

# Configuration and Verification of SDWAN Integration with ACI

## Contents

[Acronyms](#)

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

## Acronyms

ACI - Application Centric Infrastructure

EPG - EndPoint Group

L3out - Layer 3 Out

AAR - Application Aware Routing

SLA - Service Level Agreements

DC - Data Center

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

## Introduction

This document describes configuration steps to integrate Application Centric Infrastructure (ACI), Cisco's Software Defined - Data Center (SD-DC) solution with Software Defined - Wide Area Network (SD-WAN) and its verification.

Software Defined Networking (SDN) have been enhanced to accommodate specific network segment:

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

Cisco solution provides robust feature of QoS (Quality of Service) in SD-DC (Application Centric Infrastructure ACI) and AAR (Application Aware Routing)/SLA (Service Level Agreements) profiles in SD-WAN.

As more and more customers are planning to integrate and want to have seamless traffic treatment across the path, Cisco has come up with SD-DC and SD-WAN Integration.

The integration focuses on two use cases:

1. Traffic from ACI (DC) to SDWAN (non ACI Branch)
2. Traffic from SDWAN (non ACI Branch) to ACI (DC)

## Prerequisites

## Requirements

As the integration with SD-WAN happens over the L3 out configured in ACI, so L3out with supported protocol must be configured.

Integration takes place over management network so Management reachability between ACI (APIC controllers) and vManage is required.

## Components Used

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

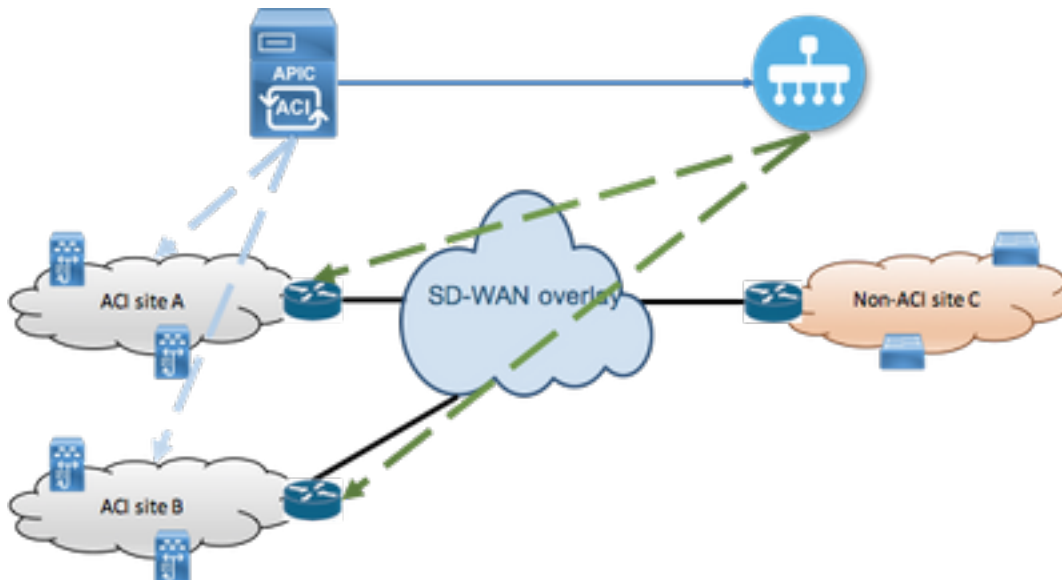
This document is based on ACI version 4.2(3l)

## Configuration

## Network Diagram

Topology for reference:

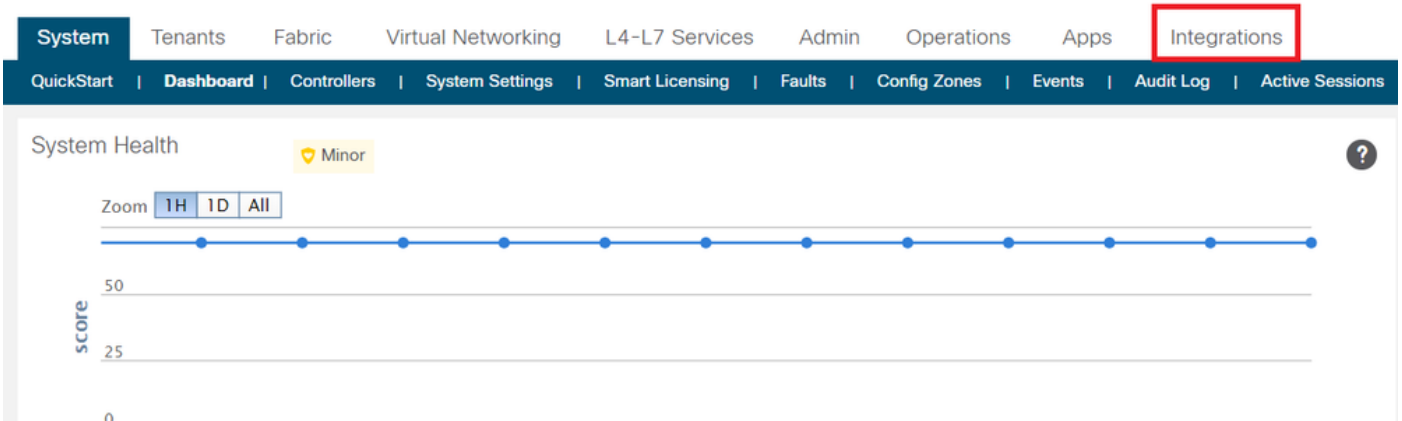
In our topology, consider only ACI site A as DC and non-ACI Site C as SDWAN Branch site.



## Configurations

### Section A: Integration Configuration

1. Open the APIC Graphical User Interface (GUI) and navigate to **Integrations** tab under **System** tab.



## 2. Create Integration Group

System | Tenants | Fabric | Virtual Networking | L4-L7 Services | Admin | Operations | Apps | **Integrations**

ALL GROUPS | **Create Group** | SDWAN1

Integrations

Name: SDWAN2

Security Domains:

Name	Description
------	-------------

Cancel | **Submit**

## 3. Navigate to newly created Integration Group "SDWAN2" and right click on vManage

System | Tenants | Fabric | Virtual Networking | L4-L7 Services | Admin | Operations | Apps | **Integrations**

ALL GROUPS | Create Group | SDWAN1 | **SDWAN2**

Group SDWAN2

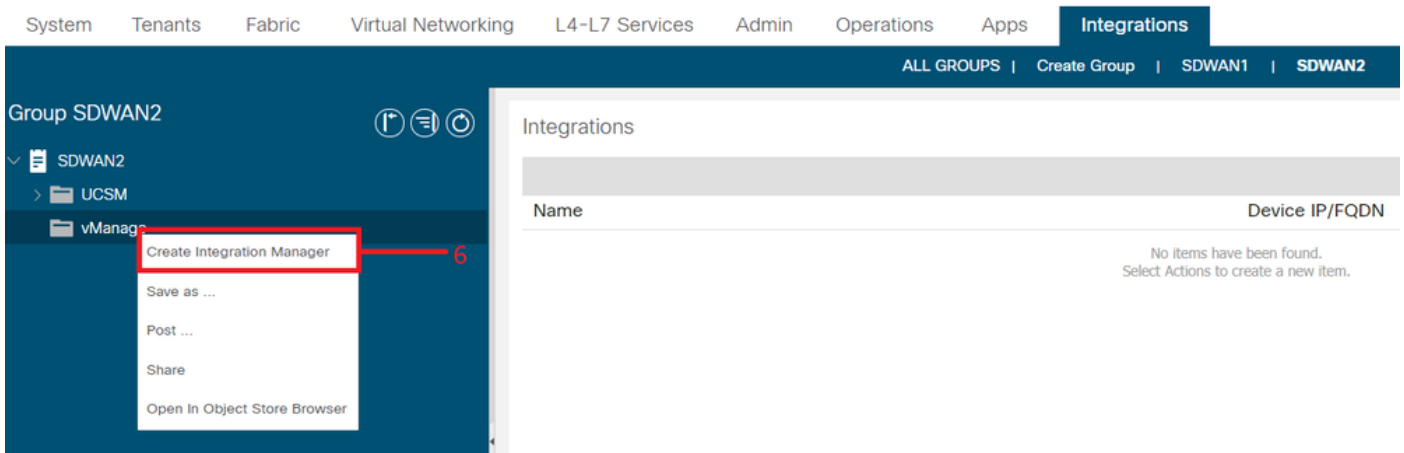
- SDWAN2
  - UCSM
  - vManage**

Integrations

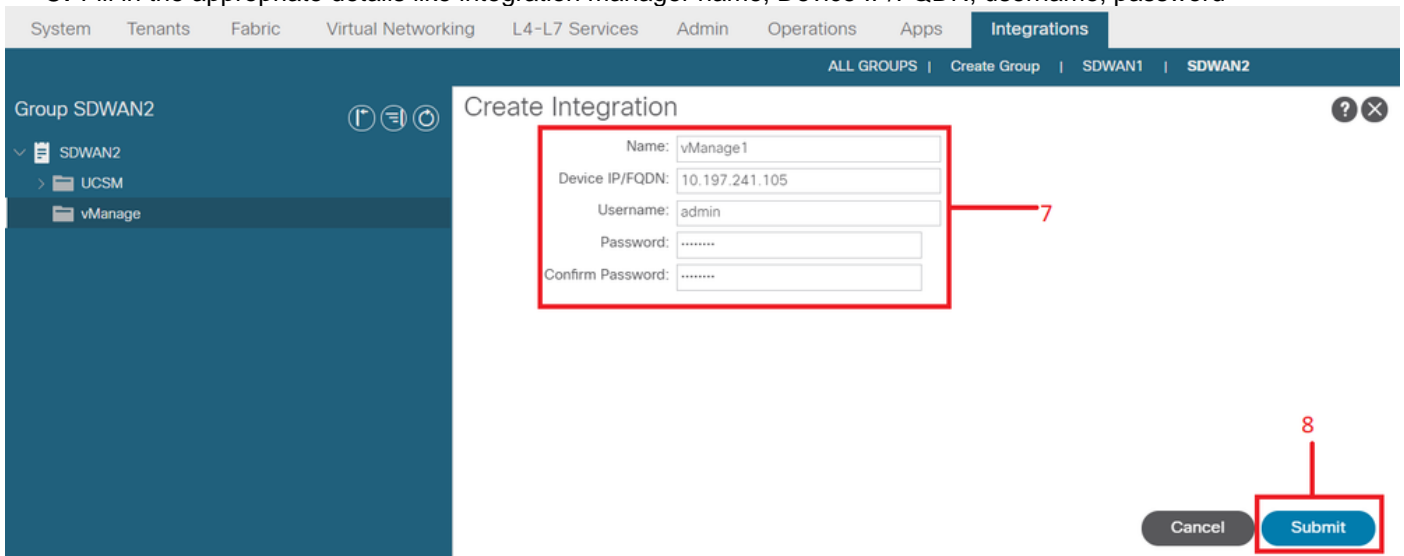
Name	Device IP/FQDN
------	----------------

No items have been found. Select Actions to create a new item.

## 4. Right click on vManage and select Create Integration Manager



5. Fill in the appropriate details like integration manager name, Device IP/FQDN, username, password



6. Ensure that registration is successful from status field. If it is not successful or if any errors observed, verify if provided information is correct. **Partner ID** is identifier of vManage controller. You can navigate to **Integrations - ><Group Name>->vManage -> <Integration Manager Name> -> System info** to verify the status.

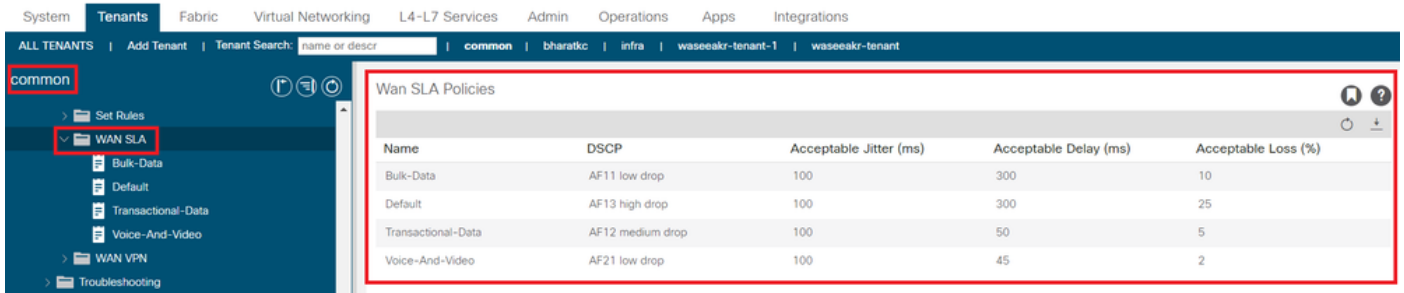


## Section B: Configuration of WAN SLA policy

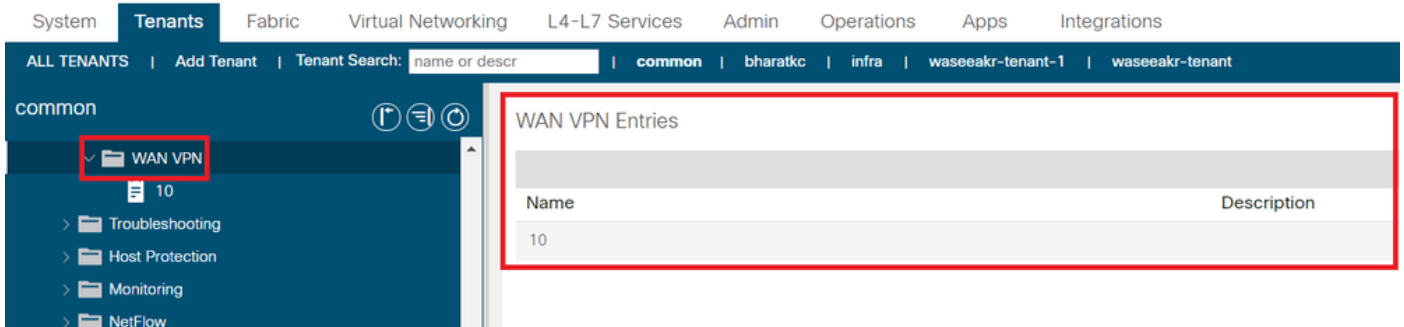
Pre-configured WAN SLA profiles can be found under **Tenants->common->Policies->Protocols->WAN SLA**

This can be inherited in other tenant while configuring the contract using WAN SLA policy.

These are pre-configured SLAs and cannot be changed.



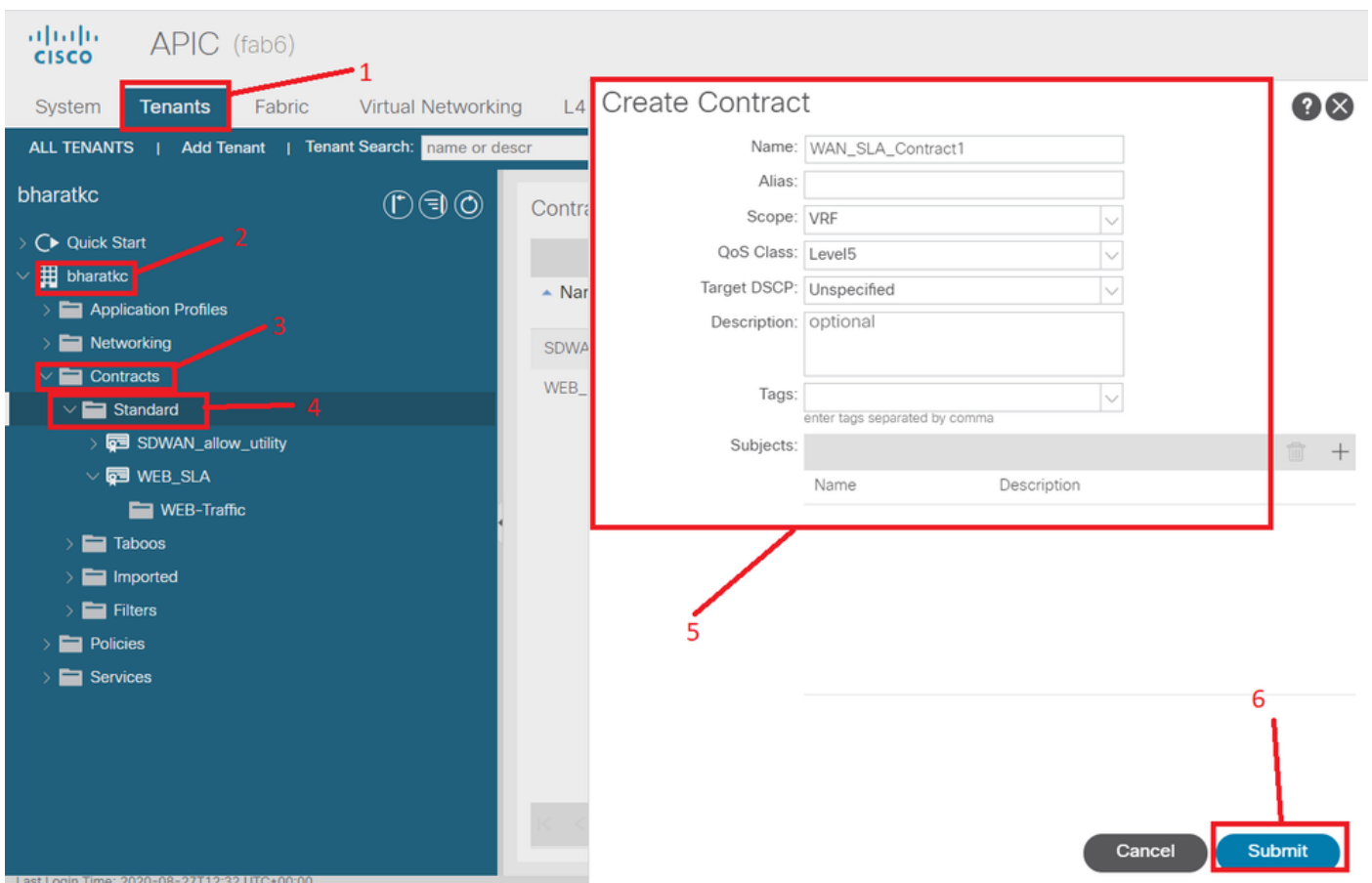
VPN configured on SD-WAN side which is mapped to this ACI integration will also be reflected under **Tenants->common->Policies->Protocols->WAN SLA**



1. Create the contract under the tenant/VRF where you want to map the WAN services.

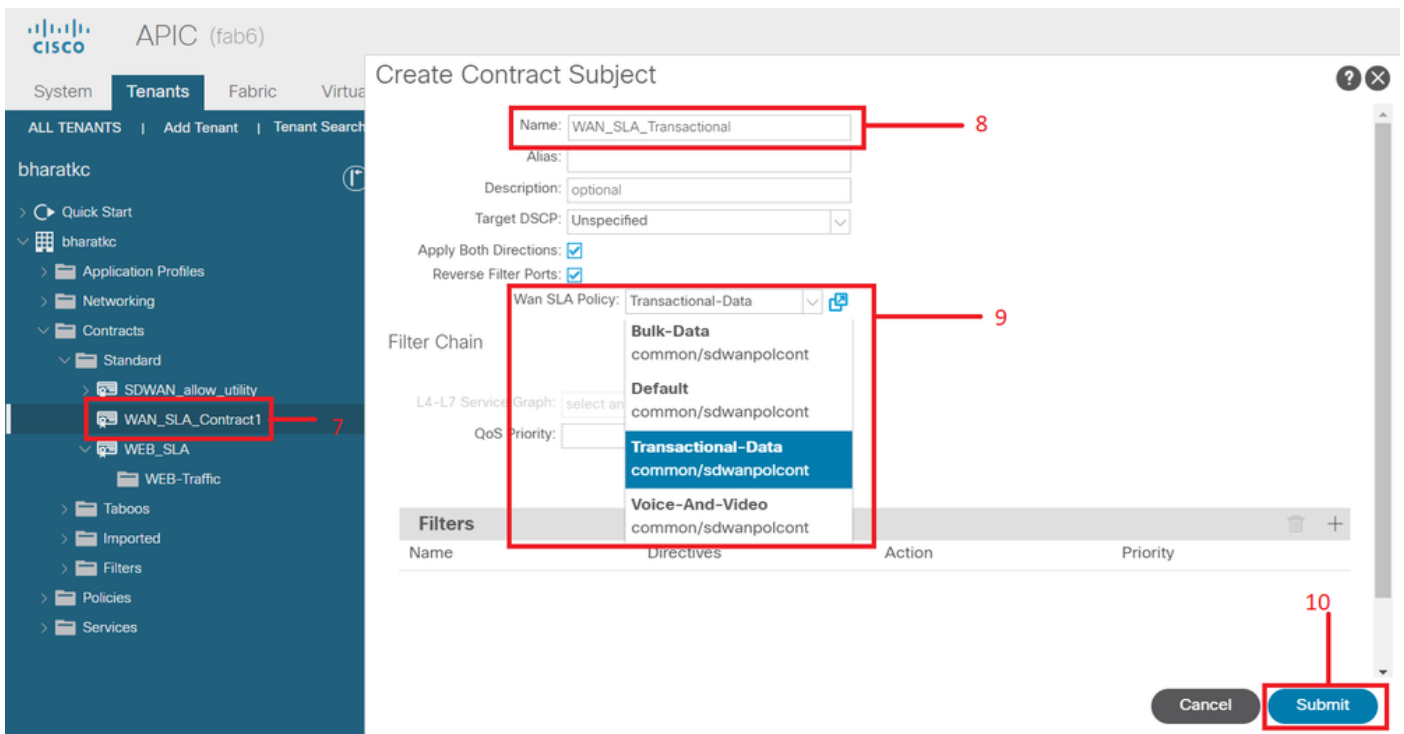
The **QoS Priority** value must be set to any value other than **Unspecified**. The **WAN SLA policies** will not work if the **QoS Priority** value is set to **Unspecified**.

Please navigate to **Tenants-><tenant name>->Contracts->Standard**



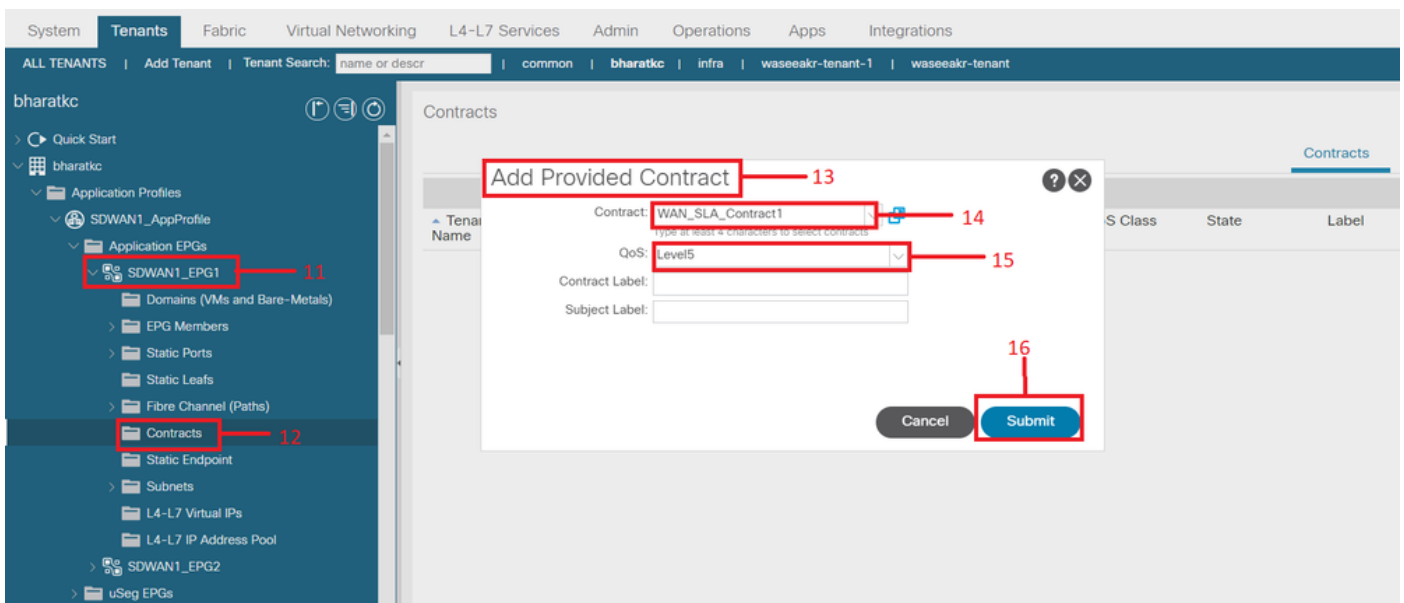
2. Create the Contract Subject and Under Contract Subject, specify WAN SLA Policy.

The **QoS Priority** value must be set to any value other than **Unspecified**. The **WAN SLA policies** will not work if the **QoS Priority** value is set to **Unspecified**.



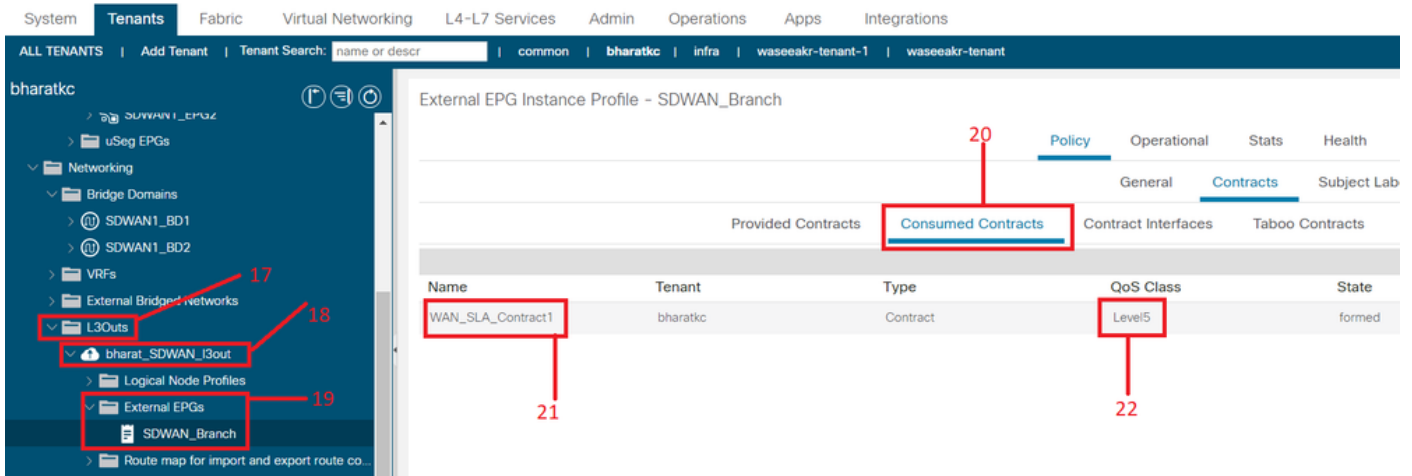
3. Provide the contract from EPG.

Please navigate to **Tenants-><tenant name>->Application Profiles->Application EPG->Contracts**



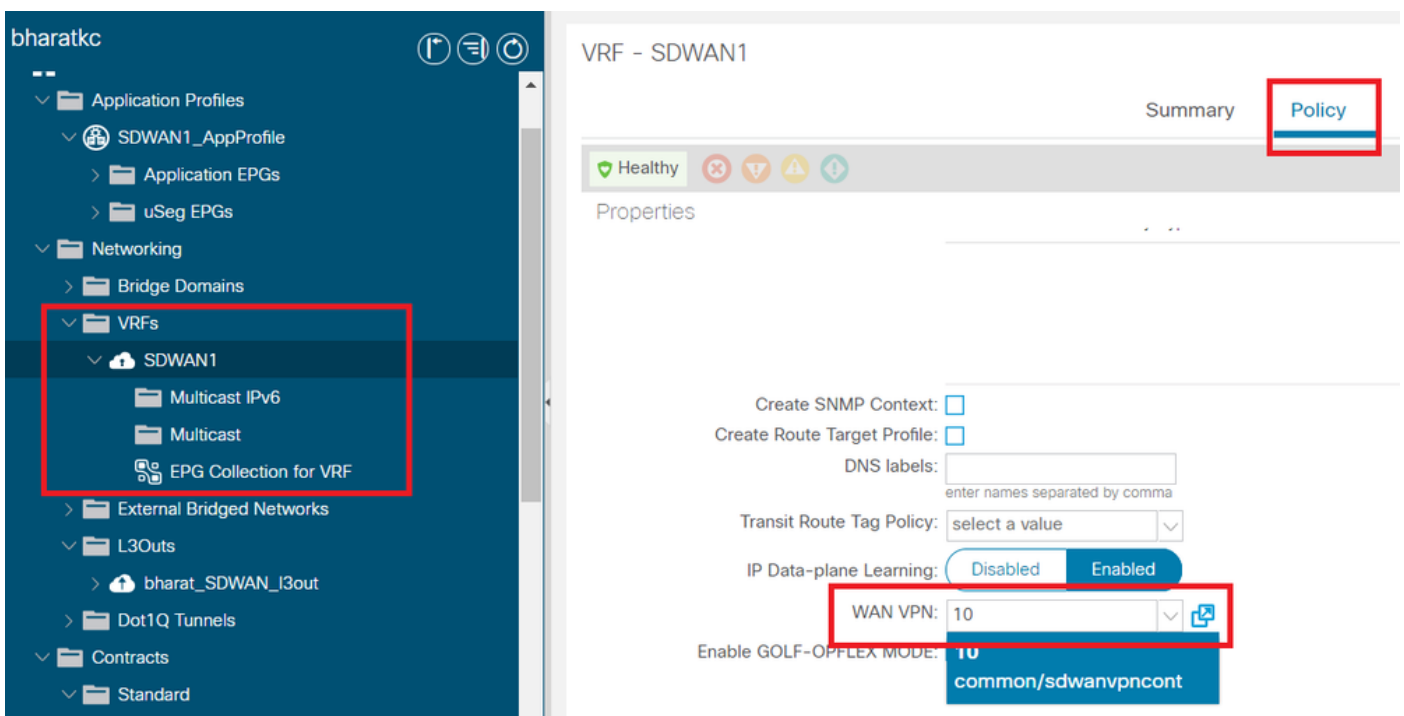
4. Consume the contract at L3out configured for SD-WAN

Please navigate to **Tenants-><tenant name>->L3outs->External EPG->Consumed Contracts**. It is also possible and valid to have contract provided by L3out External EPG and consumed by EPGs



### 5. Match a WAN VPN to a tenant VRF

Please navigate to **Tenants-><tenant name>->VRFs->Policy->WAN VPN**



### Verify

### Section 3: Verification

#### 1. Configuration verification

Configuration is pushed to both SDWAN devices according to configuration in ACI

#### DC end (connected to 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#

**Branch end SDWAN router**

```
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 verification

### Example 1

**WAN SLA Policy "Transactional-Data". Please navigate to Tenants-><tenant name>->Contracts->Standard-><Contract Name>-><Contract Subject>-> General- WAN SLA Policy**

Reverse Filter Ports:

Filters:


Name	Tenant	Action	Priority	Directives	State
default	common	Permit	default level		formed

---

L4-L7 Service Graph:

QoS Priority:

Target DSCP:

Wan SLA Policy:  

```

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

```

## Direction:

### 1. Traffic from DC to SDWAN.

As can be seen in below captures, traffic originated from DC is with **dscp 00** but the traffic reaching to SDWAN is with **DSCP 12** (hex 0x0c).

This indicates DSCP value change according to WAN SLA Policy.

Packet capture performed at source (DC) reflecting original DSCP value to 00.

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

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (**DSCP 0x00**: Default; ECN: 0x00)

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

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

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0xa0d5 (41173)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 255

Protocol: ICMP (0x01)

Header checksum: 0x9016 [correct]

[Good: True]

[Bad : False]

Source: 192.168.10.2 (192.168.10.2)

Destination: 172.16.20.2 (172.16.20.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0 ()

Checksum: 0xc16a [correct]

Identifier: 0x4158

Sequence number: 768 (0x0300)

Data (56 bytes)

Packet capture on destination (SDWAN Branch site) reflecting change in **DSCP 12 (hex 0x0c)** value according to WAN SLA Policy.

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

Version: 4

Header length: 20 bytes

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

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

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

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0xa0d1 (41169)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 251

Protocol: ICMP (0x01)

Header checksum: 0x93ea [correct]

[Good: True]

[Bad : False]

Source: 192.168.10.2 (192.168.10.2)

Destination: 172.16.20.2 (172.16.20.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0 ( )

Checksum: 0x6e30 [correct]

Identifier: 0xc057

Sequence number: 1024 (0x0400)

Data (56 bytes)

## 2. Traffic from SDWAN to DC

As can be seen in below captures, traffic originated from SDWAN Branch site is with dscp 00 but the traffic reaching to DC is with DSCP 12 (hex 0x0c) reflecting the change in DSCP value according to WAN SLA Policy applied.

Packet capture performed at source (SDWAN Branch) reflecting original DSCP value to 00.

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

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (**DSCP 0x00**: Default; ECN: 0x00)

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

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

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0xa0c8 (41160)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 255

Protocol: ICMP (0x01)

Header checksum: 0x9023 [correct]

[Good: True]

[Bad : False]

Source: 172.16.20.2 (172.16.20.2)

Destination: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0 ()

Checksum: 0xd3ff [correct]

Identifier: 0x5c79

Sequence number: 1 (0x0001)

Data (56 bytes)

Packet capture on destination (DC) reflecting change in **DSCP 12 (hex 0x0c)** value according to

WAN SLA Policy.

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

Version: 4

Header length: 20 bytes

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

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

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

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0xa073 (41075)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 251

Protocol: ICMP (0x01)

Header checksum: 0x9448 [correct]

[Good: True]

[Bad : False]

Source: 172.16.20.2 (172.16.20.2)

Destination: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0 ()

Checksum: 0x741a [correct]

Identifier: 0x5c79

Sequence number: 43776 (0xab00)

Data (56 bytes)

## Example 2

**WAN SLA Policy "Voice-And-Video"** Please navigate to Tenants-><tenant name>->Contracts->Standard-><Contract Name>-><Contract Subject>-> General- WAN SLA Policy

Contract Subject - WEB-Traffic

Name	Tenant	Action	Priority	Directives	State
default	common	Permit	default level		formed

L4-L7 Service Graph:

QoS Priority:

Target DSCP:

Wan SLA Policy:

```
sequence 20
match
  dscp 18
action
  sla-class Voice-And-Video
  no sla-class strict
1. Traffic from DC to SDWAN.
```

As can be seen in below captures, traffic originated from DC is with **DSCP 00** but the traffic reaching to SDWAN is with **DSCP 18 (hex 0x12)**.

This indicates DSCP value change according to WAN SLA Policy.

Packet capture performed at source (DC) reflecting original DSCP value to 00.

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

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (**DSCP 0x00**: Default; ECN: 0x00)

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

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

.... ..0 = ECN-CE: 0

Total Length: 84

Identification: 0xa2b6 (41654)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 255

Protocol: ICMP (0x01)

Header checksum: 0x8e35 [correct]

[Good: True]

[Bad : False]

Source: 192.168.10.2 (192.168.10.2)

Destination: 172.16.20.2 (172.16.20.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0 ( )

Checksum: 0x3614 [correct]

Identifier: 0x8c5f

Sequence number: 512 (0x0200)

Data (56 bytes)

Packet capture on **destination (SDWAN Branch site)** reflecting change in **DSCP value 18 (0x12)** matching it with WAN SLA Policy.

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

Version: 4



Header length: 20 bytes

Differentiated Services Field: 0x48 (**DSCP 0x12**: Assured Forwarding 21; ECN: 0x00)

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

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

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0xa2b8 (41656)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 255

Protocol: ICMP (0x01)

Header checksum: 0x8deb [correct]

[Good: True]

[Bad : False]

Source: 172.16.20.2 (172.16.20.2)

Destination: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0 ()

Checksum: 0x8a13 [correct]

Identifier: 0x8c5f

Sequence number: 1024 (0x0400)

Data (56 bytes)

Packet capture on source (SDWAN Branch) showing the original **DSCP value (00)**.

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

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (**DSCP 0x00**: Default; ECN: 0x00)

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

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

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0xa1bb (41403)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 255

Protocol: ICMP (0x01)

Header checksum: 0x8f30 [correct]

[Good: True]

[Bad : False]

Source: 172.16.20.2 (172.16.20.2)

Destination: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0 ()

Checksum: 0x68e5 [correct]

Identifier: 0x1d03

Sequence number: 2048 (0x0800)

Data (56 bytes)

Packet capture on destination (DC) reflecting change in **DSCP value 18 (0x12)** according to WAN SLA Policy.

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

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x48 (**DSCP 0x12**: Assured Forwarding 21; ECN: 0x00)

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

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

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0xa1bb (41403)

Flags: 0x00

0.. = Reserved bit: Not Set

.0. = Don't fragment: Not Set

..0 = More fragments: Not Set

Fragment offset: 0

Time to live: 251

Protocol: ICMP (0x01)

Header checksum: 0x92e8 [correct]

[Good: True]

[Bad : False]

Source: 172.16.20.2 (172.16.20.2)

Destination: 192.168.10.2 (192.168.10.2)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0 ()

Checksum: 0x68e5 [correct]

Identifier: 0x1d03

Sequence number: 2048 (0x0800)

Data (56 bytes)

## Troubleshoot

Following log files are useful from troubleshooting perspective. .

### **Control path debugging**

APIC techsupport files

PolicyDistributor Logs, PolicyManager Logs, PolicyElement, Edmgr logs can provide insight about relevant configuration getting pushed to leaves and spines.

### **Data path debugging**

Packet captures on L3out interface and interfaces on vEdge routers.

ELAM can also help.