Erste Schritte

Converged Systems Advisor

NetApp
May 23, 2023

This PDF was generated from https://docs.netapp.com/de-de/converged-systems-advisor/task_quick_start.html on May 23, 2023. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

Erste Schritte

Schnellstart für Converged Systems Advisor

Erste Schritte mit dem Agenten des Converged Systems Advisor und dem Portal für FlexPod

1 Bereiten Sie Ihre Umgebung vor

Überprüfen Sie die Unterstützung Ihrer Konfiguration. "Bereiten Sie Ihre Umgebung vor".

2 Erstellen von Konten auf FlexPod-Geräten

Konten einrichten, die im Cisco UCS Manager, auf Cisco Nexus Switches, für Ihre ONTAP Systeme, für VMware und im APIC eingerichtet werden. Diese Konten werden vom Agenten zum Erfassen von Konfigurationsdaten verwendet."Erstellen von Konten auf FlexPod-Geräten".

3 Gewähren Sie CSA-Benutzerberechtigungen über einen TACACS+-Server

Wenn Sie einen TACACS+-Server verwenden, müssen Sie den CSA-Benutzerberechtigungen für Ihre Switches gewähren, eine Benutzerberechtigungsgruppe erstellen und der Gruppe Zugriff auf die spezifischen von CSA benötigten Setup-Befehle gewähren."Gewähren Sie CSA-Benutzerberechtigungen über einen TACACS+-Server"

4 Einrichten und Bereitstellen des Agenten

Implementieren Sie den Converged Systems Advisor-Agent auf einem VMware ESXi-Server. Der Agent erfasst Konfigurationsdaten zu jedem Gerät in Ihrer konvergenten FlexPod Infrastruktur und sendet diese Daten an das Converged Systems Advisor Portal."Agenten bereitstellen".

5 Hinzufügen/Teilen der Infrastruktur im Portal

Fügen Sie jedes FlexPod Gerät zum Converged Systems Advisor Portal hinzu, um eine komplette Infrastruktur zu erstellen, die Sie überwachen können. Außerdem können Sie eine konvergente Infrastruktur gemeinsam nutzen, um sich andere Personen bei dem Portal anzumelden und so die Konfiguration anzuzeigen und zu überwachen."Fügen Sie im Portal Infrastruktur hinzu und teilen Sie sie".

6 Konfigurieren Sie Benachrichtigungen

Mit einer Premium-Lizenz können Sie Benachrichtigungen einrichten, die Sie über E-Mail-Benachrichtigungen bei Änderungen an Ihrer FlexPod-Infrastruktur benachrichtigen."Konfigurieren Sie Benachrichtigungen"

7 Setzen Sie eine statische IP-Adresse

Wenn in Ihrer Umgebung kein DHCP-Server vorhanden ist, können Sie eine statische IP-Adresse auf dem Converged Systems Advisor Agent festlegen."Legen Sie eine statische IP-Adresse für den Agenten fest"

Bereiten Sie Ihre Umgebung vor

Für den Einstieg in Converged Systems Advisor ist die Vorbereitung der Umgebung erforderlich. Bevor Ihre Umgebung vorbereitet wird, umfasst die Überprüfung des Supports für Ihre Konfiguration und die Registrierung für ein NetApp Support Site Konto.

Vielleicht möchten Sie es "Converged Systems Advisor funktioniert" Bevor Sie beginnen.

Schritte

1. Überprüfen Sie die Unterstützung im "NetApp Interoperabilitäts-Matrix-Tool":
   a. Vergewissern Sie sich, dass Converged Systems Advisor Ihre konvergente FlexPod Infrastruktur unterstützt.
   b. Stellen Sie sicher, dass Sie über einen unterstützten VMware ESXi-Server für den Converged Systems Advisor-Agenten verfügen.

      Um die Bandbreitenauslastung zu minimieren, empfiehlt NetApp, den Agenten im selben Datacenter zu installieren, wie die konvergente FlexPod Infrastruktur.

2. Stellen Sie sicher, dass das Netzwerk, in dem Sie den Agenten installieren, die Verbindung zwischen den Komponenten zulässt:
   - Der Agent muss mit jeder FlexPod Komponente verbunden sein, damit er Konfigurationsdaten erfassen kann.
   - Der Agent benötigt außerdem eine ausgehende Internetverbindung, um mit den folgenden Endpunkten zu kommunizieren:
     - csa.netapp.com
     - docker.com
     - docker.io
3. Wechseln Sie zum "NetApp Support Website" Und registrieren Sie sich für ein Konto, wenn Sie nicht haben ein.

   Um den Agenten zu konfigurieren und auf das Portal zuzugreifen, ist ein NetApp Support Site Konto erforderlich.

Erstellen von Konten für FlexPod-Geräte

Richten Sie zum Einstieg Konten für FlexPod-Geräte ein:

- Erstellen eines schreibgeschützten Kontos für Cisco UCS Manager
- Erstellen eines schreibgeschützten Kontos für Nexus Switches
- Erstellen eines Administratorkontos für ONTAP

- Erstellen Sie ein schreibgeschütztes Konto für VMware
- Erstellen Sie ein schreibgeschütztes Konto im APIC
- Gewähren Sie CSA-Benutzerberechtigungen über einen TACACS+-Server

Der Agent verwendet diese Konten, um Konfigurationsinformationen von jedem Gerät zu erfassen.

Erstellen eines schreibgeschützten Kontos für Cisco UCS Manager

Schritte

1. Melden Sie sich bei Cisco UCS Manager an.
2. Erstellen Sie einen lokal authentifizierten Benutzer namens *csa-Readonly*.

Alle neuen Benutzer sind standardmäßig schreibgeschützt.

Erstellen eines schreibgeschützten Kontos für Nexus Switches

Schritte

1. Melden Sie sich über SSH oder Telnet bei jedem Nexus Switch an.
2. Globalen Konfigurationsmodus aufrufen:

```
 configure terminal
.. Create a new user:
```

```
 username [name] password [password] role network-operator
.. Save the configuration:
```

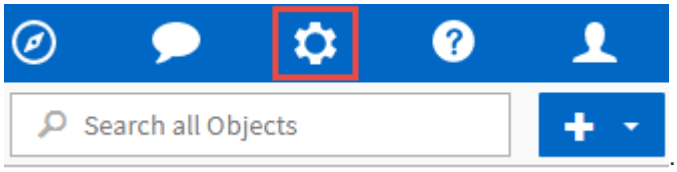
```
copy running configuration startup configuration
```

Wenn Sie einen TACACS+-Server verwenden und CSA-Benutzerrechte erteilen müssen, gehen Sie zu "Gewähren von CSA-Benutzerberechtigungen über einen TACACS+-Server".

Erstellen eines Administratorkontos für ONTAP

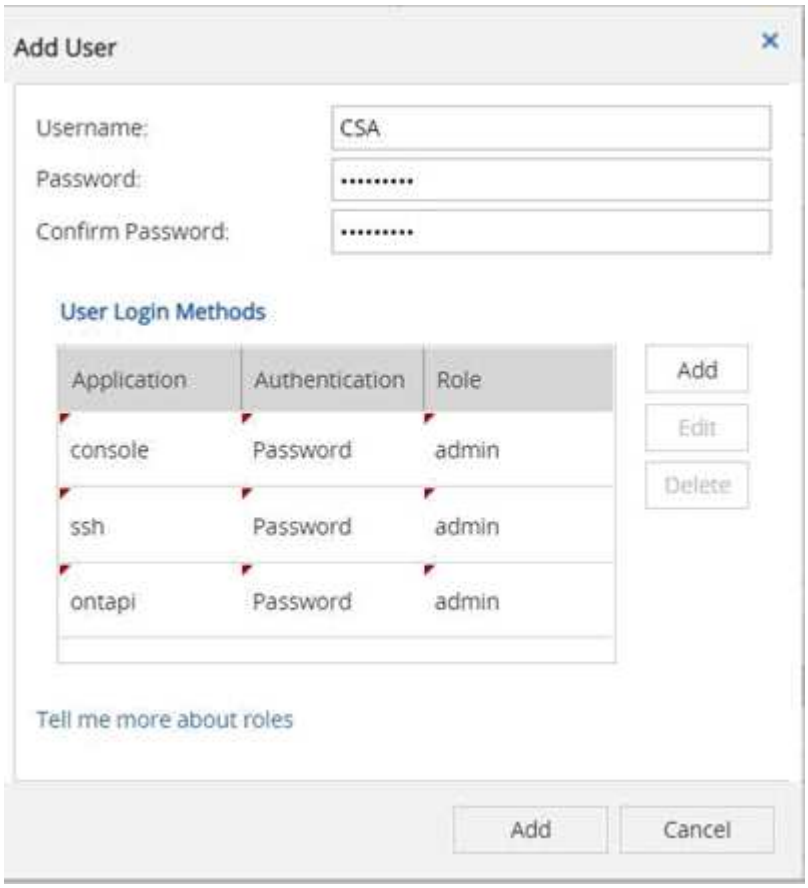
Schritte

1. Melden Sie sich bei OnCommand System Manager an und klicken Sie auf das Symbol für die Einstellungen:



2. Klicken Sie auf der Seite Benutzer auf **Hinzufügen**.

3. Geben Sie einen Benutzernamen und ein Passwort ein und fügen Sie **ssh**, **ontapi** und **Konsole** als Benutzeranmeldungsmethoden mit Admin-Zugriff hinzu.



Erstellen Sie ein schreibgeschütztes Konto für VMware

Schritte

1. Melden Sie sich bei vCenter an.
2. Wählen Sie im vCenter Menü die Option **Administration**.
3. Wählen Sie unter Rollen **schreibgeschützt**.
4. Klicken Sie auf das Symbol für **Rollenaktion klonen** und ändern Sie den Namen in **CSA**.
5. Wählen Sie die neu erstellte * CSA*-Rolle aus.
6. Klicken Sie auf das Symbol * Rolle bearbeiten*.
7. Wählen Sie unter **Rolle bearbeiten Global** und dann **Lizenzen**.
8. Wählen Sie in der Seitenleiste **Single Sign On→Users and groups→Create a New user**.
9. Benennen Sie den neuen Benutzer **CSARO** unter DOMAIN vpshere.local.
10. Wählen Sie in der Seitenleiste unter **Zugangskontrolle** die Option **Globale Berechtigungen** aus.
11. Wählen Sie den Benutzer **CSARO** und weisen SIE DIE ROLLE **CSA** zu.
12. Melden Sie sich beim Web Client an.

    Benutzerkennung: **CSARO@vsphere.local** und zuvor erstelltes Passwort.

Erstellen Sie ein schreibgeschütztes Konto im APIC

Schritte

1. Klicken Sie Auf **Admin**.
2. Klicken Sie auf **Neue lokale Benutzer erstellen**.
3. Geben Sie unter **User Identity** die Benutzerinformationen ein.
4. Wählen Sie unter **Sicherheit** alle Optionen für die Sicherheitsdomain aus.
5. Klicken Sie auf **+**, um bei Bedarf Benutzerzertifikate und SSH-Schlüssel hinzuzufügen.
6. Klicken Sie Auf **Weiter**.
7. Klicken Sie auf **+**, um Rollen für Ihre Domain hinzuzufügen.
8. Wählen Sie im Dropdown-Menü den Namen der **Rolle** aus.
9. Wählen Sie **Lesen** für den Rollentyp *.
10. Klicken Sie Auf **Fertig Stellen**.

Gewähren Sie CSA-Benutzerberechtigungen über einen TACACS+-Server

Wenn Sie einen TACACS+-Server verwenden und CSA-Benutzerberechtigungen für Ihre Switches gewähren müssen, sollten Sie eine Benutzerberechtigungsgruppe erstellen und der Gruppe Zugriff auf die spezifischen Setup-Befehle gewähren, die von CSA benötigt werden.

Die folgenden Befehle sollten in die Konfigurationsdatei Ihres TACACS+ Servers geschrieben werden.

Schritte

1. Geben Sie die folgende ein, um eine Benutzerberechtigungsgruppe mit schreibgeschütztem Zugriff zu erstellen:

```
group=group_name {
  default service=deny
  service=exec{
    priv-lvl=0
  }
}
```

1. Geben Sie Folgendes ein, um den Zugriff auf die von CSA benötigten Befehle zu gewähren:

```
cmd=show {
  permit "environment"
  permit "version"
  permit "feature"
  permit "feature-set"
  permit hardware.*
  permit "interface"
  permit "interface"
  permit "interface transceiver"
  permit "inventory"
  permit "license"
  permit "module"
  permit "port-channel database"
  permit "ntp peers"
  permit "license usage"
  permit "port-channel summary"
  permit "running-config"
  permit "startup-config"
  permit "running-config diff"
  permit "switchname"
  permit "int mgmt0"
  permit "cdp neighbors detail"
  permit "vlan"
  permit "vpc"
  permit "vpc peer-keepalive"
  permit "mac address-table"
  permit "lacp port-channel"
  permit "policy-map"
  permit "policy-map system type qos"
  permit "policy-map system type queuing"
  permit "policy-map system type network-qos"
  permit "zoneset active"
  permit "san-port-channel summary"
  permit "flogi database"
  permit "fcns database detail"
  permit "fcns database detail"
  permit "zoneset active"
  permit "vsan"
  permit "vsan usage"
  permit "vsan membership"
  }
```

1. Geben Sie Folgendes ein, um Ihr CSA-Benutzerkonto der neu erstellten Gruppe hinzuzufügen:

```
user=user_account{
  member=group_name
  login=file/etc/passwd
}
```

Richten Sie den Agenten ein und stellen Sie diesen bereit

Sie müssen den Converged Systems Advisor-Agent auf einem VMware ESXi-Server bereitstellen. Der Agent erfasst Konfigurationsdaten zu jedem Gerät in Ihrer konvergenten FlexPod Infrastruktur und sendet diese Daten an das Converged Systems Advisor Portal.

Schritte

1. Laden Sie den Agent herunter und installieren Sie ihn
2. Richten Sie das Netzwerk für den Agenten ein
3. Installieren Sie ein SSL-Zertifikat auf dem Agenten
4. Konfigurieren Sie den Agent für die Erkennung Ihrer FlexPod Infrastruktur

Laden Sie den Agent herunter und installieren Sie ihn

Sie müssen den Converged Systems Advisor-Agent auf einem VMware ESXi-Server bereitstellen.

Über diese Aufgabe

Um die Bandbreitenauslastung zu minimieren, sollten Sie den Agenten auf einem VMware ESXi Server installieren, der sich im selben Rechenzentrum wie die FlexPod-Konfiguration befindet. Der Agent muss über eine Verbindung zu jeder FlexPod-Komponente und dem Internet verfügen, damit er Konfigurationsdaten über HTTPS-Port 443 an das Converged Systems Advisor-Portal senden kann.

Der Agent wird als virtuelle VMware vSphere-Maschine aus einer OVF-Vorlage (Open Virtualization Format) bereitgestellt. Die Vorlage ist Debian-basiert mit 1 vCPU und 2 GB RAM (mehr kann für mehrere oder größere FlexPod-Systeme erforderlich sein).

Schritte

1. Laden Sie den Agent herunter:
   a. Melden Sie sich bei an "Converged Systems Advisor-Portal".
   b. Klicken Sie Auf **Download Agent**.
2. Installieren Sie den Agent, indem Sie die OVF-Vorlage auf dem VMware ESXi-Server bereitstellen.

   Bei einigen Versionen von VMware erhalten Sie möglicherweise eine Warnung bei der Bereitstellung der OVF-Vorlage. Die Virtual Machine wurde auf der aktuellen Version von vCenter entwickelt, mit Hardwarekompatibilität für ältere Versionen. Dies könnte zu der Warnung führen. Sie sollten die Konfigurationsoptionen überprüfen, bevor Sie die Warnung bestätigen und dann mit der Installation fortfahren.

Richten Sie das Netzwerk für den Agenten ein

Sie müssen sicherstellen, dass Netzwerke auf der virtuellen Agent-Maschine korrekt eingerichtet sind, um die Kommunikation zwischen den Agenten- und FlexPod-Geräten und zwischen dem Agenten und mehreren Internet-Endpunkten zu ermöglichen. Beachten Sie, dass der Netzwerk-Stack auf der virtuellen Maschine deaktiviert ist, bis das System initialisiert wird.

Schritte

1. Stellen Sie sicher, dass eine ausgehende Internetverbindung den Zugriff auf die folgenden Endpunkte ermöglicht:
   - csa.netapp.com
   - docker.com
   - docker.io
2. Melden Sie sich über den VMware vSphere Client bei der Konsole der virtuellen Maschine des Agenten an.

   Der Standardbenutzername ist `csa` Und das Standardpasswort lautet `netapp`.

   Aus Sicherheitsgründen ist SSHD standardmäßig deaktiviert.
3. Wenn Sie dazu aufgefordert werden, ändern Sie das Standardpasswort und notieren Sie sich das Kennwort, da es nicht wiederhergestellt werden kann.

   Nachdem Sie das Passwort geändert haben, startet das System neu und startet die Agent-Software.
4. Wenn DHCP im Subnetz nicht verfügbar ist, konfigurieren Sie eine statische IP-Adresse und DNS-Einstellungen unter Verwendung von Standard-Debian-Tools und starten Sie dann den Agenten neu.

   "Detaillierte Anweisungen finden Sie hier".

   Die Netzwerkkonfiguration für die virtuelle Debian-Maschine ist standardmäßig auf DHCP eingestellt. NetworkManager ist installiert und stellt eine Text-Benutzeroberfläche zur Verfügung, die Sie über den Befehl nmtui starten können (siehe "Man-Page" Entnehmen).

   Weitere Hilfe zu Netzwerken finden Sie unter "Die Netzwerkkonfigurationsseite im Debian-Wiki".
5. Wenn Ihre Sicherheitsrichtlinien vorschreiben, dass sich der Agent in einem Netzwerk befinden muss, um mit FlexPod-Geräten und einem anderen Netzwerk zu kommunizieren, fügen Sie eine zweite Netzwerkschnittstelle in vCenter hinzu und konfigurieren Sie die richtigen VLANs und IP-Adressen.
6. Wenn ein Proxyserver für den Internetzugriff benötigt wird, führen Sie den folgenden Befehl aus:

   ```
   sudo csa_set_proxy
   ```

   Der Befehl generiert zwei Eingabeaufforderungen und zeigt das erforderliche Format für den Proxy-Eintrag an. Die erste Eingabeaufforderung ermöglicht Ihnen, einen HTTP-Proxy anzugeben, während die zweite Ihnen die Angabe eines HTTPS-Proxys ermöglicht.

   Geben Sie unten den HTTP-Proxy ein und verwenden Sie das Format:
   `http://user:password@proxy-server:proxy-port`

   Lassen Sie das Feld leer, wenn für den Internetzugang kein HTTP-Proxy erforderlich ist.

7. Warten Sie nach dem Einrichten des Netzwerks etwa 5 Minuten, bis das System aktualisiert und gestartet wurde.

   Wenn der Agent betriebsbereit ist, wird auf der Konsole eine Broadcast-Meldung angezeigt.

8. Überprüfen Sie die Verbindung, indem Sie den folgenden CLI-Befehl über den Agenten ausführen:

   ```
   curl -k https://www.netapp.com/us/index.aspx
   ```

   Wenn der Befehl fehlschlägt, überprüfen Sie die DNS-Einstellungen. Die virtuelle Agent-Maschine muss über eine gültige DNS-Konfiguration und die Fähigkeit verfügen, csa.netapp.com zu erreichen.

Installieren Sie ein SSL-Zertifikat auf dem Agenten

Optional: Installieren Sie bei Bedarf ein SSL-Zertifikat auf dem Agent.

Der Agent erstellt ein selbstsigniertes Zertifikat, wenn die virtuelle Maschine zum ersten Mal gestartet wird. Falls erforderlich, können Sie dieses Zertifikat löschen und Ihr eigenes SSL-Zertifikat verwenden.

Über diese Aufgabe

Converged Systems Advisor unterstützt folgende: * Alle mit OpenSSL Version 1.0.1 oder höher * TLS 1.1 und TLS 1.2 kompatiblen Chiffren

Schritte

1. Melden Sie sich bei der Konsole der virtuellen Maschine des Agenten an.
2. Navigieren Sie zu `/opt/csa/certs`
3. Löschen Sie das selbstsignierte Zertifikat, das der Agent erstellt hat.
4. Fügen Sie Ihr SSL-Zertifikat ein.
5. Starten Sie die virtuelle Maschine neu.

Konfigurieren Sie den Agent für die Erkennung Ihrer FlexPod Infrastruktur

Sie müssen den Agent so konfigurieren, dass Konfigurationsdaten von jedem Gerät Ihrer konvergenten FlexPod Infrastruktur erfasst werden. Der Agent benötigt zur Erfassung von Konfigurationsdaten Zugangsdaten. Sie müssen die Anmeldeinformationen angeben, wenn Sie den Agenten konfigurieren.

Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse der virtuellen Agent-Maschine ein.
2. Melden Sie sich mit dem Benutzernamen und Passwort des NetApp Support Site-Kontos beim Agenten an.

   Für alle Partner, die eine lizenzierte Version von CSA im Auftrag ihres Kunden bereitstellen, ist es wichtig, dass das Kundenkonto in diesem Schritt verwendet wird (für NetApp Support und Records Management).

3. Fügen Sie die FlexPod-Geräte hinzu, die der Agent ermitteln soll.

   Sie haben zwei Möglichkeiten:

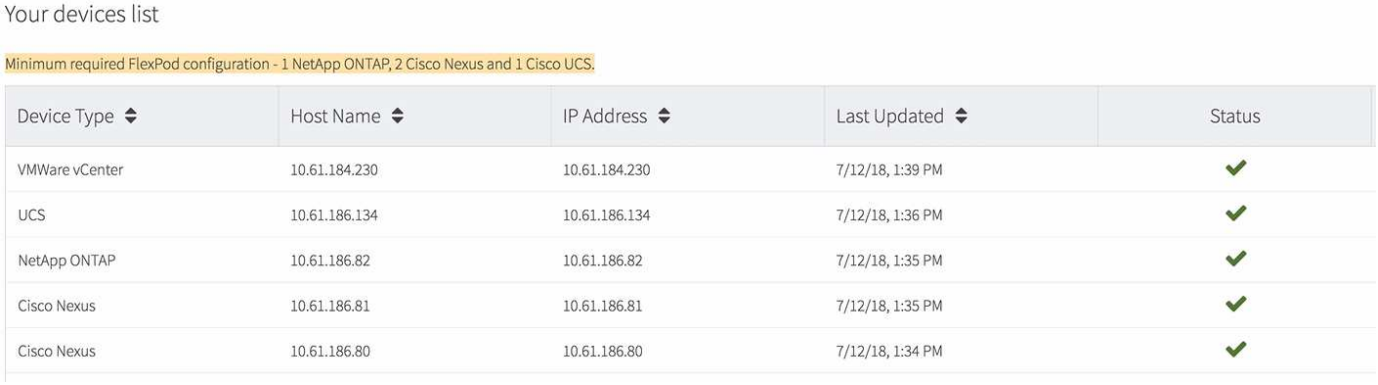
a. Klicken Sie auf **Gerät hinzufügen**, um Details zu Ihren FlexPod-Geräten einzeln einzugeben.

b. Klicken Sie auf **Geräte importieren**, um eine CSV-Vorlage mit Details zu allen Geräten auszufüllen und hochzuladen.

   Beachten Sie Folgendes: * Benutzername und Passwort sollten für das Konto verwendet werden, das Sie zuvor für das Gerät erstellt haben. * Wenn in Ihrer UCS-Umgebung die LDAP-Benutzerverwaltung konfiguriert ist, müssen Sie vor dem Benutzernamen die Domäne des Benutzers hinzufügen. Zum Beispiel: Local\csa-Readonly

Ergebnis

Jedes Gerät in der FlexPod-Infrastruktur sollte in der Tabelle mit einem Häkchen angezeigt werden.



Infrastruktur zum Portal hinzufügen

Nachdem Sie den Agent konfiguriert haben, sendet er Informationen über jedes FlexPod Gerät an das Converged Systems Advisor Portal. Sie müssen nun jede dieser Komponenten im Portal auswählen, um eine komplette Infrastruktur zu erstellen, die Sie überwachen können.

Schritte

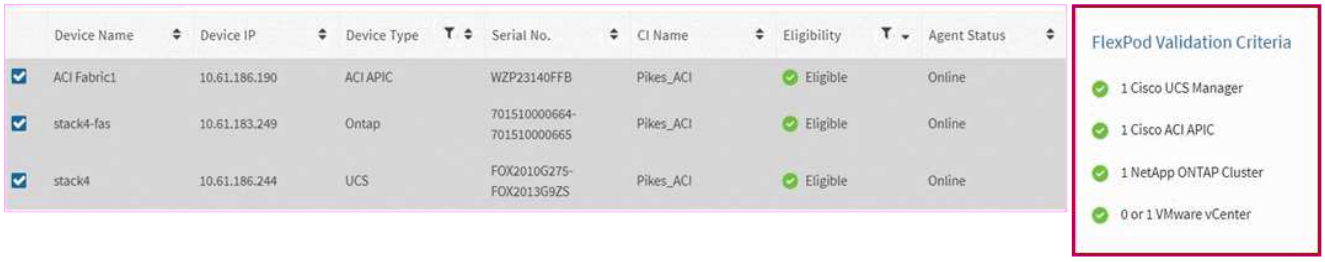
1. Im "Converged Systems Advisor-Portal"Klicken Sie auf **Infrastruktur hinzufügen**.
2. Durchführen der Schritte zum Hinzufügen der Infrastruktur:
   a. Geben Sie grundlegende Details zur Infrastruktur ein.

      Wenn Sie eine Cisco ACI Infrastruktur hinzufügen, geben Sie bei der Frage, ob Ihr FlexPod Cisco UCS Manager verwendet, **Nexus Switch im ACI Modus** ein, wenn Sie den Typ der Netzwerkkonfiguration, die Ihr FlexPod enthält, gefragt haben.

   b. Wählen Sie jedes Gerät aus, das Teil der FlexPod-Konfiguration ist.

      Wenn Sie ein Gerät auswählen, wird in der Spalte Berechtigung entweder **qualifiziert** oder **nicht geeignet** angezeigt. Ein Gerät ist nicht berechtigt, wenn es von einem anderen Agenten erkannt wurde.

3. Nachdem Sie alle erforderlichen Komponenten ausgewählt haben, sollten Sie neben jedem Gerätetyp ein grünes Häkchen sehen.



a. Fügen Sie Ihr hinzu "Seriennummer des Converged Systems Advisor" Um die Schlüsselfunktionen zu entsperren.

b. Lesen Sie die Zusammenfassung durch, akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Infrastruktur hinzufügen**.

Wenn Sie ein Partner oder Reseller sind, können Sie die Schritte zum Hinzufügen einer Lizenz oder Seriennummer überspringen und klicken Sie einfach auf **Infrastruktur hinzufügen**.

Ergebnis

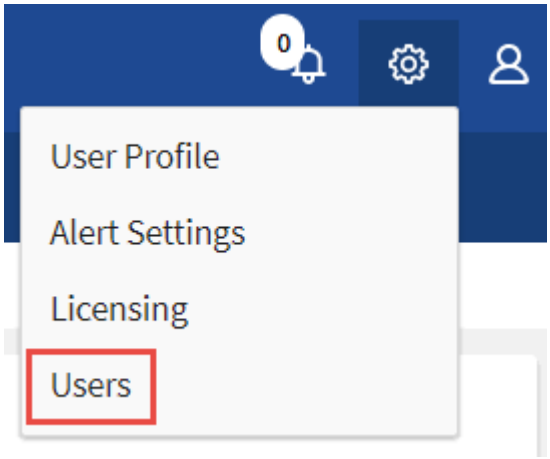
Converged Systems Advisor erweitert das Portal um die Infrastruktur und beginnt mit dem Erfassen von Konfigurationsdaten zu jedem Gerät. Warten Sie einige Minuten, bis der Agent Informationen von den Geräten erfasst.

Infrastruktur gemeinsam mit anderen Benutzern nutzen

Durch die gemeinsame Nutzung einer konvergenten Infrastruktur kann sich eine andere Person im Converged Systems Advisor Portal anmelden, damit sie die Konfiguration anzeigen und überwachen können. Der Mitarbeiter, mit dem Sie die Infrastruktur teilen, muss über eine verfügen "NetApp Support Website" Konto.

Schritte

1. Klicken Sie im Converged Systems Advisor-Portal auf das Symbol **Einstellungen** und dann auf **Benutzer**.



2. Wählen Sie die Konfiguration aus der Benutzertabelle aus.
3. Klicken Sie auf das + Symbol.
4. Geben Sie eine oder mehrere E-Mail-Adressen neben der Benutzerrolle ein, die Sie angeben möchten.

   "Zeigen Sie die Unterschiede zwischen den einzelnen Rollen an".

Sie können mehrere E-Mail-Adressen in einem Feld eingeben, indem Sie nach der ersten E-Mail-Adresse **Enter** drücken.

5. Klicken Sie Auf **Senden**.

Ergebnis

Der Benutzer sollte eine E-Mail mit Anweisungen für den Zugriff auf Converged Systems Advisor erhalten.

Konfigurieren Sie Benachrichtigungen

Wenn Sie eine Premiumlizenz besitzen, benachrichtigt Converged Systems Advisor Sie per E-Mail über Änderungen an Ihrer FlexPod Infrastruktur.

Schritte

1. Klicken Sie im Converged Systems Advisor-Portal auf das Symbol **Einstellungen** und dann auf **Warnmeldungseinstellungen**.
2. Prüfen Sie die Benachrichtigung, die Sie für jede konvergente Infrastruktur mit einer Premium-Lizenz erhalten möchten.

   Jede Benachrichtigung enthält folgende Informationen:

   Erfassungsfehler
   Warnungen, wenn Converged Systems Advisor keine Daten aus einer konvergenten Infrastruktur erfassen kann

   Offline-Agent
   Benachrichtigt Sie, wenn ein Converged Systems Advisor-Agent nicht online ist.

   Täglicher Alarmdigest
   Informiert Sie über fehlgeschlagene Regeln, die am Vortag aufgetreten sind.

3. Klicken Sie Auf **Speichern**.

Ergebnis

Converged Systems Advisor sendet nun E-Mail-Benachrichtigungen an die Benutzer, die mit der konvergenten Infrastruktur verknüpft sind.

Legen Sie eine statische IP-Adresse für den Agenten fest

Wenn in Ihrer Umgebung kein DHCP-Server vorhanden ist, können Sie eine statische IP-Adresse auf dem Converged Systems Advisor Agent festlegen.

Schritte

1. Melden Sie sich über den VMware vSphere Client bei der Konsole der virtuellen Maschine des Agenten an.

   Der Standardbenutzername ist **csa** und das Standardpasswort lautet **netapp**. Ändern Sie das Passwort, wenn Sie dazu aufgefordert werden.

2. Eingabe `sudo su -` An der csa-Eingabeaufforderung zum Root-Server.

3. Eingabe `# systemctl stop csa.service` Zum Stoppen des CSA-Dienstes.
4. Geben Sie Folgendes ein, um den korrekten Schnittstellendateinamen zu bestimmen.

   In diesem Beispiel lautet der Dateiname der Schnittstelle `eth0`.

   ```
   # ls /etc/network/interfaces.d/
   ```

5. Eingabe `# /sbin/ifdown eth0` Um die aktive Schnittstelle zu beenden.
6. Bearbeiten Sie die Datei /etc/Network/Interfaces.d/eth0 mit dem Editor Ihrer Wahl.

   ```
   # nano /etc/network/interfaces.d/eth0`Oder
   `# vi /etc/network/interfaces.d/eth0
   ```

   Die Datei enthält Folgendes:

   ```
   allow-hotplug eth0
   iface eth0 inet dhcp
   ```

7. Entfernen `iface eth0 inet dhcp` Und fügen Sie Folgendes hinzu: HINWEIS: Sie müssen die richtigen Werte für alle Einträge ersetzen, die den Feldnamen im folgenden Beispiel folgen. Zum Beispiel: `192.168.11.1` Ist der Wert für das Gateway im Beispiel. Jedoch statt `192.168.11.1`, Sie sollten die richtige Adresse für Ihr Gateway eingeben.

   ```
   iface eth0 inet static
   address 192.168.11.100
   netmask 255.255.255.0
   gateway 192.168.11.1
   dns-domain example.com
   dns-nameservers 192.168.11.1
   ```

8. Speichern Sie die Datei.

   In Nano geben Sie **Strg + o** ein, gefolgt von **Strg + x** zum Speichern.

9. Eingabe `vi/etc/resolv.conf` So öffnen Sie die Konfigurationsdatei:
10. Zusatz `nameserver <ip_address>` Zum Anfang der Datei.
11. Eingabe `# ifup eth0` Um die Netzwerkschnittstelle zu starten.
12. Eingabe `systemctl start csa.service` Um Converged Systems Advisor neu zu starten.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.