ACIとのSDWAN統合の設定と検証

内容

短縮形

ACI:Application Centric Infrastructure（アプリケーションセントリックインフラストラクチャ）

EPG:EndPointグループ

L3out – レイヤ3出力

AAR:Application Aware Routing（アプリケーション認識ルーティング）

SLA:Service Level Agreement（サービスレベル契約）

DC – データセンター

WAN:Wide Area Network（ワイドエリアネットワーク）

SDN:Software Defined Networking（ソフトウェア定義型ネットワーク）

SD DC – ソフトウェア定義型データセンター

SD WAN:Software Defined Wide Area Network（ソフトウェア定義ワイドエリアネットワーク）

QoS：Quality of Service

VRF:Virtual Routing and Forwarding（仮想ルーティングおよび転送）

はじめに

このドキュメントでは、アプリケーションセントリックインフラストラクチャ(ACI)、シスコのSoftware Defined - Data Center(SD-DC)ソリューションをSoftware Defined - Wide Area Network(SD-WAN)と統合するための設定手順と、その検証について説明します。

ソフトウェア定義型ネットワーキング（SDN）特定のネットワークセグメントに対応するように拡張されています。

1. ソフトウェア定義型 – データセンター(SD-DC)
2. ソフトウェア定義型 – ワイドエリアネットワーク(SD-WAN)

シスコのソリューションは、SD-DC（アプリケーションセントリックインフラストラクチャACI）でQoS(Quality of Service)の堅牢な機能を提供し、SD-WANでAAR（アプリケーション認識型ルーティング）/SLA（サービスレベル契約）プロファイルを提供します。

統合を計画し、パス全体でシームレスなトラフィック処理を行いたいと考えているお客様が増えるにつれて、シスコはSD-DCとSD-WANの統合を提案しました。

この統合では、次の2つの使用例に重点が置かれています。

1. ACI(DC)からSDWAN（非ACIブランチ）へのトラフィック
2. SDWAN（非ACIブランチ）からACI(DC)へのトラフィック

前提条件

要件

SD-WANとの統合は、ACIで設定されたL3アウトを介して行われるため、サポートされているプロトコルを使用したL3アウトを設定する必要があります。

統合は管理ネットワーク上で行われるため、ACI（APICコントローラ）とvManage間の管理到達可能性が必要になります。

使用するコンポーネント

ACIファブリック、SDWAN(vManage、vSmart Controller、vEdge)

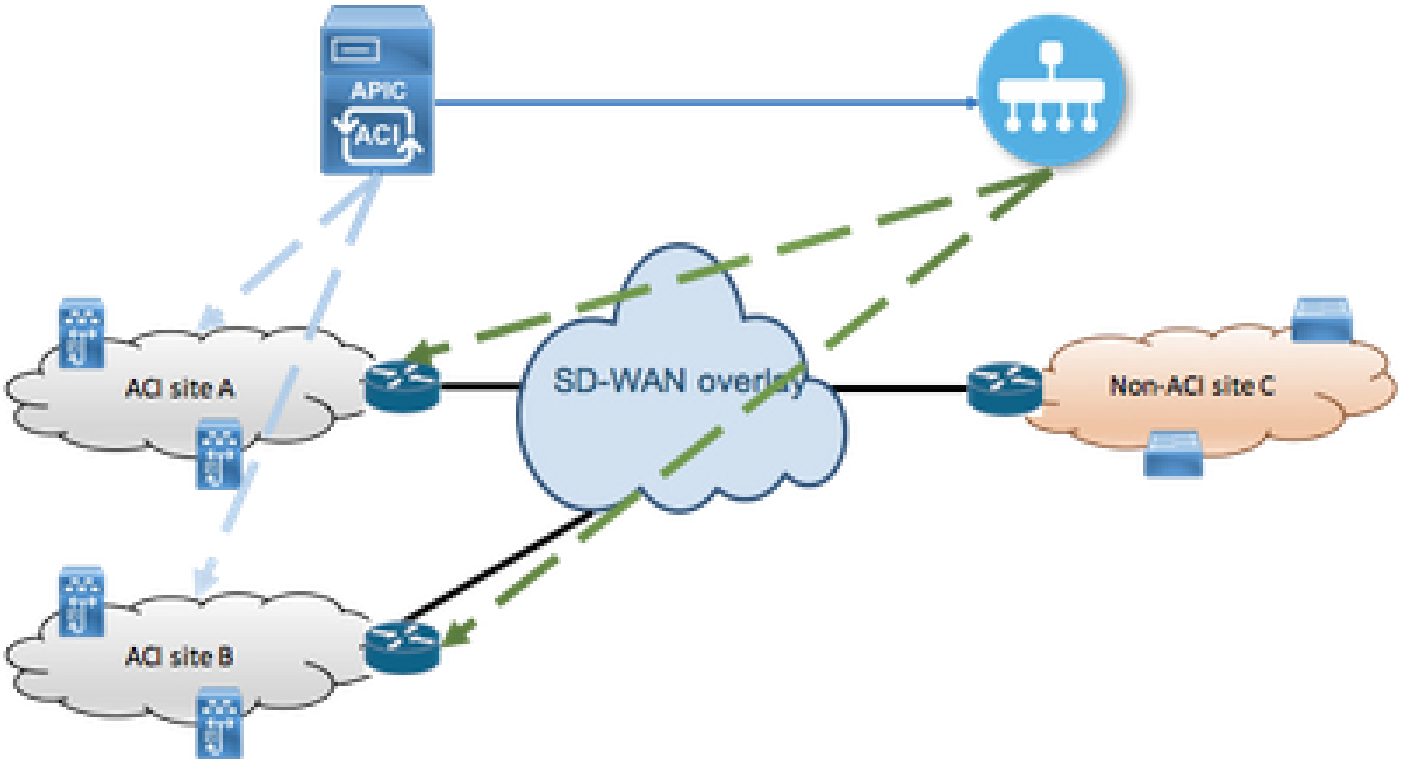
このドキュメントは、ACIバージョン4.2(3l)に基づいています

コンフィギュレーション

ネットワーク図

参考トポロジ：

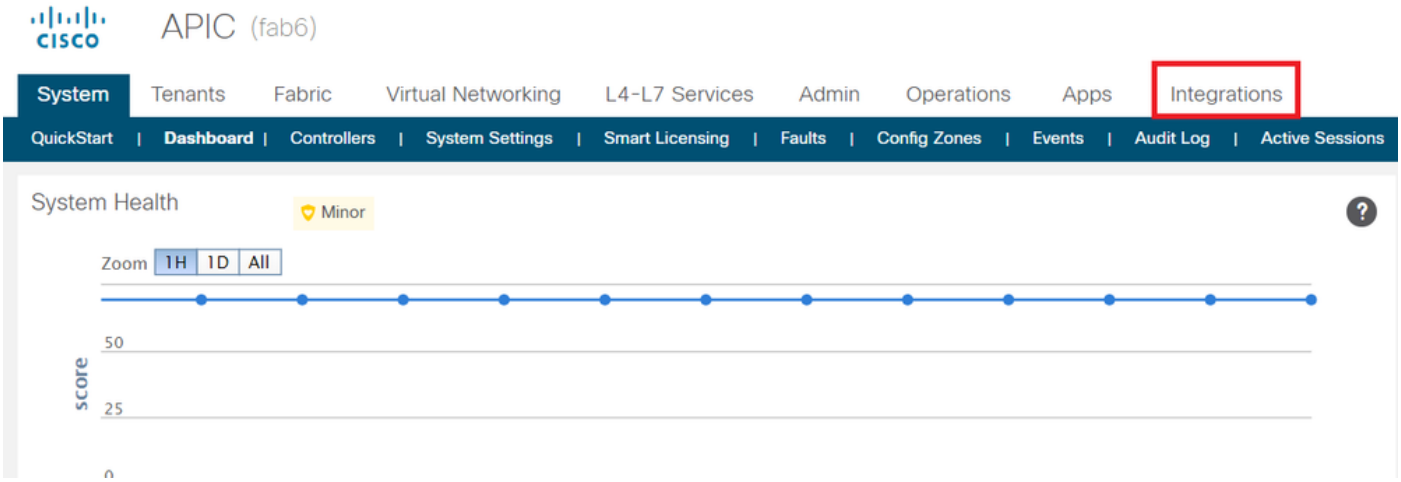
このトポロジでは、ACIサイトAのみをDCとして考慮し、非ACIサイトCをSDWANブランチサイトとして考慮します。



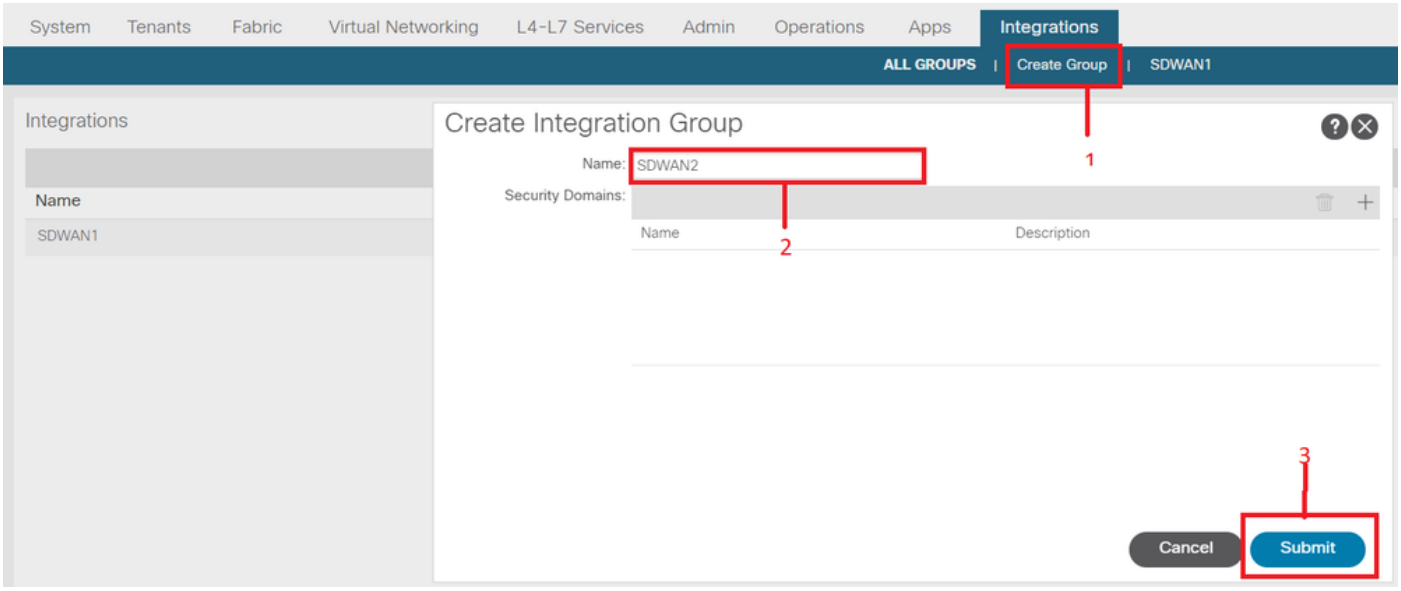
コンフィギュレーション

セクションA：統合設定

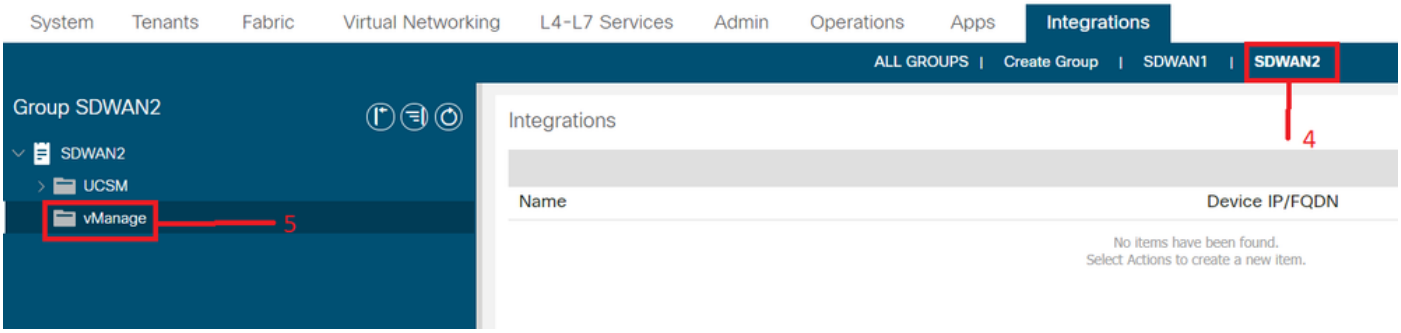
1. APICグラフィカルユーザインターフェイス(GUI)を開き、Systemタブの下のIntegrationsタブに移動します。



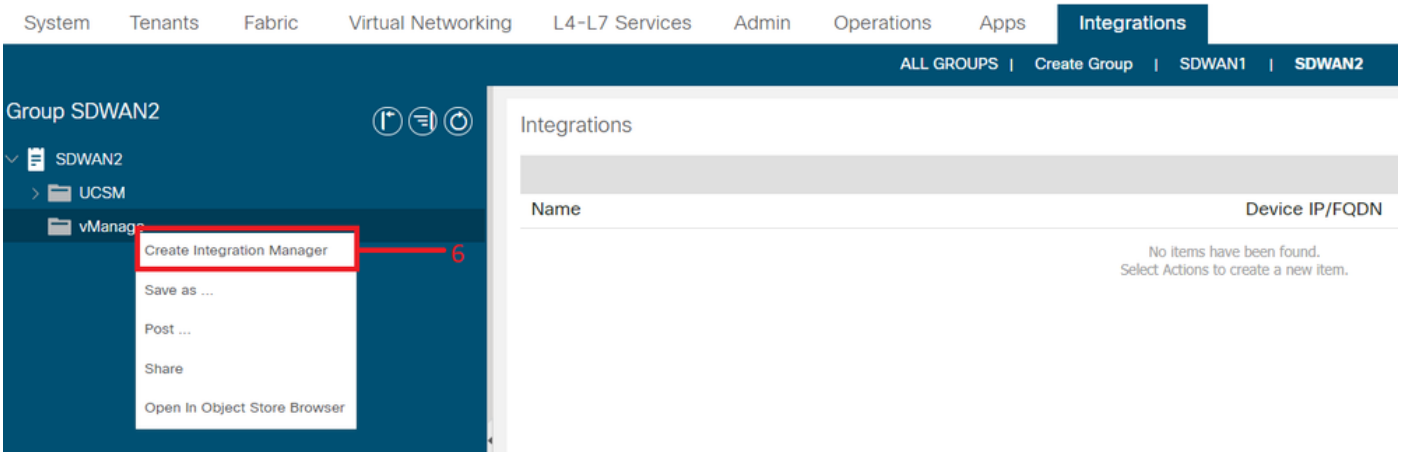
2. 統合グループの作成



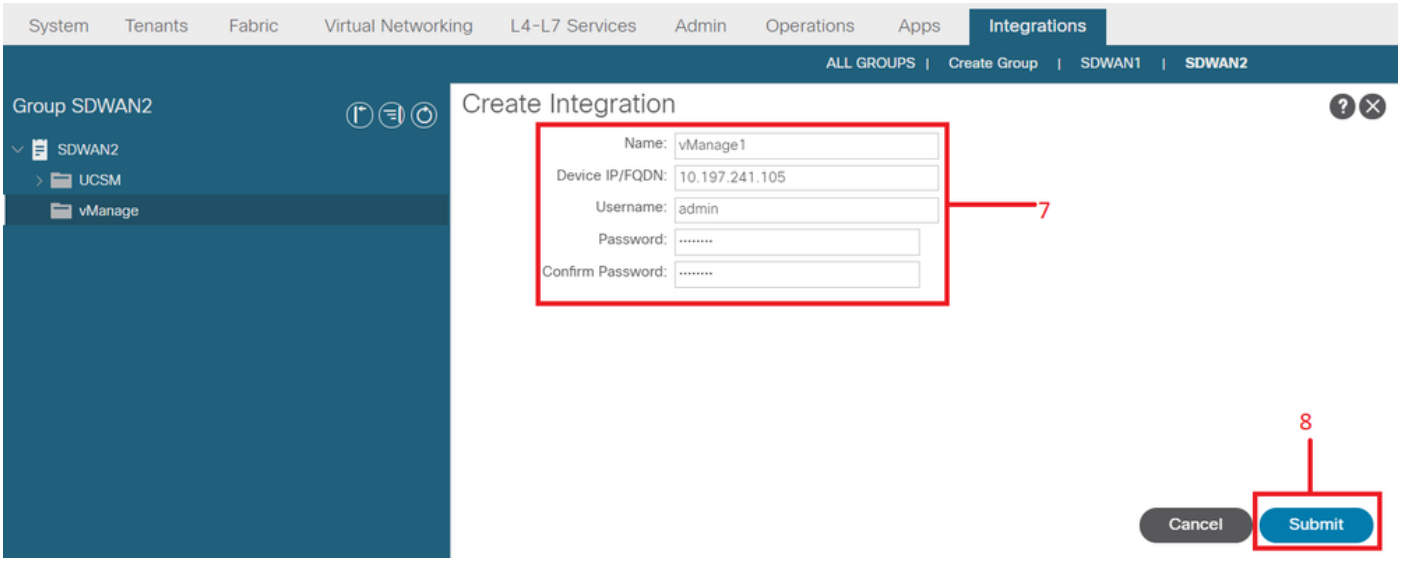
3. 新しく作成された統合グループ「SDWAN2」に移動し、vManage



4. vManageを右クリックし、Create Integration Managerを選択します。



5. 統合マネージャ名、デバイスIP/FQDN、ユーザ名、パスワードなどの適切な詳細情報を入力します



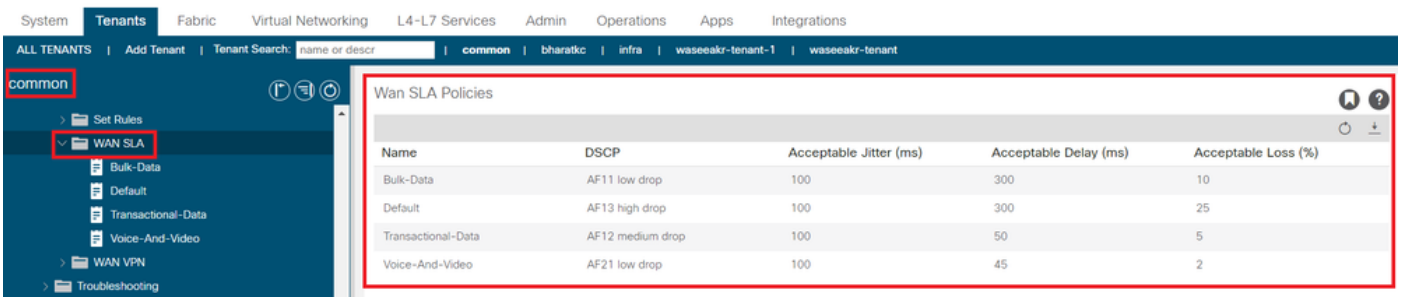
6. ステータスフィールドから登録が正常に行われたことを確認します。正常に完了しなかった場合、またはエラーが発生した場合は、提供された情報が正しいかどうかを確認します。パートナーIDはvManageコントローラのIDです。Integrations -><Group Name>->vManage -> <Integration Manager Name> -> System infoに移動して、ステータスを確認できます。

セクションB:WAN SLAポリシーの設定

事前に設定されたWAN SLAプロファイルは、Tenants->Common->Policies->Protocols->WAN SLAの下にあります。

これは、WAN SLAポリシーを使用してコントラクトを設定している間に、他のテナントに継承できます。

これらは事前設定されたSLAであり、変更できません。

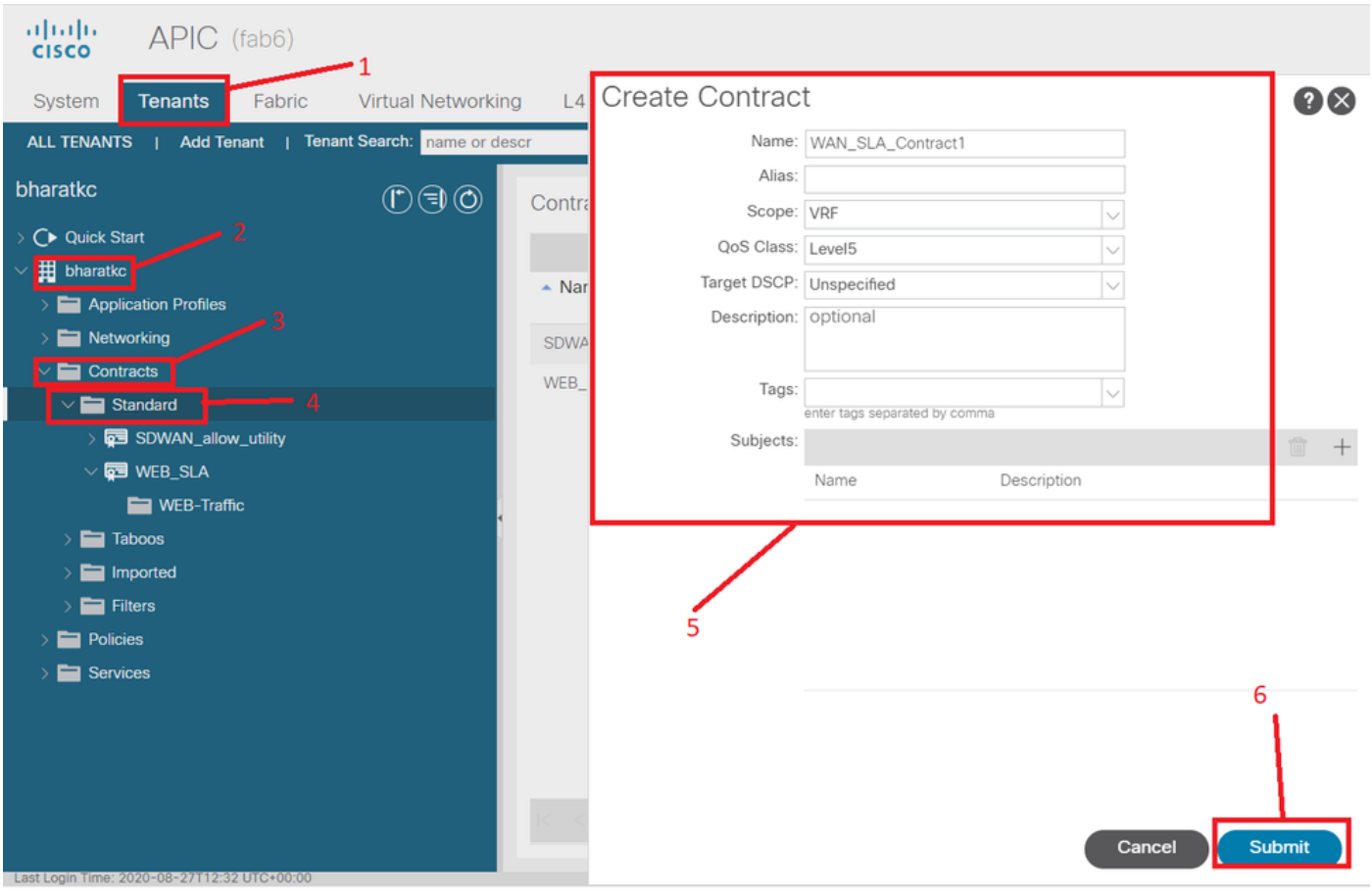


このACI統合にマッピングされるSD-WAN側で設定されたVPNは、Tenants->common->Policies->Protocols->WAN SLAにも反映されます。

1. WANサービスをマッピングするテナント/VRFでコントラクトを作成します。

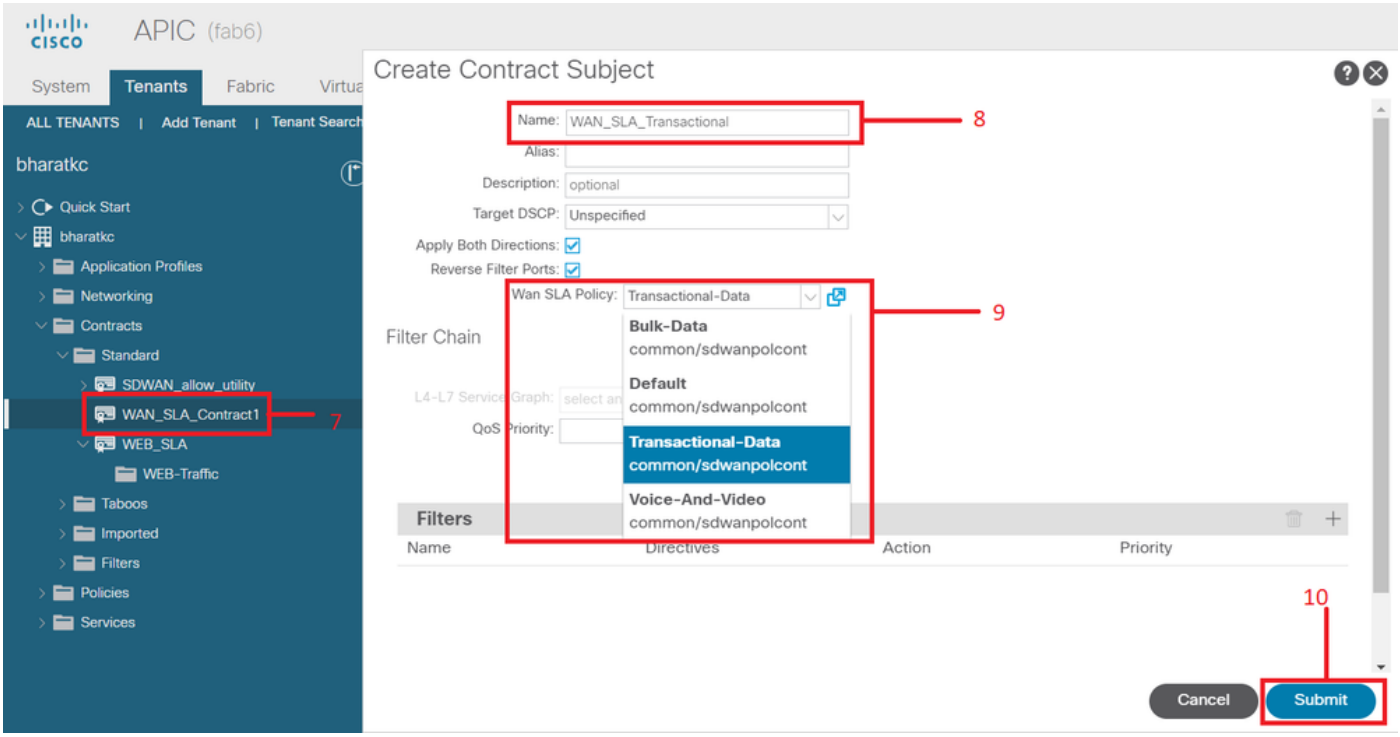
QoS Priorityの値は、Unspecified以外の値に設定する必要があります。WAN SLAポリシーは、QoS Priorityの値がUnspecifiedに設定されている場合は機能しません。

Tenants-><tenant name>->Contracts->Standardに移動してください。



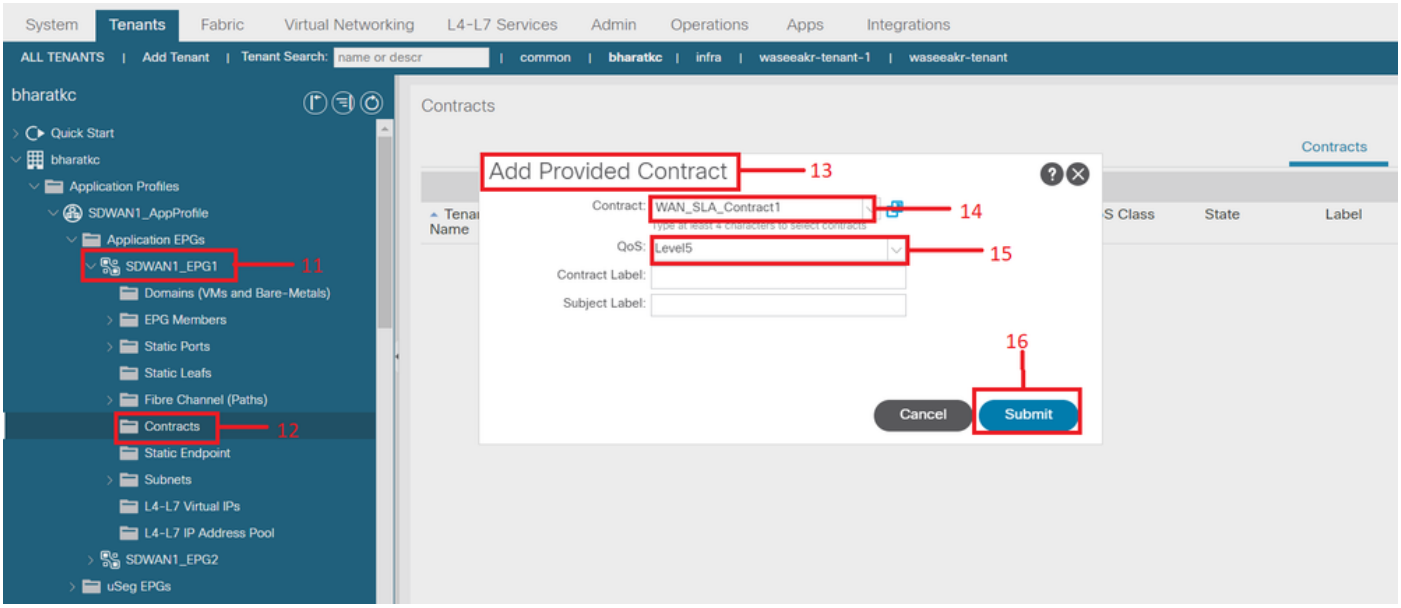
2. コントラクト対象を作成し、コントラクト対象でWAN SLAポリシーを指定します。

QoS Priorityの値は、Unspecified以外の値に設定する必要があります。WAN SLAポリシーは、QoS Priorityの値がUnspecifiedに設定されている場合は機能しません。



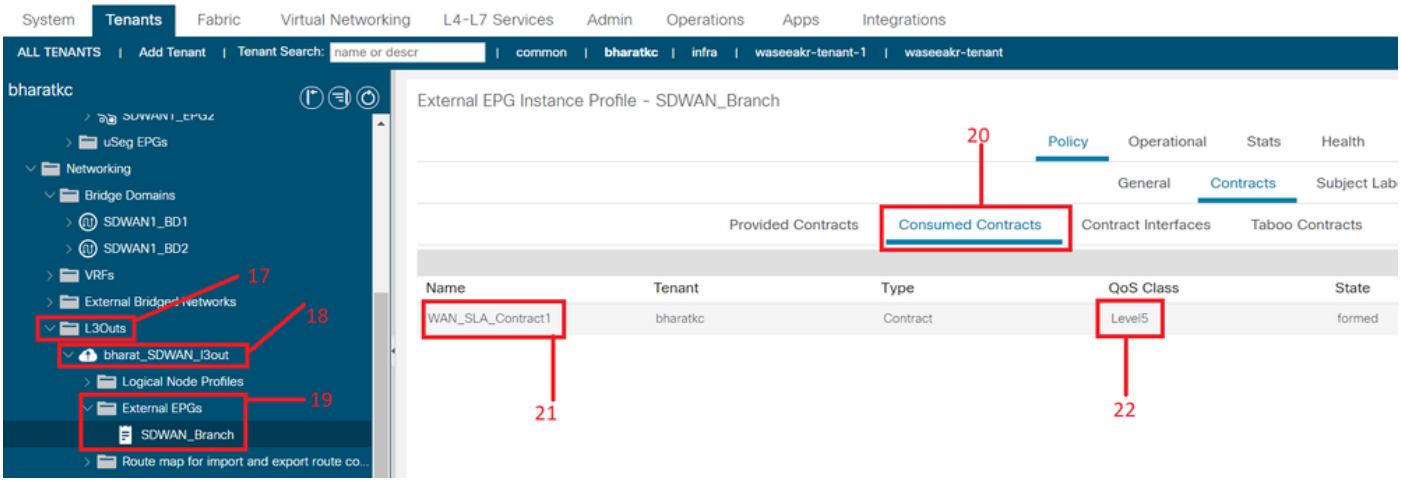
3. EPGから契約を提供します。

Tenants-><tenant name>->Application Profiles->Application EPG->Contractsに移動します。



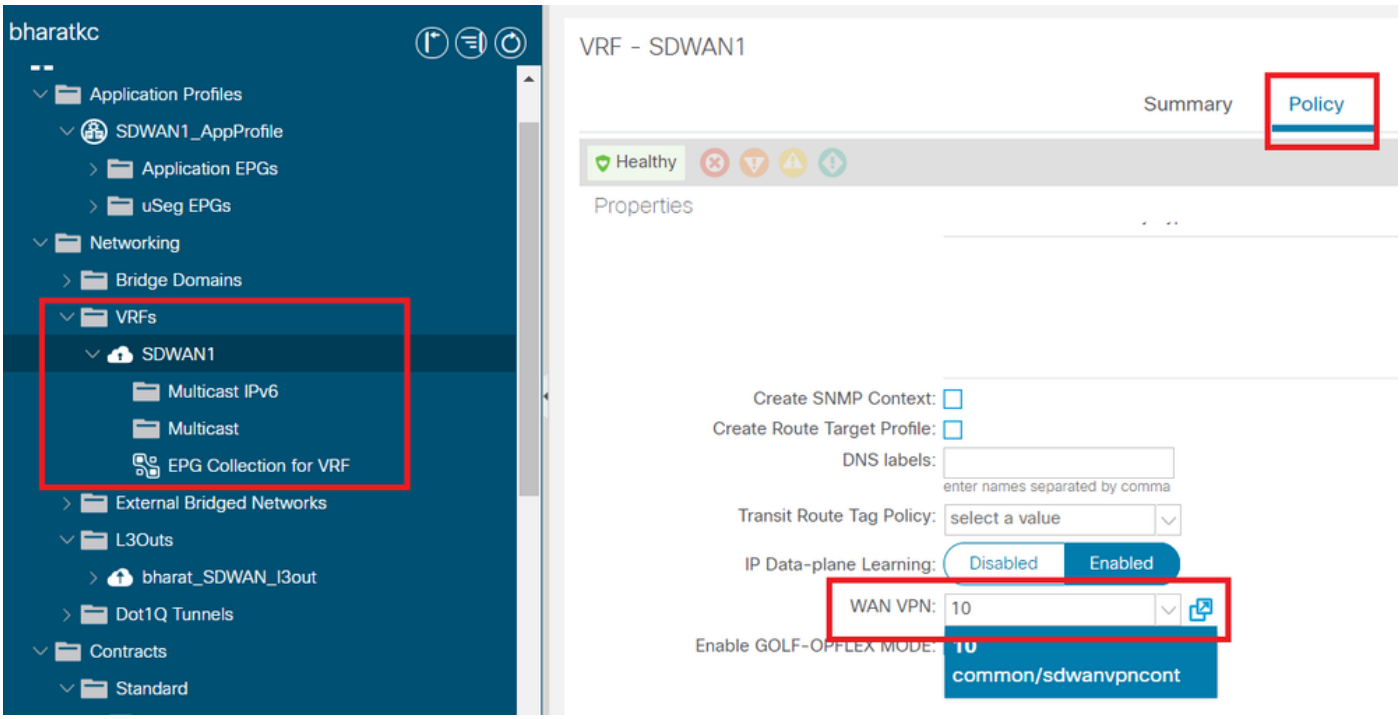
4. SD-WAN用に設定されたL3outで契約を使用します。

Tenants-><tenant name>->L3outs->External EPG->Consumed Contractsに移動してください。L3out外部EPGによって提供され、EPGによって消費されるコントラクトを持つことも可能であり、有効です



5. WAN VPNとテナントVRFのマッチング

Tenants-><tenant name>->VRF->Policy->WAN VPNに移動します。



確認

セクション3：検証

1. 設定の確認

設定は、ACIの設定に従って両方のSDWANデバイスにプッシュされます

DC側（L3outに接続）SDWANルート

<#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#
```

ブランチエンドSDWANルータ

<#root>

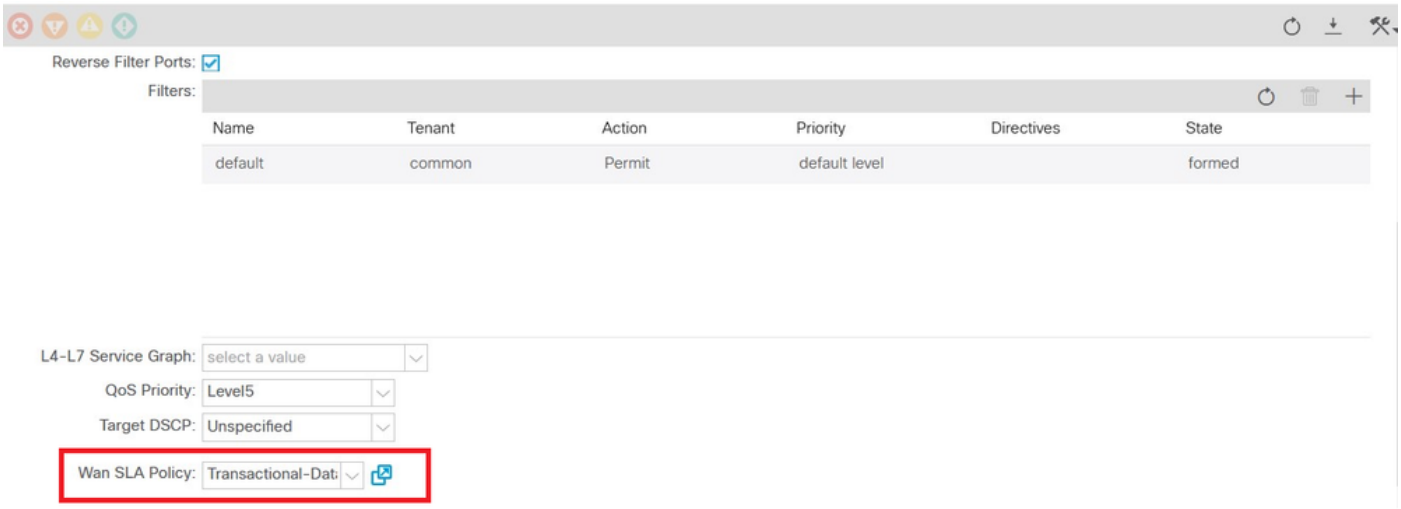
```
ASR1001-X-Branch#show sdwan policy from-vsmart
-->>> SLA Policy (parameters)
from-vsmart sla-class Bulk-Data
 loss    10
 latency 300
 jitter  100

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の検証

例 1

WAN SLAポリシー「トランザクションデータ」。 Tenants-><テナント名>->Contracts->Standard-><Contract Name>-><Contract Subject>->General- WAN SLA Policyに移動してください。



<#root>

```
  sequence 30
   match
```

dscp 12

```
   action
    sla-class
```

Transactional-Data

```
    no sla-class strict
```

[Direction]：

1. DCからSDWANへのトラフィック。

次のキャプチャからわかるように、DCから発信されたトラフィックはdscp 00を使用していますが、SDWANに到達するトラフィックはDSCP 12（16進数の0x0c）を使用しています。

これは、WAN SLAポリシーに従ってDSCP値が変更されたことを示します。

元のDSCP値を00に反映して送信元(DC)で実行されるパケットキャプチャ。

インターネットプロトコル、送信元：192.168.10.2(192.168.10.2)、Dst:172.16.20.2(172.16.20.2)

バージョン：4

ヘッダー長：20バイト

差別化サービスフィールド：0x00(DSCP 0x00：デフォルト、ECN:0x00)

0000 00.. = Differentiated Services Codepoint：デフォルト(0x00)

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別番号： 0xa0d5 (41173)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：255

プロトコル： ICMP (0x01)

ヘッダーチェックサム： 0x9016 [正解]

[良：正しい]

[不良：誤]

送信元：192.168.10.2(192.168.10.2)

宛先：172.16.20.2(172.16.20.2)

Internet Control Message Protocol

タイプ：8(エコー(ping)要求)

コード： 0 ()

チェックサム： 0xc16a [正解]

識別子： 0x4158

シーケンス番号：768(0x0300)

データ（56バイト）

WAN SLAポリシーに従ったDSCP 12（16進数0x0c）値の変更を反映した、宛先（SDWANブランチサイト）でのパケットキャプチャ。

インターネットプロトコル、送信元：192.168.10.2(192.168.10.2)、Dst:172.16.20.2(172.16.20.2)

バージョン：4

ヘッダー長：20バイト

差別化サービスフィールド：0x30(DSCP 0x0c:Assured Forwarding 12、ECN:0x00)

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

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別番号：0xa0d1(41169)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：251

プロトコル： ICMP (0x01)

ヘッダーチェックサム：0x93ea [正解]

[良：正しい]

[不良：誤]

送信元：192.168.10.2(192.168.10.2)

宛先：172.16.20.2(172.16.20.2)

Internet Control Message Protocol

タイプ：8(エコー(ping)要求)

コード： 0 ()

チェックサム： 0x6e30 [正解]

識別子： 0xc057

シーケンス番号：1024(0x0400)

データ（56バイト）

2. SDWANからDCへのトラフィック

次のキャプチャからわかるように、SDWANブランチサイトから発信されたトラフィックはdscp 00を使用していますが、DCに到達するトラフィックはDSCP 12（16進数の0x0c）を使用しています。これは、適用されるWAN SLAポリシーに従ったDSCP値の変更を反映しています。

元のDSCP値を00に反映して送信元（SDWANブランチ）で実行されるパケットキャプチャ。

インターネットプロトコル、送信元：172.16.20.2(172.16.20.2)、Dst:192.168.10.2(192.168.10.2)

バージョン：4

ヘッダー長：20バイト

Differentiated Services(DSCP)フィールド：0x00(DSCP 0x00：デフォルト、ECN:0x00)

0000 00.. = Differentiated Services Codepoint：デフォルト(0x00)

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別番号：0xa0c8(41160)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：255

プロトコル： ICMP (0x01)

ヘッダーチェックサム： 0x9023 [正解]

[良：正しい]

[不良：誤]

送信元：172.16.20.2(172.16.20.2)

宛先：192.168.10.2(192.168.10.2)

Internet Control Message Protocol

タイプ：8(エコー(ping)要求)

コード： 0 ()

チェックサム： 0xd3ff [正解]

識別子： 0x5c79

シーケンス番号：1(0x0001)

データ（56バイト）

WAN SLAポリシーに従ったDSCP 12（16進数0x0c）値の変更を反映した、宛先(DC)でのパケットキャプチャ。

インターネットプロトコル、送信元：172.16.20.2(172.16.20.2)、Dst:192.168.10.2(192.168.10.2)

バージョン：4

ヘッダー長：20バイト

差別化サービスフィールド：0x30(DSCP 0x0c:Assured Forwarding 12、ECN:0x00)

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

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別番号： 0xa073 (41075)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：251

プロトコル： ICMP (0x01)

ヘッダーチェックサム： 0x9448 [正解]

[良：正しい]

[不良：誤]

送信元：172.16.20.2(172.16.20.2)

宛先：192.168.10.2(192.168.10.2)

Internet Control Message Protocol

タイプ：8(エコー(ping)要求)

コード： 0 ()

チェックサム： 0x741a [正解]

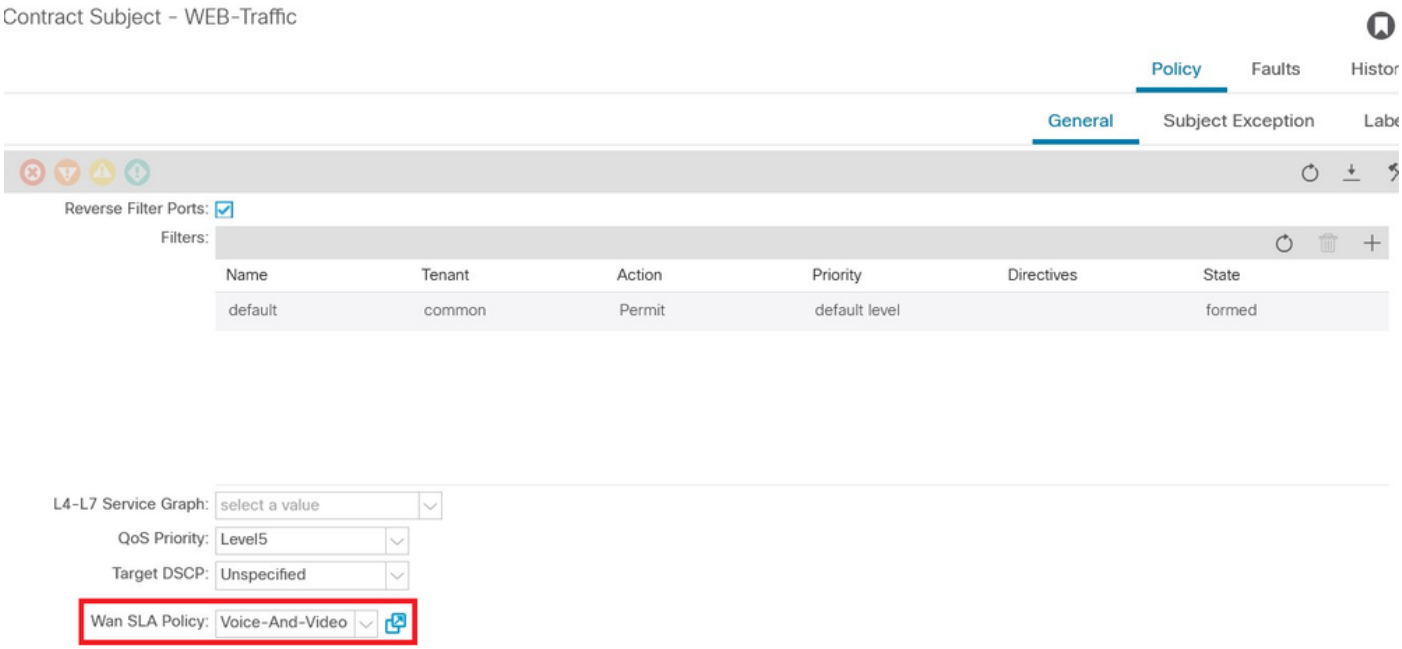
識別子： 0x5c79

シーケンス番号：43776(0xab00)

データ（56バイト）

例 2

WAN SLAポリシー「音声およびビデオ」 Please navigate to Tenants-><テナント名>->Contracts->Standard-><コントラクト名>-><コントラクトの件名>-> General- WAN SLA Policy



<#root>

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

1. DCからSDWANへのトラフィック。

次のキャプチャからわかるように、DCから発信されるトラフィックはDSCP 00を使用しますが、SDWANに到達するトラフィックはDSCP 18（16進数0x12）を使用します。

これは、WAN SLAポリシーに従ってDSCP値が変更されたことを示します。

元のDSCP値を00に反映して送信元(DC)で実行されるパケットキャプチャ。

インターネットプロトコル、送信元：192.168.10.2(192.168.10.2)、Dst:172.16.20.2(172.16.20.2)

バージョン：4

ヘッダー長：20バイト

Differentiated Services(DSCP)フィールド：0x00(DSCP 0x00：デフォルト、ECN:0x00)

0000 00.. = Differentiated Services Codepoint：デフォルト(0x00)

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別番号：0xa2b6(41654)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：255

プロトコル： ICMP (0x01)

ヘッダーチェックサム： 0x8e35 [正解]

[良：正しい]

[不良：誤]

送信元：192.168.10.2(192.168.10.2)

宛先：172.16.20.2(172.16.20.2)

Internet Control Message Protocol

タイプ：8(エコー(ping)要求)

コード： 0 ()

チェックサム： 0x3614 [正解]

識別子： 0x8c5f

シーケンス番号：512(0x0200)

データ（56バイト）

宛先（SDWANブランチサイト）でのパケットキャプチャ。DSCP値18(0x12)の変更をWAN SLAポリシーと一致させます。

インターネットプロトコル、送信元：172.16.20.2(172.16.20.2)、Dst:192.168.10.2(192.168.10.2)

バージョン：4

ヘッダー長：20バイト

差別化サービスフィールド：0x48(DSCP 0x12：確認転送21、ECN:0x00)

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

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別方法：0xa2b8(41656)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：255

プロトコル： ICMP (0x01)

ヘッダーチェックサム： 0x8deb [正解]

[良：正しい]

[不良：誤]

送信元：172.16.20.2(172.16.20.2)

宛先：192.168.10.2(192.168.10.2)

Internet Control Message Protocol

タイプ：0(エコー(ping)応答)

コード： 0 ()

チェックサム： 0x8a13 [正解]

識別子： 0x8c5f

シーケンス番号：1024(0x0400)

データ（56バイト）

2. SDWANからDCへのトラフィック。

元のDSCP値(00)を示す、送信元（SDWANブランチ）のパケットキャプチャ。

インターネットプロトコル、送信元：172.16.20.2(172.16.20.2)、Dst:192.168.10.2(192.168.10.2)

バージョン：4

ヘッダー長：20バイト

Differentiated Services(DSCP)フィールド：0x00(DSCP 0x00：デフォルト、ECN:0x00)

0000 00.. = Differentiated Services Codepoint：デフォルト(0x00)

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別番号：0xa1bb(41403)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：255

プロトコル： ICMP (0x01)

ヘッダーチェックサム： 0x8f30 [正解]

[良：正しい]

[不良：誤]

送信元：172.16.20.2(172.16.20.2)

宛先：192.168.10.2(192.168.10.2)

Internet Control Message Protocol

タイプ：8(エコー(ping)要求)

コード： 0 ()

チェックサム： 0x68e5 [正解]

識別子： 0x1d03

シーケンス番号：2048(0x0800)

データ（56バイト）

WAN SLAポリシーに従ったDSCP値18(0x12)の変更を反映した、宛先(DC)でのパケットキャプチャ。

インターネットプロトコル、送信元：172.16.20.2(172.16.20.2)、Dst:192.168.10.2(192.168.10.2)

バージョン：4

ヘッダー長：20バイト

差別化サービスフィールド：0x48(DSCP 0x12：確認転送21、ECN:0x00)

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

.....0. = ECN対応トランスポート(ECT): 0

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

全長：84

識別番号：0xa1bb(41403)

フラグ： 0x00

0.. =予約済みビット：未設定

.0. =フラグメントなし：設定なし

..0 =その他のフラグメント：未設定

フラグメントオフセット： 0

存続可能時間：251

プロトコル： ICMP (0x01)

ヘッダーチェックサム： 0x92e8 [正解]

[良：正しい]

[不良：誤]

送信元：172.16.20.2(172.16.20.2)

宛先：192.168.10.2(192.168.10.2)

Internet Control Message Protocol

タイプ：8(エコー(ping)要求)

コード： 0 ()

チェックサム： 0x68e5 [正解]

識別子： 0x1d03

シーケンス番号：2048(0x0800)

データ（56バイト）

トラブルシュート

次の口グファイルは、トラブルシューティングの観点から役に立ちます。を参照。

制御パスのデバッグ

APIC techsupportファイル
PolicyDistributorのログ、PolicyManagerのログ、PolicyElement、Edmgrのログには、関連する設定がリーフやスパインにプッシュされているかについての情報が含まれます。

データパスのデバッグ

L3outインターフェイスおよびvEdgeルータのインターフェイスでのパケットキャプチャ。

ELAMも役立ちます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。