

Konfigurationsbeispiel für Microsoft-Netzwerklastenausgleich bei Servern der UCS-B-Serie

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Microsoft NLB-Modi](#)

[Unicast-Modus](#)

[Multicast-/Multicast-IGMP-Modus](#)

[Microsoft NLB-Datenfluss](#)

[Besondere Überlegungen für Nexus 1000v](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt die Implementierung des Microsoft Network Load Balancing (NLB)-Modus auf der Cisco Unified Computing System-B (UCS-B)-Serie mit Fabric Interconnect (FI) im End-Host-Modus. Es gibt auch eine Reihe von Anforderungen an die Upstream-Geräte, um die korrekte Weiterleitung von NLB-Datenverkehr zu erleichtern. Diese werden in diesem Dokument beschrieben. Das Konfigurationsbeispiel konzentriert sich auf den Multicast Internet Group Management Protocol (IGMP)-Modus.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Microsoft-Netzwerk-Lastenausgleich
- Cisco UCS Server der B-Serie

- Cisco Catalyst- und/oder Nexus-Switches

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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.

Hintergrundinformationen

Microsoft NLB funktioniert in drei verschiedenen Betriebsmodi: Unicast-, Multicast- und Multicast-IGMP. Eine Gruppe von NLB-Knoten wird zusammen als NLB-Cluster bezeichnet. Ein NLB-Cluster stellt eine oder mehrere virtuelle IP-Adressen (VIP) bereit. Knoten im NLB-Cluster verwenden ihren Lastenausgleichsalgorithmus, um sich darüber zu einigen, welcher einzelne Knoten für den für das NLB VIP bestimmten Datenverkehrsfluss bereitstellt.

Dieses Dokument enthält keine spezifischen Bereitstellungsempfehlungen für Microsoft NLB auf dem UCS. Wie in diesem Dokument beschrieben, stützt sich die NLB auf unkonventionelle Methoden zur Übermittlung von clustergebundenem Datenverkehr. Es wurde beobachtet, dass sowohl der Multicast- als auch der Multicast-IGMP-Modus für die UCS-Server der B-Serie einen stabilen und konsistenten Betrieb zu bieten scheinen. Obwohl die NLB-Dimensionierungsrichtlinien nicht in diesem Dokument behandelt werden, wird diese Lösung in der Regel für kleinere Bereitstellungen empfohlen.

Konfiguration

Microsoft NLB-Modi

Unicast-Modus

Die NLB-StandardEinstellung ist Unicast-Modus. Im Unicast-Modus ersetzt NLB die tatsächliche MAC-Adresse jedes Servers im Cluster durch eine gemeinsame NLB-MAC-Adresse. Üblicherweise liegt etwas im Bereich 02bf:xxxx:xxxx. Alle Knoten im NLB-Cluster wissen, was die NLB-VIP- und MAC-Adresse ist. Datenverkehr, der ARP-Antworten (Address Resolution Protocol) von NLB-Knoten enthält, wird *nie* von der MAC- oder IP-Adresse des NLB *stammen*. Stattdessen verwenden NLB-Knoten eine zugewiesene MAC-Adresse, die auf der Host-ID des Mitglieds basiert. Die MAC-Adresse befindet sich normalerweise im Bereich 0201:xxxx:xxxx, 0202, 0203 usw. für jeden Knoten im Cluster. Dies ist die Quelladresse im Layer-2-Header (L2), wenn eine ARP-Anfrage beantwortet wird. Die ARP-Headerinformationen enthalten jedoch die NLB-MAC-Adresse. Hosts, die der NLB-VIP-Adresse entsprechen möchten, senden daher Datenverkehr an die NLB-MAC-Adresse.

IEEE-konforme Switches (L2-Geräte) erstellen ihre MAC-Adresstabelle basierend auf dem L2-

Quell-Header und nicht auf den Informationen in der ARP-Nutzlast. Das bedeutet, dass der an den NLB-Cluster weitergeleitete Datenverkehr an die NLB-MAC-Adresse gesendet wird, die nie die Quelle des Datenverkehrs ist. Daher wird Datenverkehr, der für die NLB-MAC-Adresse bestimmt ist, als unbekannter Unicast überflutet.

Vorsicht: Im Unicast-Modus setzt die NLB für die Bereitstellung von clustergebundenen Paketen auf unbekannte Unicast-Flooding. *Der Unicast-Modus funktioniert nicht auf Servern der UCS B-Serie, wenn sich der FI im End-Host-Modus befindet, da unbekannte Unicast-Frames nicht wie von diesem Modus gefordert überflutet werden.* Weitere Informationen zum L2-Weiterleitungsverhalten des UCS im End-Host-Modus finden Sie unter [Cisco Unified Computing System Ethernet Switching Mode](#).

Multicast-/Multicast-IGMP-Modus

Der Multicast-Modus weist der Multicast-MAC-Adresse des Clusters die virtuelle IP-Adresse der Unicast-IP-Adresse der IANA (Assigned Numbers Authority) zu (03xx.xxxx.xxxx). IGMP-Snooping registriert diese Adresse nicht dynamisch, was zu einer Überflutung des NLB-Datenverkehrs im VLAN als unbekanntes Multicast führt.

Der Multicast-IGMP-Modus weist der virtuellen IP-Adresse des Clusters und einer Multicast-MAC-Adresse im IANA-Bereich (01:00:5E:XX:XX:XX) eine Zuweisung zu. Die geclusterten Knoten senden IGMP-Mitgliedschaftsberichte für die konfigurierte Multicast-Gruppe. Daher füllt das FI seine IGMP-Snooping-Tabelle dynamisch auf, um auf die geclusterten Server zu zeigen.

Die Verwendung des Multicast-IGMP-Modus bietet einen kleinen betrieblichen Vorteil, da Statusinformationen (über IGMP-Mitgliedschaftsberichte und IGMP-Snooping) zu den interessierten L2-Ports sowohl für den Upstream- als auch für den Downstream-Modus beibehalten werden können. Ohne die Optimierung von IGMP-Snooping ist die NLB für die Bereitstellung an den Cluster über den designierten Broadcast-/Multicast-Empfänger auf unbekannte Multicast-Flooding im NLB-VLAN angewiesen. Bei Versionen, die nach UCS Version 2.0 veröffentlicht werden, wird der designierte Broadcast-/Multicast-Empfänger auf VLAN-Basis ausgewählt.

Vorsicht: Unabhängig von der gewählten Version des Multicast-Modus erfordert die NLB-VIP-Adresse einen statischen ARP-Eintrag auf dem Upstream-Gerät. Dies ist in der Regel die Switched Virtual Interface (SVI) für das VLAN. Dies ist eine Problemumgehung, da die ARP-Antworten der NLB-Knoten eine Multicast-MAC-Adresse enthalten. Gemäß RFC 1812 sollten ARP-Antworten, die eine Multicast-MAC-Adresse enthalten, ignoriert werden. Daher kann die VIP-MAC-Adresse auf RFC 1812-konformen Geräten nicht dynamisch abgerufen werden.

Eine Zusammenfassung der erforderlichen Schritte zur Unterstützung von NLB im Multicast-IGMP-Modus finden Sie hier:

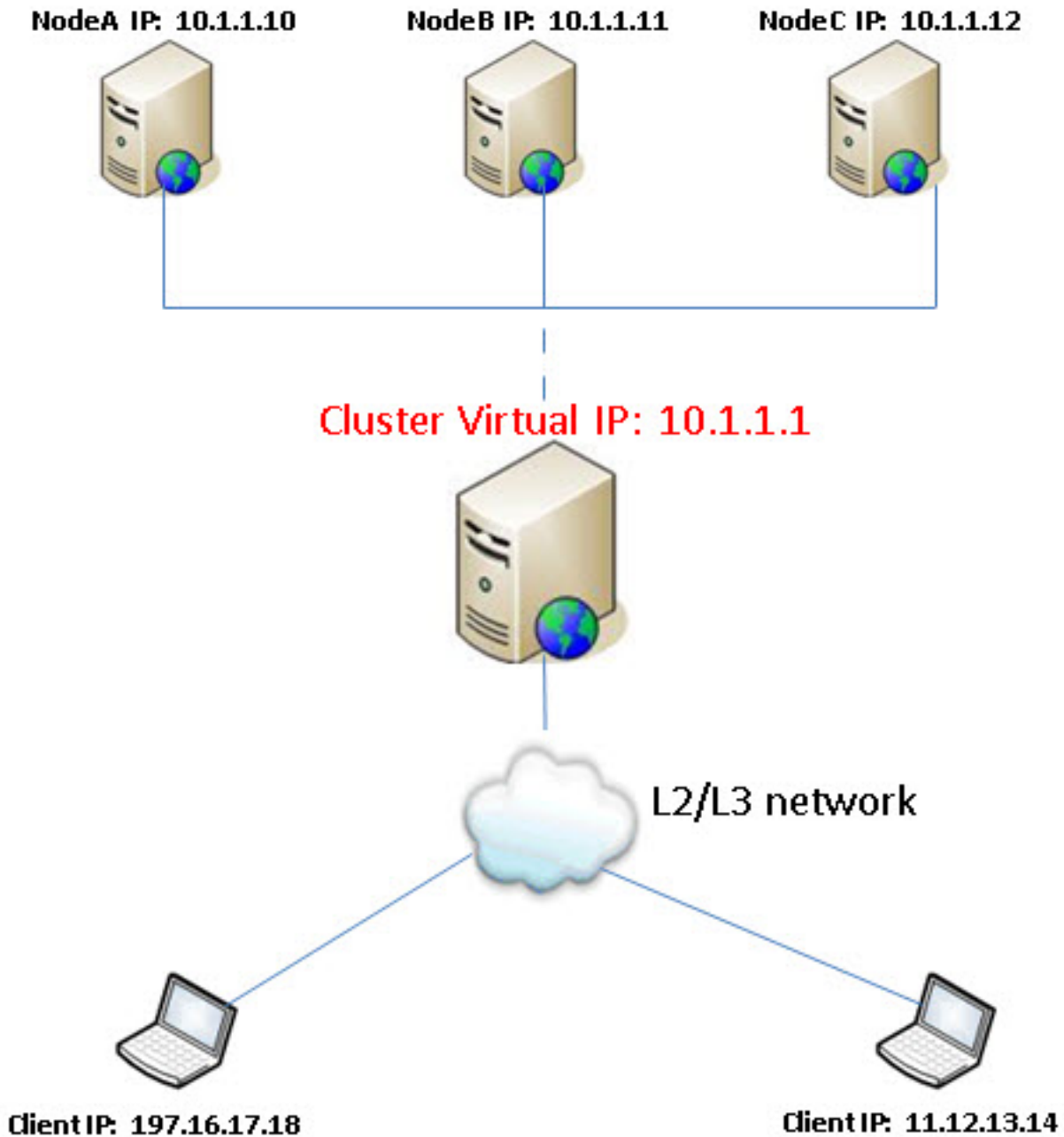
1. Statische ARP-Einträge für virtuelle NLB-IP-Adressen befinden sich in der Regel in der VLAN-SVI. Wenn Sie Hot Standby Router Protocol (HSRP) oder First Hop Redundancy Protocol (FHRP) verwenden, stellen Sie sicher, dass beide Geräte über den statischen ARP-Eintrag verfügen.
2. Ein IGMP-Snooping-Abfrager im NLB-VLAN. In Versionen nach UCS Version 2.1 wird die

Snooping Querier-Funktionalität in UCS Manager unterstützt.

3. IGMP-Snooping muss auf allen Switches aktiviert werden, einschließlich des UCS. Beachten Sie, dass bei den meisten Plattformen, zu denen das UCS gehört, IGMP-Snooping standardmäßig aktiviert ist.

Tipp: Diese Konfigurationsleitfäden gelten für Cisco Switches. Sie enthalten Details zur Implementierung verschiedener Microsoft NLB-Modi.

Eine grundlegende Konfiguration des NLB, d. h. die Knoten können virtuelle Systeme (VMs) oder Bare-Metal-Installation des Windows Server-Betriebssystems sein, ist in diesem Diagramm dargestellt.



NLB VLAN 10 mit dem IP-Subnetz 10.1.1.0 /24 Die MAC-Adresse wird aus Gründen der Kürze gekürzt.

NLB VIP (MAC = 01, IP = 10.1.1.1)

NODE-A (MAC = AA, IP = 10.1.1.10)

NODE-B (MAC = BB, IP = 10.1.1.11)

NODE-C (MAC = CC, IP = 10.1.1.12)

Microsoft NLB-Datenfluss

Der statische ARP-Eintrag auf der Upstream-Switch-SVI zeigt auf die VIP-Adresse 10.1.1.1 bis MAC 01.

Microsoft NLB-Knoten senden den IGMP-Mitgliedschaftsbericht. Die IGMP-Snooping-Tabelle kann 30 bis 60 Sekunden dauern, bis sie ausgefüllt wird.

Bei IGMP-Snooping und dem VLAN-Querier wird die Snooping-Tabelle mit der NLB-MAC-Adresse und Gruppen gefüllt, die auf die richtigen L2-Ports zeigen.

1. Externe Clients senden Datenverkehr an die NLB VIP-Adresse 10.1.1.1.
2. Dieser Datenverkehr wird an die VLAN 10-Schnittstelle weitergeleitet, die einen statischen ARP-Eintrag verwendet, um die MAC-Adresse (01) des NLB VIP aufzulösen.
3. Da es sich um ein Multicast-Frame-Ziel handelt, wird es pro IGMP-Snooping-Tabelle weitergeleitet.
4. Der Frame erreicht alle NLB-Knoten (Knoten A,B,C).
5. Der NLB-Cluster verwendet seinen Lastenausgleichsalgorithmus, um zu bestimmen, welcher Knoten den Datenfluss bedient. Nur ein Knoten reagiert.

Weitere Informationen finden Sie in diesen Dokumenten:

- [Konfigurationsbeispiel für Catalyst Switches für Microsoft-Netzwerk-Lastenausgleich](#)
- [Microsoft-Netzwerk-Lastenausgleich für Nexus 7000 - Konfigurationsbeispiel](#)

Besondere Überlegungen für Nexus 1000v

Der Nexus 1000v unterstützt nur den Unicast-Microsoft NLB-Modus. Bei Bereitstellungen des Nexus 1000v mit dem UCS funktioniert der Multicast-IGMP-Modus nur, wenn Sie das Snooping auf dem Nexus 1000v deaktivieren. Anschließend werden Microsoft NLB-Pakete in diesem VLAN als unbekanntes Multicast überflutet.

Um die Auswirkungen von Überschwemmungen so gering wie möglich zu halten,

1. Deaktivieren Sie Snooping nur für dieses VLAN auf dem Nexus 1000v.
2. Verwenden Sie ein dediziertes VLAN für Microsoft NLB-Datenverkehr.

Überprüfen

Die Prüfverfahren für die in diesem Dokument beschriebenen Konfigurationsbeispiele sind in den entsprechenden Abschnitten beschrieben.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Technischer Überblick zum Netzwerk-Lastenausgleich](#)
- [Diskussion in der Cisco Support Community](#)
- [Cisco Unified Computing System Ethernet-Switching-Modi](#) (Suche nach Microsoft Network Load Balancing)
- [Technischer Support und Dokumentation - Cisco Systems](#)