

Configuración y verificación de la integración de SDWAN con ACI

Contenido

[Acrónimos](#)

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

Acrónimos

ACI - Infraestructura centrada en aplicaciones

EPG - Grupo de terminales

L3out - Capa 3 de salida

AAR - Routing con reconocimiento de aplicaciones

SLA: acuerdos de nivel de servicio

DC - Data Center

WAN: red de área extensa

SDN - Redes definidas por software

SD DC - Data Center definido por software

SD WAN: red de área extensa definida por software

QoS - Calidad de servicio

VRP: reenvío y routing virtuales

Introducción

Este documento describe los pasos de configuración para integrar Application Centric Infrastructure (ACI), la solución definida por software de Cisco: Data Center (SD-DC) con Software Defined - Wide Area Network (SD-WAN) y su verificación.

Red definida por software (SDN) se han mejorado para adaptarse a segmentos de red específicos:

1. Definido por software: Data Center (SD-DC)
2. Definido por software: red de área extensa (SD-WAN)

La solución de Cisco proporciona una función sólida de los perfiles QoS (calidad de servicio) en SD-DC (Application Centric Infrastructure ACI) y AAR (Application Aware Routing)/SLA (Service Level Agreement) en SD-WAN.

A medida que cada vez más clientes planean integrarse y desean un tratamiento del tráfico fluido en toda la ruta, Cisco ha desarrollado una integración SD-DC y SD-WAN.

La integración se centra en dos casos prácticos:

1. Tráfico de ACI (DC) a SDWAN (sin sucursal ACI)
2. Tráfico de SDWAN (sucursal no ACI) a ACI (DC)

Prerequisites

Requirements

A medida que la integración con SD-WAN se produce sobre la L3 out configurada en ACI, se debe configurar L3out con el protocolo soportado.

La integración se produce en la red de gestión, por lo que se requiere la disponibilidad de la gestión entre ACI (controladores APIC) y vManage.

Componentes Utilizados

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

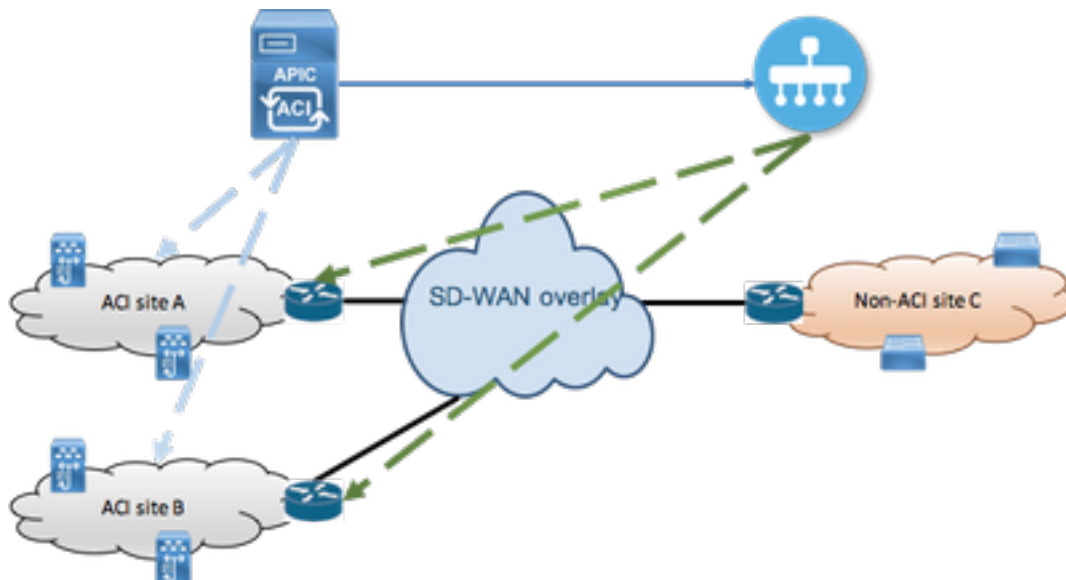
Este documento se basa en la versión 4.2(3) de ACI

Configuración

Diagrama de la red

Topología de referencia:

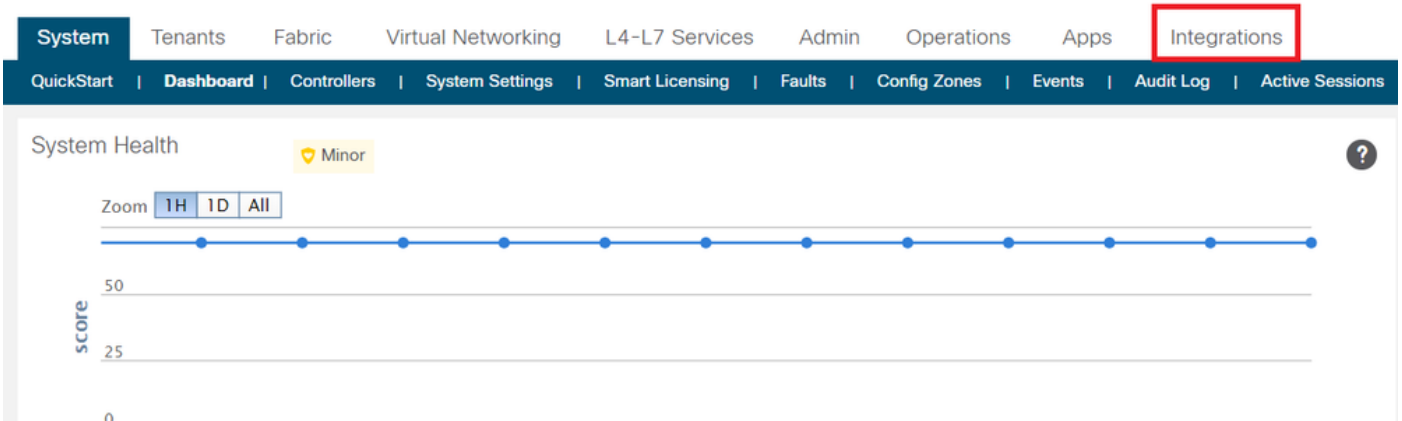
En nuestra topología, considere solo el sitio A de ACI como sitio C de DC y el sitio C no ACI como sitio de sucursal de SDWAN.



Configuraciones

Sección A: Configuración de integración

1. Abra la interfaz gráfica de usuario (GUI) de APIC y acceda a la pestaña **Integraciones** bajo la pestaña **Sistema**.



2. Crear grupo de integración

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

ALL GROUPS | **Create Group** | SDWAN1

Integrations

Name

SDWAN1

Create Integration Group

Name:

Security Domains:

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

Cancel **Submit**

3. Navegue hasta el grupo de integración recientemente creado "SDWAN2" y haga clic con el botón derecho en **vManage**

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

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

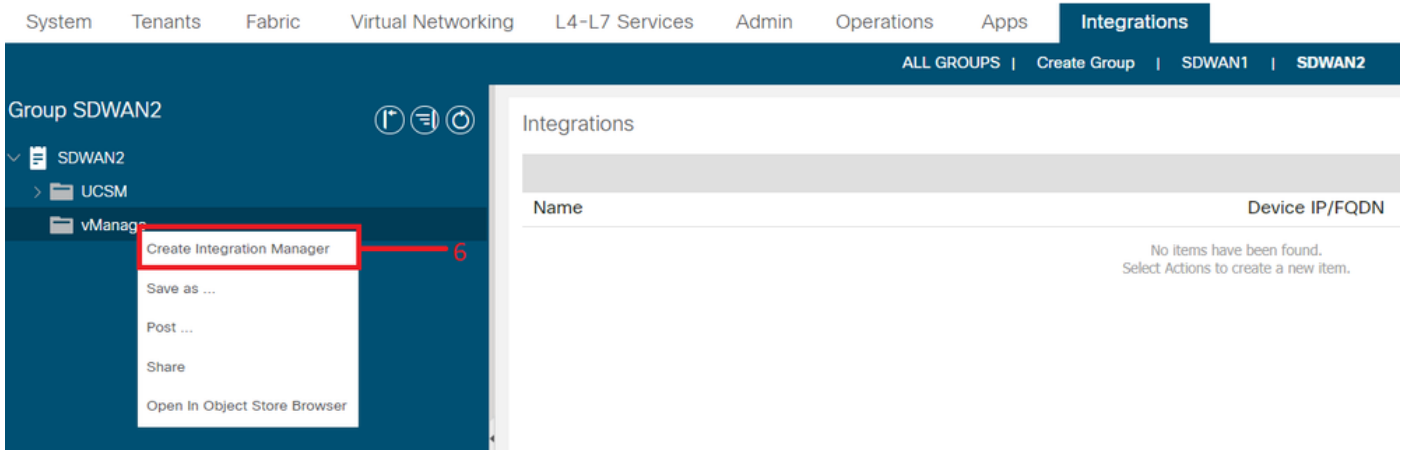
Group SDWAN2

- SDWAN2
 - UCSM
 - vManage**

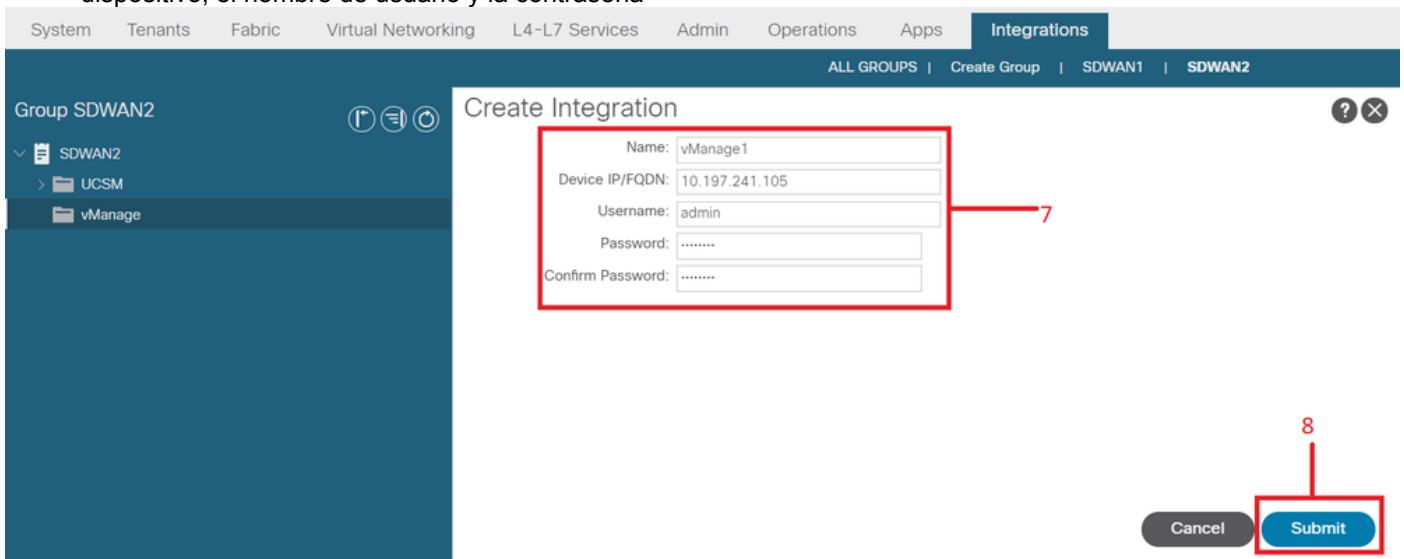
Integrations

Name	Device IP/FQDN
No items have been found. Select Actions to create a new item.	

4. Haga clic con el botón derecho en **vManage** y seleccione **Create Integration Manager**



5. Introduzca los detalles adecuados, como el nombre del administrador de integración, la dirección IP/FQDN del dispositivo, el nombre de usuario y la contraseña



6. Asegúrese de que el registro se realiza correctamente desde el campo de estado. Si no es exitosa o si se observa algún error, verifique si la información proporcionada es correcta. **La ID del partner** es el identificador del controlador vManage. Puede navegar hasta **Integrations -><Group Name>->vManage -> <Integration Manager Name> -> System info** para verificar el estado.



Sección B: Configuración de la política de SLA de WAN

Los perfiles de SLA de WAN preconfigurados se pueden encontrar en **Arrendatarios->comunes->políticas->protocolos->SLA de WAN**

Esto se puede heredar en otro arrendatario mientras se configura el contrato mediante la política WAN SLA.

Estos son SLA preconfigurados y no se pueden cambiar.

Name	DSCP	Acceptable Jitter (ms)	Acceptable Delay (ms)	Acceptable Loss (%)
Bulk-Data	AF11 low drop	100	300	10
Default	AF13 high drop	100	300	25
Transactional-Data	AF12 medium drop	100	50	5
Voice-And-Video	AF21 low drop	100	45	2

La VPN configurada en el lado SD-WAN que se asigna a esta integración de ACI también se reflejará en **Arrendatarios->comunes->políticas->protocolos->SLA de WAN**

Name	Description
10	

1. Cree el contrato en el arrendatario/VRF donde desea asignar los servicios WAN.

El valor **QoS Priority** se debe establecer en cualquier valor que no sea **Unspecific**. Las políticas WAN SLA no funcionarán si el valor **QoS Priority** se establece en **Unspecific**.

Desplácese hasta **Arrendatarios-><nombre del arrendatario>->Contratos->Estándar**

1. Tenants

2. bharatk

3. Contracts

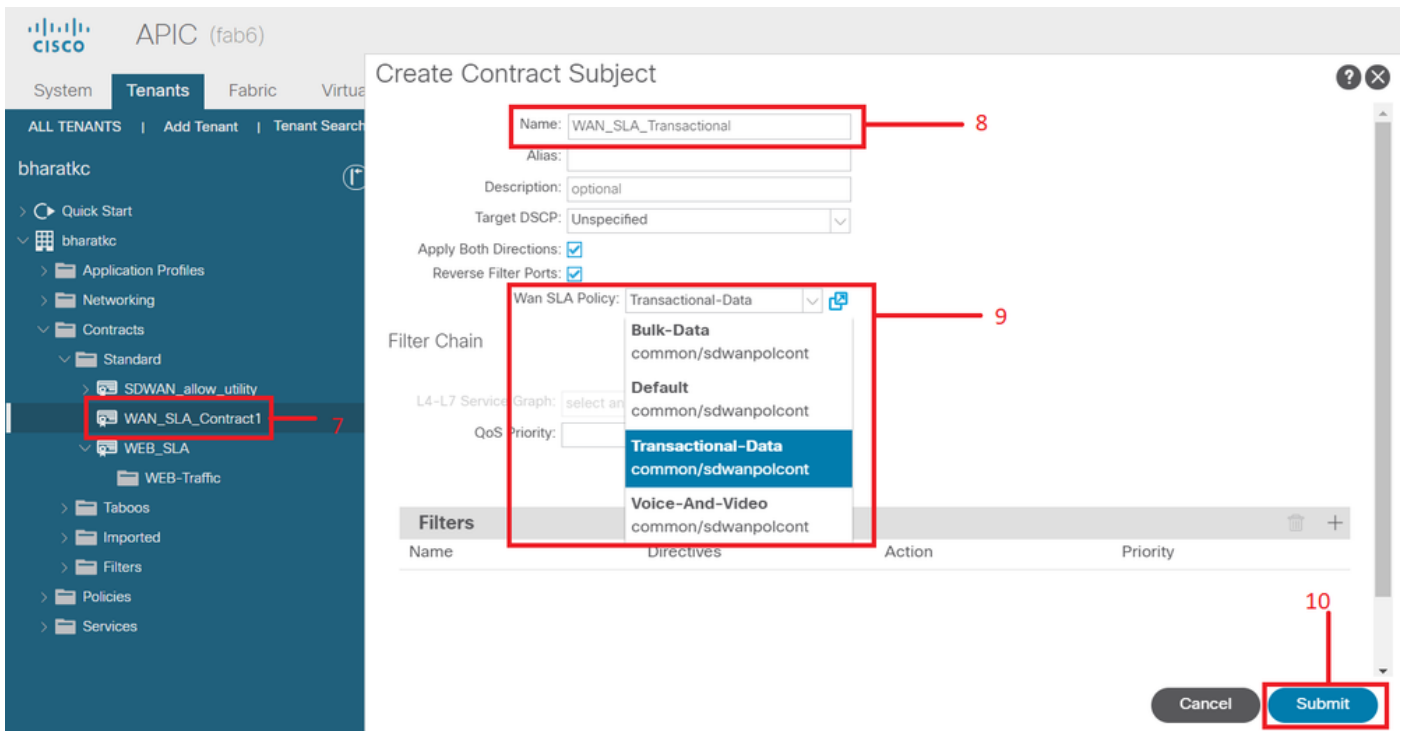
4. Standard

5. Subjects

6. Submit

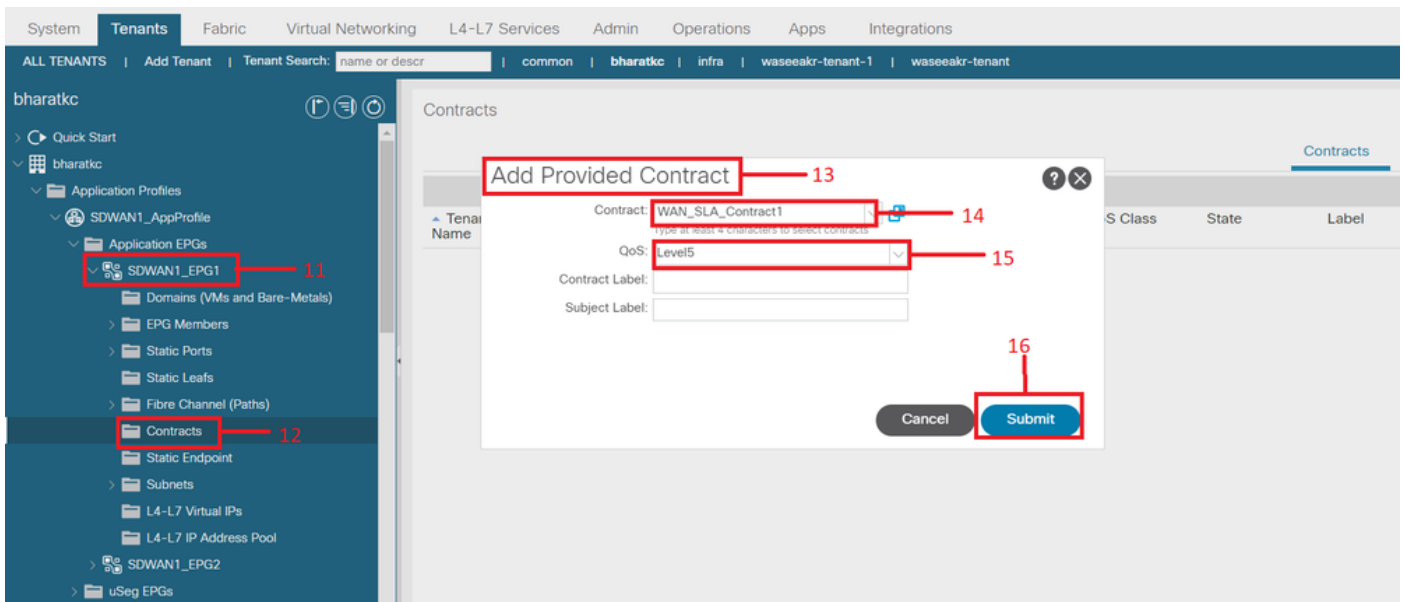
2. Cree el asunto del contrato y, en Asunto del contrato, especifique la política de SLA de WAN.

El valor **QoS Priority** se debe establecer en cualquier valor que no sea **Unspecific**. Las políticas WAN SLA no funcionarán si el valor **QoS Priority** se establece en **Unspecific**.



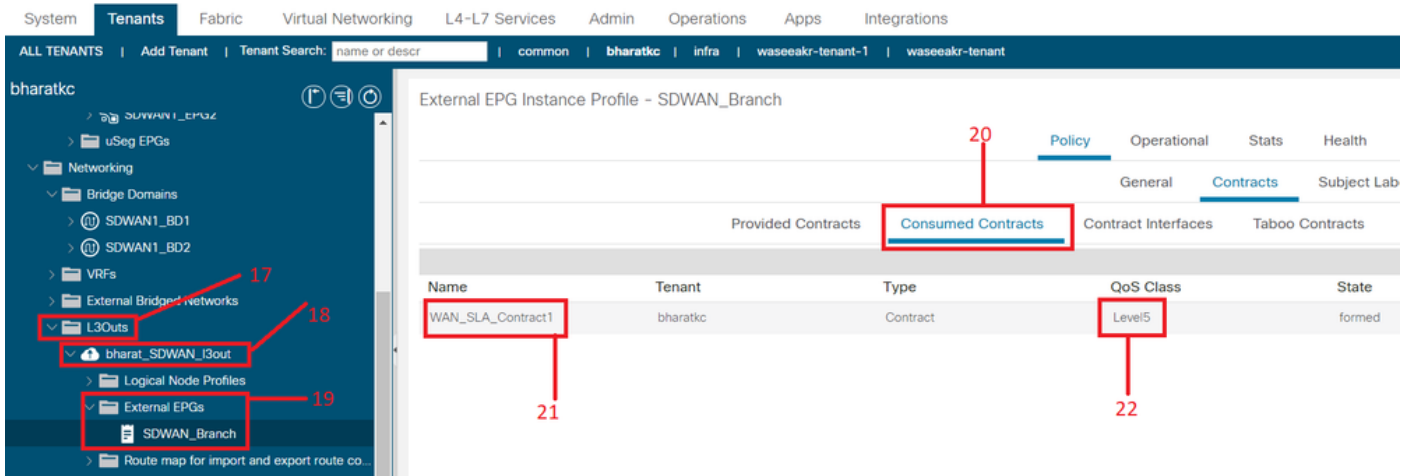
3. Proporcione el contrato de EPG.

Desplácese hasta **Arrendatarios-><nombre del arrendatario>->Perfiles de aplicación->EPG de aplicación->Contratos**

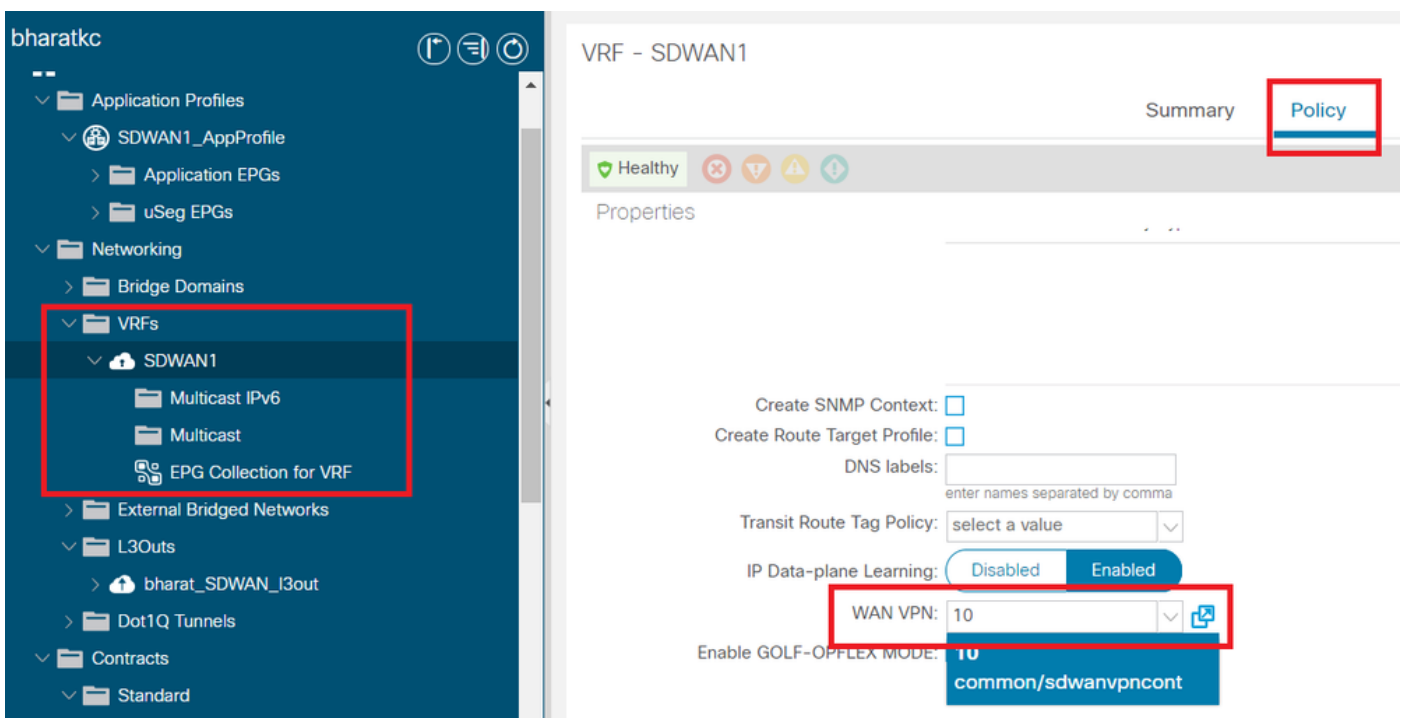


4. Consumir el contrato en L3out configurado para SD-WAN

Desplácese hasta **Arrendatarios-><nombre del arrendatario>->L3outs->EPG externo->Contratos consumidos**. También es posible y válido tener un contrato proporcionado por L3out External EPG y consumido por EPG



5. Hacer coincidir una VPN WAN con un VRF de arrendatario
 Desplácese hasta **Arrendatarios-><nombre del arrendatario>->VRF->Política->VPN WAN**



Verificación

Sección 3: Verificación

1. Verificación de la configuración

La configuración se envía a ambos dispositivos SDWAN según la configuración de ACI

Ruta SDWAN de extremo DC (conectada a L3out)

```
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#

Router de extremo de la sucursal SDWAN

```
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

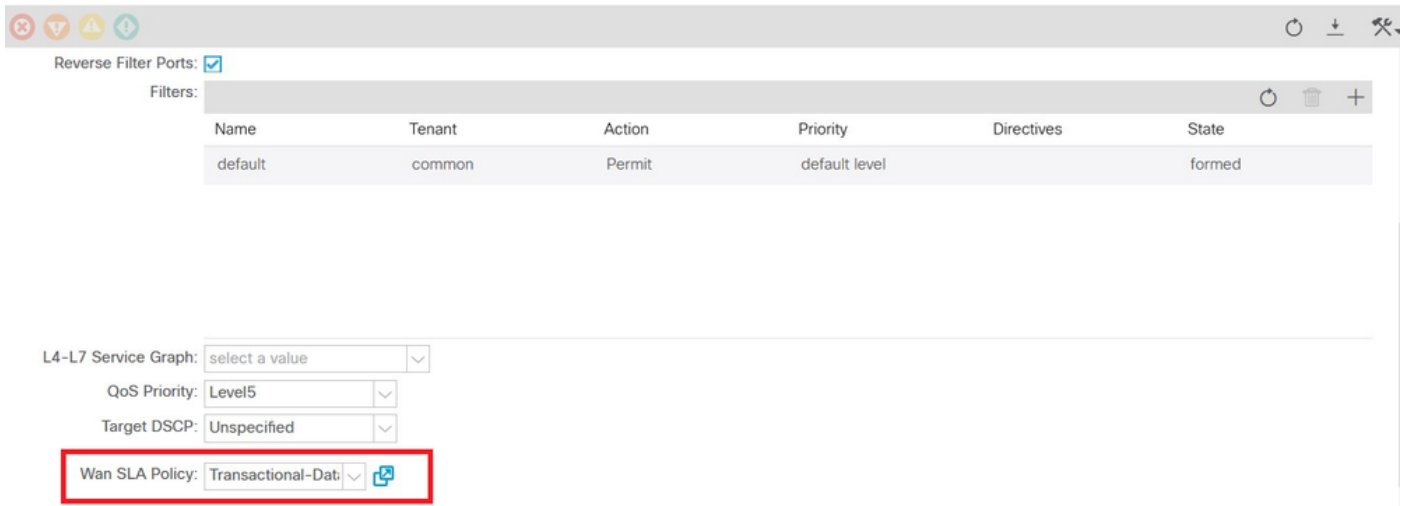
from-vsmart lists vpn-list 412898115_vpn
vpn 10
```

ASR1001-X-Branch#

1. Verificación de QoS

Ejemplo 1

Política de SLA de WAN "Transactional-Data" (Datos transaccionales). Desplácese hasta Arrendatarios-><nombre del arrendatario>->Contratos->Estándar-><nombre del contrato>-><asunto del contrato>-> General- Política de SLA de WAN



```

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

```

Dirección:

1. Tráfico de DC a SDWAN.

Como se puede ver en las capturas siguientes, el tráfico originado desde DC es con **dscp 00** pero el tráfico que llega a SDWAN es con **DSCP 12** (hex 0x0c).

Esto indica el cambio de valor DSCP según la política de SLA de WAN.

Captura de paquetes realizada en el origen (DC) que refleja el valor DSCP original a 00.

Protocolo De Internet, Src: 192.168.10.2 (192.168.10.2), Dst: 172.16.20.2 (172.16.20.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x00 (**DSCP 0x00**: Predeterminado; ECN: 0x00)

0000 00... = Codepoint de servicios diferenciados: Predeterminado (0x00)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa0d5 (41173)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 255

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x9016 [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 192.168.10.2 (192.168.10.2)

Destino: 172.16.20.2 (172.16.20.2)

Protocolo de mensajes de control de Internet

Tipo: 8 (Solicitud de eco (ping))

Código: 0 ()

Suma de comprobación: 0xc16a [correcto]

Identifier: 0x4158

Número de secuencia: 768 (0x0300)

Datos (56 bytes)

Captura de paquetes en el destino (sitio de la sucursal de SDWAN) que refleja el cambio en el valor **DSCP 12 (hex 0x0c)** según la política de SLA de WAN.

Protocolo De Internet, Src: 192.168.10.2 (192.168.10.2), Dst: 172.16.20.2 (172.16.20.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x30 (**DSCP 0x0c**: Reenvío Asegurado 12; ECN: 0x00)

0011 00.. = Codepoint de servicios diferenciados: Reenvío asegurado 12 (0x0c)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa0d1 (41169)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 251

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x93ea [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 192.168.10.2 (192.168.10.2)

Destino: 172.16.20.2 (172.16.20.2)

Protocolo de mensajes de control de Internet

Tipo: 8 (Solicitud de eco (ping))

Código: 0 ()

Suma de comprobación: 0x6e30 [correcto]

Identificador: 0xc057

Número de secuencia: 1024 (0x0400)

Datos (56 bytes)

2. Tráfico de SDWAN a DC

Como se puede ver en las capturas siguientes, el tráfico originado en el sitio de la sucursal de SDWAN es con dscp 00, pero el tráfico que llega al DC es con DSCP 12 (hex 0x0c) que refleja el cambio en el valor DSCP según la política de SLA de WAN aplicada.

Captura de paquetes realizada en el origen (rama de SDWAN) que refleja el valor DSCP original a 00.

Protocolo De Internet, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x00 (**DSCP 0x00**: Predeterminado; ECN: 0x00)

0000 00... = Codepoint de servicios diferenciados: Predeterminado (0x00)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa0c8 (41160)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 255

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x9023 [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 172.16.20.2 (172.16.20.2)

Destino: 192.168.10.2 (192.168.10.2)

Protocolo de mensajes de control de Internet

Tipo: 8 (Solicitud de eco (ping))

Código: 0 ()

Suma de comprobación: 0xd3ff [correcto]

Identifier: 0x5c79

Número de secuencia: 1 (0x0001)

Datos (56 bytes)

Captura de paquetes en el destino (DC) que refleja el cambio en el valor **DSCP 12 (hex 0x0c)** según la política de SLA de WAN.

Protocolo De Internet, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x30 (**DSCP 0x0c**: Reenvío Asegurado 12; ECN: 0x00)

0011 00.. = Codepoint de servicios diferenciados: Reenvío asegurado 12 (0x0c)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa073 (41075)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 251

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x9448 [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 172.16.20.2 (172.16.20.2)

Destino: 192.168.10.2 (192.168.10.2)

Protocolo de mensajes de control de Internet

Tipo: 8 (Solicitud de eco (ping))

Código: 0 ()

Suma de comprobación: 0x741a [correcto]

Identifier: 0x5c79

Número de secuencia: 43776 (0xab00)

Datos (56 bytes)

Ejemplo 2

Política de SLA de WAN "Voice-And-Video" Desplácese hasta Arrendatarios-><nombre del arrendatario>->Contratos->Estándar-><Nombre del contrato>-><Asunto del contrato>-> Política general de SLA de WAN

Contract Subject - WEB-Traffic

The screenshot shows a configuration page for a WAN SLA Policy. The page title is "Contract Subject - WEB-Traffic". There are tabs for "Policy", "Faults", and "Histor". Under the "Policy" tab, there are sub-tabs for "General", "Subject Exception", and "Labels". The "General" tab is active. Below the tabs, there is a "Reverse Filter Ports" checkbox which is checked. A "Filters" table is displayed with the following data:

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

Below the filters, there are several dropdown menus for configuration:

- L4-L7 Service Graph: select a value
- QoS Priority: Level5
- Target DSCP: Unspecified
- Wan SLA Policy: Voice-And-Video (highlighted with a red box)

```
sequence 20
```

```
match
```

```
  dscp 18
```

```
action
```

```
  sla-class Voice-And-Video
```

```
    no sla-class strict
```

1. Tráfico de DC a SDWAN.

Como se puede ver en las capturas siguientes, el tráfico originado desde DC es con **DSCP 00** pero el tráfico que llega a SDWAN es con **DSCP 18 (hex 0x12)**.

Esto indica el cambio de valor DSCP según la política de SLA de WAN.

Captura de paquetes realizada en el origen (DC) que refleja el valor DSCP original a 00.

Protocolo De Internet, Src: 192.168.10.2 (192.168.10.2), Dst: 172.16.20.2 (172.16.20.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x00 (**DSCP 0x00**: Predeterminado; ECN: 0x00)

0000 00... = Codepoint de servicios diferenciados: Predeterminado (0x00)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa2b6 (41654)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 255

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x8e35 [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 192.168.10.2 (192.168.10.2)

Destino: 172.16.20.2 (172.16.20.2)

Protocolo de mensajes de control de Internet

Tipo: 8 (Solicitud de eco (ping))

Código: 0 ()

Suma de comprobación: 0x3614 [correcto]

Identificador: 0x8c5f

Número de secuencia: 512 (0x0200)

Datos (56 bytes)

La captura de paquetes en **destino (sitio de sucursal de SDWAN)** refleja el cambio en el **valor DSCP 18 (0x12)** que coincide con la política de SLA de WAN.

Protocolo De Internet, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x48 (**DSCP 0x12**: Reenvío garantizado 21; ECN: 0x00)

0100 10... = Codepoint de servicios diferenciados: Reenvío garantizado 21 (0x12)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa2b8 (41656)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 255

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x8deb [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 172.16.20.2 (172.16.20.2)

Destino: 192.168.10.2 (192.168.10.2)

Protocolo de mensajes de control de Internet

Tipo: 0 (Respuesta de eco (ping))

Código: 0 ()

Suma de comprobación: 0x8a13 [correcto]

Identifier: 0x8c5f

Número de secuencia: 1024 (0x0400)

Datos (56 bytes)

2. Tráfico de SDWAN a DC.

Captura de paquetes en el origen (rama de SDWAN) que muestra el **valor DSCP original (00)**.

Protocolo De Internet, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x00 (**DSCP 0x00**: Predeterminado; ECN: 0x00)

0000 00... = Codepoint de servicios diferenciados: Predeterminado (0x00)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa1bb (41403)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 255

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x8f30 [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 172.16.20.2 (172.16.20.2)

Destino: 192.168.10.2 (192.168.10.2)

Protocolo de mensajes de control de Internet

Tipo: 8 (Solicitud de eco (ping))

Código: 0 ()

Suma de comprobación: 0x68e5 [correcto]

Identifier: 0x1d03

Número de secuencia: 2048 (0x0800)

Datos (56 bytes)

Captura de paquetes en el destino (DC) que refleja el cambio en el **valor DSCP 18 (0x12)** según la política de SLA de WAN.

Protocolo De Internet, Src: 172.16.20.2 (172.16.20.2), Dst: 192.168.10.2 (192.168.10.2)

Versión: 4

Longitud del encabezado: 20 bytes

Campo Servicios diferenciados: 0x48 (**DSCP 0x12**: Reenvío garantizado 21; ECN: 0x00)

0100 10... = Codepoint de servicios diferenciados: Reenvío garantizado 21 (0x12)

.... ..0. = Transporte compatible con ECN (ECT): 0

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

Longitud Total: 84

Identificación: 0xa1bb (41403)

Indicadores: 0x00

0. = Bit reservado: no establecido

.0. = No fragmentar: no establecido

..0 = Más fragmentos: no establecido

Desplazamiento del fragmento: 0

Tiempo de vida: 251

Protocolo: ICMP (0x01)

Checksum de encabezado: 0x92e8 [correcto]

[Bien: Verdadero]

[Malo: Falso]

Fuente: 172.16.20.2 (172.16.20.2)

Destino: 192.168.10.2 (192.168.10.2)

Protocolo de mensajes de control de Internet

Tipo: 8 (Solicitud de eco (ping))

Código: 0 ()

Suma de comprobación: 0x68e5 [correcto]

Identifier: 0x1d03

Número de secuencia: 2048 (0x0800)

Datos (56 bytes)

Troubleshoot

Los siguientes archivos de registro son útiles desde la perspectiva de la solución de problemas. .

Depuración de trayecto de control

Archivos de soporte técnico APIC

Registros de distribuidor de políticas, registros de PolicyManager, registros de PolicyElement, registros de Edmgr pueden proporcionar información sobre la configuración relevante que se envía a hojas y columnas.

Depuración de ruta de datos

Capturas de paquetes en la interfaz L3out e interfaces en los routers vEdge.

ELAM también puede ayudar.