus:



2. Wählen Sie im folgenden Fenster die entsprechende Telemetrie-Netzwerk-schnittstelle aus. Welcher Schnittstellenname für eine bestimmte Port-Nummer zu wählen ist, können Sie der Tabelle zur Zuordnung von Port-Nummern und Schnittstellennamen am Ende dieses Abschnitts entnehmen.

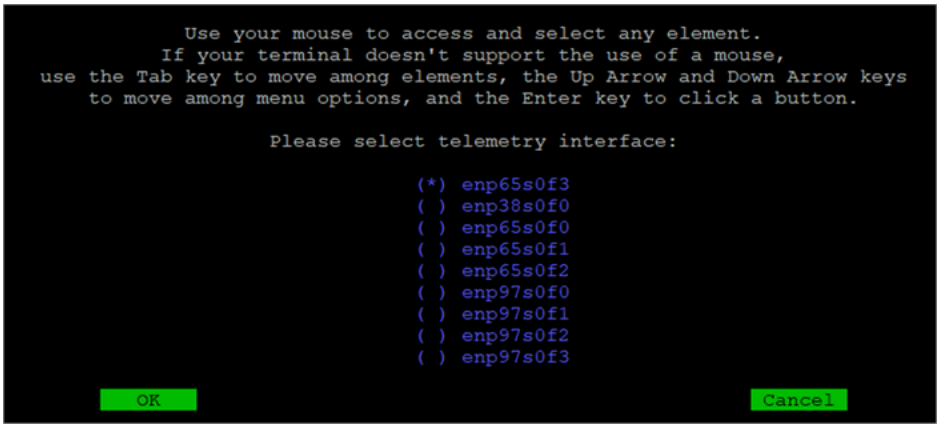
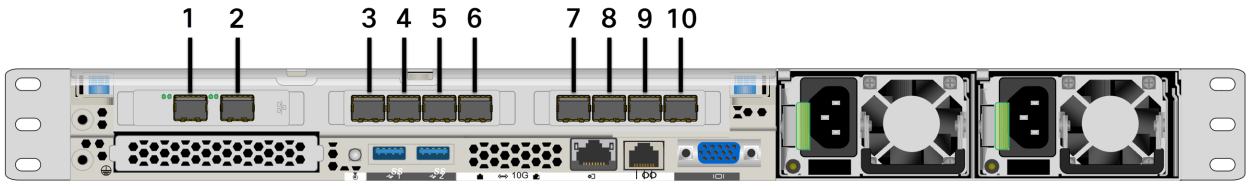


Tabelle zur Zuordnung von Port-Nummern und Schnittstellennamen



Port-Nummer	Schnittstellenname
1	enp38s0f1
2	enp38s0f0
3	enp65s0f3
4	enp65s0f2
5	enp65s0f1
6	enp65s0f0
7	enp97s0f0
8	enp97s0f1
9	enp97s0f2
10	enp97s0f3

Auf diese Port-Nummern wird auch auf den Seiten 2 und 3 im Datenblatt für den Broker-Knoten TB2300 verwiesen.

3. Ausführen des Befehls „sudo ctb-manage“

1. Führen Sie den Befehl `sudo ctb-manage` aus.
2. Geben Sie folgende Informationen ein:
    - IP-Adresse des Manager-Knotens
    - Benutzername des Superbenutzerkontos, das Sie im Manager-Knoten erstellen
    - Kennwort des Superbenutzerkontos, das Sie im Manager-Knoten erstellen

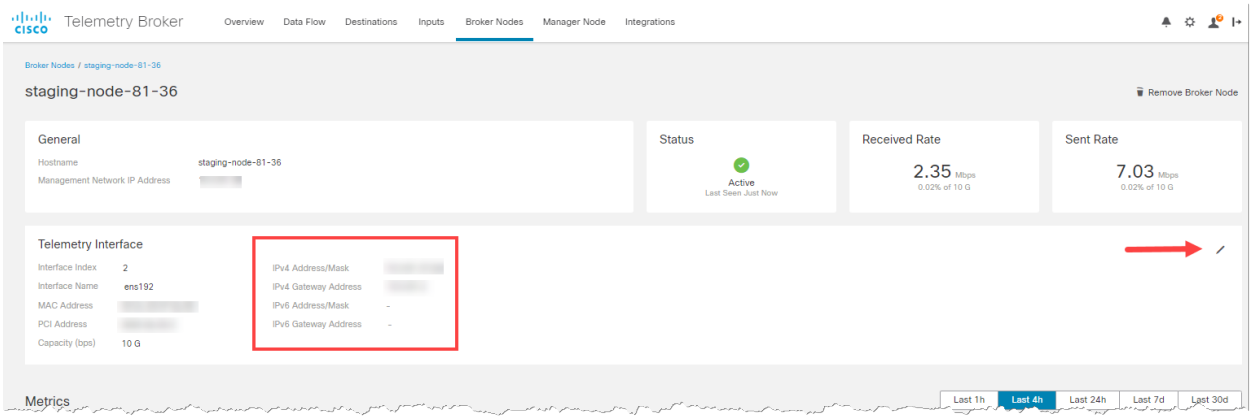
4. Abmelden

Um sich abzumelden, geben Sie `exit` ein.

5. Konfigurieren der Telemetrieschnittstelle

> Cisco Telemetry Broker ist für die Arbeit im Abrufmodus auf einer Hardware-Appliance konfiguriert.

1. Melden Sie sich bei Cisco Telemetry Broker an. Geben Sie in einem Webbrowser die IP-Adresse der Managementschnittstelle des Managers ein, und drücken Sie die **Eingabetaste**, um zur Anmeldeseite für das Web-Interface des Managers zu gelangen.
2. Wählen Sie im Hauptmenü die Option **Broker-Knoten** aus.
3. Klicken Sie in der Tabelle mit den Broker-Knoten auf den jeweiligen Broker-Knoten.
4. Klicken Sie im Abschnitt für die Telemetrieschnittstelle auf das **Bearbeitungssymbol** (in der folgenden Abbildung mit einem Pfeil gekennzeichnet).



5. Konfigurieren Sie die IP- und Gateway-Adresse (rot umrandet).

Verwalten von Hochverfügbarkeits-Clustern

Cisco Telemetry Broker -Hochverfügbarkeit bietet hochverfügbare virtuelle IPv4- und IPv6-IP-Adressen, die als Ziele für Ihre Eingaben dienen und eine zuverlässige Übermittlung der Telemetrie vom Eingang bis zum Ziel gewährleisten.

Um bei Broker-Knoten Hochverfügbarkeit zu erzielen, können Sie Hochverfügbarkeits-Cluster erstellen und diesen jeweils mehrere Broker-Knoten zuweisen. In jedem Cluster wird ein Broker-Knoten als *aktiv* bezeichnet, was bedeutet, dass er Telemetrie weiterleitet und Metriken für Cisco Telemetry Broker bereitstellt. Die übrigen werden als *passiv* bezeichnet, was bedeutet, dass sie derzeit weder Telemetrie weiterleiten noch Metriken bereitstellen. Wenn ein aktiver Broker-Knoten die Telemetrieweiterleitung beendet oder die Netzwerkverbindung zum Telemetry Broker auf andere Weise verliert, wird einer der passiven Broker-Knoten zum aktiven Broker-Knoten hochgestuft und beginnt mit der Telemetrieweiterleitung.

Beachten Sie Folgendes zu Clustern:

- Ein Broker-Knoten kann jeweils nur zu einem Cluster gehören.
- Um ein Cluster zu erstellen, müssen Sie diesem Cluster mindestens einen Broker-Knoten zuweisen.
- Wenn Sie ein Cluster mit nur einem Broker-Knoten erstellen und dieser Broker-Knoten ausfällt, ist kein anderer Broker-Knoten verfügbar, der zum aktiven Broker-Knoten befördert werden kann. Wenn alle Broker-Knoten in einem Cluster ausfallen, kann kein Broker-Knoten zum aktiven Broker-Knoten befördert werden. Wenn ein Broker-Knoten ausfällt, schalten Sie ihn so schnell wie möglich wieder online.
- Sie können nicht auswählen, welcher Broker-Knoten in einem bestimmten Cluster aktiv ist.
- Wenn ein aktiver Broker-Knoten für eine virtuelle IP-Adresse ausfällt, wird einer der passiven Broker-Knoten im selben Cluster zum aktiven Broker-Knoten für die virtuelle IP-Adresse. Wenn der ausgefallene Broker-Knoten wieder online ist, bleibt er passiv. Um diesen Knoten wieder zu aktivieren, müssen Sie manuell die in diesem Kapitel im Abschnitt Verschieben einer VIP zu einem bestimmten Knoten angegebenen Befehle durchführen.
- Sie können einem Cluster eine virtuelle IPv4-Adresse, eine virtuelle IPv6-Adresse oder beides zuweisen. Telemetry Broker verwendet diese virtuelle IP-Adresse, um mit dem Cluster zu kommunizieren und passive Broker-Knoten zu aktiven Broker-Knoten hochzustufen, wenn ein aktiver Broker-Knoten die Netzwerkverbindung mit Telemetry Broker verliert.

Informationen darüber, wie HA-Cluster während des Softwareupdateprozesses für Cisco Telemetry Broker aktualisiert werden, finden Sie im Benutzerhandbuch zu Cisco Telemetry Broker im Kapitel zu Softwareupdates.

VIPs und Routing

Hochverfügbarkeit konfiguriert die Telemetrie-Netzwerkschnittstelle des VIP-Adressbroker-Knotens. Beachten Sie, dass die Telemetrie-Netzwerkschnittstelle auf jedem Broker-Knoten im Cluster bereits mit einer primären IPv4- oder IPv6-IP-Adresse sowie mit einer Subnetzmaske und einem Gateway *konfiguriert sein muss*. Sie können diese in der Telemetrie-Netzwerkschnittstelle konfigurieren.

Sie müssen die IPv4- oder IPv6-VIP-IP-Adressen so konfigurieren, dass sie sich im selben Subnetz befinden wie die primären IP-Adressen **der Telemetrie-Netzwerk-schnittstellen** im Cluster, da sich die VIP ebenfalls im selben Subnetz befinden muss. Dadurch stellen Sie ein ordnungsgemäßes Routing über das vorkonfigurierte Gateway und ein schnelles Failover sicher.

Wenn sich die VIP-Adressen nicht im selben Subnetz wie die primären IP-Adressen der Telemetrie-Netzwerkschnittstellen befinden oder wenn die Telemetrie-Netzwerk-schnittstellen innerhalb eines Clusters mit unterschiedlichen Subnetzen konfiguriert sind, funktioniert die Hochverfügbarkeit sehr wahrscheinlich nicht.

Verwalten von Clustern

Die Cisco Telemetry Broker-Implementierung greift auf zwei häufig verwendete Linux-Pakete zurück, um die zugrunde liegende Hochverfügbarkeitsinfrastruktur bereitzustellen:

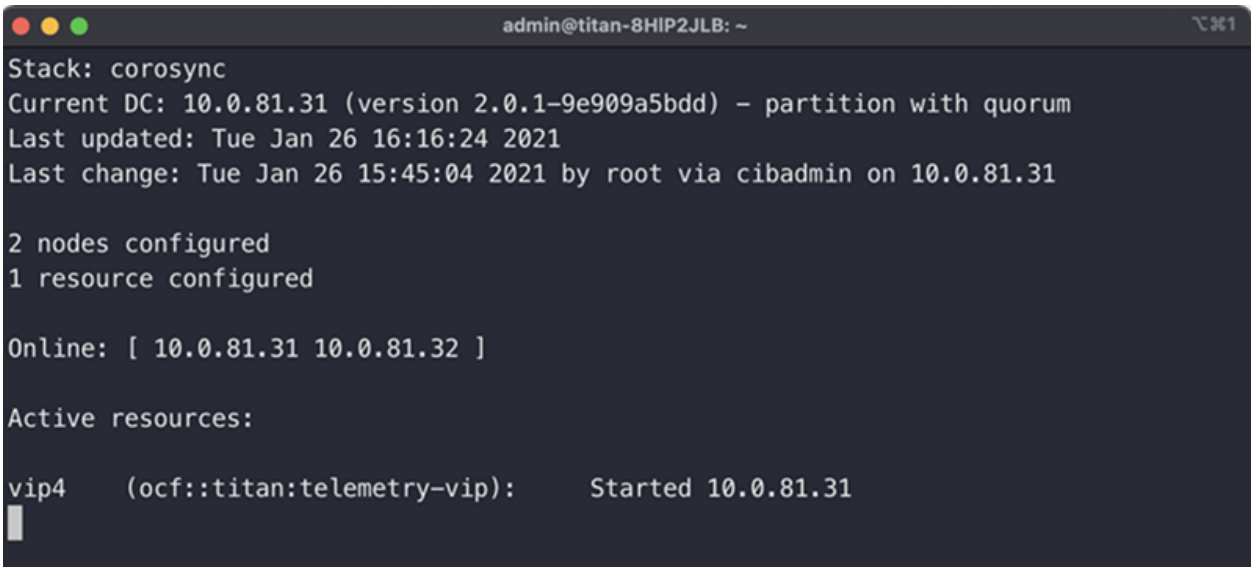
Corosync: Dies ist die Low-Level-Cluster-Engine, die die zugrunde liegende Kommunikation zwischen Cluster-Knoten bereitstellt. Sie liefert auch die Quorum-Fähigkeit, um die Entscheidung über die Rolle jedes Knotens (aktiv oder Standby) zu treffen.

Pacemaker: Dies ist der Clusterressourcenmanager, der alle Beziehungen zwischen den Geräten und den Anwendungen verwaltet. Er verwendet Corosync für die Kommunikation.

Anzeigen des aktuellen Clusterstatus

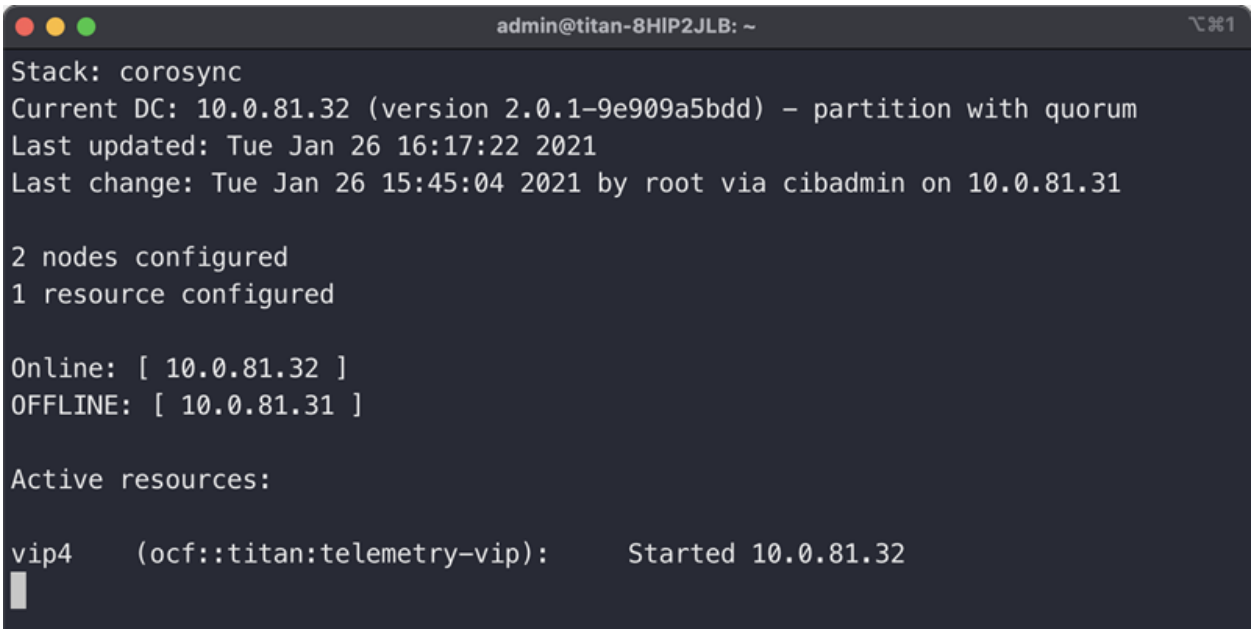
Gehen Sie wie folgt vor, um den aktuellen Status des Clusters anzuzeigen, einschließlich des Status (Offline/Online) jedes Knotens und des Standorts der IPv4-VIP (vip4) und der IPv6-VIP (vip6):

1. Melden Sie sich über SSH als **admin** bei einem der Broker-Knoten im Cluster an. Verwenden Sie das Kennwort, das während der Knoteninstallation bereitgestellt wurde.
2. Führen Sie den Befehl `sudo crm_mon` aus. Hierdurch wird eine Ansicht der aktuell konfigurierten Attribute im Cluster angezeigt. Weitere Informationen zu diesem Befehl finden Sie hier.
3. Schließen Sie das Tool, indem Sie **Strg+C** drücken.



Das obere Bild zeigt ein Cluster aus zwei Knoten (10.0.81.31 und 10.0.81.32), die beide den Status *Online* haben. Die IPv4-VIP (vip4) wird derzeit auf 10.0.81.31 ausgeführt. Die IPv6-VIP (vip6) ist nicht sichtbar, da sie nicht konfiguriert wurde.

Wenn 10.0.81.31 ausfällt, sieht der Status wie folgt aus:

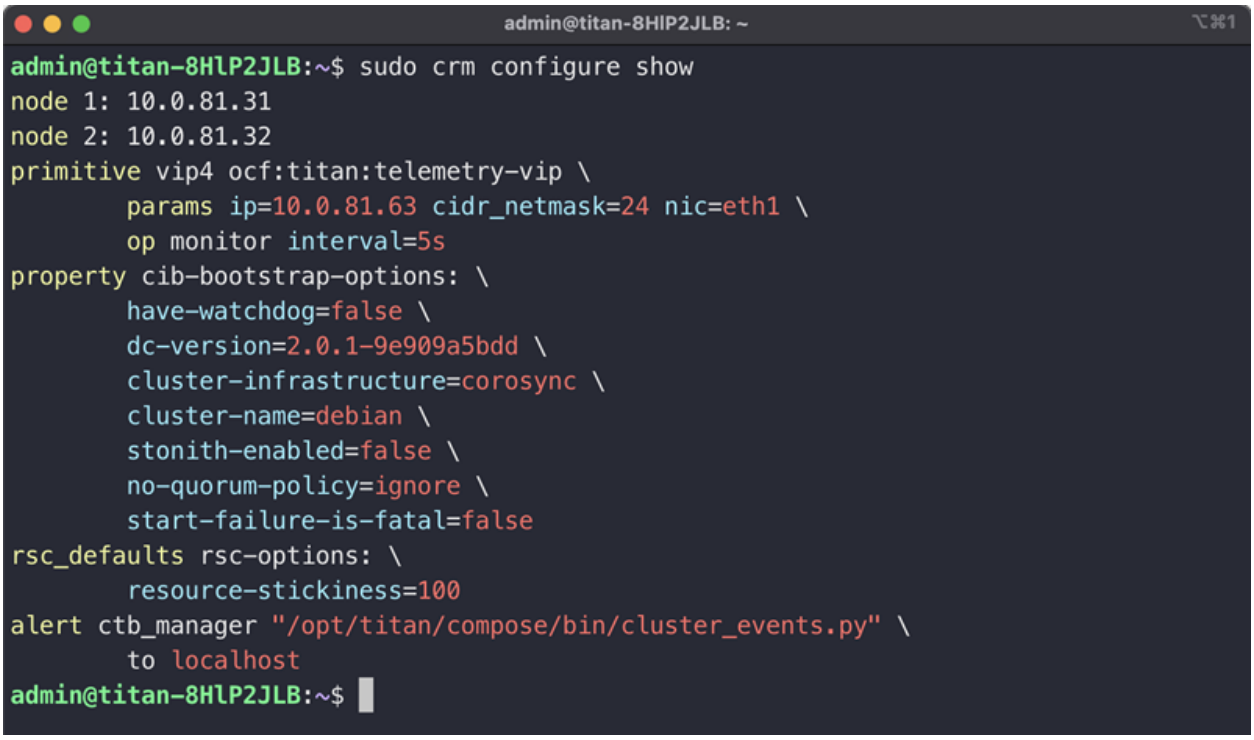


Beachten Sie, dass 10.0.81.31 jetzt als *OFFLINE* angezeigt wird und vip4 zu 10.0.81.32 verschoben wurde.

Anzeigen der aktuellen Clusterkonfiguration

Gehen Sie wie folgt vor, um die aktuelle Konfiguration des Clusters anzuzeigen und zu überprüfen, ob die Corosync- und Pacemaker-Konfiguration korrekt ist:

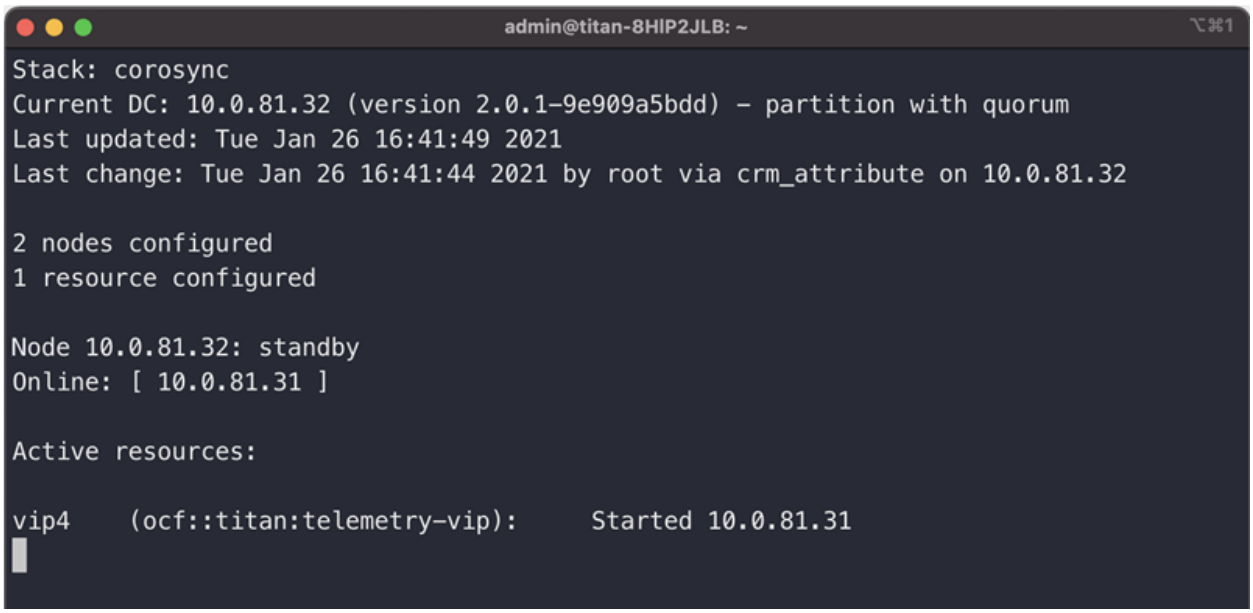
1. Melden Sie sich über SSH als **admin** bei einem der Broker-Knoten im Cluster an. Verwenden Sie das Kennwort, das während der Knoteninstallation bereitgestellt wurde.
2. Führen Sie den Befehl `sudo crm configure show` aus. Hierdurch wird eine Ansicht des aktuell konfigurierten Attributs im Cluster angezeigt. Weitere Informationen zu diesem Befehl finden Sie hier.



Aktivieren und Deaktivieren des Knoten-Standby-Modus

Im Standby-Modus kann der Knoten keine virtuellen IPv4- oder IPv6-IP-Adressen hosten.

1. Melden Sie sich über SSH als **admin** bei einem der Broker-Knoten im Cluster an. Verwenden Sie das Kennwort, das während der Knoteninstallation bereitgestellt wurde.
2. Führen Sie den Befehl `sudo crm node standby 10.0.81.32` aus. Sie können den Namen des Knotens weglassen, wenn Sie diesen Befehl auf diesem Knoten ausführen. Weitere Informationen zu diesem Befehl finden Sie hier.
3. Führen Sie den Befehl `sudo crm node online 10.0.81.32` aus, um den Knoten aus dem *Standby* zu holen. Weitere Informationen zu diesem Befehl finden Sie hier.



Wie Sie sehen können, wird unter *crm_mon* der Standby-Status des Knotens 10.0.81.32 angezeigt.

Verschieben einer VIP zu einem bestimmten Knoten

Es kann vorkommen, dass Sie festlegen müssen, auf welchem Knoten die virtuelle IPv4- oder IPv6-IP-Adresse ausgeführt werden soll. Gehen Sie in diesem Fall wie folgt vor:

1. Melden Sie sich über SSH als **admin** bei einem der Broker-Knoten im Cluster an. Verwenden Sie das Kennwort, das während der Knoteninstallation bereitgestellt wurde.
2. Führen Sie den Befehl `sudo crm resource move vip4 10.0.81.32` aus. Weitere Informationen zu diesem Befehl finden Sie hier.
3. Führen Sie den Befehl `sudo crm resource unmove vip4` aus, um sicherzustellen, dass die VIP auf dem Zielknoten verbleibt. Andernfalls wird die VIP bei der nächsten Gelegenheit zu dem Knoten zurückkehren, auf dem sie sich zuvor befand (vor der Verschiebung).

Abschließen der Konfiguration Ihres Systems

Um die Konfiguration Ihres Systems abzuschließen, lesen Sie die folgenden Abschnitte im Cisco Telemetry Broker Benutzerhandbuch:

- Ziele
- Eingaben
- Broker-Knoten

Support kontaktieren

Wenn Sie technischen Support benötigen, haben Sie folgende Möglichkeiten:

- Wenden Sie sich an Ihren lokalen Cisco Telemetry Broker-Partner.
- Wenden Sie sich an den Cisco Telemetry Broker-Support.
- Erstellen Sie online ein Ticket: http://www.cisco.com/c/en/us/support/index.html
- Erstellen Sie ein Ticket per E-Mail: tac@cisco.com
- Rufen Sie uns an: 1-800-553-2447 (USA)
- Weltweite Supportnummern finden Sie unter https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Änderungsverlauf

Dokumentversion	Veröffentlichungsdatum	Beschreibung
1_0	April 2023	Erste Version
1_1	Mai 2023	Kapitel „Migrieren der Konfiguration zu einem neuen System“ hinzugefügt

Copyright-Informationen

DIE SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN. ALLE ANWEISUNGEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH WERDEN ALS RICHTIG ANGENOMMEN, WERDEN JEDOCH OHNE JEGLICHE WIE AUCH IMMER GEARTETE, AUSDRÜCKLICHE ODER STILLSCHWEIGENDE, GARANTIE ABGEGEBEN. DIE BENUTZER TRAGEN DIE VOLLSTÄNDIGE VERANTWORTUNG FÜR IHRE ANWENDUNG VON PRODUKTEN.

DIE SOFTWARELIZENZ UND EINGESCHRÄNKTE GARANTIE FÜR DAS BEGLEITENDE PRODUKT WERDEN IM INFORMATIONSPAKET, DAS IM LIEFERUMFANG DIESES PRODUKTS ENTHALTEN IST, DARGELEGT UND GELTEN HIERMIT ALS BESTANDTEIL DIESER VEREINBARUNG. WENN SIE DIE SOFTWARELIZENZ ODER BESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, WENDEN SIE SICH AN EINEN VERTRETER VON CISCO, UM EINE KOPIE ZU ERHALTEN.

Die Cisco Implementierung der TCP-Headerkomprimierung ist eine Adaption eines Programms, das an der University of California, Berkeley (UCB), als Teil der Public-Domain-Version der UCB für das UNIX-Betriebssystem entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981 Verwaltungsrat der University of California.

UNGEACHTET JEGLICHER ANDERER HIERIN ENTHALTENEN GARANTIEBESTIMMUNG WERDEN ALLE DOKUMENTDATEIEN UND DIE SOFTWARE DIESER LIEFERANTEN„ WIE BESEHEN“ UND OHNE GARANTIE AUF FEHLERFREIHEIT ZUR VERFÜGUNG GESTELLT. CISCO UND ALLE ZUVOR GENANNTEN LIEFERANTEN ÜBERNEHMEN KEINERLEI, AUSDRÜCKLICHE ODER STILLSCHWEIGENDE, GARANTIEN, EINSCHLIEßLICH UND OHNE EINSCHRÄNKUNG, DIEJENIGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG ODER DIEJENIGEN, DIE AUS DEM VERLAUF DES HANDELNS, DER VERWENDUNG ODER DES HANDELSBRAUCHS ENTSTEHEN.

IN KEINEM FALL SIND CISCO ODER SEINE LIEFERANTEN HAFTBAR FÜR INDIREKTE, SPEZIELLE SCHÄDEN, FOLGESCHÄDEN ODER NEBENSCHÄDEN JEGLICHER ART, EINSCHLIEßLICH UND OHNE EINSCHRÄNKUNG, SCHÄDEN AUS ENTGANGENEM GEWINN ODER DATENVERLUST AUFGRUND DER VERWENDUNG ODER NICHT UNFÄHIGKEIT DER VERWENDUNG DIESES HANDBUCHS. DIES GILT AUCH FÜR DEN FALL, DASS CISCO ODER SEINE LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN AUFMERKSAM GEMACHT WURDEN.

Sämtliche in diesem Dokument verwendeten IP-Adressen und Telefonnummern sind als Beispiele zu verstehen und beziehen sich nicht auf tatsächlich existierende Adressen und Telefonnummern. Die in diesem Dokument enthaltenen Beispiele, Befehlsanzeige-

ausgaben, Netzwerktopologie-Diagramme und anderen Abbildungen dienen lediglich zur Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen oder Telefonnummern in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

Für gedruckte und kopierte digitale Versionen dieses Dokuments besteht keine Gewährleistung. Die aktuelle Online-Version enthält die neueste Version.

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Unsere Adressen und Telefonnummern finden Sie auf der Cisco Website unter https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter folgender URL: https://www.cisco.com/go/trademarks. Die genannten Handelsmarken von Drittanbietern sind Eigentum der jeweiligen Inhaber. Die Verwendung des Worts "Partner" deutet keine Handelsbeziehung zwischen Cisco und anderen Unternehmen an. (1721R)