Konfiguration und Verifizierung der SDWAN-Integration in die ACI

Inhalt

Akronyme

ACI - Application Centric Infrastructure

EPG = Endpunktgruppe

L3out - Layer 3 Out

AAR = Application Aware Routing

SLA = Service Level Agreements

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) in das Software Defined Wide Area Network (SD-WAN) und deren Verifizierung beschrieben.

Software Defined Networking (SDN) wurden für bestimmte Netzwerksegmente erweitert:

1. Software Defined - Data Center (SD-DC)
2. Software Defined - Wide Area Network (SD-WAN)

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

Da immer mehr Kunden planen, den Datenverkehr nahtlos über den gesamten Pfad zu integrieren, 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-Zweigstelle)
2. Datenverkehr vom SDWAN (nicht ACI-Zweigstelle) zur ACI (DC)

Voraussetzungen

Anforderungen

Da die Integration mit dem SD-WAN über das in der ACI konfigurierte L3-Out erfolgt, muss L3out mit unterstütztem Protokoll konfiguriert werden.

Die Integration erfolgt über das Management-Netzwerk, sodass die Erreichbarkeit der Verwaltung zwischen ACI (APIC-Controller) und vManage erforderlich ist.

Verwendete Komponenten

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

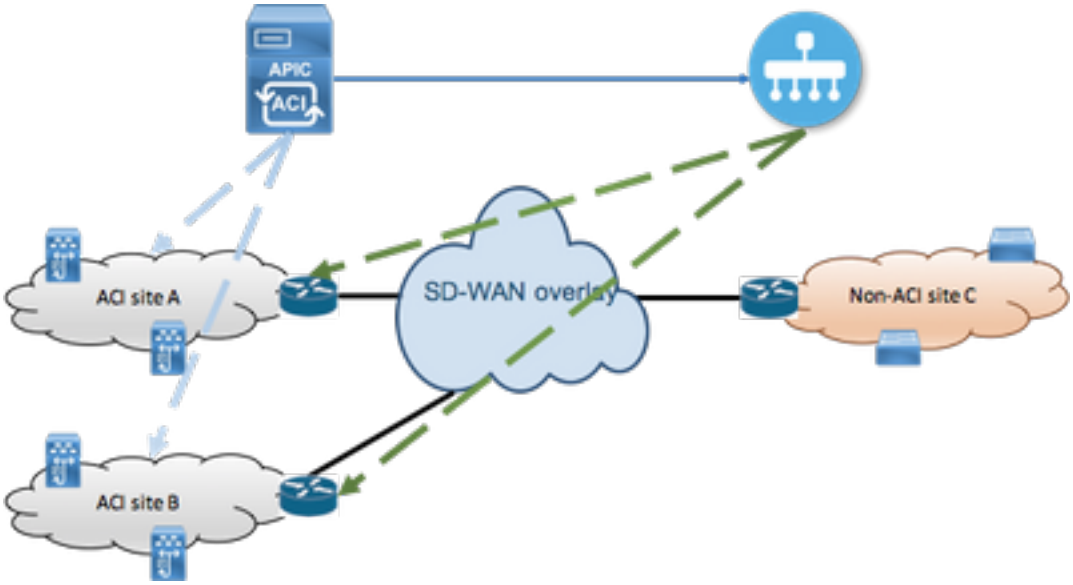
Dieses Dokument basiert auf der ACI-Version 4.2(3l).

Konfiguration

Netzwerkdiagramm

Referenztopologie:

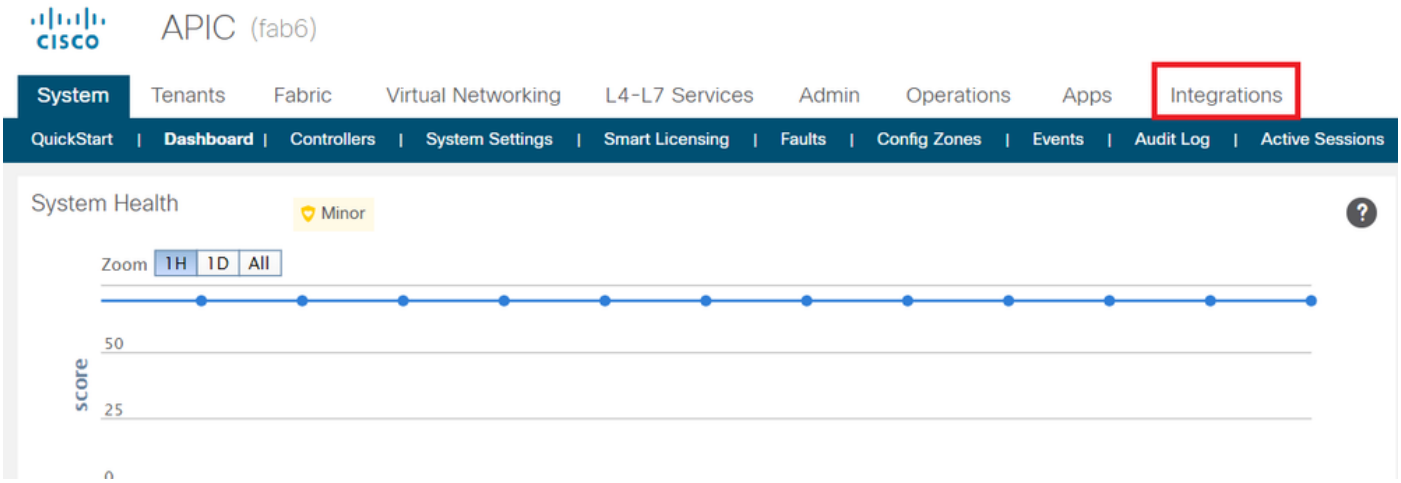
Betrachten Sie in unserer Topologie nur den ACI-Standort A als Rechenzentrum und Nicht-ACI-Standort C als SDWAN-Zweigstelle.



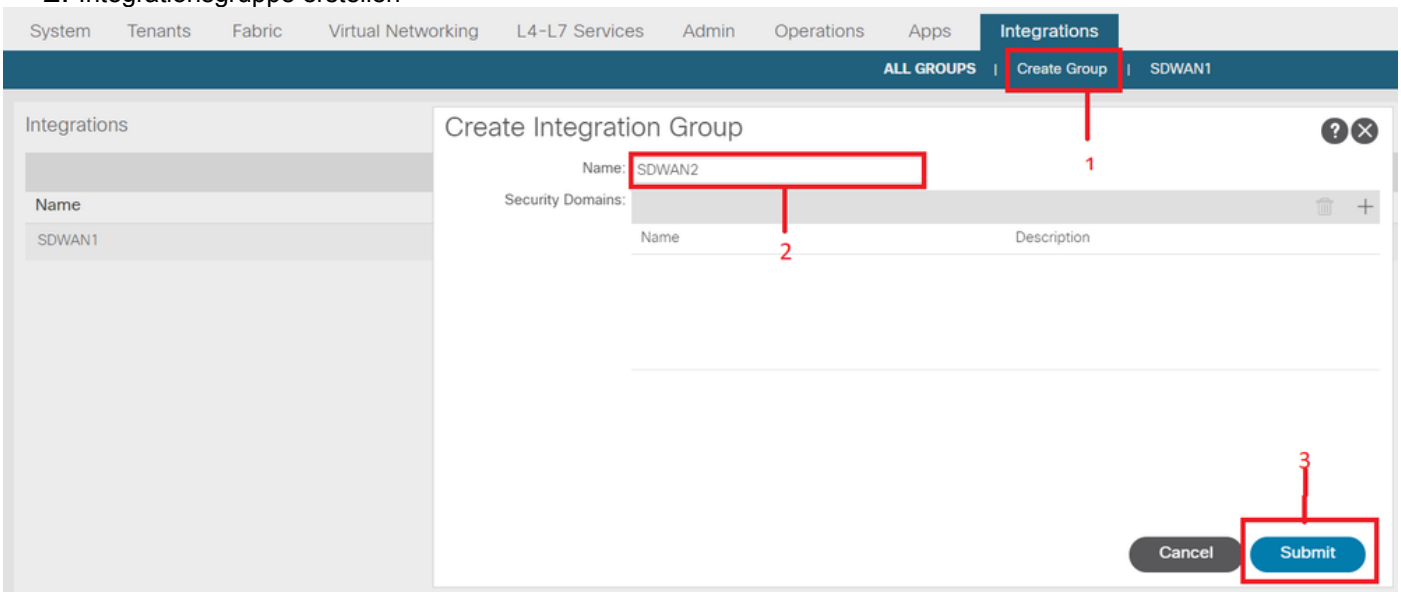
Konfigurationen

Abschnitt A: Konfiguration der Integration

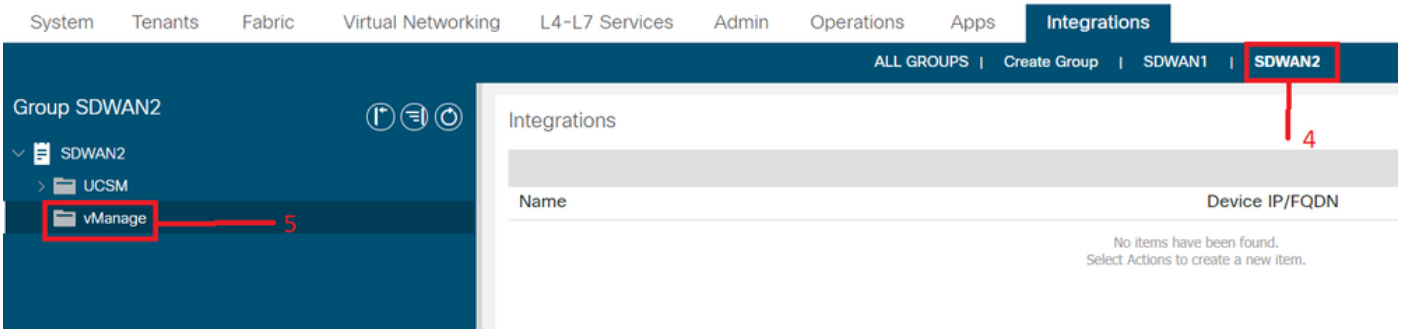
1. Öffnen Sie die grafische Benutzeroberfläche (GUI) des APIC, und navigieren Sie unter der Registerkarte **System** zur Registerkarte **Integrations**.



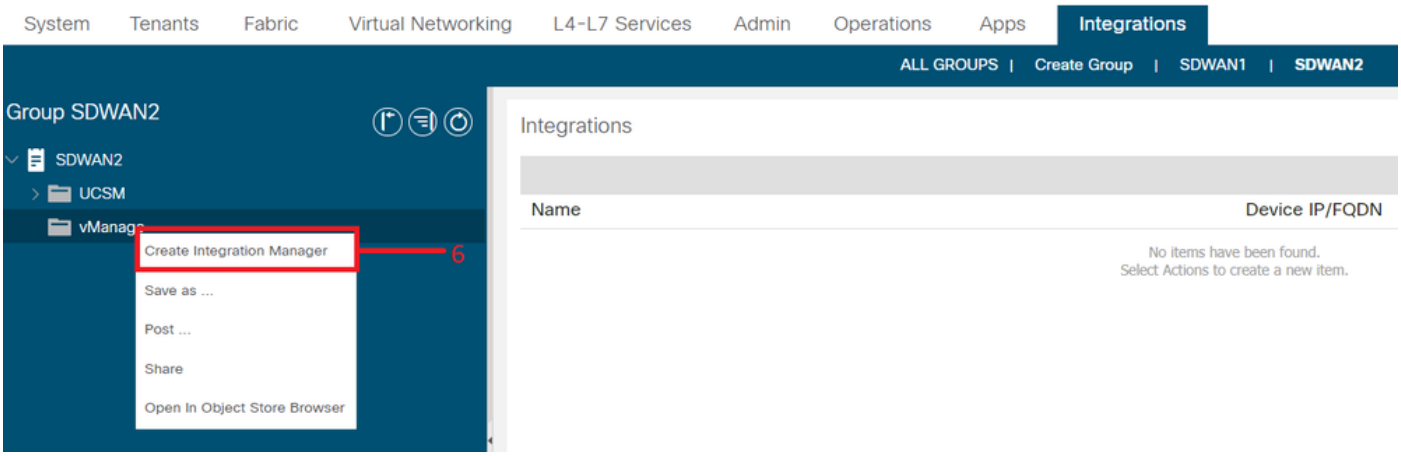
2. Integrationsgruppe erstellen



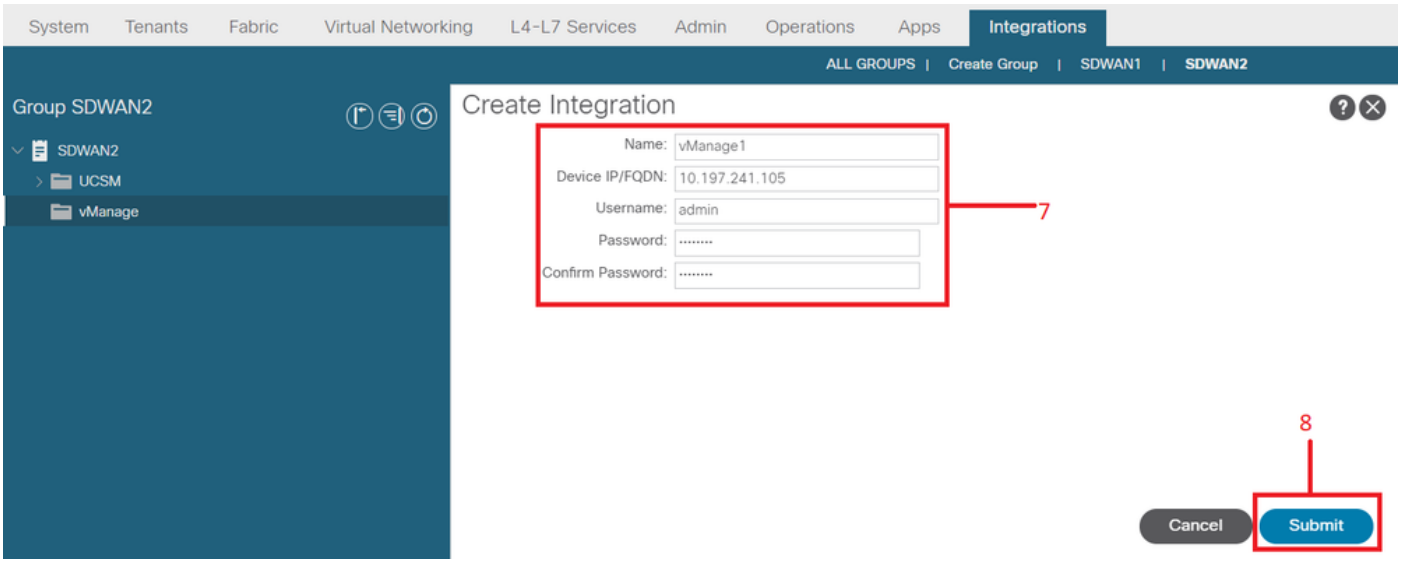
3. Navigieren Sie zur neu erstellten Integrationsgruppe "**SDWAN2**", und klicken Sie mit der rechten Maustaste auf **vManage.**



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



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



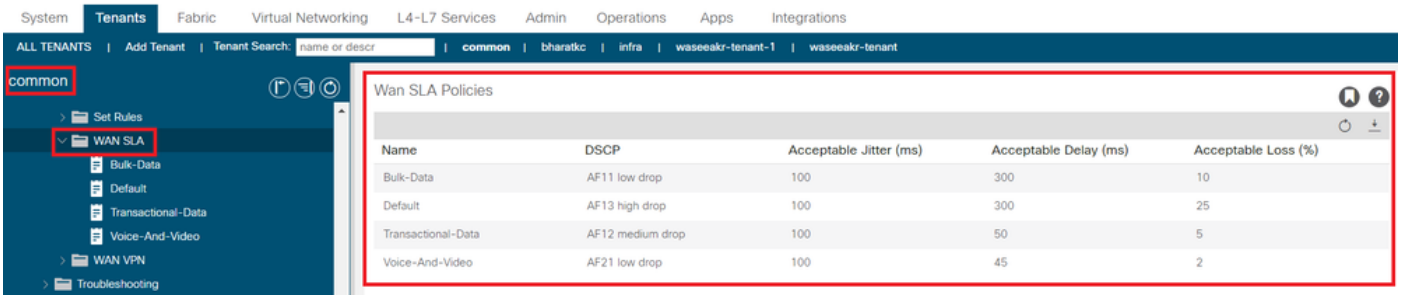
6. Stellen Sie sicher, dass die Registrierung im Statusfeld erfolgreich durchgeführt wurde. Wenn die Informationen nicht erfolgreich sind oder Fehler aufgetreten sind, überprüfen Sie, ob die angegebenen Informationen richtig sind. **Partner-ID** ist die ID des vManage-Controllers. Sie können zu **Integrations -><Gruppenname>->vManage -> <Integration Manager Name> -> System-Informationen** 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 von anderen Tenants übernommen werden, während der Vertrag mithilfe der WAN-SLA-Richtlinie konfiguriert wird.

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

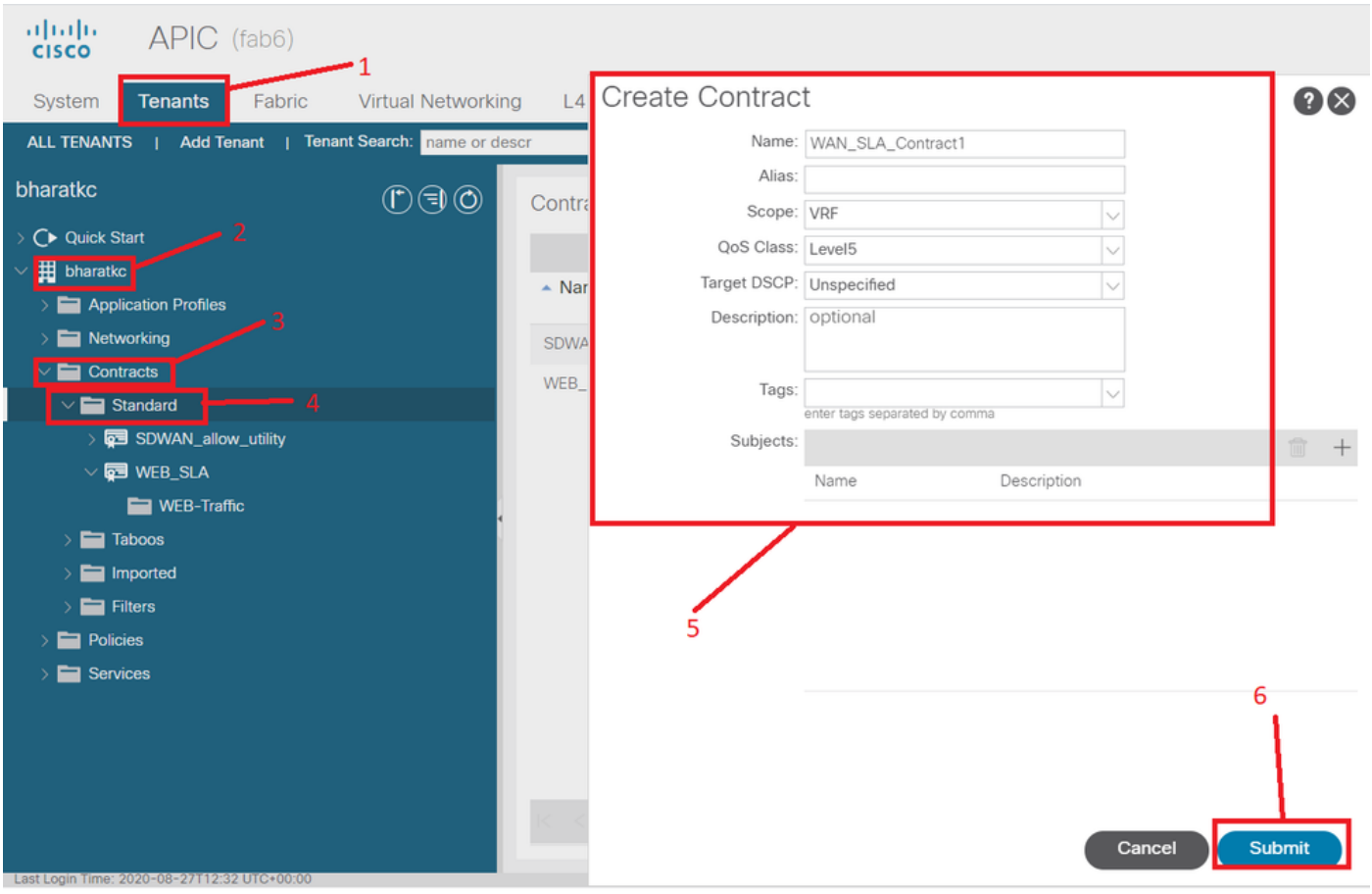


Auf SD-WAN-Seite konfiguriertes VPN, das dieser ACI-Integration zugeordnet ist, wird ebenfalls unter ***Tenants > common->policy->Protocols->WAN SLA*** angezeigt.

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

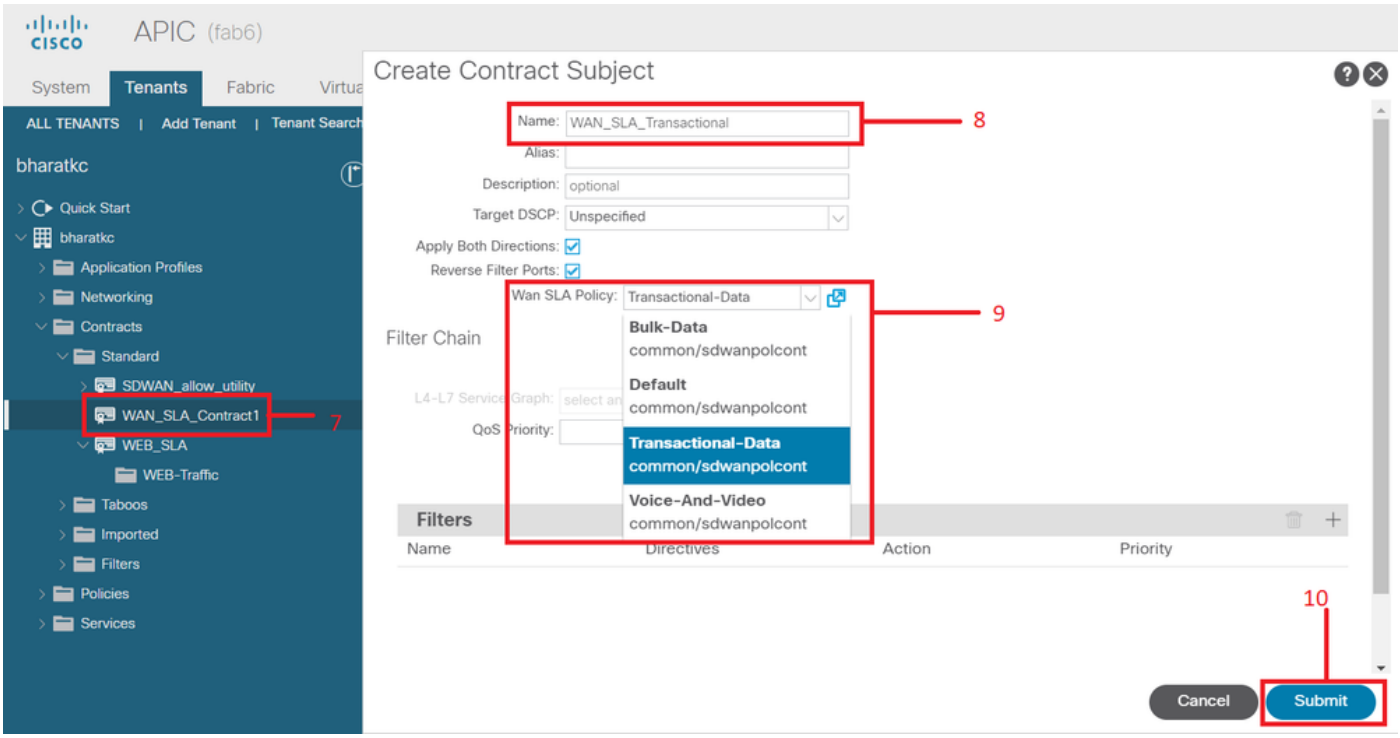
Der **QoS-Prioritätswert** muss auf einen anderen Wert als **Unspecified** festgelegt werden. Die **WAN-SLA-Richtlinien** funktionieren nicht, wenn der **QoS-Prioritätswert** auf **Unspecified (Nicht festgelegt)** festgelegt ist.

Rufen Sie die Seite **Tenants ><Tenant name>->Contracts->Standard auf.**



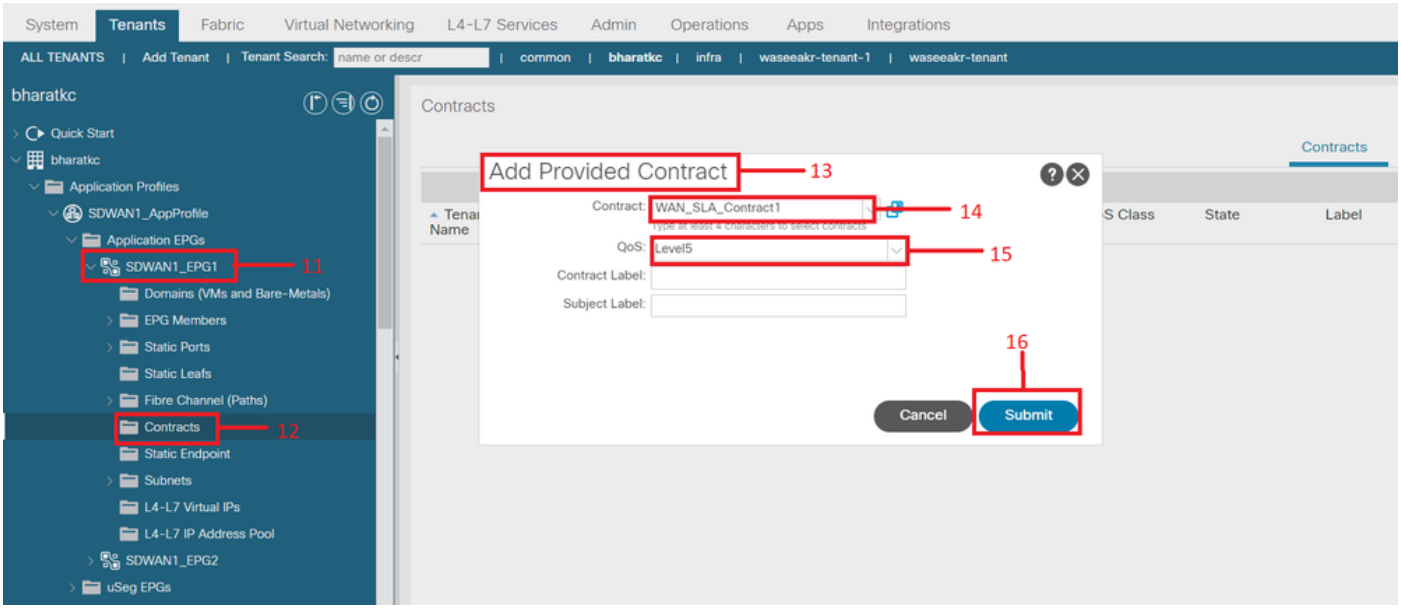
2. Erstellen Sie den Vertragsbetreff, und geben Sie unter Vertragsgegenstand die WAN-SLA-Richtlinie an.

Der **QoS-Prioritätswert** muss auf einen anderen Wert als **Unspecified** festgelegt werden. Die **WAN-SLA-Richtlinien** funktionieren nicht, wenn der **QoS-Prioritätswert** auf **Unspecified (Nicht festgelegt)** festgelegt ist.



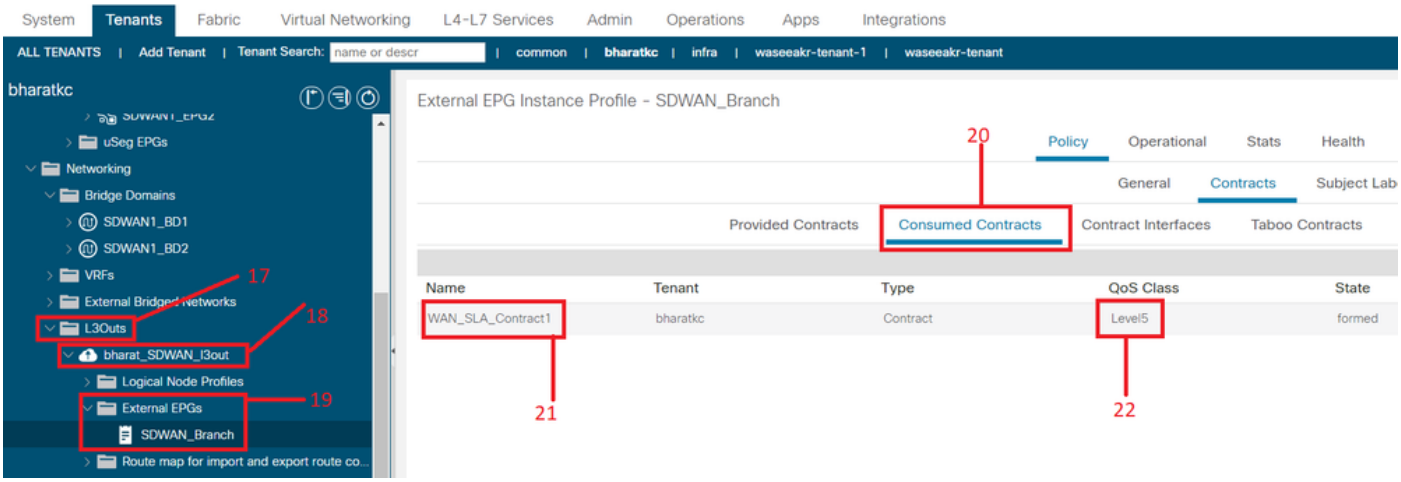
3. Geben Sie den Vertrag von der EPG an.

Rufen Sie die Seite **Tenants ><Tenant name>->Application Profiles->Application EPG->Contracts auf.**



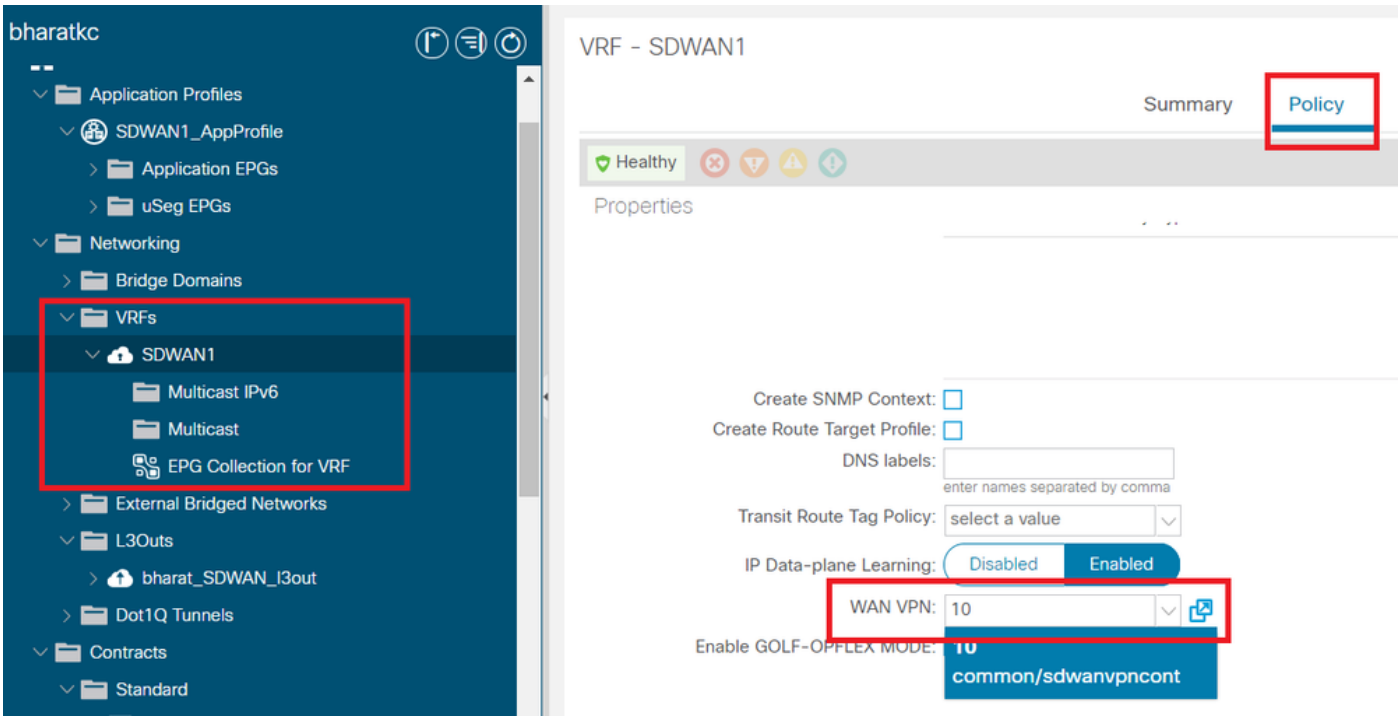
4. Vertragsnutzung bei L3out, konfiguriert für SD-WAN

Rufen Sie die Seite **Tenants ><Tenant name>->L3outs->External EPG->Consumed Contracts (Externe EPG) auf.** Ein Vertrag, der von L3out External EPG bereitgestellt und von EPGs verbraucht wird, ist ebenfalls möglich und gültig.



5. WAN-VPN einem Tenant-VRF zuordnen

Rufen Sie die Seite **Tenants ><Tenant name>->VRFs->Policy->WAN VPN auf.**



Überprüfung

Abschnitt 3: Überprüfung

1. Konfigurationsüberprüfung

Konfiguration wird entsprechend der ACI-Konfiguration auf beide SDWAN-Geräte übertragen.

DC-End (verbunden mit L3out)-SDWAN-Route

```
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

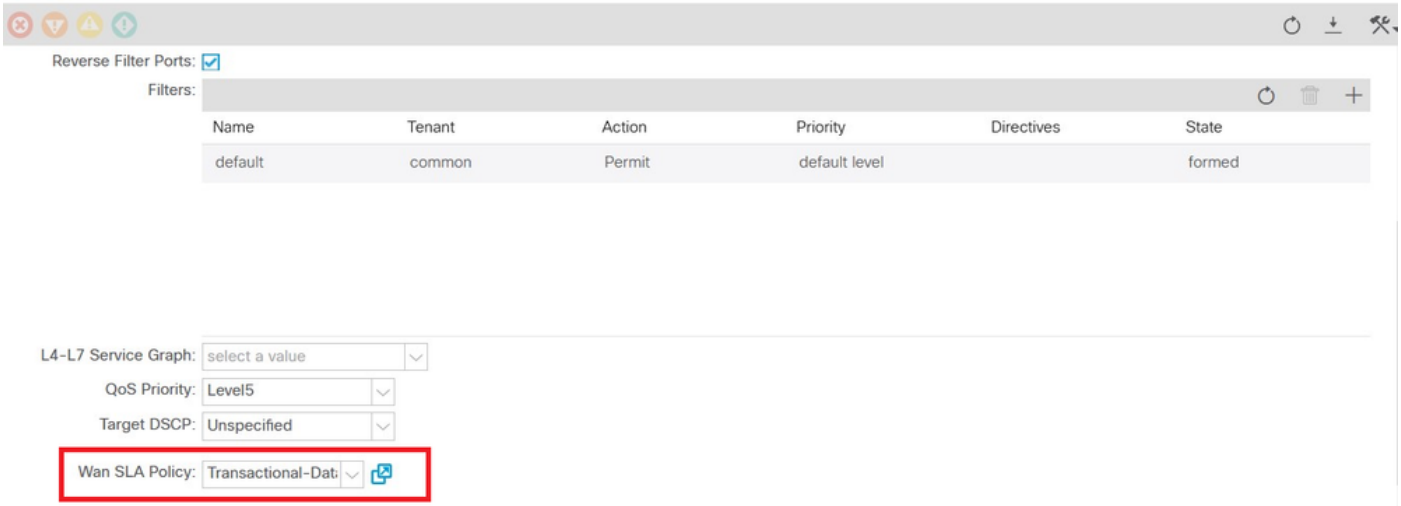
```
ASR1001-X-Branch#show sdwan policy from-vsmart
-->>> SLA Policy (parameters)
from-vsmart sla-class Bulk-Data
 loss    10
 latency 300
 jitter  100
```

```
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". Rufen Sie die Seite Tenants -><Tenant-Name>->Contracts->Standard-><Vertragsname>-><Vertragsgegenstand>-> Allgemeine WAN-SLA-Richtlinie auf.




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

Richtung:

1. Datenverkehr zwischen Rechenzentren und SDWAN.

Wie in den folgenden Captures zu sehen ist, stammt der Datenverkehr vom Rechenzentrum mit **dscp 00,** der Datenverkehr zu SDWAN jedoch mit **DSCP 12** (hex 0x0c).

Dies zeigt eine Änderung des DSCP-Werts gemäß WAN SLA Policy an.

Die Paketerfassung an der Quelle (DC) unter Berücksichtigung des ursprünglichen DSCP-Werts auf 00.

Internetprotokoll, SRC: 192.168.10.2 (192.168.10.2), Dst: 172,16,20,2 (172,16,20,2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x00 **(DSCP 0x00**: Standard; ECN: 0 x 00)

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

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa0d5 (41173)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 255

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x9016 [korrekt]

[Gut: Richtig]

[Schlecht: False]

Quelle: 192.168.10.2 (192.168.10.2)

Ziel: 172,16,20,2 (172,16,20,2)

Internet Control Message Protocol

Typ: 8 (Echoanforderung (Ping))

Code: 0 ()

Prüfsumme: 0xc16a [korrekt]

Kennung: 0 x 4158

Sequenznummer: 768 (0 x 0300)

Daten (56 Byte)

Paketerfassung am Ziel (SDWAN-Zweigstelle), die Änderungen im **DSCP 12-**Wert **(hex 0x0c)** gemäß WAN-SLA-Richtlinie widerspiegelt.

Internetprotokoll, SRC: 192.168.10.2 (192.168.10.2), Dst: 172,16,20,2 (172,16,20,2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x30 (**DSCP 0x0c**: Assured Forwarding 12; ECN: 0 x 00)

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

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa0d1 (41169)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 251

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x93ea [korrekt]

[Gut: Richtig]

[Schlecht: False]

Quelle: 192.168.10.2 (192.168.10.2)

Ziel: 172,16,20,2 (172,16,20,2)

Internet Control Message Protocol

Typ: 8 (Echoanforderung (Ping))

Code: 0 ()

Prüfsumme: 0x6e30 [korrekt]

Kennung: 0xc057

Sequenznummer: 1024 (0 x 0400)

Daten (56 Byte)

2. Datenverkehr vom SDWAN zum Rechenzentrum

Wie in der folgenden Erfassung dargestellt, stammt der Datenverkehr von der SDWAN-Zweigstelle mit DSCP 00, aber der Datenverkehr, der ins Rechenzentrum gelangt, wird mit DSCP 12 (hex 0x0c) abgewickelt, das die Änderung des DSCP-Werts gemäß der angewendeten WAN-SLA-Richtlinie widerspiegelt.

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

Internetprotokoll, SRC: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x00 (**DSCP 0x00**: Standard; ECN: 0 x 00)

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

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa0c8 (41160)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 255

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x9023 [korrekt]

[Gut: Richtig]

[Schlecht: False]

Quelle: 172,16,20,2 (172,16,20,2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echoanforderung (Ping))

Code: 0 ()

Prüfsumme: 0xd3ff [korrekt]

Kennung: 0x5c79

Sequenznummer: 1 (0 x 0001)

Daten (56 Byte)

Paketerfassung am Ziel (DC), die Änderungen im **DSCP 12-Wert (hex 0x0c)** gemäß WAN SLA-Richtlinie reflektiert.

Internetprotokoll, SRC: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x30 (**DSCP 0x0c**: Assured Forwarding 12; ECN: 0 x 00)

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

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa073 (41075)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 251

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x9448 [korrekt]

[Gut: Richtig]

[Schlecht: False]

Quelle: 172,16,20,2 (172,16,20,2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echoanforderung (Ping))

Code: 0 ()

Prüfsumme: 0x741a [korrekt]

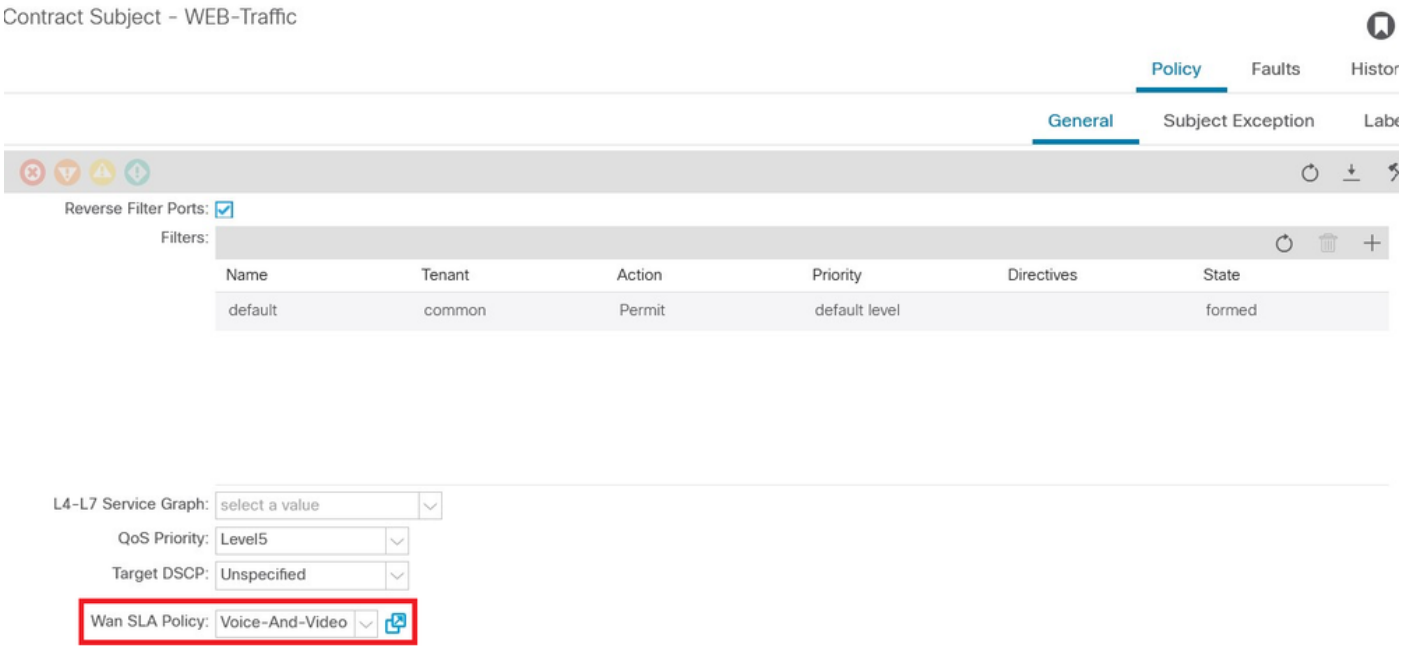
Kennung: 0x5c79

Sequenznummer: 43776 (0xab00)

Daten (56 Byte)

Beispiel 2

WAN SLA-Richtlinie "Voice-and-Video" Rufen Sie die Seite Tenants ><Tenant-Name>->Contracts->Standard-><Vertragsname>-><VertragsSubject>-> General- WAN SLA-Richtlinie auf.




```
sequence 20
match
  dscp 18
action
 sla-class Voice-And-Video
 no sla-class strict
```

1. Datenverkehr zwischen Rechenzentren und SDWAN.

Wie in der folgenden Erfassung dargestellt, stammt der Datenverkehr vom Rechenzentrum mit **DSCP 00**, der zu SDWAN gelangt, jedoch mit **DSCP 18 (Hex 0x12).**

Dies zeigt eine Änderung des DSCP-Werts gemäß WAN SLA Policy an.

Die Paketerfassung an der Quelle (DC) unter Berücksichtigung des ursprünglichen DSCP-Werts auf 00.

Internetprotokoll, SRC: 192.168.10.2 (192.168.10.2), Dst: 172,16,20,2 (172,16,20,2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x00 (**DSCP 0x00**: Standard; ECN: 0 x 00)

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

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa2b6 (41654)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 255

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x8e35 [korrekt]

[Gut: Richtig]

[Schlecht: False]

Quelle: 192.168.10.2 (192.168.10.2)

Ziel: 172,16,20,2 (172,16,20,2)

Internet Control Message Protocol

Typ: 8 (Echoanforderung (Ping))

Code: 0 ()

Prüfsumme: 0x3614 [korrekt]

Kennung: 0x8c5f

Sequenznummer: 512 (0 x 200)

Daten (56 Byte)

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

Internetprotokoll, SRC: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x48 (**DSCP 0x12**: Assured Forwarding 21; ECN: 0 x 00)

0100 10.. = Differentiated Services Codepoint: Assured Forwarding 21 (0 x 12)

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa2b8 (41656)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 255

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x8deb [korrekt]

[Gut: Richtig]

[Schlecht: False]

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 [korrekt]

Kennung: 0x8c5f

Sequenznummer: 1024 (0 x 0400)

Daten (56 Byte)

2. Datenverkehr zwischen SDWAN und Rechenzentrum.

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

Internetprotokoll, SRC: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x00 (**DSCP 0x00**: Standard; ECN: 0 x 00)

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

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa1bb (41403)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 255

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x8f30 [korrekt]

[Gut: Richtig]

[Schlecht: False]

Quelle: 172,16,20,2 (172,16,20,2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echoanforderung (Ping))

Code: 0 ()

Prüfsumme: 0x68e5 [korrekt]

Kennung: 0 x 1 d03

Sequenznummer: 2048 (0 x 0800)

Daten (56 Byte)

Paketerfassung am Ziel (DC), die Änderungen im **DSCP-Wert 18 (0x12)** gemäß WAN SLA-Richtlinie widerspiegelt.

Internetprotokoll, SRC: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Version: 4

Headerlänge: 20 Byte

Differenzierte Services: 0x48 (**DSCP 0x12**: Assured Forwarding 21; ECN: 0 x 00)

0100 10.. = Differentiated Services Codepoint: Assured Forwarding 21 (0 x 12)

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

....0 = ECN-CE: 0

Gesamtlänge: 84

Identifikation: 0xa1bb (41403)

Flaggen: 0 x 00

0. = Reserviertes Bit: Nicht festgelegt

.0. = Nicht fragmentieren: Nicht festgelegt

..0 = Mehr Fragmente: Nicht festgelegt

Fragment-Offset: 0

Zeit zum Leben: 251

Protokolle: ICMP (0 x 01)

Header-Prüfsumme: 0x92e8 [korrekt]

[Gut: Richtig]

[Schlecht: False]

Quelle: 172,16,20,2 (172,16,20,2)

Ziel: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Typ: 8 (Echoanforderung (Ping))

Code: 0 ()

Prüfsumme: 0x68e5 [korrekt]

Kennung: 0 x 1 d03

Sequenznummer: 2048 (0 x 0800)

Daten (56 Byte)

Fehlerbehebung

Die folgenden Protokolldateien sind aus Sicht der Fehlerbehebung nützlich. .

Debuggen von Steuerpfad

APIC-Technologieunterstützungsdateien
PolicyDistributor-Protokolle, PolicyManager-Protokolle, PolicyElement und Edmgr-Protokolle können Einblicke in relevante Konfigurationen bieten, die in Blätter und Spines verschoben werden.

Debuggen von Datenpfaden

Paketerfassungen an L3out-Schnittstellen und Schnittstellen an vEdge-Routern.

ELAM kann ebenfalls helfen.