Cisco Stealthwatch

Hardware-Installations- und Konfigurationshandbuch für Data Store

Inhalt

Einführung in die Data Store-Hardwareinstallation und -konfiguration 5

Überblick 5

Zielgruppe 5

Hinweise zur Verwendung dieses Handbuchs 5

Data Store-Konzepte und -Architektur 8

Anforderungen und Überlegungen zur Data Store-Bereitstellung 13

Stealthwatch Versionsunterstützung 13

Stealthwatch Lizenzierung 13

Stealthwatch Hardwarekompatibilität und Netzwerkanforderungen 13

Überlegungen zu Stealthwatch-Unternehmensbereitstellungen 15

Erforderliche Anmeldeinformationen bei der Data Store-Bereitstellung 15

Data Store-Netzwerk- und Switching-Überlegungen 15

Anforderungen und Überlegungen zur Data Store-Bereitstellung 19

Data Store Kommunikations-Ports 20

Stealthwatch Data Store-Bereitstellungsübersicht 24

Installation der Data Store-Hardware 31

Stealthwatch Hardwarebereitstellung und Überlegungen 31

SMC-Konfiguration für die Verwendung mit einem Data Store 31

Data Store Hardware-Erstbereitstellung und -konfiguration 34

UDP Director-Bereitstellung 36

Flow Collector-Konfiguration für die Verwendung mit einem Data Store 37

Flow Sensor-Bereitstellung 40

Failover-Bereitstellung der Stealthwatch Management Console 40

Data Store-Initialisierung und -Konfiguration 41

Konfiguration von Vertica Management Console 50

Konfiguration der Data Store-Datenaufbewahrung 57

Nächste Schritte nach der Data Store-Installation 63

Wartung des Data Store **64**
Neustart eines Data Node 64
Neustarten des Data Store 65
Erstellen eines Data Store-Backups 66
Wiederherstellen eines Data Store-Backups 72
Hinzufügen von drei Data Nodes zum Data Store 74
Vorbereitung des Data Store für das Hinzufügen von Data Nodes und Rebalancing 74
Hinzufügen von Data Nodes zum Data Store 75
Entfernen eines Data Node aus dem Data Store 79
Austauschen eines Data Node gegen einen Ersatz-Data Node mit einer anderen IP-Adresse 80
Vorbereiten des Data Store für den Austausch eines ausgefallenen Data Nodes 80
Ersetzen des Data Node 80
Kopieren von Data Store-Trust-Informationen auf eine Failover-SMC 82
Fehlerbehebung bei der Data Store-Bereitstellung **84**
Fehlerbehebung bei der Hardwarebereitstellung 84
Fehlerbehebung beim setup-sw-datastore-secure-connectivity-Skript 84
Fehlerbehebung beim install_SDBN_initial.py-Skript 89
Fehlerbehebung beim update_SDBN.py-Skript 99
Fehlerbehebung bei Vertica Management Console 101
Data Store Fehlerbehebung 102
Anhang A. Vorbereitung der Installation **104**
Installationswarnungen 104
Installationsrichtlinien 106
Sicherheitshinweise 108
Sicherheit bei Arbeiten mit Elektrizität 109
Vermeidung von Schäden durch ESD 109
Standortumgebung 110

Überlegungen zur Stromversorgung 110
Überlegungen zur Rack-Konfiguration 110
Anhang B. Stealthwatch Installation der Hardware 112
Montage Ihrer Appliance 112
Im Lieferumfang der Appliance enthaltene Hardware 112
Zusätzlich erforderliche Hardware 112
Verbinden Ihrer Appliance mit dem Netzwerk 113
Verbinden mit Ihrer Appliance 114
Anschluss einer Tastatur und eines Monitors 114
Verbindung mit einem Laptop herstellen 115
Konfigurieren der Netzwerkeinstellungen mit der erstmaligen Einrichtung 116
Allgemeine Konfiguration der Stealthwatch Appliance 117
Data Store-kompatible Appliances (SMC 2210, FC 4210) 119
Data Node Konfiguration 123
Ändern des Sysadmin-Benutzerkennworts 127
Ändern des Root-Benutzerkennworts 128
Anhang C. Konfigurieren Ihrer Appliances 130
Appliance Setup Tool-Anforderungen 130
Verwaltet 130
SMC-Failover 130
Best Practices 131
Konfigurationsreihenfolge 131
1. Anmelden 132
2. Konfigurieren der Appliance 133
3. Registrierung der Stealthwatch Management Console 135
4. Hinzufügen von Appliances zu Central Management 136
5. Bestätigen des Appliance-Status 137

Einführung in die Data Store-Hardwareinstallation und -konfiguration

Überblick

In dieser Anleitung wird erklärt, wie Sie den Stealthwatch Data Store als Teil einer Stealthwatch-Systembereitstellung installieren. Sie beschreibt die Komponenten des Stealthwatch-Systems und ihre Platzierung, insbesondere in Bezug auf den Data Store.

In diesem Kapitel werden die folgenden Themen behandelt:

- **Zielgruppe**
- **Hinweise zur Verwendung dieses Handbuchs**

Zielgruppe

Dieses Handbuch richtet sich an die Person, die für die Installation der Stealthwatch-Systemhardware verantwortlich ist. Wir gehen davon aus, dass Sie bereits über Grundkenntnisse in der Installation von Netzwerkgeräten (Flow Collector und Stealthwatch Management-Konsole) verfügen.

Informationen zur Konfiguration von Stealthwatch-Systemprodukten finden Sie in *Stealthwatch-Systemkonfigurationshandbuch*.

Hinweise zur Verwendung dieses Handbuchs

Neben dieser Einführung haben wir diesen Leitfaden in die folgenden Kapitel unterteilt:

Kapitel	Beschreibung
Data Store-Konzepte und -Architektur	Beschreibt die grundlegenden Konzepte, die der Data Store-Datenbank zugrunde liegen, sowie die grundlegende Architektur in Bezug auf die Data Store-Bereitstellung in Verbindung mit einer SMC und Flow Collectors.
Anforderungen und Überlegungen zur Data	Beschreibt Stealthwatch-Hardware, die mit dem Data Store kompatibel ist, und

Kapitel	Beschreibung
Store-Bereitstellung	enthält Anforderungen und Empfehlungen für die Bereitstellung Ihres Data Store, einschließlich zu öffnender Kommunikationsports.
Stealthwatch Data Store-Bereitstellungsübersicht	Bietet einen allgemeinen Überblick über die Bereitstellung von Stealthwatch-Appliances für die Verwendung mit einem Data Store.
Installation der Data Store-Hardware	Bietet einen umfassenden Überblick über die Bereitstellung von Stealthwatch-Appliances für die Verwendung mit einem Data Store sowie Konfigurationsanweisungen zur Initialisierung der Data Store-Datenbank.
Konfiguration der Data Store-Datenaufbewahrung	Enthält Informationen zur Konfiguration des Data Store-Datenaufbewahrungszeitraums.
Nächste Schritte nach der Data Store-Installation	Beschreibt die nächsten Schritte nach Abschluss der Bereitstellung und Konfiguration Ihres Data Store.
Wartung des Data Store	Beschreibt Data Store-Wartungsaufgaben.
Fehlerbehebung bei der Data Store-Bereitstellung	Beschreibt häufige Probleme, die während des Data Store-Installationsvorgangs auftreten, sowie Lösungsvorschläge.
Anhang A. Vorbereitung der Installation	Enthält Warnungen für die Installation von Hardware.

Kapitel	Beschreibung
Anhang B. Stealthwatch Installation der Hardware	Bietet einen Überblick über die Installation von Stealthwatch-Appliances und die Durchführung der Erstkonfiguration zur Zuweisung einer IP-Adresse sowie weitere zugehörige Management-Informationen.
Anhang C. Konfigurieren Ihrer Appliances	Bietet einen Überblick über die Verwendung des Appliance Setup Tools zur Konfiguration Ihrer Stealthwatch-Appliances.

Data Store-Konzepte und -Architektur

> Installieren Sie **keinen** Stealthwatch Data Store allein. Wenn Sie einen Stealthwatch Data Store erwerben möchten, wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Platzierung, Bereitstellung und Konfiguration innerhalb und im Rahmen Ihrer gesamten Stealthwatch-Bereitstellung von zu erhalten.

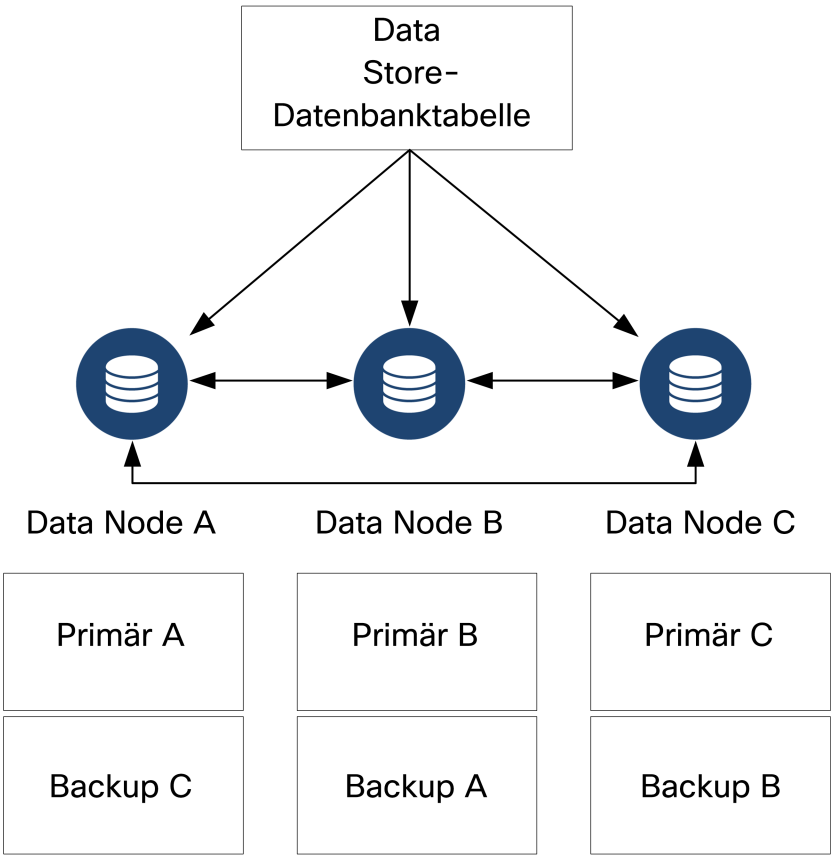
Der Stealthwatch Data Store bietet ein zentrales Repository zum Speichern der von Ihren Stealthwatch Flow Collectors gesammelten Telemetriedaten Ihres Netzwerks. Der Data Store besteht aus einem Cluster von Data Nodes, die jeweils einen Teil Ihrer Daten enthalten, und einem Backup von Daten eines separaten Data Node. Da sich alle Ihre Daten in einer zentralen Datenbank befinden und nicht über mehrere Flow Collectors verteilt sind, kann Ihre Stealthwatch Management Console Abfrageergebnisse vom Data Store schneller abrufen, als wenn alle Flow Collectors separat abgefragt werden würden. Der Data Store-Cluster bietet eine verbesserte Fehlertoleranz, eine verbesserte Antwort auf Abfragen und eine schnellere grafische Darstellung.

Data Store Speicherung und Fehlertoleranz

Der Data Store sammelt Daten von Flow Collectors und verteilt sie gleichmäßig auf Data Nodes innerhalb des Clusters. Jeder Data Node speichert nicht nur einen Teil Ihrer Gesamttelemetrie, sondern auch eine Sicherungskopie der Telemetrie eines anderen Data Nodes. Speichern von Daten auf diese Weise:

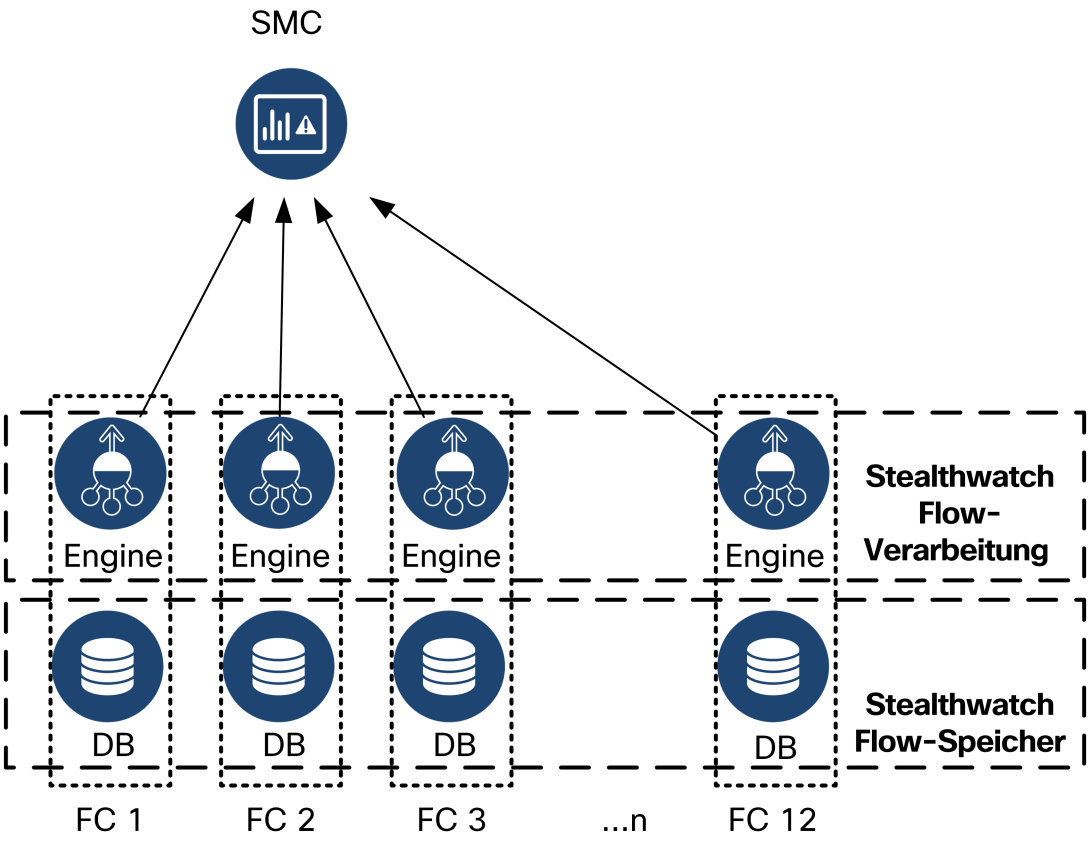
- erleichtert die Lastverteilung
- verteilt die Verarbeitung auf jeden Knoten
- stellt sicher, dass alle Daten, die der Data Store erfasst, ein Backup für Fehlertoleranz haben
- ermöglicht die Erhöhung der Anzahl von Data Nodes zur Verbesserung der gesamten Speicher- und Abfrageleistung

Wenn ein Knoten ausfällt, solange der Knoten, der seine Sicherung enthält, noch verfügbar ist und mindestens die Hälfte Ihrer gesamten Data Node noch in Betrieb ist, bleibt der gesamte Data Store aktiv. So haben Sie Zeit, die ausgefallene Verbindung oder die fehlerhafte Hardware zu reparieren. Nachdem Sie den fehlerhaften Data Node ersetzt haben, stellt der Data Store die Daten dieses Knotens aus der vorhandenen Sicherung wieder her, die auf dem benachbarten Data Node gespeichert ist, und erstellt eine Sicherung der Daten auf diesem Data Node. Im folgenden Diagramm finden Sie ein Beispiel dafür, wie Data Nodes Telemetrie speichern:

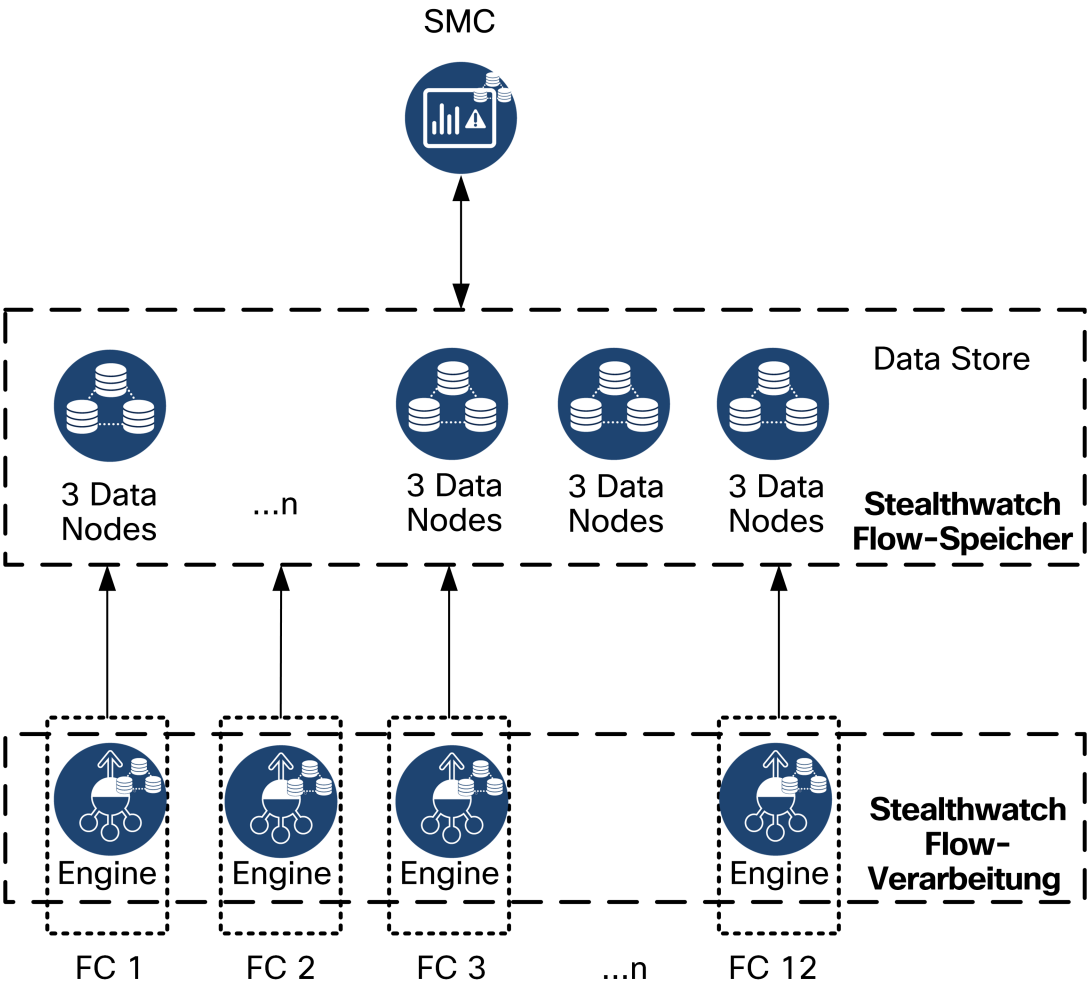


Stealthwatch Data Store-Bereitstellungsarchitektur

In einer herkömmlichen Stealthwatch-Bereitstellung ohne Data Store erfassen ein oder mehrere Flow Collectors Daten und deduplizieren sie, führen Analysen durch und melden Daten und Ergebnisse direkt an die SMC. Um vom Benutzer eingereichte Abfragen, einschließlich Grafiken und Diagramme, aufzulösen, fragt die SMC alle verwalteten Flow Collectors ab. Jeder Flow Collector gibt übereinstimmende Ergebnisse an die SMC zurück. Die SMC stellt die Informationen aus den verschiedenen Ergebnissätzen zusammen und erzeugt dann eine Grafik oder ein Diagramm, das die Ergebnisse anzeigt. Bei dieser Bereitstellung speichert jeder Flow Collector Daten in einer lokalen Datenbank. Nehmen Sie das folgende Diagramm als Beispiel.



In einer Stealthwatch-Bereitstellung mit einem Data Store sitzt der Data Store-Cluster zwischen Ihrer SMC und den Flow Collectors. Ein oder mehrere Flow Collectors erfassen Flows und deduplizieren sie, führen Analysen durch und melden Daten und Ergebnisse direkt an den Data Store, wobei sie ungefähr gleichmäßig auf alle Data Nodes verteilt werden. Der Data Store erleichtert die Datenspeicherung, hält den gesamten Datenverkehr an diesem zentralen Ort, anstatt ihn über mehrere Flow Collectors zu verteilen, und bietet eine größere Speicherkapazität als mehrere Flow Collectors. Nehmen Sie das folgende Diagramm als Beispiel.



Um vom Benutzer eingereichte Abfragen, einschließlich Graphen und Diagramme, aufzulösen, fragt die SMC den Data Store ab. Der Data Store findet übereinstimmende Ergebnisse in den für die Abfrage relevanten Spalten, ruft dann die übereinstimmenden Zeilen ab und gibt die Abfrageergebnisse an die SMC zurück. Die SMC generiert die Grafik oder das Diagramm, ohne dass mehrere Ergebnissätze von mehreren Flow Collectors zusammengestellt werden müssen. Dies reduziert die Abfragekosten im Vergleich zur Abfrage mehrerer Flow Collectors und verbessert die Abfrageleistung.

Aufgrund der Data Store-Architektur müssen die SMC und alle Flow Collectors mit dem Data Store kommunizieren und bei der Bereitstellung für die Zusammenarbeit mit dem Data Store konfiguriert werden. Eine „gemischte“ Umgebung haben, in der einige Flow Collectors direkt an die SMC und andere Flow Collectors an den Data Store berichten, ist nicht möglich.

Stealthwatch Data Store-Architektur

Jeder Data Store besteht aus 3 oder mehr Data Nodes. Jeder Data Node ist ein eigenes Hardware-Chassis. Wenn Sie einen Data Store kaufen, erhalten Sie mehrere Data

Node-Hardware-Chassis, die der durch dieses Data Store-Modell angegebenen Anzahl von Knoten entsprechen. Zum Beispiel verfügt ein DS 6200-Data Store über 3 Data Node-Hardware-Chassis.

Sie können mehr als einen Data Store für Ihre Bereitstellung erwerben. Die Data Nodes können als Teil Ihres Data Store in Vielfachen von 3 geclustert werden, von einem Minimum von 3 bis zu einem Maximum von 36.

> Cisco empfiehlt, dass Sie Ihre Data Nodes so konfigurieren, dass die benachbarten Data Nodes mit separaten, redundanten Netzteilen versorgt werden. Diese Konfiguration verbessert die Datenredundanz und die Gesamtbetriebszeit des Data Store. Weitere Informationen finden Sie unter Anforderungen und Überlegungen zur Data Store-Bereitstellung.

Um einen Data Store bereitzustellen, müssen Sie für jeden Data Node Folgendes zuweisen:

- eine routbare IP-Adresse für die Management-, Erfassungs- und Abfragekommunikation mit Ihren Stealthwatch-Appliances
- eine nicht routbare IP-Adresse (CIDR-Block `169.254.42.0/24`) in einem isolierten LAN oder VLAN für die Kommunikation zwischen den Data Nodes als Teil des Data Store-Clusters
- zwei 10G-Verbindungen – eine für die Management-, Erfassungs- und Abfragekommunikation und eine für die Inter-Data Node-Kommunikation
- optional, für Netzwerkredundanz und Kritikalität der Inter-Data Node-Kommunikation, eine zusätzliche 10G-Verbindung und einen zusätzlichen Switch zum Aufbau eines Port-Channels auf dem Data Node.

Unter Anforderungen und Überlegungen zur Data Store-Bereitstellung finden Sie weitere Informationen zur Bereitstellung und ihren Voraussetzungen.

Anforderungen und Überlegungen zur Data Store-Bereitstellung

Im Folgenden finden Sie Informationen zu den Voraussetzungen und Empfehlungen für Ihre Data Store-Bereitstellung.

> Wenn Sie eine Stealthwatch Data Store erwerben möchten, wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Platzierung, Bereitstellung und Konfiguration innerhalb und im Rahmen Ihrer gesamten Bereitstellung von Stealthwatch zu erhalten.

Stealthwatch Versionsunterstützung

Wenn Sie einen Data Store bereitstellen, müssen alle Ihre Stealthwatch-Appliances dieselbe Version (Version 7.3 oder höher) haben.

Stealthwatch Lizenzierung

Ihre Stealthwatch-Bereitstellung erfordert eine Flow Rate (FPS) Smart-Lizenz; der Data Store selbst erfordert keine zusätzliche Lizenz.

Stealthwatch Hardwarekompatibilität und Netzwerkanforderungen

Die folgende Tabelle gibt einen Überblick über die erforderliche Hardware für die Bereitstellung eines Data Store.

Hardwarekomponente	Unterstützte Kapazität
Data Store	• Mindestens 3 Data Nodes (DS 6200) • Zusätzliche Sätze von jeweils drei 3 Data Nodes zur Erweiterung des Data Store, maximal 36 Data Nodes
Stealthwatch Management Console	• Mindestens 1 Stealthwatch Management Console
Flow Collector	• Mindestens 1 Flow Collector

Beachten Sie, dass Sie eine Flow Rate (FPS) Smart-Lizenz für Ihre gesamte Stealthwatch-Bereitstellung erwerben müssen.

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

Wenn Sie einen Data Store bereitstellen möchten, müssen Sie mindestens 3 Data Nodes haben. Ein Data Store 6200 mit 3 Data Nodes kann etwa 500.000 Flows pro Sekunde verarbeiten und diese Daten etwa 90 Tage lang aufbewahren. Sie können Ihren Data Store mit zusätzlichen Data Nodes in Vielfachen von 3 erweitern, bis zu einem Maximum von 36 Data Nodes.

> ℹ Diese Empfehlungen berücksichtigen nur die Telemetrie. Ihre Leistung kann in Abhängigkeit von weiteren Faktoren variieren, einschließlich der Anzahl der Hosts, der Verwendung von Flow Sensors, Datenverkehrsprofilen und anderen Netzwerkmerkmalen. Wenden Sie sich an den Cisco Support, wenn Sie Hilfe bei der Dimensionierung benötigen.

> ℹ Zurzeit unterstützt der Data Store keine Bereitstellung von Data Node als automatischen Ersatz, wenn ein primärer Data Node ausfällt. Wenden Sie sich an den Cisco Support, wenn Sie Hilfe benötigen.

Sie müssen eine SMC mit Ihrem Data Store bereitstellen und sie für die Verwendung mit einem Data Store konfigurieren. Wenn Sie eine hohe Verfügbarkeit für Ihre SMC wünschen, können Sie auch eine Failover-SMC bereitstellen.

Darüber hinaus müssen Sie mindestens 1 Flow Collector mit Ihrem Data Store bereitstellen und die Flow Collectors für die Verwendung mit einem Data Store konfigurieren.

Für jede SMC und jeden Flow Collector, die bzw. den Sie bereitstellen, müssen Sie dem Management-Port `eth0` eine öffentliche, routbare IP-Adresse zuweisen. Bei der Bereitstellung eines Data Store können Sie die Verwendung eines BASE-T-Kupfer-1G/10G-Ports oder eines SFP+-Twinax-Kabel-10G-Ports für den `eth0`-Management-Port der SMC und des Flow Collectors konfigurieren. Cisco erfordert für den BASE-T-Kupfer-Port bei Verwendung eines Data Store einen 10G-Durchsatz. Benutzer ohne Data Store können nur die 100-Mbit/s- / 1-Gbit/s- / 10-Gbit/s-Kupferschnittstelle als `eth0` konfigurieren.

Sie können auch Flow Sensors und UDP Directors für Ihre Stealthwatch-Bereitstellung verwenden. Da diese Appliances nicht direkt mit dem Data Store kommunizieren, müssen Sie sie nicht für die Verwendung mit einem Data Store konfigurieren.

Weitere Informationen zu den unterstützten Plattformen finden Sie in den entsprechenden Datenblättern. Weitere Informationen zur Versionskompatibilität finden Sie in der Stealthwatch Hardware and Software Version Compatibility Matrix.

Überlegungen zu Stealthwatch-Unternehmensbereitstellungen

Beachten Sie Folgendes:

- Wenn Sie einen Flow Collector für die Kompatibilität mit einem Data Store konfigurieren, blendet die Appliance-Administrationsoberfläche (Appliance-Admin) bestimmte Funktionen aus. Verwenden Sie Central Management, um die Flow Collector-Konfiguration und andere damit verbundene Aufgaben durchzuführen. Wenn Sie Speicherstatistiken überwachen möchten, laden Sie die App „Report Builder“ auf Ihre SMC herunter.
- Verwenden Sie die Stealthwatch Web-App, um Ihre Stealthwatch-Installation zu überwachen und zu konfigurieren, wenn Sie einen Data Store bereitstellen. Der Stealthwatch Desktop-Client ist nicht mit einem Data Store kompatibel.
- Wenn Sie Ihre SMC für die Verwendung mit einem Data Store konfigurieren, können Sie die Apps ETA Cryptographic Audit oder Host Classifier nicht verwenden.

Erforderliche Anmeldeinformationen bei der Data Store-Bereitstellung

Bereiten Sie Kennwörter für die folgenden Benutzerkonten vor:

- `root` und `sysadmin` für jede SMC, jeden Data Node und jeden Flow Collector. Diese weisen Sie bei der Erstkonfiguration des Systems zu.
- `admin` für jede SMC, jeden Data Node und jeden Flow Collector. Diese weisen Sie mit dem Appliance Setup Tool zu.
- `dbadmin` und `readonlyuser` für den Data Store. Diese weisen Sie bei der Initialisierung des Data Store zu.

Data Store-Netzwerk- und Switching-Überlegungen

Die folgende Tabelle gibt einen Überblick über die Netzwerk- und Switching-Überlegungen bei der Bereitstellung eines Data Store.

Überlegungen zum	Beschreibung

Netzwerk	
Erforderliche Anmeldeinformationen	Für jeden Data Node, jede Stealthwatch Management Console und jeden Flow Collector: • Bei der ersten Systemkonfiguration konfiguriert: `root`, `sysadmin` • Mit dem Appliance Setup Tool konfiguriert: `admin` • Bei der Data Store-Initialisierung konfiguriert: `dbadmin`, `readonlyuser`
Inter-Data Node-Kommunikation	• Legen Sie eine empfohlene Round-Trip-Zeit-Latenz (RTT) unter 200 Mikrosekunden zwischen den Data Nodes fest. • Begrenzen Sie den Zeitversatz zwischen Ihren Data Nodes auf 1 Sekunde oder weniger. • Stellen Sie einen empfohlenen Durchsatz von 6,4 Gbit/s oder mehr (10 Gbit/s Vollduplex-Switch-Verbindung) zwischen Ihren Data Nodes her.
Stromversorgung der Data Node-Hardware	• Wenn unerwartet der Strom bei einem Hardware-Data Node ausfällt, können die Daten beschädigt werden. Verwenden Sie beide Netzteile an von unterbrechungsfreien Stromversorgungen getrennten Stromkreisen. • Wenn Sie den Data Store-Cluster initialisieren (weitere Informationen unter Data Store-Initialisierung und -Konfiguration), wechseln Sie die Data Node-Konfiguration basierend auf den Netzteilen, die jeder Data Node verwendet, ab. Dies kann die Fehlertoleranz optimieren, indem die Anzahl der Data Nodes, die bei einem Stromausfall ausfallen, minimiert wird.
Data Node Switching	• Data Nodes benötigen ihr eigenes Layer-2-VLAN, um die Inter-Data Node-Kommunikation zu ermöglichen. Hardware-Data Nodes können an einen gemeinsamen oder dedizierten 10G-Switch angeschlossen werden.

	• Cisco empfiehlt, die Hardware-Data Nodes an 2 Switches anzuschließen, um eine konstante Netzwerkverbindung bei Switch-Ausfällen und -Upgrades zu gewährleisten. Aufgrund der geringen Latenz, die für die Inter-Data Node-Kommunikation erforderlich ist, empfiehlt Cisco ein redundantes Switch-Paar, bei dem die beiden Switches miteinander verbunden sind und das Layer-2-VLAN über beide Switches übertragen.
Stealthwatch Appliance-Kommunikation	• SSH- und SSH-Root-Zugriff sind für SMC, Data Nodes und Flow Collector erforderlich und werden von der SMC aus konfiguriert. • SMC und Flow Collectors müssen in der Lage sein, alle Data Nodes zu erreichen. • Data Nodes müssen in der Lage sein, die SMC, alle Flow Collectors und jeden Data Node zu erreichen.

Sie müssen jedem Data Node folgende IP-Adressen zuweisen:

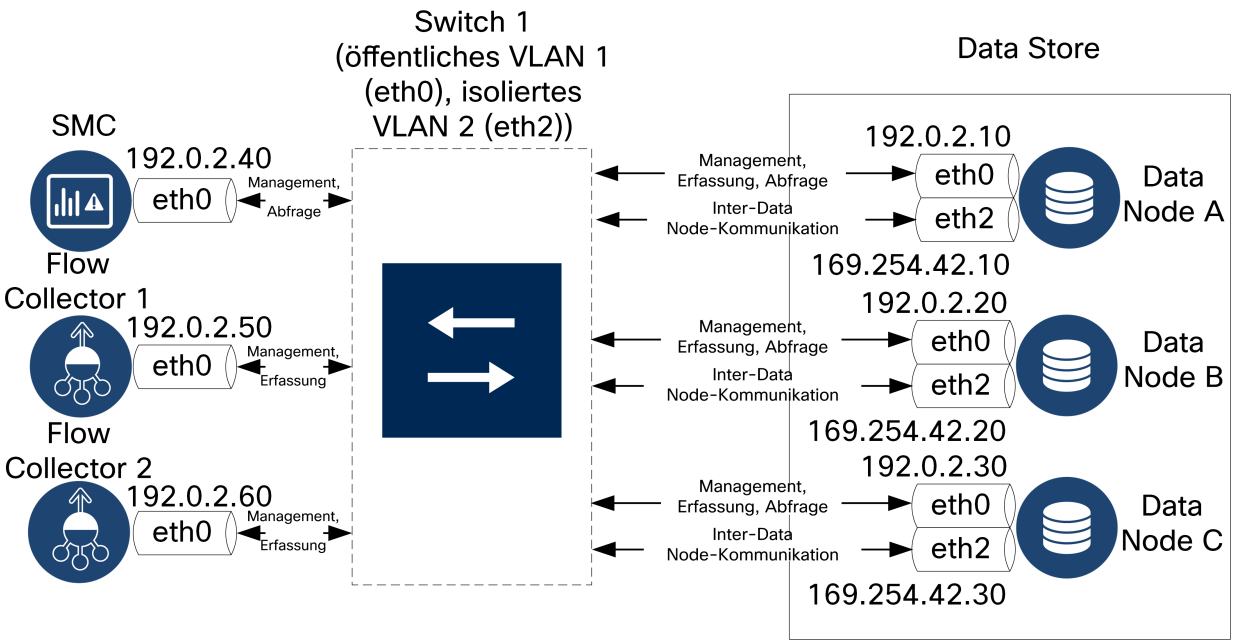
- eine routbare IP-Adresse für die Kommunikation mit Ihren Stealthwatch-Appliances (`eth0`). Verbinden Sie den Data Node-`eth0`-Port mit Ihrem Netzwerk, um die Kommunikation mit Ihrer SMC und den Flow Collectors zu ermöglichen. Sie können die Verwendung eines BASE-T-Kupfer-1G/10G-Ports oder eines SFP+-Twinax-Kabel-10G-Ports für den Data Node-`eth0`-Management-Port konfigurieren.

  Während der Data Store-Bereitstellung und -Konfiguration ordnen Sie die Data Node-`eth0`-IP-Adressen dem Data Store-Namen zu, um eine gleichmäßigere Verteilung der Telemetriespeicherung und der Abfrage- und Antwortvorgänge zu ermöglichen. Weitere Informationen finden Sie unter Initialisierung und Konfiguration der Data Store-Datenbank.
- eine nicht routbare IP-Adresse innerhalb eines privaten LANs oder VLANs, die für die Inter-Data Node-Kommunikation verwendet wird (`eth2` oder ein Port-Channel mit `eth2` und `eth3` zur Steigerung von Durchsatz und Leistung). Als Teil des Data Store kommunizieren Ihre Data Nodes untereinander. Verbinden Sie den Data Node-`eth2`-Port oder den Portkanal, der `eth2` und `eth3` enthält, mit den Switches für die Inter-Data Node-Kommunikation.

> Sie müssen die nicht routbaren IP-Adressen des `eth2`-Ports oder des `eth2/eth3`-Port-Channels aus dem CIDR-Block `169.254.42.0/24` zuweisen.

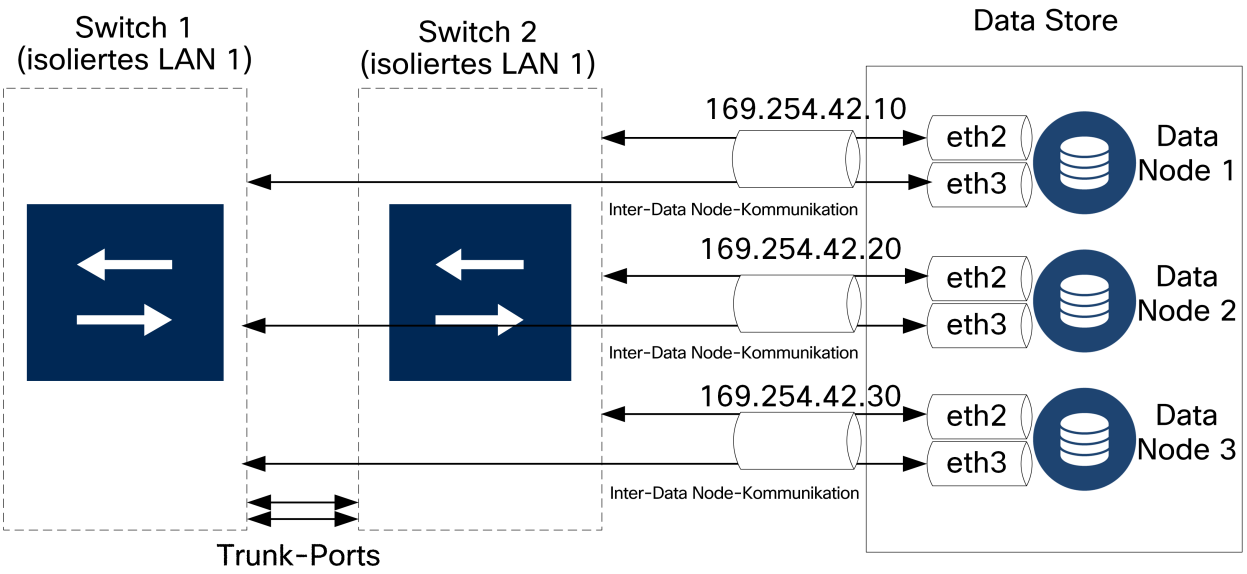
Die Konfiguration eines `eth2`-Ports für 10G-Durchsatz ist für die normale Inter-Data Node-Kommunikation ausreichend. Die Erstellung eines `eth2/eth3`-Port-Channels für bis zu 20G-Durchsatz ermöglicht eine schnellere Kommunikation der Data Nodes untereinander und ein schnelleres Hinzufügen oder Ersetzen von Data Nodes zum Data Store, da jeder neue Data Node Datenverkehr von benachbarten Data Nodes erhält, um seine Daten aufzufüllen.

Um die Inter-Data Node-Kommunikation über `eth2` oder den Port-Channel `eth2/eth3` zu ermöglichen, müssen Sie einen Switch bereitstellen, der 10G-Geschwindigkeiten unterstützt. Konfigurieren Sie ein öffentliches LAN oder VLAN für die `eth0`-Kommunikation der Data Nodes mit der SMC und den Flow Collectors und ein isoliertes LAN oder VLAN für die Inter-Data Node-Kommunikation. Sie können diese Switches mit anderen Appliances gemeinsam nutzen, aber separate LANs oder VLANs für den zusätzlichen Appliance-Datenverkehr erstellen. Nehmen Sie das folgende Diagramm als Beispiel.



Das Data Store-Cluster benötigt einen kontinuierlichen Heartbeat zwischen den Knoten innerhalb des isolierten VLANs. Ohne diesen Heartbeat können Data Nodes offline gehen, was das Risiko eines Data Store-Ausfalls erhöht. Wenn Sie zusätzliche Netzwerkredundanz wünschen, um Switch-Updates und geplante Ausfälle zu berücksichtigen, empfiehlt Cisco, dass Sie Ihre Data Nodes mit Port-Channels für die

dedizierte Inter-Data Node-Kommunikation konfigurieren. Verbinden Sie jeden Data Node mit 2 Switches, wobei jeder physikalische Port mit einem anderen Switch verbunden ist. Nehmen Sie das folgende Diagramm als Beispiel.



> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung Ihrer Bereitstellung zu erhalten.

Anforderungen und Überlegungen zur Data Store-Bereitstellung

Platzieren Sie jeden Data Node so, dass er mit allen Ihren Flow Collectors, Ihrer SMC und jedem anderen Data Node kommunizieren kann. Die beste Leistung erzielen Sie durch eine Co-Location Ihrer Data Nodes und Flow Collectors, um die Kommunikationslatenz zu minimieren, sowie Ihrer Data Nodes und der SMC für eine optimale Abfrageleistung. Cisco empfiehlt dringend, die Data Nodes innerhalb Ihrer Firewall zu platzieren, z. B. innerhalb eines NOC. Beachten Sie Folgendes für die Leistung:

- Legen Sie bei der Bereitstellung eine empfohlene Round-Trip-Zeit-Latenz (RTT) unter 200 Mikrosekunden zwischen den Data Nodes fest.
- Begrenzen Sie den Zeitversatz zwischen Ihren Data Nodes auf 1 Sekunde oder weniger.
- Stellen Sie einen empfohlenen Durchsatz von 6,4 Gbit/s oder mehr (10 Gbit/s Vollduplex-Switch-Verbindung) zwischen Ihren Data Nodes her.

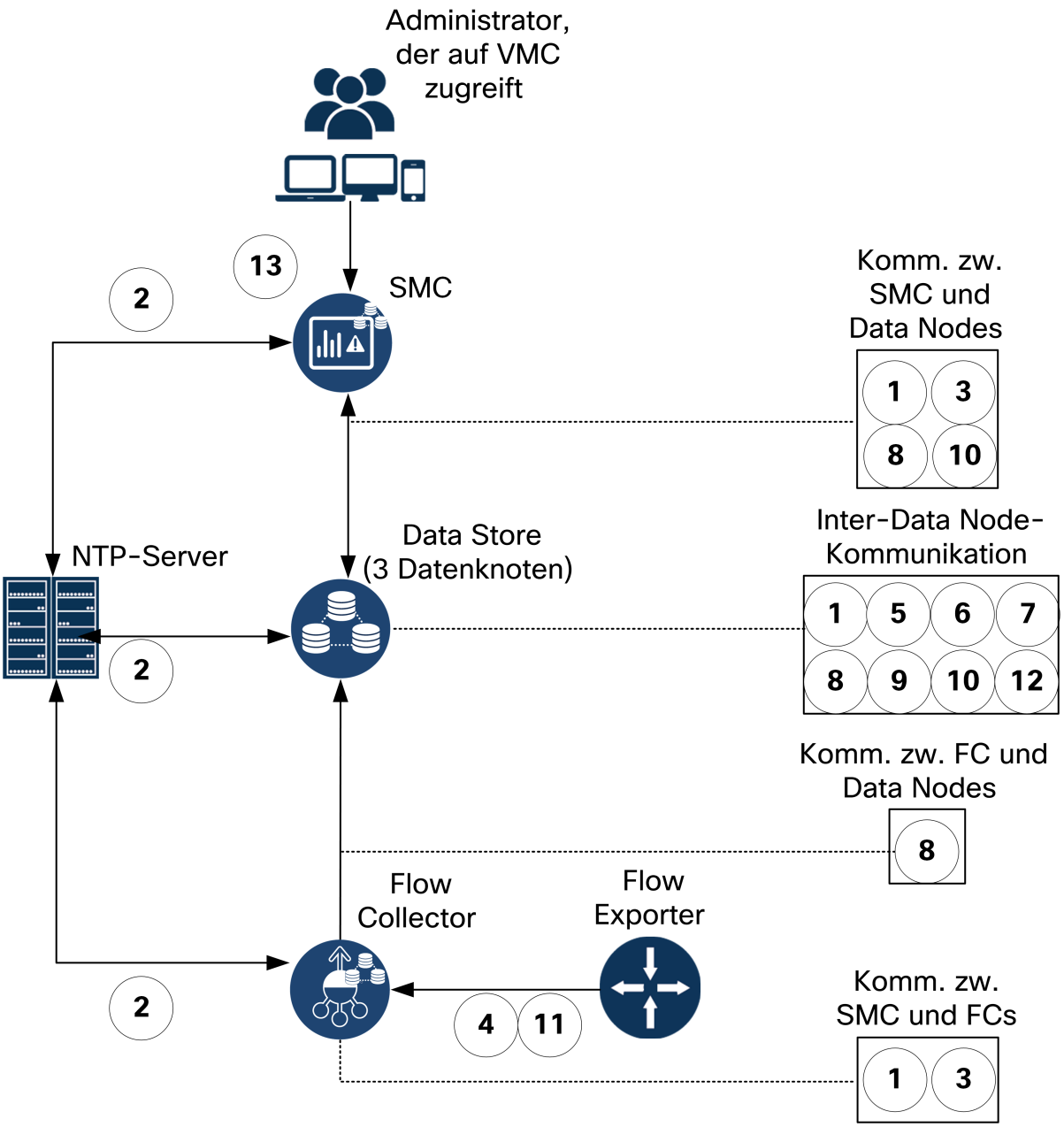
Wenn der Data Store aufgrund eines Stromausfalls oder Hardwarefehlers ausfällt, besteht ein erhöhtes Risiko von Datenbeschädigungen und Datenverlust. Cisco empfiehlt, Ihre Data Nodes so zu installieren, dass eine konstante Betriebszeit gewährleistet ist. Die folgenden Entwicklungen machen dies deutlich:

- Cisco empfiehlt dringend, redundante oder unterbrechungsfreie Stromversorgungen für jeden Data Node zu installieren, um Datenverluste oder Datenbeschädigungen im Falle eines Stromausfalls zu vermeiden.
- Prüfen Sie, ob die Richtlinie für die Wiederherstellung der Data Node-Stromversorgung auf **Restore Last State** (Letzten Status wiederherstellen) eingestellt ist. Dadurch wird der Data Node nach einem Stromausfall automatisch neu gestartet und versucht, laufende Prozesse wiederherzustellen. Weitere Informationen zum Konfigurieren der Richtlinie für die Wiederherstellung der Stromversorgung in CIMC finden Sie im UCS C-Series GUI Configuration Guide.
- Wenn Sie den Data Store initialisieren (weitere Informationen finden Sie unter Initialisierung und Konfiguration der Data Store-Datenbank), wechseln Sie die Data Node-Konfiguration je nach Stromversorgung ab. Der Data Store erstellt während der Konfiguration ein Data Node-Backup auf dem nächstfolgenden Data Node (das Backup des zuletzt konfigurierten Data Node wird auf dem als erstes konfigurierten Data Node erstellt). Wenn Sie Ihre Data Nodes mit zwei getrennten Netzteilen bereitstellen und die geraden und ungeraden Data Nodes basierend auf dem Netzteil abwechseln, kann bei einem Ausfall eines Netzteils und einer geraden Anzahl von Knoten der Data Store in Betrieb bleiben, da die Daten jedes Data Node bzw. die Backup-Daten von den mit Strom versorgten Data Nodes aus zugänglich sind.

> Wenn unerwartet die Stromversorgung eines Data Node ausfällt und Sie die Appliance neu starten, wird die Datenbankinstanz auf diesem Data Node möglicherweise nicht automatisch neu gestartet. Informationen zum manuellen Neustart der Datenbankinstanz finden Sie unter Data Store-Fehlerbehebung.

Data Store Kommunikations-Ports

Das folgende Diagramm zeigt eine Stealthwatch-Beispielarchitektur mit den Kommunikationsports, die geöffnet werden sollten. In der Tabelle finden Sie die Ports, die den einzelnen Callouts zugeordnet sind.



Im Folgenden sind die Kommunikationsports aufgelistet, die auf Ihrer Firewall geöffnet werden müssen, um den Data Store bereitzustellen. Im Stealthwatch-Systemkonfigurationshandbuch finden Sie weitere Kommunikationsports, die Sie für Ihre gesamte Stealthwatch-Bereitstellung öffnen sollten.

#	Von (Client)	An (Server)	Anschluss	Protokoll oder Zweck
1	SMC	Flow Collectors und Data Nodes	22/TCP	SSH, erforderlich zum Initialisieren der Data Store-Datenbank
1	Data Nodes	alle anderen Data Nodes	22/TCP	SSH, erforderlich zum Initialisieren der Data Store-Datenbank und für Datenbankadministrationsaufgaben
2	SMC, Flow Collectors und Data Nodes	NTP-Server	123/UDP	NTP, erforderlich für die Zeitsynchronisierung
2	NTP server	SMC, Flow Collectors und Data Nodes	123/UDP	NTP, erforderlich für die Zeitsynchronisierung
3	SMC	Flow Collectors und Data Nodes	443/TCP	HTTPS, erforderlich für die sichere Kommunikation zwischen Appliances
3	Flow Collectors	SMC	443/TCP	HTTPS, erforderlich für die sichere Kommunikation zwischen Appliances
3	Data Nodes	SMC	443/TCP	HTTPS, erforderlich für die sichere Kommunikation zwischen Appliances
4	NetFlow-Exporter	Flow Collectors – NetFlow	2055/UDP	NetFlow-Erfassung
5	Data Nodes	alle anderen	4803/TCP	Inter-Data Node-Messaging-Dienst

		Data Nodes		
6	Data Nodes	alle anderen Data Nodes	4803/UDP	Inter-Data Node-Messaging-Dienst
7	Data Nodes	alle anderen Data Nodes	4804/UDP	Inter-Data Node-Messaging-Dienst
8	SMC, Flow Collectors und Data Nodes	Data Nodes	5433/TCP	Vertica Client-Verbindungen
9	Data Node	alle anderen Data Node	5433/UDP	Vertica Messaging-Dienst-Überwachung
10	SMC	Data Nodes	5444/TCP	Vertica Management Console für sichere Kommunikation
10	Data Nodes	SMC und alle anderen Data Nodes	5444/TCP	Vertica Management Console für sichere Kommunikation
11	sFlow-Exporter	Flow Collectors – sFlow	6343/UDP	sFlow-Erfassung
12	Data Nodes	alle anderen Data Nodes	6543/UDP	Inter-Data Node-Messaging-Dienst
13	Administrator-Workstations, um auf die Vertica Management Console zuzugreifen	SMC	9450/TCP	Zugriff auf die Vertica Management Console im Webbrowser

Stealthwatch Data Store-Bereitstellungsübersicht

> ⚠ Wenn Sie einen Stealthwatch Data Store erwerben möchten, wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Platzierung, Bereitstellung und Konfiguration innerhalb und im Rahmen Ihrer gesamten Stealthwatch-Bereitstellung zu erhalten. Installieren Sie **keinen** Data Store allein.

Im Folgenden werden die allgemeinen Schritte für die Bereitstellung von Data Store mit einer Stealthwatch-Bereitstellung beschrieben:

- Stellen Sie Ihre Stealthwatch-Appliances einschließlich Ihrer Data Nodes bereit und konfigurieren Sie Ihre SMC und Flow Collectors für die Verwendung mit einer Data Store-Bereitstellung.

  > ℹ Stellen Sie sicher, dass Sie die neueste Version und den Rollup-Patch für Ihre Appliances installieren, nachdem Sie sie bereitgestellt haben, aber bevor Sie mit der Initialisierung und Konfiguration von Data Store fortfahren.

- Bereiten Sie Ihre Stealthwatch-Bereitstellung für die Data Store-Verwendung vor, indem Sie Benutzerkennwörter und Identitätszertifikate verteilen.
- Initialisieren Sie den Data Store.
- Konfigurieren Sie Vertica Management Console (VMC) auf Ihrer SMC und aktivieren Sie Warnschwellenwerte und Benachrichtigungen.
- Konfigurieren Sie die Data Store-Aufbewahrungseinstellungen über die REST-API.
- Installieren Sie Stealthwatch-Apps auf Ihrer SMC, um zusätzliche Data Store-Funktionen zu erhalten.

Überprüfen Sie, ob diese Aufgaben abgeschlossen wurden, bevor Sie mit der Bereitstellung beginnen.

Erforderliche Komponente und Aufgabe	Schritte
SMC-Installation und -Konfiguration	Weitere Informationen finden Sie unter SMC-Konfiguration für die Verwendung mit einem Data Store. 1. Stellen Sie Ihre SMC in Ihrem Netzwerk bereit. 2. Melden Sie sich über CIMC oder eine direkte Verbindung zur Appliance als `root` bei der SMC-Konsole an. Führen Sie das Systemkonfigurationsskript `systemconfig` aus und verwenden Sie den Ersteinrichtungsassistenten, um grundlegende Managementinformationen wie die IP-Adresse der Appliance, die Verwendung mit einem Data Store und den physischen Port `eth0` zu konfigurieren. 3. Navigieren Sie in einem Webbrowser zur `eth0`-IP-Adresse der SMC, um auf das Appliance Setup Tool zuzugreifen. Verwenden Sie das Appliance Setup Tool, um Administratorkennwörter, Stealthwatch-Domäne sowie DNS- und NTP-Server zu konfigurieren und Central Management zu installieren. 4. Navigieren Sie, nachdem Sie die Appliance mit dem Appliance Setup Tool konfiguriert haben, in einem Webbrowser zur IP-Adresse der SMC, um auf die Stealthwatch Web App zuzugreifen. Aktivieren Sie in Central Management den SSH-Zugriff und den SSH-Root-Zugriff auf die SMC. 5. Aktualisieren Sie Ihre SMC auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.
Data Node Installation und -Konfiguration	Weitere Informationen finden Sie unter Data Store-Hardware-Erstbereitstellung und -konfiguration. 1. Stellen Sie Ihre Data Nodes in Ihrem Netzwerk bereit.

	2. Melden Sie sich über CIMC oder eine direkte Verbindung zur Appliance bei jeder Data Node-Konsole als `root` an. Führen Sie das Systemkonfigurationsskript `systemconfig` aus und verwenden Sie den Ersteinrichtungsassistenten, um grundlegende Managementinformationen wie die Management-IP-Adresse der Appliance und die nicht routbare IP-Adresse für die Konfiguration zwischen den Data Nodes zu konfigurieren. Weisen Sie dem `eth2`- oder dem `eth2/eth3`-Port-Channel eine nicht routbare IP-Adresse aus dem CIDR-Block `169.254.42.0/24` zu. 3. Navigieren Sie für jeden Data Node in einem Webbrowser zur routbaren `eth0`-IP-Adresse des Data Nodes, um auf das Appliance Setup Tool zuzugreifen. Verwenden Sie Appliance Setup Tool auf jedem Data Node, um Administratorkennwörter, Stealthwatch-Domäne, DNS und NTP-Server zu konfigurieren sowie die Verwaltung des Data Node durch Central Management einzurichten. 4. Wechseln Sie in der Stealthwatch-Web-App zu „Central Management“ (zentrales Management) und aktivieren Sie SSH-Zugriff und SSH-Root-Zugriff auf jeden Data Node. 5. Aktualisieren Sie Ihre Data Nodes auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes. **Lesen Sie alle zutreffenden Aktualisierungsleitfäden und die Patch-Readme-Dokumentation, bevor Sie fortfahren. Der Data Node-Aktualisierungsprozess erfordert im Vergleich zu anderen Stealthwatch-Appliances zusätzliche Schritte.**
Flow Collector-Installation und -Konfiguration	Weitere Informationen finden Sie unter Flow Collector-Konfiguration für die Verwendung mit einem Data Store. 1. Stellen Sie Ihre Flow Collectors in Ihrem Netzwerk bereit.

	2. Melden Sie sich über CIMC oder eine direkte Verbindung zur Appliance bei jeder Flow Collector-Konsole als `root` an. Führen Sie das Systemkonfigurationsskript `systemconfig` aus und verwenden Sie den Ersteinrichtungsassistenten, um grundlegende Managementinformationen wie die IP-Adresse der Appliance, die Verwendung mit einem Data Store und den physischen Port eth0 zu konfigurieren. 3. Navigieren Sie in einem Webbrowser zur `eth0`-IP-Adresse jedes Flow Collectors, um auf das Appliance Setup Tool zuzugreifen. Verwenden Sie das Appliance Setup Tool auf jedem Flow Collector, um Administratorkennwörter, Stealthwatch-Domänen, DNS- und NTP-Server sowie die Flow Collection-Port-Nummer (`2055` für NetFlow oder `6343` für sFlow) zu konfigurieren und die Verwaltung des Flow Collectors durch Central Management einzurichten. 4. Wechseln Sie in der Stealthwatch-Web-App zu „Central Management“ (zentrales Management) und aktivieren Sie SSH-Zugriff und SSH-Root-Zugriff auf jeden Flow Collector. 5. Aktualisieren Sie Ihre Flow Collectors auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.
Data Store Initialisierung und Konfiguration	Weitere Informationen finden Sie unter Initialisierung und Konfiguration der Data Store-Datenbank. 1. Gehen Sie in der Stealthwatch-Web-App zu Central Management und stellen Sie sicher, dass alle Data Nodes und Flow Collectors in Central Management verwaltet werden, dass die Verbindung besteht und dass sowohl SSH-Zugriff als auch SSH-Root-Zugriff aktiviert sind. 2. Melden Sie sich an der Konsole der primären SMC als `sysadmin`an. Verteilen Sie mithilfe des Skripts `setup-sw-datastore-secure-connectivity` für sichere

	Datenbankverbindungen die Datenbank-Kennwörter und -Identitätszertifikate `dbadmin` und `readonlyuser` an Ihre SMCs, Data Nodes und Flow Collectors. 3. Melden Sie sich basierend auf der Ausgabe des Skripts `setup-sw-datastore-secure-connectivity` für die sichere Verbindung bei der Konsole des angegebenen Data Node als `root` an. Kopieren Sie die Beispiel-Konfigurationsdatei `install_SDBN_example.cfg` für die Datenbankinitialisierung als `install_SDBN.cfg` und aktualisieren Sie sie mit den IP-Adressen und dem Subnetz Ihres Data Node. Führen Sie das Initialisierungsskript aus und referenzieren Sie die Initialisierungskonfigurationsdatei (`python install_SDBN_initial.py -i install_SDBN.cfg`). 4. Rufen Sie auf dem Data Node, auf dem Sie das Initialisierungsskript ausgeführt haben, die API-Schlüsselzeichenfolge unter `/opt/vertica/config/apikey.dat` ab. Sie verwenden diesen API-Schlüssel, um in einem späteren Schritt eine Verbindung zwischen der Data Store-Datenbank und VMC herzustellen. 5. Gehen Sie in der Stealthwatch-Web-App zu Central Management und verwenden Sie für die SMC und alle Flow Collectors die lokale Auflösung, um jeder routbaren Data Node-IP-Adresse den Data Store-Datenbanknamen (`sw-datastore`) zuzuordnen. Um eine optimale Leistung zu erzielen, ordnen Sie die Data Node-`eth0`-IP-Adressen für jede Appliance in der gleichen Reihenfolge zu.
Installation und Konfiguration der Vertica Management Console (VMC) auf der SMC	Weitere Informationen finden Sie unter Konfiguration der Vertica Management Console. 1. Kopieren Sie das Serverzertifikat `/lancope/var/admin/cds/ server.crt` von Ihrer SMC auf Ihre lokale Workstation. 2. Navigieren Sie in einem Webbrowser auf Ihrer lokalen Workstation zu `[smc-ipv4-`

	address]:9450/webui/login, um auf die VMC zuzugreifen. Führen Sie die Erstkonfiguration und -einrichtung der VMT durch. Deaktivieren Sie Verbindungen, die weniger sichere Versionen von TLS verwenden. Verwenden Sie die API-Schlüsselzeichenfolge und die Zertifikatsdatei server.crt, um eine Verbindung mit dem Data Store herzustellen. Konfigurieren Sie Warngrenzwerte und Warnmeldungen, um Data Store-Zustandswarnungen zu erhalten.
Data Store Datenaufbewahrung	Weitere Informationen finden Sie unter Konfiguration der Data Store-Datenaufbewahrung. • Verwenden Sie die REST-API, um den Datenaufbewahrungszeitraum Ihres Data Store zu konfigurieren.
Nach Abschluss der Data Store-Bereitstellung siehe „Nächste Schritte“.	Siehe Nächste Schritte nach der Data Store-Installation: 1. Installieren Sie die App „Stealthwatch Report Builder“ auf Ihrer SMC, um Berichte zu Ihrer Stealthwatch-Bereitstellung zu erstellen und Data Store-Speicherstatistiken anzuzeigen. Weitere Informationen finden Sie in den Versionshinweisen. 2. Weitere Informationen zur Verwendung von Stealthwatch finden Sie in der Online-Hilfe der Stealthwatch Web App.

Optional können Sie auch Folgendes durchführen:

Optionale Komponente und Aufgabe	**Schritte**
Installation und Konfiguration von UDP Director	• Stellen Sie UDP Director bereit, wie im Hardware-Installationshandbuch zur Stealthwatch x2xx-Serie und im Stealthwatch-Systemkonfigurationshandbuch beschrieben. Aktualisieren Sie Ihren UDP Director auf die neueste Version und den neuesten Patch. Weitere Informationen zum

	Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.
Flow Sensor	• Stellen Sie den Flow Sensor bereit, wie im Hardware-Installationshandbuch zur Stealthwatch x2xx-Serie und im Stealthwatch-Systemkonfigurationshandbuch beschrieben. Aktualisieren Sie Ihren Flow Sensor auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.
Failover bei SMC-Installation und -Konfiguration	• Stellen Sie die Failover-SMC bereit, wie im Hardware-Installationshandbuch zur Stealthwatch x2xx-Serie, im Stealthwatch-Systemkonfigurationshandbuch und im Stealthwatch Failover-Konfigurationsleitfaden beschrieben. Aktualisieren Sie Ihre SMC auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.

Installation der Data Store-Hardware

> Wenn Sie eine Stealthwatch Data Store erwerben möchten, wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Platzierung, Bereitstellung und Konfiguration innerhalb und im Rahmen Ihrer gesamten Bereitstellung von Stealthwatch zu erhalten.

Stealthwatch Hardwarebereitstellung und Überlegungen

Stellen Sie Ihre SMC-, Data Node- und Flow Collector-Stealthwatch-Appliances gemäß den folgenden Anweisungen bereit und konfigurieren Sie sie, und installieren Sie Switches für den Data Store in Ihrem Netzwerk. Wenn Sie Ihre Data Nodes bereitstellen und mit Ihrem Netzwerk verbinden, lesen Sie die Anforderungen und Überlegungen zur Data Store-Bereitstellung. Stellen Sie sicher, dass Ihre SMC, Data Nodes und Flow Collectors dieselbe Version haben (7.3 und höher). Weitere Informationen zur Erstinstallation und Konfiguration der Appliance finden Sie im Hardware-Installationshandbuch für die Stealthwatch x210-Serie oder in **Anhang A. Vorbereitung der Installation** sowie **Anhang B. Stealthwatch Installation der Hardware**.

> Wenn Sie einen Data Store in Ihrem Netzwerk als Teil einer vorhandenen Stealthwatch-Bereitstellung bereitstellen möchten, arbeiten Sie mit Cisco Professional Services zusammen, um den Data Store zu integrieren. Wenden Sie sich für weitere Informationen an den Cisco Support.

> Verwenden Sie die Stealthwatch Web-App, um Ihre Stealthwatch-Installation zu überwachen und zu konfigurieren, wenn Sie einen Data Store bereitstellen. Der Stealthwatch Desktop-Client ist nicht mit einem Data Store kompatibel.

SMC-Konfiguration für die Verwendung mit einem Data Store

Stellen Sie Ihre SMC bereit und konfigurieren Sie sie für die Verwendung mit einem Data Store. Richten Sie sie außerdem zur Verwaltung Ihrer Data Nodes und Flow Collectors ein.

> Wenn Sie eine sekundäre SMC haben, konfigurieren Sie diese zuerst, damit die primäre SMC mit ihr kommunizieren kann. Weitere Informationen zum Einrichten eines SMC-Failover-Paares finden Sie im Stealthwatch-

> Systemkonfigurationshandbuch. Weitere Informationen zur Bereitstellung und Konfiguration einer sekundären SMC für die Zusammenarbeit mit einem **Failover-Bereitstellung der Stealthwatch Management Console**Failover-Bereitstellung der Stealthwatch Management Console Data Store.

Führen Sie die folgenden Schritte aus:

1. Stellen Sie zunächst Ihre SMC in Ihrem Netzwerk bereit. Verbinden Sie sich dann über CIMC, eine Tastatur und einen Monitor oder einen Laptop mit Ihrer Appliance und melden Sie sich bei der Konsole als `root` an. Führen Sie `systemconfig` aus und verwenden Sie den Ersteinrichtungsassistenten, um die Management-Port-Einstellungen, die Verwendung mit einem Data Store und die `root`- und `sysadmin`-Benutzerkennwörter zu aktualisieren. Weitere Informationen finden Sie im Hardware-Installationshandbuch für die Stealthwatch x210-Serie oder in **Anhang A. Vorbereitung der Installation** sowie **Anhang B. Stealthwatch Installation der Hardware**.

   > Wenn Sie zum ersten Mal auf die Systemkonfiguration zugreifen (und nur dann), führt Sie das System zum Ersteinrichtungsmodus, der Sie automatisch durch den anfänglichen Konfigurationsprozess der Appliance führt.

   > ⚠ Nachdem Sie Ihre SMC oder Ihren Flow Collector für die Verwendung mit einem Data Store konfiguriert haben, können Sie die Konfiguration der Appliance nicht mehr aktualisieren, um diese Konfiguration zu ändern. Sie müssen RFD für die Appliance ausführen, wenn Sie die falsche Auswahl treffen. Aktivieren Sie diese Option nur, wenn Sie planen, einen Data Store in Ihrem Netzwerk bereitzustellen.

2. Navigieren Sie als nächstes in einem Webbrowser zu der IP-Adresse, die Sie dem Management-Port zugewiesen haben. Verwenden Sie das Appliance Setup Tool, um zusätzliche Konfigurationen durchzuführen, einschließlich der Zuweisung des `admin`-Benutzerkennworts (sowie des `root`- und des `sysadmin`-Kennworts, wenn Sie diese nicht während der Systemkonfiguration zugewiesen haben), der Stealthwatch-Domänenkonfiguration, anderer Netzwerkkonfigurationen, DNS- und NTP-Einstellungen und der Installation von Central Management auf der SMC. Weitere Informationen finden Sie im Stealthwatch-Systemkonfigurationshandbuch oder in **Anhang C. Konfigurieren Ihrer Appliances**.
3. Aktivieren Sie dann SSH-Zugriff und SSH-Root-Zugriff auf Ihrer SMC. Um den

Data Store zu initialisieren, wie unter **Data Store-Initialisierung und -Konfiguration** beschrieben, müssen Sie ein Skript ausführen, das den SSH-Zugriff auf jede Appliance verwendet.

> ⚠ Wenn SSH aktiviert ist, steigt das Kompromittierungsrisiko des Systems. Es ist wichtig, SSH nur zu aktivieren, wenn Sie es brauchen. Wenn Sie SSH nicht mehr verwenden, deaktivieren Sie es.

Aktualisieren Sie die SSH-Zugriffsberechtigung der SMC:

Vorbereitungen

- Melden Sie sich bei der SMC-Web-App als Systemadministrator an.

Verfahren

1. Greifen Sie auf das Appliance Manager-Dashboard zu. Folgende Optionen sind hierzu verfügbar:
   - Das Appliance Setup Tool wird im Appliance Manager-Dashboard geöffnet, wenn Sie die Appliance-Einrichtung abgeschlossen haben.
   - Klicken Sie auf das Symbol **Global Settings** (Globale Einstellungen). Wählen Sie **Central Management** (Zentrales Management). Das Appliance Manager-Dashboard wird angezeigt.
2. Klicken Sie beim SMC-Posteneintrag auf das Menü „Actions“ (Aktionen) und wählen Sie **Edit Appliance Configuration** (Appliance-Konfiguration bearbeiten) aus.
3. Wählen Sie die Registerkarte „Appliance“ aus.
4. Wählen Sie im Bereich „SSH“ die Option **Enable SSH** (SSH aktivieren) aus.
5. Wählen Sie **Enable Root SSH Access** (SSH-Root-Zugriff aktivieren) aus.
6. Klicken Sie auf **Apply Settings** (Einstellungen übernehmen).

Nächste Schritte

- Aktualisieren Sie Ihre SMC auf die neueste Version und den neuesten Patch, wie im nächsten Schritt beschrieben.

1. Aktualisieren Sie zuletzt Ihre SMC auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden

Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.

Nachdem Sie Ihre SMC aktualisiert haben, haben Sie die folgenden Optionen:

- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
- Ihre Data Nodes bereitstellen und konfigurieren, wie im nächsten Abschnitt beschrieben.

Data Store Hardware-Erstbereitstellung und -konfiguration

Nachdem Sie Ihre SMC bereitgestellt haben, stellen Sie Ihre Data Node-Appliances bereit und konfigurieren Sie sie. Wenn Sie Ihre Data Nodes bereitstellen und mit Ihrem Netzwerk verbinden, lesen Sie die Anforderungen und Überlegungen zur Data Store-Bereitstellung.

Führen Sie für jeden Data Node die folgenden Schritte aus:

1. Stellen Sie zunächst den Data Node im Netzwerk bereit. Verbinden Sie sich dann über CIMC, eine Tastatur und einen Monitor oder einen Laptop mit der Data Node-Appliance und melden Sie sich bei der Konsole als `root` an. Führen Sie `systemconfig` aus, und verwenden Sie den Ersteinrichtungsassistenten, um die Management-Port-Einstellungen, die Einstellungen der Ports für die Kommunikation zwischen den Data Nodes und die Benutzerkennwörter für `root` und `sysadmin` zu aktualisieren. Weitere Informationen finden Sie im Hardware-Installationshandbuch für die Stealthwatch x210-Serie oder in **Anhang A. Vorbereitung der Installation** sowie **Anhang B. Stealthwatch Installation der Hardware**.

   > Wenn Sie zum ersten Mal auf die Systemkonfiguration zugreifen (und nur dann), führt Sie das System zum Ersteinrichtungsmodus, der Sie automatisch durch den anfänglichen Konfigurationsprozess der Appliance führt.

2. Navigieren Sie als nächstes in einem Webbrowser zu der IP-Adresse, die Sie dem Management-Port zugewiesen haben. Verwenden Sie das Appliance Setup Tool, um zusätzliche Konfigurationen durchzuführen, einschließlich der Zuweisung des `admin`-Benutzerkennworts (sowie des `root`- und des `sysadmin`-Kennworts, wenn Sie diese nicht während der Systemkonfiguration zugewiesen haben), der Stealthwatch-Domänenkonfiguration, anderer Netzwerkkonfigurationen, DNS-

und NTP-Einstellungen und der Einrichtung des Data Node über Central Management. Weitere Informationen finden Sie im Stealthwatch-Systemkonfigurationshandbuch oder in **Anhang C. Konfigurieren Ihrer Appliances**.

3. Aktivieren Sie zuletzt SSH-Zugriff und SSH-Root-Zugriff auf Ihrem Data Node. Um den Data Store zu initialisieren, wie unter **Data Store-Initialisierung und -Konfiguration** beschrieben, müssen Sie ein Skript ausführen, das den SSH-Zugriff auf jede Appliance verwendet.

> ⚠ Wenn SSH aktiviert ist, steigt das Kompromittierungsrisiko des Systems. Es ist wichtig, SSH nur zu aktivieren, wenn Sie es brauchen. Wenn Sie SSH nicht mehr verwenden, deaktivieren Sie es.

Aktualisieren der SSH-Zugriffsberechtigung eines Data Node:

Vorbereitungen

- Melden Sie sich bei der SMC-Web-App als Systemadministrator an.

Verfahren

1. Greifen Sie auf das Appliance Manager-Dashboard zu. Folgende Optionen sind hierzu verfügbar:
   - Das Appliance Setup Tool wird im Appliance Manager-Dashboard geöffnet, wenn Sie die Appliance-Einrichtung abgeschlossen haben.
   - Klicken Sie auf das Symbol **Global Settings** (Globale Einstellungen). Wählen Sie **Central Management** (Zentrales Management). Das Appliance Manager-Dashboard wird angezeigt.

   Überprüfen Sie die Liste der Appliances und vergewissern Sie sich, dass Ihr Data Node aufgeführt ist und dass der Appliance-Status **Up** ist.
2. Klicken Sie beim Data Node-Posteneintrag auf das Menü „Actions“ (Aktionen) und wählen Sie **Edit Appliance Configuration** (Appliance-Konfiguration bearbeiten) aus.
3. Wählen Sie die Registerkarte „Appliance“ aus.
4. Wählen Sie im Bereich „SSH“ die Option **Enable SSH** (SSH aktivieren) aus.

5. Wählen Sie **Enable Root SSH Access** (SSH-Root-Zugriff aktivieren) aus.
6. Klicken Sie auf **Apply Settings** (Einstellungen übernehmen).

Nächste Schritte

- Aktualisieren Sie Ihren Data Node auf die neueste Version und den neuesten Patch, wie im nächsten Schritt beschrieben.

1. Aktualisieren Sie zuletzt Ihren Data Node auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.

   > Lesen Sie alle zutreffenden Aktualisierungsleitfäden und die Patch-Readme-Dokumentation, bevor Sie fortfahren. Der Data Node-Aktualisierungsprozess erfordert im Vergleich zu anderen Stealthwatch-Appliances zusätzliche Schritte.

   Nach der Aktualisierung Ihres Data Node haben Sie folgende Optionen:

   - Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
   - Zu **Data Store Hardware-Erstbereitstellung und -konfiguration** zurückkehren und die Data Node-Installation und -Erstkonfiguration, die Konfiguration des Appliance Setup Tools sowie die Einrichtung von Central Management für die verbleibenden Data Nodes wiederholen.
2. Nachdem Sie alle Ihre Data Nodes bereitgestellt und konfiguriert haben, haben Sie die folgenden Optionen:
   - Ihren UDP Director, falls vorhanden, konfigurieren, wie im nächsten Abschnitt beschrieben.
   - Ihre Flow Collectors konfigurieren, wenn Sie keinen UDP Director haben, wie unter **Flow Collector-Konfiguration für die Verwendung mit einem Data Store** beschrieben.

UDP Director-Bereitstellung

Wenn Sie einen UDP Director bereitstellen möchten, befolgen Sie die Anweisungen im Hardware-Installationshandbuch zur Stealthwatch x210-Serie und im Stealthwatch-Systemkonfigurationshandbuch. Beachten Sie, dass der UDP Director-Installationsprozess unverändert bleibt, egal ob Sie einen Data Store bereitstellen oder nicht. Sie müssen keinen UDP Director für die Verwendung mit einem Data Store konfigurieren.

Nachdem Sie UDP Director bereitgestellt haben, haben Sie die folgenden Optionen.

- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
- Ihre Flow Collectors bereitstellen und konfigurieren, wie im nächsten Abschnitt beschrieben.

Flow Collector-Konfiguration für die Verwendung mit einem Data Store

Nachdem Sie Ihre Data Nodes und, sofern bereitgestellt, Ihre UDP Directors konfiguriert haben, stellen Sie Ihre Flow Collectors bereit und konfigurieren Sie sie.

Führen Sie für jeden Flow Collector die folgenden Schritte aus:

1. Stellen Sie zunächst den Flow Collector in Ihrem Netzwerk bereit. Verbinden Sie sich dann über CIMC, eine Tastatur und einen Monitor oder einen Laptop mit dem Flow Collector und melden Sie sich bei der Konsole als `root` an. Führen Sie `systemconfig` aus und verwenden Sie den Ersteinrichtungsassistenten, um die Management-Port-Einstellungen, die Verwendung mit einem Data Store und die `root`- und `sysadmin`-Benutzerkennwörter zu aktualisieren. Weitere Informationen finden Sie im Hardware-Installationshandbuch für die Stealthwatch x210-Serie oder in **Anhang A. Vorbereitung der Installation** sowie **Anhang B. Stealthwatch Installation der Hardware**.

   > Wenn Sie zum ersten Mal auf die Systemkonfiguration zugreifen (und nur dann), führt Sie das System zum Ersteinrichtungsmodus, der Sie automatisch durch den anfänglichen Konfigurationsprozess der Appliance führt.

   > Nachdem Sie Ihre SMC oder Ihren Flow Collector für die Verwendung mit einem Data Store konfiguriert haben, können Sie die Konfiguration der Appliance nicht mehr aktualisieren, um diese Konfiguration zu ändern. Sie müssen RFD für die Appliance ausführen, wenn Sie die falsche Auswahl treffen. Aktivieren Sie diese Option nur, wenn Sie planen, einen Data Store in Ihrem Netzwerk bereitzustellen.

2. Navigieren Sie als nächstes in einem Webbrowser zu der IP-Adresse, die Sie dem Management-Port zugewiesen haben. Verwenden Sie das Appliance Setup Tool, um zusätzliche Konfigurationen durchzuführen, einschließlich der Zuweisung des `admin`-Benutzerkennworts (sowie des `root`- und des `sysadmin`-Kennworts,

wenn Sie diese nicht während der Systemkonfiguration zugewiesen haben), der Stealthwatch-Domänenauswahl, anderer Netzwerkkonfigurationen, DNS- und NTP-Einstellungen, der Flow Collection-Port-Nummer (`2055` für NetFlow oder `6343` für sFlow) und der Einrichtung des Flow Collectors durch Central Management. Weitere Informationen finden Sie im Stealthwatch-Systemkonfigurationshandbuch oder in **Anhang C. Konfigurieren Ihrer Appliances**.

> Wenn Sie einen Flow Collector für die Verwendung mit einem Data Store konfigurieren, blendet die Appliance-Administrationsoberfläche (Appliance-Admin) bestimmte Funktionen aus. Verwenden Sie Central Management, um die Flow Collector-Konfiguration und andere damit verbundene Aufgaben durchzuführen. Wenn Sie Speicherstatistiken überwachen möchten, laden Sie die App „Data Store Storage Statistics“ auf Ihre SMC herunter.

3. Aktivieren Sie zuletzt SSH-Zugriff und SSH-Root-Zugriff auf Ihren Flow Collectors. Um den Data Store zu initialisieren, wie unter **Data Store-Initialisierung und -Konfiguration** beschrieben, müssen Sie ein Skript ausführen, das den SSH-Zugriff auf jede Appliance verwendet.

> Wenn SSH aktiviert ist, steigt das Kompromittierungsrisiko des Systems. Es ist wichtig, SSH nur zu aktivieren, wenn Sie es brauchen. Wenn Sie SSH nicht mehr verwenden, deaktivieren Sie es.

Aktualisieren der SSH-Zugriffsberechtigung eines Flow Collectors:

Vorbereitungen

- Melden Sie sich bei der SMC-Web-App als Systemadministrator an, wenn Sie das Appliance Setup Tool nicht verwenden.

Verfahren

1. Greifen Sie auf das Appliance Manager-Dashboard zu. Folgende Optionen sind hierzu verfügbar:
    - Das Appliance Setup Tool wird im Appliance Manager-Dashboard geöffnet, wenn Sie die Appliance-Einrichtung abgeschlossen haben.

- Klicken Sie auf das Symbol **Global Settings** (Globale Einstellungen). Wählen Sie **Central Management** (Zentrales Management). Das Appliance Manager-Dashboard wird angezeigt.

Überprüfen Sie die Liste der Appliances und vergewissern Sie sich, dass Ihr Flow Collector aufgeführt ist und dass der Appliance-Status **Up** ist.

2. Klicken Sie beim Flow Collector-Posteneintrag auf das Menü „Actions“ (Aktionen) und wählen Sie **Edit Appliance Configuration** (Appliance-Konfiguration bearbeiten) aus.
3. Wählen Sie die Registerkarte „Appliance“ aus.
4. Wählen Sie im Bereich „SSH“ die Option **Enable SSH** (SSH aktivieren) aus.
5. Wählen Sie **Enable Root SSH Access** (SSH-Root-Zugriff aktivieren) aus.
6. Klicken Sie auf **Apply Settings** (Einstellungen übernehmen).

Nächste Schritte

- Aktualisieren Sie Ihren Flow Collector auf die neueste Version und den neuesten Patch, wie im nächsten Schritt beschrieben.

1. Aktualisieren Sie zuletzt Ihren Flow Collector auf die neueste Version und den neuesten Patch. Weitere Informationen zum Aktualisieren auf die neueste Version finden Sie in den Aktualisierungsleitfäden. Weitere Informationen zu Patch-Updates finden Sie in den Patch-Readmes.

   Nach der Aktualisierung Ihres Flow Collector haben Sie folgende Optionen:

   - Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
   - Für jeden Flow Collector das bei der Flow Collector-Installation unter **Flow Collector-Konfiguration für die Verwendung mit einem Data Store** beschriebene Verfahren sowie die Erstkonfiguration, die Konfiguration mit Appliance Setup Tool und die Einrichtung von Central Management für die übrigen Flow Collectors wiederholen.
2. Nachdem Sie alle Ihre Flow Collectors bereitgestellt und konfiguriert haben, haben Sie die folgenden Optionen:

   - Ihren Flow Sensor, falls vorhanden, konfigurieren, wie im nächsten Abschnitt beschrieben.
   - Ihre sekundäre SMC, falls vorhanden, konfigurieren, wie unter **Failover-Bereitstellung der Stealthwatch Management Console** beschrieben.

- Wenn Sie keinen Flow Sensor und keine sekundäre SMC haben, den Data Store initialisieren und konfigurieren Sie, wie unter **Data Store-Initialisierung und -Konfiguration** beschrieben.

Flow Sensor-Bereitstellung

Wenn Sie einen Flow Sensor bereitstellen möchten, befolgen Sie die Anweisungen im Hardware-Installationshandbuch zur Stealthwatch x210-Serie und im Stealthwatch-Systemkonfigurationshandbuch. Beachten Sie, dass der Flow Sensor-Installationsprozess unverändert bleibt, egal ob Sie einen Data Store bereitstellen oder nicht. Sie müssen keinen Flow Sensor für die Verwendung mit einem Data Store konfigurieren.

Nachdem Sie Ihren Flow Sensor bereitgestellt und konfiguriert haben, haben Sie die folgenden Optionen:

- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
- Ihre sekundäre SMC, falls vorhanden, als Failover-SMC konfigurieren, wie im nächsten Abschnitt beschrieben.
- Wenn Sie keine sekundäre SMC haben, den Data Store initialisieren, wie unter **Data Store-Initialisierung und -Konfiguration** beschrieben.

Failover-Bereitstellung der Stealthwatch Management Console

Wenn Sie eine sekundäre SMC haben, die Sie als Failover-SMC konfigurieren möchten, befolgen Sie die Anweisungen im Hardware-Installationshandbuch zur Stealthwatch x210-Serie, im Stealthwatch-Systemkonfigurationshandbuch und im Stealthwatch Failover-Konfigurationsleitfaden.

Nachdem Sie die Konfiguration der sekundären SMC abgeschlossen haben und die primäre SMC diese über Central Management verwaltet, haben Sie folgende Optionen:

- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
- Wenn Sie eine sekundäre SMC haben und sie zur primären SMC hochstufen, ist eine zusätzliche Konfiguration erforderlich, bevor Sie erneut das Skript `setup-sw-datastore-secure-connectivity` verwenden. Weitere Informationen finden Sie unter Kopieren von Data Store-Trust-Informationen auf eine Failover-SMC.

- Den Data Store initialisieren und konfigurieren, wie unter **Data Store-Initialisierung und -Konfiguration** beschrieben.

Data Store-Initialisierung und -Konfiguration

Nachdem Sie Ihre SMCs, Data Nodes und Flow Collectors bereitgestellt und konfiguriert haben, initialisieren und konfigurieren Sie den Data Store. Stellen Sie sicher, dass alle Ihre SMCs, Data Nodes und Flow Collectors auf die neueste Version und den neuesten Patch aktualisiert wurden, bevor Sie fortfahren.

> Wenn Sie eine sekundäre SMC haben und sie zur primären SMC hochstufen, ist eine zusätzliche Konfiguration erforderlich, bevor Sie erneut das Skript `setup-sw-datastore-secure-connectivity` verwenden. Weitere Informationen finden Sie unter Kopieren von Data Store-Trust-Informationen auf eine Failover-SMC.

Führen Sie die folgenden Schritte aus:

1. Stellen Sie zunächst sicher, dass alle Data Nodes und Flow Collectors sowie die sekundäre SMC, falls bereitgestellt, in Central Management verwaltet werden und auf allen sowohl SSH-Zugriff als auch SSH-Root-Zugriff aktiviert sind.
2. Führen Sie als Nächstes über die SMC ein Skript aus, um die Data Store-`dbadmin` und `-readonlyuser`-Kennwörter und -Identitätszertifikate für die sichere Data Store-Kommunikation an Ihre Stealthwatch-Appliances zu verteilen.
3. Führen Sie dann von dem im vorherigen Schritt angegebenen Data Node ein Skript aus, um den Data Store zu initialisieren und sichere Verbindungen zwischen den Data Nodes und Ihren Stealthwatch-Appliances herzustellen.
4. Ordnen Sie zuletzt in Central Management den Data Store-IP-Adressen auf Ihrer SMC und Ihren Flow Collectors einen internen `-Namen (`sw-datastore Data Node) zu, um die Data Node-Lastverteilung und die Abfrageleistung zu verbessern.

Sicherstellen, dass Ihre Data Nodes und Flow Collectors durch Central Management verwaltet werden:

Vorbereitungen

- Erstellen Sie eine Liste aller Data Node- und Flow Collector-IP-Adressen und -Hostnamen, die in Central Management verwaltet werden sollen.

- Melden Sie sich bei der SMC-Web-App als Systemadministrator an und gehen Sie zu „Central Management“ (Zentrales Management).

Verfahren

1. Vergleichen Sie Ihre Liste der Data Nodes und Flow Collectors sowie die sekundäre SMC, falls bereitgestellt, mit der Liste im Appliance Inventory und stellen Sie sicher, dass der **Appliance-Status** überall **Up** lautet. Fahren Sie **nicht** mit der Data Store-Initialisierung fort, bis alle Ihre erwarteten Appliances verwaltet werden und ihr **Appliance-Status Up** ist.

   Wenn der Status einer Appliance **Down** ist, überprüfen Sie Ihre Appliance-Konfiguration und die Verbindung zwischen der SMC und dieser Appliance.

   Wenn eine Appliance nicht im Inventory angezeigt wird, fügen Sie sie hinzu.
2. Klicken Sie für jede Appliance auf das Menü „Actions“ (Aktionen) und wählen Sie dann **Edit Appliance Configuration** (Appliance-Konfiguration bearbeiten).
3. Wählen Sie die Registerkarte „Appliance“ aus. Stellen Sie sicher, dass **Enable SSH** (SSH aktivieren) und **Enable Root SSH Access** (Root-SSH-Zugriff aktivieren) ausgewählt sind. Fahren Sie **nicht** mit der Data Store-Initialisierung fort, bis bei allen erwarteten Appliances SSH-Zugriff und SSH-Root-Zugriff aktiviert sind.

   Wenn eine oder beide Optionen nicht ausgewählt sind, wählen Sie die Option aus und klicken Sie dann auf **Apply Settings** (Einstellungen übernehmen).

Verteilen von Data Store-Kennwörtern an Ihre SMC, Data Nodes und Flow Collectors:

Über die Kommandozeile der SMC können Sie ein Skript ausführen, das Ihre Stealthwatch-Bereitstellung auf die Data Store-Initialisierung vorbereitet, indem es die für den Aufbau sicherer Data Store-Verbindungen erforderlichen Informationen verteilt. Mit der ersten Option des Skripts können Sie Kennwörter für die Benutzerkonten `dbadmin` und `readonlyuser` erstellen und sie sicher an die SMC, Data Nodes und Flow Collectors verteilen. Jedes Kennwort muss die folgenden Anforderungen erfüllen:

- mindestens eine Ziffer enthalten
- mindestens 1 Kleinbuchstaben enthalten
- mindestens 1 Großbuchstaben enthalten

- mindestens 1 Sonderzeichen aus der folgenden Liste enthalten:
  `<>.,?/'"|:;`~!@#$%^&*()-_+={}[]`
- mindestens 8 Zeichen enthalten (es gibt keine Maximallänge)
- nur ASCII-codierte Zeichen enthalten

Wenn Sie ein Skript zur Initialisierung des Data Store ausführen, verwendet es diese Informationen, um die Anmeldeinformationen für die Benutzerkonten `dbadmin` und `readonlyuser` festzulegen und sichere Verbindungen zwischen jeder Appliance und dem Data Store herzustellen.

> Wenn Sie diese Kennwörter festlegen und dann verlieren, wenden Sie sich an den Cisco Support, um Unterstützung bei der Wiederherstellung zu erhalten.

Beachten Sie, dass Sie diese Option verwenden, wenn Sie den Data Store zum ersten Mal bereitstellen. Wenn Sie den Data Store bereits initialisiert haben und diese Kennwörter aktualisieren möchten, finden Sie weitere Informationen unter Aktualisieren der dbadmin- und readonlyuser-Kennwörter auf dem Data Store.

Vorbereitungen

- Stellen Sie eine Liste der Root-Kennwörter für Ihre SMC, Data Nodes, Flow Collectors und die sekundäre SMC, falls bereitgestellt, zusammen.
- Melden Sie sich bei der SMC-Konsole als `root` an.

Verfahren

1. Geben Sie in der Kommandozeile `cd /lancope/admin/cds` ein und drücken Sie die Eingabetaste, um in das entsprechende Verzeichnis zu wechseln.
2. Geben Sie `./setup-sw-datastore-secure-connectivity` ein und drücken Sie die Eingabetaste, um das Bash-Skript für die sichere Verbindung des Data Store auszuführen.
3. Wählen Sie im Hauptmenü des Skripts **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen) aus.

   Das Skript zeigt eine Liste mit der SMC, den von der SMC verwalteten Data Nodes, den vom Data Store unterstützten und von der SMC verwalteten Flow Collectors sowie alle eventuell vorhandenen vom Data Store unterstützten und von der primären SMC verwalteten sekundären SMCs an.
4. Überprüfen Sie die Liste der Appliances und wählen Sie **OK** aus. Wenn Sie dieses Skript bei der Konfiguration Ihrer Stealthwatch-Bereitstellung für die Verwendung des Data Store zum ersten Mal ausführen, werden alle Appliances ausgewählt.

5. Wenn Sie in der Kommandozeile nach dem `root`-Kennwort für jede Appliance gefragt werden, geben Sie das Kennwort ein und drücken Sie die Eingabetaste.

   > Da Sie mehrere Kennwörter eingeben, achten Sie darauf, das richtige Kennwort für die jeweilige Appliance einzugeben.

   Nachdem Sie alle `root`-Kennwörter der Appliances eingegeben haben, fordert das Skript Sie zur Eingabe der `dbadmin`- und `readonlyuser`-Kennwörter auf.
6. Geben Sie das **dbadmin**-Kennwort ein.
7. Geben Sie dasselbe `dbadmin`-Kennwort zur Bestätigung in das Feld **dbadmin (confirmation)** ein.
8. Geben Sie das **readonlyuser**-Kennwort ein.
9. Geben Sie dasselbe `readonlyuser`-Kennwort zur Bestätigung in das Feld **readonlyuser (confirmation)** ein.

   > Geben Sie nicht dasselbe Kennwort für `dbadmin` und `readonlyuser` ein. Wenn Sie dasselbe Kennwort zuweisen, schlägt das Skript fehl und vergibt für beide Benutzerkonten keine Kennwörter.
10. Wählen Sie **OK**.

    Das Skript verteilt diese Kennwörter sicher an die ausgewählten Appliances. Wenn dieser Vorgang abgeschlossen ist, wird eine Liste der aktualisierten Appliances angezeigt.
11. Wählen Sie **OK**, um zum Hauptmenü des Skripts zurückzukehren.

Nächste Schritte

- Verteilen Sie Data Store-Identitätszertifikate für die sichere Kommunikation, wie im nächsten Verfahren beschrieben.

Verteilen von Identitätszertifikaten für die sichere Data Store-Kommunikation an Ihre Appliances

Im Skript zum Herstellen sicherer Data Store-Verbindungen können Sie mit der zweiten Option ein Identitätszertifikat generieren und es an die SMC, Data Nodes und Flow Collectors verteilen. Wenn Sie ein Skript zur Initialisierung des Data Store ausführen, verwendet es dieses Identitätszertifikat, um sichere Verbindungen zwischen Ihren Appliances und dem Data Store herzustellen.

Das Identitätszertifikat ist selbstsigniert, für 5 Jahre gültig und auf den Common Name `sw-datastore.stealthwatch.cisco.com` ausgestellt.

Vorbereitungen

- Führen Sie in der SMC-Kommandozeile das Skript `setup-sw-datastore-secure-connectivity` aus.

Verfahren

1. Wählen Sie im Hauptmenü des Skripts **2. Distribute Certificates for Secure DB Connection** (Verteilen von Zertifikaten für sichere DB-Verbindungen) aus.
2. Das Skript zeigt eine Liste mit der SMC, den von der SMC verwalteten Data Nodes, den von der SMC verwalteten Flow Collectors sowie aller eventuell vorhandenen von der primären SMC verwalteten sekundären SMCs an.

   Wenn Sie die Liste der Appliance bereits nach der Auswahl von **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen) bestätigt haben, zeigt das Skript diese Liste der Appliances möglicherweise nicht an. Fahren Sie mit Schritt 4 fort.
3. Bestätigen Sie die Liste der Appliances und wählen Sie **OK**. Wenn Sie dieses Skript bei der Konfiguration Ihrer Stealthwatch-Bereitstellung für die Verwendung des Data Store zum ersten Mal ausführen, werden alle Appliances ausgewählt.

   Das Skript generiert ein Identitätszertifikat für die sichere Kommunikation und den privaten Schlüssel des Paares.
4. Wenn Sie in der Kommandozeile nach dem `root`-Kennwort für jede Appliance gefragt werden, geben Sie das Kennwort ein und drücken Sie die Eingabetaste.

   > Da Sie mehrere Kennwörter eingeben, achten Sie darauf, das richtige Kennwort für die jeweilige Appliance einzugeben.
5. Wenn das Skript erfolgreich ist, zeigt es eine Erfolgsmeldung und eine Data Node-IP-Adresse an. Im nächsten Schritt melden Sie sich per SSH bei der Konsole dieses Data Node an, um das Data Store-Initialisierungsskript auszuführen.

   > Notieren Sie sich die IP-Adresse, bevor Sie von dieser Meldung weg navigieren. Sie können sie nicht mehr abrufen, nachdem die Meldung geschlossen wurde.

Nächste Schritte

- Initialisieren Sie den Data Store, wie im nächsten Verfahren beschrieben.

Ausführen eines Scripts zur Initialisierung des Data Store und zum Erzwingen sicherer Verbindungen

Nachdem Sie die `dbadmin`- und `readonlyuser`-Benutzerkennwörter und das Identitätszertifikat an Ihre Appliances verteilt haben, melden Sie sich beim Data Node an, wie im vorangegangenen Verfahren angegeben. Ändern die Konfigurationsdatei `install_SDBN.cfg` und führen das Initialisierungsskript `install_SDBN.initial.py` aus. Dieses Skript initialisiert den Data Store, verbindet Ihre Data Nodes, legt die bereitgestellten `dbadmin`- und `readonlyuser`-Anmeldeinformationen fest und erzwingt die Voraussetzung für sichere Verbindungen zwischen Ihren Stealthwatch-Appliances und dem Data Store.

Nachdem Sie den Data Store initialisiert haben, kopieren Sie den Data Store-Master-API-Schlüssel von diesem Data Node. Sie verwenden diese Informationen später im Abschnitt **Konfiguration von Vertica Management Console**, um Vertica Management Console (VMC) auf Ihrer SMC zu installieren.

Vorbereitungen

- Stellen Sie eine Liste aller Ihrer öffentlichen Data Node-`eth0`-IP-Adressen und privaten `eth2`- oder `eth2/eth3`-Port-Channel-IP-Adressen zusammen.
- Melden Sie sich als `root` bei der Konsole des Data Node an, dessen IP-Adresse angezeigt wurde, nachdem Sie Identitätszertifikate mit dem Skript für die sichere Data Store-Verbindung verteilt haben, wie in **Verteilen von Identitätszertifikaten für die sichere Data Store-Kommunikation an Ihre Appliances** beschrieben.

Verfahren

1. Geben Sie in der Kommandozeile `cd /lancope/database` ein und drücken Sie die Eingabetaste, um in das entsprechende Verzeichnis zu wechseln.
2. Geben Sie `cp install_SDBN_example.cfg install_SDBN.cfg` ein und drücken Sie die Eingabetaste, um eine Kopie der Beispielkonfigurationsdatei zu erstellen.
3. Geben Sie `vi install_SDBN.cfg` ein und drücken Sie die Eingabetaste, um die Konfigurationsdatei in einem Texteditor zu ändern.
4. Erstellen Sie fortlaufend nummerierte `[nodeN]`-Abschnitte, die der Anzahl der von Ihnen bereitgestellten Data Nodes entsprechen. Wenn Sie z. B. 6 Data Nodes bereitgestellt haben, sieht Ihre Datei wie folgt aus:

```
[node1]
private = 169.254.42.30
public = 10.0.16.30
[node2]
private = 169.254.42.31
public = 10.0.16.31
[node3]
private = 169.254.42.32
public = 10.0.16.32
[node4]
private = 169.254.42.33
public = 10.0.16.33
[node5]
private = 169.254.42.34
public = 10.0.16.34
[node6]
private = 169.254.42.35
public = 10.0.16.35
[common]
subnet = 10.0.16.0
```

5. Beginnen Sie mit dem Abschnitt `[node1]` und geben Sie die privaten (`eth2`- oder `eth2/eth3`-Port-Channel) und öffentlichen (`eth0`) IP-Adressen für jeden Data Node ein. Beachten Sie Folgendes:
   - Dieses Skript ordnet Data Nodes den Data Store in der Reihenfolge zu, in der sie aufgelistet sind. Wenn Sie Ihre Data Nodes mit mehreren redundanten Netzteilen bereitgestellt haben, wechseln Sie die Knotenzuordnung basierend auf der Stromversorgung ab, um die Gesamtbetriebszeit des Data Store und die Datenredundanz zu maximieren.
   - Die privaten IP-Adressen sollten nicht routbar sein und sich in einem privaten LAN oder VLAN befinden. Sie müssen IP-Adressen aus dem CIDR-Block `169.254.42.0/24` zuweisen.
   - Überlappen Sie keine IP-Adressen zwischen oder unter Data Nodes.
   - Fügen Sie nur Data Nodes hinzu, die Teil des Data Store sein sollen.
6. Aktualisieren Sie im Abschnitt `[common]` das `subnet` so, dass es die niedrigste IP-Adresse im CIDR-Block für öffentliche IP-Adressen ist.
7. Drücken Sie die Esc-Taste, geben Sie `:wq` ein und drücken Sie die Eingabetaste, um Ihre Änderungen zu speichern und den Texteditor zu beenden.

8. Geben Sie in der Kommandozeile `python install_SDBN_initial.py -i install_SDBN.cfg` ein und drücken Sie die Eingabetaste, um das Python-Skript zur Data Store-Initialisierung auszuführen. Dieses Skript verwendet die Konfigurationsdatei `install_SDBN.cfg`, um die Data Nodes in der von Ihnen angegebenen Reihenfolge zu initialisieren.

   Nachdem das Skript beendet ist, überprüfen Sie die Statusmeldungen der Kommandozeile, um sicherzustellen, dass das Skript erfolgreich war.

   > Für jeden Data Node gibt die Konsole `Prerequisites not fully met during local (OS) configuration` (Voraussetzungen, die bei der lokalen (Betriebssystem-)Konfiguration nicht vollständig erfüllt wurden) aus und listet eine Reihe von Protokollmeldungen auf: `HINT (S0305)`, `HINT (S0041)`, `HINT (S0040)`, `WARN (N0010)`, `FAIL (s0180)` und `FAIL (s0311)`. Diese Protokollmeldungen sind zu erwarten und deuten nicht auf einen Fehler bei der Initialisierung des Data Store hin. Weitere Informationen zu diesen Meldungen finden Sie unter **Fehlerbehebung bei der Data Store-Bereitstellung**.

   > Die Konsole gibt für jeden Data Node `INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified` (SSLCA-Konfigurationsparameter nicht festgelegt; Client-Zertifikate werden nicht angefordert oder verifiziert) aus. Diese Protokollmeldungen sind zu erwarten und deuten nicht auf einen Fehler beim Aufbau sicherer Verbindungen mit dem Data Store hin. Weitere Informationen zu diesen Meldungen finden Sie unter **Fehlerbehebung bei der Data Store-Bereitstellung**.

9. Geben Sie `cd /opt/vertica/config` ein, um in das entsprechende Verzeichnis zu wechseln.
10. Geben Sie `cat apikeys.dat` ein, um die API-Schlüsselzeichenfolge in der Konsole anzuzeigen.
11. Kopieren Sie die API-Schlüsselzeichenfolge und fügen Sie sie in einen Texteditor ein. Sie verwenden diesen API-Schlüssel später im Abschnitt **Konfiguration von Vertica Management Console**, um VMC auf Ihrer SMC zu konfigurieren.
12. Notieren Sie sich die IP-Adresse dieses Data Nodes. Sie verwenden diese IP-Adresse später im Abschnitt **Konfiguration von Vertica Management Console**, um VMC auf Ihrer SMC zu konfigurieren.

Nächste Schritte

- Verwenden Sie die lokale Auflösung in Central Management, um die Data Node-IP-Adressen dem Data Store-Namen zuzuordnen, wie im nächsten Verfahren beschrieben.

Zuordnung des Data Store-Namens zu Ihren Data Nodes über die lokale Auflösung

Nachdem Sie den Data Store initialisiert haben, verwenden Sie Central Management, um den Data Store-Namen (`sw-datastore`) allen Ihren Data Node-IP-Adressen für Ihre SMC und Flow Collectors zuzuordnen. Da der Data Store mehrere Data Nodes enthält, hilft diese Zuordnung mithilfe der lokalen Auflösung dabei, den Flow-Speicher und die Abfrageanforderungen gleichmäßiger über Ihre Data Nodes zu verteilen, was Leistung und Reaktion verbessert.

> Um eine optimale Leistung zu erzielen, ordnen Sie die Data Node-`eth0`-IP-Adressen für jede Appliance in der **gleichen Reihenfolge** zu.

Vorbereitungen

- Stellen Sie eine Liste aller Ihrer öffentlichen Data Node-IP-Adressen zusammen.
- Stellen Sie eine Liste Ihrer in Central Management verwalteten Flow Collectors zusammen.
- Melden Sie sich bei der SMC-Web-App als Administrator an und gehen Sie zu „Central Management“ (Zentrales Management).

Verfahren

1. Beginnen Sie mit der SMC. Klicken Sie auf das Menü „Actions“ (Aktionen) und wählen Sie **Edit Appliance Configuration** (Appliance-Konfiguration bearbeiten) aus.
2. Wählen Sie die Registerkarte „Network Services“ (Netzwerkdienste) aus.
3. Klicken Sie im Abschnitt „Local Resolution“ (Lokale Auflösung) auf **Add New** (Neu hinzufügen).
4. Geben Sie in das Feld **Host Name** `sw-datastore` ein.
5. Geben Sie die erste öffentliche Data Node-IP-Adresse aus Ihrer Liste ein.
6. Klicken Sie auf **Add** (Hinzufügen).

7. Wiederholen Sie die vorherigen drei Schritte für alle Ihre verbleibenden Data Nodes und verwenden Sie dabei die Liste der öffentlichen Data Node-IP-Adressen.
8. Klicken Sie auf **Apply Settings** (Einstellungen übernehmen) und bestätigen Sie dann Ihre Änderungen.
9. Wiederholen Sie diesen Vorgang für alle Flow Collectors in Ihrer Liste sowie Ihre sekundäre SMC, falls bereitgestellt.

> Um eine optimale Leistung zu erzielen, ordnen Sie die Data Node-`eth0`-IP-Adressen für jede Appliance in der **gleichen Reihenfolge** zu.

Nächste Schritte

- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
- Konfigurieren Sie Vertica Management Console (VMC) auf Ihrer SMC. Im nächsten Abschnitt finden Sie weitere Informationen.

Konfiguration von Vertica Management Console

Nachdem Sie den Data Store initialisiert und konfiguriert haben, konfigurieren Sie Vertica Management Console (VMC) auf Ihrer SMC, um eine Verbindung mit dem Data Store herzustellen. Sie können VMC verwenden, um den Data Store-Zustand zu überwachen und Benachrichtigungen basierend auf konfigurierbaren Schwellenwerten zu erhalten. Führen Sie die folgenden Schritte aus:

1. Führen Sie von einem Webbrowser auf Ihrer lokalen Workstation die VMC-Erstkonfiguration durch. Konfigurieren Sie VMC dabei so, dass die Verwendung von TLS 1.0 und 1.1 sowohl für den Webbrowser-Zugriff als auch für E-Mail-Benachrichtigungen verboten wird.
2. Konfigurieren Sie in VMC eine sichere Verbindung mit Ihrem Data Store.
3. Konfigurieren Sie in VMC automatische Benachrichtigungen (z. B. per E-Mail) und Benachrichtigungsschwellenwerte.

> Wenn Sie Option **3. Update SW DataStore password on appliances** (SW-DataStore-Kennwort auf Appliances aktualisieren) in `setup-sw-datastore-secure-connectivity` verwenden, um das `dbadmin`-Kennwort zu aktualisieren, nachdem Sie es bereits festgelegt haben, müssen Sie sich als `dbadmin` in VMC anmelden, um das Kennwort manuell zu aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der

dbadmin- und readonlyuser-Kennwörter auf dem Data Store nach der Initialisierung.

Durchführen der VMC-Erstkonfiguration

Die VMC-Erstkonfiguration führen Sie beim ersten Zugriff auf VMC durch.

Standardmäßig erlaubt VMC TLS 1.0- und TLS 1.1- Verbindungen von einem Webbrowser. Da diese älteren Versionen von TLS weniger sicher sind als TLS 1.2 und höher, konfigurieren Sie VMC so, dass keine Verbindungen über TLS 1.0 und TLS 1.1 zugelassen werden.

Vorbereitungen

- Sie benötigen die IPv4-Adresse Ihrer SMC.
- Stellen Sie sicher, dass der Kommunikations-Port `9450/TCP` zwischen Ihrer Workstation und der SMC geöffnet ist.

Verfahren

1. Öffnen Sie auf Ihrer Workstation einen Webbrowser und geben Sie in die Adresszeile `https://[smc-ipv4-address]:9450/webui/login` ein. Ersetzen Sie `[smc-ipv4-address]` durch die IPv4-Adresse Ihrer SMC. Navigieren Sie zu dieser URL.
2. Akzeptieren Sie die Vertica-Lizenz und klicken Sie dann auf **Next** (Weiter).
3. Geben Sie das `dbadmin`-**Kennwort** in das Kennwortfeld sowie unter **Confirm Password** (Kennwort bestätigen) ein.

   > Dieses `dbadmin`-Benutzerkonto ist ein VMC-Benutzerkonto, das später Ihrem Data Store-`dbadmin`-Benutzerkonto zugeordnet wird. Sie können diesem Konto ein anderes Kennwort zuweisen als dem Data Store-`dbadmin`-Benutzerkonto.

4. Geben Sie `dbadmin` als **Unix group name** ein.
5. Ändern Sie nicht die Standard-Dateipfade (`/home/dbadmin`) oder den Standard-Port (`5450`), und klicken Sie dann auf **Next** (Weiter).

   Die Speicheroptionen werden angezeigt.
6. Klicken Sie auf **Next** (Weiter).

   Optionen für die Autorisierung der Management-Konsole werden angezeigt.
7. Klicken Sie auf **Next** (Weiter). Warten Sie auf den Neustart des Vertica-Dienstes.

   Dies kann 20 Minuten oder länger dauern. Wenn das Browserfenster nicht automatisch aktualisiert wird, aktualisieren Sie die Seite manuell.
8. Geben Sie Ihre `dbadmin`-Anmeldedaten ein und klicken Sie auf **Log in**, um sich im VMC anzumelden.
9. Klicken Sie auf der VMC-Hauptseite auf **MC Settings** (MC-Einstellungen).
10. Klicken Sie auf die Registerkarte „Configuration“ (Konfiguration).
11. Wählen Sie **Disable TLS 1.0 and 1.1 connections from browser** (TLS 1.0- und 1.1-Verbindungen im Browser deaktivieren) und speichern Sie die Änderung.

Konfigurieren einer sicheren VMC-Verbindung zum

Data Store

Bevor Sie mit der Konfiguration dieser sicheren Verbindung beginnen, kopieren Sie die Datei `/lancope/var/admin/cds/server.crt` von Ihrer SMC auf Ihre lokale Workstation. Mit dieser Datei stellen Sie eine sichere Verbindung zwischen VMC und dem Data Store her.

Vorbereitungen

- Kopieren Sie die Datei `/lancope/var/admin/cds/server.crt` von Ihrer SMC auf Ihre lokale Workstation.
- Halten Sie eine Kopie Ihres Data Store-Master-API-Schlüssels bereit, wie in **Ausführen eines Scripts zur Initialisierung des Data Store und zum Erzwingen sicherer Verbindungen** beschrieben.
- Sie benötigen außerdem die IP-Adresse des Data Node, von dem Sie den API-Schlüssel kopiert haben, wie in **Ausführen eines Scripts zur Initialisierung des Data Store und zum Erzwingen sicherer Verbindungen** beschrieben.

Verfahren

1. Klicken Sie auf der VMC-Startseite auf **Import a Vertica Database Cluster** (Vertica-Datenbankcluster importieren).
2. Geben Sie die Data Node-`eth0`-**IP-Adresse** ein, von der Sie den API-Schlüssel kopiert haben, und klicken Sie dann auf **Next** (Weiter).
3. Ändern Sie optional im Feld **Cluster Name** den Clusternamen.
4. Geben Sie den Data Store-Master-**API-Schlüssel** ein und klicken Sie dann auf **Next** (Weiter).

   VMC lokalisiert den Data Store.
5. Geben Sie `dbadmin` als **Benutzernamen** ein und geben Sie das `dbadmin`-**Kennwort** ein.
6. Wählen Sie **Use TLS** (TLS verwenden).
7. Klicken Sie auf **Configure TLS and Import DB** (TLS konfigurieren und DB importieren).

   Das Fenster „Configure TLS Connection Certificates“ (TLS-Verbindungszertifikate konfigurieren) wird angezeigt.
8. Klicken Sie auf **Configure TLS Connection** (TLS-Verbindung konfigurieren).
9. Wählen Sie **Upload a new CA Certificate** (Neues CA-Zertifikat hochladen) und klicken Sie dann auf **Next** (Weiter).

10. Klicken Sie auf **Browse** (Durchsuchen) und wählen Sie dann die Datei `server.crt` aus, die Sie von der SMC auf Ihre lokale Workstation heruntergeladen haben.
11. Geben Sie als **CA Certificate alias** (CA-Zertifikat-Alias) `sw-datastore-cert` ein und klicken Sie dann auf **Next** (Weiter).
12. Klicken Sie auf **Review** (Überprüfen).
13. Klicken Sie auf **Configure TLS for DB** (TLS für DB konfigurieren).

    VMC konfiguriert sichere Verbindungen zum Data Store.
14. Klicken Sie auf **Close** (Schließen).

> Möglicherweise wird die Meldung „Error while importing database on MC. undefined“ (Fehler beim Importieren der Datenbank auf MC. undefiniert) angezeigt. Dies ist zu erwarten und deutet nicht auf einen Fehler beim Aufbau einer sicheren Verbindung mit dem Data Store hin.

Konfigurieren von VMC-Alarmbenachrichtigungen per E-Mail

Sie können VMC so konfigurieren, dass es Alarmbenachrichtigungen per E-Mail versendet.

Vorbereitungen

- Melden Sie sich in VMC als `dbadmin` an.

Verfahren

1. Klicken Sie auf der Seite „MC Settings“ (MC-Einstellungen) auf die Registerkarte „Email Gateway „(E-Mail-Gateway).
2. Geben Sie einen **SMTP-Server (Hostname)** ein. Sie können einen Namen mit bis zu 255 Zeichen oder eine IP-Adresse eingeben.
3. Geben Sie einen **SMTP-Server-Port** ein.
4. Wählen Sie bei **Session Type (SSL or TLS)** (Sitzungstyp (SSL oder TLS)) **Use TLS** (TLS verwenden) aus.
5. Geben Sie bei **SMTP Username** einen Benutzernamen ein.
6. Geben Sie bei **SMTP Password** das zugehörige Kennwort ein.
7. Geben Sie bei **Originating Email Alias** ein Absender-Alias ein, von dem aus VMC E-Mail-Alarme versenden soll.

8. Klicken Sie auf **Test**, um Ihre Einstellungen zu überprüfen.

   Aktualisieren Sie die Einstellungen, wenn Sie keine Test-E-Mail erhalten.
9. Klicken Sie auf **Apply** (Anwenden).

Konfigurieren von VMC-Alarmschwellenwerten

Sie können verschiedene obere und untere Schwellenwerte konfigurieren, ab denen VMC einen Alarm generiert, wenn der Data Store einen Schwellenwert überschreitet.

Vorbereitungen

- Melden Sie sich in VMC als `dbadmin` an.

Verfahren

1. Wählen Sie **Settings > Thresholds**(Einstellungen > Schwellenwerte) aus.
2. Aktivieren Sie das Kontrollkästchen eines Schwellenwerts für Alarmmeldungen, um ihn zu aktivieren, oder deaktivieren Sie das Kontrollkästchen, um ihn zu deaktivieren. Cisco empfiehlt, die Benachrichtigung `Node State Change` (Knoten-Statusänderung) zu aktivieren, um Benachrichtigungen zu erhalten, wenn ein Data Node ausfällt.

   > Wenn Sie untere Schwellenwerte konfigurieren, kann dies zu übermäßigen Fehlalarm-Benachrichtigungen führen. Wenn Sie z. B. einen unteren Schwellenwert für die CPU-Auslastung eines Knotens festlegen, wird dieser möglicherweise häufig ausgelöst, wenn die CPU-Nutzung schwankt.
3. Wählen Sie *Priority 1* für jeden Benachrichtigungsschwellenwert, für den Sie E-Mails erhalten möchten.
4. Wenn Sie *Priority 1* wählen, klicken Sie auf das Durchsuchen-Symbol neben **Email Destination** (E-Mail-Ziel).
5. Geben Sie eine E-Mail-Adresse in **Entering New Field** (Neues Feld) ein, und klicken Sie dann auf das Symbol **+**.
6. Klicken Sie auf **OK**.
7. Wählen Sie bei **Email Interval** ein E-Mail-Intervall aus, um die E-Mail-Häufigkeit zu bestimmen, wenn Data Store einen Schwellenwert überschreitet.
8. Klicken Sie auf **Anwenden**.

Nächste Schritte

- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
- Konfigurieren Sie die Data Store-Datenaufbewahrung, wie im nächsten Abschnitt beschrieben.

Konfiguration der Data Store-Datenaufbewahrung

Standardmäßig bewahrt der Data Store Daten maximal sieben (7) Tage auf, bevor sie automatisch gelöscht werden. Über die Stealthwatch-REST-API können Sie diese Aufbewahrungsfrist ändern:

- auf eine andere Anzahl von Tagen, bis zu 3000, oder
- auf eine Speicherung der Daten so lange wie möglich, bis der Data Store seine maximale Kapazität erreicht hat.

Beachten Sie die folgenden Hinweise zur Data Store-Datenaufbewahrung:

- Nachdem Sie die Einstellungen für die Datenaufbewahrung aktualisiert haben, müssen Sie weder eine Stealthwatch-Appliance noch den Data Store neu starten. Die Einstellungen werden nach einigen Minuten wirksam.
- Wenn Sie die Aufbewahrung auf einen längeren Zeitraum ändern, müssen Sie den Ablauf der Zeitdifferenz abwarten, bis die gespeicherten Daten genau den Aufbewahrungseinstellungen entsprechen.Bis zu diesem Zeitpunkt werden die Daten mit der am stärksten reduzierten (d. h. gröbsten) Auflösung angezeigt. Wenn Sie z. B. die Aufbewahrung von 3 Tagen auf 10 Tage ändern, müssen Sie 7 Tage warten, bis die gespeicherten Daten genau den Aufbewahrungseinstellungen entsprechen.
- Ihre Daten werden möglicherweise aufgrund einer kritischen Datenreduzierung je nach Festplattennutzung früher als die von Ihnen gewählte Aufbewahrungsfrist gelöscht. Wenn Sie sich dafür entscheiden, Daten so lange wie möglich zu speichern, beginnt das System, die ältesten Daten zu löschen, wenn die Kapazität des Data Store erschöpft ist.
- Wenn Sie die Daten nicht speichern möchten, können Sie die Admin-Benutzeroberfläche für jeden Ihrer Flow Collectors aufrufen und **Support > Advanced Settings** (Erweiterte Einstellungen) wählen. Ändern Sie für jeden Flow Collector den Eintrag „interface_retention_days“ in der Spalte „Option Label“ auf 0 (Null) und starten Sie Ihren Flow Collector neu (oder die Flow Collector Engine, falls möglich).

Um diese Einstellungen zu aktualisieren, führen sie mithilfe der REST-API Folgendes aus:

Authentifizierung bei der SMC-REST-API

Abfrage von Ressourceninformationen

Ressource	Beschreibung
URI	`https://[smc-eth0-ip]/token/v2/authenticate`
Beschreibung	Authentifizieren Sie sich bei der REST-API des SMC.
URI-Parameter	• *[smc-eth0-ip]* – SMC-eth0-Management-IP-Adresse
HTTP-Methode	POST
Anfragetext-MIME-Typ	application/x-www-form-urlencoded
Anfragetext	`username=[username]&password=[password]`
Anfragetext-Parameter	• *[username]* – (ERFORDERLICH) SMC-Admin-Benutzer • *[password]* – (ERFORDERLICH) Kennwort für das SMC-Admin-Benutzerkonto

Erfolgs-Antwortcode und Definition

Reaktion	Beschreibung
Antwortcode	200 - Success
Antworttext	Der Antworttext enthält Cookie-Informationen, die Sie in nachfolgenden REST-API-Aufrufen für diese Sitzung übergeben müssen. Ihre Sitzung ist für 20 Minuten gültig.

Abrufen der aktuellen Data Store-Datenaufbewahrungseinstellungen

Abfrage von Ressourceninformationen

Ressource	Beschreibung
URI	`https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings`
Beschreibung	Abrufen der aktuellen Data Store-

Ressource	Beschreibung
	Datenaufbewahrungseinstellungen
URI-Parameter	• *[smc-eth0-ip]* – eth0-Management-IP-Adresse der SMC
HTTP-Methode	GET
Anfragetext-MIME-Typ	k. A.
Anfragetext	k. A.
Anfragetext-Parameter	k. A.

Erfolgs-Antwortcode und Information

Ressource	Beschreibung
Antwortcode	200 - Success
Antworttext	Der Antworttext enthält die aktuellen Einstellungen für die Data Store-Datenaufbewahrung. Wenn Sie sie nicht geändert haben, ist der Standardwert 7 Tage.

Aktualisieren der Einstellungen für die Data Store-Datenaufbewahrung

Abfrage von Ressourceninformationen

Ressource	Beschreibung
URI	`https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings`
Beschreibung	Aktualisierung der Einstellungen für die Data Store-Datenaufbewahrung
URI-	• *[smc-eth0-ip]* – eth0-Management-IP-Adresse der SMC

Ressource	Beschreibung
Parameter	
HTTP-Methode	PUT
Anfragetext-MIME-Typ	application/json

Anfragetext	`{`
	`"interfaceRetentionType":"[type]",`
	`"interfaceRetentionAmount":"[#]"`
	`}`

Anfragetext-Parameter	• *[type]* – (ERFORDERLICH) Die Art der Datenaufbewahrung, eingestellt auf einen der folgenden Zeichenfolgenwerte:
	  • `AMOUNT`: speichert Daten bis zu der in interfaceRetentionAmount festgelegten Anzahl von Tagen, bevor sie gelöscht werden
	  • `FOREVER`: speichert Daten so lange wie möglich, bis die maximale Kapazität des Data Store erreicht ist, bevor sie gelöscht werden
	• *[#]* – (ERFORDERLICH) Die maximale Anzahl von Tagen, die der Data Store Daten aufbewahrt, bevor sie gelöscht werden, eingestellt auf eine Ganzzahl zwischen `1 und 3000`.
	  Wenn Sie `interfaceRetentionType` auf `FOREVER` setzen, müssen Sie noch einen `interfaceRetentionAmount` übergeben, den das System ignoriert. Es speichert diesen Wert intern als `7` als Standardwert, unabhängig davon, welchen `interfaceRetentionAmount` Sie in dieser Situation übergeben.

Erfolgs-Antwortcode und Information

Ressource	Beschreibung
Antwortcode	204 – Success (No Content)
Antworttext	Der Antworttext hat keinen Inhalt.

Weitere Informationen zur REST-API finden Sie in der Stealthwatch Enterprise-REST-API-Dokumentation.

Das folgende Verfahren bietet eine Curl-Syntax zum Aktualisieren des Data Store-Datenaufbewahrungszeitraums:

Aktualisieren des Data Store-Aufbewahrungszeitraums

Vorbereitungen

- Melden Sie sich bei der Konsole einer Linux-basierten Appliance an, auf der curl installiert ist.

Verfahren

1. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   curl -c cookies.txt -d "username=[username]&password=
   [password]" https://[smc-eth0-ip]/token/v2/authenticate
   ```

2. Ersetzen Sie *[username]* durch einen SMC-Admin-Benutzernamen.
3. Ersetzen Sie *[password]* durch das zugehörige SMC-Admin-Kennwort.
4. Ersetzen Sie *[smc-eth0-ip]* durch die eth0-IP-Adresse der SMC.
5. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Kommandozeile ein und drücken Sie die Eingabetaste, um sich bei der SMC für die Verwendung der REST-API zu authentifizieren.

   Ihre Sitzung ist für 20 Minuten gültig.

6. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   curl -X GET -b cookies.txt https://[smc-eth0-ip]/smc-
   configuration/rest/v1/cds/retentionsettings
   ```

7. Ersetzen Sie *[smc-eth0-ip]* durch die eth0-IP-Adresse der SMC.

8. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Kommandozeile ein und drücken Sie die Eingabetaste, um die aktuellen Data Store-Aufbewahrungseinstellungen abzurufen.

   Wenn Sie dies zum ersten Mal überprüfen, ist der Data Store mit einem standardmäßigen Aufbewahrungszeitraum von 7 Tagen konfiguriert.

9. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   curl -X PUT -b cookies.txt -H "Content-
   Type:application/json" -d '{"interfaceRetentionType":"
   [type]","interfaceRetentionAmount":"[#]"}' https://[smc-
   eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings
   ```

10. Ersetzen Sie *[type]* durch eine der folgenden Angaben:
    - AMOUNT, wenn Sie eine Anzahl von Tagen für die Aufbewahrung festlegen möchten.
    - FOREVER, wenn Sie die Daten so lange wie möglich speichern wollen.
11. Ersetzen Sie *[#]* durch eine Ganzzahl von 1 bis 3000 für die Anzahl von Tagen für die Aufbewahrung.

    Sie müssen dies auch dann definieren, wenn Sie *[type]*=FOREVER einstellen. In diesem Fall ignoriert das System diesen Wert und setzt ihn intern auf 7.
12. Ersetzen Sie *[smc-eth0-ip]* durch die eth0-IP-Adresse der SMC.
13. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Kommandozeile ein und drücken Sie die Eingabetaste, um die Aufbewahrungseinstellungen zu aktualisieren.

    > Nachdem Sie die Einstellungen für die Aufbewahrung aktualisiert haben, müssen Sie weder eine Stealthwatch-Appliance noch den Data Store neu starten. Die Einstellungen werden nach einigen Minuten wirksam. Wenn Sie die Aufbewahrung auf einen längeren Zeitraum ändern, müssen Sie jedoch den Ablauf der Zeitdifferenz abwarten, bis die gespeicherten Daten genau den Aufbewahrungseinstellungen entsprechen.

Nächste Schritte

- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.
- Gehen Sie die weiteren Schritte im nächsten Abschnitt durch.

Nächste Schritte nach der Data Store-Installation

Nachdem Sie Ihre Stealthwatch-Bereitstellung für die Verwendung mit einem Data Store bereitgestellt und konfiguriert haben:

- Installieren Sie die App „Stealthwatch Report Builder“ auf Ihrer SMC, um Berichte zu Ihrer Stealthwatch-Bereitstellung zu erstellen und Data Store-Speicherstatistiken anzuzeigen. Weitere Informationen finden Sie in den Versionshinweisen.
- Weitere Informationen zur Verwendung von Stealthwatch finden Sie in der Online-Hilfe der Stealthwatch Web App.
- Zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.

Wartung des Data Store

Im Folgenden werden folgende Data Store- und Data Store-bezogenen Wartungsaufgaben beschrieben:

- Neustarten eines Data Nodes und des Data Store
- Data Store Sicherung und -Wiederherstellung
- Hinzufügen, Entfernen und Ersetzen von Data Nodes
- Kopieren von Trust-Informationen auf eine Failover-SMC, bevor sie zur primären SMC hochgestuft wird

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Neustart eines Data Node

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Wenn Sie einen Data Node neu starten müssen, geben Sie den Befehl zum Stoppen und dann den Befehl zum Neustart.

Stoppen und Neustarten des Data Node

Vorbereitungen

- Melden Sie sich bei einer Data Node-Konsole als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   `/opt/vertica/bin/admintools -t stop_node -s [`*`data-node-hostname`*`]`

3. Ersetzen Sie `[`*`data-node-hostname`*`]` durch den Data Node-Hostnamen, den Sie stoppen und neu starten möchten.
4. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um den Data Node zu stoppen.

5. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   `/opt/vertica/bin/admintools -t restart_node -s [data-node-hostname]`

6. Ersetzen Sie `[data-node-hostname]` durch den Data Node-Hostnamen, den Sie neu starten möchten.
7. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um den Data Node neu zu starten.

Neustarten des Data Store

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Um den Data Store neu zu starten, geben Sie den Befehl zum Stoppen und dann den Befehl zum Neustart.

Stoppen und Neustarten des Data Store

Vorbereitungen

- Stellen Sie sicher, dass Ihre Flow Collectors nicht mit dem Data Store verbunden sind und Daten weiterleiten.
- Stellen Sie sicher, dass Ihre SMC nicht mit dem Data Store verbunden ist und den nicht Data Store abfragt oder anderweitig aktualisiert.
- Melden Sie sich bei einer Data Node-Konsole als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Folgende Optionen sind hierzu verfügbar:
   - Geben Sie in der Eingabeaufforderung `/opt/vertica/bin/admintools -t stop_db -d sw` ein und drücken Sie die Eingabetaste, um den Data Store zu stoppen.
   - Geben Sie in der Eingabeaufforderung `/opt/vertica/bin/admintools -t stop_db -d sw -F` ein und drücken Sie die Eingabetaste, um den Data Store zu stoppen und dabei alle Flow Collector- oder SMC-Verbindungen zu überschreiben.

3. Geben Sie in der Eingabeaufforderung `/opt/vertica/bin/admintools -t start_db -d sw` ein und drücken Sie die Eingabetaste, um den Data Store neu zu starten.

Erstellen eines Data Store-Backups

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Um ein Backup Ihres Data Store zu erstellen, müssen Sie Folgendes tun:

- Schätzen Sie die Größe des Backups.
- Bereiten Sie einen Backup-Host mit der doppelten Speicherkapazität der geschätzten Backup-Größe vor.

  > Verwenden Sie einen Linux-basierten Host getrennt von Ihren Stealthwatch-Appliances.

- Installieren Sie Python 3.7 und rsync 3.0.5 auf dem Backup-Host.
- Stellen Sie sicher, dass alle Data Nodes den Backup-Host über kennwortlosen SSH-Zugang erreichen können.
- Initialisieren Sie das Backup-Verzeichnis auf dem Backup-Host.
- Erstellen Sie ein Backup des Data Store.

Schätzen des Speicherbedarfs auf dem Backup-Host

Vorbereitungen

- Melden Sie sich bei der Konsole eines Data Nodes als `root` an.

Verfahren

1. Kopieren Sie den folgenden Befehl, fügen Sie ihn in die Kommandozeile ein, und drücken Sie die Eingabetaste, um eine Verbindung zur Datenbank mit vsql herzustellen und die Abfrage auszuführen. Geben Sie Ihr Kennwort ein, wenn Sie dazu aufgefordert werden. Notieren Sie die Ergebnisse.

   ```
   /opt/vertica/bin/vsql -U dbadmin -c "SELECT SUM(used_bytes) FROM storage_containers;"
   ```

2. Multiplizieren Sie die Summe mit 2, um abzuschätzen, wie viel Speicherplatz Ihr Backup-Host benötigt.

Vorbereitung eines Backup-Hosts

Vorbereitungen

- Identifizieren Sie auf der Grundlage der in der vorherigen Aufgabe geschätzten Speicheranforderungen einen Host mit Linux in Ihrem Netzwerk, auf dem das Backup gespeichert werden soll, oder stellen Sie einen Host mit Linux bereit, der die erforderlichen Speicheranforderungen erfüllt.

  > Verwenden Sie einen Linux-basierten Host getrennt von Ihren Stealthwatch-Appliances.

- Melden Sie sich bei der Konsole des Backup-Hosts als `root` an.

Verfahren

1. Geben Sie in der Eingabeaufforderung `python --version` ein und drücken Sie die Eingabetaste, um zu sehen, welche Version von Python Sie installiert haben. Folgende Optionen sind hierzu verfügbar:
   - Wenn Python geschützt 3.7 installiert ist, fahren Sie mit Schritt 4 fort.
   - Andernfalls installieren Sie Python 3.7. Fahren Sie mit Schritt 2 fort.
2. Geben Sie `sudo apt-get update` ein und drücken Sie die Eingabetaste, um aktualisierte Versionen der Pakete, einschließlich Python, herunterzuladen. Geben Sie Ihr Kennwort ein, wenn Sie dazu aufgefordert werden.
3. Geben Sie `sudo apt-get install python3.7` ein und drücken Sie die Eingabetaste, um Python 3.7 zu installieren.
4. Geben Sie in der Eingabeaufforderung rsync -version ein und drücken Sie die Eingabetaste, um zu sehen, welche Version von rsync Sie installiert haben. Folgende Optionen sind hierzu verfügbar:

   Wenn rsync 3.0.5 installiert ist, fahren Sie mit Schritt 7 fort.

   Andernfalls installieren Sie rsync 3.0.5. Fahren Sie mit Schritt 5 fort.
5. Geben Sie `sudo apt-get update` ein und drücken Sie die Eingabetaste, um aktualisierte Versionen der Pakete, einschließlich rsync, herunterzuladen. Geben Sie Ihr Kennwort ein, wenn Sie dazu aufgefordert werden.
6. Geben Sie `sudo apt-get install rsync` ein und drücken Sie die Eingabetaste, um rsync zu installieren.
7. Geben Sie in der Eingabeaufforderung `getent passwd | grep dbadmin` ein

und drücken Sie die Eingabetaste, um festzustellen, ob ein `dbadmin`-Benutzerkonto auf diesem Host existiert. Folgende Optionen sind hierzu verfügbar:

- Wenn ein `dbadmin`-Benutzerkonto existiert, ist der Backup-Host bereit. Fahren Sie mit dem Abschnitt **Aktivieren des kennwortlosen SSH-Zugriffs für dbadmin** fort.
- Andernfalls erstellen Sie ein `dbadmin`-Benutzerkonto auf diesem Host. Fahren Sie mit Schritt 5 fort.

8. Geben Sie in der Eingabeaufforderung `useradd dbadmin` ein und drücken Sie die Eingabetaste, um ein `dbadmin`-Benutzerkonto zu erstellen.
9. Geben Sie `passwd dbadmin` ein und drücken Sie die Eingabetaste, um ein Kennwort für `dbadmin` zu vergeben.
10. Geben Sie bei **New password** ein Neues Kennwort ein und drücken Sie die Eingabetaste, um das `dbadmin`-Kennwort festzulegen. Bestätigen Sie bei entsprechender Aufforderung das Kennwort.

Nächste Schritte

- Aktivieren Sie den kennwortlosen SSH-Zugriff für das Benutzerkonto `dbadmin`, wie im nächsten Abschnitt beschrieben.

Aktivieren des kennwortlosen SSH-Zugriffs für dbadmin

Vorbereitungen

- Öffnen Sie Port 22/TCP zwischen dem Backup-Host und jedem Data Node für SSH, und Port 50000/TCP zwischen dem Backup-Host und jedem Data Node für rsync.
- Lesen Sie die OpenSSH-Dokumentation unter `ssh-copy-id` für weitere Informationen.
- Melden Sie sich auf dem ersten Data Node als `root` an.

Verfahren

1. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   `ssh-copy-id -i dbadmin@[`*`hostname`*`]`

2. Ersetzen Sie `[`*`hostname`*`]` durch den Namen Ihres Backup-Hosts.

3. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um den SSH-autorisierten Schlüssel für `dbadmin` auf den Backup-Host zu kopieren.
4. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   `ssh 'dbadmin@[hostname]'`
5. Ersetzen Sie `[hostname]` durch den Namen Ihres Backup-Hosts.
6. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um zu überprüfen, ob Sie sich über SSH bei der Konsole des Remote-Hosts anmelden können, ohne ein Kennwort von diesem Data Node zu benötigen.

Initialisieren des Backup-Verzeichnisses auf dem Backup-Host:

Vorbereitungen

- Melden Sie sich als root bei der Konsole des ersten Data Node an.

  Achten Sie auf den Data Node, den Sie zum Initialisieren des Backup-Verzeichnisses verwenden. Von diesem Data Node führen Sie auch das Backup aus, wie in Backup des Data Store beschrieben.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Kopieren Sie den folgenden Befehl in einen Texteditor: `ssh [backup-host-ip]`
3. Ersetzen Sie `[backup-host-ip]` durch die IP-Adresse Ihres Backup-Hosts.
4. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um zu überprüfen, ob Sie sich als `dbadmin` bei der Schnittstelle des Backup-Hosts anmelden können, ohne zur Eingabe eines Kennworts aufgefordert zu werden. Wenn Sie vom Backup-Host zur Eingabe eines Kennworts aufgefordert werden, überprüfen Sie Ihre Einstellungen.
5. Geben Sie `cd /home/dbadmin` ein und drücken Sie die Eingabetaste, um in das entsprechende Verzeichnis zu wechseln.
6. Geben Sie `mkdir backups` ein und drücken Sie die Eingabetaste, um das Verzeichnis `backups` zu erstellen.

7. Geben Sie `exit` ein und drücken Sie die Eingabetaste, um zur Kommandozeilen-Eingabeaufforderung des Data Node zurückzukehren.
8. Geben Sie `vi pw.ini` ein und drücken Sie die Eingabetaste, um die Backup-Kennwort Datei `pw.ini` zu erstellen und zu bearbeiten.

   > Wenn Sie das `dbadmin`-Kennwort mit dem Skript `setup-sw-datastore-secure-connectivity` aktualisieren, müssen Sie auch das Kennwort aktualisieren, das in der Backup-Kennwort Datei `pw.ini` gespeichert ist. Ansonsten schlägt das Backup fehl. Weitere Informationen finden Sie unter Aktualisieren der dbadmin- und readonlyuser-Kennwörter auf dem Data Store nach der Initialisierung.

9. Kopieren Sie die folgenden Zeilen in einen Texteditor:

   ```
   [Passwords]
   dbPassword = [dbadmin-password]
   ```

10. Aktualisieren Sie `[dbadmin-password]` auf das Data Store `dbadmin`-Kennwort.
11. Kopieren Sie die geänderten Zeilen und fügen Sie sie in die Backup-Kennwortdatei `pw.ini` ein.
12. Drücken Sie Esc, geben Sie dann `:wq` ein und drücken Sie die Eingabetaste, um den Vorgang zu beenden und Ihre Änderungen zu speichern.
13. Geben Sie `chmod 640 pw.ini` ein und drücken Sie die Eingabetaste, um die Dateiberechtigungen von `pw.ini` so zu ändern, dass der `dbadmin`-Benutzer die Datei lesen und bearbeiten kann.
14. Geben Sie `vi config.ini` ein und drücken Sie die Eingabetaste, um die Backup-Konfigurationsdatei`config.ini` zu erstellen und zu bearbeiten.
15. Kopieren Sie die folgenden Zeilen und fügen Sie sie in einen Texteditor ein:

    ```
    [Mapping]
    v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
    v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
    v_sw_node0003 = backup-host-ip:/home/dbadmin/backups

    [Misc]
    snapshotName = data_store_backup
    passwordFile = /home/dbadmin/pw.ini
    enableFreeSpaceCheck = True
    retryCount = 2
    ```

```
retryDelay = 1

[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

16. Ersetzen Sie *backup-host-ip* durch die IP-Adresse des Backup-Hosts.
17. Wenn die Hostnamen unter `[Mapping]` nicht mit Ihren Data Nodes übereinstimmen, aktualisieren Sie diese Hostnamen.
18. Stellen Sie sicher, dass Sie für jeden Data Node einen Eintrag haben, wenn Sie mehr als 3 in Ihrer Umgebung bereitgestellt haben.
19. Kopieren Sie die geänderten Zeilen und fügen Sie sie in die Datei `config.ini` ein.
20. Drücken Sie Esc, geben Sie dann `:wq` ein und drücken Sie die Eingabetaste, um den Vorgang zu beenden und Ihre Änderungen zu speichern.
21. Geben Sie `vbr -t init -c config.ini` ein und drücken Sie die Eingabetaste, um das Verzeichnis `/home/dbadmin/backups` auf dem Backup-Host für den Empfang von Data Store-Backups zu initialisieren.

Erstellung eines Backups der Data Store-Datenbank

Vorbereitungen

- Melden Sie sich als `root` an der Konsole des Data Node an, von dem aus Sie das Verzeichnis des Backup-Hosts initialisiert haben, wie in Initialisieren des Backup-Verzeichnisses auf dem Backup-Host beschrieben.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Geben Sie `vbr -t backup -c config.ini --debug 3 --dry-run` ein und drücken Sie die Eingabetaste, um einen Test des Backups durchzuführen, ohne ein Backup zu erstellen. Folgende Optionen sind hierzu verfügbar:
    - Wenn der Backup-Test führen Sie ein Backup des Data Store durch. Fahren Sie mit Schritt 2 fort.
    - Wenn der Backup-Test fehlschlägt, überprüfen Sie die Debug-Protokolldateien im Verzeichnis `/tmp/vbr`, beheben Sie die Grundursache

und testen Sie das Backup dann erneut. Wenden Sie sich an den Cisco-Support, wenn Sie das Problem nicht beheben können.

3. Geben Sie `vbr -t backup -c config.ini` ein und drücken Sie die Eingabetaste, um den Data Store im Verzeichnis `/home/dbadmin/backups` auf dem Backup-Host zu sichern.

Wiederherstellen eines Data Store-Backups

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Um den Data Store aus einem Backup wiederherzustellen, müssen Sie Folgendes sicherstellen:

- Der Data Store ist nicht aktiv. Sie können den Data Store nur stoppen, wenn Ihre Flow Collectors und SMC nicht verbunden sind und keine Änderungen vornehmen.
- Das Backup und der Data Store haben identische Knotennamen und dieselbe Anzahl von Knoten.

Stoppen des Data Store:

Vorbereitungen

- Stellen Sie sicher, dass Ihre Flow Collectors nicht mit dem Data Store verbunden sind und Daten weiterleiten.
- Stellen Sie sicher, dass Ihre SMC nicht mit dem Data Store verbunden ist und den nicht Data Store abfragt oder anderweitig aktualisiert.
- Melden Sie sich bei einer Data Node-Konsole als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Folgende Optionen sind hierzu verfügbar:
    - Geben Sie in der Eingabeaufforderung `/opt/vertica/bin/admintools -t stop_db -d sw` ein und drücken Sie die Eingabetaste, um den Data Store zu stoppen.
    - Geben Sie in der Eingabeaufforderung `/opt/vertica/bin/admintools -t stop_db -d sw -F` ein und drücken Sie die Eingabetaste, um den

Data Store zu stoppen und dabei alle Flow Collector- oder SMC-Verbindungen zu überschreiben.

Wiederherstellen des Data Store von einem Backup:

Vorbereitungen

- Wenn Sie das `dbadmin`-Kennwort mit dem Skript `setup-sw-datastore-secure-connectivity` aktualisiert haben, müssen Sie auch das Kennwort aktualisieren, das in der Backup-Kennwort Datei `pw.ini` gespeichert ist. Ansonsten schlägt die Wiederherstellung fehl. Weitere Informationen finden Sie unter Aktualisieren der dbadmin- und readonlyuser-Kennwörter auf dem Data Store nach der Initialisierung.
- Identifizieren Sie den Data Node, auf dem Sie die Backup-Konfigurationsdatei `config.ini` gespeichert haben, und melden Sie sich bei dessen Konsole als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Geben Sie in der Eingabeaufforderung `vbr --task restore --config-file config-file.ini` ein und drücken Sie die Eingabetaste, um den Data Store vom Backup-Host wiederherzustellen.

Starten des Data Store:

Vorbereitungen

- Melden Sie sich bei einer Data Node-Konsole als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Geben Sie in der Eingabeaufforderung `/opt/vertica/bin/admintools -t start_db -d sw` ein und drücken Sie die Eingabetaste, um den Data Store zu starten.

Nächste Schritte

- Entfernen Sie den catalog-Snapshot, wie im nächsten Abschnitt beschrieben.

Entfernen des catalog-Snapshots

Nachdem Sie den Data Store neu gestartet haben, entfernen Sie den Snapshot mit dem Namen `catalog`. Dieser Snapshot wird nach der Wiederherstellung nicht mehr benötigt und hindert Vertica an der Ausführung der Aufbewahrungsverwaltung.

Vorbereitungen

- Melden Sie sich bei einer Data Node-Konsole als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w [password] -c "select remove_database_snapshot('catalog');"
   ```

3. Ersetzen Sie `[password]` durch Ihr `dbadmin`-Kennwort.
4. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um den `catalog`-Snapshot zu entfernen.

Nächste Schritte

- Verbinden Sie Ihre Flow Collectors erneut mit dem Data Store und stellen Sie sicher, dass sie Daten weiterleiten.
- Verbinden Sie Ihre SMC wieder mit dem Data Store.

Hinzufügen von drei Data Nodes zum Data Store

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Sie können Ihren Data Store in Schritten von drei Data Nodes oder Vielfachen von drei Data Nodes erweitern. Wenn Sie die Anzahl der Data Nodes in Ihrem Data Store erweitern möchten, führen Sie die folgenden Aufgaben aus:

Vorbereitung des Data Store für das Hinzufügen von Data Nodes und Rebalancing

Bevor Sie einen Data Node hinzufügen, gehen Sie wie folgt vor:

- Führen Sie ein Backup des Data Store durch. Weitere Informationen finden Sie unter **Erstellen eines Data Store-Backups**.
- Stellen Sie sicher, dass Ihre Flow Collectors nicht mit dem Data Store verbunden sind und Daten weiterleiten.
- Stellen Sie sicher, dass Ihre SMC nicht mit dem Data Store verbunden ist und den nicht Data Store abfragt oder anderweitig aktualisiert.
- Löschen Sie alte, ungenutzte Datenpartitionen. Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Identifizierung dieser Partitionen zu erhalten.
- Deaktivieren Sie lokale Segmente. Geben Sie von vsql aus den Befehl `SELECT DISABLE_LOCAL_SEGMENTS()`
- Aktualisieren Sie Ihre Ressourcenpool-Einstellungen. Geben Sie von vsql aus den Befehl `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '70%;`

Hinzufügen von Data Nodes zum Data Store

Als Nächstes müssen Sie, falls noch nicht geschehen, die Data Nodes in Vielfachen von 3 in Ihrem Netzwerk bereitstellen. Führen Sie mithilfe von First Time Setup in der Systemkonfiguration die Erstkonfiguration durch und schließen Sie sie mit dem und dem Appliance Setup Tool ab. Weitere Informationen finden Sie in **Anhang B. Stealthwatch Installation der Hardware** und **Anhang C. Konfigurieren Ihrer Appliances**.

Nachdem Sie die Data Nodes konfiguriert haben, einschließlich der Zuweisung einer routbaren `eth0`-Management-IP-Adresse und einer nicht routbaren `eth2`- oder `eth2/eth3`-Port-Channel-IP-Adresse, führen Sie Folgendes aus:

- Melden Sie sich bei einem Data Node an und konfigurieren Sie die Konfigurationsdatei `update_SDBN.cfg`, um Ihre neuen Data Nodes hinzuzufügen.
- Führen Sie das Skript `update_SDBN.py` aus, um die Data Nodes zum Data Store hinzuzufügen, und fügen Sie sie optional auch zur Data Store-Datenbank hinzu.

Hinzufügen von Data Nodes zum Data Store:

Vorbereitungen

- Melden Sie sich bei der Konsole eines Data Nodes als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Geben Sie in der Kommandozeile `cd /lancope/database` ein und drücken Sie die Eingabetaste, um in das entsprechende Verzeichnis zu wechseln.
3. Geben Sie `cp update_SDBN_example.cfg update_SDBN.cfg` ein und drücken Sie die Eingabetaste, um eine Kopie der Beispielkonfigurationsdatei zum Hinzufügen von Data Nodes zu erstellen.
4. Geben Sie `vi update_SDBN.cfg` ein und drücken Sie die Eingabetaste, um die Konfigurationsdatei zum Hinzufügen von Data Nodes in einem Texteditor zu ändern.
5. Erstellen Sie fortlaufend nummerierte `[nodeN]`-Abschnitte, die der Anzahl der neuen Data Nodes entsprechen, die Sie zum Data Store hinzufügen möchten. Wenn Sie z. B. bereits 3 Data Nodes in Ihrem Netzwerk bereitgestellt haben und 6 Data Nodes hinzufügen möchten, sieht Ihre Datei wie folgt aus:

```
[node1]
private = 169.254.42.30
public = 10.0.16.114
[node2]
private = 169.254.42.31
public = 10.0.16.115
[node3]
private = 169.254.42.32
public = 10.0.16.116
[node4]
private = 169.254.42.33
public = 10.0.16.117
[node5]
private = 169.254.42.34
public = 10.0.16.118
[node6]
private = 169.254.42.35
public = 10.0.16.119
[common]
subnet = 10.0.16.0
firstNode = 4
```

6. Geben Sie, beginnend mit dem Abschnitt `[node1]`, die privaten und öffentlichen IP-Adressen für jeden neuen Data Node ein. Beachten Sie Folgendes:

- Dieses Skript fügt Data Nodes in der Reihenfolge, in der sie aufgelistet sind, zum Data Store hinzu. Die fortlaufende Nummerierung beginnt dabei nach der höchsten Nummer eines Data Node, der bereits Teil des Data Store ist. Wenn Sie Ihre Data Nodes in verschiedenen Racks bereitgestellt haben, wechseln Sie die Knotenzuordnung zwischen den Racks ab, um die Datenredundanz zu maximieren.
- Die privaten IP-Adressen sollten nicht routbar sein und sich in einem privaten LAN oder VLAN befinden. Sie müssen IP-Adressen aus dem CIDR-Block `169.254.42.0/24` zuweisen.
- Überlappen Sie keine IP-Adressen zwischen oder unter Data Nodes.
- Fügen Sie hier nicht Ihren Ersatz-Data Node hinzu, auch wenn Sie ihn in Ihrer Umgebung bereitgestellt haben, ohne ihn zu konfigurieren. Fügen Sie nur Data Nodes hinzu, die Teil des Data Store sein sollen.

7. Aktualisieren Sie im Abschnitt `[common]` das `subnet` so, dass es Ihren öffentlichen IP-Adressen entspricht.
8. Aktualisieren Sie im Abschnitt `[common]` den Wert `firstNode` so, dass er um eins höher ist als die Anzahl der Data Nodes, die bereits Teil Ihrer Data Store-Bereitstellung sind.
9. Drücken Sie die Esc-Taste, geben Sie `:wq` ein und drücken Sie die Eingabetaste, um Ihre Änderungen zu speichern und den Texteditor zu beenden.
10. In der Kommandozeile haben Sie die folgenden Optionen:

    Geben Sie `python update_SDBN.py -i update_SDBN.cfg` ein und drücken Sie die Eingabetaste, um das Python-Skript zum Hinzufügen von Data Nodes auszuführen. Dieses Skript verwendet die Konfigurationsdatei `update_SDBN.cfg`, um die neuen Data Nodes in der von Ihnen angegebenen Reihenfolge zum Data Store hinzuzufügen. Beachten Sie, dass sie in diesem Fall **nicht** zur Datenbank hinzugefügt werden.

    Geben Sie `python update_SDBN.py -i update_SDBN.cfg -d` ein und drücken Sie Enter, um das Python-Skript zum Hinzufügen von Data Nodes auszuführen. Dieses Skript verwendet die Konfigurationsdatei `update_SDBN.cfg`, um die neuen Data Nodes in der von Ihnen angegebenen Reihenfolge zum Data Store hinzuzufügen, und fügt die Data Nodes auch zur Datenbank hinzu.

    Nachdem das Skript beendet ist, überprüfen Sie die Statusmeldungen der Kommandozeile, um sicherzustellen, dass das Skript erfolgreich war.
11. Geben Sie `cd /opt/vertica/config` ein, um in das entsprechende Verzeichnis zu wechseln.

12. Geben Sie `vi apikeys.dat` ein, um die API-Schlüsseldatei in einem Texteditor zu öffnen.
13. Drücken Sie Esc, geben Sie dann `q!` ein und drücken Sie die Eingabetaste, um den Texteditor zu verlassen, ohne die Änderungen zu speichern.
14. Notieren Sie sich die IP-Adresse dieses Data Nodes. Sie verwenden diese IP-Adresse später im Abschnitt **Wartung des Data Store**, um VMC auf Ihrer SMC zu konfigurieren.

Wenn Sie die neuen Data Nodes nicht mit dem Skript `update_SDBN.py` zur Datenbank hinzufügen, können Sie die Data Nodes stattdessen manuell hinzufügen. Melden Sie sich bei einem Data Node in Ihrem Data Store an und fügen Sie die Data Nodes zum Data Store hinzu.

Hinzufügen neuer Data Stores zum Data Node:

Vorbereitungen

- Melden Sie sich bei einem Data Node als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   admintools -t db_add_node -d sw -p '[dbadmin-password]' -s
   [data-node-eth0-addresses]
   ```

3. Ersetzen Sie `[dbadmin-password]` durch Ihr `dbadmin`-Kennwort.
4. Ersetzen Sie `[data-node-eth0-addresses]` durch eine kommagetrennte Liste der routbaren `eth0`-IP-Adressen der neuen Data Node.
5. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um die neuen Data Nodes zur Datenbank hinzuzufügen.

Nachdem Sie die Data Nodes zu Ihrer Datenbank hinzugefügt haben, führen Sie ein Daten-Rebalancing auf den Data Nodes aus, um eine ausgeglichene Datenspeicherung auf jedem Data Node zu gewährleisten.

Rebalancing der Daten im Data Store

Vorbereitungen

- Melden Sie sich bei einem Data Node als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   /opt/vertica/bin/vsql --timing -x -c "SELECT rebalance_
   cluster()" -a -d sw -U dbadmin -w [dbadmin-password]
   ```

3. Ersetzen Sie `[dbadmin-password]` durch das `dbadmin`-Kennwort.
4. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um das Daten-Rebalancing zu starten. Beachten Sie, dass dies eine Weile dauern kann. Der Zeitbedarf hängt von mehreren Faktoren ab, unter anderem von der Anzahl der Projektionen und der Datenmenge.
5. Aktualisieren Sie nach Abschluss des Rebalancing Ihre Ressourcenpool-Einstellungen. Geben Sie von vsql aus den Befehl `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '0%;`

Entfernen eines Data Node aus dem Data Store

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Wenn Sie einen Data Node aus dem Data Store entfernen möchten, beachten Sie Folgendes:

- Der Data Store muss aktiv sein.
- Führen Sie zuerst ein Backup durch. Weitere Informationen finden Sie unter **Erstellen eines Data Store-Backups**.
- Wegen der Fehlertoleranzeinstellungen müssen Sie mindestens 3 Knoten im Data Store haben. Wenn Sie einen Knoten austauschen möchten, finden Sie weitere Informationen unter **Austauschen eines Data Node gegen einen Ersatz-Data Node mit einer anderen IP-Adresse**.

Entfernen eines Knotens aus dem Data Store:

Vorbereitungen

- Melden Sie sich bei Vertica Management Console als `dbadmin` an.

Verfahren

1. Wählen Sie **Manage** (Verwalten). Die Seite „Manage Tags“ (Tags verwalten) wird angezeigt.
2. Wählen Sie den Knoten aus, den Sie entfernen möchten, und klicken Sie dann auf **Remove Node** (Knoten entfernen).

Austauschen eines Data Node gegen einen Ersatz-Data Node mit einer anderen IP-Adresse

> Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung und Umsetzung dieser Aufgaben zu erhalten.

Vorbereiten des Data Store für den Austausch eines ausgefallenen Data Nodes

- Führen Sie ein Backup des Data Store durch. Weitere Informationen finden Sie unter **Erstellen eines Data Store-Backups**.
- Fügen Sie den Ersatz-Data Node zum Data Store hinzu. Weitere Informationen finden Sie unter **Hinzufügen von Data Nodes zum Data Store:**.

Ersetzen des Data Node

Wenn Vertica noch auf dem Data Node läuft, den Sie ersetzen möchten, stoppen Sie Vertica. Ersetzen Sie dann den ursprünglichen Data Node durch den neuen Data Node und verteilen Sie die erforderliche Konfiguration an den neuen Data Node. Entfernen Sie den ursprünglichen Data Node und starten Sie den neuen Data Node neu.

Vertica auf einem Data Node stoppen

Wenn auf dem Data Node, den Sie entfernen möchten, noch Vertica ausgeführt wird, beenden Sie Vertica auf diesem Data Node. Wenn dieser Data Node ausgefallen ist oder Vertica aus anderen Gründen nicht ausgeführt wird, fahren Sie mit dem nächsten Schritt fort.

Vorbereitungen

- Melden Sie sich bei der Konsole eines Data Nodes als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   `/opt/vertica/bin/admintools -t stop_host -s [node-ip-addresses]`
3. Ersetzen Sie `[node-ip-addresses]` durch eine kommagetrennte Liste der routbaren Data Node-`eth0`-IP-Adressen, die Sie aus dem Data Store entfernen möchten.
4. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um Vertica auf diesem Data Node zu stoppen.

Ersetzen eines Data Nodes

Vorbereitungen

- Melden Sie sich bei der Konsole eines Data Nodes als `root` an.

Verfahren

1. Geben Sie `su - dbadmin` ein und drücken Sie die Eingabetaste, um die folgenden Befehle als Benutzer `dbadmin` auszuführen.
2. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   `/opt/vertica/bin/admintools -t db_replace_node -d sw -o [old-data-node-hostname] -n [new-data-node-hostname]`
3. Ersetzen Sie `[old-data-node-hostname]` durch den Data Node-Hostnamen, den Sie aus dem entfernen Data Store möchten.
4. Ersetzen Sie `[new-data-node-hostname]` durch den Data Node-Hostnamen, den Sie als Ersatz zum Data Store hinzufügen möchten.
5. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um den ursprünglichen Data Node durch den neuen Data Node zu ersetzen.
6. Kopieren Sie `/opt/vertica/bin/admintools -t distribute_config_files`, fügen Sie es in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um die Konfigurationsdateien auf den neuen Data Node zu verteilen.
7. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   `/opt/vertica/sbin/update_vertica --remove-hosts [old-data-node-hostname]`

8. Ersetzen Sie `[old-data-node-hostname]` durch den Data Node-Hostnamen, den Sie aus dem Data Store entfernen möchten.
9. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um den ursprünglichen Data Node aus dem Data Store zu entfernen.
10. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

    `/opt/vertica/bin/admintools -t restart_node -s [new-data-node-hostname]`

11. Ersetzen Sie `[new-data-node-hostname]` durch den Data Node-Hostnamen, den Sie als Ersatz zum Data Store hinzufügen möchten.
12. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um den neuen Data Node neu zu starten.

Kopieren von Data Store-Trust-Informationen auf eine Failover-SMC

Wenn Sie eine Failover-SMC in Ihrer Umgebung bereitstellen und diese von Ihrer primären SMC verwaltet wird, werden beim Ausführen des Skripts `setup-sw-datastore-secure-connectivity` bestimmte Trust-Informationen, einschließlich `dbadmin`- und `readonlyuser`-Kennwörter und Identitätszertifikate für die sichere Kommunikation mit Data Nodes, nicht auf die Failover-SMC kopiert. Bevor Sie die Failover-SMC in einer Data Store-Bereitstellung zur primären SMC hochstufen können, müssen Sie Dateien von Ihrer primären SMC auf die Failover-SMC kopieren. Wenn Sie diese Trust-Informationen nicht kopieren, kann Ihre SMC keine Verbindung mit dem Data Store herstellen.

Wenn Sie Ihre Failover-SMC bereits zur primären SMC hochgestuft und Ihre primäre SMC zur Failover-SMC heruntergestuft haben und neue Appliances zu Ihrer Stealthwatch-Bereitstellung hinzufügen möchten, müssen Sie darüber hinaus die Trust-Informationen auf die neue Failover-SMC kopieren, bevor Sie `setup-sw-datastore-secure-connectivity` ausführen. Wenn Sie diese Trust-Informationen nicht kopieren, kann das Skript fehlschlagen.

Kopieren von Trust-Informationen zwischen SMCs:

Vorbereitungen

- Identifizieren Sie die IP-Adressen und Root-Anmeldeinformationen der primären und der Failover-SMC.

- Wenn Ihre Failover-SMC gerade zur primären SMC hochgestuft wurde, melden Sie sich bei der Konsole dieser SMC als `root` an.

Verfahren

1. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   scp root@[demoted-smc-ip-
   address]:/lancope/var/admin/cds/sw-datastore-*
   /lancope/var/admin/cds
   ```

2. Ersetzen Sie `[demoted-smc-ip-address]` durch die IP-Adresse Ihrer soeben heruntergestuften SMC (aktuelle Failover-SMC).
3. Kopieren Sie den geänderten Befehl, fügen Sie ihn in die Eingabeaufforderung ein und drücken Sie die Eingabetaste, um die Data Store-Trust-Informationen von Ihrer soeben herabgestuften (aktuellen Failover-) SMC auf Ihre soeben hochgestufte (aktuelle primäre) SMC zu kopieren. Geben Sie Ihr `root`-Kennwort für die soeben herabgestufte (aktuelle Failover-) SMC ein, wenn Sie dazu aufgefordert werden.

Fehlerbehebung bei der Data Store-Bereitstellung

Fehlerbehebung bei der Hardwarebereitstellung

Bei Problemen mit der Bereitstellung oder Konfiguration Ihrer SMC oder Flow Collectors finden Sie weitere Informationen im Stealthwatch x210-Hardware-Installationshandbuch und im Stealthwatch-Systemkonfigurationshandbuch.

Fehlerbehebung beim setup-sw-datastore-secure-connectivity-Skript

Wenn Sie eine Failover-SMC zur primären SMC hochgestuft haben, finden Sie unter Kopieren von Data Store-Trust-Informationen auf eine Failover-SMC Informationen zum Kopieren der Trust-Informationen vom Data Store auf Ihre soeben hochgestufte (aktuelle primäre) SMC.

Das `setup-sw-datastore-secure-connectivity`-Skript für die sichere Data Store-Verbindung protokolliert Meldungen in den Protokolldateien unter `/lancope/var/logs/containers/setup-sw-datastore-secure-connectivity.log`. Dort finden Sie weitere Informationen.

Allgemeine setup-sw-datastore-secure-connectivity-Fehlermeldungen

In der folgenden Tabelle sind Fehlermeldungen aufgeführt, die möglicherweise angezeigt werden, wenn das Skript `setup-sw-datastore-secure-connectivity` auf einen Fehler stößt, sowie mögliche Lösungen für das Problem.

Fehlermeldung	Beschreibung	Mögliche Lösungen
Error authorizing remote login for `[ip-address]`	Das Skript `setup-sw-datastore-secure-connectivity` konnte sich nicht remote bei einer	• Prüfen Sie, ob Sie das richtige Root-Kennwort für den Zugriff angegeben haben. • Vergewissern Sie sich, dass die Appliance gerade läuft. • Vergewissern Sie sich, dass die

	Appliance anmelden, um Schlüsselinformationen bereitzustellen.	Verbindung zwischen dem Skript und der Appliance aktuell hergestellt ist.
Error generating key pair.	Das Skript `setup-sw-datastore-secure-connectivity` ist auf einen Fehler beim Generieren der Schlüssel gestoßen, die den für sichere Data Store-Verbindungen verwendeten Identitätszertifikaten zugeordnet sind.	• Wenden Sie sich für weitere Informationen an den Cisco Support.
Failed to authenticate with token authority.	Das Skript `setup-sw-datastore-secure-connectivity` konnte die Verbindung mit Central Management nicht ordnungsgemäß herstellen.	• Wenden Sie sich für weitere Informationen an den Cisco Support.
Failed to get inventory from SMC.	Das Skript	• Überprüfen Sie `/lancope/var/logs/contai`

	`setup-sw-datastore-secure-connectivity` konnte die Informationen von Central Management nicht richtig abrufen.	`ner/svc-central-management.log`, um festzustellen, ob es ein Problem mit Central Management gibt. • Wenden Sie sich für weitere Informationen an den Cisco Support.
No DB Clients found.	Die SMC und die Flow Collectors wurden nicht richtig für die Verwendung mit einem Data Store konfiguriert.	• Melden Sie sich bei der CLI der Appliance an, führen Sie die Systemkonfiguration aus und aktivieren Sie die Verwendung mit einem Data Store.
Password is not available. You may want to delete /lancope/var/etc/keystore/store and rerun setup-sw-datastore-secure-connectivity.	Im Skript `setup-sw-datastore-secure-connectivity` ist ein Problem beim Speichern oder Verteilen des `dbadmin`- und des `readonlyuser`-Kennworts aufgetreten.	• Löschen Sie den Inhalt von `/lancope/var/etc/keystore/store` und führen Sie dann das Skript `setup-sw-datastore-secure-connectivity` erneut aus.
Register the data nodes with Central Management before attempting to setup the secure connection.	Ihre Data Nodes werden nicht von Central Management verwaltet.	• Verwalten Sie Ihre Data Nodes mit Central Management.

SMC inventory is empty. Please add an appliance to Central Management.	Central Management verwaltet keine Data Nodes oder Flow Collectors.	• Verwalten Sie Ihre Flow Collector und Data Nodes mit Central Management.
sw-datastore-dbadmin-password and/or sw-datastore-readonlyuser-password not present in input	Das `dbadmin`- oder das `readonlyuser`-Kennwort wurde nicht definiert.	• Führen Sie im Skript **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen) erneut aus, falls Sie den Data Store noch nicht initialisiert haben, und definieren Sie sowohl ein `dbadmin`- als auch ein `readonlyuser`-Kennwort. • Wenn Sie den Data Store initialisiert haben, führen Sie im Skript **3. Update SW DataStore password on appliances** (SW-DataStore-Kennwort auf Appliances aktualisieren) aus, um das `dbadmin`- und das `readonlyuser`-Kennwort zu aktualisieren.
SW Datastore password (s) already initialized on `[ip-address]`.	Der Data Store ist bereits initialisiert; Sie können **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances	• Führen Sie im Skript **3. Update SW DataStore password on appliances** (SW-DataStore-Kennwort auf Appliances aktualisieren) aus, um das `dbadmin`- und das `readonlyuser`-Kennwort zu aktualisieren.

	verteilen) in `setup-sw-datastore-secure-connectivity` nicht verwenden, um das `dbadmin`- oder das `readonlyuser`-Kennwort zu ändern.	
SW Datastore password (s) are not stored due to: Empty value	Das `dbadmin`- oder das `readonlyuser`-Kennwort wurde nicht definiert.	• Führen Sie im Skript **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen) erneut aus, falls Sie den Data Store noch nicht initialisiert haben, und definieren Sie sowohl ein `dbadmin`- als auch ein `readonlyuser`-Kennwort. • Wenn Sie den Data Store initialisiert haben, führen Sie im Skript **3. Update SW DataStore password on appliances** (SW-DataStore-Kennwort auf Appliances aktualisieren) aus, um das `dbadmin`- und das `readonlyuser`-Kennwort zu aktualisieren.
There are no data nodes currently managed.	Ihre Data Nodes werden nicht von Central Management verwaltet.	• Verwalten Sie Ihre Data Nodes mit Central Management.

There are no SMC/FCs currently managed.	Ihre Flow Collectors (und alle Failover-SMC) werden nicht von Central Management verwaltet.	• Verwalten Sie Ihre Flow Collectors (und Failover-SMC) mit Central Management.
Unknown error code: `[error-code]` on `[ip-address]`	Das Skript ist beim Versuch, das `dbadmin`- und das `readonlyuser`-Kennwort zu verteilen, auf einen Fehler gestoßen.	• Wenden Sie sich für weitere Informationen an den Cisco Support.

Fehlerbehebung beim install_SDBN_initial.py-Skript

Das Data Store-Initialisierungsskript `install_SDBN_initial.py` protokolliert Meldungen in den Protokolldateien unter `/lancope/var/database/logs/db_initial_install_[datestamp].log`. Dort finden Sie weitere Informationen.

Voraussetzungen bei der lokalen (Betriebssystem-m-)Konfiguration für verify-[data-node-ip-address].xml nicht vollständig erfüllt

Bei der Initialisierung des Data Store in Data Store-Initialisierung und -Konfiguration durch Ausführen des Python-Skripts `install_SDBN_initial.py` gibt die Konsole möglicherweise `Prerequisites not fully met during local (OS) configuration for verify-[data-node-ip-address].xml` gefolgt von einer Reihe von Protokollierungsmeldungen aus. Diese Protokollmeldungen sind zu erwarten und deuten nicht auf einen Fehler bei der Initialisierung des Data Store hin. Sie müssen bei keiner dieser Protokollmeldungen etwas unternehmen.

Die folgende Tabelle beschreibt diese Meldungen im Einzelnen.

Protokollstufe und Fehlercode	Beschreibung	Erklärung
FAIL (s0180)	Insufficient swap size. Need 2.00 GB, have 1.50 GB	Der zugewiesene Speicherplatz für die Auslagerungspartition entspricht nicht den Empfehlungen. Ändern Sie **nicht** die Zuweisung des Auslagerungsbereichs. Cisco hat Ihren Data Store mit der korrekten Auslagerungsbereichs-Zuweisung konfiguriert.
FAIL (s0311)	root account is not in /etc/sudoers	Das Installationsprogramm hat das Root-Konto in der Superuser-Berechtigungsliste `/etc/sudoers` nicht gefunden und empfiehlt, Vertica zu aktualisieren, um das Problem zu beheben. Aktualisieren Sie Vertica **nicht**! Diese Konfiguration ist aus Sicherheitsgründen beabsichtigt.
HINT (S0040)	Could not find the following tools normally provided by the pstack or gstack package: pstack/gstack	Das Installationsprogramm kann weder das Paket `pstack` noch das Paket `gstack` für die Protokollierung von Stack-Traces finden. Diese sind für Ihren Data Store nicht erforderlich.
HINT (S0041)	Could not find the following tools normally provided by the mcelog package: mcelog	Das Installationsprogramm kann das Paket `mcelog` zur Protokollierung von Maschinenprüfungen nicht finden. Dies ist für Ihren Data Store nicht erforderlich.
HINT (S0305)	TZ is unsert for dbadmin. Consider updating	Das Installationsprogramm hat keine `TZ`-Umgebungsvariable für das dbadmin-Benutzerkonto gefunden, die für Zeitzonen verwendet wird. Dies ist für Ihren Data Store

	`.profile or .bashrc`	nicht erforderlich, da Sie NTP-Server für Ihre Stealthwatch-Bereitstellung konfigurieren.
`WARN (N0010)`	`Linux iptables (firewall) has some non-trivial rules in tables: filter`	`iptables` auf dem Data Node enthält bereits existierende Regeln. Das System protokolliert eine Warnung, wenn `iptables` Regeln enthält, aber nicht auf Kollisionen mit erforderlichen Kommunikationsports prüft. Dies ist zu erwarten und sollte keine Probleme mit Ihrer Data Node-Bereitstellung verursachen.

SSLCA-Konfigurationsparameter ist nicht festgelegt – Client-Zertifikate werden nicht angefordert oder verifiziert

Bei der Initialisierung des Data Store in Data Store-Initialisierung und -Konfiguration durch Ausführen des Python-Skripts `install_SDBN_initial.py` gibt die Konsole möglicherweise `Enable SSL/TLS for remote connections` gefolgt von `INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified` aus (einmal für jeden Data Node, den Sie initialisieren). Diese Protokollmeldung ist zu erwarten und deutet nicht auf einen Fehler beim Aufbau sicherer Verbindungen mit dem Data Store hin. Sie müssen bei keiner dieser Protokollmeldungen etwas unternehmen.

Der Data Store ist im TLS-Server-Modus konfiguriert, der erfordert, dass Appliances beim Herstellen einer sicheren Verbindung zum Data Store auch das Serverzertifikat der Datenbank verifizieren. Im Gegensatz dazu steht die Konfiguration im TLS-Mutual-Modus, der erfordert, dass beim Herstellen einer sicheren Verbindung zum Data Store die Appliance das Serverzertifikat der Datenbank und die Datenbank die Client-Zertifikate der Appliances verifizieren muss. Der TLS-Mutual-Modus erfordert die Konfiguration des Parameters `SSLCA` mit der Datei `root.crt`, die die Zertifizierungsstelle (CA) oder die CA-Vertrauenskette enthält, die zum Signieren der Client-Zertifikate verwendet wurde. Da der Mutual-Modus nicht aktiviert ist, ist `SSLCA` nicht konfiguriert, und der Data Store überprüft die Client-Zertifikate beim Aufbau einer sicheren Verbindung nicht. Die Verbindung zwischen Appliances und dem Data Store im TLS-Server-Modus ist jedoch weiterhin eine sichere Verbindung über TLS.

Allgemeine Fehlermeldungen von install_SDBN_

initial.py

In der folgenden Tabelle sind Fehlermeldungen aufgeführt, die möglicherweise angezeigt werden, wenn das Skript `install_SDBN_initial.py` auf einen Fehler stößt, sowie mögliche Lösungen für das Problem.

Fehlermeldung	Beschreibung	Mögliche Lösungen
Config file not found or no valid sections	Das Skript `install_SDBN_initial.py` kann die Konfigurationsdatei `install_SDBN.cfg` nicht finden, oder die Daten in der Konfigurationsdatei liegen nicht in einem erwarteten Format vor.	• Stellen Sie sicher, dass Sie eine Kopie von `install_SDBN_example.cfg` unter `/lancope/database/install_SDBN.cfg` auf diesem Data Node gespeichert haben. • Stellen Sie sicher, dass die Formatierung in `install_SDBN.cfg` mit der Formatierung in `install_SDBN_example.cfg` übereinstimmt, dass Sie jeden Knotenabschnitt im Format `node#` benennen, dass Sie sowohl eine private als auch eine öffentliche IP-Adresse für jeden Data Node-Konfigurationsabschnitt definiert haben und dass Sie im Abschnitt „common“ ein Subnetz definiert haben.
Could not find the expected jar file to retrieve DB user passwords, check that you are running an image containing this support	Das Skript `install_SDBN_initial.py` kann die Datei `sw-datastore-admin.jar` nicht finden, die das `dbadmin`- und das `readonlyuser`-Kennwort enthält.	• Stellen Sie sicher, dass Ihre Appliance die Version 7.3+ hat. • Führen Sie das Skript `setup-sw-datastore-secure-connectivity` unter `/lancope/admin/cds` aus und wählen Sie Option **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen), um das dbadmin- und das readonlyuser-Kennwort zu verteilen. Führen Sie

		danach, falls noch nicht geschehen, auch Option **2. Distribute Certificates for Secure DB Connection** (Verteilen von Zertifikaten für sichere DB-Verbindungen) aus. • Wenden Sie sich an den Cisco Support, wenn der Fehler weiterhin besteht.
each node must have a public and private address entry	Die Konfigurationsdatei `install_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die nicht sowohl eine private als auch eine öffentliche IP-Adresse definiert ist.	• Stellen Sie sicher, dass Sie in `/lancope/database/install_SDBN.cfg` für jeden Data Node-Konfigurationsabschnitt sowohl eine private als auch eine öffentliche IP-Adresse definiert haben.
Either the secret store file does not exist OR the password does not exist in the file. Please login to the SMC and run the appropriate script to set and distribute the DB passwords.	Das Skript `install_SDBN_initial.py` ist beim Versuch, das `dbadmin`- und das `readonlyuser`-Kennwort abzurufen, auf ein Problem gestoßen.	• Führen Sie von der SMC-CLI aus das Skript `setup-sw-datastore-secure-connectivity` unter `/lancope/admin/cds` aus und wählen Sie Option **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen), um das dbadmin- und das readonlyuser-Kennwort zu verteilen. Führen Sie danach, falls noch nicht geschehen, auch Option **2. Distribute Certificates for Secure DB Connection** (Verteilen von Zertifikaten für sichere DB-Verbindungen) aus.

Failed to retrieve the database passwords	Das Skript `install_SDBN_initial.py` ist beim Versuch, das `dbadmin`- und das `readonlyuser`-Kennwort abzurufen, auf ein Problem gestoßen.	• Führen Sie von der SMC-CLI aus das Skript `setup-sw-datastore-secure-connectivity` unter `/lancope/admin/cds` aus und wählen Sie Option **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen), um das dbadmin- und das readonlyuser-Kennwort zu verteilen. Führen Sie danach, falls noch nicht geschehen, auch Option **2. Distribute Certificates for Secure DB Connection** (Verteilen von Zertifikaten für sichere DB-Verbindungen) aus.
I/O exception while attempting to read the file	Das Skript `install_SDBN_initial.py` ist beim Versuch, das `dbadmin`- und das `readonlyuser`-Kennwort abzurufen, auf ein Problem gestoßen.	• Wenden Sie sich an den Cisco Support und geben Sie die Fehlermeldung an.
One of both of the passwords does not exists in the file. Please login to the SMC and run the appropriate script to set and distribute the DB passwords.	Das Skript `install_SDBN_initial.py` ist beim Versuch, das `dbadmin`- und das `readonlyuser`-Kennwort abzurufen, auf ein Problem gestoßen.	• Führen Sie von der SMC-CLI aus das Skript `setup-sw-datastore-secure-connectivity` unter `/lancope/admin/cds` aus und wählen Sie Option **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen), um das dbadmin- und das readonlyuser-Kennwort zu verteilen. Führen Sie danach, falls noch nicht geschehen, auch Option **2. Distribute Certificates**

		for Secure DB Connection (Verteilen von Zertifikaten für sichere DB-Verbindungen) aus.
privateAddrs must be specified	Die Konfigurationsdatei `install_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die keine private IP-Adresse definiert ist.	• Stellen Sie sicher, dass Sie in `/lancope/database/install_SDBN.cfg` für jeden Data Node-Konfigurationsabschnitt eine private IP-Adresse definiert haben. Beachten Sie, dass der Data Node diese nicht routbare IP-Adresse auf `eth2` verwendet, um mit anderen Data Nodes als Teil des Data Store zu kommunizieren.
publicAddrs must be specified	Die Konfigurationsdatei `install_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die keine öffentliche IP-Adresse definiert ist.	• Stellen Sie sicher, dass Sie in `/lancope/database/install_SDBN.cfg` für jeden Data Node-Konfigurationsabschnitt eine öffentliche IP-Adresse definiert haben. Beachten Sie, dass der Data Node diese routbare IP-Adresse auf `eth0` verwendet, um mit anderen Stealthwatch-Appliances als Teil Ihrer Stealthwatch-Bereitstellung zu kommunizieren.
publicSubnet must be specified	Die Konfigurationsdatei `install_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die kein Subnetz definiert ist.	• Vergewissern Sie sich, dass Sie im allgemeinen Konfigurationsabschnitt in `/lancope/database/install_SDBN.cfg` ein Subnetz definiert haben. Beachten Sie, dass dieses Subnetz den routbaren IP-Adressen auf `eth0` zugeordnet ist, die Data Nodes zur Kommunikation mit anderen Stealthwatch-Appliances als Teil Ihrer Stealthwatch-Bereitstellung verwenden.

Unexpected exception while reading the secrets	Das Skript `install_SDBN_initial.py` ist beim Versuch, das `dbadmin`- und das `readonlyuser`-Kennwort abzurufen, auf ein Problem gestoßen.	• Führen Sie das Skript `setup-sw-datastore-secure-connectivity` unter `/lancope/admin/cds` aus und wählen Sie Option **1. Distribute SW DataStore password to appliances** (SW DataStore-Kennwort an Appliances verteilen), um das dbadmin- und das readonlyuser-Kennwort zu verteilen. Führen Sie danach, falls noch nicht geschehen, auch Option **2. Distribute Certificates for Secure DB Connection** (Verteilen von Zertifikaten für sichere DB-Verbindungen) aus. • Wenden Sie sich an den Cisco Support, wenn der Fehler weiterhin besteht.
Unexpected return value	Das Skript `install_SDBN_initial.py` hat einen Wert empfangen und die Ausführung abgebrochen, weil es nicht fortfahren konnte.	• Wenden Sie sich an den Cisco Support und geben Sie die Fehlermeldung an.

Aktualisieren der dbadmin- und readonlyuser-Kennwörter auf dem Data Store nach der Initialisierung:

Wenn Sie den Data Store bereits initialisiert haben, wie unter Data Store-Initialisierung und -Konfiguration beschrieben, und das `dbadmin`- und das `readonlyuser`-Kennwort ändern möchten, führen Sie das Bash-Skript `setup-sw-datastore-secure-connectivity` für die sichere Verbindung aus. Nachdem Sie das aktuelle `dbadmin`-Kennwort eingegeben haben, können Sie neue `dbadmin`- und `readonlyuser`-Kennwörter vergeben. Das Skript verteilt die aktualisierten

Anmeldeinformationen über SSH an Ihre Appliances und aktualisiert die Anmeldeinformationen der Benutzerkonten `dbadmin` und `readonlyuser`.

> Wenn Sie das `dbadmin`-Kennwort verloren haben, wenden Sie sich an den Cisco-Support, um Unterstützung bei der Wiederherstellung zu erhalten.

Jedes Kennwort muss die folgenden Anforderungen erfüllen:

- mindestens eine Ziffer enthalten
- mindestens 1 Kleinbuchstaben enthalten
- mindestens 1 Großbuchstaben enthalten
- mindestens 1 Sonderzeichen aus der folgenden Liste enthalten: `<>.,?/'"|:;`~!@#$%^&*()-_+={}[]`
- mindestens 8 Zeichen enthalten (es gibt keine Maximallänge)
- nur ASCII-codierte Zeichen enthalten

Beachten Sie, dass Sie diese Option verwenden, wenn Sie den Data Store bereits initialisiert haben. Wenn Sie den Data Store zum ersten Mal bereitstellen und konfigurieren, finden Sie unter Verteilen von Data Store-Kennwörtern an Ihre SMC, Data Nodes und Flow Collectors, um ein `dbadmin`- und ein `readonlyuser`-Kennwort zuzuweisen und die Einstellungen für die sichere Verbindung mit der Data Store-Datenbank zu konfigurieren.

Wenn Sie ein Backup Ihrer Data Store Datenbank erstellt und dann das `dbadmin`-Kennwort geändert haben, aktualisieren Sie die Backup-Kennwortdatei `pw.ini` mit dem neuen `dbadmin`-Kennwort. Weitere Informationen finden Sie unter Erstellen eines Data Store-Backups.

Vorbereitungen

- Stellen Sie eine Liste der Root-Kennwörter für Ihre SMC, Data Nodes, Flow Collectors und die sekundäre SMC, falls bereitgestellt, zusammen.
- Aktivieren Sie SSH-Zugriff und SSH-Root-Zugriff auf Ihrer SMC, den Data Nodes und den Flow Collectors.

  > Wenn SSH aktiviert ist, steigt das Kompromittierungsrisiko des Systems. Es ist wichtig, SSH nur zu aktivieren, wenn Sie es brauchen. Wenn Sie SSH nicht mehr verwenden, deaktivieren Sie es.

- Melden Sie sich als Root-Benutzer bei Ihrer SMC-CLI an.

Verfahren

1. Geben Sie in der Kommandozeile `cd /lancope/admin/cds` ein und drücken Sie die Eingabetaste, um in das entsprechende Verzeichnis zu wechseln.
2. Geben Sie `./setup-sw-datastore-secure-connectivity` ein und drücken Sie die Eingabetaste, um das Bash-Skript für die sichere Verbindung des Data Store auszuführen.
3. Wählen Sie im Hauptmenü des Skripts **3. Update SW DataStore password on appliances** (SW-DataStore-Kennwort auf Appliances aktualisieren) aus.
4. Geben Sie das aktuelle **dbadmin**-Kennwort ein und wählen Sie **OK**.
5. Wenn Sie in der Kommandozeile nach dem root-Kennwort für jede Appliance gefragt werden, geben Sie das Kennwort ein und drücken Sie die Eingabetaste.

   > Da Sie mehrere Kennwörter eingeben, achten Sie darauf, das richtige Kennwort für die jeweilige Appliance einzugeben.

   Nachdem Sie alle root-Kennwörter der Appliances eingegeben haben, fordert das Skript Sie zur Eingabe der `dbadmin`- und `readonlyuser`-Kennwörter auf.
6. Geben Sie das neue **dbadmin**-Kennwort ein.
7. Geben Sie dasselbe `dbadmin`-Kennwort zur Bestätigung in das Feld **dbadmin (confirmation)** ein.
8. Geben Sie das neue **readonlyuser**-Kennwort ein.
9. Geben Sie dasselbe `readonlyuser`-Kennwort zur Bestätigung in das Feld **readonlyuser (confirmation)** ein.

   > Geben Sie nicht dasselbe Kennwort für `dbadmin` und `readonlyuser` ein. Wenn Sie dasselbe Kennwort zuweisen, schlägt das Skript fehl und vergibt für beide Benutzerkonten keine Kennwörter.
10. Wählen Sie **OK**.

    Das Skript verteilt diese Kennwörter sicher an Ihre Appliances. Wenn dieser Vorgang abgeschlossen ist, wird eine Liste der aktualisierten Appliances angezeigt.
11. Wählen Sie **OK**, um zum Hauptmenü des Skripts zurückzukehren.

Nächste Schritte

- Melden Sie sich in VMC als `dbadmin` an. Sie werden aufgefordert, Ihr Kennwort zu aktualisieren.

> Wenn Sie das Kennwort nicht aktualisieren, sodass es mit dem neuen `dbadmin`-Kennwort übereinstimmt, sendet VMC keine Benachrichtigungen über Zustandswarnungen und überwacht Ihren Data Store auch anderweitig nicht mehr ordnungsgemäß.

Fehlerbehebung beim update_SDBN.py-Skript

Das Skript `update_SDBN_initial.py` zum Hinzufügen von Data Nodes protokolliert Meldungen in den Protokolldateien unter `/lancope/var/database/logs/db_update_[datestamp].log`. Dort finden Sie weitere Informationen.

Allgemeine Fehlermeldungen von update_SDBN_initial.py

In der folgenden Tabelle sind Fehlermeldungen aufgeführt, die möglicherweise angezeigt werden, wenn das Skript `update_SDBN_initial.py` auf einen Fehler stößt, sowie mögliche Lösungen für das Problem.

Fehlermeldung	Beschreibung	Mögliche Lösungen
Config file not found or no valid sections	Das Skript `update_SDBN.py` kann die Konfigurationsdatei `update_SDBN.cfg` nicht finden, oder die Daten in der Konfigurationsdatei liegen nicht in einem erwarteten Format vor.	• Stellen Sie sicher, dass Sie eine Kopie von `update_SDBN.cfg` unter `/lancope/database/update_SDBN.cfg` auf diesem Data Node gespeichert haben. • Stellen Sie sicher, dass die Formatierung in `update_SDBN.cfg` mit der Formatierung in `update_SDBN_example.cfg` übereinstimmt, dass Sie jeden Knotenabschnitt im Format `node#` benennen, dass Sie sowohl eine private als auch eine öffentliche IP-Adresse für jeden Data Node-Konfigurationsabschnitt definiert haben, dass Sie im Abschnitt „common“ ein Subnetz definiert haben und dass der erste Knoten so definiert ist, dass seine Nummer um eins höher ist als die

		Gesamtzahl aller Knoten, die sich bereits in Ihrem Data Store befinden.
each node must have a public and private address entry	Die Konfigurationsdatei `update_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die nicht sowohl eine private als auch eine öffentliche IP-Adresse definiert ist.	• Stellen Sie sicher, dass Sie in `/lancope/database/update_SDBN.cfg` für jeden Data Node-Konfigurationsabschnitt sowohl eine private als auch eine öffentliche IP-Adresse definiert haben.
Failed to retrieve the database dbadmin password	Das Skript `update_SDBN.py` kann das `dbadmin`-Kennwort nicht finden.	• Stellen Sie sicher, dass Ihre Appliance die Version 7.3+ hat. • Führen Sie das Skript `setup-sw-datastore-secure-connectivity` unter `/lancope/admin/cds` aus und wählen Sie Option **3. Update SW DataStore password on appliances** (SW-DataStore-Kennwort auf Appliances aktualisieren) aus, um das `dbadmin`- und das `readonlyuser`-Kennwort festzulegen. • Wenden Sie sich an den Cisco Support, wenn der Fehler weiterhin besteht.
firstNode must be specified	In der Konfigurationsdatei `update_SDBN.cfg` ist kein `firstNode`-Wert definiert.	• Vergewissern Sie sich, dass Sie im allgemeinen Konfigurationsabschnitt in `/lancope/database/update_SDBN.cfg` einen firstNode-Wert definiert haben.

privateAddrs must be specified	Die Konfigurationsdatei `update_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die keine private IP-Adresse definiert ist.	• Stellen Sie sicher, dass Sie in `/lancope/database/update_SDBN.cfg` für jeden Data Node-Konfigurationsabschnitt eine private IP-Adresse definiert haben. Beachten Sie, dass der Data Node diese nicht routbare IP-Adresse auf `eth2` verwendet, um mit anderen Data Nodes als Teil der Data Store-Datenbank zu kommunizieren.
publicAddrs must be specified	Die Konfigurationsdatei `update_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die keine öffentliche IP-Adresse definiert ist.	• Stellen Sie sicher, dass Sie in `/lancope/database/update_SDBN.cfg` für jeden Data Node-Konfigurationsabschnitt eine öffentliche IP-Adresse definiert haben. Beachten Sie, dass der Data Node diese routbare IP-Adresse auf `eth0` verwendet, um mit anderen Stealthwatch-Appliances als Teil Ihrer Stealthwatch-Bereitstellung zu kommunizieren.
publicSubnet must be specified	Die Konfigurationsdatei `update_SDBN.cfg` enthält einen oder mehrere Knoteneinträge, für die kein Subnetz definiert ist.	• Vergewissern Sie sich, dass Sie im allgemeinen Konfigurationsabschnitt in `/lancope/database/update_SDBN.cfg` ein Subnetz definiert haben. Beachten Sie, dass dieses Subnetz den routbaren IP-Adressen auf `eth0` zugeordnet ist, die Data Nodes zur Kommunikation mit anderen Stealthwatch-Appliances als Teil Ihrer Stealthwatch-Bereitstellung verwenden.

Fehlerbehebung bei Vertica Management Console

Wenn Ihre VMC-Instanz nicht automatisch in Ihrem Webbrowser aktualisiert wird, müssen Sie sie möglicherweise manuell aktualisieren, um Änderungen an Ihrem Data Store oder Konfigurationsänderungen anzuzeigen.

Data Store Fehlerbehebung

Beachten Sie, dass der Data Store bis zu 40 % des verfügbaren Speicherplatzes für die Wartung des Data Store reserviert. Mindestens 60 % des Gesamtspeicherplatzes stehen für den Flow-Speicher zur Verfügung.

Vertica Analytics Platform startet nicht automatisch neu, nachdem die Stromversorgung eines Data Nodes ausgefallen ist und der Knoten neu gestartet wurde

Wenn unerwartet die Stromversorgung eines Data Node ausfällt und Sie die Appliance neu starten, wird die Vertica Analytics Platform- (Vertica)-Instanz auf diesem Data Node möglicherweise nicht automatisch neu gestartet, da die Daten beschädigt sein können. Wenn noch genügend Data Nodes aktiv sind, damit der Data Store weiterlaufen kann, fährt der Data Store mit dem Erfassen der Daten von den Flow Collectors fort. Sie müssen jedoch den Data Node so schnell wie möglich neu starten, damit er sich wieder in den Data Store einfügt, fehlende Daten von benachbarten Data Nodes abruft und zum Rest der Data Nodes aufschließen kann.

Melden Sie sich in dieser Situation beim Data Node an und erzwingen Sie einen manuellen Neustart von Vertica. Dadurch werden die beschädigten Daten gelöscht und Vertica kann ordnungsgemäß neu starten.

Außerdem müssen Sie möglicherweise die Richtlinien für die Wiederherstellung der Stromversorgung des Data Node aktualisieren, bevor er neu gestartet wird. Wenn die Richtlinie zur Wiederherstellung der Stromversorgung auf „Power Off“ (Ausschalten) eingestellt ist, müssen Sie den Data Node nach einem Stromausfall manuell neu starten. Weitere Informationen zum Konfigurieren der Richtlinie für die Wiederherstellung der Stromversorgung in CIMC finden Sie im UCS C-Series GUI Configuration Guide.

Vorbereitungen

- Melden Sie sich bei der CLI des Data Node als root an.

Verfahren

1. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   tail /lancope/var/database/dbs/sw/v_sw_[node_name]_
   catalog/ErrorReport.txt
   ```

2. Ersetzen Sie *[node_name]* durch den Namen Ihres Data Node (zum Beispiel `node0001`).

3. Kopieren Sie den geänderten Befehl und fügen Sie ihn in die CLI ein. Drücken Sie dann die Eingabetaste, um die neuesten Einträge in der Fehlerdatei `ErrorReport.txt` zu überprüfen. Wenn die Fehlermeldung auf mögliche Datenkonsistenz- oder Datenbeschädigungsprobleme hinweist, fahren Sie mit dem nächsten Schritt fort, um einen Neustart von Vertica zu erzwingen.
4. Kopieren Sie den folgenden Befehl und fügen Sie ihn in einen Texteditor ein:

   ```
   admintools -t restart_node --hosts=[data-node-ip-address]
   --database='sw-datastore' --password="[dbadmin-password]"
   --force
   ```

5. Ersetzen Sie *`[data-node-ip-address]`* durch die IP-Adresse Ihres betroffenen Data Nodes.
6. Ersetzen Sie *`[dbadmin-password]`* durch Ihr Data Store-`dbadmin`-Kennwort.
7. Kopieren Sie den geänderten Befehl und fügen Sie ihn in die CLI ein. Drücken Sie dann die Eingabetaste, um einen Neustart von Vertica auf dem betroffenen Data Node zu erzwingen. Vertica löscht alle beschädigten Daten und stellt diese Daten aus benachbarten Data Nodes wieder her.
8. Wenn das System `Do you want to continue waiting? (yes/no) [yes]` (Möchten Sie weiter warten (ja/nein) [ja]) anzeigt, geben Sie `yes` (ja) ein und drücken Sie die Eingabetaste, um weiter zu warten.

   Da Vertica die Informationen des betroffenen Data Node von benachbarten Data Node wiederherstellt, kann es einige Zeit dauern, bis der betroffene Data Node wiederhergestellt ist, wenn diese Data Node eine große Menge an Flo-Datenverkehr erfasst haben, während der betroffene Data Node ausgefallen war.

Nächste Schritte

- Lesen Sie die Empfehlungen von Cisco für die Stromversorgung Ihrer Data Nodes unter Anforderungen und Überlegungen zur Data Store-Bereitstellung.

Anhang A. Vorbereitung der Installation

Installationswarnungen

Lesen Sie das Dokument Erfüllung gesetzlicher Auflagen und Sicherheitsinformationen, bevor Sie die Stealthwatch Data Store-Appliances installieren.

Beachten Sie die folgenden Warnhinweise:

Anweisung 1071 – Warnungsdefinition:

WICHTIGE SICHERHEITSHINWEISE

⚠ Dieses Warnsymbol bedeutet Gefahr. 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 1005 – Schutzschalter

⚠ 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 1004 – Installationshinweise

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

Anweisung 12 – Warnung zur Trennung 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 – Warnung zum Entfernen von Schmuck

Bevor Sie an Geräten arbeiten, die mit Stromleitungen verbunden sind, entfernen Sie Ihren Schmuck (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 – Warnung zum Tragen von Erdungsarmbändern

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 – Sicherheitskleinspannungs-Schaltkreise (SELV)

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 werden. 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 einen Elektriker.

Anweisung 1040 – Produktentsorgung

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

Anweisung 1074 – Übereinstimmung mit den 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 19 – Warnung zu TN-Stromversorgungssystemen

Das Gerät ist mit TN-Stromversorgungssystemen kompatibel.

Installationsrichtlinien

Beachten Sie die folgenden Warnhinweise:

Anweisung 1047 – Vermeidung von 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 –Hauptabschaltgerät

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

Anweisung 1005 – Schutzschalter

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 den 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 – Stromkabel und AC-Adapter

Nutzen Sie für die Installation des Produktes die bereitgestellten oder designierten Verbindungskabel/Stromkabel/AC-Adapter. 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

Im Inneren 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, medizinische Betreuung zu leisten. 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 Eingangsspannungsanforderungen 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 darüberliegenden 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.

Anhang B. Stealthwatch Installation der Hardware

In diesem Abschnitt wird die Installation Ihrer Appliances in Ihrer Umgebung beschrieben. Enthalten sind:

- **Montage Ihrer Appliance**
- **Verbinden Ihrer Appliance mit dem Netzwerk**
- **Verbinden mit Ihrer Appliance**
- **Konfigurieren der Netzwerkeinstellungen mit der erstmaligen Einrichtung**

Montage Ihrer Appliance

Sie können Stealthwatch-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 Stealthwatch-Appliances enthalten:

- Wechselstromkabel
- Zugangsschlüssel (für Frontplatte)
- Gleitschienen-Satz für die Rackmontage oder Montagelaschen für kleinere Appliances
- Für den Flow Collector 5210 ist ein 10-GB-SFP-Kabel erforderlich

Zusätzlich erforderliche Hardware

Sie müssen die folgende zusätzlich erforderliche Hardware bereitstellen:

- Befestigungsschraube für ein Standard-19“-Rack
- Unterbrechungsfreie Stromversorgung (USV) für jede Appliance, die 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

Verbinden Ihrer Appliance mit dem Netzwerk

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

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

Detaillierte Informationen zu den einzelnen Appliances finden Sie in den Stealthwatch-Datenblättern.

> ⓘ Alle Hardwarekomponenten der Cisco x2xx Serie verwenden die gleiche UCS-Plattform, UCSC-C220-M5SX. Die einzige Ausnahme ist der Flow Collector 5210 DB, der UCSC-C240-M5SX verwendet. Die Unterschiede in den Appliances liegen bei NIC-Karten, Prozessor, Arbeitsspeicher, Speicher und RAID.

> ⓘ Der Flow Collector 5210 besteht aus zwei miteinander verbundenen Servern (Engine und Datenbank), so dass sie wie eine einzige Appliance funktionieren. Dadurch unterscheidet sich die Installation leicht vom Verfahren bei anderen Appliances. Verbinden Sie sie zunächst direkt über ein 10G-SFP+-DA-Cross-Connect-Kabel. Stellen Sie anschließend eine Verbindung mit Ihrem Netzwerk her.

So verbinden Sie Ihre Appliance mit Ihrem Netzwerk:

1. Schließen Sie ein Ethernet-Kabel an den Management-Port auf der Rückseite der Appliance an.
2. Schließen Sie mindestens einen Überwachungs-Port für Flow Sensoren und UDP Directors an.

   Verbinden Sie beim UDP Director HA die beiden UDP Directors durch Crossover-

Kabel. Verbinden Sie den eth2-Port eines UDP Directors mit dem eth2-Port des zweiten UDP Directors. Verbinden Sie ebenfalls den eth3-Port jedes UDP-Directors mit einem zweiten Crossover-Kabel. Das Kabel kann aus Glasfaser oder Kupfer sein.

Notieren Sie unbedingt das Ethernet-Label (eth2, eth3 usw.) für jeden Port. Diese Bezeichnungen entsprechen den Netzwerkschnittstellen (eth2, eth3 usw.), die auf der Startseite der Verwaltungsoberfläche der Appliance angezeigt und konfiguriert werden können.

3. Verbinden Sie das jeweils andere Ende der Ethernet-Kabel mit dem Switch Ihres Netzwerks.
4. Verbinden Sie die Netzkabel mit dem Netzteil. Einige Appliances verfügen über zwei Stromanschlüsse: Netzteil 1 und Netzteil 2.

Verbinden mit Ihrer Appliance

In diesem Abschnitt wird beschrieben, wie Sie sich mit Ihrer Appliance verbinden, um die Standard-Benutzerkennwörter zu ändern.

Sie können sich auf zwei Arten mit der Appliance verbinden:

- mit Tastatur und Monitor
- mit einem Laptop (und einem Terminal-Emulator)

Bei neuen Appliances ist SSH deaktiviert. Sie müssen sich bei der Weboberfläche „Administration“ der Appliance anmelden, um es zu aktivieren.

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 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.

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. Fahren Sie fort mit dem Abschnitt **Konfigurieren der Netzwerkeinstellungen mit der erstmaligen Einrichtung**.

Verbindung mit einem Laptop herstellen

Sie können die Appliance auch mit einem Laptop mit Terminal-Emulator verbinden.

So verbinden Sie eine Appliance mit einem Laptop:

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. Übernehmen Sie die folgenden Einstellungen:

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

   Der Anmeldebildschirm und die Anmeldeaufforderung werden angezeigt.

6. Fahren Sie fort mit dem nächsten Abschnitt, **Konfigurieren der Netzwerkeinstellungen mit der erstmaligen Einrichtung**.

Konfigurieren der Netzwerkeinstellungen mit der erstmaligen Einrichtung

Nachdem Sie die Verbindung zur Appliance hergestellt haben, konfigurieren Sie die Netzwerkeinstellungen, einschließlich der IP-Adressen, mithilfe der Ersteinrichtung. Beachten Sie Folgendes:

- Wenn Sie SMC 2210 oder Flow Collector 4210 mit einem Data Store bereitstellen, können Sie zusätzlich zum Konfigurieren von IP-Adressen auch SMC oder Flow Collector für die Data Store-Verwendung und den Typ des physischen Ports, der für den `eth0`-Management-Port verwendet wird, konfigurieren.

> Nachdem Sie Ihre SMC oder Ihren Flow Collector für die Verwendung mit einem Data Store konfiguriert haben, können Sie die Konfiguration der Appliance nicht mehr aktualisieren, um diese Konfiguration zu ändern. Sie müssen RFD für die Appliance ausführen, wenn Sie die falsche Auswahl treffen. Aktivieren Sie diese Option nur, wenn Sie planen, einen Data Store in Ihrem Netzwerk bereitzustellen.

- Wenn Ihre Appliance ein Data Node ist, können Sie den Typ des physischen Ports, den sie für den `eth0`-Management-Port verwendet, und die IP-Adresse und zugehörige Informationen für den `eth2`- oder `eth2`/`eth3`--Port-Channel für die Data Node-Kommunikation konfigurieren.

Weitere Informationen zur Installation von SMC 2210, FC 4210 und Data Node-Appliances finden Sie im Hardware-Installations- und Konfigurationshandbuch für Data Store-Cluster.

Nachdem Sie die IP-Adressen und Ports konfiguriert haben, ändern Sie die Benutzerkennwörter.

> Wenn Sie die Systemkonfiguration zum ersten Mal aufrufen, wird der Ersteinrichtungsassistent gestartet und führt Sie durch die Erstkonfiguration der Appliance. Wenn Sie die Ersteinrichtung beenden, bevor Sie den Assistenten abgeschlossen haben, wird der Ersteinrichtungsassistent beim nächsten Aufruf der Systemkonfiguration erneut gestartet.

Gehen Sie abhängig von Ihrer Appliance zum folgenden Abschnitt:

- **Data Store-kompatible Appliances (SMC 2210, FC 4210)**
- **Allgemeine Konfiguration der Stealthwatch Appliance**
- **Data Node Konfiguration**

Allgemeine Konfiguration der Stealthwatch Appliance

Für alle Appliances mit Ausnahme von Data Nodes zeigt die SMC 2210- und FC 4210-Ersteinrichtung die folgende Konfiguration an:

- Konfigurieren der IP-Adresse der Appliance und der Managementinformationen

Konfigurieren der IP-Adresse der Appliance und der Managementinformationen:

Sie konfigurieren die eth0-Management-IP-Adresse Ihrer Appliance und zugehörige Informationen in der Ersteinrichtung. Für die meisten Appliances ist dies die erste Konfiguration in der Ersteinrichtung.

Vorbereitungen

- Wenn Sie einen Data Node konfigurieren, gehen Sie zu Data Node-Konfiguration.
- Wenn Sie eine Data Store-kompatible SMC oder einen Flow Collector konfigurieren, gehen Sie zu Data Store-kompatible Appliances (SMC 2210, FC 4210).
- Wenn Sie eine andere Stealthwatch-Appliance konfigurieren, beginnen Sie mit Schritt 1.

Verfahren

1. Melden Sie sich beim Systemkonfigurationsprogramm an:
   - Wenn Sie einen Data Node oder eine mit Data Store kompatible Appliance konfigurieren, geben Sie `root` ein, und drücken Sie dann die **Eingabetaste**. Wenn Sie eine andere Appliance konfigurieren, geben Sie `sysadmin` ein, und drücken Sie dann die **Eingabetaste**.

     > `Root`-Berechtigungen sind erforderlich, um die Kompatibilität mit Data Store und Data Store ordnungsgemäß zu konfigurieren.

   - Wenn die Kennwortabfrage erscheint, geben Sie **lan1cope** ein und drücken Sie dann die **Eingabetaste**.
   - Geben Sie bei der nächsten Eingabeaufforderung **SystemConfig** ein und drücken Sie dann die **Eingabetaste**.
2. Wenn Sie zum ersten Mal die Systemkonfiguration für diese Appliance aufrufen, wird die Ersteinrichtung gestartet.

   Andernfalls wird das Menü „Systemkonfiguration“ geöffnet. Wählen Sie **Management** und drücken Sie dann die **Eingabetaste**.
3. Geben Sie eine **IP-Adresse** für diese Appliance ein.
4. Geben Sie eine **Netzmaske** für das Netzwerk ein.
5. Geben Sie eine **Gateway**-Adresse für die IP-Adresse dieser Appliance ein.
6. Geben Sie eine **Broadcast**-Adresse für die Appliance ein.
7. Geben Sie einen **Hostnamen** für Ihre Appliance ein.
8. Geben Sie eine **Domäne** für Ihre Appliance ein.
9. Wählen Sie **Select** (Auswählen) und dann **Yes** (Ja) aus, um Ihre Eingaben zu bestätigen.

Dies ist die letzte Konfigurationsoption in der Ersteinrichtung. Ihre Appliance startet neu und übernimmt die Änderungen. Nach Abschluss öffnet sich die Anmmeldeseite.

Nächste Schritte

- Benutzerkennwörter ändern Weitere Informationen finden Sie unter **Ändern des Sysadmin-Benutzerkennworts**.

Data Store-kompatible Appliances (SMC 2210, FC 4210)

Für SMC 2210 und FC 4210 zeigt die Ersteinrichtung die folgende Konfiguration an:

1. Konfigurieren des physischen Management-Ports eth0
2. Konfigurieren der IP-Adresse der Appliance und der Managementinformationen
3. Konfigurieren der Data Store-Kompatibilität

Konfigurieren des physischen Management-Ports eth0

Wenn Sie eine SMC oder einen Flow Collector konfigurieren, die bzw. der mit Data Store kompatibel ist, und einen Data Store bereitstellen, können Sie `eth0` optional als SFP+-DAC-Port anstelle des standardmäßigen BASE-T-Kupfer-Ports konfigurieren. Für diese Appliances ist dies die erste Konfiguration in der Ersteinrichtung.

Vorbereitungen

- Wenn Sie einen Data Node oder eine mit Data Store kompatible SMC bzw. Flow Collector konfigurieren, finden Sie im Stealthwatch-Datenblatt für Ihre Appliance Informationen zu den unterstützten SFP+- und BASE-T-Ports.
- Wenn Sie einen Data Node konfigurieren, gehen Sie zu Data Node-Konfiguration.
- Wenn Sie neben Data Store-kompatiblen Appliances auch andere Stealthwatch-Appliances konfigurieren, lesen Sie Allgemeine Konfiguration der Stealthwatch Appliance.

Verfahren

1. Melden Sie sich beim Systemkonfigurationsprogramm an:
   - Geben Sie **root** ein, und drücken Sie die **Eingabetaste**.

     > `Root`-Berechtigungen sind erforderlich, um die Data Store-Kompatibilität richtig zu konfigurieren.

   - Wenn die Kennwortabfrage erscheint, geben Sie **lan1cope** ein und drücken Sie dann die **Eingabetaste**.
   - Geben Sie bei der nächsten Eingabeaufforderung **SystemConfig** ein und drücken Sie dann die **Eingabetaste**.
2. Wenn Sie zum ersten Mal die Systemkonfiguration für diese Appliance aufrufen, wird die Ersteinrichtung gestartet und die Konfiguration der Portreihenfolge wird angezeigt. Fahren Sie mit Schritt 5 fort.

   Andernfalls wird das Menü „Systemkonfiguration“ geöffnet. Wählen Sie **Management** und drücken Sie dann die **Eingabetaste**.
3. Wählen Sie im Menü „Systemkonfiguration“ **Network** (Netzwerk), und drücken Sie dann die **Eingabetaste**.
4. Wählen Sie **Port Order** (Portreihenfolge) aus, und drücken Sie die Eingabetaste.
5. Folgende Optionen sind hierzu verfügbar:
   - Wählen Sie **LOM** aus, um Ihre Appliance für die Verwendung eines BASE-T-Kupfer-Ports für eth0 zu konfigurieren.
   - Wählen Sie **SFP+** aus, um Ihre Appliance für die Verwendung eines SFP+-Fiber-Ports für eth0 zu konfigurieren.
6. Wählen Sie **OK**, um Ihre Auswahl zu bestätigen.

Nächste Schritte

- Konfigurieren Sie die IP-Adresse des eth0-Management-Ports und die Managementinformationen. Siehe nächstes Verfahren.

Konfigurieren der IP-Adresse der Appliance und der Managementinformationen:

Sie konfigurieren die eth0-Management-IP-Adresse Ihrer Appliance und zugehörige Informationen in der Ersteinrichtung. Bei mit Data Store kompatiblen Appliances erfolgt diese Konfiguration nach der Konfiguration des physischen Management-Ports eth0.

Vorbereitungen

- Wenn Sie eine(n) mit Data Store kompatible(n) SMC oder Flow Collector konfigurieren, zeigt der Ersteinrichtungsassistent nach der Konfiguration der Portreihenfolge die `eth0`-Managementkonfiguration an. Gehen Sie zu Schritt 3.

Verfahren

1. Melden Sie sich beim Systemkonfigurationsprogramm an:
   - Wenn Sie eine mit Data Store kompatible Appliance konfigurieren, geben Sie `root` ein, und drücken Sie dann die **Eingabetaste**.

     > `Root`-Berechtigungen sind erforderlich, um die Kompatibilität mit Data Store und Data Store ordnungsgemäß zu konfigurieren.

   - Wenn die Kennwortabfrage erscheint, geben Sie **lan1cope** ein und drücken Sie dann die **Eingabetaste**.
   - Geben Sie bei der nächsten Eingabeaufforderung **SystemConfig** ein und drücken Sie dann die **Eingabetaste**.
2. Wenn Sie zum ersten Mal die Systemkonfiguration für diese Appliance aufrufen, wird die Ersteinrichtung gestartet.

   Andernfalls wird das Menü „Systemkonfiguration“ geöffnet. Wählen Sie **Management** und drücken Sie dann die **Eingabetaste**.
3. Geben Sie eine **IP-Adresse** für diese Appliance ein.
4. Geben Sie eine **Netzmaske** für das Netzwerk ein.
5. Geben Sie eine **Gateway**-Adresse für die IP-Adresse dieser Appliance ein.
6. Geben Sie eine **Broadcast**-Adresse für die Appliance ein.
7. Geben Sie einen **Hostnamen** für Ihre Appliance ein.
8. Geben Sie eine **Domäne** für Ihre Appliance ein.
9. Wählen Sie **Select** (Auswählen) und dann **Yes** (Ja) aus, um Ihre Eingaben zu bestätigen.

Nächste Schritte

- Konfigurieren Sie die Appliance für den Betrieb ohne Data Store. Weitere Informationen finden Sie im nächsten Verfahren.

Konfigurieren der Data Store-Verwendung

Konfigurieren Sie Ihre SMC 2210 oder Ihren FC 4210 für die Zusammenarbeit mit einem

Data Store. Ihre Flow Collectors stellen eine Verbindung zum Data Store her und Ihre SMC fragt den Data Store ab.

> ⚠ Nachdem Sie Ihre SMC oder Ihren Flow Collector für die Verwendung mit einem Data Store konfiguriert haben, können Sie die Konfiguration der Appliance nicht mehr aktualisieren, um diese Konfiguration zu ändern. Sie müssen RFD für die Appliance ausführen, wenn Sie die falsche Auswahl treffen. Aktivieren Sie diese Option **nur**, wenn Sie planen, einen Data Store in Ihrem Netzwerk bereitzustellen.

> ⓘ Sie müssen alle Ihre SMCs und Flow Collectors für die Verwendung mit einem Data Store konfigurieren, wenn Sie einen Data Store bereitstellen. Es ist nicht möglich, einige Ihrer Flow Collectors so zu konfigurieren, dass sie eine Verbindung mit dem Data Store herstellen, während andere eine direkte Verbindung mit dem SMC herstellen.

Vorbereitungen

- Wenn Sie sich in der Ersteinrichtung befinden, zeigt die Systemkonfiguration die Data Store-Konfiguration an, nachdem Sie die IP-Adresse der Appliance konfiguriert haben. Fahren Sie mit Schritt 3 fort.

Verfahren

1. Im Menü „System Configuration“ (Systemkonfiguration). Wählen Sie **Advanced** (Erweitert), und drücken Sie die **Eingabetaste**.
2. Wählen Sie **Data Store** aus, und drücken Sie dann die Eingabetaste.
3. Wählen Sie **Yes** (Ja) aus, um die Kompatibilität Ihrer Appliance mit einem Data Store zu konfigurieren.

   > ⚠ Nachdem Sie Ihre SMC oder Ihren Flow Collector für die Verwendung mit einem Data Store konfiguriert haben, können Sie die Konfiguration der Appliance nicht mehr aktualisieren, um diese Konfiguration zu ändern. Sie müssen RFD für die Appliance ausführen, wenn Sie die falsche Auswahl treffen. Aktivieren Sie diese Option **nur**, wenn Sie planen, einen Data Store in Ihrem Netzwerk bereitzustellen.

4. Wählen Sie **OK**, um Ihre Auswahl zu bestätigen.

Dies ist die letzte Konfigurationsoption in der Ersteinrichtung. Ihre Appliance startet neu und übernimmt die Änderungen. Nach Abschluss öffnet sich die Anmmeldeseite.

Nächste Schritte

- Benutzerkennwörter ändern Weitere Informationen finden Sie unter **Ändern des Sysadmin-Benutzerkennworts**.

Data Node Konfiguration

Für Data Nodes zeigt die Ersteinrichtung die folgende Konfiguration an:

1. Konfigurieren des physischen Management-Ports eth0
2. Konfigurieren der IP-Adresse der Appliance und der Managementinformationen
3. Konfigurieren von eth2 und eth3 für die Inter-Data Node-Kommunikation

Konfigurieren des physischen Management-Ports eth0

Wenn Sie einen Data Node konfigurieren, können Sie `eth0` optional als BASE-T-Kupfer-Port anstelle des Standard-SFP+-DAC-Ports konfigurieren. Für diese Appliances ist dies die erste Konfiguration in der Ersteinrichtung.

Vorbereitungen

- Wenn Sie einen Data Node konfigurieren, finden Sie im Stealthwatch-Datenblatt für Ihre Appliance Informationen zu den unterstützten SFP+- und BASE-T-Ports.
- Wenn Sie eine Data Store-kompatible SMC oder einen Flow Collector konfigurieren, gehen Sie zu Data Store-kompatible Appliances (SMC 2210, FC 4210).
- Wenn Sie neben Data Store-kompatiblen Appliances auch andere Stealthwatch-Appliances konfigurieren, lesen Sie Allgemeine Konfiguration der Stealthwatch Appliance.

Verfahren

1. Melden Sie sich beim Systemkonfigurationsprogramm an:
   - Geben Sie **root** ein, und drücken Sie die **Eingabetaste**.

     > `Root`-Berechtigungen sind erforderlich, um die Data Store-Kompatibilität richtig zu konfigurieren.

   - Wenn die Kennwortabfrage erscheint, geben Sie **lan1cope** ein und drücken Sie dann die **Eingabetaste**.
   - Geben Sie bei der nächsten Eingabeaufforderung **SystemConfig** ein und drücken Sie dann die **Eingabetaste**.
2. Wenn Sie zum ersten Mal die Systemkonfiguration für diese Appliance aufrufen, wird die Ersteinrichtung gestartet und die Konfiguration der Portreihenfolge wird angezeigt. Fahren Sie mit Schritt 5 fort.

   Andernfalls wird das Menü „Systemkonfiguration“ geöffnet. Wählen Sie **Management** und drücken Sie dann die **Eingabetaste**.
3. Wählen Sie im Menü „Systemkonfiguration“ **Network** (Netzwerk), und drücken Sie dann die **Eingabetaste**.
4. Wählen Sie **Port Order** (Portreihenfolge) aus, und drücken Sie die Eingabetaste.
5. Folgende Optionen sind hierzu verfügbar:
   - Wählen Sie **SFP+** aus, um Ihre Appliance für die Verwendung eines SFP+-Fiber-Ports für eth0 zu konfigurieren.
   - Wählen Sie **LOM** aus, um Ihre Appliance für die Verwendung eines BASE-T-Kupfer-Ports für eth0 zu konfigurieren.
6. Wählen Sie **OK**, um Ihre Auswahl zu bestätigen.

Nächste Schritte

- Konfigurieren Sie die IP-Adresse des eth0-Management-Ports und die Managementinformationen. Siehe nächstes Verfahren.

Konfigurieren der IP-Adresse der Appliance und der Managementinformationen:

Sie konfigurieren die eth0-Management-IP-Adresse Ihrer Appliance und zugehörige Informationen in der Ersteinrichtung.

Vorbereitungen

- Wenn Sie einen Data Node konfigurieren, zeigt der Ersteinrichtungsassistent nach der Konfiguration der Portreihenfolge die `eth0`-Managementkonfiguration an. Gehen Sie zu Schritt 3.

Verfahren

1. Melden Sie sich beim Systemkonfigurationsprogramm an:
   - Wenn Sie einen Data Node konfigurieren, geben Sie `root` ein, und drücken Sie dann die **Eingabetaste**.

     > `Root`-Berechtigungen sind erforderlich, um die Kompatibilität mit Data Store und Data Store ordnungsgemäß zu konfigurieren.

   - Wenn die Kennwortabfrage erscheint, geben Sie **lan1cope** ein und drücken Sie dann die **Eingabetaste**.
   - Geben Sie bei der nächsten Eingabeaufforderung **SystemConfig** ein und drücken Sie dann die **Eingabetaste**.
2. Wenn Sie zum ersten Mal die Systemkonfiguration für diese Appliance aufrufen, wird die Ersteinrichtung gestartet.

   Andernfalls wird das Menü „Systemkonfiguration“ geöffnet. Wählen Sie **Management** und drücken Sie dann die **Eingabetaste**.
3. Geben Sie eine **IP-Adresse** für diese Appliance ein.
4. Geben Sie eine **Netzmaske** für das Netzwerk ein.
5. Geben Sie eine **Gateway**-Adresse für die IP-Adresse dieser Appliance ein.
6. Geben Sie eine **Broadcast**-Adresse für die Appliance ein.
7. Geben Sie einen **Hostnamen** für Ihre Appliance ein.
8. Geben Sie eine **Domäne** für Ihre Appliance ein.
9. Wählen Sie **Select** (Auswählen) und dann **Yes** (Ja) aus, um Ihre Eingaben zu bestätigen.

Nächste Schritte

- Konfigurieren Sie die Managementinformationen für den Data Node-Kommunikationsport. Weitere Informationen finden Sie unter **Konfigurieren von eth2 und eth3 für die Inter-Data Node-Kommunikation:**.

Konfigurieren von eth2 und eth3 für die Inter-Data Node-Kommunikation:

Wenn Sie eine Data Node-Appliance konfigurieren, konfigurieren Sie den Port für die Inter-Data Node-Kommunikation mit einer nicht routbaren IP-Adresse. Sie können Folgendes konfigurieren:

- `eth2`
- Port-Channel, der `eth2` und `eth3` enthält

> Sie müssen nicht routbare IP-Adressen aus dem CIDR-Block `169.254.42.0/24` zuweisen.

Vorbereitungen

- Informationen zu den `eth2`- und `eth3`-SFP+-Ports finden Sie im Stealthwatch-Datenblatt für Ihre Appliance. Beachten Sie, dass `eth2` und `eth3` davon abhängen, wie Sie `eth0` konfigurieren.
- Wenn Sie sich in der Ersteinrichtung befinden, zeigt die Systemkonfiguration die Konfiguration des `eth2`- oder `eth2/eth3`-Port-Channels an, nachdem Sie die Konfiguration der `eth0`-Managementinformationen der Appliance abgeschlossen haben. Fahren Sie mit Schritt 3 fort.

Verfahren

1. Wählen Sie im Menü „Systemkonfiguration“ **Network** (Netzwerk), und drücken Sie dann die **Eingabetaste**.
2. Wählen Sie **Node Communications** (Knotenkommunikation) aus und drücken Sie dann die Eingabetaste.
3. Wählen Sie die Port-Konfiguration für die Inter-Data Node-Kommunikation aus. Folgende Optionen sind hierzu verfügbar:
    - Wählen Sie **Yes** (Ja), um `eth2` und `eth3` als Port-Channel für die Inter-Data Node-Kommunikation zu aggregieren.
    - Wählen Sie **No** (Nein) aus, um `eth2` für die Inter-Data Node-Kommunikation zu verwenden.
4. Geben Sie eine nicht routbare **IP-Adresse** aus dem CIDR-Block `169.254.42.0/24` für `eth2`- oder den `eth2/eth3`-Port-Channel ein.
5. Geben Sie eine **Netzmaske** von `255.255.255.0` für diese IP-Adresse ein.
6. Geben Sie eine **Gateway-Adresse** für diese IP-Adresse ein.
7. Geben Sie eine **Broadcast-Adresse** für diese IP-Adresse ein.
8. Wählen Sie **Select** (Auswählen) und dann **Yes** (Ja) aus, um Ihre Eingaben zu

bestätigen.

Dies ist die letzte Konfigurationsoption in der Ersteinrichtung. Ihre Appliance startet neu und übernimmt die Änderungen. Nach Abschluss öffnet sich die Anmmeldeseite.

Nächste Schritte

- Benutzerkennwörter ändern Weitere Informationen finden Sie unter **Ändern des Sysadmin-Benutzerkennworts**.

Ändern des Sysadmin-Benutzerkennworts

Um die Sicherheit Ihres Netzwerks zu gewährleisten, ändern Sie das Standard-Sysadmin-Kennwort für Appliances.

Ändern Sie das Sysadmin-Kennwort:

Vorbereitungen

- Melden Sie sich bei der Appliance-Konsole als **sysadmin** an.
- Geben Sie „System Configuration“ (Systemkonfiguration) ein.

Verfahren

1. Wählen Sie im Menü „System Configuration“ (Systemkonfiguration) **Password** (Kennwort) und drücken Sie die **Eingabetaste**.

   Wenn Sie in den Standardeinstellungen die Liste der vertrauenswürdigen Hosts ändern, stellen Sie sicher, dass jede Stealthwatch-Appliance in der Liste der vertrauenswürdigen Hosts für jede andere Stealthwatch-Appliance in Ihrer Bereitstellung enthalten ist. Andernfalls können die Appliances nicht miteinander kommunizieren.

   Unterhalb des Menüs erscheint eine Eingabeaufforderung für das aktuelle Kennwort.

2. Geben Sie das aktuelle Kennwort ein und drücken Sie dann die **Eingabetaste**.

   Die Aufforderung zur Eingabe eines neuen Kennworts wird angezeigt.

3. Geben Sie das neue Kennwort ein und drücken Sie dann die **Eingabetaste**.

   Das Kennwort muss zwischen 8 und 30 alphanumerische Zeichen lang sein und darf keine Leerzeichen enthalten. Außerdem können Sie folgende Sonderzeichen verwenden: `$.~!@#%_=?:,{}()`

4. Geben Sie das Kennwort erneut ein und drücken Sie dann die **Eingabetaste**.

5. Wenn Ihr Kennwort akzeptiert wird, drücken Sie erneut die **Eingabetaste**, um zum Menü „Systemkonfiguration“ zurückzukehren.
6. Fahren Sie fort mit dem nächsten Abschnitt, **Ändern des Root-Benutzerkennworts**.

Ändern des Root-Benutzerkennworts

Nachdem Sie das Standard-Sysadmin-Benutzerkennwort geändert haben, ändern Sie das Standard-Root-Benutzerkennwort, um die Sicherheit Ihres Netzwerks zusätzlich zu schützen.

Ändern des Root-Benutzerkennworts:

Vorbereitungen

- Melden Sie sich bei der Appliance-Konsole als **sysadmin** an.
- Geben Sie „System Configuration“ (Systemkonfiguration) ein.

Verfahren

1. Navigieren Sie zur Root-Shell.
2. Wählen Sie im Menü „System Configuration“ (Systemkonfiguration) **Advanced** (Erweitert) und drücken Sie dann die **Eingabetaste**. Das Menü „Advanced“ (Erweitert) wird angezeigt.
3. Wählen Sie **RootShell** und drücken Sie dann die **Eingabetaste**.

   Es erscheint eine Eingabeaufforderung für das Root-Kennwort.
4. Geben Sie das aktuelle Root-Kennwort ein, und drücken Sie dann die **Eingabetaste**. Die Eingabeaufforderung für die Root-Shell wird angezeigt.
5. Geben Sie **SystemConfig** ein und drücken Sie die **Eingabetaste**.

   Dadurch kehren Sie zum Menü „Systemkonfiguration“ zurück, damit Sie das Root-Kennwort ändern können.
6. Wählen Sie **Password** (Kennwort) und drücken Sie dann die **Eingabetaste**. Die Kennwortabfrage erscheint unterhalb des Menüs.
7. Geben Sie das neue Root-Kennwort ein und drücken Sie dann die **Eingabetaste**. Es erscheint eine zweite Eingabeaufforderung.
8. Geben Sie das neue Root-Kennwort erneut ein und drücken Sie dann die **Eingabetaste**.

9. Wenn Ihre Kennwortänderung erfolgreich war, drücken Sie die **Eingabetaste**. Sie haben nun sowohl Ihr Standard-Sysadmin- als auch Ihr Root-Kennwort geändert. Dadurch kehren Sie zum Konsolenmenü „Systemkonfiguration“ zurück.
10. Wählen Sie **Cancel** (Abbrechen) und drücken Sie die **Eingabetaste**. Die Konsole „Systemkonfiguration“ wird geschlossen und die Root-Shell-Eingabeaufforderung wird angezeigt.
11. Geben Sie **exit** ein und drücken Sie die **Eingabetaste**. Die Anmeldeaufforderung wird angezeigt.
12. Drücken Sie **Strg+Alt**, um die Konsolenumgebung zu verlassen.

Sie sind nun bereit, Ihre Appliance zu konfigurieren. Informationen zur Konfiguration Ihrer Appliance finden Sie im entsprechenden **Stealthwatch-Handbuch für die Systemkonfiguration** für Ihre Softwareversion. Die x2xx Serie ist kompatibel mit den Stealthwatch-Softwareversionen 7.x.

Anhang C. Konfigurieren Ihrer Appliances

Wenn Sie sich zum ersten Mal bei der Appliance anmelden, verwenden Sie das Appliance Setup Tool, um Ihre Appliance-Einstellungen zu konfigurieren.

Appliance Setup Tool-Anforderungen

- Bestätigen Sie, dass Ihre Firewalls und ACLs (Access Control List) den Zugriff erlauben.
- Erfassen Sie den Hostnamen für die Appliance und die IP-Adressen für Folgendes:
    - Appliance
    - Subnetzmaske
    - Standard- und Broadcast-Gateways
    - NTP- und DNS-Server
    - IP-Adresse der SMC für Central Management

Verwaltet

Als Teil des Appliance-Setup-Tools konfigurieren Sie Ihre Appliance so, dass sie von Ihrer primären Stealthwatch Management Console (SMC) verwaltet wird.

Wenn Ihre Appliances von Ihrer Stealthwatch Management Console (SMC) verwaltet werden, können Sie Central Management nutzen, um Appliance-Konfigurationen zu bearbeiten, Software zu aktualisieren, neu zu starten, herunterzufahren und vieles mehr.

SMC-Failover

Wenn Sie mehr als eine Stealthwatch Management Console (SMC) haben, können Sie ein SMC-Failover-Paar einrichten, so dass eine der beiden Konsolen als Backup-Konsole für die andere dient.

- Verwenden Sie das Appliance Setup Tool, um jede einzelne SMC zu konfigurieren.
- Planen Sie, welche SMC primär und welche sekundär sein wird.
- Nachdem Sie jede einzelne SMC eingerichtet haben, verwenden Sie den Truststore von Central Management und den Stealthwatch Desktop Client, um die SMC-Failover-Beziehung zu konfigurieren.

Best Practices

Um Ihr System erfolgreich zu konfigurieren, stellen Sie sicher, dass Sie die Anweisungen in diesem Handbuch befolgen.

Wir empfehlen Folgendes:

- **One at a Time:** Konfigurieren Sie jeweils eine Appliance einzeln. Bestätigen Sie, dass die Appliance **Up** (aktiv) ist, bevor Sie mit der Konfiguration der nächsten Appliance in Ihrem Cluster beginnen.
- **Reihenfolge:** Beachten Sie die Konfigurationsreihenfolge.
- **Mehrere Central Manager:** Sie können mehr als einen Central Manager in Ihrem System konfigurieren. Jede Appliance kann jedoch nur von einer primären SMC/einem Central Manager verwaltet werden.
- **Zugriff:** Sie benötigen Administratorrechte für den Zugriff auf Central Management.

Konfigurationsreihenfolge

Konfigurieren Sie Ihre Appliances in der folgenden Reihenfolge und notieren Sie die Details für jede Appliance:

Reihenfolge	Appliance	Details
1.	Primäre SMC	Ihre primäre SMC ist Ihr Central Manager. Stellen Sie sicher, dass die SMC als „Up“ (aktiv) angezeigt wird, bevor Sie mit der Konfiguration der nächsten Appliance im System beginnen.
2.	UDP Directors (auch als FlowReplicators bezeichnet)	
3.	Data Nodes	
4.	Datenbank der Flow Collector 5000-Serie	Stellen Sie sicher, dass die Datenbank der Flow Collector 5000-Serie als „Up“ (aktiv) angezeigt wird,

		bevor Sie mit der Konfiguration der Engine beginnen.
5.	Engine der Flow Collector 5000-Serie	Stellen Sie sicher, dass die Datenbank der Flow Collector 5000-Serie als „Up“ (aktiv) angezeigt wird, bevor Sie mit der Konfiguration der Engine beginnen.
6.	Alle anderen Flow Collectors (NetFlow und sFlow)	
7.	Flow Sensors	Stellen Sie sicher, dass Ihr Flow Collector als „Up“ (aktiv) angezeigt wird, bevor Sie mit der Konfiguration des Flow Sensor beginnen.
8.	Endpoint Concentrator	
9.	Sekundäre SMC (falls verwendet)	Stellen Sie sicher, dass die primäre SMC als „Up“ (aktiv) angezeigt wird, bevor Sie mit der Konfiguration der sekundären SMC beginnen. Die sekundäre SMC wählt sich selbst als Central Manager aus. Konfigurieren Sie das Failover, nachdem alle Appliances konfiguriert sind.

Ihr System verfügt möglicherweise nicht über alle hier gezeigten Appliances.

1. Anmelden

Verwenden Sie die folgenden Anweisungen, um jede Appliance mit dem Appliance Setup Tool zu konfigurieren.

1. Geben Sie in das Adressfeld Ihres Browsers **https://** gefolgt von der IP-Adresse der Appliance ein.

- **Primäre SMC:** Konfigurieren Sie zuerst die primäre SMC.
- **Up:** Bestätigen Sie, dass jede Appliance aktiv ist, bevor Sie mit der Konfiguration der nächsten Appliance in Ihrem Cluster beginnen.
- **Reihenfolge:** Stellen Sie sicher, dass Sie Ihre Appliances in der richtigen Reihenfolge konfigurieren, damit sie korrekt kommunizieren.

2. Geben Sie die folgenden Anmeldedaten ein:

   - **Benutzername:** admin
   - **Kennwort:** lan411cope

2. Konfigurieren der Appliance

Wenn Sie sich zum ersten Mal bei der Appliance anmelden, führt Sie das Appliance Setup Tool durch jeden Konfigurationsschritt.

1. **Standardkennwort ändern:** Geben Sie neue Kennwörter für admin, root und sysadmin ein. Klicken Sie auf **Next** (Weiter), um zu jedem Benutzer zu blättern.

   Verwenden Sie folgende Kriterien:

   - **Länge:** 8 bis 30 Zeichen
   - **Ändern:** Stellen Sie sicher, dass sich das neue Kennwort um mindestens 4 Zeichen vom Standardkennwort unterscheidet.

Benutzer	Standardkennwort
Administrator	lan411cope
root	lan1cope
sysadmin	lan1cope

Die sysadmin- und root-Menüs sind nicht verfügbar, wenn Sie die Standardkennwörter bereits bei der Hardwareinstallation geändert haben. Einzelheiten finden Sie im Hardware-Installationshandbuch zur Stealthwatch x210-Serie.

2. **Management-Netzwerk Schnittstelle:** Überprüfen Sie die Felder „IP address“ (IP-Adresse) und „network interface“ (Netzwerkschnittstelle). Vergewissern Sie sich, dass die Standardeinstellungen korrekt sind. Klicken Sie auf **Next** (Weiter).

    - **Änderungen:** Um diese Informationen zu ändern, wenden Sie sich an Ihren Netzwerkadministrator und lesen Sie den Abschnitt zur Fehlerbehebung.
    - **IPv6 (optional):** Um IPv6 zu aktivieren, klicken Sie auf **IPv6**. Aktivieren Sie das Kontrollkästchen **Enable IPv6** (IPv6 aktivieren) und füllen Sie die Felder aus.

3. **Hostname und Domänen:** Geben Sie den Hostnamen und den Netzwerkdomänennamen ein. Klicken Sie auf **Next** (Weiter).

    - **Hostname:** Für jede Appliance ist ein eindeutiger Hostname erforderlich. Wenn Sie mehreren Appliances denselben Hostnamen zuweisen, werden sie nicht erfolgreich installiert.
    - **Netzwerkdomäne:** Für jede Appliance ist ein vollständig qualifizierter Domänenname erforderlich.
    - **Stealthwatch-Domäne (nur SMC):** Geben Sie eine Stealthwatch-Domäne für Ihre Stealthwatch-Appliances ein.
    - **IP-Adressbereiche (nur SMC):** Wählen Sie den IP-Adressbereich für Ihr Stealthwatch-Netzwerk aus.

4. **DNS-Einstellungen**: Bestätigen Sie, dass die Standardeinstellung korrekt ist, oder geben Sie die IP-Adresse Ihres Domänenservers ein. Klicken Sie auf **Next** (Weiter).

    Hinzufügen oder Löschen von DNS-Servern (optional):

    - **Hinzufügen:** Klicken Sie auf das +-Symbol.
    - **Löschen:** Klicken Sie auf das Kontrollkästchen, um den DNS-Server auszuwählen. Klicken Sie auf das −-Symbol.

5. **NTP-Einstellungen:** Bestätigen Sie, dass die Standardeinstellung korrekt ist, oder klicken Sie auf das Symbol **Menu** (Menu), um Ihren NTP-Server (Network Time Protocol) auszuwählen. Klicken Sie auf **Next** (Weiter).

    - **Mehrere NTP-Server:** Wir empfehlen, mehrere NTP-Server einzurichten,

um Redundanz und Genauigkeit zu gewährleisten.

- **Öffentliche Quelle:** pool.ntp.org ist eine gute öffentliche Quelle für NTP.

Hinzufügen oder Löschen von NTP-Servern (optional):

- **Hinzufügen:** Klicken Sie auf das +-Symbol.
- **Löschen:** Klicken Sie auf das Kontrollkästchen, um den NTP-Server auszuwählen. Klicken Sie auf das −-Symbol.

6. Wenn die Appliance eine SMC ist, gehen Sie zu **3. Registrierung der Stealthwatch Management Console**.

   Wenn die Appliance keine SMC ist, gehen Sie zu **4. Hinzufügen von Appliances zu Central Management**.

3. Registrierung der Stealthwatch Management Console

1. **Überprüfen Sie Ihre Einstellungen**: Bestätigen Sie, dass die Appliance-Informationen korrekt sind.
2. Klicken Sie auf **Apply** (Übernehmen) oder **Restart and Proceed** (Neu starten und fortfahren).

   Befolgen Sie die Anweisungen auf dem Bildschirm, während die Appliance neu startet.

   Warten Sie ein paar Minuten, bis die neuen Systemeinstellungen wirksam werden. Möglicherweise müssen Sie die Seite aktualisieren.

3. Melden Sie sich bei der Stealthwatch Management Console an.
4. Das Appliance Setup Tool öffnet sich erneut. Klicken Sie auf **Continue** (Weiter).
5. Überprüfen Sie auf der Registerkarte „Register Your Appliance“ (Ihre Appliance registrieren) die IP-Adresse und klicken Sie auf **Save** (Speichern).

   - Dadurch wird Central Management auf der Stealthwatch Management Console installiert.

   - Die IP-Adresse der SMC wird automatisch erkannt und kann nicht geändert werden.

6. Wenn die Einrichtung der Appliance abgeschlossen ist, klicken Sie auf **Go to Dashboard** (Zum Dashboard).
7. Klicken Sie auf das Symbol **Global Settings** (Globale Einstellungen). Wählen Sie **Central Management** (Zentrales Management).
8. Überprüfen Sie den Bestand. Bestätigen Sie, dass der Status der SMC-Appliance als **Up** (aktiv) angezeigt wird.

> ⚠ Vergewissern Sie sich, dass die primäre SMC und jede Appliance als „Up“ angezeigt wird, bevor Sie mit der Konfiguration der nächsten Appliance in Ihrem Cluster unter Verwendung der -Konfigurationsreihenfolge und -details beginnen.

9. Stellen Sie Ihren Data Store bereit und konfigurieren Sie ihn. Kehren Sie zum Stealthwatch Data Store-Bereitstellungsüberblickzurück, um den Bereitstellungsprozess zu überprüfen.

4. Hinzufügen von Appliances zu Central Management

Das Appliance Setup Tool führt Sie weiter durch die Appliance-Konfiguration mit Central Management. Einige Schritte können je nach Appliance abweichen. Befolgen Sie die Anweisungen auf dem Bildschirm.

1. Geben Sie auf der Registerkarte „Central Management“ (Zentrales Management) die IP-Adresse Ihrer primären SMC ein.

   Ihre primäre SMC ist Ihr Central Manager.

2. Klicken Sie auf **Save** (Speichern).
3. Befolgen Sie die Anweisungen auf dem Bildschirm, um dem Identitätszertifikat der primären SMC-Appliance zu vertrauen. Klicken Sie auf **Yes** (Ja), um dem Zertifikat zu vertrauen und der Appliance die Kommunikation mit der SMC zu ermöglichen.
4. Geben Sie die Anmeldedaten für Ihre primäre SMC ein.
5. Wählen Sie Ihre Stealthwatch-Domäne aus.

   - **Flow Collectors:** Geben Sie die Flow Collection-Port-Nummer ein.

     Netflow-Standard: 2055

     sFlow-Standard: 6343

- **Flow Sensors:** Wählen Sie einen Flow Collector aus.

6. Klicken Sie auf **Go to Central Management** (Zum zentralen Management). Gehen Sie zu **5. Bestätigen des Appliance-Status**.

5. Bestätigen des Appliance-Status

Nachdem Sie eine Appliance im Appliance Setup Tool konfiguriert haben, bestätigen Sie den Status der Appliance in Central Management.

1. Das Appliance Setup Tool öffnet sich im Inventar von Central Management, oder Sie können es wie folgt öffnen:

   - Melden Sie sich bei Ihrer primären Stealthwatch Management Console an.
   - Klicken Sie auf das Symbol **Global Settings** (Globale Einstellungen).
   - Wählen Sie **Central Management** (Zentrales Management).

2. Überprüfen Sie die Appliances in der Appliance Manager-Bestandsliste.

   - Vergewissern Sie sich, dass die Appliance im Inventar angezeigt wird.
   - Vergewissern Sie sich, dass als Status der Appliance „Up“ (aktiv) angezeigt wird.

> ⚠ Vergewissern Sie sich, dass die primäre SMC und jede Appliance als „Up“ angezeigt wird, bevor Sie mit der Konfiguration der nächsten Appliance in Ihrem Cluster unter Verwendung der -Konfigurationsreihenfolge und -details beginnen.

3. Um die nächste Appliance in Ihrem System zu konfigurieren, gehen Sie zu **1. Anmelden** und führen Sie die Vorgänge bis **5. Bestätigen des Appliance-Status** durch.

   Wenn keine weitere Appliance mehr eingerichtet werden muss, finden Sie im Stealthwatch-Systemkonfigurationshandbuch weitere Informationen zum Abschluss der Appliance-Konfigurationen. Alternativ können Sie zum Stealthwatch Data Store-Bereitstellungsüberblick zurückkehren, um den Bereitstellungsprozess zu überprüfen.

Copyright-Informationen