Cisco IOS XE SD-WAN ルータの CLI テンプレート

Cisco IOS XE SD-WAN デバイスの CLI テンプレートは、次の方法で設定できます。

（注） Cisco vManage の上位バージョンで CLI テンプレートを生成し、それを下位バージョンに適用しようとすると、構成によってはサポートされない場合があります。この場合、Cisco vManage はアクセスを拒否し、エラーメッセージを生成することもあります。Cisco vManage の以前のバージョンで生成された CLI テンプレートを使用することをお勧めします。たとえば、Cisco vManage リリース 20.7.x を使用している場合、Cisco vManage リリース 20.6.x 以前のリリースで生成された CLI テンプレートを使用できます。

Cisco IOS XE SD-WAN デバイス のデバイス設定ベース CLI テンプレート

Cisco vManage は、機能テンプレートとポリシー（ローカライズされたポリシー、セキュリティポリシー）の組み合わせを使用して Cisco IOS XE SD-WAN デバイス を設定します。Cisco vManage 20.1.1 以降では、Cisco vManage により、Cisco IOS XE SD-WAN デバイス でデバイス設定を使用する CLI テンプレートを指定できます。これらのテンプレートを使用して、デバイス設定（yang-cli）をデバイスに直接プッシュできます。

1 回の操作で、Cisco vManage は、デバイス設定とテンプレートでユーザーが指定した設定の相違部分を Cisco IOS XE SD-WAN デバイス に直接プッシュします。Cisco vManage は、他のテンプレートの場合と同様に、デバイスにプッシュする前に設定のプレビューも表示します。既述のワークフローは、テンプレートに対して追加、変更、または削除を行う場合にも適用されます。

（注） Cisco vManage を使用してアクセスできない機能を構成するには、次の手順を実行することをお勧めします。

1. CLI アドオン機能テンプレートに加えて、関連する機能テンプレートを使用します。詳細については、CLI アドオン機能テンプレートの認定 CLIを参照してください。
2. 前のオプションでは不十分な場合は、このセクションで説明されているデバイス設定ベース CLI テンプレートを使用します。

Cisco XE SD-WAN ルータの CLI テンプレートに関する機能情報

表 *1:* 機能の履歴

機能名	リリース情報	説明
デバイス設定 CLI テンプレート	Cisco IOS XE リリース 17.2.1r Cisco vManage 20.1.1	CLI テンプレート機能は、デバイス設定ベースの CLI をサポートするように更新されました。これらのテンプレートを使用して、デバイス設定（yang-cli）をデバイスに直接プッシュできます。

制限事項

補助ポート：補助ポートを持つ Cisco サービス統合型ルータの CLI テンプレートを使用する場合は、補助ポート用のコマンド（**line aux 0** など）を含めないでください。そうした場合、エラーが発生します。これらのコマンドは、デバイス上で直接実行できます。

コマンド `show sdwan running-config` を使用して CLI テンプレート設定をインポートする場合は、Cisco vManage 上の CLI テンプレートの引用符を手動で追加する必要があります。

Cisco vManage での CLI テンプレートの設定

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[CLI Template] を選択します。

4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. [Template Name] に、テンプレートの名前を入力します。

   名前の最大長は 128 文字で、英数字のみを使用できます。
6. [Template Description] に、テンプレートの説明を入力します。

   説明の最大長は 2048 文字で、英数字のみを使用できます。
7. [Device configuration] を選択します。このオプションを使用すると、`show sdwan running-config` コマンドの出力に表示される IOS-XE 設定コマンドを指定できます。
8. （オプション）接続されたデバイスの実行構成をロードするには、[Load Running config from reachable device] リストから選択し、[Search] をクリックします。
9. [CLI Configuration] で、手入力するか、カットアンドペーストするか、ファイルをアップロードして、設定を入力します。
10. 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。{{*variable-name*}}; の形式で変数名を直接入力することもできます。たとえば、{{hostname}} です。

    これらの変数は、テンプレートをアタッチした後、デバイスごとにデバイス変数ページに入力できます。値は手入力するか、CSV ファイル使用してアップロードできます。
11. 機能テンプレートを保存するには、[Add] をクリックします。新しいデバイステンプレートが [Device Template] テーブルに表示されます。

Cisco IOS XE SD-WAN ルータ用のインテントベースの CLI テンプレート

Cisco IOS XE SD-WAN デバイス の CLI テンプレート機能により、Cisco vManage を使用して、Cisco IOS XE SD-WAN デバイス のインテントベースの CLI テンプレートを設定できます。インテントベースの CLI テンプレートは、Cisco vEdge デバイスの構文に基づくコマンド ライン インターフェイス設定を参照します。CLI テンプレートを使用して、Cisco vManage では Cisco vEdge 構文ベースのコマンドを Cisco IOS XE 構文の Cisco IOS XE SD-WAN デバイス にプッシュできるようになります。

（注） デバイス設定ベースの CLI テンプレートのサポートにより、インテントベースの CLI テンプレートは廃止されます。Cisco IOS XE SD-WAN デバイス のデバイス設定ベース CLI テンプレート （1 ページ）で説明されているように、デバイス設定ベースの CLI テンプレートを使用することをお勧めします。

Cisco vManage CLI テンプレートを使用すると、機能テンプレートを設定する手間が大幅に削減されます。

Cisco XE SD-WAN ルータの CLI テンプレートに関する機能情報

表 *2:* 機能の履歴

機能名	リリース情報	説明
Cisco XE SD-WAN ルータの CLI テンプレート	Cisco IOS XE リリース 16.11.1a Cisco SD-WAN リリース 19.1	Cisco XE SD-WAN ルータの CLIテンプレート機能により、vManage を使用して Cisco XE SD-WAN ルータのインテントベースの CLI テンプレートを設定できます。
VRF 設定	Cisco IOS XE リリース 17.2.1r	VRF設定のサポートが合計100から合計 300 VRF に増加しました。サポート対象：Cisco ASR 1001-HX および Cisco ASR 1002-HX

CLI テンプレートの利点

- Cisco IOS XE ルータ用の Cisco vEdge 固有の vManage 機能テンプレートを再利用できます。Cisco XE SDWAN 機能テンプレートを使用してデバイステンプレートを作成すると、vManage はインテントベースの設定（vEdge CLI 構文）と対応するデバイスベース（Cisco XE SDWAN ルータ）の設定を表示します。インテントベースの設定を調べて、それを再利用して、XE SDWAN ルータ用の個別の CLI テンプレートを作成できます。
- 1 回の編集で CLI テンプレートに複数の変更を加えることができます。
- 同じデバイスモデルの複数のデバイスで 1 つの設定を使用できます。変数はデバイスごとに固有の設定を使用した一括設定の迅速な展開に使用することができます。システム IP、サイト ID、ホスト名、IP アドレスなどの一般的な設定は、テンプレートで編集可能な変数として定義でき、同じテンプレートを複数のデバイスにアタッチできます。
- CLI テンプレートで変数のカスタム長を定義できます。
- CLI テンプレートの入力として、既存の IOS-XE デバイスインテント設定を使用できます。
- CLI テンプレートのコンテンツは、複数の IOS-XE デバイスタイプ（VPN、VPN インターフェイス、BGP、OSPF などの一般的な CLI）で使用できます。

制限事項

補助ポート：補助ポートを持つ Cisco サービス統合型ルータの CLI テンプレートを使用する場合は、補助ポート用のコマンド（**line aux 0** など）を含めないでください。そうした場合、エラーが発生します。これらのコマンドは、デバイス上で直接実行できます。

Cisco vManage での CLI テンプレートの設定

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] をクリックし、[Create Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[CLI Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. [Template Name] に、テンプレートの名前を入力します。

   名前の最大長は 128 文字で、英数字のみを使用できます。
6. [Template Description] に、テンプレートの説明を入力します。

   説明の最大長は 2048 文字で、英数字のみを使用できます。
7. CLI テンプレートの設定は、インテントベースまたはデバイス設定に基づくことができます。
   - [Intent]：[Intent] を指定する場合は、Cisco vEdge 形式でコマンドを指定します。選択したデバイスが Cisco IOS XE SD-WAN デバイス の場合、Cisco vManage はデバイスの設定を変換します。
   - [Device configuration]：このオプションは、Cisco IOS XE リリース 17.2.1r 以降で、Cisco IOS XE SD-WAN デバイス でのみ使用できます。このオプションでは、`show sd-wan running config` に表示されるデバイス設定全体を指定する必要があります。

（注） この機能は、CLI アドオン機能テンプレートの認定 CLIで詳しく説明されている認定 CLI でのみ使用できます。

[Select a File] を使用して設定ファイルをアップロードするか、CLI 設定をコピーして貼り付けることができます。以下は、変数を使用したインテントベースの CLI の例です。

```
system

   host-name {{hostname}}
   system-ip {{system_ip}}
   domain-id 1

   site-id {{site_id}}
   port-offset           1
   admin-tech-on-failure
   organization-name "XYZ"
   logging
    disk
```

```
    enable
! !
```

これらの変数は、テンプレートをアタッチした後、デバイスごとにデバイス変数ページに入力できます。値は手入力するか、CSV ファイル使用してアップロードできます。

8. 機能テンプレートを保存するには、[Add] をクリックします。

（注） デバイスをテンプレートにアタッチし、同じデバイスモデルの複数のデバイスにテンプレートを再利用する方法の詳細については、このトピックの、デバイステンプレートへのデバイスの接続のセクションを参照してください。

CLI テンプレートのサンプル設定

システムレベルの設定

表 *3:* システムレベルのパラメータ

CLI テンプレート設定	デバイスの設定
system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name "XYZ Inc Regression" organization-name "XYZ Regression" console-baud-rate 115200 vbond 10.0.12.26 port 12346	system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name “XYZ Inc Regression” organization-name “XYZ Inc Regression” console-baud-rate 11520 vbond 10.0.12.26 port 12346

AAA 設定：RADIUS および TACACS+ を使用した認証、許可、およびアカウンティング（AAA）

表 *4 : AAA* 設定

CLI テンプレート設定	デバイスの設定

aaa
 auth- order local radius tacacs
 usergroup basic
 	
 task system read write
 task interface read write
!
 	
usergroup netadmin
!
 	
usergroup operator
task system read
task interface read
task policy read
task routing read
task security read
!
user admin password
 	
6nbbLkA==$ae/DO78l/wluPUohhBU2L6h/
Q.PLkurGvxjRlS9OWB9iTtFwSGNQcABV6F
MW57vuEHvo3zp3qdYVinLmMIu/p/
secret
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiLMOFQfD.QPAmMxDdxz.c
 	
! !
radius
 	
 server 10.99.144.200
  source-interface GigabitEthernet0/0/1
 exit
 server 10.99.144.201
 	
  source-interface GigabitEthernet0/1/0
 exit
!
tacacs
 	
 server 10.0.1.1
  auth-port 50
 	
  vpn 0
 	
  source-interface GigabitEthernet0/0/1
 	
  key 1
 	
  secret-key
8Kcuva0CM871E8czESwV5g/YX4Q8pY1LSNk/+PIDrpCg=
 	
 exit !
!
	aaa group server tacacs+ server-10.0.1.1
	  server-private 10.0.1.1 timeout 5 key
	8vs5hzVg/Z6EeuUdNHTzOwWPsUv9V/50xmcRfShWp3YI=
	
	 ip tacacs source-interface
	GigabitEthernet0/0/1
	!
	aaa group server radius server-10.99.144.200
	
	 server-private 10.99.144.200 auth-port 1812
	 timeout 5 retransmit 3
	 ip radius source-interface
	GigabitEthernet0/0/1
	!
	
	aaa group server radius server-10.99.144.201
	
	 server-private 10.99.144.201 auth-port 1812
	 timeout 5 retransmit 3
	 ip radius source-interface
	GigabitEthernet0/1/0
	!
	aaa authentication login default local group
	 radius group tacacs+
	aaa authorization exec default local group
	radius group tacacs+ a
	aa session-id common --- added by default
	
	username admin privilege 15 secret 9
	$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiLMOFQfD.QPAmMxDdxz.c

ロギングの設定：ローカルハードドライブまたはリモートホストへのロギングを設定します

表 *5:* ロギングの設定

CLI テンプレート設定	デバイスの設定
logging disk enable file size 12 file rotate 6 ! server 192.168.13.1 vpn 0 source-interface Loopback1 priority alert exit !	logging disk enable ! ! logging persistent size 75497472 filesize 12582912 logging buffered 512000 --- added by default logging host 192.168.13.1 no logging rate-limit logging source-interface Loopback1 logging persistent

スイッチポートと VLAN の設定

表 *6:* スイッチ ポートの設定

CLI テンプレート設定	デバイスの設定
interface GigabitEthernet0/1/4 switchport mode trunk access vlan vlan 10 access vlan name "DHCP Vlan" trunk allowed vlan 10 ! no shutdown vpn 10 name "DHCP VPN" interface Vlan10 description "Vlan 10 Mgmt interface" ip address 10.29.35.1/24 no shutdown ! !	interface GigabitEthernet0/1/4 switchport ios-sw:mode trunk switchport ios-sw:trunk allowed vlan 10 no shutdown no ip address exit interface Vlan10 description Vlan 10 Mgmt interface no shutdown arp timeout 1200 vrf forwarding 10 ip address 10.29.35.1 255.255.255.0 ip mtu 1500 exit

セルラーの設定

表 *7:* セルラーの設定：セルラーコントローラとセルラーインターフェイスを設定します

CLI テンプレート設定	デバイスの設定

vpn 0
  interface Cellular0/2/0
  description "Cellular interface"
  no shutdown
  !
 	
  controller cellular 0/2/0
  lte sim max-retry 1
  lte failovertimer 7
  profile id 1 apn Broadband
  !
	interface Cellular0/2/0
	  description Cellular interface
	  no shutdown
	  ip address negotiated
	  ip mtu 1428
	  mtu 1500
	  exit
	
	  controller Cellular 0/2/0
	  lte sim max-retry 1
	  lte failovertimer 7
	  profile id 1 apn Broadband authentication none pdn-type ipv4

BGP、**OSPF**、および **EIGRP**：トランスポートまたはサービス **VPN** で **BGP**、**OSPF**、および **EIGRP** ルーティングプロトコルを設定します

表 ***8 : BGP***、***OSPF*** および ***EIGRP*** の設定

CLI テンプレート設定	デバイスの設定

CLI テンプレート設定	デバイスの設定

vpn1
  bgp 2
     shutdown
     distance external 30
     distance internal 250
     distance local 10
     address-family ipv4-unicast
      network 10.0.100.0/24
      redistribute static route-policy
route_map
      redistribute connected route-policy
route_map
     !
     neighbor 10.0.100.1
      no shutdown
      remote-as   3
      timers
       keepalive   12
       holdtime   20
       connect-retry   300
       advertisement-interval 123
      !
      update-source GigabitEthernet0/0/1
      ebgp-multihop 1
      password
$8$9pou4PH9b60B072hcw3MmSSdLCfJk8bVys12lLVb+08=
 	
      address-family ipv4-unicast
 	
vpn 1
   router
    ospf
     router-id 172.16.255.15
     compatible rfc1583
     timers spf 200 1000 10000
     redistribute connected route-policy
route_map
     max-metric router-lsa administrative
     area 23
      stub
      interface GigabitEthernet0/0/1
       cost 23
       authentication type message-digest
       authentication authentication-key
key1
      exit
     exit
    !
 	
vpn 1
 router
  eigrp 1
   af-interface GigabitEthernet0/0/2
   no split-horizon
   exit-af-interface
  !
 address-family ipv4 network 10.1.10.1/32
 address-family ipv4 topology base
 redistribute omp
 exit-af-topology	

CLI テンプレート設定	デバイスの設定
	router bgp 2 bgp log-neighbor-changes distance bgp 30 250 10 address-family ipv4 unicast vrf 1 neighbor 10.0.100.1 remote-as 3 neighbor 10.0.100.1 activate neighbor 10.0.100.1 ebgp-multihop 1 neighbor 10.0.100.1 maximum-prefix 2147483647 100 neighbor 10.0.100.1 password 0 password neighbor 10.0.100.1 send-community both neighbor 10.0.100.1 timers 12 20 neighbor 10.0.100.1 update-source GigabitEthernet0/0/1 network 10.0.100.0 mask 255.255.255.0 redistribute connected redistribute static route-map route_map exit-address-family ! timers bgp 60 180 router ospf 1 vrf 1 auto-cost reference-bandwidth 100 max-metric router-lsa timers throttle spf 200 1000 10000 router-id 172.16.255.15 default-information originate distance ospf external 110 distance ospf inter-area 110 distance ospf intra-area 110 redistribute connected subnets route-map route_map ! interface GigabitEthernet0/0/1 no shutdown arp timeout 1200 vrf forwarding 1 ip address 10.1.100.14 255.255.255.0 ip redirects ip mtu 1500 ip ospf 1 area 23 ip ospf network broadcast mtu 1500 negotiation auto exit ! router eigrp eigrp-name address-family ipv4 vrf 1 autonomous-system 1 af-interface GigabitEthernet0/0/2 hello-interval 5 hold-time 15 no split-horizon exit-af-interface ! network 10.1.10.1 0.0.0.0 topology base redistribute omp

CLI テンプレート設定	デバイスの設定
	exit-af-topology ! exit-address-family ! !

WAN および LAN インターフェイスの VPN、インターフェイス、およびトンネルの設定

表 *9 : VPN*、インターフェイス、およびトンネルの設定

CLI テンプレート設定	デバイスの設定

vpn 0
  interface GigabitEthernet0/2/0
  ip address 10.1.14.14/24
  tunnel-interface
  encapsulation ipsec
  color lte
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  !
  autonegotiate
  no shutdown
  !
  ip route 0.0.0.0/0 10.1.14.13
 	
vpn 512
interface GigabitEthernet0
  ip dhcp-client
ipv6 dhcp-client autonegotiate
no shutdown
! !
	ip route 0.0.0.0 0.0.0.0 10.1.14.13 1
	
	interface GigabitEthernet0/2/0
	  no shutdown
	  arp timeout 1200 – added by default
	  ip address 10.1.14.14 255.255.255.0
	  ip redirects --> added by default
	  ip mtu 1500
	  mtu 1500
	  negotiation auto --> added by default
	  exit
	
	interface Tunnel20 ---> based on the
	interface 0/2/0
	  no shutdown
	  ip unnumbered GigabitEthernet0/2/0
	  no ip redirects
	  ipv6 unnumbered GigabitEthernet0/2/0
	  no ipv6 redirects
	  tunnel source GigabitEthernet0/2/0
	  tunnel mode sdwan
	
	sdwan
	  interface GigabitEthernet0/2/0
	  tunnel-interface
	  encapsulation ipsec weight 1
	  color lte
	  no last-resort-circuit
	  vmanage-connection-preference 5
	  no allow-service all
	  no allow-service bgp
	  allow-service dhcp
	  allow-service dns
	  allow-service icmp
	  no allow-service sshd
	  no allow-service netconf
	  no allow-service ntp
	  no allow-service ospf
	  no allow-service stun
	
	interface GigabitEthernet0
	no shutdown
	arp timeout 1200
	vrf forwarding Mgmt-intf
	ip address dhcp client-id GigabitEthernet0
	ip redirects
	ip dhcp client default-router distance 1 ip
	  mtu 1500
	mtu 1500
	negotiation auto

ダイレクト インターネット アクセス（DIA）経由のネットワークアドレス変換（NAT）

表 *10 : DIA* 経由の *NAT*

CLI テンプレート設定	デバイスの設定
vpn 201 interface GigabitEthernet0/0/2.2901 description gigi21 ip address 10.201.201.1/24 mtu 1496 no shutdown vrrp 100 track-omp ipv4 10.201.201.3 ! ! ! dhcp-server address-pool 10.201.201.0/24 exclude 10.201.201.1-10.201.201.10 10.201.201.20-10.201.201.22 offer-time 600 lease-time 86400 admin-state up options default-gateway 10.201.201.1 dns-servers 10.99.139.201 tftp-servers 10.99.139.201 ! ! ! ip route 0.0.0.0/0 vpn 0 ! vpn 0 interface GigabitEthernet0/0/0 ip address 172.16.10.1/24 nat udp-timeout 3 tcp-timeout 40 respond-to-ping ! !	interface GigabitEthernet0/0/2.2901 no shutdown encapsulation dot1Q 2901 vrf forwarding 201 ip address 10.201.201.1 255.255.255.0 ip mtu 1496 vrrp 100 address-family ipv4 vrrpv2 address 10.201.201.3 priority 100 track omp shutdown exit exit ip dhcp excluded-address vrf 201 10.201.201.1 10.201.201.10 ip dhcp excluded-address vrf 201 10.201.201.20 10.201.201.22 ip dhcp pool vrf-201-GigabitEthernet0/0/2.2901 option 150 ip 10.99.139.201 vrf 201 lease 1 0 0 default-router 10.201.201.1 dns-server 10.99.139.201 network 10.201.201.0 255.255.255.0 exit ip dhcp use hardware-address client-id no ip dhcp use class ip dhcp use vrf remote ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload ip nat translation tcp-timeout 40 ip nat translation udp-timeout 3 ip nat route vrf 201 0.0.0.0 0.0.0.0 global interface GigabitEthernet1/0/2 no shutdown arp timeout 1200 ip address 10.1.15.15 255.255.255.0 ip nat outside ip redirects ip mtu 1500 mtu 1500 negotiation auto

NAT64 の設定

表 *11 : NAT64* の設定

vpn 1
  nat64
  v4 pool pool1 start-address 10.1.1.10
  v4 pool pool1 end-address 10.1.1.100
  !
  interface GigabitEthernet3
  ip address 10.1.19.15/24
  nat64
  !
  autonegotiate
  no shutdown
  !
	interface GigabitEthernet3
	  no shutdown
	  arp timeout 1200
	  vrf forwarding 1
	  ip address 10.1.19.15 255.255.255.0
	  negotiation auto
	  nat64 enable
	  nat64 prefix stateful 2001::F/64 vrf 1
	
	  nat64 v4 pool pool1 10.1.1.10 10.1.1.100
	  nat64 v6v4 list global-list pool pool1 vrf 1
	  nat64 translation timeout tcp 60
	  nat64 translation timeout udp 1

マルチリンクおよび T1/E1 : T1/E1 コントローラおよびシリアル、マルチリンク インターフェイスを設定します

表 *12 :* マルチリンクの設定

CLI テンプレート設定	デバイスの設定

card type t1 0 2
  controller T1 0/2/0
  framing esf
  clock source internal
  linecode b8zs
  cablelength long 0db
  channel-group 1 timeslots 15
  channel-group 2 timeslots 12
  channel-group 3 timeslots 10
  channel-group 4 timeslots 10
!
interface Multilink1
  no shutdown
  encapsulation ppp
  ip address 10.1.10.30 255.255.255.0
  ppp pap sent-username admin password admin
  ppp authentication pap
  ppp multilink
  ppp multilink links minimum 1
  ppp multilink fragment disable
  ppp multilink group 1
exit
interface Serial0/2/0:1
  no shutdown
  encapsulation ppp
  bandwidth 1536
  no ip address
  load-interval 30
  ppp pap sent-username admin password admin
  ppp authentication pap
  ppp multilink
  ppp multilink group 1
exit
	interface Multilink1
	ip address 10.1.10.30/24 shutdown
	controller T1 0/2/0
	  linecode b8zs
	  channel-group 1
	  channel-group 3
	!
	ppp pap sent-username admin password admin
	ppp authentication pap
	ppp multilink
	ppp multilink group 1

ローカル QoS ポリシー

表 *13 :* ローカル *QoS* ポリシー

CLI テンプレート設定	デバイスの設定

CLI テンプレート設定	デバイスの設定
vpn 1 interface GigabitEthernet0/0/1 ip address 10.2.54.15/24 no shutdown access-list MyACL in ! policy class-map class best-effort queue 3 class bulk-data queue 2 class critical-data queue 1 class voice queue 0 ! access-list MyACL sequence 10 match dscp 46 ! action accept class voice ! ! sequence 20 match source-ip 10.1.1.0/24 destination-ip 192.168.10.0/24 ! action accept class bulk-data set dscp 32 ! ! ! sequence 30 match destination-ip 192.168.20.0/24 ! action accept class critical-data set dscp 22 ! ! ! sequence 40 action accept class best-effort set dscp 0 ! ! ! default-action accept ! qos-scheduler be-scheduler class best-effort bandwidth-percent 20 buffer-percent 20 drops red-drop ! qos-scheduler bulk-scheduler	interface GigabitEthernet0/0/1 access-list MyACL in exit class-map match-any best-effort match qos-group 3 ! class-map match-any bulk-data match qos-group 2 ! class-map match-any critical-data match qos-group 1 ! class-map match-any voice match qos-group 0 ! policy-map MyQoSMap class best-effort random-detect bandwidth percent 20 ! class bulk-data random-detect bandwidth percent 20 ! class critical-data random-detect bandwidth percent 40 ! class voice priority percent 20 ! ! policy no app-visibility no flow-visibility no implicit-acl-logging log-frequency 1000 class-map class best-effort queue 3 class bulk-data queue 2 class critical-data queue 1 class voice queue 0 ! access-list MyACL sequence 10 match dscp 46 ! action accept class voice ! ! sequence 20 match source-ip 10.1.1.0/24 destination-ip 192.168.10.0/24 ! action accept class bulk-data set dscp 32 !

CLI テンプレート設定	デバイスの設定
class bulk-data bandwidth-percent 20 buffer-percent 20 drops red-drop ! qos-scheduler critical-scheduler class critical-data bandwidth-percent 40 buffer-percent 40 drops red-drop ! qos-scheduler voice-scheduler class voice bandwidth-percent 20 buffer-percent 20 scheduling llq ! qos-map MyQoSMap qos-scheduler be-scheduler qos-scheduler bulk-scheduler qos-scheduler critical-scheduler qos-scheduler voice-scheduler ! ! ! !	! ! sequence 30 match destination-ip 192.168.20.0/24 ! action accept class critical-data set dscp 22 ! ! sequence 40 action accept class best-effort set dscp 0 ! ! default-action accept ! ! ! !

セキュリティポリシー（ZBFW、IPS/IDS、URL フィルタリング）の設定

表 *14 :* セキュリティポリシー（*ZBFW*、*IPS/IDS*、*URL* フィルタリング）

CLI テンプレート設定	デバイスの設定
policy zone internet vpn 0 ! zone zone1 vpn 1 ! zone zone2 vpn 2 ! zone-pair ZP_zone1_internet_fw_policy source-zone zone1 destination-zone internet zone-policy fw_policy ! zone-pair ZP_zone1_zone2_fw_policy source-zone zone1 destination-zone zone2 zone-policy fw_policy ! zone-based-policy fw_policy sequence 1 match source-data-prefix-list subnet1 ! action inspect ! ! default-action pass ! zone-to-nozone-internet deny lists data-prefix-list subnet1 ip-prefix 10.0.10.0/24 ! ! url-filtering url_filter web-category-action block web-categories games block-threshold moderate-risk block text "<![CDATA[<h3>Access" to the requested page has been denied]]>" target-vpns 1 ! intrusion-prevention intrusion_policy security-level connectivity inspection-mode protection log-level err target-vpns 1 ! failure-mode open ! ! !	

CLI テンプレート設定	デバイスの設定
	ip access-list extended fw_policy-seq-1-acl_ 11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl 10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_ match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy class fw_policy-seq-1-cm_ inspect ! class class-default pass ! ! object-group service fw_policy-seq-1-service-og_ ip ! parameter-map type inspect-global alert on log dropped-packets multi-tenancy vpn zone security ! parameter-map type umbrella global token A5EA676087BF66A42DC4F722C2AFD10D00256274 dnscrypt vrf 1 dns-resolver umbrella match-local-domain-to-bypass ! ! zone security internet vpn 0 ! zone security zone1 vpn 1 ! zone security zone2 vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2 service-policy type inspect fw_policy ! app-hosting appid utd app-resource package-profile cloud-low app-vnic gateway0 virtualportgroup 0

CLI テンプレート設定	デバイスの設定

	guest-interface 0
	  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
	 !
	 app-vnic gateway1 virtualportgroup 1 guest-interface 1
	  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
	 !
	 start
	 !
	 utd multi-tenancy
	 utd engine standard multi-tenancy
	  web-filter block page profile block-url_filter
	  text <\![CDATA[Access to the requested page has been denied Please contact your Network Administrator]]>
	 !
	 web-filter url profile url_filter
	  categories block
	  games
	  !
	  block page-profile block-url_filter
	  log level error
	  reputation
	  block-threshold moderate-risk
	  !
	 !
	 threat-inspection profile intrusion_policy
	
	  threat protection
	  policy connectivity
	  logging level err
	 !
	 utd global
	 !
	 policy utd-policy-vrf-1
	  all-interfaces
	  vrf 1
	  threat-inspection profile intrusion_policy
	  web-filter url profile url_filter
	 exit
	 !

NTP の設定

表 *15 : NTP* の設定

CLI テンプレート設定	デバイスの設定
ntp server 10.29.43.1 source-interface GigabitEthernet1 version 4 exit ! !	ntp server 198.51.241.229 source GigabitEthernet1 version 4

IPv6 設定

表 *16 : IPv6* 設定

CLI テンプレートの設定	デバイスの設定
vpn 1 interface GigabitEthernet3 ipv6 address 2671:123A::1/128 shutdown ! !	interface GigabitEthernet3 shutdown arp timeout 1200 vrf forwarding 1 no ip address ip redirects ip mtu 1500 ipv6 address 2671:123A::1/128 ipv6 redirects mtu 1500 negotiation auto exit vrf definition 1 rd 1:1 address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! !

サービス構成

Cisco IOS XE リリース 17.7.1a 以前は、CLI テンプレートを介して設定できるのは、**service** の下の次の設定のみです。

```
service pad
service config
service tcp-keepalives-in
service tcp-keepalives-out
service tcp-small-servers
service udp-small-servers
```

no service password-recovery コマンドは、Cisco vManage からデバイスにプッシュできません。

VRF 設定

各 VRF に対応するサブインターフェイスを使用して、最大 300 の VRF を設定します。この例では、2 つの VRF を設定します。

（注） VLAN 1 は設定しないでください。ネイティブ VLAN 用に予約されています。

CLI テンプレート設定	デバイスの設定
! vpn 2 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.2.2 no shutdown remote-as 2 ! ipv6-neighbor 2001:DB8:2::2 remote-as 2 ! ! interface GigabitEthernet0/0/0.2 ip address 192.0.2.1/24 ipv6 address 2001: DB8:2::1/64 mtu 1496 no shutdown ! ! vpn 3 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.3.2 no shutdown remote-as 3 ! ipv6-neighbor 2001: DB8:3::2 remote-as 3 ! ! interface GigabitEthernet0/0/0.3 ip address 192.0.3.1/24 ipv6 address 2001: DB8:3::1/64 mtu 1496 no shutdown !	

CLI テンプレート設定	デバイスの設定

	vrf definition 2
	rd 1:2
	address-family ipv4
	  route-target export 1000:2
	  route-target import 1000:2
	  exit-address-family
	!
	address-family ipv6
	  exit-address-family
	!
	!
	router bgp 1000
	bgp log-neighbor-changes
	distance bgp 20 200 20
	!
	address-family ipv4 vrf 2
	  redistribute omp
	  neighbor 192.0.2.2 remote-as 2
	  neighbor 192.0.2.2 activate
	  neighbor 192.0.2.2 send-community both
	exit-address-family
	!
	address-family ipv6 vrf 2
	  redistribute omp
	  neighbor 2001:DB8:2::2 remote-as 2
	  neighbor 2001: DB8:2::2 activate
	  neighbor 2001: DB8:2::2 send-community
	both
	exit-address-family
	!
	interface GigabitEthernet0/0/0.2
	encapsulation dot1Q 2
	vrf forwarding 2
	ip address 192.0.2.1 255.255.255.0
	ip mtu 1496
	ipv6 address 2001:DB8:2::1/64
	end
	
	vrf definition 3
	rd 1:3
	address-family ipv4
	  route-target export 1000:3
	  route-target import 1000:3
	  exit-address-family
	!
	address-family ipv6
	  exit-address-family
	!
	!
	router bgp 1000
	bgp log-neighbor-changes
	distance bgp 20 200 20
	!
	address-family ipv4 vrf 3
	  redistribute omp
	  neighbor 192.0.3.2 remote-as 3
	  neighbor 192.0.3.2 activate
	  neighbor 192.0.3.2 send-community both
	exit-address-family
	!
	address-family ipv6 vrf 3
	  redistribute omp

CLI テンプレート設定	デバイスの設定
	neighbor 2001:DB8:3::2 remote-as 3 neighbor 2001: DB8:3::2 activate neighbor 2001: DB8:3::2 send-community both exit-address-family ! interface GigabitEthernet0/0/0.3 encapsulation dot1Q 3 vrf forwarding 3 ip address 192.0.3.1 255.255.255.0 ip mtu 1496 ipv6 address 2001:DB8:3::1/64 end

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。