Konfiguration und Verifizierung der SDWAN-Integration mit der ACI

Inhalt

Abkürzungen

ACI = Application Centric Infrastructure

EPG = EndPoint Group

L3out - Layer-3-Out

AAR = Application Aware Routing

SLA = Service Level Agreement

Rechenzentrum - Rechenzentrum

WAN: Wide Area Network

SDN - Software Defined Networking

SD DC - Software Defined Data Center

SD WAN = Software Defined Wide Area Network

QoS = Quality of Service

VRF = Virtual Routing and Forwarding

Einleitung

In diesem Dokument werden die Konfigurationsschritte zur Integration der Application Centric Infrastructure (ACI), der Cisco Lösung für Software Defined - Data Center (SD-DC) mit Software Defined - Wide Area Network (SD-WAN) und deren Verifizierung beschrieben.

Software-defined Networking (SDN) wurden erweitert, um bestimmte Netzwerksegmente zu berücksichtigen:

1. Software-Defined - Rechenzentrum (SD-DC)

2. Software-Defined - Wide Area Network (SD-WAN)

Die Lösung von Cisco bietet zuverlässige QoS-Funktionen (Quality of Service) in SD-DC- (Application Centric Infrastructure ACI) und AAR- (Application Aware Routing)/SLA-Profilen (Service Level Agreements) im SD-WAN.

Da immer mehr Kunden eine Integration planen und eine nahtlose Datenverkehrsbehandlung über den Pfad wünschen, hat Cisco eine SD-DC- und SD-WAN-Integration entwickelt.

Die Integration konzentriert sich auf zwei Anwendungsfälle:

1. Datenverkehr von ACI (DC) zu SDWAN (nicht ACI-Außenstelle)
2. Datenverkehr von SDWAN (keine ACI-Außenstelle) zur ACI (DC)

Voraussetzungen

Anforderungen

Da die Integration mit dem SD-WAN über den in der ACI konfigurierten L3-Ausgang erfolgt, muss L3out mit unterstütztem Protokoll konfiguriert werden.

Die Integration erfolgt über ein Managementnetzwerk, sodass eine Erreichbarkeit des Managements zwischen den ACI (APIC-Controller) und vManage erforderlich ist.

Verwendete Komponenten

ACI-Fabric, SDWAN (vManage, vSmart Controller, vEdge)

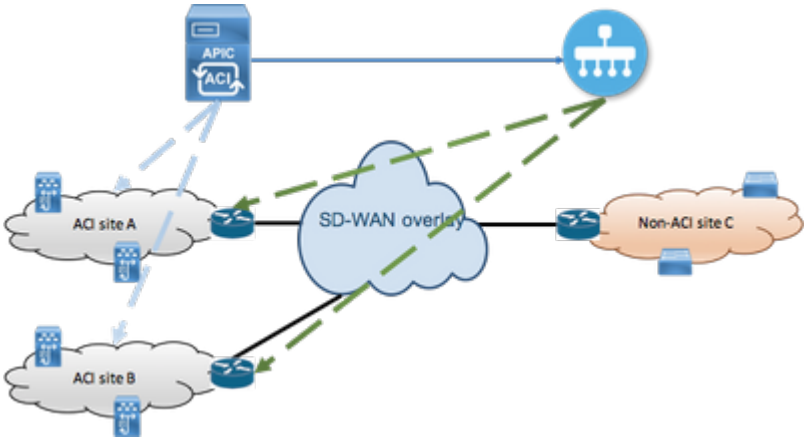
Dieses Dokument basiert auf der ACI-Version 4.2(3l)

Konfiguration

Netzwerkdiagramm

Topologie als Referenz:

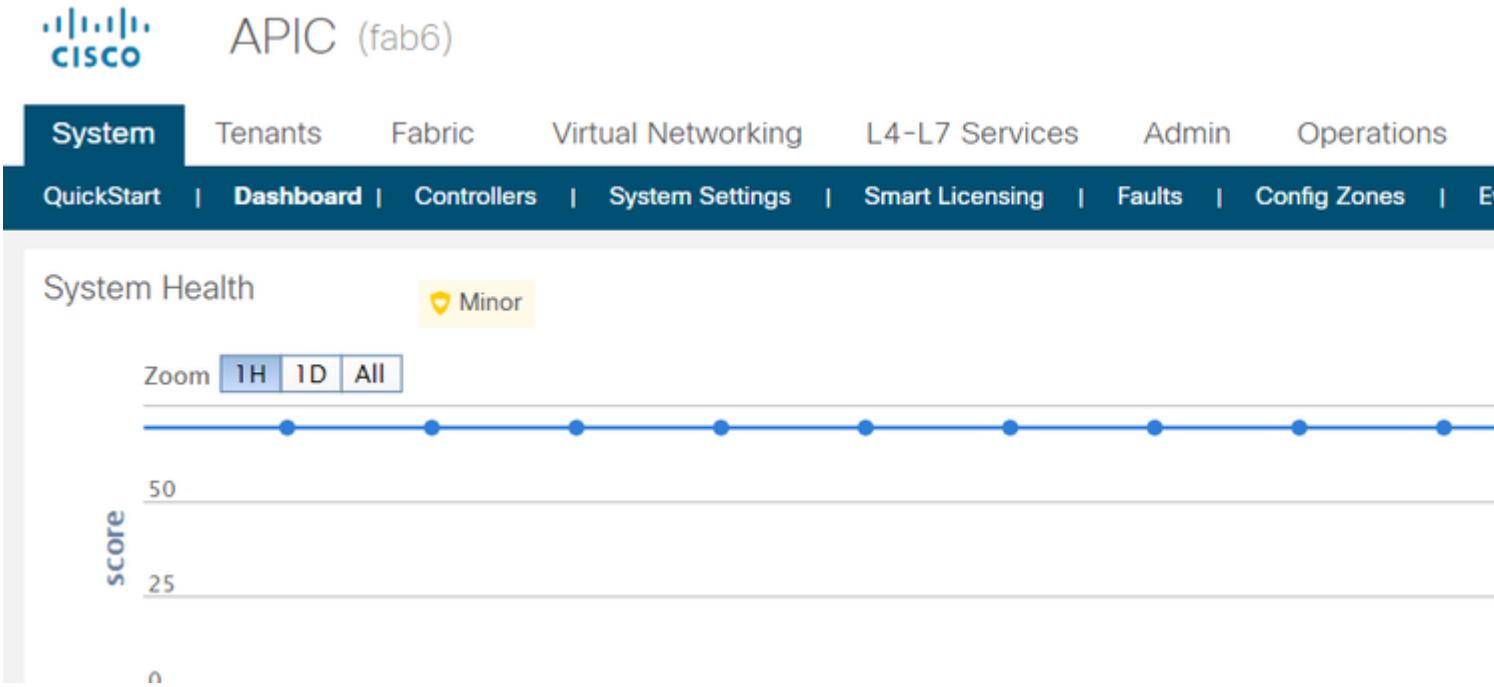
In unserer Topologie betrachten wir nur den ACI-Standort A als Rechenzentrum und den nicht ACI-Standort C als SDWAN-Zweigstelle.



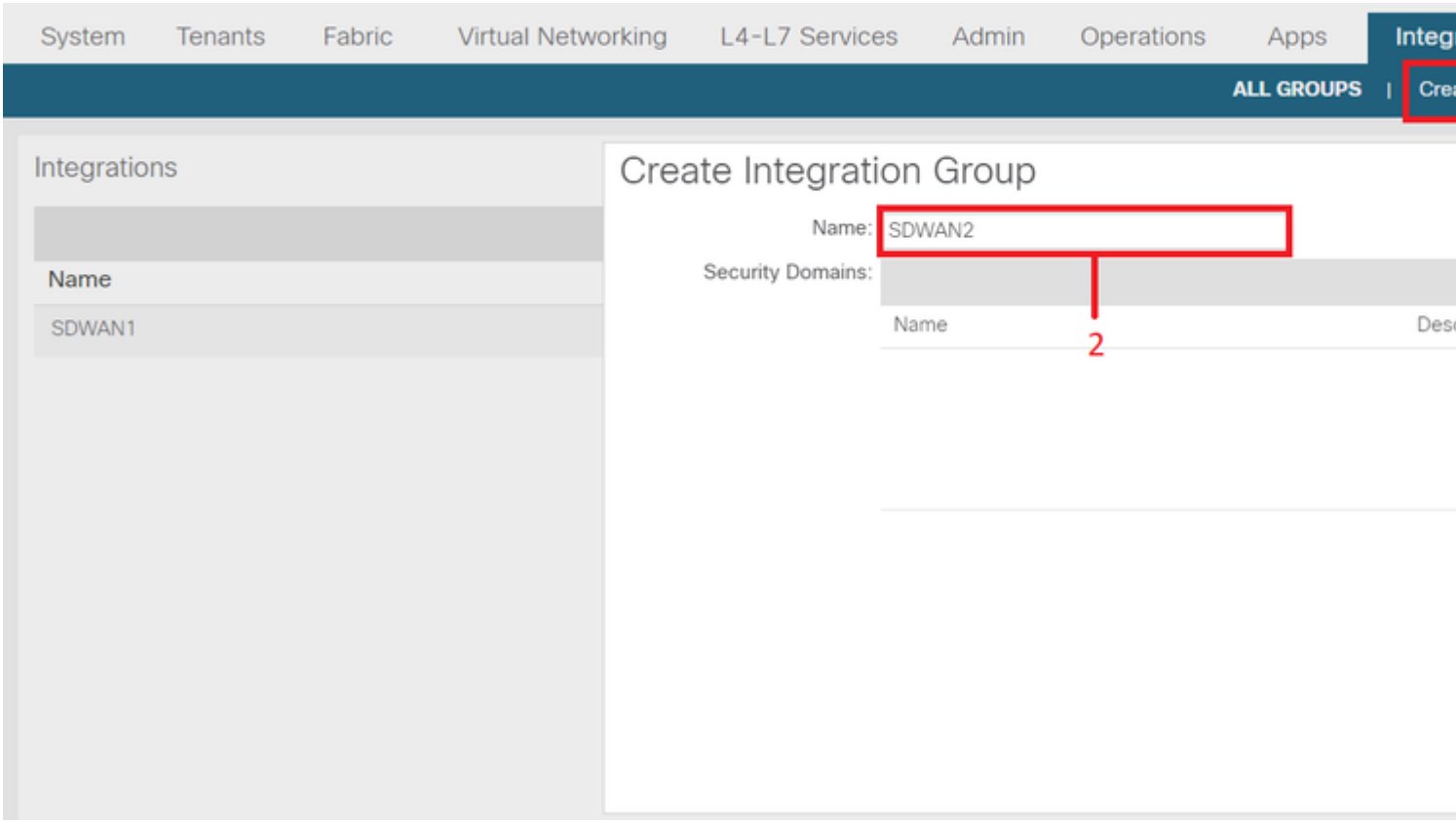
Konfigurationen

Abschnitt A: Konfiguration der Integration

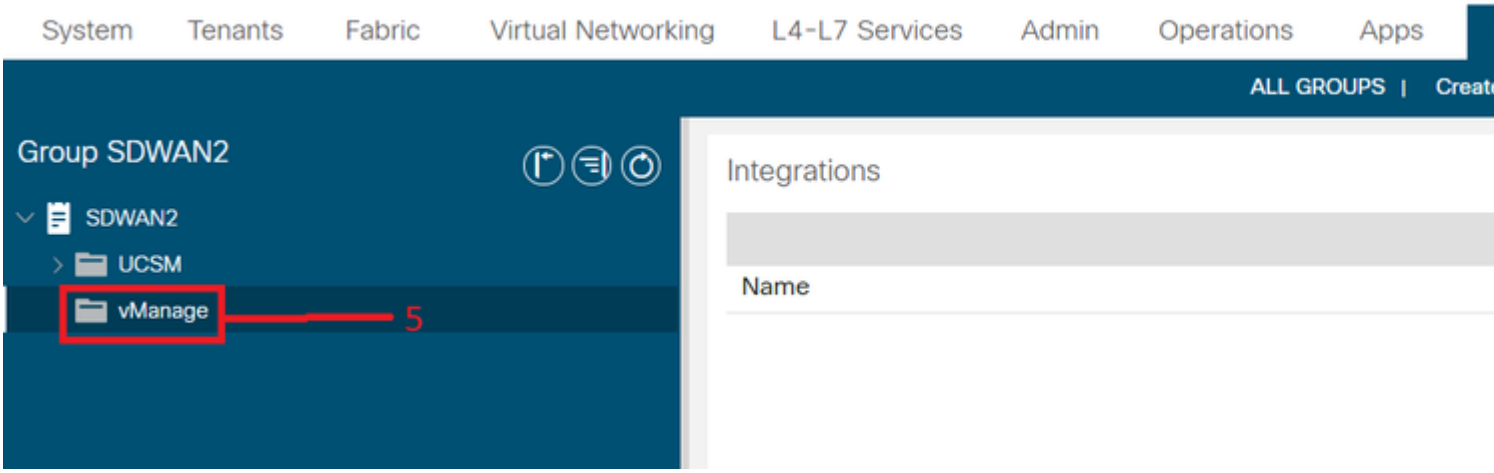
1. Öffnen Sie die grafische Benutzeroberfläche (GUI) des APIC, und navigieren Sie zur Registerkarte **Integrationen** unter der Registerkarte **System**.



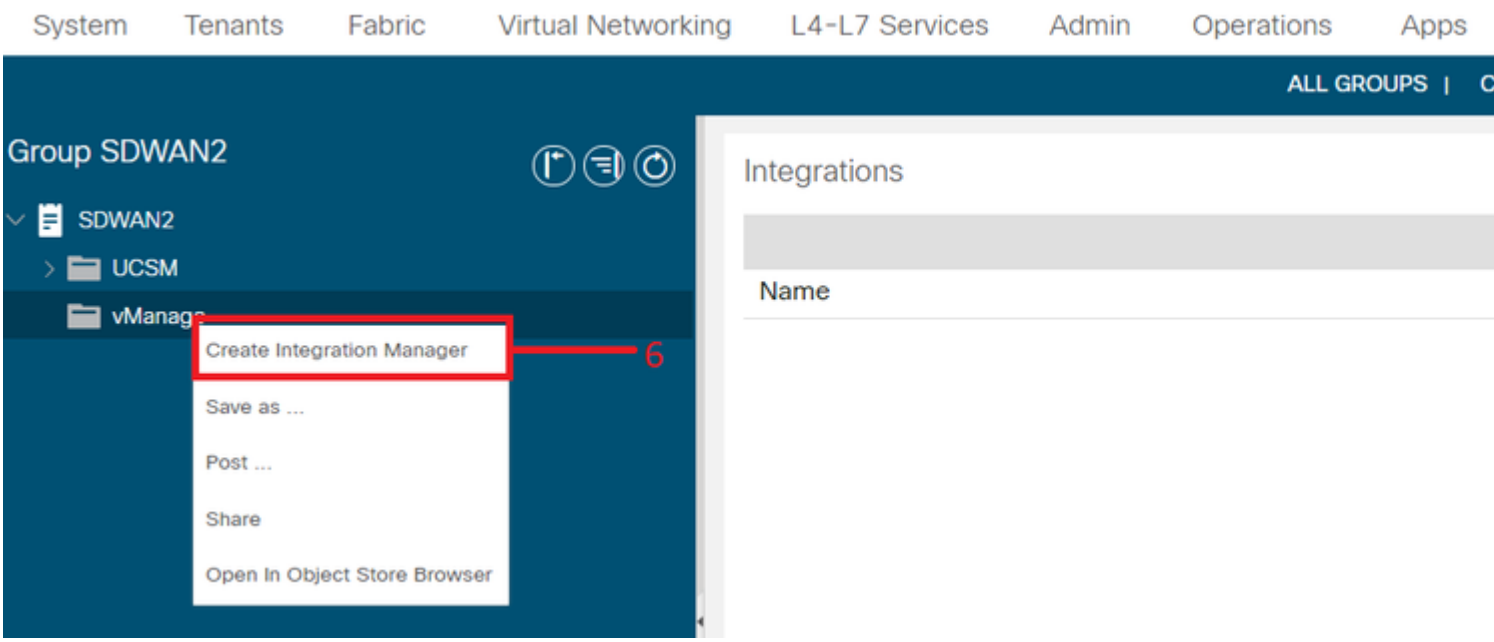
2. Integrationsgruppe erstellen



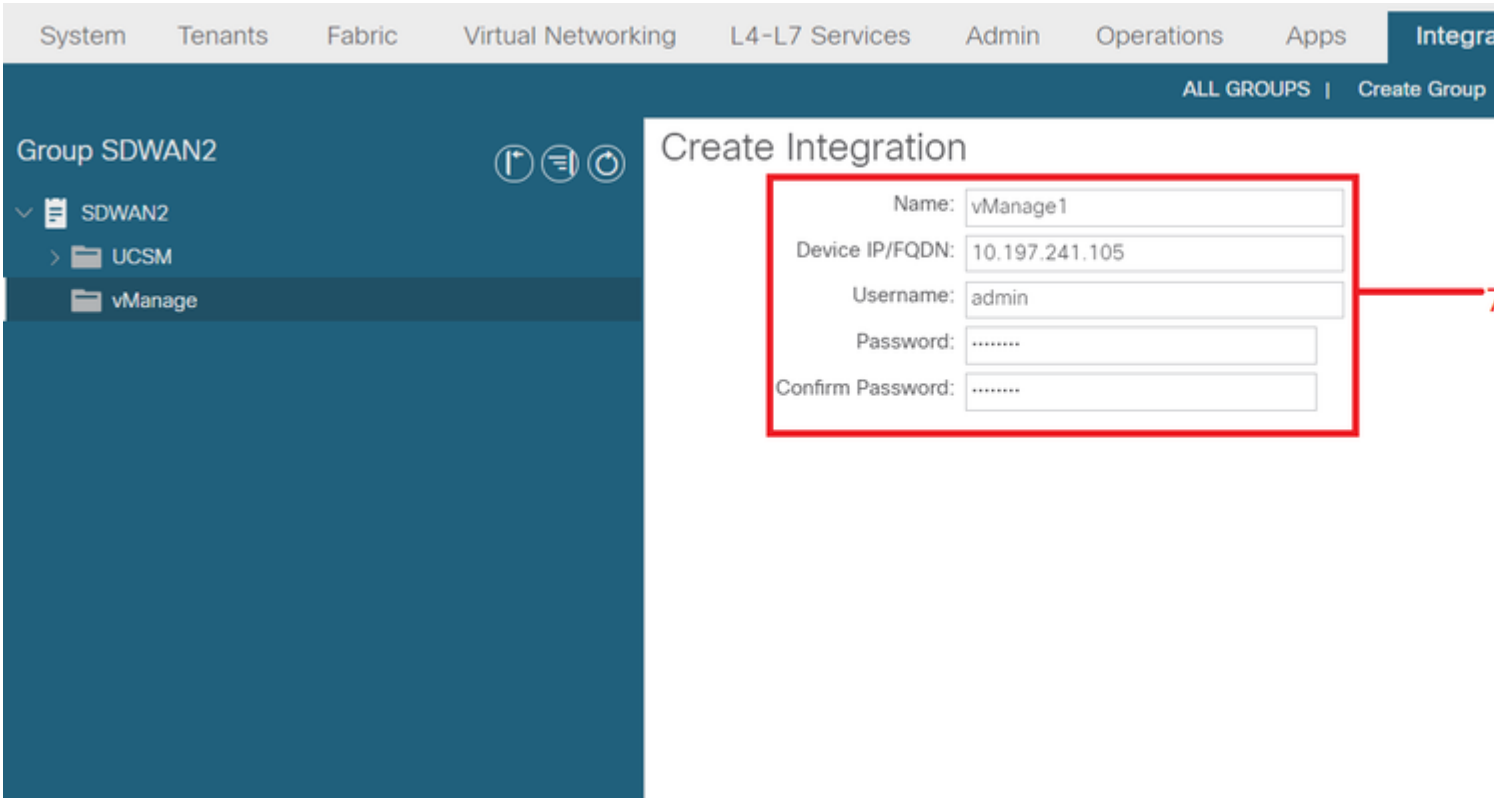
3. Navigieren Sie zur neu erstellten Integrationsgruppe "**SDWAN2"**, und klicken Sie mit der rechten Maustaste auf **vManage.**



4. Klicken Sie mit der rechten Maustaste auf **vManage**, und wählen Sie **Integration Manager erstellen aus.**



5. Geben Sie die entsprechenden Details wie den Namen des Integrations-Managers, die Geräte-IP/FQDN, den Benutzernamen und das Kennwort ein.



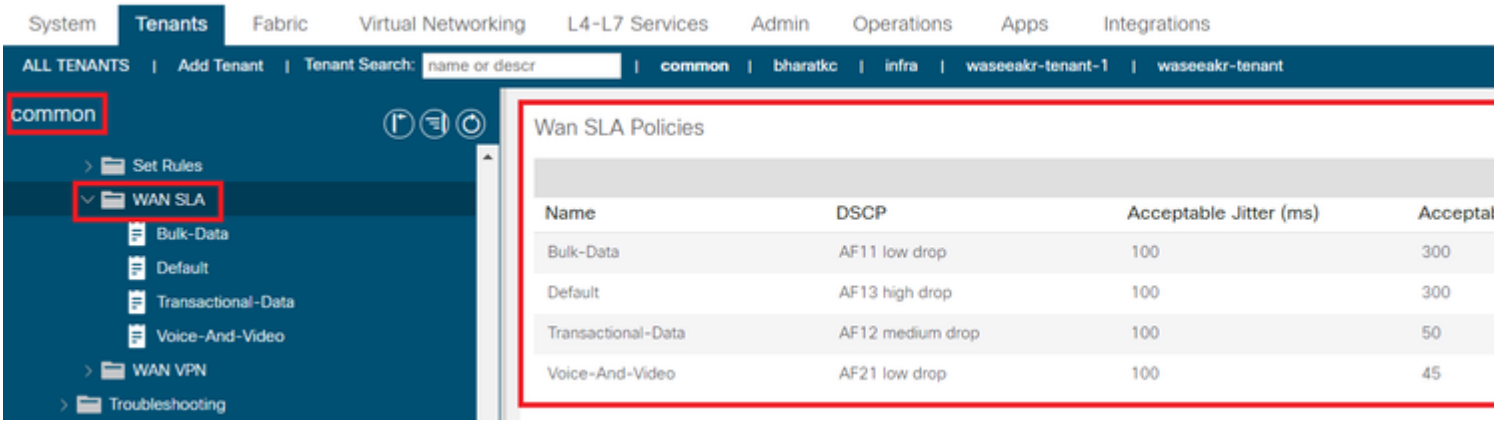
6. Vergewissern Sie sich, dass die Registrierung im Statusfeld erfolgreich war. Wenn sie nicht erfolgreich ist oder Fehler festgestellt wurden, überprüfen Sie, ob die angegebenen Informationen richtig sind. **Partner-ID** ist die Kennung des vManage-Controllers. Sie können zu **Integrations -><Gruppenname>->vManage -> <Integration Manager Name> -> System info** navigieren, um den Status zu überprüfen.

Abschnitt B: Konfiguration der WAN-SLA-Richtlinie

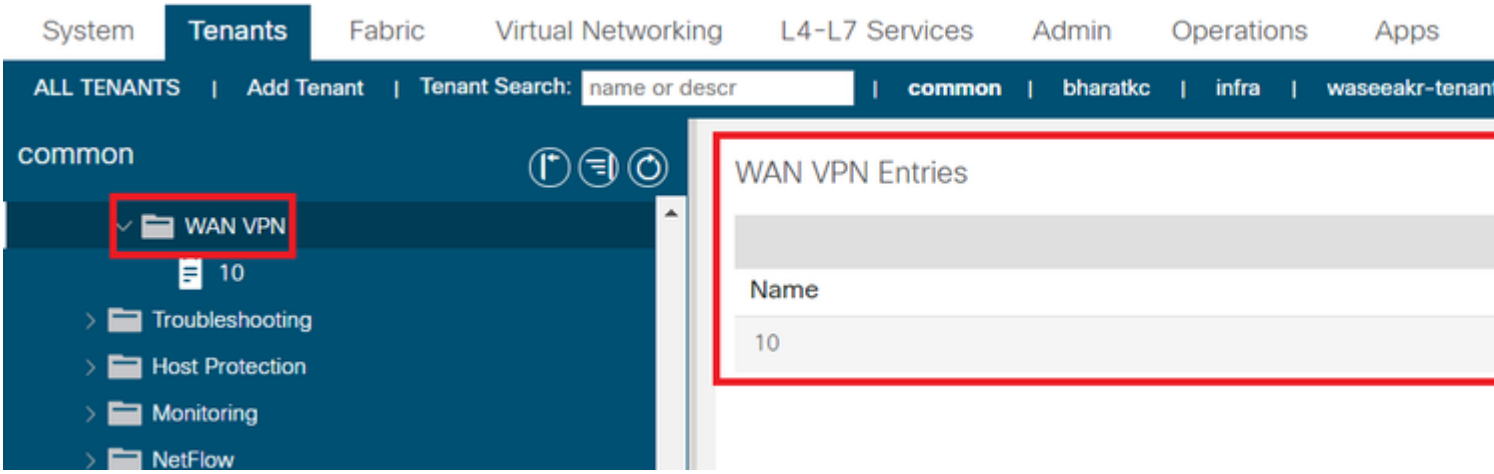
Vorkonfigurierte WAN-SLA-Profile finden Sie unter **Tenants->common->Policies->Protocols->WAN SLA.**

Dies kann bei der Vertragskonfiguration mithilfe einer WAN-SLA-Richtlinie von einem anderen Tenant übernommen werden.

Hierbei handelt es sich um vorkonfigurierte SLAs, die nicht geändert werden können.



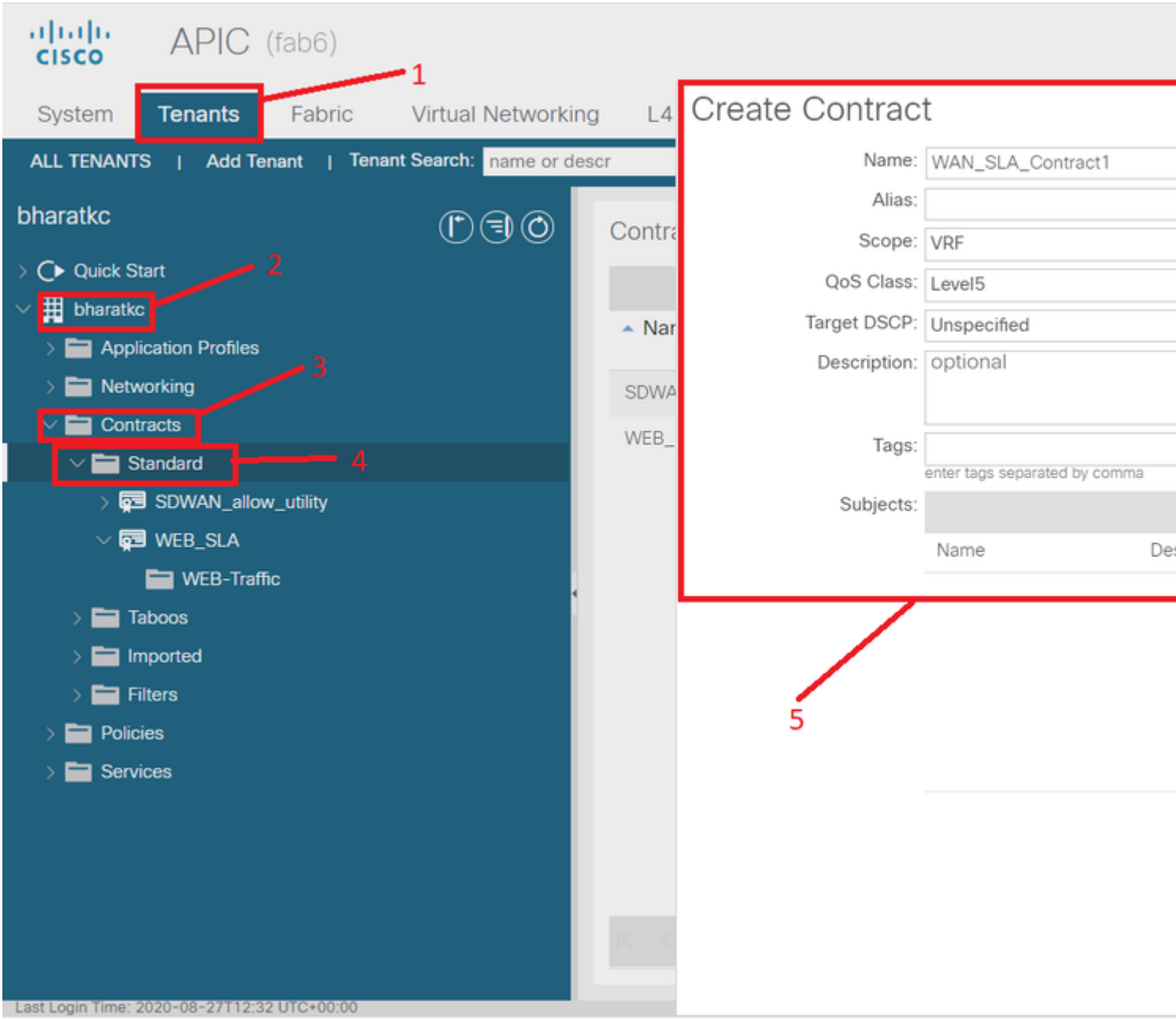
Auf der SD-WAN-Seite konfiguriertes VPN, das dieser ACI-Integration zugeordnet ist, wird auch unter ***Tenants->common->Policies->Protocols->WAN SLA*** angezeigt.



1. Erstellen Sie den Vertrag unter dem Tenant/der VRF-Instanz, in der Sie die WAN-Services zuordnen möchten.

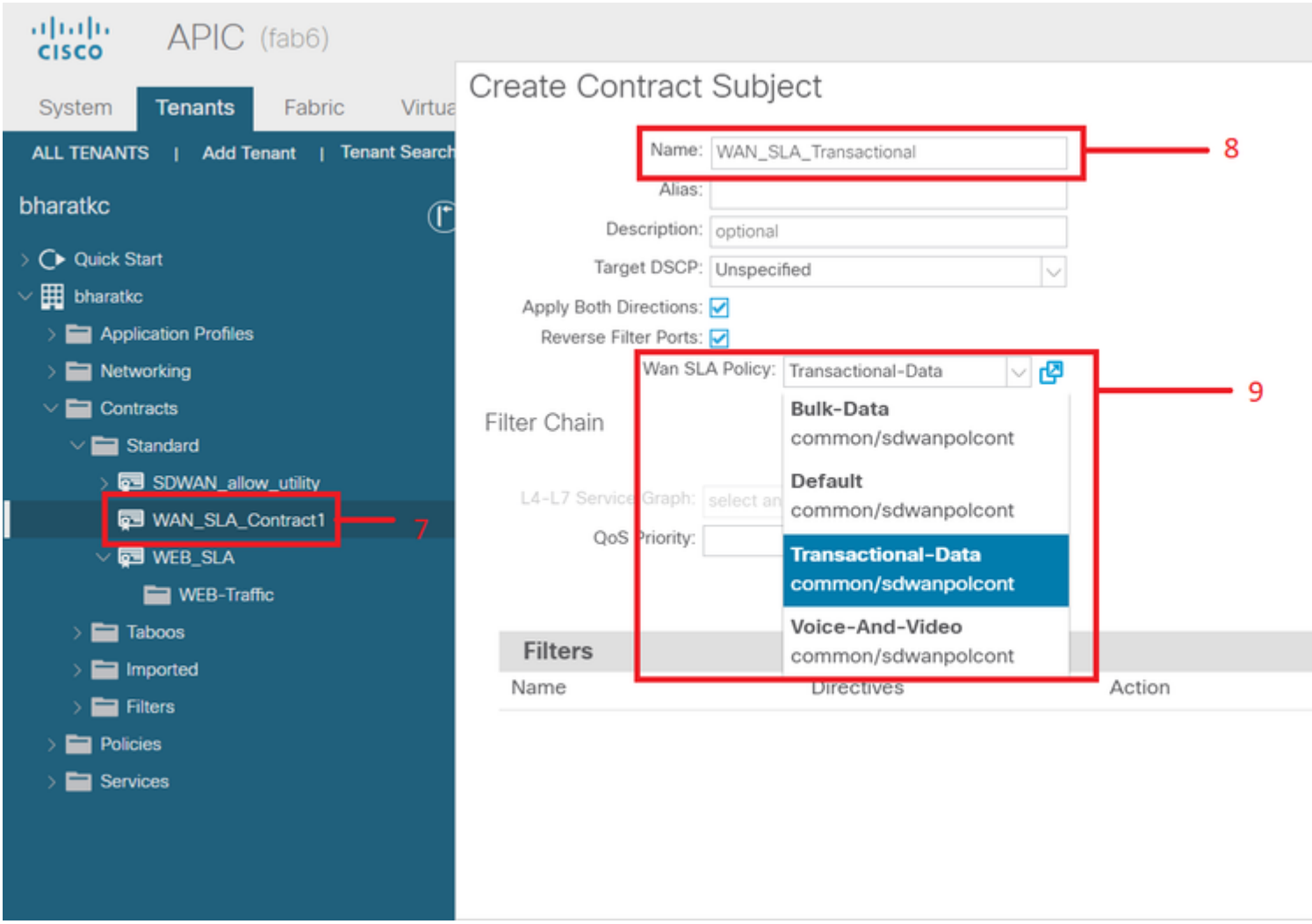
Der Wert für die **QoS-Priorität** muss auf einen anderen Wert als "**Nicht angegeben**" festgelegt werden. Die **WAN-SLA-Richtlinien** funktionieren nicht, wenn der Wert für die **QoS-Priorität** auf **Nicht angegeben** festgelegt ist.

Bitte navigieren Sie zu **Tenants-><Tenant-Name>->Contracts->Standard**



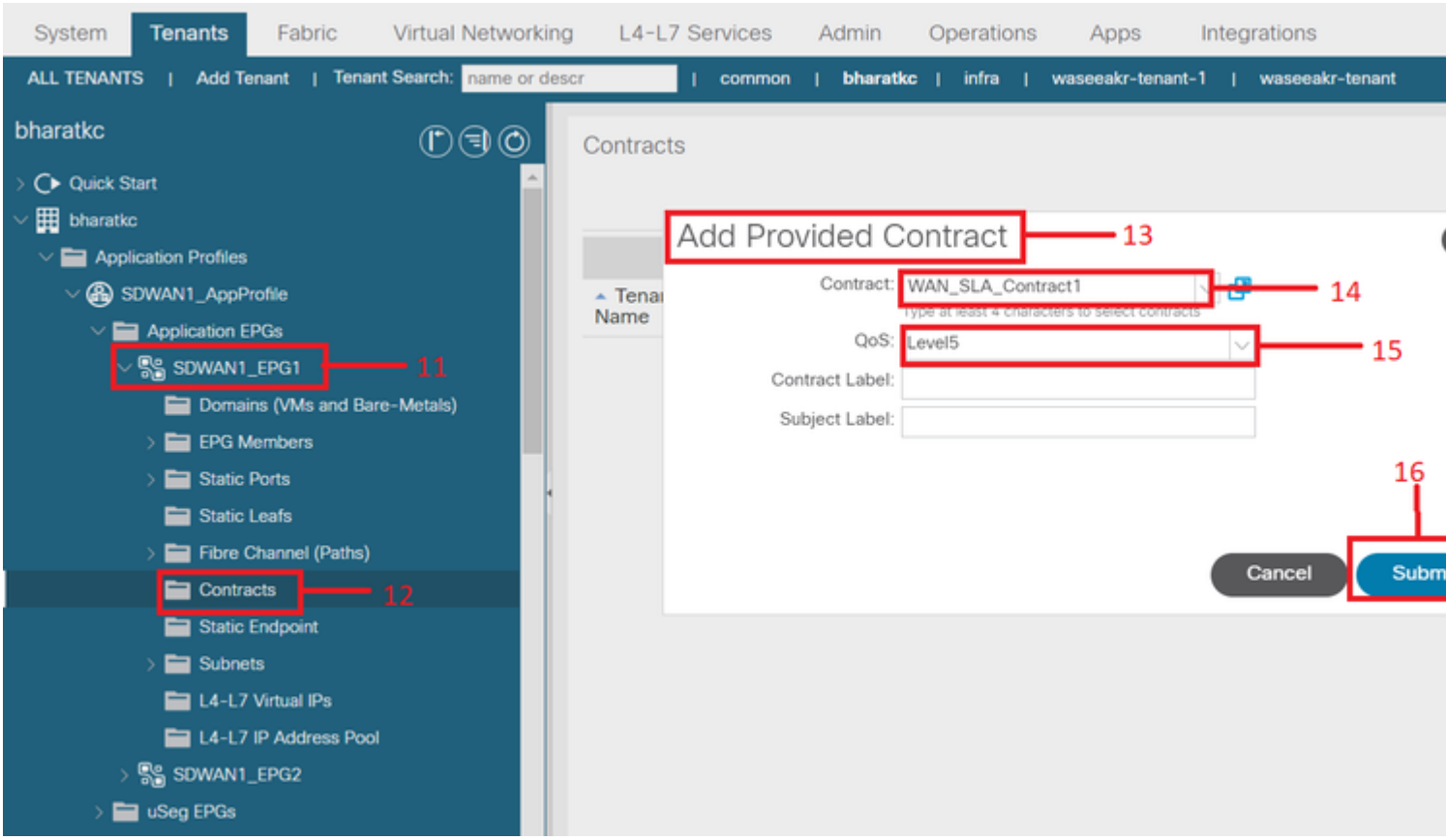
2. Erstellen Sie den Vertragssubjekt, und geben Sie unter "Vertragssubjekt" die WAN-SLA-Richtlinie an.

Der Wert für die **QoS-Priorität** muss auf einen anderen Wert als "**Nicht angegeben**" festgelegt werden. Die **WAN-SLA-Richtlinien** funktionieren nicht, wenn der Wert für die **QoS-Priorität** auf **Nicht angegeben** festgelegt ist.



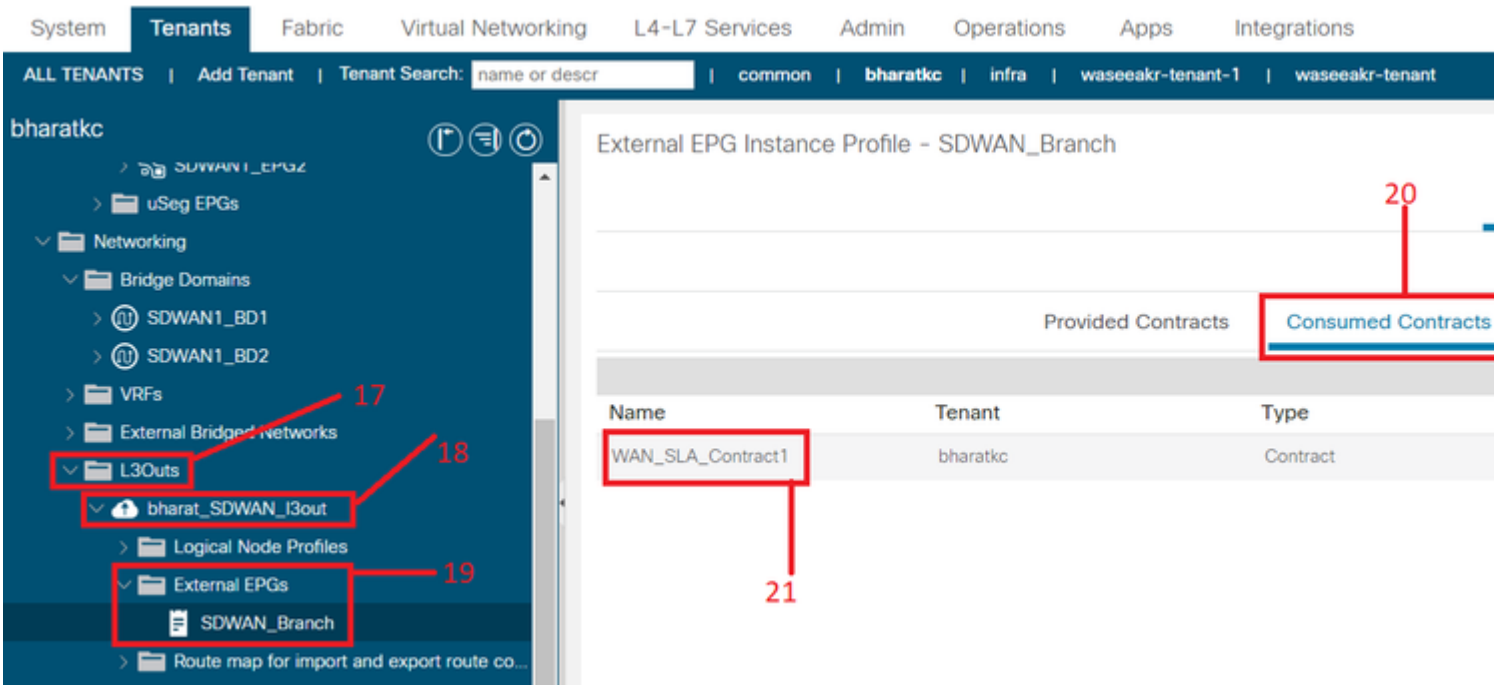
3. Stellen Sie den Vertrag über EPG zur Verfügung.

Navigieren Sie zu **Tenants-><Tenant-Name>->Application Profiles->Application EPG->Contracts**



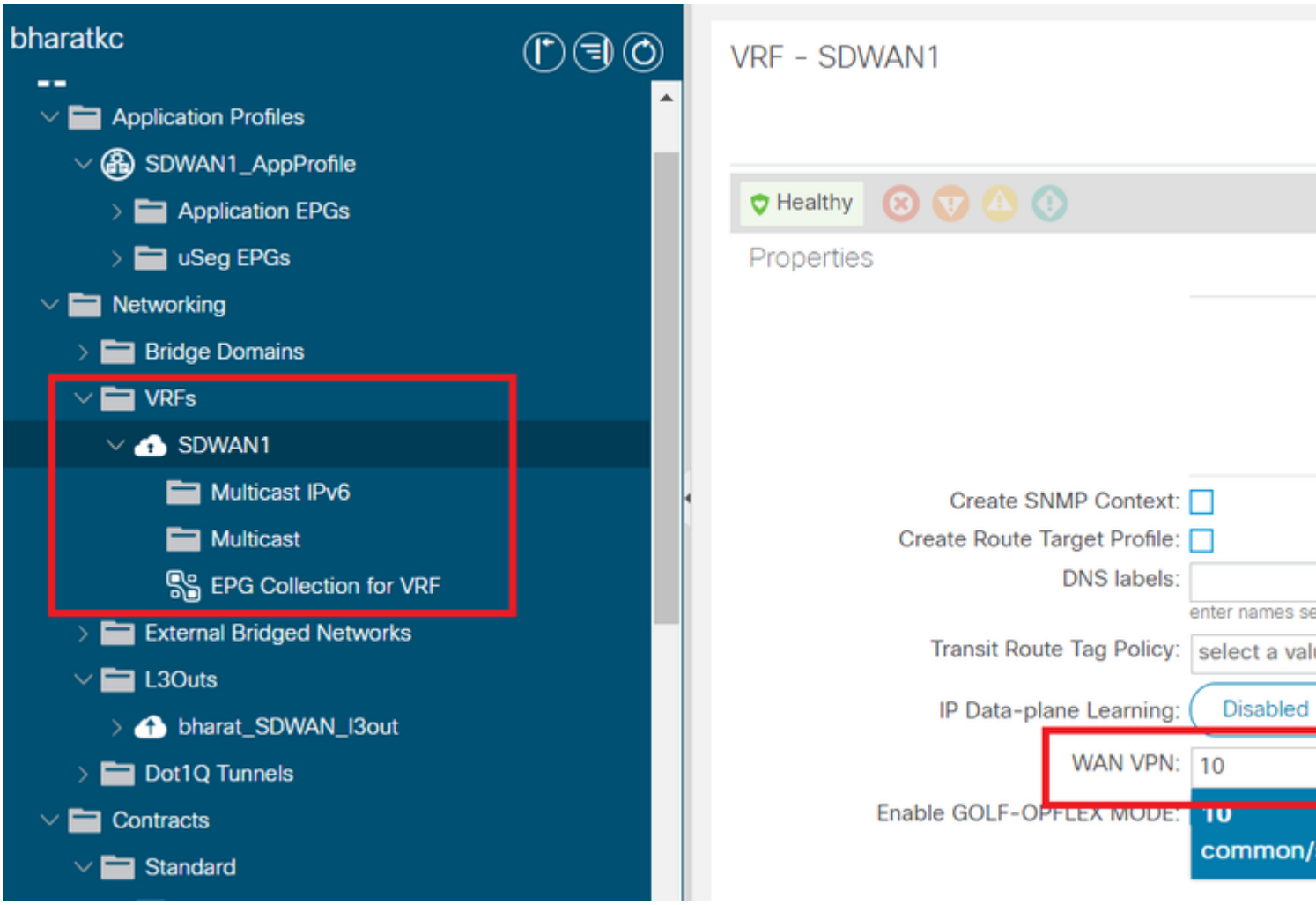
4. Nutzung des Vertrags über L3out, konfiguriert für SD-WAN

Navigieren Sie zu **Tenants-><Tenant-Name>->L3outs->Externe EPG->Verbrauchte Verträge.** Es ist auch möglich und gültig, dass ein Vertrag von einer externen L3out-EPG bereitgestellt und von EPGs verbraucht wird.



5. Zuordnung eines WAN-VPN zu einer Tenant-VRF-Instanz

Navigieren Sie zu **Tenants-><Tenant-Name>->VRFs->Policy->WAN VPN.**



Überprüfung

Abschnitt 3: Überprüfung

1. **Konfigurationsüberprüfung**

Die Konfiguration wird gemäß der ACI-Konfiguration auf beide SDWAN-Geräte übertragen.

Rechenzentrumsende (mit L3out verbunden) SDWAN-Route

<#root>

```
ASR1001-X-DC#show sdwan policy from-vsmart
-->>> SLA Policy (parameters)

from-vsmart sla-class Bulk-Data


 loss    10
 latency 300
 jitter  100

from-vsmart sla-class Default
 loss    25
 latency 300
 jitter  100
```

```
from-vsmart sla-class Transactional-Data
 loss    5
 latency 50
 jitter  100

from-vsmart sla-class Voice-And-Video
 loss    2
 latency 45
 jitter  100

from-vsmart data-policy _vpn-10_data_policy
 direction from-service
 vpn-list vpn-10
  default-action accept

-->>> DSCP to SLA Mapping
from-vsmart app-route-policy _412898115_vpn_412898115
 vpn-list 412898115_vpn


sequence 10


   match


    dscp 14


   action


    sla-class Default


    no sla-class strict


  sequence 20


   match


    dscp 18


   action


    sla-class Voice-And-Video


    no sla-class strict
```

```
  sequence 30
   match
    dscp 12
   action
    sla-class Transactional-Data
    no sla-class strict
  sequence 40
   match
    dscp 10
   action
    sla-class Bulk-Data
    no sla-class strict

from-vsmart lists vpn-list 412898115_vpn
 vpn 10

from-vsmart lists vpn-list vpn-10
 vpn 10

ASR1001-X-DC#
```

SDWAN-Router für Zweigstellen

<#root>

```
ASR1001-X-Branch#show sdwan policy from-vsmart
-->>> SLA Policy (parameters)
from-vsmart sla-class Bulk-Data
 loss    10
 latency 300
```

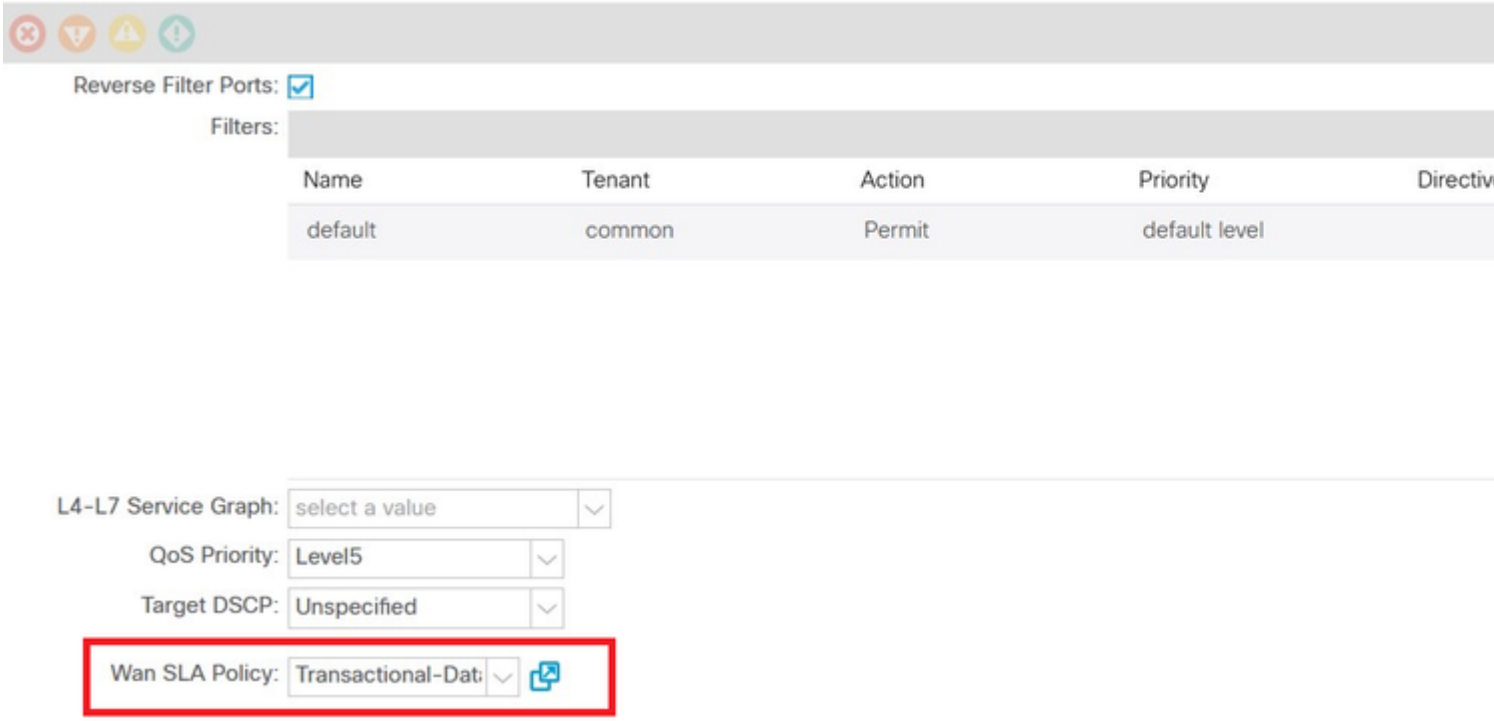
```
 jitter  100

from-vsmart sla-class Default
 loss    25
 latency 300
 jitter  100

from-vsmart sla-class Transactional-Data
 loss    5
 latency 50
 jitter  100

from-vsmart sla-class Voice-And-Video
 loss    2
 latency 45
 jitter  100

-->>> DSCP to SLA Mapping
from-vsmart app-route-policy _412898115_vpn_412898115
 vpn-list 412898115_vpn


sequence 10


   match


    dscp 14


   action


    sla-class Default


    no sla-class strict


  sequence 20


   match


    dscp 18


   action


    sla-class Voice-And-Video


    no sla-class strict
```

```
  sequence 30
   match
    dscp 12
   action
    sla-class Transactional-Data
    no sla-class strict
  sequence 40
   match
    dscp 10
   action
    sla-class Bulk-Data
    no sla-class strict

from-vsmart lists vpn-list 412898115_vpn
 vpn 10

ASR1001-X-Branch#
```

1. **QoS-Verifizierung**

Beispiel 1

WAN-SLA-Richtlinie "Transaktionsdaten". Navigieren Sie zu **Tenants->><Tenant-Name>->Contracts->Standard->><Contract Name>->><Contract Subject>-> General- WAN SLA Policy.**



<#root>

```
  sequence 30
   match
```

dscp 12

```
   action
    sla-class
```

Transactional-Data

```
    no sla-class strict
```

Richtung:

1. Datenverkehr vom Rechenzentrum zu SDWAN

Wie in den folgenden Aufnahmen zu sehen ist, stammt der Datenverkehr vom Rechenzentrum von **dscp 00,** der Datenverkehr, der bis zum SDWAN reicht, erfolgt über **DSCP 12 (**hex 0x0c).

Dies weist auf eine Änderung des DSCP-Werts gemäß der WAN-SLA-Richtlinie hin.

Paketerfassung an der Quelle (DC), die den ursprünglichen DSCP-Wert auf 00 angibt.

Internet Protocol, Src: 192.168.10.2 (192.168.10.2), Dst: 172.16.20.2 (172.16.20.2)

Version: 4

Header-Länge: 20 Byte

Feld für differenzierte Services: 0x00 **(DSCP 0x00**: Standard; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Standard (0x00)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Kennung: 0xa0d5 (41173)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 255

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x9016 [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 192.168.10.2 (192.168.10.2)

Ziel: 172.16.20.2 (172.16.20.2)

Internet Control Message Protocol

Typ: 8 (Echo (Ping)-Anfrage)

Code: 0 ()

Prüfsumme: 0xc16a [richtig]

Kennung: 0x4158

Sequenznummer: 768 (0x0300)

Daten (56 Bytes)

Paketerfassung am Ziel (SDWAN-Zweigstelle), die die Änderung des **DSCP 12-Werts (hex 0x0c)** gemäß der WAN-SLA-Richtlinie widerspiegelt.

Internet Protocol, Src: 192.168.10.2 (192.168.10.2), Dst: 172.16.20.2 (172.16.20.2)

Version: 4

Header-Länge: 20 Byte

Differentiated Services Field: 0x30 (**DSCP 0x0c**: Assured Forwarding 12; ECN: 0x00)

0011 00.. = Differentiated Services Codepoint: Assured Forwarding 12 (0x0c)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Kennung: 0xa0d1 (41169)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 251

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x93ea [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 192.168.10.2 (192.168.10.2)

Ziel: 172.16.20.2 (172.16.20.2)

Internet Control Message Protocol

Typ: 8 (Echo (Ping)-Anfrage)

Code: 0 ()

Prüfsumme: 0x6e30 [korrekt]

Kennung: 0xc057

Sequenznummer: 1024 (0x0400)

Daten (56 Bytes)

2. Datenverkehr von SDWAN zu Rechenzentrum

Wie in den folgenden Aufnahmen zu sehen ist, stammt der Datenverkehr von der SDWAN-Außenstelle von dscp 00, der Datenverkehr, der das Rechenzentrum erreicht, wird jedoch mit DSCP 12 (hex 0x0c) übermittelt, was die Änderung des DSCP-Werts entsprechend der angewendeten WAN-SLA-Richtlinie widerspiegelt.

Paketerfassung an der Quelle (SDWAN-Außenstelle), die den ursprünglichen DSCP-Wert auf 00 angibt.

Internet Protocol, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Header-Länge: 20 Byte

Feld für differenzierte Services: 0x00 (**DSCP 0x00**: Standard; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Standard (0x00)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Kennung: 0xa0c8 (41160)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 255

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x9023 [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 172.16.20.2 (172.16.20.2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echo (Ping)-Anfrage)

Code: 0 ()

Prüfsumme: 0xd3ff [richtig]

Kennung: 0x5c79

Sequenznummer: 1 (0x0001)

Daten (56 Bytes)

Paketerfassung am Ziel (DC), die die Änderung des **DSCP 12-Werts (hex 0x0c)** gemäß der WAN-SLA-Richtlinie widerspiegelt.

Internet Protocol, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Header-Länge: 20 Byte

Differentiated Services Field: 0x30 (**DSCP 0x0c**: Assured Forwarding 12; ECN: 0x00)

0011 00.. = Differentiated Services Codepoint: Assured Forwarding 12 (0x0c)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa073 (41075)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 251

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x9448 [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 172.16.20.2 (172.16.20.2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echo (Ping)-Anfrage)

Code: 0 ()

Prüfsumme: 0x741a [korrekt]

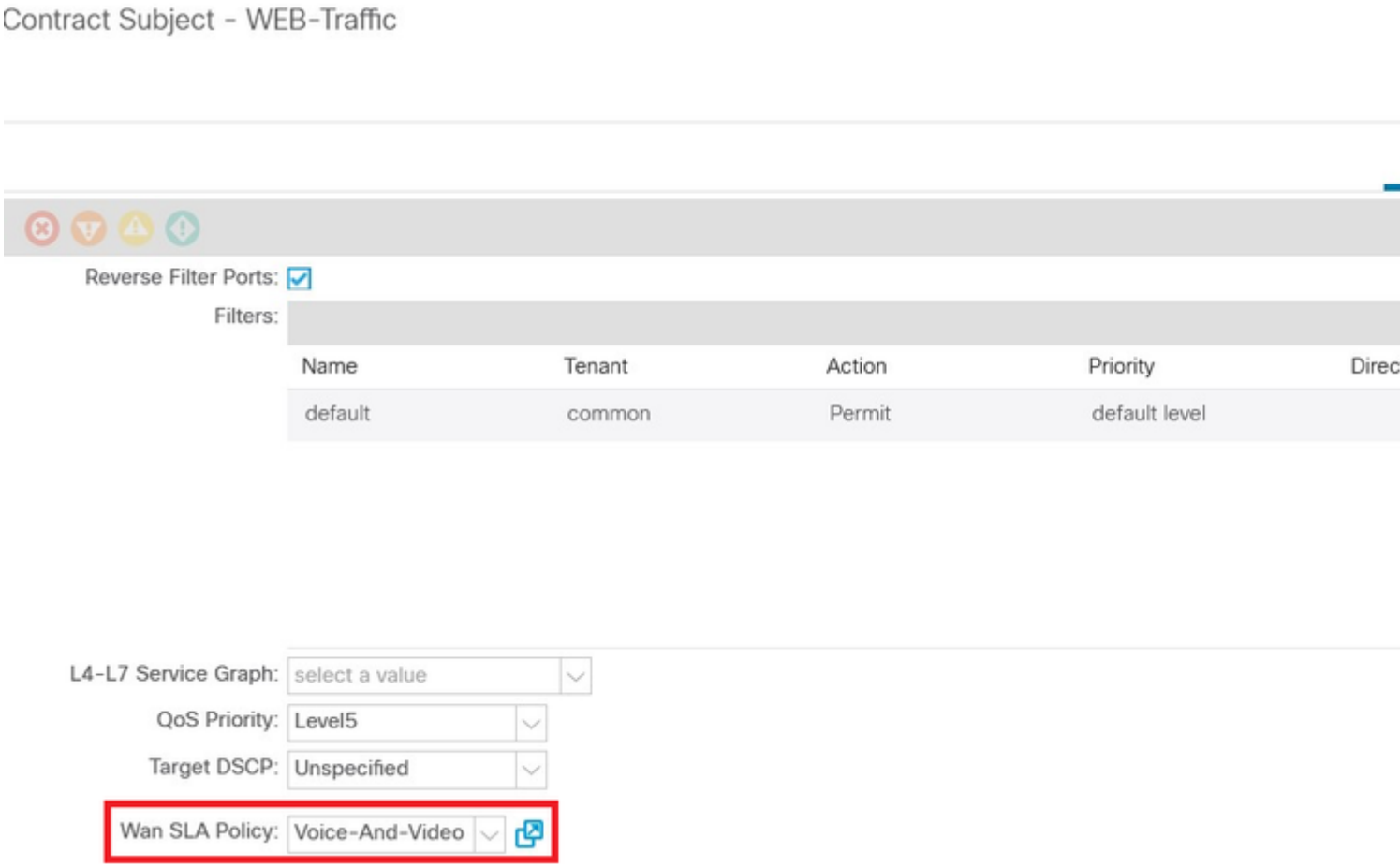
Kennung: 0x5c79

Sequenznummer: 43776 (0xab00)

Daten (56 Bytes)

Beispiel 2

WAN-SLA-Richtlinie "Voice-And-Video" Bitte navigieren Sie zu **Tenants->><Tenant-Name>->Contracts->Standard->><Vertragsname>->><Vertragssubjekt>-> General- WAN-SLA-Richtlinie**



<#root>

```
  sequence 20
   match
```

dscp 18

```
   action
```

sla-class Voice-And-Video

```
    no sla-class strict
```

1. Datenverkehr vom Rechenzentrum zu SDWAN

Wie in den folgenden Aufnahmen zu sehen ist, stammt der Datenverkehr vom Rechenzentrum von **DSCP 00,** der Datenverkehr, der bis zum SDWAN reicht, erfolgt über **DSCP 18 (hex 0x12).**

Dies weist auf eine Änderung des DSCP-Werts gemäß der WAN-SLA-Richtlinie hin.

Paketerfassung an der Quelle (DC), die den ursprünglichen DSCP-Wert auf 00 angibt.

Internet Protocol, Src: 192.168.10.2 (192.168.10.2), Dst: 172.16.20.2 (172.16.20.2)

Version: 4

Header-Länge: 20 Byte

Feld für differenzierte Services: 0x00 (**DSCP 0x00**: Standard; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Standard (0x00)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa2b6 (41654)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 255

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x8e35 [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 192.168.10.2 (192.168.10.2)

Ziel: 172.16.20.2 (172.16.20.2)

Internet Control Message Protocol

Typ: 8 (Echo (Ping)-Anfrage)

Code: 0 ()

Prüfsumme: 0x3614 [richtig]

Kennung: 0x8c5f

Sequenznummer: 512 (0x0200)

Daten (56 Bytes)

Paketerfassung am **Ziel (SDWAN-Zweigstelle)** spiegelt die Änderung des **DSCP-Werts 18 (0x12) wider, der** mit der WAN-SLA-Richtlinie übereinstimmt.

Internet Protocol, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Header-Länge: 20 Byte

Differentiated Services Field: 0 x 48 (**DSCP 0 x 12**: Assured Forwarding 21; ECN: 0 x 00)

0100 10.. = Differentiated Services Codepoint: Assured Forwarding 21 (0x12)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa2b8 (41656)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 255

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x8deb [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 172.16.20.2 (172.16.20.2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 0 (Echo (Ping) Antwort)

Code: 0 ()

Prüfsumme: 0x8a13 [richtig]

Kennung: 0x8c5f

Sequenznummer: 1024 (0x0400)

Daten (56 Bytes)

2. Datenverkehr von SDWAN zu Rechenzentrum

Paketerfassung an der Quelle (SDWAN Branch) mit dem ursprünglichen **DSCP-Wert (00).**

Internet Protocol, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Header-Länge: 20 Byte

Feld für differenzierte Services: 0x00 (**DSCP 0x00**: Standard; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Standard (0x00)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Kennung: 0xa1bb (41403)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 255

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x8f30 [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 172.16.20.2 (172.16.20.2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echo (Ping)-Anfrage)

Code: 0 ()

Prüfsumme: 0x68e5 [richtig]

Kennung: 0x1d03

Sequenznummer: 2048 (0x0800)

Daten (56 Bytes)

Die Paketerfassung am Ziel (DC) spiegelt die Änderung des **DSCP-Werts 18 (0x12)** gemäß der WAN-SLA-Richtlinie wider.

Internet Protocol, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Header-Länge: 20 Byte

Differentiated Services Field: 0 x 48 (**DSCP 0 x 12**: Assured Forwarding 21; ECN: 0 x 00)

0100 10.. = Differentiated Services Codepoint: Assured Forwarding 21 (0x12)

.... ..0. = ECN-fähiger Transport (ECT): 0

....0 = ECN-CE: 0

Gesamtlänge: 84

Kennung: 0xa1bb (41403)

Flags: 0x00

0.. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Weitere Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zu leben: 251

Protokoll: ICMP (0x01)

Header-Prüfsumme: 0x92e8 [richtig]

[Gut: Richtig]

[Schlecht: Falsch]

Quelle: 172.16.20.2 (172.16.20.2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echo (Ping)-Anfrage)

Code: 0 ()

Prüfsumme: 0x68e5 [richtig]

Kennung: 0x1d03

Sequenznummer: 2048 (0x0800)

Daten (56 Bytes)

Fehlerbehebung

Die folgenden Protokolldateien sind im Hinblick auf die Fehlerbehebung hilfreich. .

Debuggen von Steuerpfaden

APIC-Dateien für technischen Support
PolicyDistributor-Protokolle, PolicyManager-Protokolle, PolicyElement- und Edmgr-Protokolle bieten Einblicke in relevante Konfigurationen, die an Leaf- und Spines weitergeleitet werden.

Datenpfad-Debugging

Paketerfassung über L3out-Schnittstelle und Schnittstellen auf vEdge-Routern.

Auch die ELAM kann helfen.

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.