

Zugriffsrichtlinien, statische Bindung (Pfade), L2Outs, L3Outs und VMM Integration (vDS) konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Beispieltopologie](#)

[Zugriffsrichtlinien für die Verbindung über eine physische Domäne](#)

[High-Level-Anweisungen](#)

[Detaillierte Anweisungen](#)

[Statische Bindung \(Pfade\) für Bare-Metal-Server oder L2Out-Konfiguration mithilfe der statischen Bindungsmethode](#)

[Voraussetzungen für die L2Out-Konfiguration unter Verwendung der statischen Bindungsmethode](#)

[High-Level-Anweisungen](#)

[Detaillierte Anweisungen](#)

[L2Out-Konfiguration unter Verwendung der Routed Bridge Network-Methode](#)

[High-Level-Anweisungen](#)

[Detaillierte Anweisungen](#)

[L3Out-Konfiguration](#)

[Voraussetzungen](#)

[High-Level-Anweisungen](#)

[Detaillierte Anweisungen](#)

[VMM-Integration in eine vDS-Konfiguration](#)

[High-Level-Anweisungen](#)

[Detaillierte Anweisungen](#)

[Konnektivität überprüfen](#)

Einführung

Dieses Dokument beschreibt die Konfiguration von Zugriffsrichtlinien, statischen Bindungen (Pfade) oder Layer 2 Outside (L2Out) mithilfe der statischen Bindungsmethode, L2Out mithilfe der Routed Bridge Network-Methode, Layer 3 Outside (L3Out) und Virtual Machine Manager (VMM) Integration mit einem vSphere Distributed Switch (vDS) von unten nach oben, beginnend mit dem Schnittstellenauswahl über den Application Policy Infrastructure Controller (APIC)) GUI ohne QuickStart-Assistenten.

Dieses Dokument gilt jedoch ab 2.0(1q). Es gibt einige Unterschiede in der Konfiguration für 2.1(1h).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der Cisco Application Centric Infrastructure (ACI)-Technologie

Verwendete Komponenten

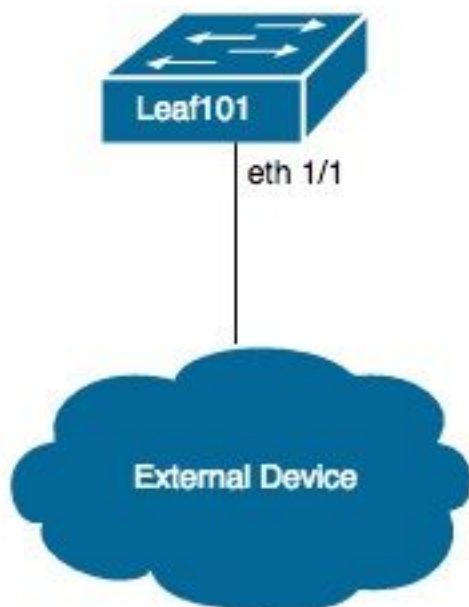
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Application Policy Infrastructure Controller (APIC) Image Release 2.0(1q)
- Cisco Nexus ACI Mode Switch Software Version 12.0(1q) der Serie 9000

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Beispieltopologie

Diese Topologie wird für alle diese Beispiele verwendet. Beim externen Gerät kann es sich um den externen Switch, den Bare-Metal-Server, den externen Router oder vDS handeln.



Zugriffsrichtlinien für die Verbindung über eine physische Domäne

Hinweis: Die Beinamen für die Richtlinien werden nach dem Zweck der Verbindung benannt. Beispiel: Wenn N3K physisch mit einem Nexus 3000 (N3K)-Switch verbunden ist.

Die Namenskonvention muss nicht strikt eingehalten werden.

High-Level-Anweisungen

1. Konfigurieren von Schnittstellenprofil und Schnittstellenauswahl.
2. Konfigurieren Sie die Schnittstellenrichtliniengruppe.
3. Switch-Profil konfigurieren und Schnittstellenauswahl dem Switch-Profil zuordnen
4. (Optional) Konfigurieren Sie Virtual Port Channel Security Policy (Virtual Port Channel-Sicherheitsrichtlinie), wenn Sie einen virtuellen Port-Channel (vPC) konfigurieren.
5. Konfigurieren Sie das angehängte ZugriffsEntity-Profil, und ordnen Sie das angehängte ZugriffsEntity-Profil der Schnittstellenrichtliniengruppe zu.
6. Konfigurieren Sie den Domänen- und VLAN-Pool, und ordnen Sie ihm das Umgebungsprofil an die Domäne an.

Detaillierte Anweisungen

1. Navigieren Sie zu **Fabric> Zugriffsrichtlinien**.
2. Navigieren Sie zu **Schnittstellenrichtlinien > Profile>Leaf-Profile**.
3. Klicken Sie mit der rechten Maustaste auf **Leaf-Profile** und dann auf **Leaf-Schnittstellenprofil erstellen**. Geben Sie nun einen Namen ein (z. B. N3K).
4. Klicken Sie auf **+** Zeichen neben **Schnittstellenauswahl**. Geben Sie nun einen Namen ein (z. B. N3K) und die Schnittstellen-IDs (z. B. 1/1).
5. Klicken Sie auf **OK** und dann auf **Senden**.
6. Navigieren Sie zu **Schnittstellenrichtlinien>Richtliniengruppen>Leaf-Richtliniengruppen**.
7. Klicken Sie mit der rechten Maustaste auf **Leaf Policy Groups** (Leaf-Richtliniengruppen), und klicken Sie auf die entsprechende Option für eine einzelne, Port-Channel- oder vPC-Schnittstelle. Geben Sie einen Namen ein (z. B. N3K), und wählen Sie die entsprechenden Richtlinien aus oder erstellen Sie diese.
8. Klicken Sie auf **Senden**.
9. Navigieren Sie zurück zu **Interface Policies > Profiles > Leaf Profiles > N3K (Leaf Interface Profile) >N3K (Access Port Selector)**.
10. Wählen Sie im Dropdown-Menü die **Richtliniengruppe aus**, die zugeordnet werden soll (z. B. N3K).

11. Klicken Sie auf **Senden**.
12. Navigieren Sie zu **Switch Policies> Profiles>Leaf Profiles**.
13. Klicken Sie mit der rechten Maustaste auf **Leaf-Profile** und dann auf **Leaf-Profil erstellen**. Geben Sie nun einen Namen ein (z. B. Leaf101).
14. Klicken Sie auf **+** neben **Leaf Selectors**. Geben Sie nun einen Namen ein (z. B. Leaf (101) und wählen Sie mithilfe des Dropdown-Menüs unter **Blöcke** den bzw. die zu verknüpfenden Switches aus.
15. Klicken Sie auf **Aktualisieren**, dann auf **Weiter** und dann auf **Fertig stellen**.
16. Die Schritte 17 und 19 sind nur bei der Konfiguration eines vPC erforderlich.
17. (Optional) Navigieren Sie zu **Switch Policies > Policies > Virtual Port Channel default**.
18. (Optional) Klicken Sie neben **Explicit VPC Protection Groups (Explizite VPC-Schutzgruppen)** auf **+** Zeichen. Geben Sie nun einen Namen ein (z. B. Leaf101-Leaf102), ID (z. B. 100), und wählen Sie mithilfe der Dropdown-Menüs Switch 1 aus (z. B. 101) und Switch 2 (z. B. 102).
19. (Optional) Klicken Sie auf **Senden**.
20. Wählen Sie **Leaf101** (Leaf-Profil) aus.
21. Klicken Sie auf **+** neben **Zugeordnete Schnittstellenauswahl-Profile**; Wählen Sie im Dropdown-Menü das zuzuordnende **Schnittstellenprofil** aus (z. B. N3K).
22. Klicken Sie auf **Senden**.
23. Navigieren Sie zu **Globale Richtlinien> Angehängte ZugriffsEntity-Profile**.
24. Klicken Sie mit der rechten Maustaste auf **Attachable Access Entity Profiles**, und klicken Sie auf **Create Attachable Access Entity Profile**. Geben Sie nun einen Namen ein (z. B. N3K).
25. Klicken Sie auf **Weiter** und anschließend auf **Beenden**.
26. Navigieren Sie zurück zu **Schnittstellenrichtlinien>Richtliniengruppen> Leaf Policy Groups > N3K** (Richtliniengruppe).
27. Wählen Sie im Dropdown-Menü unter **Attached Entity Profile (Angefügte Entitätsprofile)** das **angehängte Zugriffsprofil** aus (z. B. N3K).
28. Klicken Sie auf **Senden**.
29. Navigieren Sie zu **Physische und externe Domänen > Physische Domänen**.

30. Klicken Sie mit der rechten Maustaste auf **Physische Domänen**, und klicken Sie dann in **Physische Domäne erstellen**. Geben Sie einen Namen ein (z. B. N3K) können Sie das **Associated Attachable Entity Profile (Associated Attachable Entity Profile (z. B. N3K)**, verwenden Sie das Dropdown-Menü, um **einen VLAN-Pool zu erstellen**.
31. Geben Sie einen Namen ein (z. B. N3K) und wählen Sie die entsprechende dynamische/statische Zuweisung aus.
32. Klicken Sie auf **+** neben **Encap Blocks**. Geben Sie nun die VLAN-Nummern ein, und wählen Sie die entsprechende dynamische/statische Zuweisung aus.
33. Klicken Sie auf **OK**, dann auf **Senden** und dann auf **Senden**.

Statische Bindung (Pfade) für Bare-Metal-Server oder L2Out-Konfiguration mithilfe der statischen Bindungsmethode

Voraussetzungen für die L2Out-Konfiguration unter Verwendung der statischen Bindungsmethode

Es wird davon ausgegangen, dass die Endpunktgruppe (EPG), die Bridge-Domäne (BD) und die VRF-Instanz erstellt wurden und dass der BD auf den Layer 2 (L2)-Modus eingestellt ist (Deaktivieren Sie Unicast Routing unter L3-Konfigurationen, und legen Sie alle Optionen in Main auf Flood fest).

High-Level-Anweisungen

1. Konfigurieren von Zugriffsrichtlinien
2. Domäne der EPG zuordnen
3. Konfigurieren der statischen Bindung (Pfade) an Bare-Metal-Server oder L2Out-Switch

Detaillierte Anweisungen

1. Vollständige Zugriffsrichtlinien für die Verbindung über die Anweisungen oben in der physischen Domäne.
2. Navigieren Sie zur EPG, um die statische Bindung zu hinzuzufügen (z. B. **Tenants > Tenant1 > Application Profiles > AP1 > Application EPGs > EPG1**).
3. Wählen Sie **Domains (VMs und Bare-Metals)** aus.
4. Navigieren Sie zu **AKTIONEN > Physische Domänenzuordnung hinzufügen**. Wählen Sie jetzt

aus dem Dropdown-Menü die **Physical Domain (Physische Domäne)** aus, die zugeordnet werden soll (z. B. N3K), und wählen Sie die entsprechende Unmittelbarkeit (z. B. Sofort/Sofort).

5. Klicken Sie auf **Senden**.
6. Wählen Sie **Statische Bindungen (Pfade)**.
7. Navigieren Sie zu **AKTIONEN > Statische EPG auf PC, VPC oder Schnittstelle bereitstellen**. Wählen Sie nun den entsprechenden Pfadtyp und Pfad aus, geben Sie das Encap VLAN ein, und wählen Sie die entsprechende Unmittelbarkeit (z. B. Sofort) und Modus (z. B. Trunk).
8. Klicken Sie auf **Senden**.

L2Out-Konfiguration unter Verwendung der Routed Bridge Network-Methode

High-Level-Anweisungen

1. Konfigurieren von Zugriffsrichtlinien
2. Konfigurieren eines externen Bridge-Netzwerks
3. Anwenden geeigneter Verträge.

Detaillierte Anweisungen

1. Vollständige Zugriffsrichtlinien für die Anbindung über physische Domänen, außer Schritt 29 durch **externe Bridge-Domänen** und Schritt 30 durch **Erstellen einer Layer-2-Domäne** zu ersetzen.
2. Navigieren Sie zum entsprechenden **Tenant** (z. B. Tenant1) > **Networking>Externe Bridge-Netzwerke**.
3. Klicken Sie mit der rechten Maustaste auf **Externe Bridge-Netzwerke** und klicken Sie dann auf **Created Bridged Outside (Von außen erstellte Bridge erstellt)**. Geben Sie nun einen Namen ein (z. B. L2Out), wählen Sie mithilfe des Dropdown-Menüs die **Externe Bridge-Domäne** aus, die zugeordnet werden soll (z. B. N3K), wählen Sie im Dropdown-Menü die **Bridge Domain (Bridge-Domäne)** aus, die zugeordnet werden soll (z. B. BD1), und geben Sie das VLAN für diesen L2Out ein.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
5. Navigieren Sie zu **L2Out (L2-Außenbereich) >Knotenprofile**.

6. Klicken Sie mit der rechten Maustaste auf **Knotenprofile** und klicken Sie dann auf **Knotenprofil erstellen**. Geben Sie nun einen Namen ein (z. B. Leaf101).
7. Klicken Sie auf **+** neben **Schnittstellenprofile**. Geben Sie nun einen Namen ein (z. B. eth1_1).
8. Klicken Sie auf **+** neben **Schnittstellen**. Wählen Sie nun den entsprechenden Pfadtyp und den entsprechenden Pfad aus.
9. Klicken Sie auf **OK**, dann auf **OK** und dann auf **Senden**.
10. Navigieren Sie zu **Netzwerke**.
11. Klicken Sie mit der rechten Maustaste auf **Netzwerke**, und klicken Sie auf **Externes Netzwerk erstellen**. Geben Sie einen Namen ein (z. B. L2Out-EPG).
12. Klicken Sie auf **Senden**.
13. Ordnen Sie Verträge zwischen der L2Out EPG entsprechend an (z. B. L2Out-EPG) und die Anwendungs-EPG (z. B. EPG1) für die Kommunikation.

L3Out-Konfiguration

Voraussetzungen

Es wird davon ausgegangen, dass das Routing über statische Routen mit einem einzelnen Tenant und einer VRF-Instanz erfolgt, dass EPG, BD und VRF erstellt und der BD auf den Layer 3 (L3)-Modus eingestellt wird (Aktivieren Sie Unicast Routing unter L3-Konfigurationen).

High-Level-Anweisungen

1. Konfigurieren von Zugriffsrichtlinien
2. Konfigurieren Sie ein externes geroutetes Netzwerk.
3. Ordnen Sie die L3Out-Domäne der Bridge-Domäne zu.
4. Anwenden geeigneter Verträge.

Detaillierte Anweisungen

1. Vollständige Zugriffsrichtlinien für die Verbindung über die Anweisungen für die physische Domäne, außer Schritt 25 durch **externe geroutete Domänen** und Schritt 26 durch **Layer-3-Domäne erstellen** zu ersetzen.

2. Navigieren Sie zum entsprechenden Tenant (z. B. Tenant1) > **Networking** > **External Routed Networks**.
3. Klicken Sie mit der rechten Maustaste auf **Externe Routing-Netzwerke** und klicken Sie auf **Routed Outside (Routing außerhalb erstellen)**. Geben Sie einen Namen ein (z. B. L3Out), wählen Sie mithilfe des Dropdown-Menüs die **VRF-Instanz** für die Zuordnung aus (z. B. VRF1), und wählen Sie mithilfe des Dropdown-Menüs die **externe weitergeleitete Domäne** aus, die zugeordnet werden soll (z. B. N3K).
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
5. Navigieren Sie zu **L3Out (L3-Außenbereich)** > **Logical Node Profiles**.
6. Klicken Sie mit der rechten Maustaste auf **Logische Knotenprofile**, und klicken Sie auf **Knotenprofil erstellen**. Geben Sie nun einen Namen ein (z. B. Leaf101).
7. Klicken Sie auf **+** neben **Knoten**. Wählen Sie nun den entsprechenden Knoten aus, und geben Sie eine Router-ID ein.
8. Klicken Sie auf **+** neben **Statische Routen**. Geben Sie jetzt das Routenpräfix ein.
9. Klicken Sie auf **+** neben **Next Hop Addresses**. Geben Sie jetzt die Next Hop IP ein.
10. Klicken Sie auf **Aktualisieren**, dann auf **OK** und dann auf **OK**.
11. Wiederholen Sie die Schritte 7 und 10 je nach Bedarf für jeden hinzuzufügenden Knoten.
12. Klicken Sie auf **Senden**.
13. Navigieren Sie zu **Leaf101 (Logical Node Profile)** > **Logical Interface Profiles**.
14. Klicken Sie mit der rechten Maustaste auf **Logische Schnittstellenprofile**, und klicken Sie auf **Schnittstellenprofil erstellen**. Geben Sie nun einen Namen ein (z. B. eth1_1).
15. Klicken Sie auf **Senden**.
16. Wählen Sie **eth1_1** (logisches Schnittstellenprofil) aus.
17. Klicken Sie abhängig von der gewünschten Konfiguration neben geroutete Schnittstellen, SVI oder geroutete Subschnittstellen auf **+**. Wählen Sie nun den entsprechenden Pfadtyp und Pfad aus, und weisen Sie die entsprechenden IP-Adressen für die Schnittstelle(n) zu.
18. Klicken Sie auf **Senden**.
19. Wählen Sie **Netzwerke** aus.
20. Klicken Sie mit der rechten Maustaste auf **Netzwerke** und klicken Sie auf **Externes**

Netzwerk erstellen. Geben Sie nun einen Namen ein (z. B. L3Out-EPG).

21. Klicken Sie auf **Senden**.
22. Wählen Sie **L3Out-EPG** (External Network Instance Profile) aus.
23. Klicken Sie neben **Subnets** auf **+Zeichen**. Geben Sie nun ein externes Subnetz hinter diesem L3Out ein, und überprüfen Sie **externe Subnetze für die externe EPG**.
24. Klicken Sie auf **Senden**.
25. Wiederholen Sie die Schritte 23 und 24 je nach Bedarf für jedes hinzuzufügende Subnetz.
26. Klicken Sie auf **Senden**.
27. Navigieren Sie zum BD der Anwendungs-EPG (z. B. BD1) **>L3-Konfigurationen**.
28. Klicken Sie auf **+** neben **Zugeordnete L3-Einträge**. Wählen Sie jetzt aus dem Dropdown-Menü den **L3Out** aus, der zugeordnet werden soll (z. B. Tenant1/L3Out).
29. Klicken Sie auf **Aktualisieren**.
30. Ordnen Sie Verträge zwischen der L3Out EPG entsprechend an (z. B. L3Out-EPG) und die Anwendungs-EPG (z. B. EPG1) für die Kommunikation.

VMM-Integration in eine vDS-Konfiguration

Hinweis: Die vCenter-Anweisungen gehen davon aus, dass sie mit vCenter vertraut sind. Daher sind sie kurz. Die Namen unter den Zugriffsrichtlinien wurden in diesem Beispiel von N3K zu DVS (Distributed Virtual Switch) geändert. Die Begriffe vSphere Distributed Switch (vDS) und Distributed Virtual Switch (DVS) werden synonym verwendet, da sie dasselbe betreffen.

High-Level-Anweisungen

1. Konfigurieren von Zugriffsrichtlinien
2. Konfigurieren der VMM-Domäne
3. Fügen Sie Uplinks zu vDS hinzu.
4. Ordnen Sie VMM-Domäne der EPG zu.
5. Hinzufügen von VMs zur Portgruppe

6. Überprüfen der Verbindung

Detaillierte Anweisungen

1. Vollständige Zugriffsrichtlinien für die Verbindung über physische Domänen (Physical Domain Instruktions), mit Ausnahme der Beendigung nach Abschluss von Schritt 24.
2. Navigieren Sie zu **VM Networking > Inventory > VMWare**.
3. Klicken Sie mit der rechten Maustaste auf **VMWare** und klicken Sie auf **vCenter-Domäne erstellen**.
4. Geben Sie einen Namen ein (z. B. DVS), wählen Sie im Dropdown-Menü das zuzuordnende **angehängte Entitätsprofil** aus (z. B. DVS), und wählen Sie im Dropdown-Menü **Create VLAN Pool (VLAN-Pool erstellen, um den VLAN-Pool für den DVS zu erstellen**.
5. Geben Sie einen Namen ein (z. B. DVS), und wählen Sie die entsprechende dynamische/statische Zuweisung aus (z. B. Dynamische Zuweisung).
6. Klicken Sie auf **+** neben **Encap Blocks**. Geben Sie nun die VLAN-Nummern ein, und wählen Sie die entsprechende dynamische/statische Zuweisung (z. B. Erben Sie allocMode von parent).
7. Klicken Sie auf **OK** und dann auf **Senden**.
8. Klicken Sie auf **+** neben **vCenter-Anmeldeinformationen**. Geben Sie nun einen Namen ein (z. B. vCenter-6), Benutzername (z. B. root) und ein Kennwort ein.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf **+** neben **vCenter/vShield**. Geben Sie nun einen Namen ein (z. B. vCenter-6), IP-Adresse, wählen Sie die entsprechende DVS-Version aus (z. B. vCenter Default), geben Sie den Namen des Rechenzentrums ein, wie er in vCenter angezeigt wird (z. B. DC), und wählen Sie im Dropdown-Menü die **Zugeordnete Anmeldeinformationen aus**.
11. Klicken Sie auf **OK** und dann auf **Senden**.
12. Navigieren Sie zu **DVS (Domäne)**, scrollen Sie nach unten zu **vSwitch-Richtlinien** und wählen Sie die entsprechenden vSwitch-Richtlinien aus.
13. Klicken Sie auf **Senden**.
14. Wechsel zu vCenter; die neue vDS erstellt werden soll (z. B. DVS) unter einem Ordner im Rechenzentrum (z. B. DC).
15. Klicken Sie mit der rechten Maustaste auf den vDS, und fügen Sie die Hosts und

entsprechenden Uplinks zum vDS hinzu.

16. Wechseln Sie zurück zur APIC-GUI.

17. Navigieren Sie zur entsprechenden EPG (z. B. **Tenant1 > AP1 > EPG1**) **>Domänen (VMs und Bare-Metals)**.

18. Klicken Sie auf **ACTIONS >Add VMM Domain Association**. Wählen Sie jetzt mithilfe des Dropdown-Menüs die **VMM Domain** für die Zuordnung aus (z. B. DVS), und wählen Sie die entsprechende Unmittelbarkeit aus (z. B. Sofort/Sofort).

19. Klicken Sie auf **Senden**.

20. Wechsel zu vCenter; Die neue Portgruppe sollte unter dem vDS erstellt werden (z. B. Tenant1|AP1|EPG1).

21. Wählen Sie eine VM aus. die Einstellungen für die Netzwerkkarte bearbeiten, die dieser Portgruppe zugeordnet werden soll.

Konnektivität überprüfen

1. Wechseln Sie zurück zur APIC-GUI.

2. Navigieren Sie zur entsprechenden EPG (z. B. EPG1) **> Operativ**.

3. Das virtuelle System sollte auf dieser Registerkarte erfasst werden (vmm = vCenter weiß von der IP-Adresse; Gelernt = ACI-Leaf sieht Datenverkehr von dieser IP).