

Konfiguration des Citrix NetScaler Load Balancer für Cisco Unified Intelligence Center (CUIC)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm](#)

[Zugriff auf den Unified Intelligence Center-Bericht über HTTP/HTTPS](#)

[Konfiguration](#)

[Systemeinstellungen](#)

[Lizenz hochladen](#)

[Netzwerkkonfiguration](#)

[Subnetz-IP erstellen](#)

[VIP erstellen](#)

[Routen erstellen](#)

[Konfiguration des HTTPS-Load Balancing](#)

[Monitore erstellen](#)

[Monitor für HTTP-Port 80 erstellen](#)

[Server erstellen](#)

[Services erstellen](#)

[Virtueller Server erstellen](#)

[Persistenzgruppen erstellen](#)

[Referenz](#)

Einführung

In diesem Dokument werden die Konfigurationsschritte zur Verwendung des Citrix NetScaler Load Balancer für CUIC beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CUIC
- Citrix Netscaler

Verwendete Komponenten

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

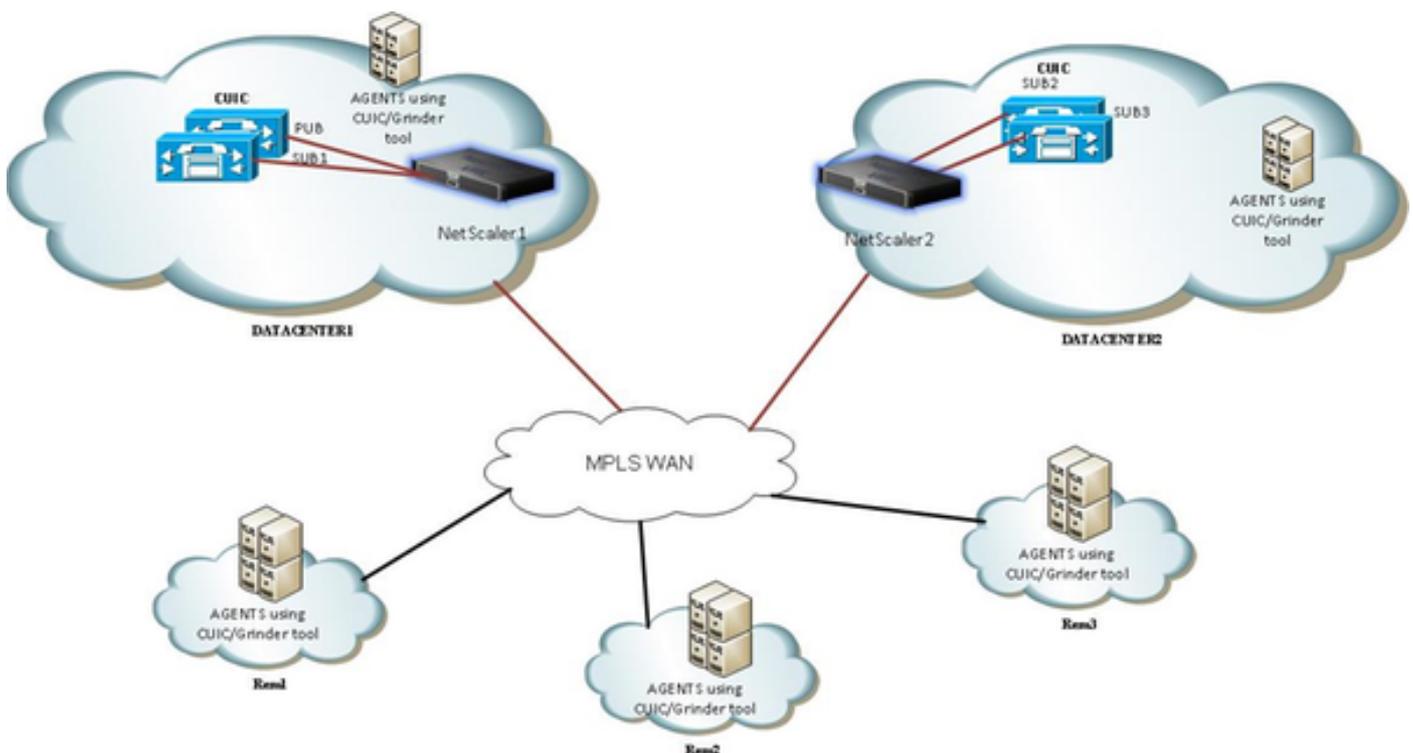
- CUIC 11.0(1)
- Citrix NS: Appliance Edition: Citrix NetScaler 1000v (10.1 Build 125.8)

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

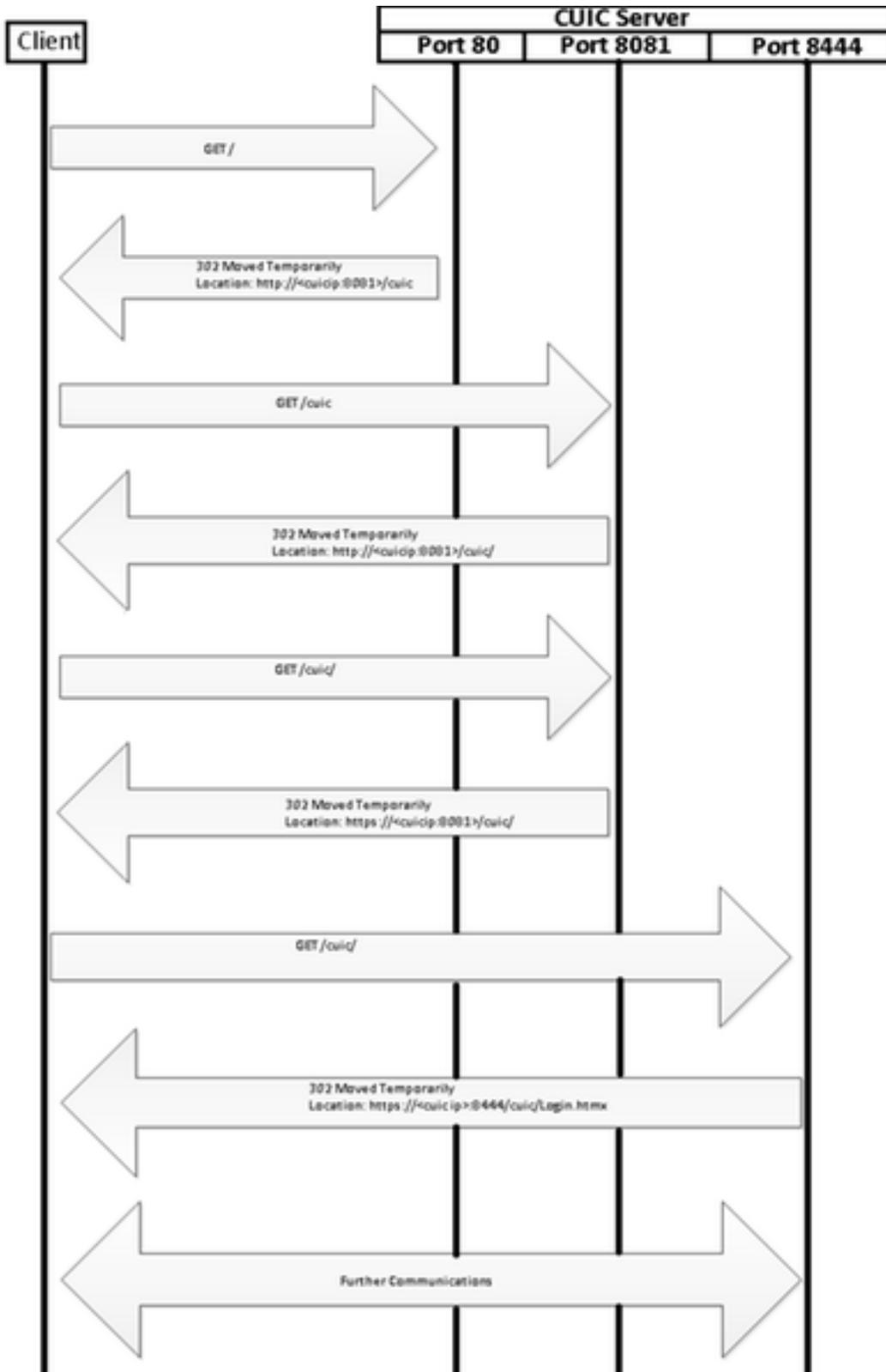
CUIC ist eine flexible und intuitive webbasierte Reporting-Plattform, die Ihnen Berichte zu relevanten Geschäftsdaten liefert. Mit CUIC können Sie ein umfassendes Informationsportal erstellen, in dem Berichte und Dashboards von Contact Centern entwickelt und im gesamten Unternehmen gemeinsam genutzt werden. In großen CUIC-Bereitstellungen wird der Citrix NetScaler 1000v (Load Balancer) zum Lastenausgleich von CUIC Hypertext Transfer Protocol (HTTP)- und Hypertext Transfer Protocol Secure (HTTPS)-Datenverkehr verwendet.

Netzwerkdiagramm



Zugriff auf den Unified Intelligence Center-Bericht über HTTP/HTTPS

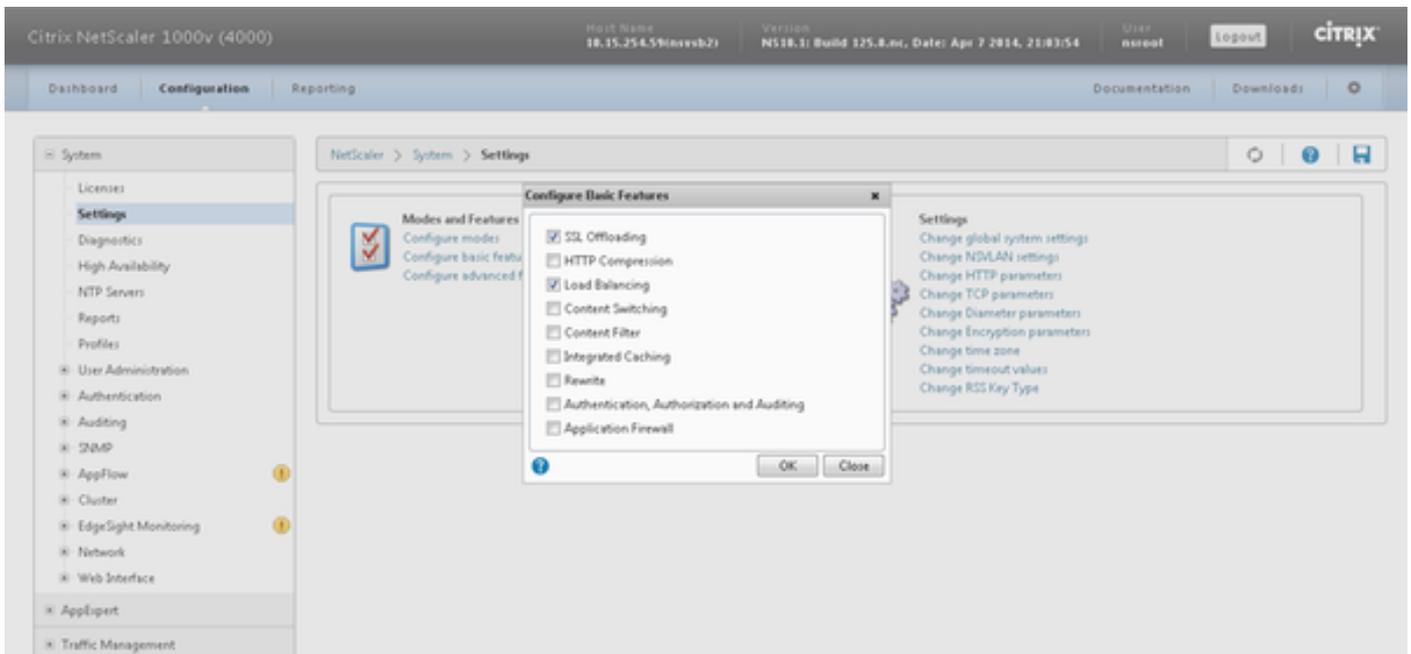
Wenn HTTP im CUIC-Server deaktiviert ist, ist dies der HTTP-Fluss zu verschiedenen Ports.



Konfiguration

Systemeinstellungen

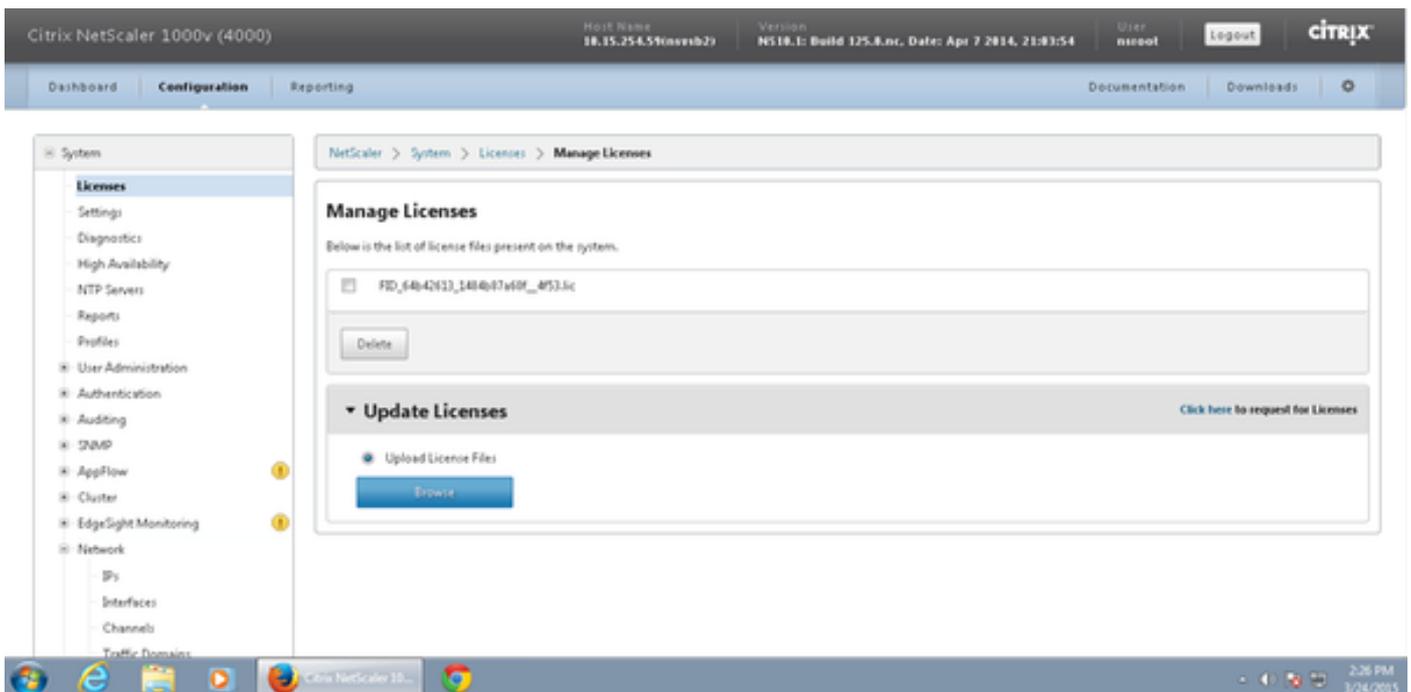
Konfiguration > Einstellungen > Grundlegende Funktionen konfigurieren



Lizenz hochladen

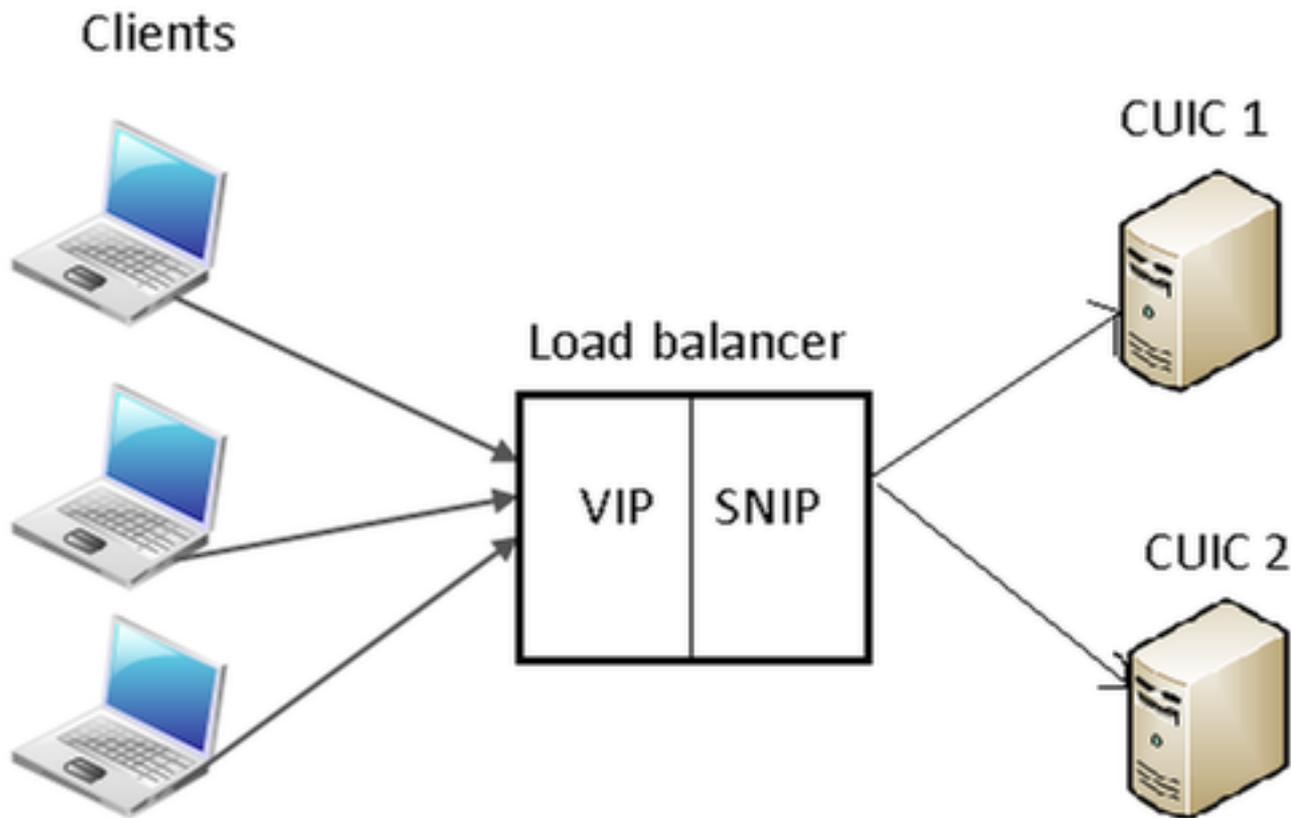
Ohne Lizenz funktioniert SSL möglicherweise nicht.

Navigieren Sie zu **System > Lizenzen > Lizenzen verwalten > Lizenz aktualisieren**.



Netzwerkkonfiguration

Clients kommunizieren mit dem Load Balancer über Virtual IP (VIP), und der Load Balancer kommuniziert über seine Subnet-IP (SNIP) mit CUIC.



Klicken Sie auf **System > Netzwerk > IPs > IPv4s**

NetScaler > System > Network > IPs > IPv4s

IPv4s | IPv6s

Add... Open... Remove Action Search

IP Address	Traffic Domain ID	State	Type	Mode	ARP	ICMP	Virtual Server
10.15.254.59	0	Enabled	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
10.10.2.58	0	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
10.10.2.61	0	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED

25 Per Page 1 - 3 of 3 1

Subnetz-IP erstellen

Schritt 1: Klicken Sie auf **Hinzufügen**, um die **IP-Adresse** hinzuzufügen, und wählen Sie **Typ** als **Subnetz-IP** aus.

Schritt 2: Klicken Sie auf **Erstellen**, um die gewünschte IP-Adresse zu erstellen.

Configure IP

IP Address: 10 . 10 . 2 . 58 Netmask: 255 . 255 . 255 . 0

Type: Subnet IP Mode: Active

Virtual Router ID: ICMP Response*: NONE

ARP Response*: NONE Traffic Domain ID:

Options

ARP ICMP Virtual Server Dynamic Routing

Host Route

Enable

Gateway IP: Metric:

OSPF LSA Type

TYPE5 TYPE1 Area:

Vserver RHI Level

NONE ONE_VSERVER ALL_VSERVERS

Application Access Controls

Enable Management Access control to support the below listed applications.

?

Create Close

VIP erstellen

Schritt 1: Klicken Sie auf **Hinzufügen**, um die **IP-Adresse** hinzuzufügen, und wählen Sie **Typ** als **virtuelle IP** aus.

Schritt 2: Klicken Sie auf **Erstellen**, um die gewünschte IP-Adresse zu erstellen.

Configure IP

IP Address: 10 . 10 . 2 . 61 Netmask: 255 . 255 . 255 . 255

Type: Virtual IP Mode: Active

Virtual Router ID: ICMP Response*: NONE

ARP Response*: NONE Traffic Domain ID:

Options

ARP ICMP Virtual Server Dynamic Routing

Host Route

Enable

Gateway IP: 0 . 0 . 0 . 0 Metric: 0

OSPF LSA Type

TYPE5 TYPE1 Area:

Vserver RHI Level

NONE ONE_VSERVER ALL_VSERVERS

Application Access Controls

Enable Management Access control to support the below listed applications.

?

Create Close

Routen erstellen

Erstellen Sie ggf. Routen zum Netzwerk, von dem aus HTTP-/HTTPS-Anforderungen an den Load Balancer kommen.

Configure Route

Network: 10 . 3 . 4 . 0

Netmask: 255 . 255 . 255 . 0

Traffic Domain ID: [Dropdown]

NULL Route: Yes No

Gateway: 10 . 10 . 2 . 1

Distance: 1

Weight: 1

Cost: 0

Route Advertisement

Global State DISABLED

Over-ride Global

Protocol

OSPF RIP BGP ISIS

Monitored Static Route

Buttons: [Create] [Close]

Klicken Sie auf **Erstellen**, um die gewünschte Route zu erstellen.

Konfiguration des HTTPS-Load Balancing

Um Einträge für virtuelle Server zu erstellen, muss ein Port in CUIC für jeden Port überwacht werden (HTTP-Ports 80, 8081 und HTTPS-Port 844). Jeder virtuelle Servereintrag ist die IP- und Port-Kombination, die den HTTP-Datenverkehr vom Client (Zugriff auf den CUIC-Bericht) empfängt.

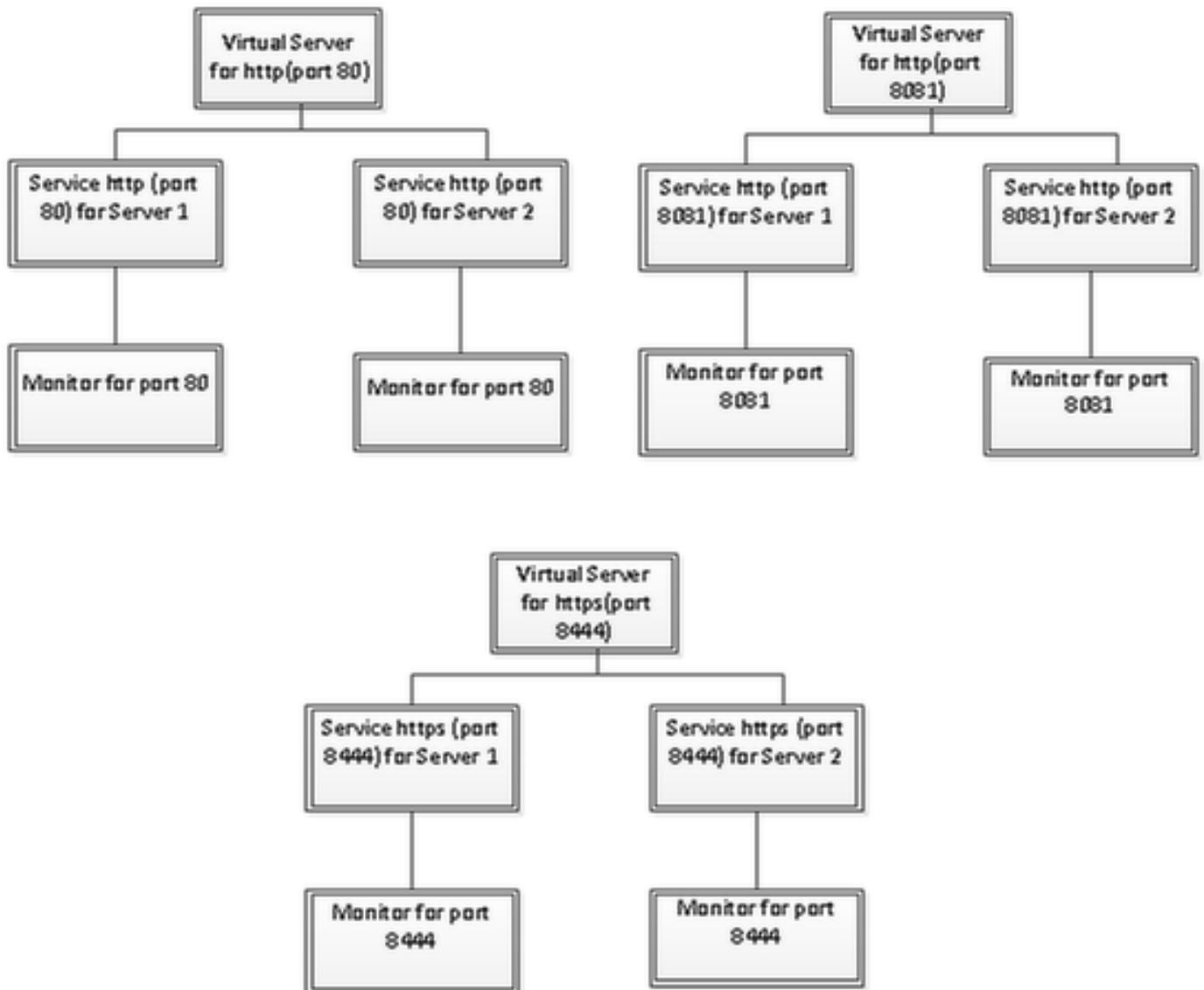
Virtuelle Server müssen mit Servern verknüpft werden, um den Lastverkehr zu senden. Um den Status der Server-Monitore zu überprüfen, müssen diese jedem Server zugewiesen werden. Über die Monitore erkennt die Last den Serverausfall (CUIC) und verteilt den eingehenden Datenverkehr an Server, die einwandfrei arbeiten, um die Anfragen zu erfüllen.

Die Verknüpfung ist Virtual Server->Service- und Server->Monitor.

Zusammenfassung der Konfigurationen:

- Monitore erstellen
- Server erstellen
- Erstellen von Services mit Serverzuordnung
- Verknüpfen Sie jeden Service mit den entsprechenden Monitoren
- Virtuelle Server erstellen
- Verknüpfen der entsprechenden Services mit virtuellen Servern
- Persistenzgruppe erstellen und virtuelle Server hinzufügen

Dieses Bild zeigt drei Einträge für virtuelle Server und deren Zuordnung.



Monitore erstellen

Navigieren Sie zu **Datenverkehrsmanagement > Load Balancing > Monitors**.

NetScaler > Traffic Management > Load Balancing > Monitors

Name	State	Type
ping-default	Enabled	PING
tcp-default	Enabled	TCP
arp	Enabled	ARP
nd6	Enabled	ND6
ping	Enabled	PING
tcp	Enabled	TCP

Um einen Monitor zu erstellen, navigieren Sie zu **Traffic Management > Load Balancing > Monitors**, und klicken Sie auf die Schaltfläche **Add (Hinzufügen)**.

Es werden drei Arten von Monitoren für die Ports 80, 8081 und 844 erstellt.

Monitor für HTTP-Port 80 erstellen

Wählen Sie **Type** als **TCP** (Typ als **TCP**) und geben Sie **Interval** (Intervall), **Response Time-Out** (Reaktionszeit), **Down Time** (Abbruchzeit), **Retries** (Wiederholungen) usw. entsprechend an. Klicken Sie auf **Erstellen**, um den Monitor zu erstellen. Für HTTPS müssen zwei Monitore erstellt werden (einer pro Server).

Create Monitor

Name* Type*

Standard Parameters | Special Parameters

Interval Destination IP IPv6

Response Time-out Destination Port

Down Time Dynamic Time-out

Deviation Dynamic Interval

Retries Resp Time-out Threshold

SNMP Alert Retries Action

Success Retries Custom Header

Failure Retries Treat back slash as escape character

Enabled Reverse

LRTM (Least Response Time using Monitoring) Transparent Secure IP Tunnel

TOS TOSId

Create Monitor [X]

Name* Type* HTTP

Standard Parameters | Special Parameters

Interval Destination IP IPv6

Response Time-out Destination Port

Down Time Dynamic Time-out

Deviation Dynamic Interval

Retries Resp Time-out Threshold

SNMP Alert Retries Action

Success Retries Custom Header

Failure Retries Treat back slash as escape character

Enabled Reverse

LRTM (Least Response Time using Monitoring)

TOS TOSId Net Profile

Transparent Secure IP Tunnel

Help [Create] [Close]

Konfigurieren Sie für die HTTPS-Typüberwachung den Abschnitt für spezielle Parameter. Dieser Monitor meldet den Erfolg, wenn die Antwort auf die HTTP-Anfrage 200 oder 302 beträgt.

Wenn HTTP in CUIIC deaktiviert ist, wird erwartet, dass 302 ansonsten 200 Geräte verwendet werden. Um sowohl die Situationen zu bewältigen, sind 200 und 302 enthalten.

Configure Monitor

Name* Type HTTP

Standard Parameters | Special Parameters

HTTP Request

Treat back slash as escape character

Response Codes

Create Monitor

Name* Type* HTTP-ECV

Standard Parameters | Special Parameters

Interval Destination IP IPv6

Response Time-out Destination Port

Down Time Dynamic Time-out

Deviation Dynamic Interval

Retries Resp Time-out Threshold

SNMP Alert Retries Action

Success Retries Custom Header

Failure Retries Treat back slash as escape character

Enabled Reverse

LRTM (Least Response Time using Monitoring)

TOS TOSId Net Profile

Transparent Secure IP Tunnel

Konfigurieren Sie für die HTTPS-Typüberwachung den Abschnitt für spezielle Parameter. Dieser Monitor meldet nur dann Erfolg, wenn die Antwort eine Zeichenfolge **In Service** enthält.

Configure Monitor ✕

Name* Type HTTP-ECV

Standard Parameters | Special Parameters

Send String

```
GET https://10.10.2.46:8444/cuic/probe
```

Treat back slash as escape character

Receive String

```
In Service
```

Treat back slash as escape character

Create Monitor



Name*

Type*

Standard Parameters

Special Parameters

Interval

Response Time-out

Down Time

Deviation

Retries

SNMP Alert Retries

Success Retries

Failure Retries

Enabled Reverse

LRTM (Least Response Time using Monitoring)

TOS TOSId

Destination IP IPv6

Destination Port

Dynamic Time-out

Dynamic Interval

Resp Time-out Threshold

Action

Custom Header

Treat back slash as escape character

Net Profile

Transparent

Secure

IP Tunnel

Help

Create

Close

Create Monitor x

Name* Type*

Standard Parameters Special Parameters

Send String

Treat back slash as escape character

Receive String

Treat back slash as escape character

[Help](#)

Server erstellen

Server stellt einen CUIC-Knoten dar. Für jeden vom Load Balancer bereitgestellten CUIC-Knoten ist ein Servereintrag erforderlich.

NetScaler > Traffic Management > Load Balancing > Servers Refresh Help Save

Search

Name	State	IPAddress / Domain	Traffic Domain ID
ATL-CUIC-SUB4	Enabled	10.10.2.46	0
ATL-CUIC-SUB5	Enabled	10.10.2.47	0

25 Per Page 1 - 2 of 2 1

Um einen Server zu erstellen, navigieren Sie zu **Traffic Management > Load Balancing > Servers**, und klicken Sie auf die Schaltfläche **Add (Hinzufügen)**.

Create Server ✕

Server Name*

IP Address Domain Name

IPAddress* IPv6

Traffic Domain ID

Translation IP Address

Translation Mask

Resolve Retry (secs)

IPv6 Domain

Enable after Creating

Comments

? Create Close

Create Server ✕

Server Name*

IP Address Domain Name

IPAddress* IPv6

Traffic Domain ID

Translation IP Address

Translation Mask

Resolve Retry (secs)

IPv6 Domain

Enable after Creating

Comments

? Create Close

Services erstellen

Um einen Monitor zu erstellen, navigieren Sie zu **Datenverkehrsmanagement > Load Balancing > Services**, und klicken Sie auf **Hinzufügen**.

NetScaler > Traffic Management > Load Balancing > Services

Buttons: Add..., Open..., Remove, Action

Search

Name	State	IP Address/Domain Name	Traffic Domain ID	Port	Protocol	Max Clients	Max Requests	Cache Type
cuic-http80-sub4	Up	10.10.2.46	0	80	HTTP	0	0	SERVER
cuic-http80-sub5	Up	10.10.2.47	0	80	HTTP	0	0	SERVER
cuic-http80801-sub4	Up	10.10.2.46	0	8081	HTTP	0	0	SERVER
cuic-http80801-sub5	Up	10.10.2.47	0	8081	HTTP	0	0	SERVER
cuic-https-sub4	Up	10.10.2.46	0	8444	SSL_BRIDGE	0	0	SERVER
cuic-https-sub5	Up	10.10.2.47	0	8444	SSL_BRIDGE	0	0	SERVER

25 Per Page | 1 - 6 of 6 | 1

Wenn keine Monitore zugeordnet sind, wird möglicherweise ein Standardmonitor im konfigurierten Feld angezeigt. Ohne diese zu entfernen, wählen Sie den richtigen Monitor aus der verfügbaren Liste aus (in diesem Bild ist es **cust_tcp**) und klicken Sie auf **Hinzufügen**, um ihn in die konfigurierte Liste zu verschieben. Klicken Sie auf **OK**. Beim nächsten Öffnen dieser Seite wird nur der ausgewählte Monitor angezeigt. Der Standardmonitor wird ausgeblendet. Dies geschieht aus folgenden Gründen: Ein Service muss immer einem überwachten Service zugeordnet werden. Wenn nichts konfiguriert ist, stellt Load Balancer eine Standardeinstellung bereit. Wenn der Benutzer jedoch einen überwachten Modus auswählt, wird der Standardmonitor durch Load Balancer ersetzt.

Configure Service

Service Name*: cuic-http80-sub4 Server*: ATL-CUIC-SUB4 (10.10.2.46)

Protocol*: HTTP Port*: 80

Traffic Domain: 0

Service State: UP Number of Active Clients:

 Enable Health Monitoring AppFlow Logging

Monitors | Policies | Profiles | Advanced | SSL Settings

Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp

Configured

Monitors	Weight	State
cust_tcp	1	<input checked="" type="checkbox"/>

State: UP
 Probes: 68341 Failed [Total: 5614 Current: 0]
 Last Response: Success - TCP syn+ack received.
 Response Time: 0.357 millisec

Comments:

Configure Service

Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP Down Number of Active Clients

Enable Health Monitoring AppFlow Logging

Thresholds

Max Requests	<input type="text" value="0"/>	Max Bandwidth (kbits)	<input type="text" value="0"/>
Max Clients	<input type="text" value="0"/>	Monitor Threshold	<input type="text" value="0"/>

Idle Time-out (secs)

Client Server

Settings

Use Source IP Client Keep-Alive TCP Buffering Compression
 Client IP Header

Comments

Configure Service

Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP Number of Active Clients
 Enable Health Monitoring AppFlow Logging

- Monitors
- Policies
- Profiles
- Advanced
- SSL Settings

Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp

Configured

Monitors	Weight	State
http_8081	1	<input checked="" type="checkbox"/>

State: UP
Probes: 68352 Failed [Total: 5630 Current: 0]
Last Response: Success - HTTP response code 302 received.
Response Time: 0.754 millise

Comments

Help

Configure Service

Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP DOWN Number of Active Clients
 Enable Health Monitoring AppFlow Logging

Thresholds

Max Requests	<input type="text" value="0"/>	Max Bandwidth (kbits)	<input type="text" value="0"/>
Max Clients	<input type="text" value="0"/>	Monitor Threshold	<input type="text" value="0"/>

Idle Time-out (secs)

Client Server

Settings

Use Source IP Client Keep-Alive TCP Buffering Compression

Client IP Header

Comments

Configure Service



Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP DOWN
Number of Active Clients
 Enable Health Monitoring AppFlow Logging

- Monitors
- Policies
- Profiles
- Advanced
- SSL Settings

Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp

Configured

Monitors	Weight	State
cust_sub4_https-ecv	1	<input checked="" type="checkbox"/>

State: UP
Probes: 384901 Failed [Total: 8624 Current: 0]
Last Response: Success - Pattern found in response.
Response Time: 1.463 millisec

Comments

Help

Configure Service

Service Name* Server*

 Protocol* Port*

 Traffic Domain

 Service State UP Number of Active Clients

 Enable Health Monitoring AppFlow Logging

Monitors | Policies | Profiles | **Advanced** | SSL Settings

Thresholds

Max Requests	<input type="text" value="0"/>	Max Bandwidth (kbits)	<input type="text" value="0"/>
Max Clients	<input type="text" value="0"/>	Monitor Threshold	<input type="text" value="0"/>

Idle Time-out (secs)

Client	<input type="text" value="180"/>	Server	<input type="text" value="360"/>
--------	----------------------------------	--------	----------------------------------

Settings

Use Source IP Client Keep-Alive TCP Buffering Compression

Client IP Header

Comments

Virtueller Server erstellen

NetScaler > Traffic Management > Load Balancing > Virtual Servers

Add... Open... Remove Action Search

Name	State	Effective State	IP Address	Traffic Domain ID	Port	Protocol	Method	Persistence	% Health
DC2-CUBC-HTTP	Up	Up	10.10.2.61	0	80	HTTP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN
DC2-CUBC-HTTP8081	Up	Up	10.10.2.61	0	8081	HTTP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN
DC2-CUBC-HTTPS	Up	Up	10.10.2.61	0	8444	SSL_BRIDGE	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN

25 Per Page 1 - 3 of 3 1

Um einen virtuellen Server zu erstellen, navigieren Sie zu **Datenverkehrsmanagement > Load Balancing > Virtuelle Server**, und klicken Sie auf **Hinzufügen**.

Überprüfen Sie die Services, die diesem virtuellen Service zugeordnet werden müssen.

Wählen Sie auf der Registerkarte **Method and Persistence (Methode und Beständigkeit)** **Method** als **geringste Verbindung**, **Persistence** als **SOURCEIP** und **Time-Out** als **40 Minuten** aus. Der Grund hierfür ist, dass die voreingestellte Aktualisierungsrate für historische Berichte auf 30 Minuten festgelegt ist. Sie müssen einen Wert konfigurieren, der größer ist als die Aktualisierungsrate. Wenn Sie eine andere Aktualisierungsrate für Verlaufsberichte konfigurieren, ändern Sie diesen Wert ebenfalls.

Configure Virtual Server (Load Balancing)

Name* IP Address Based IP Pattern Based

Protocol* IP Address*

Network VServer Range Port*

Enable DNS64 Bypass AAAA Requests Traffic Domain ID

State UP AppFlow Logging

Services | Service Groups | Policies | Method and Persistence | **Advanced** | Profiles | SSL Settings

LB Method

Method New Service Startup Request Rate

Increment Interval

Current Method: Round Robin
Reason: Bound service's state changed to UP

Persistence

Persistence Backup Persistence

Time-out (min) Time-out (min)

IPv4 Netmask IPv6 Mask Length

Configure Virtual Server (Load Balancing)

Name* IP Address Based IP Pattern Based

Protocol* IP Address*

Network VServer Range Port*

Enable DNS64 Bypass AAAA Requests Traffic Domain ID

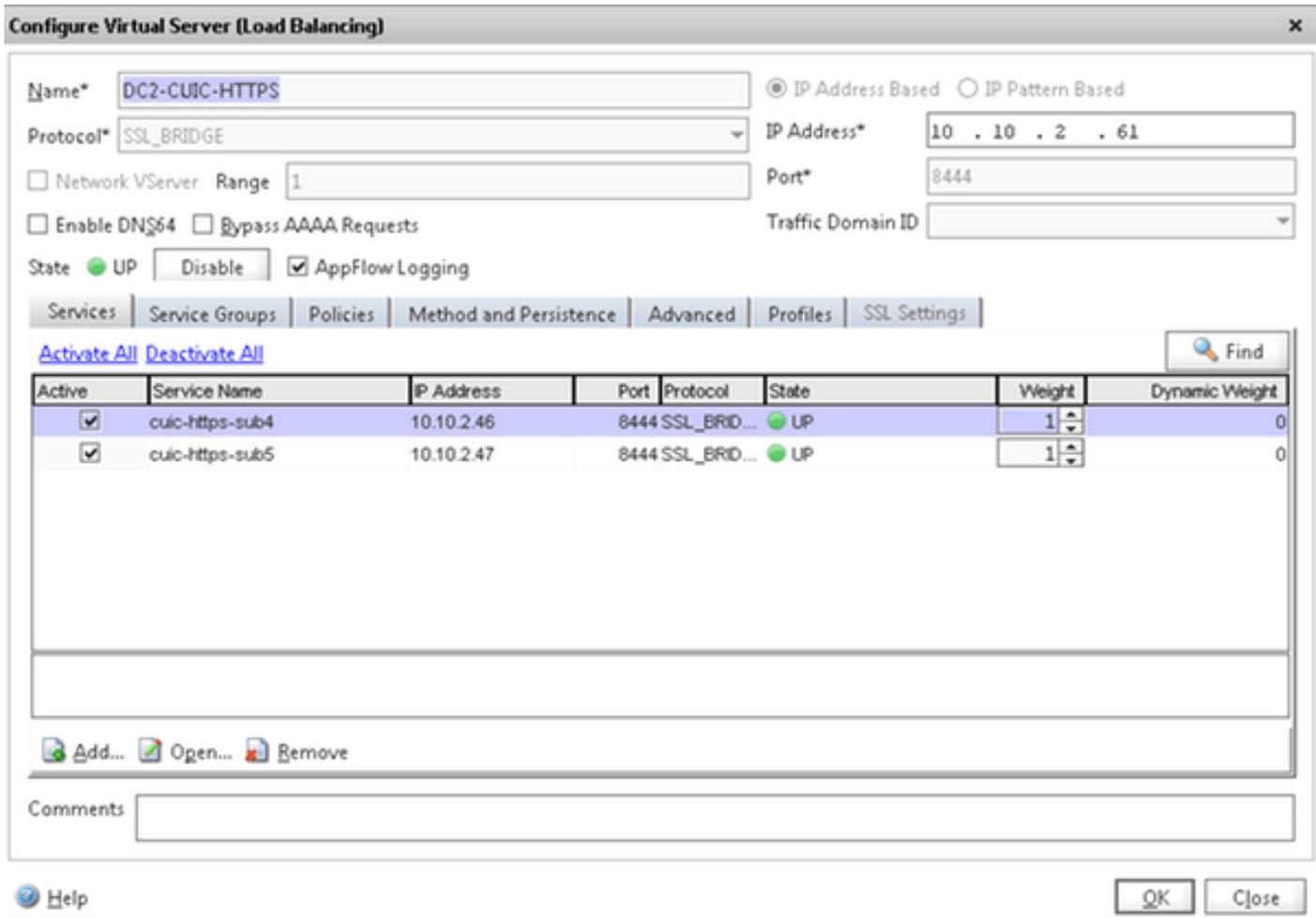
State UP AppFlow Logging

Services | Service Groups | Policies | Method and Persistence | **Advanced** | Profiles | SSL Settings

[Activate All](#) [Deactivate All](#)

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
<input checked="" type="checkbox"/>	cuic-http80801-sub4	10.10.2.46	8081	HTTP	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	0
<input checked="" type="checkbox"/>	cuic-http80801-sub5	10.10.2.47	8081	HTTP	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	0
<input type="checkbox"/>	cuic-http80-sub4	10.10.2.46	80	HTTP	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	
<input type="checkbox"/>	cuic-http80-sub5	10.10.2.47	80	HTTP	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	

Comments



Persistenzgruppen erstellen

Um eine Persistenzgruppe zu erstellen, navigieren Sie zu **Traffic Management > Load Balancing > Persistency Groups**, und klicken Sie auf **Add**.

Wählen Sie **Method** als **geringste Verbindung**, **Persistence** als **SOURCEIP** und **Time-Out** als **40 Minuten aus**. Der Grund hierfür ist, dass die voreingestellte Aktualisierungsrate für historische Berichte auf 30 Minuten festgelegt ist. Sie müssen einen Wert konfigurieren, der größer ist als die Aktualisierungsrate. Wenn Sie eine andere Aktualisierungsrate für Verlaufsberichte konfigurieren, ändern Sie diesen Wert ebenfalls.

Da jeder CUIC-Server drei Ports abhört, müssen alle drei virtuellen Server hier eingeschlossen werden. Wenn ein Client einen HTTP 80-Port anfordert, der bereits an einen bestimmten CUIC-Server gesendet wurde, werden alle Anfragen dieses Clients, die auf Port 8081, 8444 abzielen, an denselben CUIC weitergeleitet.

Configure Persistency Group

Group Name: PgroupDC2

Persistence*: SOURCEIP

IPv4 Netmask: 255 . 255 . 255 . 255

IPv6 Mask Length: 128

Time-out: 40

Backup Persistence*: NONE

Virtual Server Name*

Configured (3)	Remove All
DC2-CUIC-HTTP	-
DC2-CUIC-HTTP8081	-
DC2-CUIC-HTTPS	-

+ Add

OK Close

Referenz

1. <http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html>

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.