PRÜFPUNKT 1

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine benutzerdefinierte Nexus-Rolle für TACACS über die CLI auf NK9 konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- TACACS+
- ISE 3.2

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Die Cisco Nexus 9000 NXOS-Image-Datei lautet: bootflash:///nxos.9.3.5.bin
- Identity Service Engine Version 3.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Lizenzanforderungen

Cisco NX-OS - TACACS+ erfordert keine Lizenz.

Cisco Identity Service Engine

Für neue ISE-Installationen verfügen Sie über eine 90-Tage-Testlizenz mit Zugriff auf alle ISE-Funktionen. Wenn Sie keine Testlizenz besitzen, benötigen Sie für die Verwendung der ISE TACACS-Funktion eine Device Admin-Lizenz für den Policy Server Node, der die Authentifizierung vornimmt.

Nachdem sich die Admin-/Helpdesk-Benutzer auf dem Nexus-Gerät authentifiziert haben, gibt die

ISE die gewünschte Nexus Shell-Rolle zurück.

Der Benutzer mit dieser Rolle kann eine grundlegende Fehlerbehebung durchführen und bestimmte Ports zurückweisen.

Die TACACS-Sitzung, die die Nexus-Rolle übernimmt, muss nur die folgenden Befehle und Aktionen verwenden und ausführen können:

- Zugriff auf das konfigurierte Terminal, um NUR herunterzufahren und keine heruntergefahrenen Schnittstellen vom 1/1-1/21 und 1/25-1/30 auszuführen
- SSH
- SSH6
- telnet
- Telnet6
- Routenverfolgung
- Routenverfolgung6
- Ping
- Ping 6:
- Enable

Konfigurieren

Netzwerkdiagramm

Schritt 1: Nexus 9000 konfigurieren

1. AAA konfigurieren

> Warnung: Nachdem Sie die TACACS-Authentifizierung aktiviert haben, beendet das Nexus-Gerät die lokale Authentifizierung und beginnt mit der auf AAA-Servern basierenden Authentifizierung.

```
Nexus9000(config)# feature tacacs+
Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample
Nexus9000(config)# tacacs-server key 0 "Nexus3xample"
Nexus9000(config)# aaa group server tacacs+ IsePsnServers
Nexus9000(config-tacacs+)# server <Your ISE IP>
Nexus9000(config)# aaa authentication login default group IsePsnServers local
```

2. Konfigurieren Sie die benutzerdefinierte Rolle mit den angegebenen Anforderungen.

```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)#   description Can perform basic Toubleshooting and bounce certain  ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
```

```
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown

vlan policy deny
interface policy deny

Nexus9000(config-role-interface)#     permit interface Ethernet1/1
Nexus9000(config-role-interface)#     permit interface Ethernet1/2
Nexus9000(config-role-interface)#     permit interface Ethernet1/3
Nexus9000(config-role-interface)#     permit interface Ethernet1/4
Nexus9000(config-role-interface)#     permit interface Ethernet1/5
Nexus9000(config-role-interface)#     permit interface Ethernet1/6
Nexus9000(config-role-interface)#     permit interface Ethernet1/7
Nexus9000(config-role-interface)#     permit interface Ethernet1/8
Nexus9000(config-role-interface)#     permit interface Ethernet1/8
Nexus9000(config-role-interface)#     permit interface Ethernet1/9
Nexus9000(config-role-interface)#     permit interface Ethernet1/10
Nexus9000(config-role-interface)#     permit interface Ethernet1/11
Nexus9000(config-role-interface)#     permit interface Ethernet1/12
Nexus9000(config-role-interface)#     permit interface Ethernet1/13
Nexus9000(config-role-interface)#     permit interface Ethernet1/14
Nexus9000(config-role-interface)#     permit interface Ethernet1/15
Nexus9000(config-role-interface)#     permit interface Ethernet1/16
Nexus9000(config-role-interface)#     permit interface Ethernet1/17
Nexus9000(config-role-interface)#     permit interface Ethernet1/18
Nexus9000(config-role-interface)#     permit interface Ethernet1/19
Nexus9000(config-role-interface)#     permit interface Ethernet1/20
Nexus9000(config-role-interface)#     permit interface Ethernet1/21
Nexus9000(config-role-interface)#     permit interface Ethernet1/22
Nexus9000(config-role-interface)#     permit interface Ethernet1/25
Nexus9000(config-role-interface)#     permit interface Ethernet1/26
Nexus9000(config-role-interface)#     permit interface Ethernet1/27
Nexus9000(config-role-interface)#     permit interface Ethernet1/28
Nexus9000(config-role-interface)#     permit interface Ethernet1/29
Nexus9000(config-role-interface)#     permit interface Ethernet1/30

Nexus9000# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...

Copy complete.
```

Schritt 2: Identity Service Engine 3.2 konfigurieren

1. Konfigurieren Sie die Identität, die während der Nexus TACACS-Sitzung verwendet wird.

Die lokale ISE-Authentifizierung wird verwendet.

Navigieren Sie zur Registerkarte Administration > Identity Management > Groups (Verwaltung > Identitätsverwaltung > Gruppen), und erstellen Sie die Gruppe, der der Benutzer angehören muss.

Die für diese Demonstration erstellte Identitätsgruppe lautet iseUsers (iseUsers).

Klicken Sie auf die Schaltfläche "Senden".

Navigieren Sie anschließend zu Administration > Identity Management > Identity (Verwaltung > Identität).

Klicken Sie auf die Schaltfläche Hinzufügen.

Beginnen Sie in den Pflichtfeldern mit dem Namen des Benutzers. In diesem Beispiel wird der Benutzername iseiscool verwendet.

Der nächste Schritt besteht darin, dem erstellten Benutzernamen ein Kennwort zuzuweisen. VainillaISE97 ist das Passwort, das in dieser Demonstration verwendet wird.

Weisen Sie schließlich den Benutzer der zuvor erstellten Gruppe zu, in diesem Fall iseUsers (iseUsers).

2. Konfigurieren und Hinzufügen des Netzwerkgeräts

Fügen Sie das NEXUS 9000-Gerät der ISE-Administration > Network Resources > Network Devices hinzu.

Klicken Sie auf die Schaltfläche Hinzufügen, um zu starten.

Geben Sie die Werte in das Formular ein, weisen Sie dem von Ihnen erstellten NAD einen Namen und eine IP-Adresse zu, über die der NAD die ISE für die TACACS-Konversation kontaktiert.

Die Dropdown-Optionen können leer gelassen und weggelassen werden. Mit diesen Optionen können Sie Ihre NADs nach Standort, Gerätetyp und Version kategorisieren und dann den Authentifizierungsfluss auf Basis dieser Filter ändern.

Fügen Sie unter Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings den unter Ihrer NAD-Konfiguration verwendeten Shared Secret hinzu. In dieser Demonstration wird Nexus3xample verwendet.

Speichern Sie die Änderungen, indem Sie auf die Schaltfläche Submit (Senden) klicken.

3. Konfigurieren Sie TACACS auf der ISE.

Überprüfen Sie noch einmal, ob für das von Ihnen in Nexus 9000 konfigurierte PSN die Option Device Admin (Geräteadministrator) aktiviert ist.

> Anmerkung: Die Aktivierung des Geräte-Admin-Dienstes führt NICHT zu einem Neustart auf der ISE.

Dies kann über das ISE-Menü Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services überprüft werden.

- Erstellen Sie ein TACACS-Profil, das bei erfolgreicher Authentifizierung die Rolle Helpdesk

an das Nexus-Gerät zurückgibt.

Navigieren Sie im ISE-Menü zu Workcenters > Device Administration > Policy Elements > Results > TACACS Profiles, und klicken Sie auf die Schaltfläche Add (Hinzufügen).

Weisen Sie einen Namen und optional eine Beschreibung zu.

Ignorieren Sie den Abschnitt Aufgabenattributansicht, und navigieren Sie zum Abschnitt Rohansicht.

Geben Sie den Wert shell:roles="helpdesk" ein

Konfigurieren Sie den Richtliniensatz, der die Authentifizierungsrichtlinie und die Autorisierungsrichtlinie enthält.

Wählen Sie im Menü ISE Work Centers > Device Administration > Device Admin Policy Sets.

Zu Demonstrationszwecken wird die Standardrichtlinie verwendet. Es kann jedoch auch ein anderer Richtliniensatz erstellt werden, dessen Bedingungen bestimmten Szenarien entsprechen.

Klicken Sie auf den Pfeil am Ende der Zeile.

Führen Sie innerhalb der Konfiguration des Richtliniensatzes einen Bildlauf nach unten durch, und erweitern Sie den Abschnitt Authentifizierungsrichtlinie.

Klicken Sie auf das Symbol Hinzufügen.

In diesem Konfigurationsbeispiel lautet der Name-Wert Internal Authentication (Interne Authentifizierung), und die ausgewählte Bedingung ist die IP-Adresse des Netzwerkgeräts (Nexus) (ersetzt A.B.C.D.). Diese Authentifizierungsrichtlinie verwendet den Identitätsspeicher für interne Benutzer.

Hier sehen Sie, wie die Bedingung konfiguriert wurde.

Wählen Sie Network Access > Device IP address Dictionary Attribute aus.

Ersetzen Sie den Kommentar <Nexus IP address> durch die richtige IP.

Klicken Sie auf die Schaltfläche Verwenden.

Diese Bedingung wird nur von dem von Ihnen konfigurierten Nexus-Gerät erfüllt. Wenn diese Bedingung jedoch für eine große Anzahl von Geräten aktiviert werden soll, sollten Sie eine andere Bedingung in Betracht ziehen.

Navigieren Sie anschließend zum Abschnitt Autorisierungsrichtlinie, und erweitern Sie ihn.

Klicken Sie auf das Pluszeichen (+).

In diesem Beispiel wurde NEXUS HELP DESK als Name der Autorisierungsrichtlinie verwendet.

Die in der Authentifizierungsrichtlinie konfigurierte Bedingung wird auch für die Autorisierungsrichtlinie verwendet.

In der Spalte Shell Profiles (Shell-Profile) wurde das Profil konfiguriert, bevor Nexus Helpdesk ausgewählt wurde.

Klicken Sie abschließend auf die Schaltfläche Speichern.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Navigieren Sie in der ISE-GUI zu Operations > TACACS > Live Logs. Identifizieren Sie den Datensatz, der mit dem verwendeten Benutzernamen übereinstimmt, und klicken Sie auf Live Log Detail (Live-Protokolldetail) des Authorization-Ereignisses.

Als Teil der Details, die dieser Bericht enthält, finden Sie einen Antwort-Abschnitt, in dem Sie sehen können, wie ISE den Wert shell:roles="helpdesk" zurückgab.

Auf dem Nexus-Gerät:

```
Nexus9000 login: iseiscool
Password: VainillaISE97

Nexus9000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus9000(config)# interface ethernet 1/23
% Interface permission denied

Nexus9000(config)# ?
  interface  Configure interfaces
  show       Show running system information
  end        Go to exec mode
  exit       Exit from command interpreter

Nexus9000(config)# role name test
% Permission denied for the role

Nexus9000(config)#

Nexus9000(config)# interface loopback 0
% Interface permission denied

Nexus9000(config)#
Nexus9000# conf t

Nexus9000(config)# interface ethernet 1/5
Notice that only the commands allowed are listed.
Nexus9000(config-if)# ?

  no        Negate a command or set its defaults
  show      Show running system information
  shutdown  Enable/disable an interface
  end       Go to exec mode
  exit      Exit from command interpreter

Nexus9000(config-if)# cdp
```

```
Nexus9000(config-if)# cdp enable
% Permission denied for the role
Nexus9000(config-if)#
```

Fehlerbehebung

- Überprüfen Sie, ob die ISE vom Nexus-Gerät aus erreichbar ist:

  Nexus9000# ping <Ihre ISE-IP>
  PING <Ihre ISE IP> (<Ihre ISE IP> 56 Datenbytes
  64 Byte von <Ihre ISE-IP> : icmp_seq=0 ttl=59 time=1,22 ms
  64 Byte von <Ihre ISE-IP> : icmp_seq=1 ttl=59 time=0,739 ms
  64 Byte von <Ihre ISE-IP> : icmp_seq=2 ttl=59 time=0,686 ms
  64 Byte von <Ihre ISE-IP> : icmp_seq=3 ttl=59 time=0,71 ms
  64 Byte von <Ihre ISE-IP> : icmp_seq=4 ttl=59 time=0,72 ms

- Stellen Sie sicher, dass Port 49 zwischen der ISE und dem Nexus-Gerät geöffnet ist:
  Nexus9000# Telnet <Ihre ISE-IP> 49
  <Ihre ISE IP> wird versucht ...
  Verbunden mit <Ihre ISE-IP> .
  Das Escapezeichen ist '^]'.
- Verwenden Sie folgende Debugging-Optionen:

debug tacacs+ all
Nexus9000
Nexus9000# 2024 Apr 19 22:50:44.199329 TACACS: event_loop(): Prozess_rd_fd_set wird aufgerufen
2024 Apr 19 22:50:44.199355 takacs: Prozess_rd_fd_set: Rückruf für FD 6
2024 Apr 19 22:50:44.199392 takacs: fsrv verbrauchte 8421-Opcode nicht
2024 Apr 19 22:50:44.199406 takacs: process_implicit_cfs_session_start: eingehend...
2024 Apr 19 22:50:44.199414 takacs: process_implicit_cfs_session_start: Beenden; wir befinden uns in Distribution deaktiviert
2024 Apr 19 22:50:44.199424 takacs: process_aaa_tplus_request: Eingabe für aaa-Sitzungs-ID 0
2024 Apr 19 22:50:44.199438 takacs: process_aaa_tplus_request:Status des mgmt0-Ports mit Servergruppe "IsePsnServers" wird geprüft
2024 Apr 19 22:50:44.199451 takacs: tacacs_global_config(4220): eingeben...
2024 Apr 19 22:50:44.199466 takacs: tacacs_global_config(4577): GET_REQ...
2024 Apr 19 22:50:44.208027 takacs: tacacs_global_config(4701): Rückgabewert des globalen Protokollkonfigurationsvorgangs zurückerhalten:ERFOLG
2024 Apr 19 22:50:44.208045 takacs: tacacs_global_config(4716): ANFORDERUNG: Anzahl Server 0
2024 Apr 19 22:50:44.208054 takacs: tacacs_global_config: REQ:Num-Gruppe 1
2024 Apr 19 22:50:44.208062 takacs: tacacs_global_config: REQ:Anzahl Timeout 5
2024 Apr 19 22:50:44.208070 takacs: tacacs_global_config: REQ:Anzahl Endzeit 0
2024 Apr 19 22:50:44.208078 takacs: tacacs_global_config: REQ:Num encryption_type 7
2024 Apr 19 22:50:44.208086 takacs: tacacs_global_config: Rückgabe Retrieval 0

2024 Apr 19 22:50:44.208098 takacs: process_aaa_tplus_request:group_info wird in aaa_req eingetragen, also Using servergroup IsePsnServers
2024 Apr 19 22:50:44.208108 takacs: tacacs_servergroup_config: Eingabe für Servergruppe, Index 0
2024 Apr 19 22:50:44.208117 takacs: tacacs_servergroup_config: GETNEXT_REQ für Protokollserver-Gruppenindex: 0 Name
2024 Apr 19 22:50:44.208148 takacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = kein solcher pss-Schlüssel
2024 Apr 19 22:50:44.208160 takacs: tacacs_pss2_move2key: pss2_getkey wird aufgerufen
2024 Apr 19 22:50:44.208171 takacs: tacacs_servergroup_config: GETNEXT_REQ hat Protokollservergruppenindex erhalten:2 Name:IsePsnServers
2024 Apr 19 22:50:44.208184 takacs: tacacs_servergroup_config: Rückgabewert des Protokollgruppenvorgangs zurückerhalten:ERFOLG
2024 Apr 19 22:50:44.208194 takacs: tacacs_servergroup_config: Rückgabe von Retval 0 für Protokoll-Servergruppe:IsePsnServers
2024 Apr 19 22:50:44.208210 takacs: process_aaa_tplus_request: Gruppe IsePsnServers gefunden. entsprechendes VRF ist Standard, source-intf ist 0
2024 Apr 19 22:50:44.208224 takacs: process_aaa_tplus_request: Überprüfen von "mgmt0 vrf:management" im Vergleich zu "vrf:default" der angeforderten Gruppe
2024 Apr 19 22:50:44.208256 takacs: process_aaa_tplus_request:mgmt_if 83886080
2024 Apr 19 22:50:44.208272 takacs: process_aaa_tplus_request:global_src_intf : 0, "src_intf" ist 0 und "vrf_name" ist der Standardwert
2024 Apr 19 22:50:44.208286 takacs: create_tplus_req_state_machine(902): Eingabe für aaa-Sitzungs-ID 0
2024 Apr 19 22:50:44.208295 takacs: Statuscomputeranzahl 0
2024 Apr 19 22:50:44.208307 takacs: init_tplus_req_state_machine: Eingabe für aaa-Sitzungs-ID 0
2024 Apr 19 22:50:44.208317 takacs: init_tplus_req_state_machine(1298):tplus_ctx ist NULL, wenn Autor und Test
2024 Apr 19 22:50:44.208327 takacs: tacacs_servergroup_config: Eingabe für ServergruppeIsePsnServers, Index 0
2024 Apr 19 22:50:44.208339 takacs: tacacs_servergroup_config: GET_REQ für Protokollservergruppenindex:0 Name:IsePsnServers
2024 Apr 19 22:50:44.208357 takacs: find_tacacs_serverGruppe: Eingabe für Servergruppe IsePsnServers
2024 Apr 19 22:50:44.208372 takacs: tacacs_pss2_move2key: rcode = 0 syserr2str = ERFOLG
2024 Apr 19 22:50:44.208382 takacs: find_tacacs_serverGruppe: IsePsnServers-Index für Servergruppe wird beendet auf 2
2024 Apr 19 22:50:44.208401 takacs: tacacs_servergroup_config: GET_REQ: find_tacacs_servergroup Fehler 0 für Protokollservergruppe IsePsnServers
2024 Apr 19 22:50:44.208420 takacs: tacacs_pss2_move2key: rcode = 0 syserr2str = ERFOLG
2024 Apr 19 22:50:44.208433 takacs: tacacs_servergroup_config: GET_REQ hat Protokollservergruppenindex erhalten:2 Name:IsePsnServers
2024 A2024 19. April 2022:52024 19. April 2022:52024 19. April 22:5
Nexus9000

- Führen Sie eine Paketerfassung durch. (Um die Paketdetails anzuzeigen, müssen Sie die Wireshark TACACS+-Einstellungen ändern und den von Nexus und der ISE verwendeten gemeinsamen Schlüssel aktualisieren.)
- Überprüfen Sie, ob der gemeinsame Schlüssel auf ISE- und Nexus-Seite identisch ist. Dies kann auch in Wireshark überprüft werden.

Einleitung

In diesem Dokument wird die Installation von Produkt A beschrieben.

Test A

1. Die erste ul hat ein Problem.
2. Stellen Sie sicher, dass VMs mit den folgenden zusätzlichen Einstellungen konfiguriert sind, indem Sie in VMware ESXi mit der rechten Maustaste auf das gewünschte VM klicken und dann auf Einstellungen bearbeiten klicken.
    - ul2test tag, No Span tag CPU: Wählen Sie Lowaus der ersten Dropdown-ListeShares aus.
    - ul2 tag, No Span tag CPU: Wählen Sie Lowaus der ersten Dropdown-ListeShares aus.
    - ul2 tag, Kein span tag Speicher: Aktivieren Sie das Kontrollkästchen Gesamten Gastspeicher reservieren (Alle gesperrt).
    - ul2-Tag. Kein span-Tag Legen Sie CPU und RAM basierend auf Ihrer Skalierungsgröße fest. Siehe für weitere Informationen
    - ul3 wurde von ul kopiert, es liegt ein Problem vor. span tag entfernt, p tag.CPU hinzugefügt: Wählen Sie Lowaus der ersten Dropdown-ListeShares aus.
    - ul3 wurde von ul kopiert, es liegt ein Problem vor. span tag entfernt, p tag.Memory hinzugefügt: Aktivieren Sie das Kontrollkästchen Gesamten Gastspeicher reservieren (Alle gesperrt).
    - ul3 wurde von ul kopiert, es liegt ein Problem vor. span tag entfernt, p tag hinzugefügt. Legen Sie CPU und RAM auf Grundlage Ihrer Skalierungsgröße fest. Siehe Test Self Link für weitere Details
    - ul4. gerade von ul1.CPU kopiert: Wählen Sie Lowaus der ersten Dropdown-ListeShares aus.
    - ul4. gerade aus ul1.Memory kopiert: Aktivieren Sie das Kontrollkästchen Gesamten Gastspeicher reservieren (Alle gesperrt).
    - ul4. nur aus ul1 kopiert. Legen Sie CPU und RAM basierend auf Ihrer

Skalierungsgröße fest. Siehe Für weitere Details verwendete Komponenten

- ul5. kopiert vom Original, kein p-Tag, mit span-TagCPU: Wählen Sie in der ersten Dropdown-Liste Freigaben die Option Niedrig aus.
- ul5. kopiert vom Original, kein p-Tag, mit span tagMemory: Aktivieren Sie das Kontrollkästchen Gesamten Gastspeicher reservieren (Alle gesperrt).
- ul5. kopiert von Original, kein p-Tag, mit span tagSet CPU und RAM basierend auf Ihrer Skalierungsgröße. SieheHardware- und VM-Ressourcenanforderungen für weitere Informationen

- ul1 mit einem Problem. span tag entfernt, p tag.CPU hinzugefügt: Wählen Sie Lowaus der ersten Dropdown-ListeShares aus.

- ul1 mit einem Problem. span tag entfernt, p tag.Memory hinzugefügt: Aktivieren Sie das Kontrollkästchen Gesamten Gastspeicher reservieren (Alle gesperrt).

- ul1 mit einem Problem. span tag entfernt, p tag hinzugefügt. Legen Sie CPU und RAM auf Grundlage Ihrer Skalierungsgröße fest. Siehe Hardware- und VM-Ressourcenanforderungen für weitere Details

1. Das ist OK Version. Melden Sie sich mit Administratoranmeldeinformationen beim Red Hat Host-BS-Server an.

2. Nehmen Sie im Dialogfeld die folgende Konfiguration vor:

    - Geben Sie unter Ready to begin the installation (Bereit zum Starten der Installation) einen Namen für die Cisco IQ Link-Instanz ein.

    - Klicken Sie vor der Installation auf Konfiguration anpassen.

    - Stellen Sie sicher, dass Sie unter Network selection (Netzwerkauswahl) das entsprechende virtuelle Netzwerk auswählen.

3. Klicken Sie auf Fertig stellen, um das Hinzufügen des ersten Datenträgers abzuschließen.

4. Passen Sie auf der VMM-Konsole die Kennwortkonfiguration und die IP-Eigenschaften an.

Informationen zu dieser Übersetzung

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