

Reconstrua sua malha Catalyst SD-WAN

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Pré-requisitos antes de recriar a estrutura](#)

[Opções de implantação](#)

[Etapas Comuns Aplicáveis a Todas as Combinações](#)

[Instalar e ativar controladores SD-WAN \(Gerenciador, Validador, Controlador\)](#)

[Ativar um nó do Cisco Manager](#)

[Ativar o validador](#)

[Ativar um nó de controlador \(vSmart\)](#)

[Configuração CLI básica em todos os controladores](#)

[Combinação 1: vManage autônomo + sem DR](#)

[Passo 1: Pré-verificações](#)

[Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage](#)

[Passo 3: Backup/Restauração do Config-db](#)

[Passo 4: Reautenticação de controladores e invalidação de controladores antigos](#)

[Passo 5: Pós-cheques](#)

[Combinação 2: vManage autônomo + DR de nó único](#)

[Passo 1: Pré-verificações](#)

[Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage](#)

[Passo 3: Backup/Restauração do Config-db](#)

[Passo 4: Configuração de DR de nó único](#)

[Passo 5: Reautenticação de controladores e invalidação de controladores antigos](#)

[Passo 6: Pós-cheques](#)

[Combinação 3: vManage Cluster + Sem DR](#)

[Passo 1: Pré-verificações](#)

[Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage](#)

[Passo 3: Construir cluster vManage](#)

[Passo 4: Backup/Restauração do Config-db](#)

[Passo 5: Reautenticação de controladores e invalidação de controladores antigos](#)

[Passo 6: Pós-cheques](#)

[Combinação 4: vManage Cluster + DR manual/em espera fria](#)

[Passo 1: Pré-verificações](#)

[Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage](#)

[Passo 3: Construir cluster vManage](#)

[Passo 4: Configuração de cluster DR em standby frio](#)

[Passo 5: Backup/Restauração do Config-db](#)

[Passo 6: Reautenticação de controladores e invalidação de controladores antigos](#)

[Passo 7: Pós-cheques](#)

[Combinação 5: vManage Cluster + DR ativado](#)

[Passo 1: Pré-verificações](#)

[Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage](#)

[Passo 3: Construir cluster vManage](#)

[Passo 4: Backup/Restauração do Config-db](#)

[Passo 5: Ativar a recuperação de desastres em um cluster vManage](#)

[Passo 6: Reautenticação de controladores e invalidação de controladores antigos](#)

[Pós-cheques](#)

Introdução

Este documento descreve como reconstruir uma estrutura Cisco SD-WAN, incluindo backup e restauração de configurações do controlador para várias implantações.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN)
- Cisco Software Central
- Baixe o software de controladores em software.cisco.com

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Pré-requisitos antes de recriar a estrutura

- Novo conjunto de system-ips, site-ids deve ser configurado para a nova malha dos controladores
- Verifique se as regras de firewall estão em vigor para permitir a comunicação entre os controladores e as bordas
- Observe o nome de usuário e a senha do neo4j(configuration-db) (devem ser os mesmos em todos os nós do vManage em um cluster)
- Desativar o port-hop em todas as bordas

- Aumente os temporizadores de reinicialização da energia - normal para 7 dias
- Limpar alarmes em ferramentas de terceiros antes da migração
- Os dados históricos de estatísticas (alarmes, eventos, estatísticas de dispositivo etc.) são perdidos, a menos que haja uma configuração anterior para exportar estatísticas para um servidor externo, como asvAnalytics
- Se o Cloud OnRamp estiver configurado, verifique se você tem acessibilidade ao c8000v implantado na nuvem antes do início desta atividade
- Se você tiver o SDAVC habilitado na malha antiga, certifique-se de que a nova malha o tenha habilitado (para cluster, ele precisa ser habilitado apenas em um único nó)
- A restauração do banco de dados de configuração é suportada somente na mesma versão da malha original
- Confirme a persona usada para os controladores. Oferecemos suporte a persona COMPUTE_DATA e DATA (detalhes em cada seção)
- Para a Autoridade de Certificação Corporativa, é necessário usar o certificado raiz emitido pela Autoridade de Certificação Corporativa, que é usado na sobreposição existente, e o certificado é assinado usando o servidor da Autoridade de Certificação corporativa e instalado para todos os controladores via interface do usuário

Opções de implantação

Implantação do vManage

- Autônomo (1 nó)
- Cluster (3 ou 6 nós)

Opções de DR

- Sem DR
- DR de nó único
- Cluster de recuperação de desastres em standby (manual/acionado pelo administrador)



Note: Para obter mais detalhes sobre o tipo de recuperação de desastres, consulte este [link](#)

Combinações:

#	Configuração do vManage	Opção DR
1	Autônomo (1 nó)	Sem DR
2	Autônomo (1 nó)	DR de nó único
3	Cluster (3 ou 6 nós)	Sem DR
4	Cluster (3 ou 6 nós)	Cluster de DR em standby

Etapas Comuns Aplicáveis a Todas as Combinações

Essas etapas são comuns a todas as combinações de implantação. Eles abordam o processo de ativar instâncias de VM e aplicar a configuração CLI básica. Cada seção de combinação informa quantas instâncias devem ser implantadas e quais etapas adicionais devem ser concluídas.

Instalar e ativar controladores SD-WAN (Gerenciador, Validador, Controlador)



Note: A Cisco renomeou determinados termos, de modo que esses termos são intercambiáveis. Cisco vManage = Cisco Catalyst Manager, Cisco vBond = Cisco Catalyst Validator, Cisco vSmart = Cisco Catalyst Controller

Faça o download dos arquivos OVA para controladores SD-WAN da página de download do software Cisco [aqui](#):

- Escolha vEDGE Cloud e faça o download do vBond OVA para obter a versão de software necessária.
- Escolha o software vManage e baixe o vManage OVA para a versão de software necessária.
- Escolha o software vSmart e faça download do vSmart OVA para obter a versão de software necessária.



Note: Nas plataformas ESXi/cloud, ative os controladores vSmart, vBond e vManage usando o arquivo OVA. Consulte o documento vinculado e certifique-se de que CPU, RAM e discos suficientes estejam alocados para todos os controladores, dependendo do tipo de implantação da SD-WAN. Navegue [aqui](#) para obter informações adicionais. Certifique-se de atribuir um disco secundário ao nó vManage conforme mencionado na coluna Tamanho de armazenamento* no guia de computação vinculado.

Ativar um nó do Cisco Manager

- Quando a VM do Cisco Manager ou vManage estiver implantada e o console do gerenciador estiver acessível, aguarde a conclusão da inicialização. Uma indicação é que vemos que um sistema de mensagens está pronto e solicita o nome de usuário e a senha.
- Insira o nome de usuário das credenciais de usuário padrão como admin e a senha como admin. Poste que ele solicita que o usuário altere a senha, defina a senha que é necessária para o administrador de usuário de acordo com sua escolha.
- Em seguida, ele solicita que o usuário selecione a persona. Essa é uma etapa crítica se a intenção for ter um cluster vManage. Escolha a persona conforme os cenários mostrados

aqui:

For a standalone vManage, choose the persona as COMPUTE_AND_DATA.

For a 3 node cluster, on 3 vManage nodes, the persona is set to COMPUTE_AND_DATA.

For a 6 node cluster, on 3 vManage nodes the persona is COMPUTE_AND_DATA and on rest 3 vManage nodes pe

Exemplo: Escolha 1 para COMPUTE_AND_DATA

```
booted via startup_32()
Physical KASLR using RDRAND RDTSC...
Virtual KASLR using RDRAND RDTSC...

Decompressing Linux... Parsing ELF... Performing relocations... done.
Booting the kernel.

viptela 20.12.5.1

vmanage login:
viptela 20.12.5.1

vmanage login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
You must set an initial admin password different from default password.
Password:
Re-enter password:
1) COMPUTE_AND_DATA
2) DATA
3) COMPUTE
Select persona for vManage [1,2 or 3]: 1
You chose persona COMPUTE_AND_DATA (1)
Are you sure? [y/n] _
```

Escolha o disco secundário conforme mostrado:

```

2) DATA
3) COMPUTE
Select persona for vManage [1,2 or 3]: 1
You chose persona COMPUTE_AND_DATA (1)
Are you sure? [y/n] y
Available storage devices:
sdb      100GB
1) sdb
Select storage device to use: 1
Would you like to format sdb? (y/n): y
mount: /dev/sdb: not mounted.
mke2fs 1.45.7 (28-Jan-2021)
Discarding device blocks: done
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 5a94db1f-71c4-4e25-a6d1-8ef2495c1de2
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done

```

- Escolha o disco secundário e digite Y para confirmar.
- O Cisco Manager é recarregado. Depois de inicializar, insira o nome de usuário e a senha com a nova senha que foi recém-configurada.

```

early console in extract_kernel
input_data: 0x00000000021753b4
input_len: 0x000000000121c7f3
output: 0x0000000001000000
output_len: 0x000000000237ea6c
kernel_total_size: 0x0000000001fb0000
booted via startup_32()
Physical KASLR using RDRAND RDTSC...
Virtual KASLR using RDRAND RDTSC...

Decompressing Linux... Parsing ELF... Performing relocations... done.
Booting the kernel.

viptela 20.12.5.1

vmanage login:
viptela 20.12.5.1

vmanage login: admin
Password:
Last login: Wed Feb 18 10:52:47 UTC 2026 on tty0
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
vmanage#

```

- Você pode configurar a interface de gerenciamento VPN 512 para permitir o acesso de gerenciamento fora de banda ao controlador.
- Use o comando `show interface |` para verificar as VPNs para as quais as interfaces estão mapeadas no momento.

- configure as interfaces de acordo.

Exemplo

VPN	INTERFACE		TYPE	SPEED		MSS		RX		TX	
	MTU	HWADDR		IP ADDRESS	DUPLEX	STATUS ADJUST	STATUS UPTIME	STATUS PACKETS	TYPE	TYPE	TYPE
0	eth0		ipv4	192.168.45.218/24		Up	Up	-	null	servi	
-	-	00:50:56:bd:36:6b		1000	full	-	0:00:38:49	12116	281		
0	eth1		ipv4	-		Down	Down	-	-	-	-
-	-	00:50:56:bd:7a:c6		1000	full	-	-	-	-	-	-
0	eth2		ipv4	-		Down	Down	-	-	-	-
-	-	00:50:56:bd:be:90		1000	full	-	-	-	-	-	-
0	docker0		ipv4	-		Down	Down	-	-	-	-
-	-	02:42:6d:57:e5:4e		1000	full	-	-	-	-	-	-
0	cbr-vmanage		ipv4	-		Down	Up	-	-	-	-
-	-	02:42:22:37:90:ef		1000	full	-	-	-	-	-	-

vmanage#



Note: Você pode consultar a configuração do vManage existente e configurar o mesmo esquema de endereço IP aqui.

Configurações da interface de gerenciamento (VPN 512)

- Se uma interface precisar ser movida da VPN 0 para a VPN 512, use esses comandos e configure o endereço IP na interface

```
Conf t
vpn 0
no interface eth0
vpn 512
interface eth0
ip address

no shutdown
!
ip route 0.0.0.0/0
```

!

Ativar o validador

- No hipervisor, configure o computador necessário (CPU, RAM e disco) para o nó vBond e ligue-o.
- Quando o console estiver acessível, aguarde até que o vBond inicialize completamente. Aguarde a mensagem Sistema pronto.
- O sistema então solicita o nome de usuário e a senha. Insira o nome de usuário das credenciais de usuário padrão como admin e a senha como admin. Depois disso, ele solicita que o usuário altere a senha, defina a senha necessária para o usuário admin de acordo com sua escolha.
- Você pode configurar a interface de gerenciamento VPN 512 para permitir o acesso de gerenciamento fora de banda ao controlador.
- Use o comando `show interface |` para verificar as VPNs para as quais as interfaces estão mapeadas no momento.
- Configure as interfaces de acordo.

Exemplo:

```
admin connected from 127.0.0.1 using console on vbond-01
vbond-01# sh int : tab
```

VPN	INTERFACE	AF	IP ADDRESS	SPEED	IF	TCP	IF	IF	ENCAP	TX
E	MTU	HWADDR	TYPE	MBPS	DUPLEX	ADMIN	OPER	TRACKER	RX	PORT
						STATUS	STATUS	STATUS	PACKETS	PACKETS
						ADJUST	UPTIME			
0	ge0/0	ipv4	10.106.51.184/24	1000	full	Up	Up	-	null	transpor
t	-	00:50:56:bd:be:68				-	0:04:39:15	1838		1843
0	ge0/1	ipv4	-	1000	full	Down	Down	-	-	-
-	-	00:50:56:bd:04:8e				-	-	-	-	-
0	ge0/2	ipv4	-	1000	full	Down	Down	-	-	-
-	-	00:50:56:bd:f1:d5				-	-	-	-	-
0	system	ipv4	1.1.1.4/32	1000	full	Up	Up	-	null	loopback
-	-					-	0:04:40:46	0		0
0	loopback1	ipv4	192.168.51.15/32	1000	full	Up	Up	-	null	loopback
-	-					-	0:04:39:18	0		0
512	eth0	ipv4	10.106.51.169/24	1000	full	Up	Up	-	null	mgmt
-	-	00:50:56:bd:3c:9b				-	0:04:39:18	1839		1839

```
vbond-01#
```



Note: Você pode consultar a configuração do vBond existente e configurar as mesmas configurações aqui.

Configurações da interface de gerenciamento (VPN 512)

- Se uma interface precisar ser movida da VPN 0 para a VPN 512, use esses comandos e configure o endereço IP na interface.

```
Conf t
vpn 0
no interface eth0
vpn 512
interface eth0
ip address

no shutdown
!
ip route 0.0.0.0/0

!
commit
```

Ativar um nó de controlador (vSmart)

- Execute as mesmas etapas que o Validador para ativar o nó vSmart.
- Depois que o endereço IP do VPN 512 for configurado em todos os controladores SD-WAN, você poderá acessá-los usando SSH no endereço IP do VPN 512.

Configuração CLI básica em todos os controladores

Quando você tiver acesso SSH a todos os controladores, configure essas configurações CLI em cada controlador.

Configuração do sistema

```
config t
```

```
system
host-name
```

```
system-ip
```

```
site-id
```

```
organization-name
```

```
vbond
```

```
commit
```



Observação: se estamos usando URL como endereço vBond, certifique-se de configurar os endereços IP do servidor DNS na configuração VPN 0 ou de garantir que eles possam ser resolvidos.

Configuração da Interface de Transporte (VPN 0)

Essas configurações são necessárias em todos os controladores para ativar a interface de transporte usada para estabelecer conexões de controle com os roteadores e o restante dos controladores.

```
config t
vpn 0
dns
```

```
primary
dns

secondary
interface eth1
ip address

tunnel-interface
allow-service all
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service stun
allow-service https
!
no shutdown
!
ip route 0.0.0.0/0

commit
```



Observação: você pode consultar as configurações da sua controladora existente e, se a configuração estiver presente, poderá adicioná-la às novas controladoras.

Configure o protocolo de controle como TLS somente se houver um requisito para que os roteadores estabeleçam conexões de controle seguras com os nós do vManage usando TLS. Por padrão, todos os controladores e roteadores estabelecem conexões de controle usando DTLS. Essa é uma configuração opcional necessária apenas nos nós vSmart e vManage, dependendo de sua necessidade.

```
Conf t
security
  control
    protocol tls
Commit
```

Combinação 1: vManage autônomo + sem DR

Instâncias necessárias:

- 1 vManage (COMPUTE_AND_DATA)
- 1 ou mais vBond
- 1 ou mais vSmart

Etapas:

1. Ativar todas as instâncias usando as Etapas Comuns
2. Pré-verificações
3. Configurar a interface do usuário, os certificados e os controladores integrados do vManage
4. Backup/restauração de config-db
5. Pós-cheques

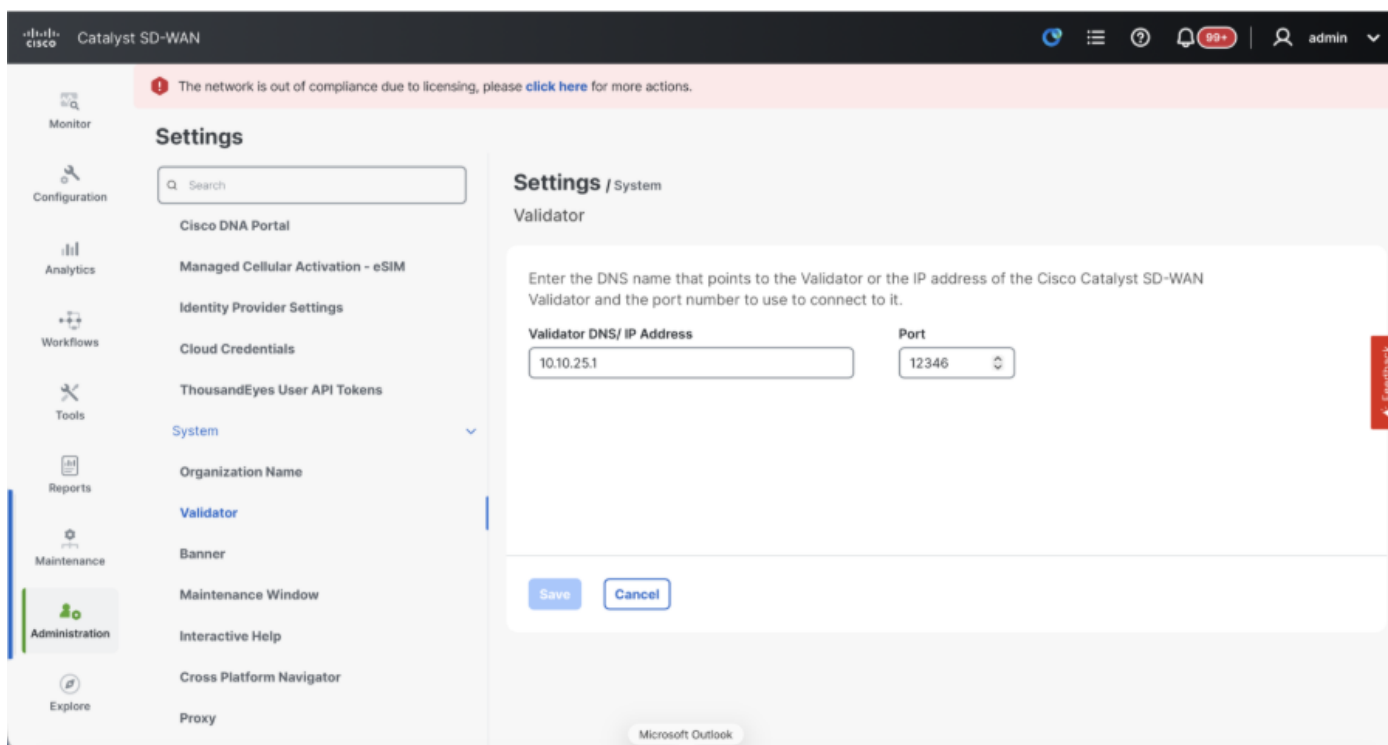
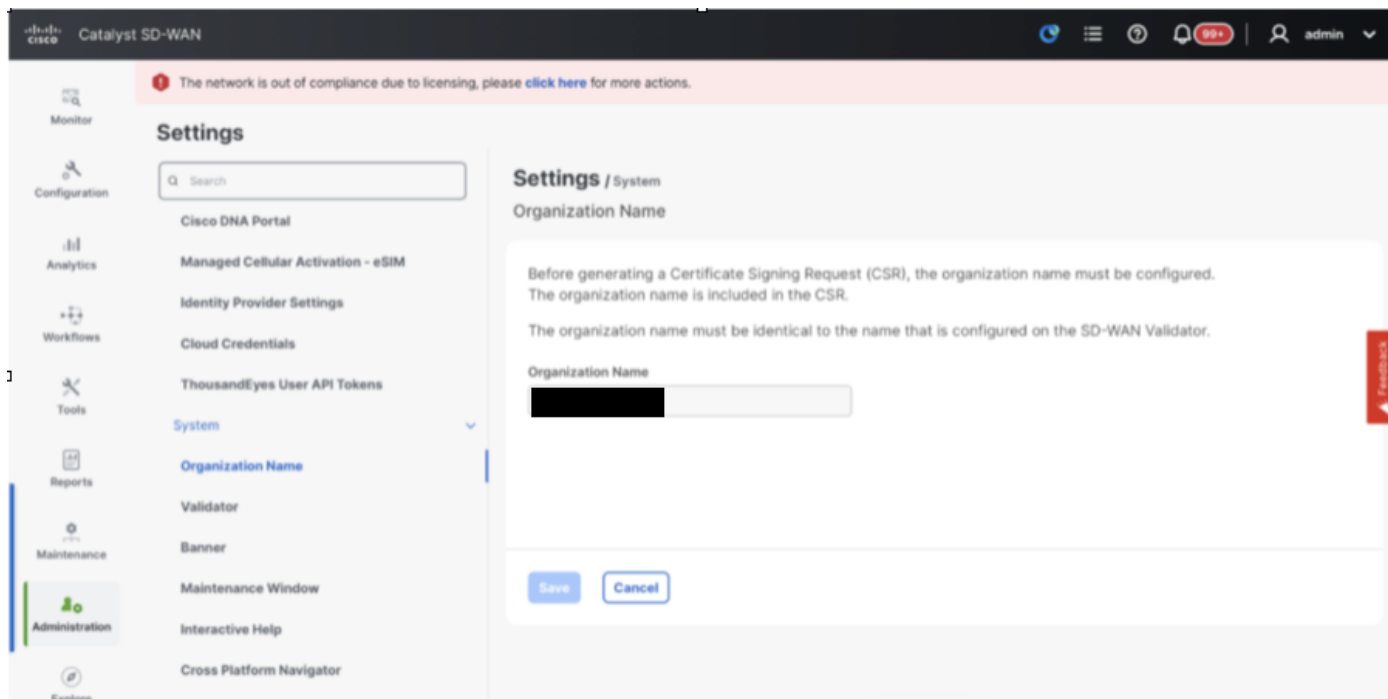
Passo 1: Pré-verificações

- Certifique-se de que o número de instâncias ativas do Cisco SD-WAN Manager seja idêntico ao número de instâncias recém-instaladas do Cisco SD-WAN Manager .
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager executem a mesma versão de software.
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager possam acessar o endereço IP de gerenciamento do Cisco SD-WAN Validator.
- Verifique se os certificados foram instalados nas instâncias recém-instaladas do Cisco SD-WAN Manager.
- Certifique-se de que os relógios em todos os dispositivos Cisco Catalyst SD-WAN, incluindo as instâncias recém-instaladas do Cisco SD-WAN Manager, estejam sincronizados.
- Verifique se um novo conjunto de IPs do sistema e IDs do local está configurado nas instâncias do Cisco SD-WAN Manager recém-instalado, juntamente com a mesma configuração básica do cluster ativo.

Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage

Atualizar as configurações na interface do usuário do vManage

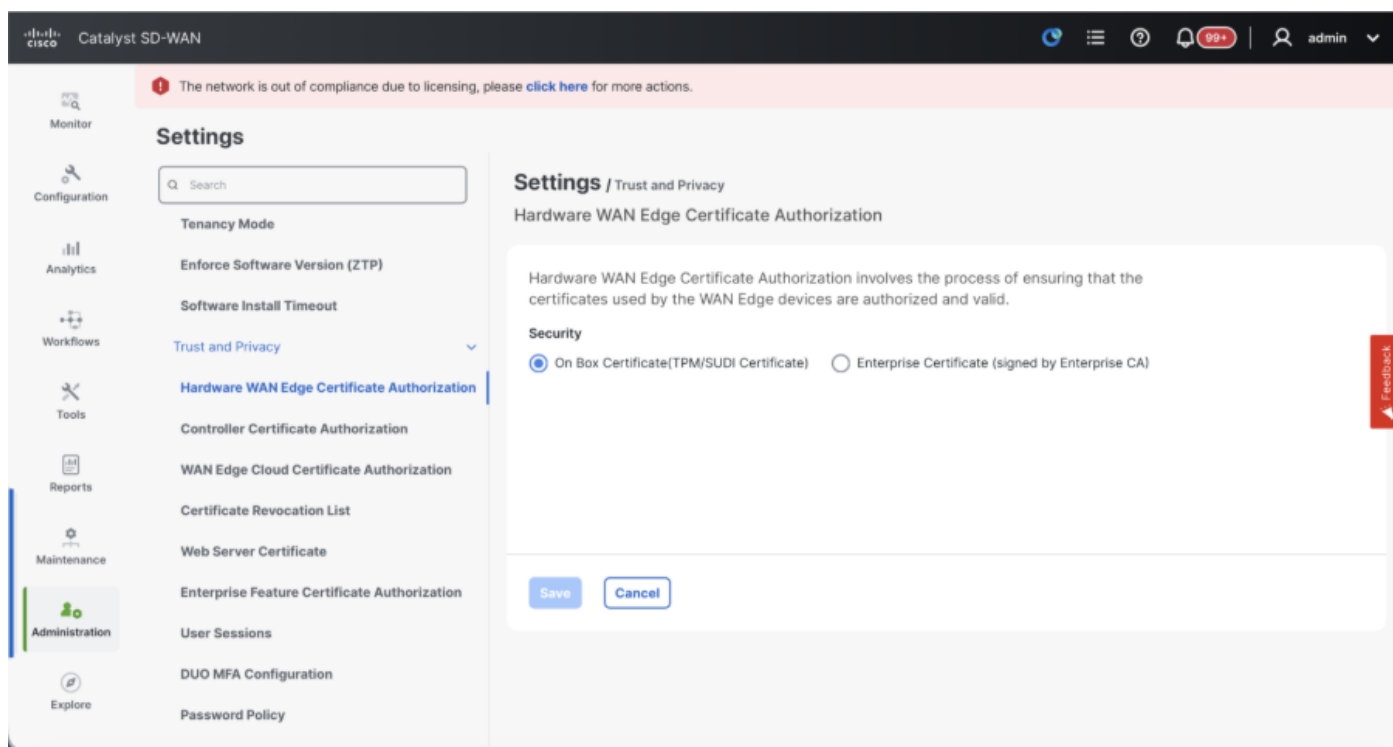
- Depois que as configurações na Etapa 1 forem adicionadas à CLI de todos os controladores, poderemos acessar a webUI do vManage, usando o URL `https://<vmanage-ip>` em seu navegador. Use o endereço IP VPN 512 dos respectivos nós do vManage. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue até Administration > Settings e conclua estas etapas.
- Configure o nome da organização e o endereço IP/URL do validador/vBond. Configure o mesmo valor da CLI do nó do vManage.
- No vManage 20.15/20.18, essas configurações estão disponíveis na seção Sistema.



- Verifique as configurações da CA (Certificate Authorization, Autorização de Certificado), que decide a autoridade de certificação usada para assinar os certificados. Podemos ver 3 opções aqui:

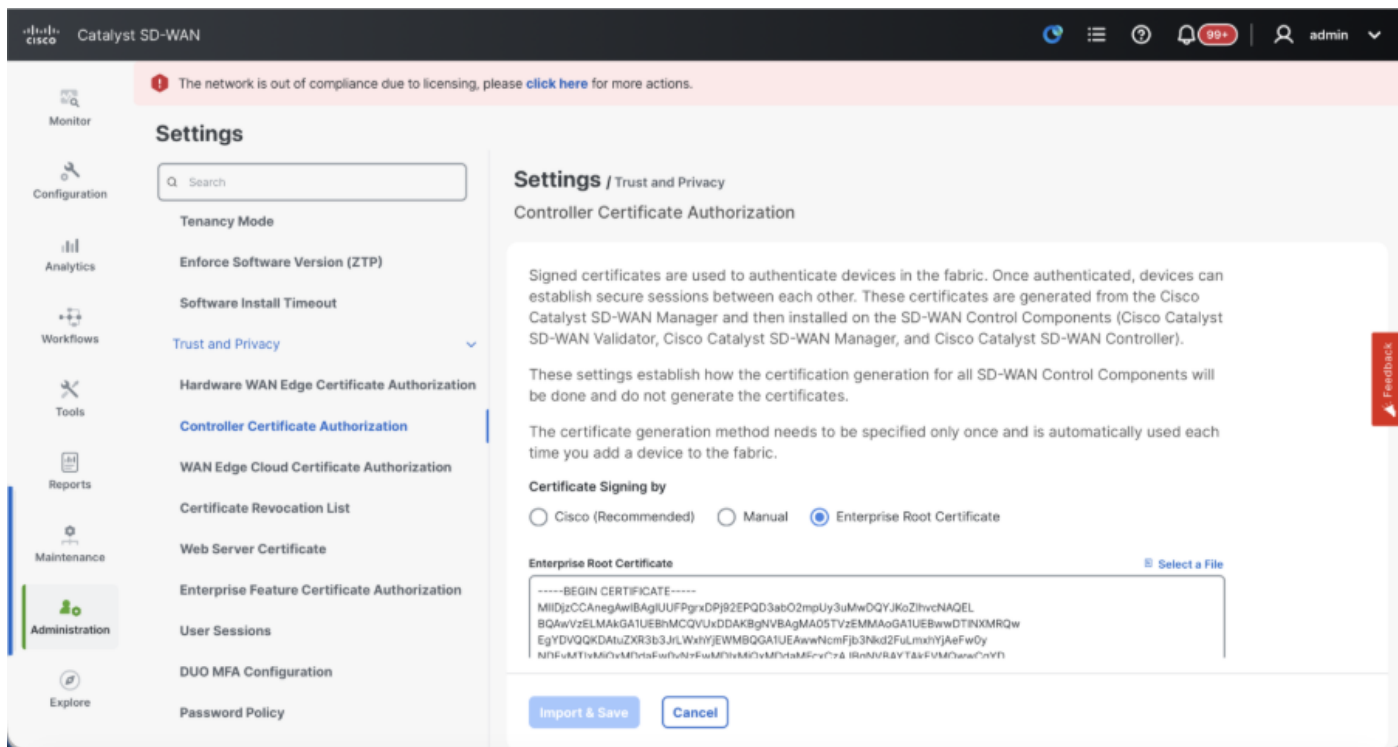
1. Autorização do certificado de borda da WAN de hardware - decide a CA para os roteadores de borda da SD-WAN de hardware.

- On Box Certificate (TPM/SUDI Certificate) - Com essa opção, o certificado pré-instalado no hardware do roteador é usado para estabelecer as conexões de controle (conexões TLS/DTLS)
- Certificado corporativo (assinado pela autoridade de certificação corporativa) - Com essa opção, os roteadores usam certificados assinados pela autoridade de certificação corporativa da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



2. Controller Certificate Authorization - Decide a CA para controladores SD-WAN.

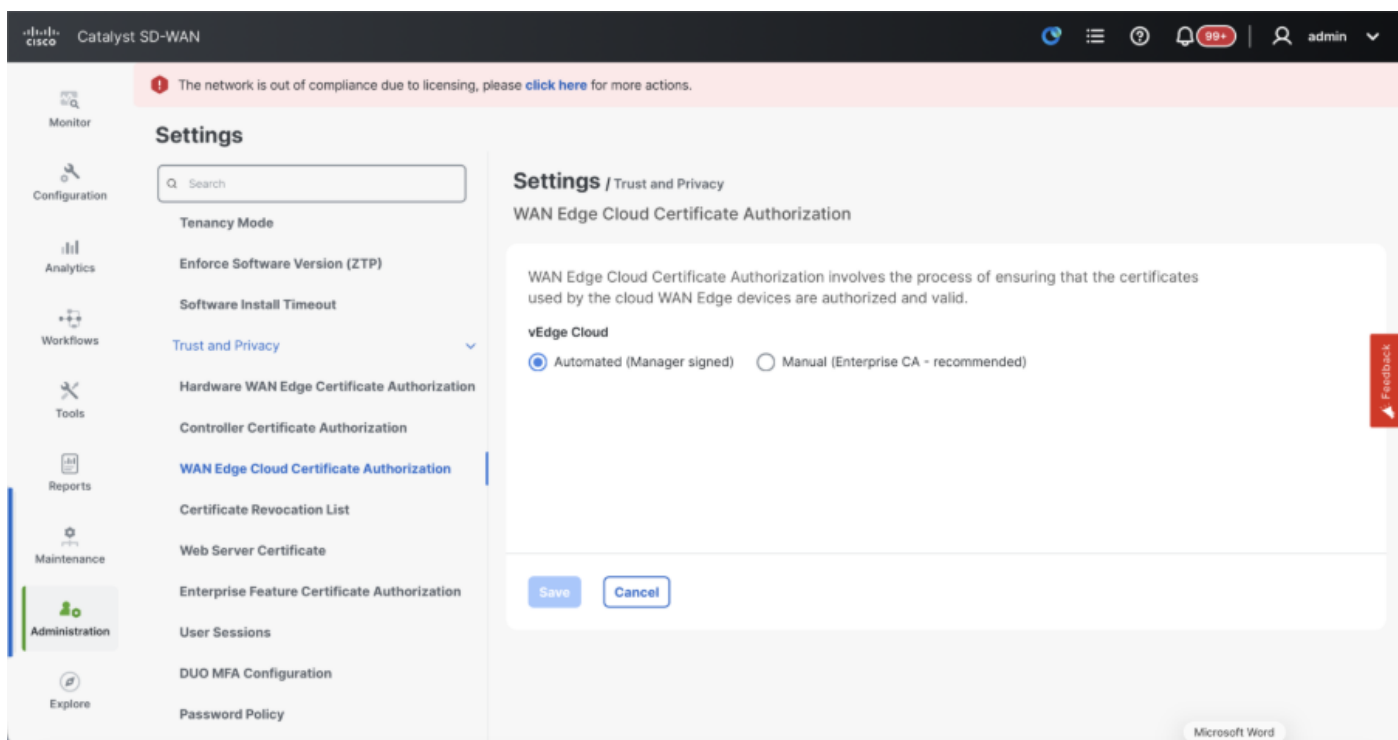
- Cisco (Recomendado) - Os controladores usam os certificados assinados pelo Cisco PKI. O vManage entra em contato automaticamente com o portal PNP usando as credenciais de Smart Account configuradas no vManage e obtém o certificado assinado e é instalado no controlador.
- Manual - Os controladores usam os certificados assinados pela PKI da Cisco. Assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Certificado raiz empresarial - com esta opção, os roteadores usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



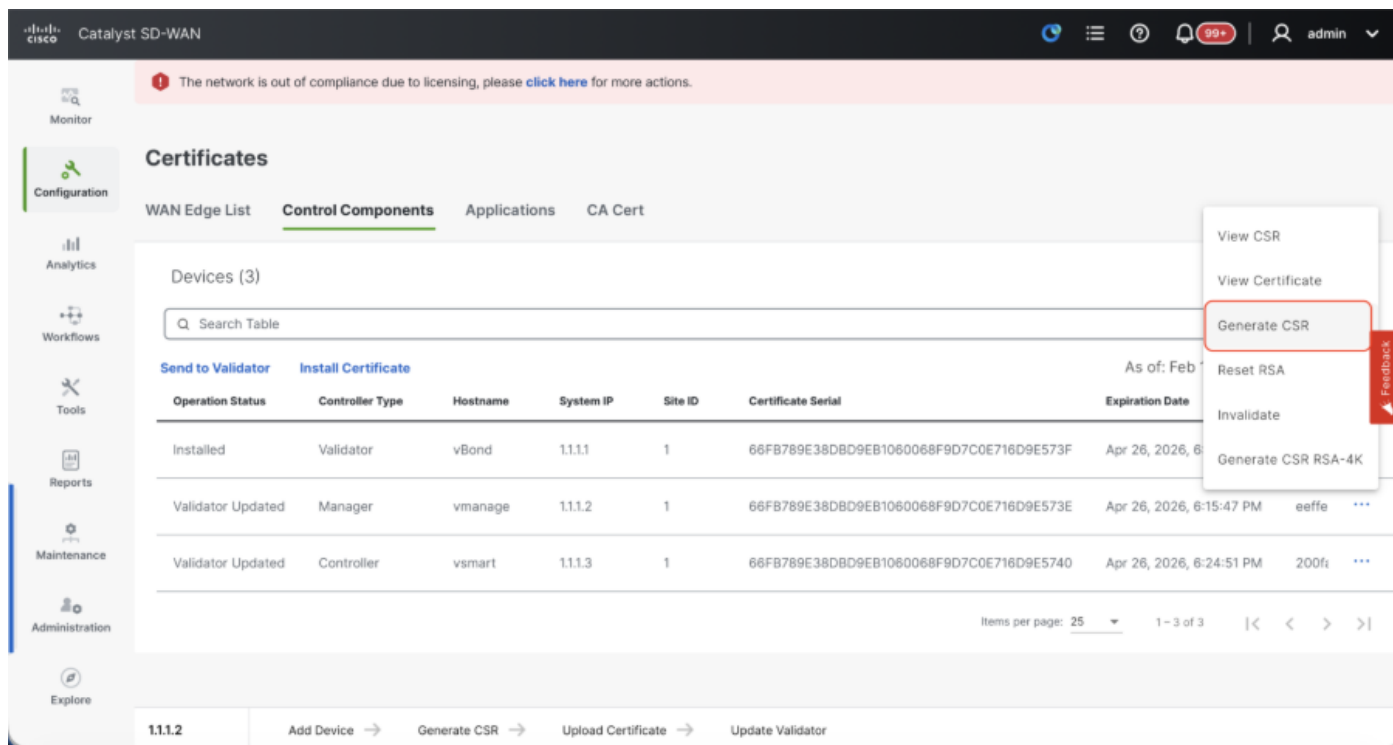
3. Autorização de certificado de nuvem de borda de WAN - decide a CA para roteadores de borda de SD-WAN virtuais (CSR1000v, C8000v, nuvem vEdge)

- Automatizado (vManage assinado) - O vManage assina automaticamente o CSR para os roteadores de borda virtual e instala o certificado no roteador.
- Manual (CA empresarial - recomendado) - Os roteadores virtuais usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.

Caso estejamos usando nossa própria CA, autoridade de certificação empresarial, escolha Empresa.



- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores
- Clique em ... para Gerente/vManage e clique em Gerar CSR.



- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.

Integração do vBond/Validator e vSmart/Controller ao vManage

Navegue para Configuration > Devices > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Onboarding vBond/Validador

- Clique em Add vBond no caso de 20.12 vManage ou Adicionar validador no caso de 20.15/20.18 vManage. Um pop-up é aberto, insira o O IP de transporte VPN 0 de vBond que pode ser acessado a partir do vManage.
- Verifique a acessibilidade usando ping se permitido a partir do CLI de vManage to vBond IP.

- Insira as credenciais de usuário do vBond.



Observação: Precisamos usar credenciais de administrador de VoBond ou uma parte do usuário de netadmingroup. Você pode verificar isso no CLI do vBond. Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vBond.



Note: Se o vBond estiver por trás de um dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vBond está traduzido para um IP público. Se o IP da interface VPN 0 não estiver acessível no vManage, use o endereço IP público da interface VPN 0 nesta etapa.

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. On the left, the 'Configuration' tab is selected, and the 'Control Components' section is active. A table titled 'Control Components (3)' lists the following components:

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Version
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

On the right, the 'Add Validator' dialog box is open. It contains the following fields:

- Validator Management IP Address (text input)
- Username (text input)
- Password (password input)
- Generate CSR (dropdown menu set to 'No')

At the bottom of the dialog are 'Cancel' and 'Add' buttons. A red 'Feedback' button is also visible on the right side of the dialog.

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se a Cisco (recomendada) for escolhida, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, será instalado no vBond automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver várias vBonds, repita as mesmas etapas.

vSmart/controlador integrado

- Clique em Add vSmart no caso do vManage 20.12 ou Add Controller no caso do vManage 20.15/20.18.
- Um pop-up é aberto, insira o IP de transporte VPN 0 do vSmart que pode ser acessado no vManage.
- Verifique a acessibilidade usando ping se permitido do CLI do vManage para o vSmart IP.
- Insira as credenciais de usuário do vSmart. Observe que precisamos usar credenciais de administrador do vSmart ou uma parte do usuário do grupo netadmin.
- Você pode verificar isso na CLI do vSmart.
- Defina o protocolo como TLS, se pretendemos usar TLS para roteadores para estabelecer conexões de controle com vSmart. Essa configuração também precisa ser configurada na CLI dos nós vSmarts e vManage.
- Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vSmart.



Observação: se o vSmart estiver por trás do dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vSmart está convertido em um IP público e se o IP da interface VPN 0 não pode ser acessado do vManage, use o endereço IP público do IP da interface VPN 0 nesta etapa.

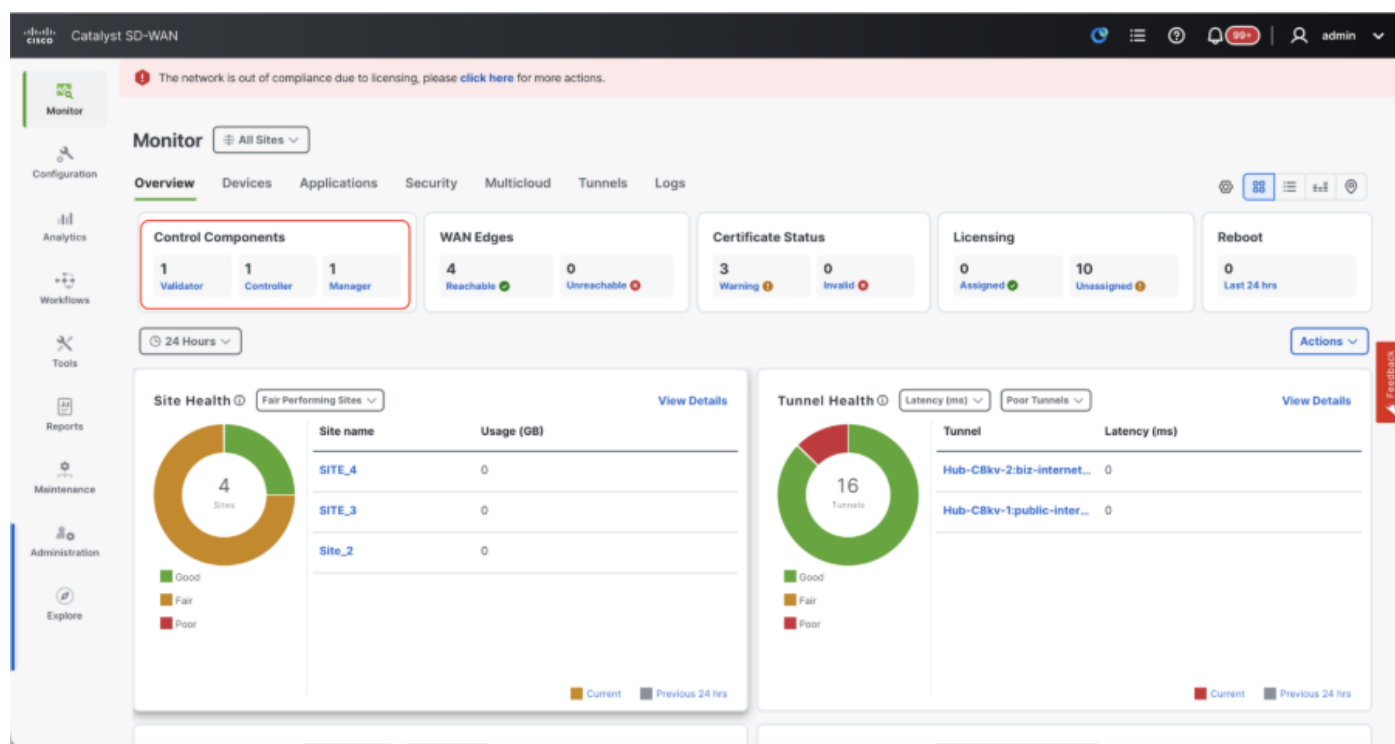
The screenshot shows the Cisco Catalyst SD-WAN vManage interface. The main panel displays the 'Devices' section with a table of 'Control Components (3)'. The table has columns: Controller Type, Site Name, Hostname, Config Locked, Managed By, Device Status, and Sy. The table lists three components: a Validator (SITE_1, vBond, No, Unmanaged, In Sync), a Manager (SITE_1, vmanage, No, Unmanaged, In Sync), and a Controller (SITE_1, vsmart, Yes, Template vSmart-template, In Sync). On the right, the 'Add Controller' modal is open, showing fields for Controller Management IP Address, Username, Password, Protocol (set to DTLS), Port, and Generate CSR (set to No). A red 'Feedback' button is visible on the right side of the modal.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sy
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vSmart automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. O mesmo procedimento será aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- Se houver vários vSmarts, repita as mesmas etapas.

Verificação

Após concluir todas as etapas, verifique se todos os componentes de controle estão acessíveis em Monitor>Dashboard



- Clique nos respectivos componentes de controle e confirme se todos estão acessíveis.
- Navegue até Monitor > Devices e confirme se todos os componentes de controle estão acessíveis.

The screenshot shows the Catalyst SD-WAN Monitor interface. At the top, there's a navigation bar with 'Monitor' selected. Below it, a 'Devices' tab is active. A table titled 'Devices (7)' is displayed with the following data:

Hostname	Device Model	Site Name	System IP	Health	Reachability	Control	BFD	TLOC	Up Since	CPU Load	Memory utilization	Act
vBond	Validator	SITE_1	1.1.1.1	OK	↑	14 / 14	N/A	- / -	Jan 13, 2026 11:32 AM	0.79%	13%	...
vmanage	Manager	SITE_1	1.1.1.2	Warning	↑	6 / 6	N/A	8 / 8	Feb 06, 2026 10:07 AM	2.48%	77%	...
vsmart	Controller	SITE_1	1.1.1.3	OK	↑	7 / 7	N/A	2 / 2	Jan 13, 2026 11:33 AM	1.32%	16%	...

Passo 3: Backup/Restauração do Config-db

Coletar backup e restauração do banco de dados de configuração do vManage em outro nó do vManage

Coletar backup do BD de configuração:

- Na estrutura SD-WAN atualmente em uso, é possível gerar backup de configuração-db nas configurações de cluster autônomas do vManage e do vManage.
- No caso do vManage autônomo, o próprio vManage é o líder do banco de dados de configuração.

Confirme se o configuration-db está sendo executado no nó vManage.

Você pode verificar o mesmo usando o comando `request nms configuration-db status` `onvManageCLI`. A saída é a mostrada

```
vmanage# request nms configuration-db status
NMS configuration database
  Enabled: true
  Status: running PID:32632 for 1066085s
  Native metrics status: ENABLED
  Server-load metrics status: ENABLED
vmanage#
```

Use esse comando para coletar o backup configuration-db do nó vManage líder configuration-db identificado.

```
request nms configuration-db backup path /opt/data/backup/
```

A saída esperada é a seguinte:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Anote as credenciais do configuration-db se ele tiver sido atualizado.
- Se você não souber as credenciais do configuration-db, entre em contato com o TAC para recuperar as credenciais do configuration-db dos nós vManage existentes.
- As credenciais padrão do configuration-db são nome de usuário: neo4j e senha: senha

Restaurar backup do banco de dados de configuração para outro nó do vManage

Copie o backup do configuration-db para o diretório /home/admin/ do vManage usando SCP.

Exemplo de saída do comando scp:

```
XXXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1

(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Para restaurar o backup do configuration-db, primeiro precisamos configurar as credenciais do configuration-db. Se suas credenciais de configuração-db forem default (neo4j/password), podemos pular esta etapa.

Para configurar as credenciais do configuration-db, use o comando request nms configuration-db update-admin-user. Use o nome de usuário e a senha de sua escolha.

Observe que o servidor de aplicativos do vManage é reiniciado. Devido ao qual a interface do usuário do vManage fica inacessível por um curto período.

```
vmanage# request nms configuration-db update-admin-user
```

```
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operation)
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Post que podemos continuar para restaurar o backup do configuration-db:

Podemos usar o comando request nms configuration-db restore path /home/admin/< > para restaurar o configuration-db para o novo vManage:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Resetting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Depois que o configuration-db for restaurado, verifique se a interface do usuário do vManage está acessível. Aguarde cerca de 5 minutos e tente acessar a interface do usuário.

Depois de fazer logon na interface do usuário com êxito, verifique se a lista de roteadores de borda, o modelo, as políticas e todas as configurações presentes na interface do usuário do vManage anterior ou existente estão refletidas na nova interface do usuário do vManage.

Passo 4: Reautenticação de controladores e invalidação de controladores antigos

Depois que o configuration-db for restaurado, precisamos autenticar novamente todos os novos controladores (vmanage/vsmart/vbond) na malha.



Observação: na produção real, se o IP da interface usado para reautenticar for o IP da interface do túnel, será necessário garantir que o serviço NETCONF seja permitido na interface do túnel do vManage, vSmart e vBond e também nos firewalls ao longo do caminho. A porta de firewall a ser aberta é a porta TCP 830 como regra bidirecional do cluster DR para todos os vBonds e vSmarts.

Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers

- Clique nos três pontos próximos a cada controlador e clique em Editar

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. The top navigation bar includes 'Cisco Catalyst SD-WAN', 'Select Resource Group', and 'Configuration > Devices'. Below this, there are tabs for 'WAN Edge List' and 'Controllers'. The main content area shows a table of controllers (5 total) with columns for Controller Type, Site Name, Hostname, Config Locked, Managed By, Device Status, System-ip, Draft Mode, Certificate Status, Policy Name, and Policy Version. The table lists vBond, vManage, and vSmart controllers. On the right, an 'Edit' sidebar is open, showing fields for IP Address, Username, and Password.

The screenshot shows the Cisco vManage Administration > Disaster Recovery page. The page displays the Primary Cluster Status and Standby Cluster Status. A red box highlights the 'Manage Disaster Recovery' section, which includes buttons for 'Pause Disaster Recovery', 'Resume Disaster Recovery', and 'Delete Disaster Recovery'. The details section shows the last replicated time, time to replicate, size of data, status, and history.

- Substitua o endereço ip (system-ip do controlador) pelo endereço ip da vpn 0 de transporte (interface de túnel). Insira o nome de usuário e a senha e clique em salvar
- Faça o mesmo para todos os novos controladores na malha

Sincronizar a cadeia de certificados raiz

Depois que todos os controladores estiverem integrados, conclua esta etapa:

Em qualquer servidor Cisco SD-WAN Manager no cluster recém-ativo, execute estas ações:

Digite este comando para sincronizar o certificado raiz com todos os dispositivos Cisco Catalyst SD-WAN no cluster recém-ativo:

<https://vmanage-url/dataservice/system/device/sync/rootcertchain>

Digite este comando para sincronizar o UUID do Cisco SD-WAN Manager com o Cisco SD-WAN Validator:

<https://vmanage-url/dataservice/certificate/syncvbond>

Depois que a estrutura for restaurada e as sessões de controle e bfd estiverem ativas para todas as bordas e controladores na estrutura, precisamos invalidar os controladores antigos (vmanage/vsmart/vbond) da interface do usuário

- Na interface do usuário do vmanage, clique em Configuration > Certificates > Controllers
- Clique em Controladores
- Clique nos três pontos no lado direito da controladora (vmanage/vsmart/vbond) da estrutura antiga. Clique em invalidar
- Clique em enviar para vbond
- Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers
- Clique nos três pontos no lado direito da controladora (vmanage/vsmart/vbond) da estrutura antiga. Clique em Excluir

Passo 5: Pós-cheques



Note: Continue com a seção Post Checks mostrada aqui, que é comum a todas as combinações de implantação.

Combinação 2: vManage autônomo + DR de nó único

Instâncias necessárias:

- 1 vManage (principal, COMPUTE_AND_DATA)
- 1 vManage (DR em standby, COMPUTE_AND_DATA)
- 1 ou mais vBond
- 1 ou mais vSmart

Etapas:

1. Ativar todas as instâncias usando as Etapas Comuns
2. Verificações prévias
3. Configurar a interface do usuário, os certificados e os controladores integrados do vManage
4. Configuração de DR de nó único
5. Backup/restauração de config-db
6. Pós-cheques

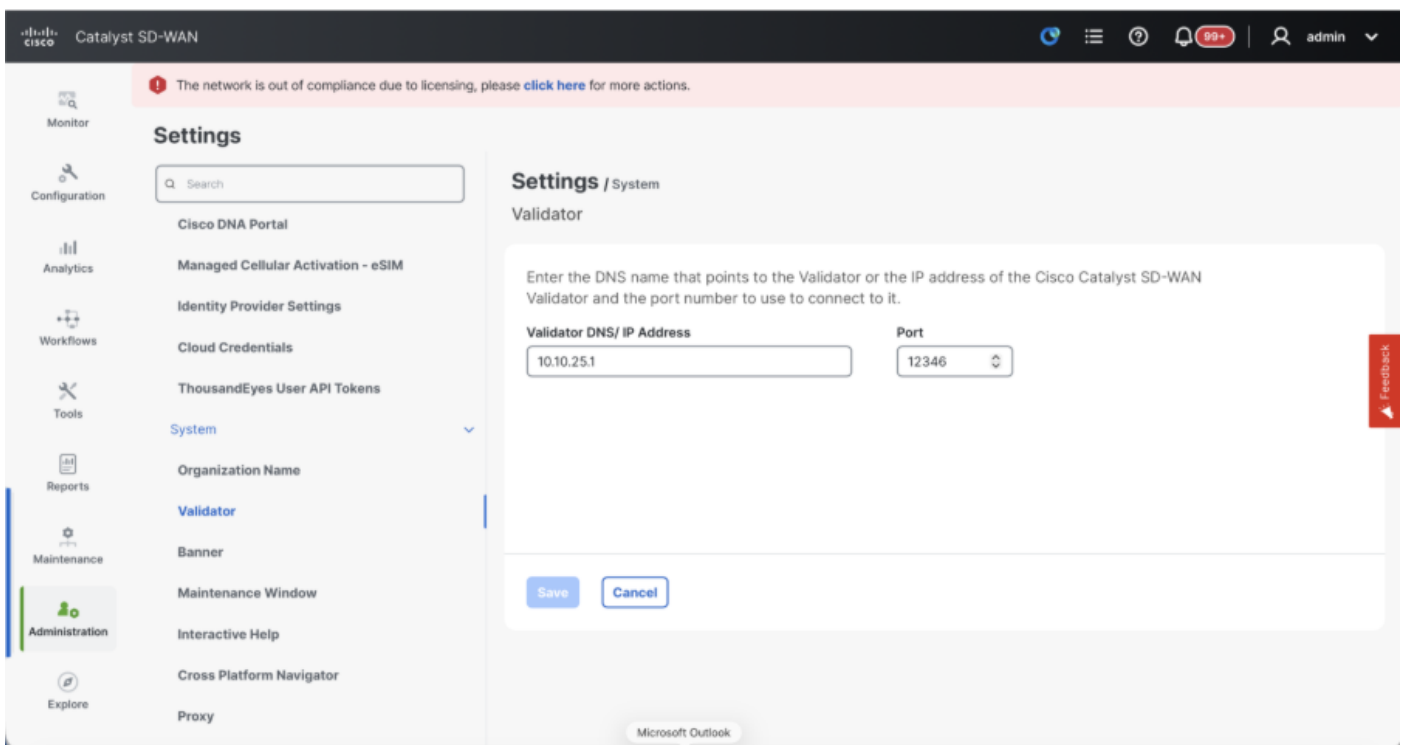
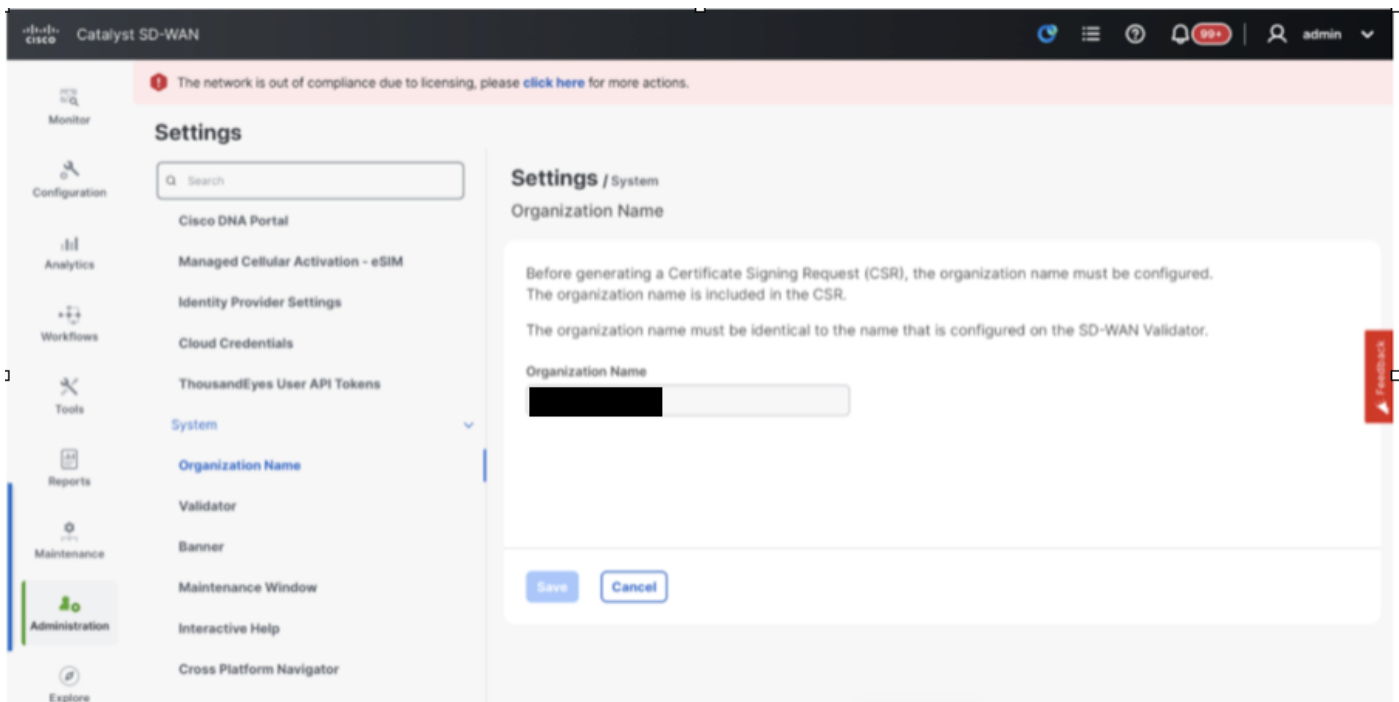
Passo 1: Pré-verificações

- Certifique-se de que o número de instâncias ativas do Cisco SD-WAN Manager seja idêntico ao número de instâncias recém-instaladas do Cisco SD-WAN Manager.
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager executem a mesma versão de software.
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager possam acessar o endereço IP de gerenciamento do Cisco SD-WAN Validator.
- Verifique se os certificados foram instalados nas instâncias recém-instaladas do Cisco SD-WAN Manager.
- Certifique-se de que os relógios em todos os dispositivos Cisco Catalyst SD-WAN, incluindo as instâncias recém-instaladas do Cisco SD-WAN Manager, estejam sincronizados.
- Verifique se um novo conjunto de IPs do sistema e IDs do local está configurado nas instâncias do Cisco SD-WAN Manager recém-instalado, juntamente com a mesma configuração básica do cluster ativo.

Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage

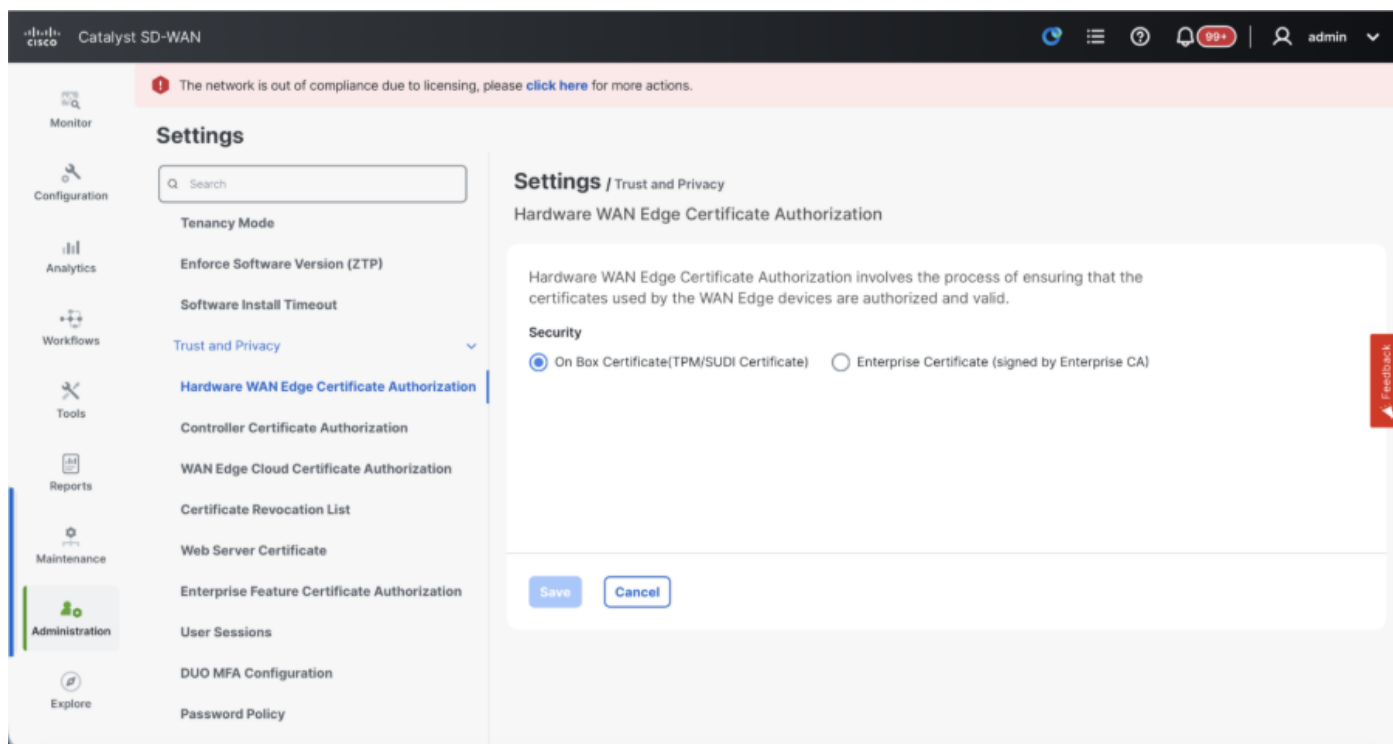
Atualizar as configurações na interface do usuário do vManage

- Depois que as configurações na Etapa 1 forem adicionadas à CLI de todos os controladores, poderemos acessar a webUI do vManage, usando o URL `https://<vmanage-ip>` em seu navegador. Use o endereço IP VPN 512 dos respectivos nós do vManage. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue até Administration > Settings e conclua estas etapas.
- Configure o nome da organização e o endereço IP/URL do validador/vBond. Configure o mesmo valor da CLI do nó do vManage.
- No vManage 20.15/20.18, essas configurações estão disponíveis na seção Sistema.



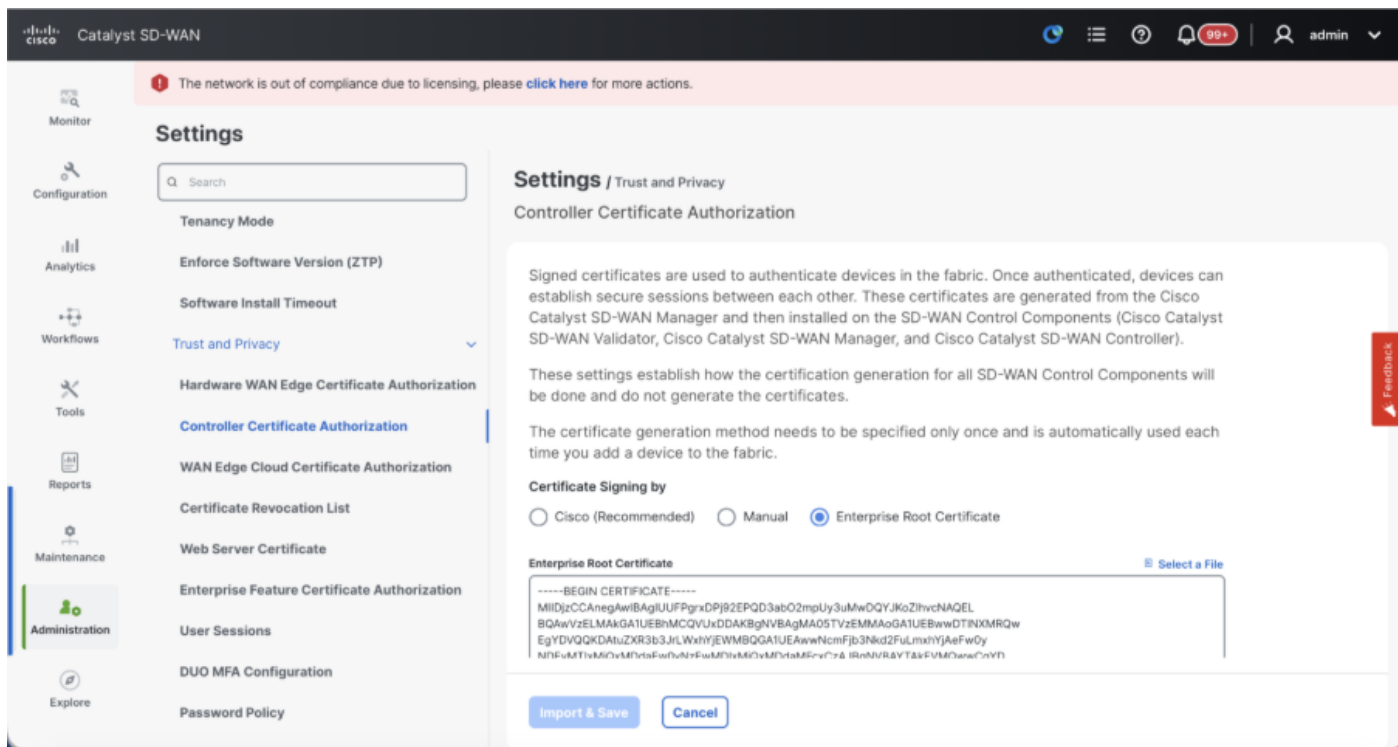
- Verifique as configurações da CA (Certificate Authorization, Autorização de Certificado), que decide a autoridade de certificação usada para assinar os certificados. Podemos ver 3 opções aqui:
1. Autorização do certificado de borda da WAN de hardware - decide a CA para os roteadores de borda da SD-WAN de hardware.
 - On Box Certificate (TPM/SUDI Certificate) - Com essa opção, o certificado pré-instalado no hardware do roteador é usado para estabelecer as conexões de controle (conexões TLS/DTLS)
 - Certificado corporativo (assinado pela autoridade de certificação corporativa) - Com essa opção, os roteadores usam certificados assinados pela autoridade de certificação

corporativa da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



2. Controller Certificate Authorization - Decide a CA para controladores SD-WAN.

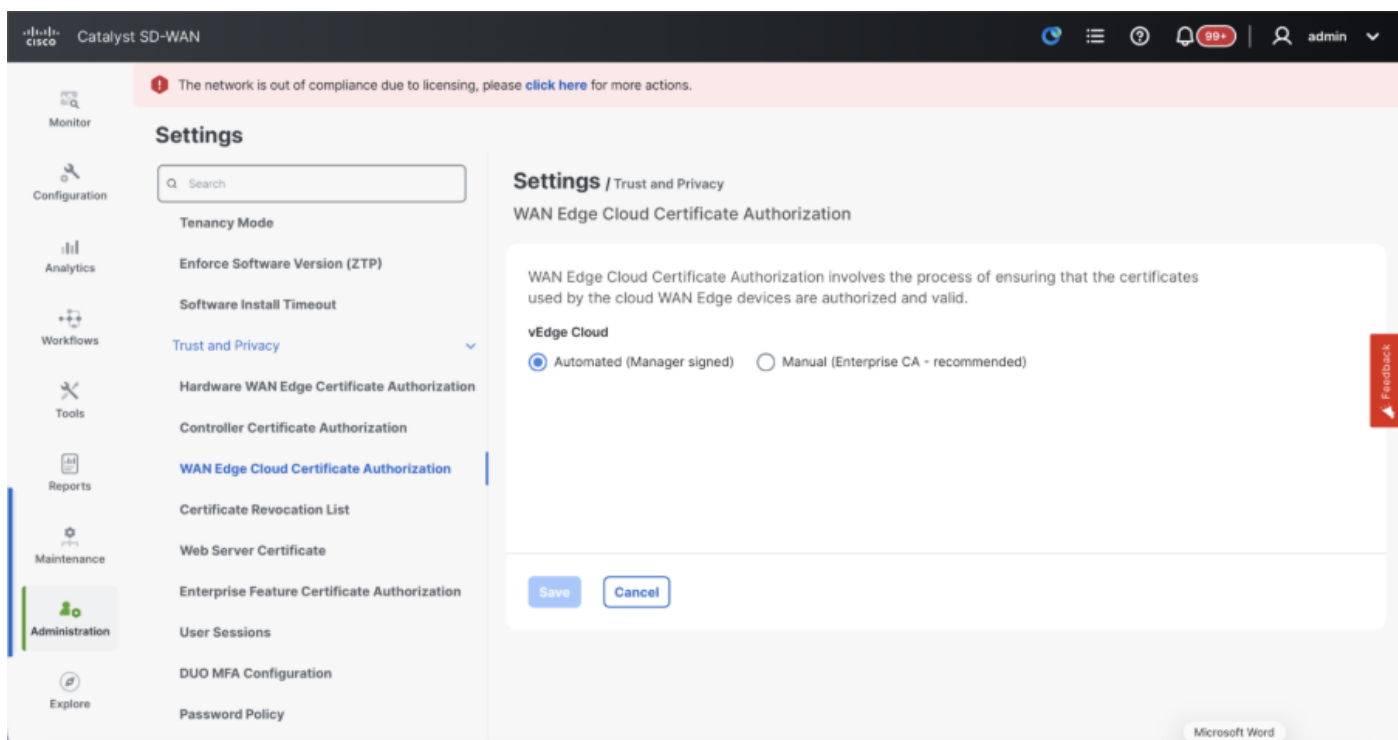
- Cisco (Recomendado) - Os controladores usam os certificados assinados pelo Cisco PKI. O vManage entra em contato automaticamente com o portal PNP usando as credenciais de Smart Account configuradas no vManage e obtém o certificado assinado e é instalado no controlador.
- Manual - Os controladores usam os certificados assinados pela PKI da Cisco. Assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Certificado raiz empresarial - com esta opção, os roteadores usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



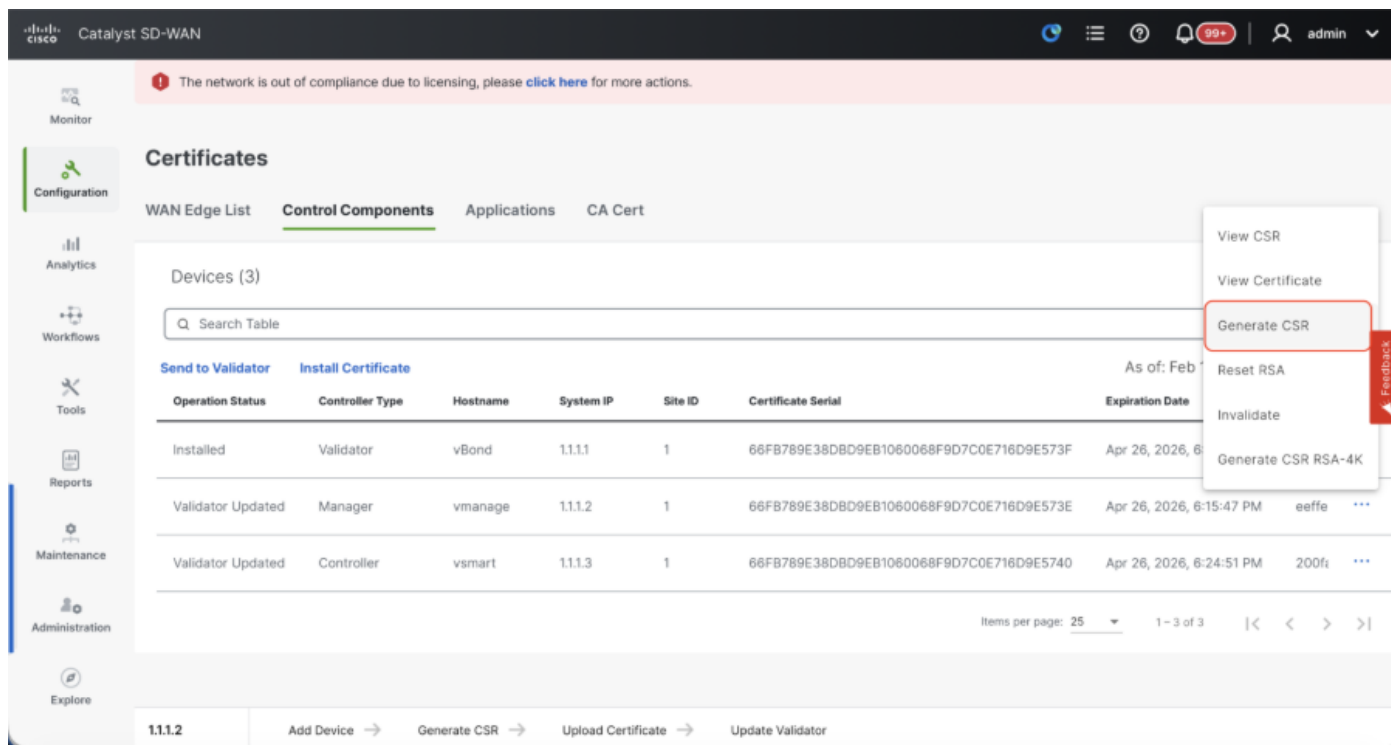
3. Autorização de certificado de nuvem de borda de WAN - decide a CA para roteadores de borda de SD-WAN virtuais (CSR1000v, C8000v, nuvem vEdge)

- Automatizado (vManage assinado) - O vManage assina automaticamente o CSR para os roteadores de borda virtual e instala o certificado no roteador.
- Manual (CA empresarial - recomendado) - Os roteadores virtuais usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.

Caso estejamos usando nossa própria CA, autoridade de certificação empresarial, escolha Empresa.



- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores
- Clique em ... para Gerente/vManage e clique em Gerar CSR.



- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.

Integração do vBond/Validator e vSmart/Controller ao vManage

Navegue para Configuration > Devices > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Onboarding vBond/Validador

- Clique em Add vBond no caso de 20.12 vManage ou Adicionar validador no caso de 20.15/20.18 vManage. Um pop-up é aberto, insira o O IP de transporte VPN 0 de vBond que pode ser acessado a partir do vManage.
- Verifique a acessibilidade usando ping se permitido a partir do CLI de vManage to vBond IP.

- Insira as credenciais de usuário do vBond.



Observação: Precisamos usar credenciais de administrador de VoBond ou uma parte do usuário de netadmingroup. Você pode verificar isso no CLI do vBond. Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vBond



Note: Se o vBond estiver por trás de um dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vBond está traduzido para um IP público. Se o IP da interface VPN 0 não estiver acessível no vManage, use o endereço IP público da interface VPN 0 nesta etapa

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. On the left, a sidebar contains navigation options: Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main area is titled 'Devices' and has three tabs: 'WAN Edge List', 'Control Components', and 'Unclaimed WAN Edges'. The 'Control Components' tab is active, showing a table with 3 components. A red box highlights the 'Add Validator' button. To the right, the 'Add Validator' dialog box is open, showing fields for 'Validator Management IP Address', 'Username', 'Password', and a 'Generate CSR' dropdown menu set to 'No'. A 'Feedback' button is visible on the right side of the dialog. At the bottom of the dialog are 'Cancel' and 'Add' buttons.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sync
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se a Cisco (recomendada) for escolhida, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, será instalado no vBond automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver várias vBonds, repita as mesmas etapas.

vSmart/controlador integrado

- Clique em Add vSmart no caso do vManage 20.12 ou Add Controller no caso do vManage 20.15/20.18.
- Um pop-up é aberto, insira o IP de transporte VPN 0 do vSmart que pode ser acessado no vManage.
- Verifique a acessibilidade usando ping se permitido do CLI do vManage para o vSmart IP.
- Insira as credenciais de usuário do vSmart. Observe que precisamos usar credenciais de administrador do vSmart ou uma parte do usuário do grupo netadmin.
- Você pode verificar isso na CLI do vSmart.
- Defina o protocolo como TLS, se pretendemos usar TLS para roteadores para estabelecer conexões de controle com vSmart. Essa configuração também precisa ser configurada na CLI dos nós vSmarts e vManage.
- Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vSmart.



Observação: se o vSmart estiver por trás do dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vSmart está convertido em um IP público e se o IP da interface VPN 0 não pode ser acessado do vManage, use o endereço IP público do IP da interface VPN 0 nesta etapa.

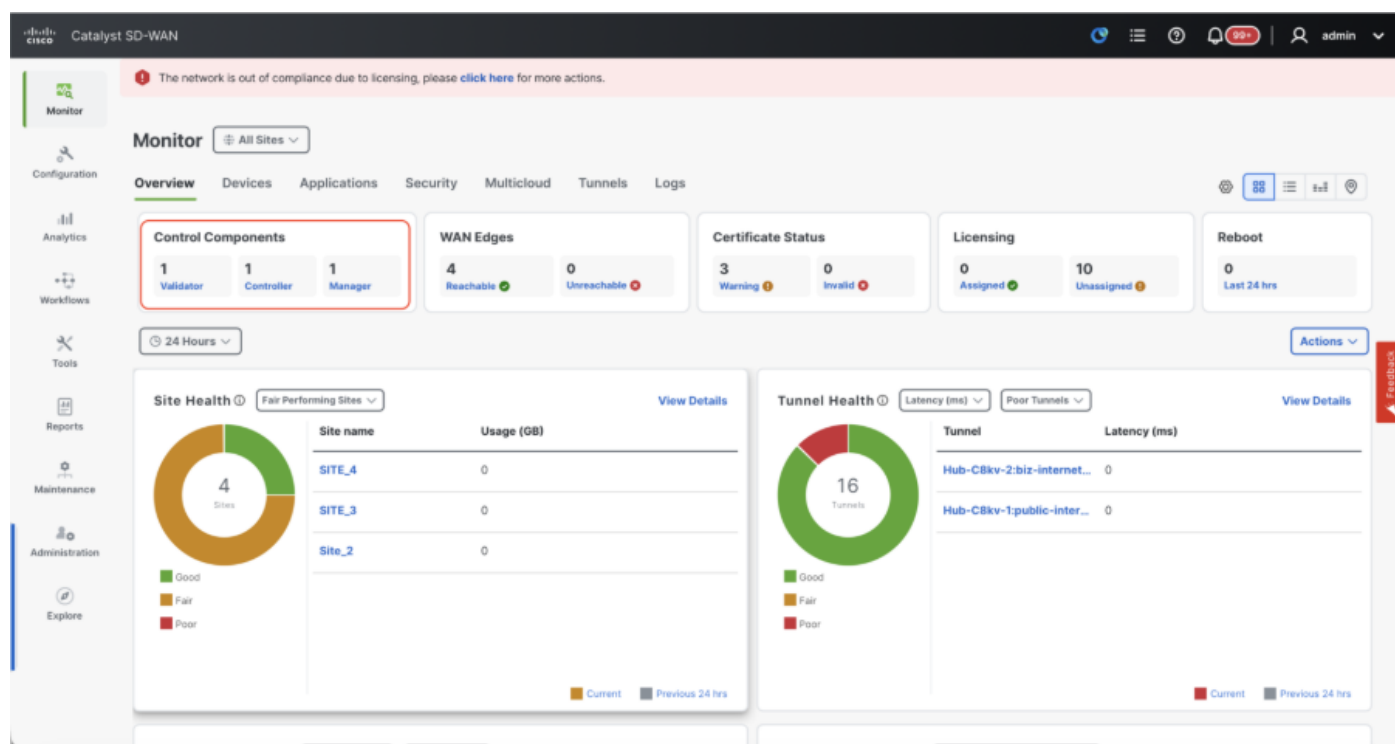
The screenshot shows the Cisco Catalyst SD-WAN vManage interface. The main panel displays the 'Devices' section with a table of 'Control Components (3)'. The table has columns for Controller Type, Site Name, Hostname, Config Locked, Managed By, Device Status, and Sy. The table lists three components: a Validator (SITE_1, vBond, No, Unmanaged, In Sync), a Manager (SITE_1, vmanage, No, Unmanaged, In Sync), and a Controller (SITE_1, vsmart, Yes, Template vSmart-template, In Sync). On the right, the 'Add Controller' modal is open, showing fields for Controller Management IP Address, Username, Password, Protocol (set to DTLS), Port, and Generate CSR (set to No). The modal has 'Cancel' and 'Add' buttons at the bottom right.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sy
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vSmart automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. O mesmo procedimento será aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- Se houver vários vSmarts, repita as mesmas etapas.

Verificação

Após concluir todas as etapas, verifique se todos os componentes de controle estão acessíveis em Monitor>Dashboard



- Clique nos respectivos componentes de controle e confirme se todos estão acessíveis.
- Navegue até Monitor > Devices e confirme se todos os componentes de controle estão acessíveis.

Cisco

Catalyst SD-WAN

Monitor

Configuration

Analytics

Workflows

Tools

Reports

Maintenance

Administration

Monitor

All Sites

Overview

Devices

Applications

Security

Multicloud

Tunnels

Logs

Devices

Certificates

Licensing

Device Group

All

Devices (7)

Export

Search Table

As of: Feb 18, 2026 11:28 AM

Refresh

Hostname	Device Model	Site Name	System IP	Health	Reachability	Control	BFD	TLOC	Up Since	CPU Load	Memory utilization	Act
vBond	Validator	SITE_1	1.1.1.1			14 / 14	N/A	- / -	Jan 13, 2026 11:32 AM			...
vmanage	Manager	SITE_1	1.1.1.2			6 / 6	N/A	8 / 8	Feb 06, 2026 10:07 AM			...
vsmart	Controller	SITE_1	1.1.1.3			7 / 7	N/A	2 / 2	Jan 13, 2026 11:33 AM			...

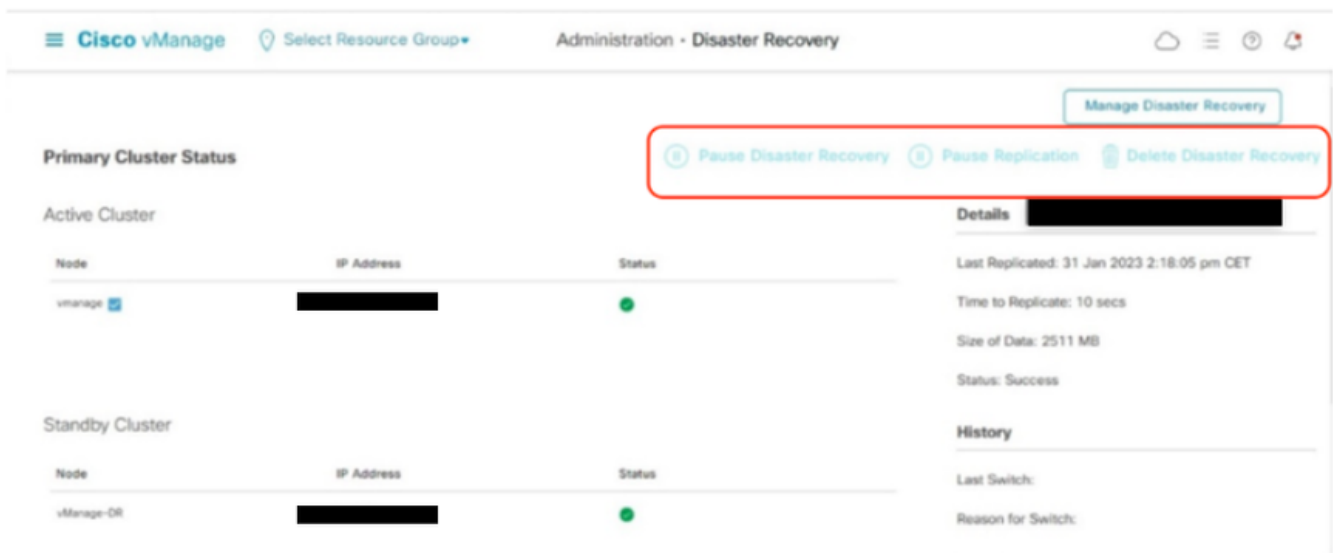
Passo 3: Backup/Restauração do Config-db

Coletar backup e restauração do banco de dados de configuração do vManage em outro nó do vManage

Note: Ao coletar o backup do banco de dados de configuração do nó vManage existente que tem a recuperação de desastres ativada, certifique-se de que ele seja coletado após a recuperação de desastres nesse nó ser pausada e excluída.

Confirme se não há replicação de recuperação de desastres em andamento. Navegue até Administração > Recuperação de desastres e verifique o status Sucesso e não em um estado transitório, como Importação pendente, Exportação pendente ou Download pendente. Se o status não for sucesso, entre em contato com o Cisco TAC e certifique-se de que a replicação seja bem-sucedida antes de continuar a pausar a recuperação de desastres.

Primeiro, pause a recuperação de desastres e certifique-se de que a tarefa esteja concluída. Em seguida, exclua a recuperação de desastre e confirme se a tarefa foi concluída.



Entre em contato com o Cisco TAC para garantir que a recuperação de desastres seja limpa com êxito.

Coletar backup do BD de configuração:

- Na estrutura SD-WAN atualmente em uso, é possível gerar backup de configuração-db nas configurações de cluster autônomas do vManage e do vManage.
- No caso do vManage autônomo, o próprio vManage é o líder do banco de dados de configuração.

Confirme se o configuration-db está sendo executado no nó vManage.

Você pode verificar o mesmo usando o comando `request nms configuration-db statusonvManageCLI`. A saída é a mostrada

```
vmanage# request nms configuration-db status
NMS configuration database
  Enabled: true
  Status: running PID:32632 for 1066085s
  Native metrics status: ENABLED
  Server-load metrics status: ENABLED
vmanage#
```

Use esse comando para coletar o backup configuration-db do nó vManage líder configuration-db identificado.

```
request nms configuration-db backup path /opt/data/backup/
```

A saída esperada é a seguinte:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Anote as credenciais do configuration-db se ele tiver sido atualizado.
- Se você não souber as credenciais do configuration-db, entre em contato com o TAC para recuperar as credenciais do configuration-db dos nós vManage existentes.
- As credenciais padrão do configuration-db são nome de usuário: neo4j e senha: senha

Restaurar backup do banco de dados de configuração para outro nó do vManage

Copie o backup do configuration-db para o diretório /home/admin/ do vManage usando SCP.

Exemplo de saída do comando scp:

```
XXXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1

(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Para restaurar o backup do configuration-db, primeiro precisamos configurar as credenciais do configuration-db. Se suas credenciais de configuração-db forem default (neo4j/password), podemos pular esta etapa.

Para configurar as credenciais do configuration-db, use o comando request nms configuration-db update-admin-user. Use o nome de usuário e a senha de sua escolha.

Observe que o servidor de aplicativos do vManage é reiniciado. Devido ao qual a interface do usuário do vManage fica inacessível por um curto período.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
```

```
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operation)
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Post que podemos continuar para restaurar o backup do configuration-db:

Podemos usar o comando `request nms configuration-db restore path /home/admin/< >` para restaurar o configuration-db para o novo vManage:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Resetting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Depois que o configuration-db for restaurado, verifique se a interface do usuário do vManage está acessível. Aguarde cerca de 5 minutos e tente acessar a interface do usuário.

Depois de fazer login na interface do usuário com êxito, verifique se a lista de roteadores de borda, o modelo, as políticas e todas as configurações presentes na interface do usuário do vManage anterior ou existente estão refletidas na nova interface do usuário do vManage.

Passo 4: Configuração de DR de nó único

Consulte a Etapa 2: Pré-verificações na Combinação 2: vManage autônomo + DR de nó único e certifique-se de que cumprimos todos os requisitos antes de continuar a habilitar a recuperação de desastres.

DR de nó único

Pré-requisitos

- Certifique-se de que o nó primário e o secundário estejam acessíveis por HTTPS em uma VPN de transporte (VPN 0).
- Verifique se o nó primário e o nó secundário do Cisco vManage estão executando a mesma versão do Cisco vManage.

Interface de cluster fora de banda na VPN 0

1. Para cada instância do vManage em um cluster, é necessária uma terceira interface (link de cluster) além das interfaces usadas para VPN 0 (transporte) e VPN 512 (gerenciamento).
 2. Essa interface é usada para comunicação e sincronização entre os servidores vManage no cluster.
 3. Essa interface deve ter pelo menos 1 Gbps e uma latência de 4 ms ou menos. Recomenda-se uma interface de 10 Gbps.
 4. Ambos os nós do vManage devem ser capazes de alcançar um ao outro por meio dessa interface: seja um segmento da camada 2 ou através do roteamento da camada 3.
- Verifique se todos os serviços (servidor de aplicativos, configuração-db, servidor de mensagens, servidor de coordenação e estatística-db) estão habilitados em ambos os nós do Cisco vManage.
 - Distribua todos os controladores, incluindo os Cisco vBond Orchestrators, em data centers primários e secundários. Verifique se esses controladores podem ser acessados pelos nós do Cisco vManage que estão distribuídos nesses data centers. Os controladores se conectam apenas ao nó principal do Cisco vManage.
 - Certifique-se de que nenhuma outra operação esteja em andamento no nó ativo (principal) e no nó standby (secundário) do Cisco vManage. Por exemplo, certifique-se de que nenhum servidor esteja em processo de atualização ou que nenhum modelo esteja em processo de anexação de modelos a dispositivos.
 - Desative o servidor proxy HTTP/HTTPS do Cisco vManage se ele estiver ativado. Se você não desativar o servidor proxy, o Cisco vManage tentará estabelecer comunicação de recuperação de desastres por meio do endereço IP do proxy, mesmo que os endereços IP do cluster fora de banda do Cisco vManage sejam diretamente acessíveis. Você pode reativar o servidor proxy HTTP/HTTPS do Cisco vManage após a conclusão do registro de recuperação de desastres.
 - Antes de iniciar o processo de registro de recuperação de desastres, vá para a janela Tools → Rediscover Network (Ferramentas de redescoberta da rede) no nó principal do Cisco vManage e redescubra os Cisco vBond Orchestrators.

Configuração

Defina as configurações CLI de todos os nós do vManage que estão atuando como nó de

recuperação de desastres

A configuração mínima básica do vManage antes do registro do Disaster Recovery é como mostrado

```
config t
system
host-name
```

```
system-ip
```

```
site-id
```

```
organization-name
```

```
vbond
```

```
commit
```



Observação: se estamos usando URL como endereço vBond, certifique-se de configurar os endereços IP do servidor DNS na configuração VPN 0 ou de garantir que eles possam ser resolvidos.

Essas configurações são necessárias para ativar a interface de transporte usada para estabelecer conexões de controle com os roteadores e o restante dos controladores

```
config t
vpn 0
dns
```

```
        primary
dns
```

```
        secondary
interface eth1
ip address
```

```
tunnel-interface
allow-service all
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service stun
allow-service https
!
no shutdown
!
ip route 0.0.0.0/0
```

```
commit
```

Configure também a interface de gerenciamento VPN 512 para permitir o acesso de gerenciamento fora de banda ao controlador.

```
Conf t
vpn 512
interface eth0
ip address
```

```
no shutdown
!  
ip route 0.0.0.0/0
```

```
!  
commit
```

Configure a interface de serviço no DR vManage

Configure a interface de serviço no nó do vManage. Essa interface é usada para comunicação DR,

```
conf t  
interface eth2  
ip address
```

```
no shutdown  
commit
```

Certifique-se de que a mesma sub-rede IP seja usada para a interface de serviço no vManage primário e no DR vManage

Atualizar as configurações na interface do usuário do vManage

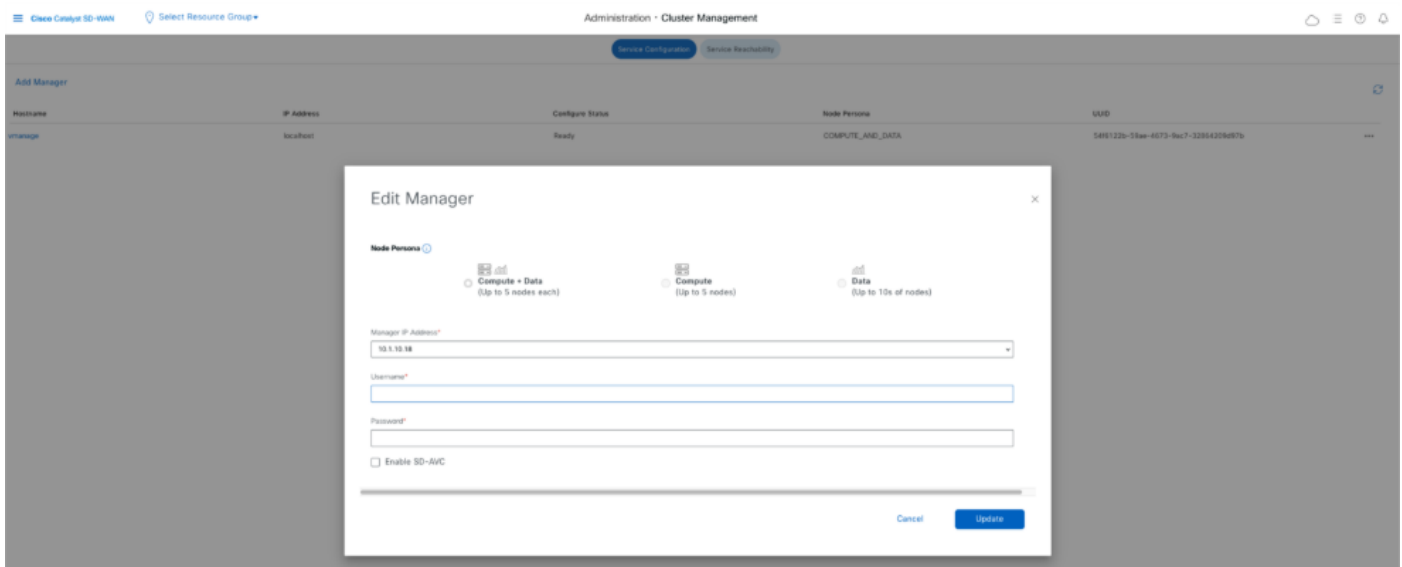
- Quando as configurações forem adicionadas à CLI de todos os controladores, poderemos acessar a webUI do vManage, usando a URL <https://<vmanage-ip>> em seu navegador. Use o endereço IP VPN 512 dos respectivos nós do vManage. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue até Administration > Settings e conclua estas etapas.
- Configure o nome da organização. Configure o mesmo valor da CLI do nó do vManage.
- No vManage 20.15/20.18, essas configurações estão disponíveis na seção Sistema.

Instalação do Certificado no DR vManage

Continue com os passos dados na seção Combinação 2: vManage independente + DR de nó único Etapa 3: Configure a interface do usuário do vManage, certificados e controladores integrados para instalar o certificado no vManage de recuperação de desastres.

Adicionando a configuração de recuperação de desastres

- Para isso, vá para o vManage principal.
- Navegue até Administration → Cluster Management e indique o endereço IP da interface fora de banda depois de clicar nos três pontos no lado direito da entrada do vManage e inclua o nome de usuário e a senha. É recomendável criar um usuário local separado, por exemplo, dradmin no vmanage principal e DR para essa configuração.



- O VManage é reinicializado após essa alteração.
- Depois que o vManage principal for ativado, navegue até Administração → Recuperação de desastres. Clique em "Manage Disaster Recovery" (Gerenciar a recuperação de desastres).
- Na janela pop-up, preencha os detalhes do vManage principal e secundário.
- Os endereços IP a serem indicados são os endereços IP das interfaces de cluster fora de banda (eth2).
- As credenciais devem ser as de um usuário do netadmin (dradmin) e não devem ser alteradas após a configuração do DR. Uma credencial de usuário local do vManage separada para recuperação de desastres pode ser usada. Precisamos verificar se o usuário local do vManage faz parte do grupo netadmin. Até mesmo as credenciais de administrador podem ser usadas aqui.
- Depois de preenchido, clique em "Avançar".
- Preencha os detalhes dos controladores vBond.
- Os controladores vBond devem estar acessíveis no endereço IP especificado via Netconf.
- As credenciais devem ser as de um usuário do netadmin (dradmin) e não devem ser alteradas após a configuração do DR.

- Para isso, recomenda-se que o vBond tenha esse usuário dradmin configurado localmente ou você pode usar o usuário admin para adicionar o vBond.

Manage Disaster Recovery ×

Connectivity Info

vBond Info

Recovery Mode

Replication Schedule

vBond Information

IP

User Name

Password

dr-user

.....

IP

User Name

Password

dr-user

.....

Back

Next

Cancel

- Depois de preenchido, clique em "Avançar".
- No Modo de Recuperação, escolha "Manual". Clique em "Avançar".

Manage Disaster Recovery ×

Connectivity Info

vBond Info

Recovery Mode

Replication Schedule

Select Recovery Mode

Manual

Automation

Back

Next

Cancel

Na Programação de Replicação, defina a opção 'Intervalo de Replicação'. A cada intervalo de replicação, os dados são replicados do principal vManage para o vManage secundário. O valor mínimo configurável é de 15 minutos.

Manage Disaster Recovery



Progress bar: Connectivity Info (green), vBond Info (green), Recovery Mode (green), Replication Schedule (blue)

Start Time: 3:00 AM

Replication Interval: 15 mins

Buttons: Back, Save, Cancel

- Defina o valor e clique em "Salvar".
- O registro do DR começa agora. Clique no botão atualizar para atualizar manualmente o estado e os logs de andamento. Esse processo pode levar de 20 a 30 minutos.

Browser address bar: https://vmanage-1/#/app/device/status?activity=disaster_recovery_registration&pid=3c5c151b-8875-49b9-a34b-eaf78c71f566

Cisco vManage | Select Resource Group

Disaster Recovery Registration | Initiated By: admin | From: 10.61.76.160

Total Task: 1 | In Progress : 1

Search bar

Total Rows: 1 [Refresh] [Settings]

Status	Device IP	Message	Start Time
In progress	default	Data Centers Registration	31 Jan 2023 2:13:00 PM CET

- Observe que a GUI do vManage é reiniciada durante esse processo.
- Uma vez concluído, o status Success deve ser visto.

Cisco vManage

Select Resource Group

Disaster Recovery Registration

Initiated By: admin From: 10.61.76.160

Total Task: 1 | Success : 1

Search

Total Rows: 1

Status	Device IP	Message	Start Time
Success	default	Data Centers Registration	31 Jan 2023 2:13:00 PM CET

Verificar

Navegue até Administração → Recuperação de desastres para ver o status da recuperação de desastres e quando os dados foram replicados pela última vez.

Passo 5: Reautenticação de controladores e invalidação de controladores antigos

Depois que o configuration-db for restaurado, precisamos autenticar novamente todos os novos controladores (vmanage/vsmart/vbond) na malha



Observação: na produção real, se o IP da interface usado para reautenticar for o IP da interface do túnel, será necessário garantir que o serviço NETCONF seja permitido na interface do túnel do vManage, vSmart e vBond e também nos firewalls ao longo do caminho. A porta de firewall a ser aberta é a porta TCP 830 como regra bidirecional do cluster DR para todos os vBonds e vSmarts .

Na interface de usuário do vmanage, clique em Configuration > Devices > Controllers

- Clique nos três pontos próximos a cada controlador e clique em Editar

The screenshot shows the Cisco Catalyst SD-WAN Configuration - Devices page. The 'WAN Edge List' tab is selected, displaying a table of 5 controllers. The 'Edit' sidebar is open on the right, showing fields for IP Address, Username, and Password.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	System-ip	Draft Mode	Certificate Status	Policy Name	Policy Version
vbond	SITE_300	vedge	No	Unmanaged	In Sync	3.3.3.3	Disabled	Installed	-	-
vmanage	SITE_300	vmanage1-20121	No	Unmanaged	In Sync	1.1.1.1	Disabled	Installed	-	-
vmanage	SITE_300	vmanage2-20121	No	Unmanaged	In Sync	1.1.1.2	Disabled	Installed	-	-
vmanage	SITE_300	vmanage3-20121	No	Unmanaged	In Sync	1.1.1.3	Disabled	Installed	-	-
vsmart	SITE_300	vsmart	No	Unmanaged	In Sync	2.2.2.2	Disabled	Installed	-	-

- Substitua ip-address (system-ip do controlador) pelo endereço ip transport vpn 0(tunnel interface) .Insira o nome de usuário e a senha e clique em save
- Faça o mesmo para todos os novos controladores na malha

Sincronizar a cadeia de certificados raiz

Depois que todos os controladores estiverem integrados, conclua esta etapa:

Em qualquer servidor Cisco SD-WAN Manager no cluster recém-ativo, execute estas ações:

Digite este comando para sincronizar o certificado raiz com todos os dispositivos Cisco Catalyst SD-WAN no cluster recém-ativo:

<https://vmanage-url/dataservice/system/device/sync/rootcertchain>

Digite este comando para sincronizar o UUID do Cisco SD-WAN Manager com o Cisco SD-WAN Validator:

<https://vmanage-url/dataservice/certificate/syncvbond>

Depois que a estrutura for restaurada e as sessões de controle e bfd estiverem ativas para todas as bordas e controladores na estrutura, precisamos invalidar os controladores antigos (vmanage/vsmart/vbond) da interface do usuário

- Na interface do usuário do vmanage, clique em Configuration > Devices > Certificates
- Clique em Controladores
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em invalidar
- Clique em enviar para vbond
- Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em Excluir

Passo 6: Pós-cheques



Note: Continue com a seção Post Checks mostrada aqui, que é comum a todas as combinações de implantação.

Combinação 3: vManage Cluster + Sem DR

Instâncias necessárias:

- 3 vManage (cluster de 3 nós, todos COMPUTE_AND_DATA) ou 6 vManage (3 COMPUTE_AND_DATA + 3 DATA)
- 1 ou mais vBond
- 1 ou mais vSmart

Etapas:

1. Ativar todas as instâncias usando as Etapas Comuns
2. Verificações prévias
3. Configurar a interface do usuário, os certificados e os controladores integrados do vManage
4. Construir cluster vManage
5. Backup/restauração de config-db
6. Pós-cheques

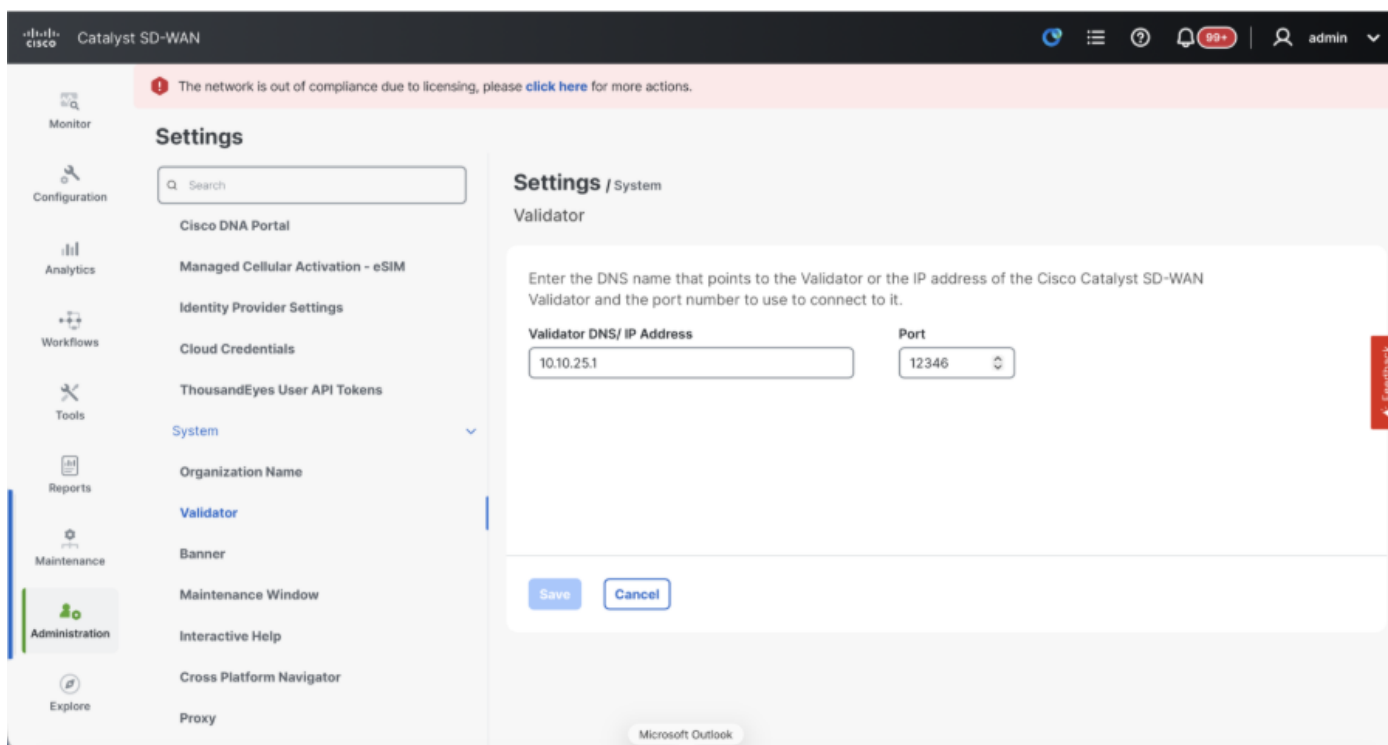
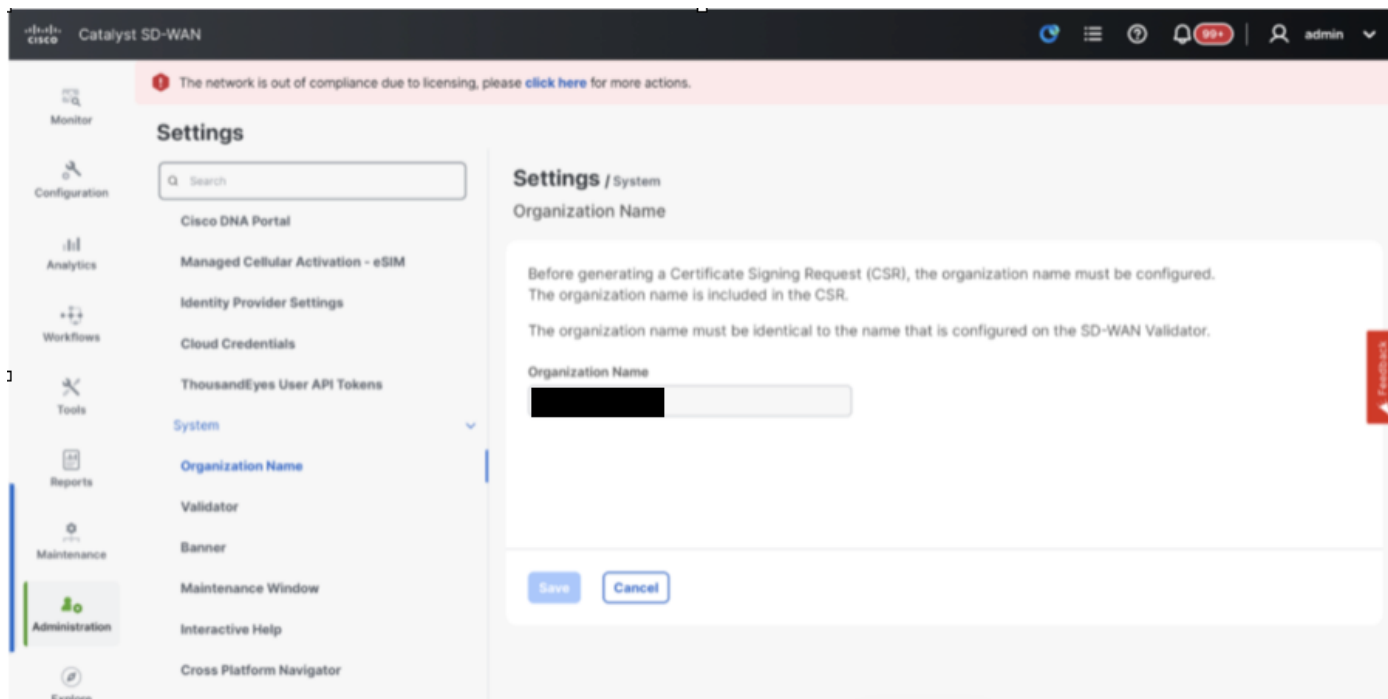
Passo 1: Pré-verificações

- Certifique-se de que o número de instâncias ativas do Cisco SD-WAN Manager seja idêntico ao número de instâncias recém-instaladas do Cisco SD-WAN Manager.
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager executem a mesma versão de software.
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager possam acessar o endereço IP de gerenciamento do Cisco SD-WAN Validator.
- Verifique se os certificados foram instalados nas instâncias recém-instaladas do Cisco SD-WAN Manager.
- Certifique-se de que os relógios em todos os dispositivos Cisco Catalyst SD-WAN, incluindo as instâncias recém-instaladas do Cisco SD-WAN Manager, estejam sincronizados.
- Verifique se um novo conjunto de IPs do sistema e IDs do local está configurado nas instâncias do Cisco SD-WAN Manager recém-instalado, juntamente com a mesma configuração básica do cluster ativo.

Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage

Atualizar as configurações na interface do usuário do vManage

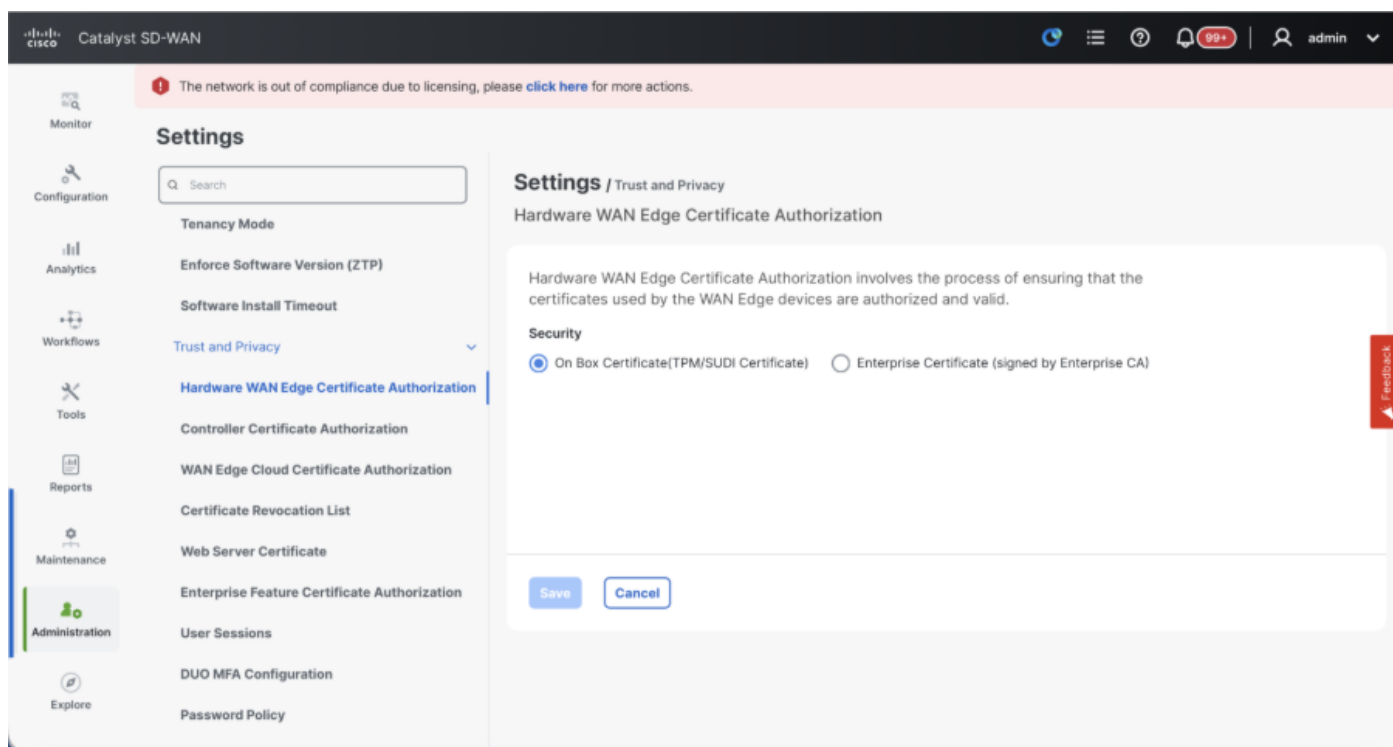
- Depois que as configurações na Etapa 1 forem adicionadas à CLI de todos os controladores, poderemos acessar a webUI do vManage, usando o URL `https://<vmanage-ip>` em seu navegador. Use o endereço IP VPN 512 dos respectivos nós do vManage. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue até Administration > Settings e conclua estas etapas.
- Configure o nome da organização e o endereço IP/URL do validador/vBond. Configure o mesmo valor da CLI do nó do vManage.
- No vManage 20.15/20.18, essas configurações estão disponíveis na seção Sistema.



- Verifique as configurações da CA (Certificate Authorization, Autorização de Certificado), que decide a autoridade de certificação usada para assinar os certificados. Podemos ver 3 opções aqui:

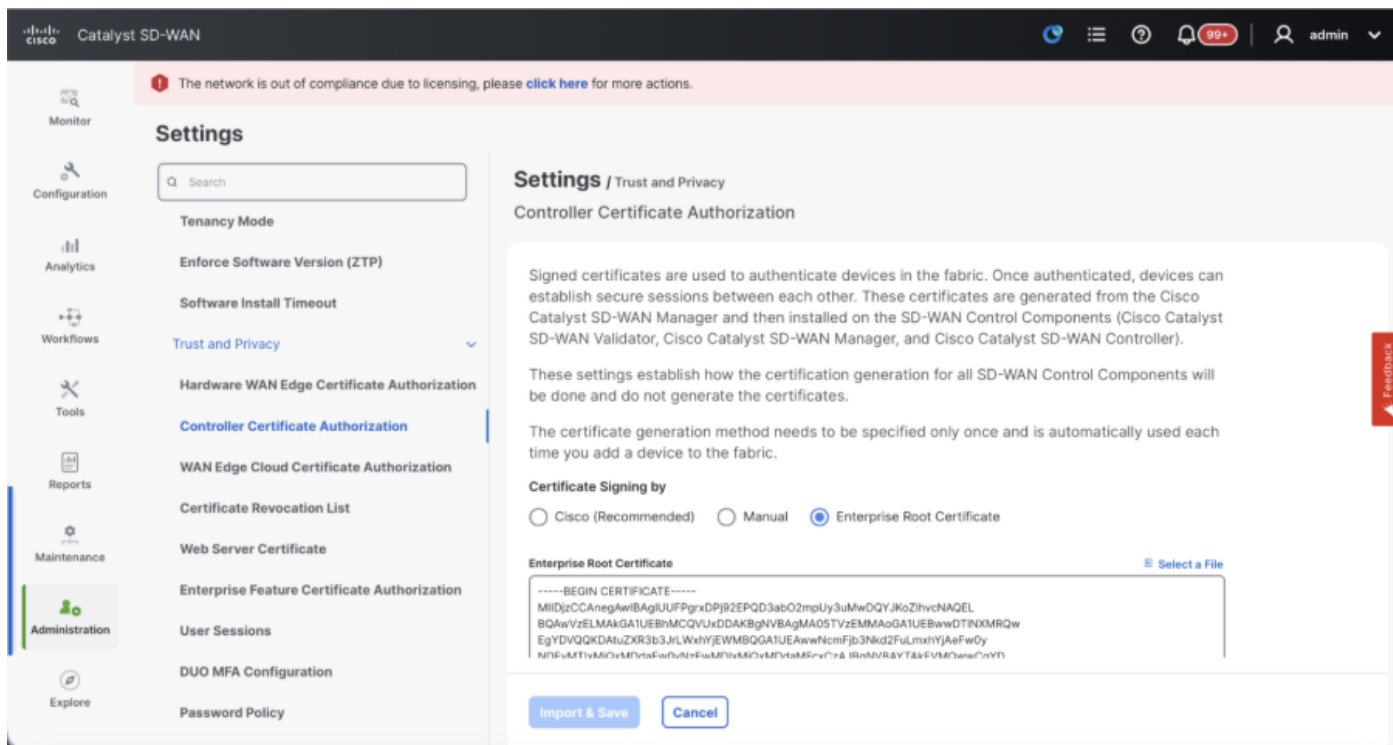
1. Autorização do certificado de borda da WAN de hardware - decide a CA para os roteadores de borda da SD-WAN de hardware.

- On Box Certificate (TPM/SUDI Certificate) - Com essa opção, o certificado pré-instalado no hardware do roteador é usado para estabelecer as conexões de controle (conexões TLS/DTLS)
- Certificado corporativo (assinado pela autoridade de certificação corporativa) - Com essa opção, os roteadores usam certificados assinados pela autoridade de certificação corporativa da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



2. Controller Certificate Authorization - Decide a CA para controladores SD-WAN.

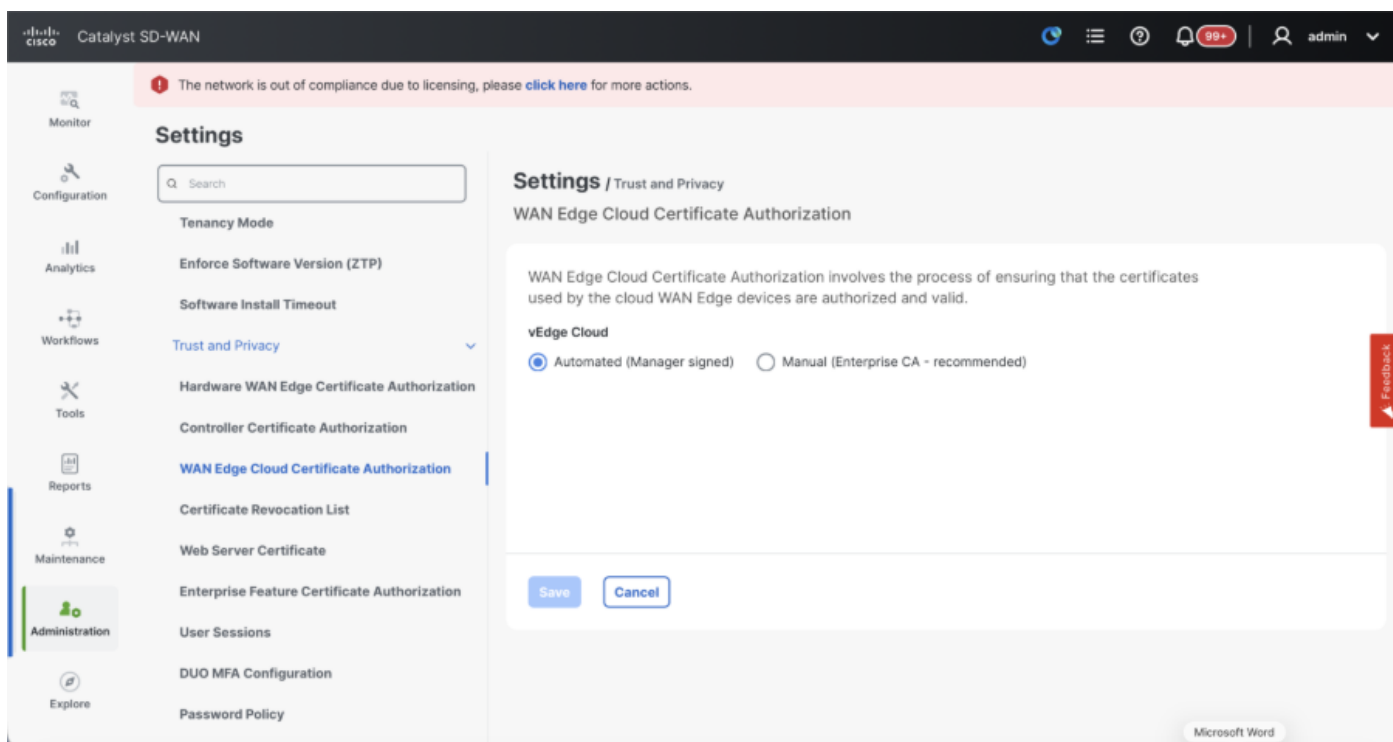
- Cisco (Recomendado) - Os controladores usam os certificados assinados pelo Cisco PKI. O vManage entra em contato automaticamente com o portal PNP usando as credenciais de Smart Account configuradas no vManage e obtém o certificado assinado e é instalado no controlador.
- Manual - Os controladores usam os certificados assinados pela PKI da Cisco. Assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Certificado raiz empresarial - com esta opção, os roteadores usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



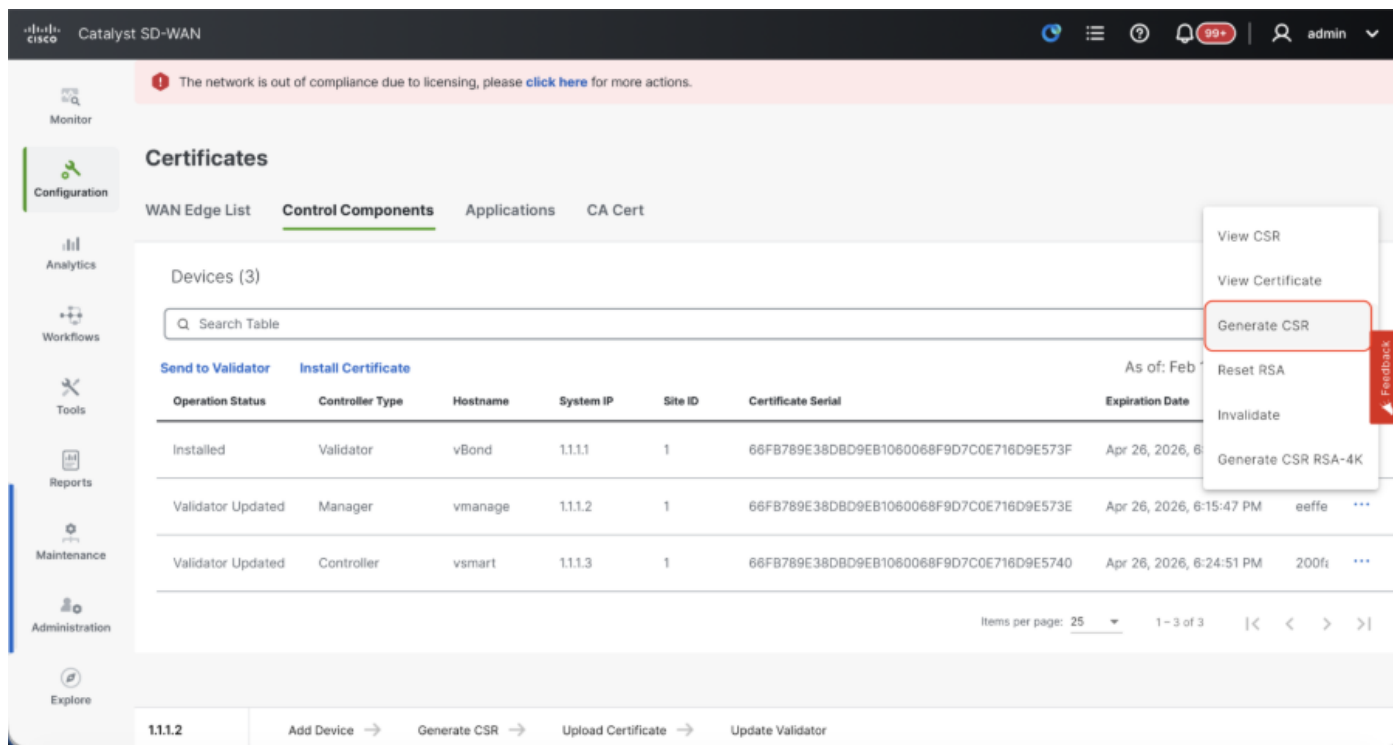
3. Autorização de certificado de nuvem de borda de WAN - decide a CA para roteadores de borda de SD-WAN virtuais (CSR1000v, C8000v, nuvem vEdge)

- Automatizado (vManage assinado) - O vManage assina automaticamente o CSR para os roteadores de borda virtual e instala o certificado no roteador.
- Manual (CA empresarial - recomendado) - Os roteadores virtuais usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.

Caso estejamos usando nossa própria CA, autoridade de certificação empresarial, escolha Empresa.



- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores
- Clique em ... para Gerente/vManage e clique em Gerar CSR.



- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.

Integração do vBond/Validator e vSmart/Controller ao vManage

Navegue para Configuration > Devices > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Onboarding vBond/Validador

- Clique em Add vBond no caso de 20.12 vManage ou Adicionar validador no caso de 20.15/20.18 vManage. Um pop-up é aberto, insira o O IP de transporte VPN 0 de vBond que pode ser acessado a partir do vManage.
- Verifique a acessibilidade usando ping se permitido a partir do CLI de vManage to vBond IP.

- Insira as credenciais de usuário do vBond.



Observação: Precisamos usar credenciais de administrador de VoBond ou uma parte do usuário de netadmingroup. Você pode verificar isso no CLI do vBond. Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vBond



Note: Se o vBond estiver por trás de um dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vBond está traduzido para um IP público. Se o IP da interface VPN 0 não estiver acessível no vManage, use o endereço IP público da interface VPN 0 nesta etapa

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. On the left is a navigation sidebar with options like Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main area is titled 'Devices' and has tabs for 'WAN Edge List', 'Control Components', and 'Unclaimed WAN Edges'. The 'Control Components' tab is active, showing a table with 3 components. A red box highlights the 'Add Validator' button. On the right, the 'Add Validator' dialog box is open, showing fields for 'Validator Management IP Address', 'Username', 'Password', and a 'Generate CSR' dropdown menu set to 'No'. There are 'Cancel' and 'Add' buttons at the bottom right of the dialog.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sync
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se a Cisco (recomendada) for escolhida, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, será instalado no vBond automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver várias vBonds, repita as mesmas etapas.

vSmart/controlador integrado

- Clique em Add vSmart no caso do vManage 20.12 ou Add Controller no caso do vManage 20.15/20.18.
- Um pop-up é aberto, insira o IP de transporte VPN 0 do vSmart que pode ser acessado no vManage.
- Verifique a acessibilidade usando ping se permitido do CLI do vManage para o vSmart IP.
- Insira as credenciais de usuário do vSmart. Observe que precisamos usar credenciais de administrador do vSmart ou uma parte do usuário do grupo netadmin.
- Você pode verificar isso na CLI do vSmart.
- Defina o protocolo como TLS, se pretendemos usar TLS para roteadores para estabelecer conexões de controle com vSmart. Essa configuração também precisa ser configurada na CLI dos nós vSmarts e vManage.
- Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vSmart.



Observação: se o vSmart estiver por trás do dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vSmart está convertido em um IP público e se o IP da interface VPN 0 não pode ser acessado do vManage, use o endereço IP público do IP da interface VPN 0 nesta etapa.

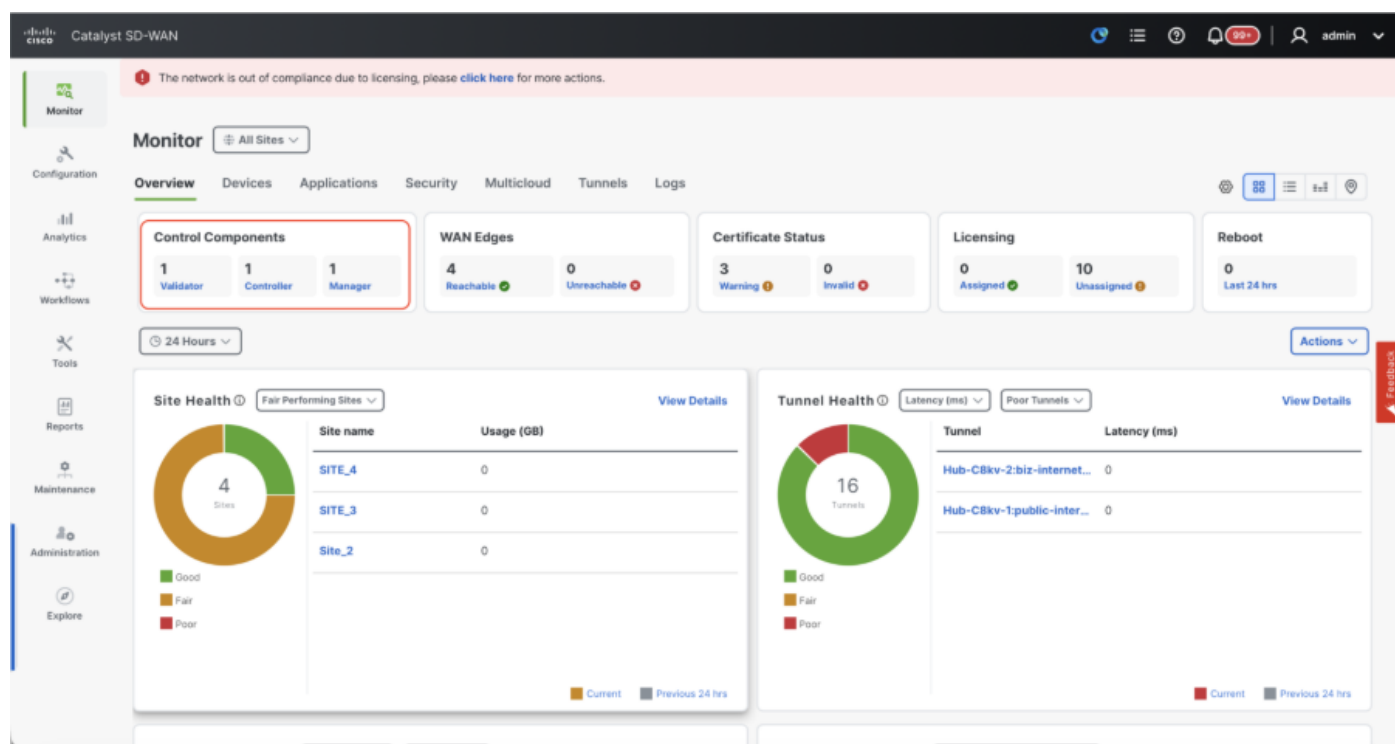
The screenshot shows the Cisco Catalyst SD-WAN vManage interface. The main panel displays the 'Devices' section with a table of 'Control Components (3)'. The table has columns for Controller Type, Site Name, Hostname, Config Locked, Managed By, Device Status, and Sy. The table lists three components: a Validator (SITE_1, vBond, No, Unmanaged, In Sync), a Manager (SITE_1, vmanage, No, Unmanaged, In Sync), and a Controller (SITE_1, vsmart, Yes, Template vSmart-template, In Sync). A modal titled 'Add Controller' is open on the right, with fields for Controller Management IP Address, Username, Password, Protocol (set to DTLS), Port, and Generate CSR (set to No). The modal has 'Cancel' and 'Add' buttons at the bottom right.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sy
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vSmart automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver vários vSmarts, repita as mesmas etapas.

Verificação

Após concluir todas as etapas, verifique se todos os componentes de controle estão acessíveis em Monitor>Dashboard



- Clique nos respectivos componentes de controle e confirme se todos estão acessíveis.
- Navegue até Monitor > Devices e confirme se todos os componentes de controle estão acessíveis.


```
organization-name
```

```
vbond
```

```
commit
```



Observação: se estamos usando URL como endereço vBond, certifique-se de configurar os endereços IP do servidor DNS na configuração VPN 0 ou de garantir que eles possam ser resolvidos.

Configurar a interface de Transporte em todos os nós do vManage

Essas configurações são necessárias para ativar a interface de transporte usada para estabelecer conexões de controle com os roteadores e o restante dos controladores.

```
config t
vpn 0
  dns
```

```
    primary
  dns
```

```
    secondary
interface eth1
  ip address
```

```
tunnel-interface
```

```
allow-service all
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service stun
allow-service https
!
no shutdown
!
ip route 0.0.0.0/0
```

commit

Configurar a interface de gerenciamento em todos os nós do vManage

Configure também a interface de gerenciamento VPN 512 para permitir o acesso de gerenciamento fora de banda ao controlador.

```
Conf t
vpn 512
interface eth0
ip address

no shutdown
!
ip route 0.0.0.0/0
```

```
!
Commit
```

Configuração opcional:

- Você pode consultar as configurações da sua controladora existente e, se a configuração listada aqui estiver presente, poderá adicionar essa configuração às novas controladoras.
- Configure o protocolo de controle como TLS somente se houver um requisito para que os roteadores estabeleçam conexões de controle seguras com os nós do vManage que usam TLS. Por padrão, todos os controladores e roteadores estabelecem uma conexão de controle usando DTLS. Essa é uma configuração opcional necessária apenas nos nós vSmart e vManage, dependendo de sua necessidade.

```
Conf t
security
  control
    protocol tls
commit
```

Configurar a interface de serviço em todos os nós do vManage

Configure a interface de serviço em todos os vManageEnodes, incluindo o vManage-1, que já foi integrado. Essa interface é usada para comunicação de cluster, o que significa comunicação entre os vManagenodes no cluster.

```
conf t
interface eth2
  ip address
```

```
no shutdown
commit
```

Certifique-se de que a mesma sub-rede IP seja usada para a interface de serviço em todos os nós no cluster vManagern.

Configurar credenciais do cluster

Podemos usar as mesmas credenciais de administrador dos modosv para configurar o cluster do gerenciamento. Caso contrário, podemos configurar uma nova credencial de usuário que faz parte de netadmin group. As configurações para configurar a credencial do novo usuário são as mostradas

```
conf t
system
aaa
user
```

```
password
```

```
group netadmin
commit
```

Certifique-se de configurar as mesmas credenciais de usuário em todos os vManagenodes que fazem parte do cluster. Se decidirmos usar credenciais de administrador, ele deverá ser o mesmo nome de usuário/senha em todos os vManagenodes.

Instalar o certificado do dispositivo em todos os nós do vManage

- Faça login na vManageUI de todos os nós de gerenciamento usando a URL <https://<vmanage-ip>> em seu navegador. Use o endereço IP VPN 512 dos respectivos vManagenodes. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Clique em ... para Gerente/vManage e clique em Gerar CSR.

The screenshot shows the Cisco Catalyst SD-WAN web interface. The top navigation bar includes the Cisco logo, 'Catalyst SD-WAN', and user information. A notification banner at the top states: 'The network is out of compliance due to licensing, please [click here](#) for more actions.' The left sidebar contains navigation links: Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main content area is titled 'Certificates' and has tabs for 'WAN Edge List', 'Control Components', 'Applications', and 'CA Cert'. The 'Control Components' tab is selected, showing a table of devices. A context menu is open over the table, with 'Generate CSR' highlighted. The table has columns: Operation Status, Controller Type, Hostname, System IP, Site ID, Certificate Serial, and Expiration Date. At the bottom, there is a breadcrumb trail: 1.1.1.2 > Add Device > Generate CSR > Upload Certificate > Update Validator.

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. O mesmo procedimento será aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- Conclua esta etapa em todos os nós do vManage que fazem parte do cluster.

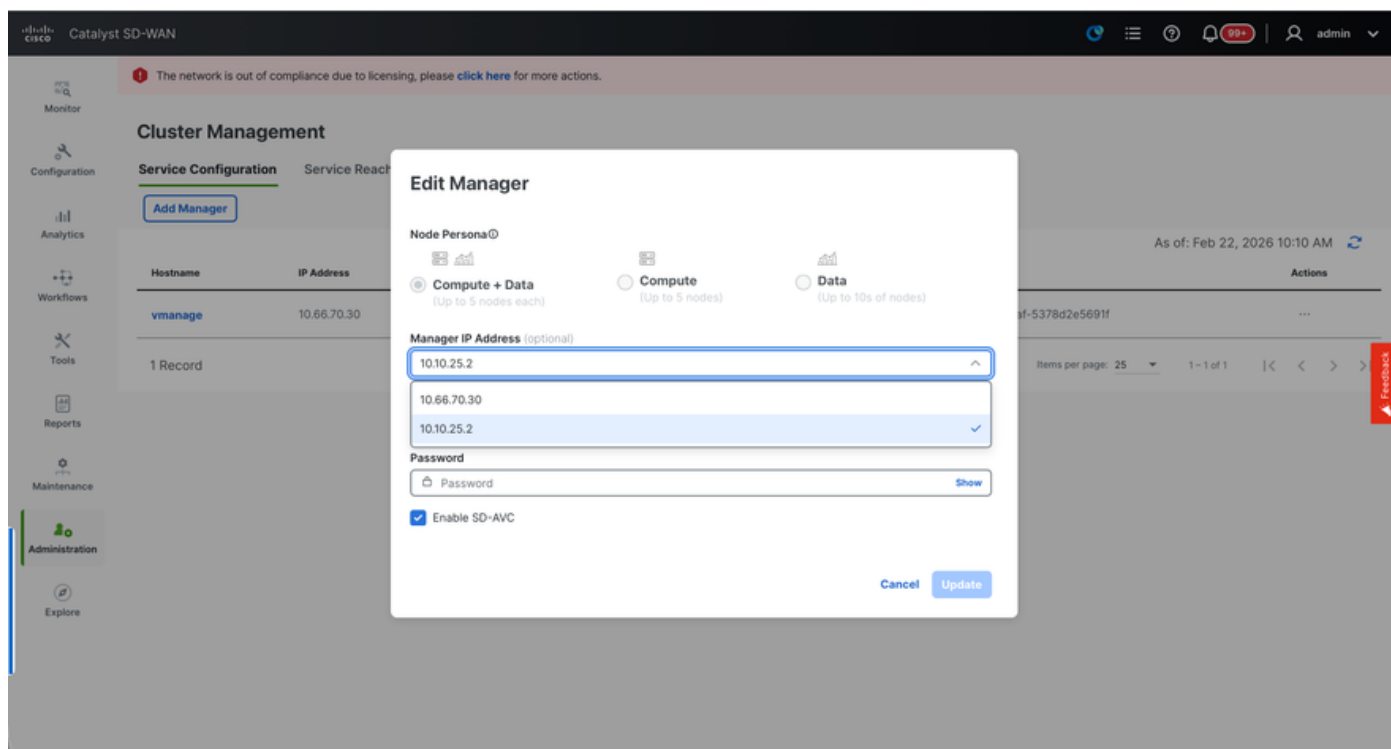
Prepare-se para criar o cluster vManage

- Na webUI do vManage-1, navegue para Administração > Gerenciamento de cluster, clique em ... em Ações para vManage-1, escolha Editar.
- A persona do nó é escolhida automaticamente com base na persona que escolhemos enquanto a VM estava ativada.



Note: Para um cluster de 3 nós, todos os 3 nós do vManage são ativados com computação+dados como persona.

- Para um cluster de 6 nós, 3 nós do vManage são ativados com computação+dados como o persona e 3 nós do vManage são ativados com dados como o persona.
- No menu suspenso do endereço IP do gerente, certifique-se de escolher o IP da interface de serviço do vManage.



- Insira o nome de usuário e a senha que desejamos usar para habilitar o cluster vManage, que é conhecido como credenciais de cluster.
- Como mencionado anteriormente, as mesmas credenciais devem ser configuradas em todos os nós do vManage e devem ser usadas ao adicionar todos os nós ao cluster.



Note: Consulte essa configuração no cluster existente para Habilitar SDAVC - Só precisa ser verificado se for necessário e só é necessário em um nó vManage do cluster.

Clique em Atualizar.

- Depois disso, o serviço vManage NMS é reiniciado em segundo plano e a interface do usuário não fica disponível por alguns minutos, em torno de 5 a 10 minutos. Durante esse período, o acesso do vManage via CLI estará disponível.
- Quando a interface do usuário do vManage-1 estiver acessível, navegue para Administração > Gerenciamento de cluster, certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona é refletido corretamente.
- Alterne para a seção Alcançabilidade do serviço na mesma página e certifique-se de que todos os serviços estejam acessíveis.

Cisco Catalyst SD-WAN

The network is out of compliance due to licensing, please [click here](#) for more actions.

Cluster Management

Service Configuration **Service Reachability**

Current Manager : 10.66.70.30

Q Search Table

As of: Feb 22, 2026 10:14 AM

IP Address	Application Server	Statistics Database	Configuration Database	Messaging Server	SD-AVC
10.66.70.30	Reachable	Reachable	Healthy	Reachable	Reachable

Items per page: 25 1 - 1 of 1

Monitor
Configuration
Analytics
Workflows
Tools
Reports
Maintenance
Administration
Explore

- Se algum dos serviços ainda não estiver acessível, aguarde. Geralmente leva em torno de 20 a 30 minutos.

Construir o cluster vManage

- Na webUI do vManage-1, navegue para Administração > Gerenciamento de cluster, na seção Configuração de serviço,
- Clique em Add Manager, uma janela pop-up será exibida:

Cisco Catalyst SD-WAN

The network is out of compliance due to licensing, please [click here](#) for more actions.

Cluster Management

Service Configuration Service Reachability

Add Manager

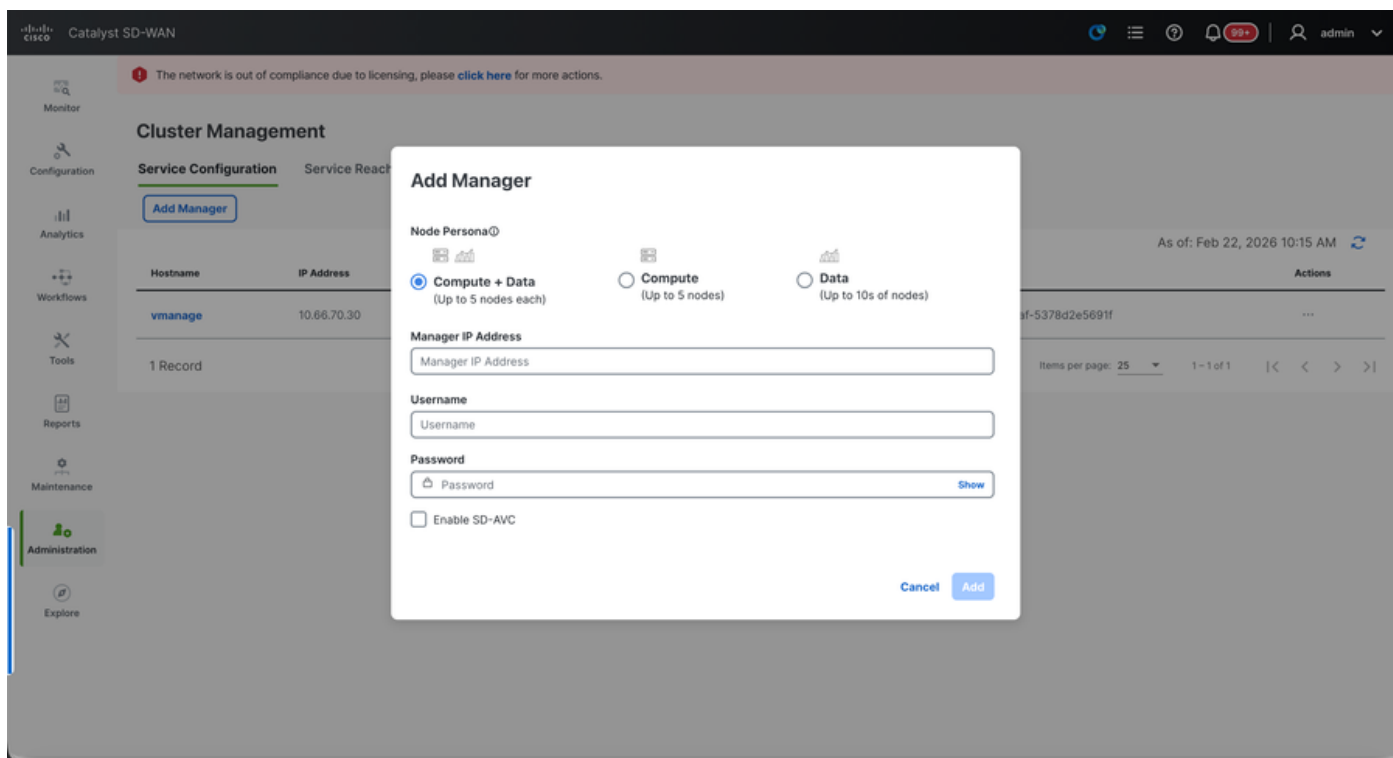
As of: Feb 22, 2026 10:15 AM

Hostname	IP Address	Configure Status	Node Persona	UUID	Actions
vmanage	10.66.70.30	Ready	COMPUTE_AND_DATA	eeffeab2-027e-4cab-b9af-5378d2e5691f	...

1 Record

Items per page: 25 1 - 1 of 1

Monitor
Configuration
Analytics
Workflows
Tools
Reports
Maintenance
Administration
Explore



- Escolha o Node persona com base nas configurações personalizadas feitas enquanto o nó do vManage - 2 foi girado.
- Insira o IP da interface de serviço do vManage-2 em Endereço IP do gerente
- Insira o nome de usuário e a senha, que são as mesmas credenciais usadas na Etapa 6.
- Ativar SDAVC - Para ser deixado desmarcado, pois já o habilitaríamos no vManage-1
- Clique em Adicionar.
- Depois disso, os serviços NMS do vManage são reiniciados em segundo plano para os nós 1 e 2 do vManage. A interface do usuário não está disponível por alguns minutos, em torno de 5 a 10 minutos, para o vManage 1 e 2.
- Durante esse período, o acesso via CLI do vManage 1 e 2 estará disponível.
- Quando a interface do usuário do vManage-1 estiver acessível, navegue para Administração > Gerenciamento de cluster, certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona esteja refletido corretamente.
- Alterne para a seção Alcance do serviço na mesma página e verifique se todos os serviços estão acessíveis para ambos os nós do vManage.
- Se algum dos serviços ainda não estiver acessível, aguarde. Geralmente leva cerca de 5 a 10 minutos.
- Você pode verificar o status do processo de adição de cluster na lista de tarefas disponível no canto superior direito da interface do usuário do vManage.

The screenshot shows the Cisco Catalyst SD-WAN interface. The top navigation bar includes a menu icon (circled in red), a help icon, a notification bell with '99+', and a user profile 'admin'. A sidebar on the left lists various functions: Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main area is titled 'Cluster Management' and has two tabs: 'Service Configuration' (selected) and 'Service Reachability'. Under 'Service Configuration', there is an 'Add Manager' button. Below this is a table with columns: Hostname, IP Address, Configure Status, Node Persona, UUID, and Actions. The table contains one record for 'vmanage' with IP 10.66.70.30, status 'Ready', and persona 'COMPUTE_AND_DATA'. A message at the top states: 'The network is out of compliance due to licensing, please click here for more actions.'

- Você pode procurar a lista de tarefas Ativas e, se a tarefa ainda estiver listada nessa lista, isso indica que a tarefa ainda não foi concluída.
- Você pode clicar na tarefa para verificar o andamento da mesma. Se a tarefa não estiver listada na lista de tarefas Ativas, alterne para Concluído e verifique se a tarefa foi concluída com êxito.
- Somente depois que esses pontos forem validados, vá para a próxima etapa.

Esses pontos precisam ser levados em consideração antes de adicionar o próximo nó ao cluster:

Verifique esses pontos em todas as IUs dos nós do vManage que foram adicionados ao cluster até o momento:

- Navegue para Monitor > Overview da interface do usuário do vManage e verifique se o número de nós do vManage está refletido corretamente e pode ser visto como acessível, dependendo do número de nós adicionados ao cluster.
- Navegue para Administração > Gerenciamento de cluster e certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona esteja refletido corretamente.
- Alterne para a seção Alcance do serviço na mesma página e verifique se todos os serviços estão acessíveis para ambos os nós do vManage.
- Cada vez que um nó é adicionado ao cluster, os serviços NMS de todos os nós no cluster são reiniciados, portanto, a interface do usuário de todos esses nós fica inacessível por algum tempo.
- Dependendo do número de nós no cluster, pode levar mais tempo para que a interface do usuário seja copiada e todos os serviços sejam acessíveis.
- Você pode monitorar a tarefa na Lista de tarefas disponível no canto superior direito da interface do usuário do vManage.
- Na interface do usuário do vManage de cada nó adicionado ao cluster, precisamos ver

todos os roteadores, modelos e políticas, se estiverem disponíveis no vManage-1.

- Se essas configurações não estiverem presentes no vManage-1, os vBonds e vSmarts que foram adicionados ao vManage-1 e também Administration > Settings para Organization-name, vBond, Certificate Authorization devem ser refletidos no restante dos nós do vManage adicionados ao cluster.
- Repita as mesmas etapas para o restante dos nós do vManage.

Depois que todos os controladores estiverem integrados, conclua esta etapa:

Passo 4: Backup/Restauração do Config-db

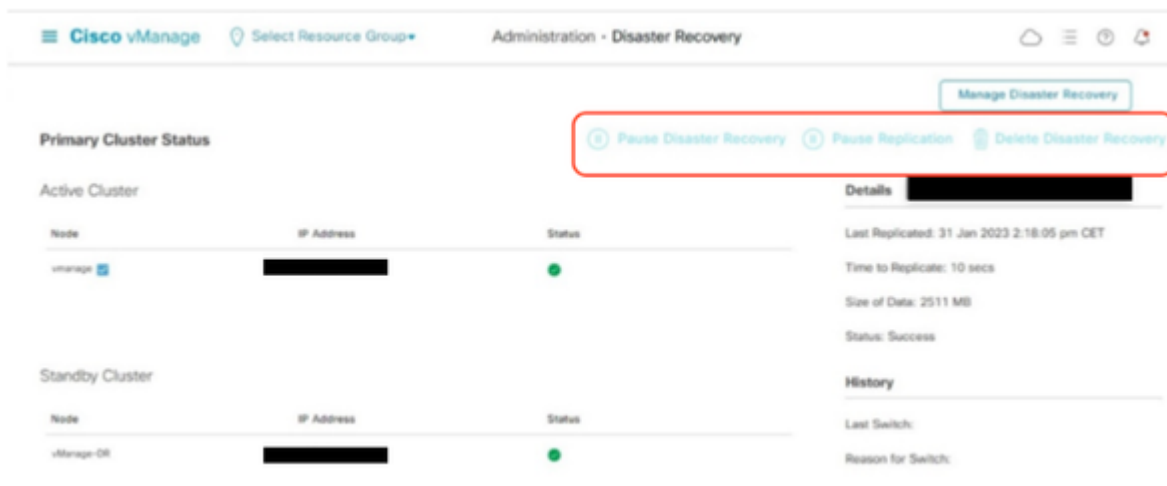
Coletar backup e restauração do banco de dados de configuração do vManage em outro nó do vManage



Note: Ao coletar o backup do banco de dados de configuração do cluster vManage existente que tem a recuperação de desastres ativada, certifique-se de que ele seja coletado após a recuperação de desastres nesse nó ser pausada e excluída.

Confirme se não há replicação de recuperação de desastres em andamento. Navegue até Administração > Recuperação de desastres e verifique o status Sucesso e não em um estado transitório, como Importação pendente, Exportação pendente ou Download pendente. Se o status não for sucesso, entre em contato com o Cisco TAC e certifique-se de que a replicação seja bem-sucedida antes de continuar a pausar a recuperação de desastres.

Primeiro, pause a recuperação de desastres e certifique-se de que a tarefa esteja concluída. Em seguida, exclua a recuperação de desastre e confirme se a tarefa foi concluída.



Entre em contato com o Cisco TAC para garantir que a recuperação de desastres seja limpa com êxito.

Coletar backup do BD de configuração:

- Na estrutura SD-WAN atualmente em uso, é possível gerar backup de configuração-db a partir do cluster vManage.
- Observe que devemos gerar o backup do configuration-db apenas em um nó do cluster vManage, que é o líder do configuration-db.
- No caso do vManage autônomo, o próprio vManage é o líder do banco de dados de configuração.
- No cluster do vManage, identifique o nó do líder configuration-db usando o comando `request nms configuration-db diagnostics`. Você pode executar esse comando em todos os nós do cluster vManage de 3 nós.
- Em um cluster de 6 nós, certifique-se de executar esse comando nos nós vManage onde configuration-db está habilitado para identificar o nó líder. Navegue até Administração > Gerenciamento de cluster para verificar o mesmo:
- Como vemos na captura de tela, os nós configurados com persona COMPUTE_AND_DATA têm configuration-db em execução.

Você pode verificar o mesmo usando o comando `request nms configuration-db status` no vManageCLI. A saída é a mostrada

```
vmanage# request nms configuration-db status
NMS configuration database
  Enabled: true
  Status: running PID:32632 for 1066085s
  Native metrics status: ENABLED
  Server-load metrics status: ENABLED
vmanage#
```

- Depois de executar o comando solicite o diagnóstico `nms configuration-db` nesses nós, a saída é a seguinte:
- Procure o campo destacado para "IsLeader". Se estiver definido como 1, indica que o nó é o nó líder e podemos coletar backup configuration-db a partir dele.

```
vManage-3# request nms configuration-db diagnostics
NMS configuration database
Checking cluster connectivity for ports 7687,7474 ...
Pinging vManage node 0 on 169.254.1.5:7687,7474...
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2026-02-18 12:41 UTC
SENT (0.0013s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (0.0022s) Handshake with 169.254.1.5:7474 completed
SENT (1.0024s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (1.0028s) Handshake with 169.254.1.5:7687 completed
SENT (2.0044s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (2.0050s) Handshake with 169.254.1.5:7474 completed
SENT (3.0064s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (3.0072s) Handshake with 169.254.1.5:7687 completed
SENT (4.0083s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (4.0091s) Handshake with 169.254.1.5:7474 completed
SENT (5.0106s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (5.0115s) Handshake with 169.254.1.5:7687 completed
```

Max rtt: 0.906ms | Min rtt: 0.392ms | Avg rtt: 0.724ms
 TCP connection attempts: 6 | Successful connections: 6 | Failed: 0 (0.00%)
 Nping done: 1 IP address pinged in 5.01 seconds
 Pinging vManage node 1 on 169.254.2.5:7687,7474...
 ===== SNIP =====
 Connecting to 10.10.10.3...

type	row	attributes[row]["value"]
"StoreSizes"	"TotalStoreSize"	85828934
"PageCache"	"Flush"	4268666
"PageCache"	"EvictionExceptions"	0
"PageCache"	"UsageRatio"	0.09724264705882353
"PageCache"	"Eviction"	2068
"PageCache"	"HitRatio"	1.0
"ID Allocations"	"NumberOfRelationshipIdsInUse"	2068
"ID Allocations"	"NumberOfPropertyIdsInUse"	56151
"ID Allocations"	"NumberOfNodeIdsInUse"	7561
"ID Allocations"	"NumberOfRelationshipTypeIdsInUse"	31
"Transactions"	"LastCommittedTxId"	214273
"Transactions"	"NumberOfOpenTransactions"	1
"Transactions"	"NumberOfOpenedTransactions"	441742
"Transactions"	"PeakNumberOfConcurrentTransactions"	11
"Transactions"	"NumberOfCommittedTransactions"	414568
"Causal Cluster"	"IsLeader"	1 >>>>>>>>
"Causal Cluster"	"MsgProcessDelay"	0
"Causal Cluster"	"InFlightCacheTotalBytes"	0

18 rows
 ready to start consuming query after 388 ms, results consumed after another 13 ms
 Completed
 Connecting to 10.10.10.3...
 Displaying the Neo4j Cluster Status

name	aliases	access	address	role	requestedStatus	currentStatus
"neo4j"	[""]	"read-write"	"169.254.3.5:7687"	"leader"	"online"	"online"
"neo4j"	[""]	"read-write"	"169.254.2.5:7687"	"follower"	"online"	"online"
"neo4j"	[""]	"read-write"	"169.254.1.5:7687"	"follower"	"online"	"online"
"system"	[""]	"read-write"	"169.254.3.5:7687"	"follower"	"online"	"online"
"system"	[""]	"read-write"	"169.254.2.5:7687"	"follower"	"online"	"online"
"system"	[""]	"read-write"	"169.254.1.5:7687"	"leader"	"online"	"online"

6 rows
 ready to start consuming query after 256 ms, results consumed after another 3 ms
 Completed
 Total disk space used by configuration-db:
 60M .

Use esse comando para coletar o backup configuration-db do nó vManage líder configuration-db identificado.

request nms configuration-db backup path /opt/data/backup/

A saída esperada é a seguinte:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Anote as credenciais do configuration-db se ele tiver sido atualizado.
- Se você não souber as credenciais do configuration-db, entre em contato com o TAC para recuperar as credenciais do configuration-db dos nós vManage existentes.
- As credenciais padrão do configuration-db são nome de usuário: neo4j e senha: senha

Restaurar backup do banco de dados de configuração para outro nó do vManage

Copie o backup do configuration-db para o diretório /home/admin/ do vManage usando SCP.

Exemplo de saída do comando scp:

```
XXXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1

(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Para restaurar o backup do configuration-db, primeiro precisamos configurar as credenciais do configuration-db. Se suas credenciais de configuração-db forem default (neo4j/password), podemos pular esta etapa.

Para configurar as credenciais do configuration-db, use o comando request nms configuration-db update-admin-user. Use o nome de usuário e a senha de sua escolha.

Observe que o servidor de aplicativos do vManage é reiniciado. Devido ao qual a interface do usuário do vManage fica inacessível por um curto período.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
```

```
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operation)
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Post que podemos continuar para restaurar o backup do configuration-db:

Podemos usar o comando `request nms configuration-db restore path /home/admin/< >` para restaurar o configuration-db para o novo vManage:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Resetting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Depois que o configuration-db for restaurado, verifique se a interface do usuário do vManage está acessível. Aguarde cerca de 5 minutos e tente acessar a interface do usuário.

Depois de fazer login na interface do usuário com êxito, verifique se a lista de roteadores de borda, o modelo, as políticas e todas as configurações presentes na interface do usuário do vManage anterior ou existente estão refletidas na nova interface do usuário do vManage.

Passo 5: Reautenticação de controladores e invalidação de controladores antigos

Depois que o configuration-db for restaurado, precisamos autenticar novamente todos os novos controladores (vmanage/vsmart/vbond) na malha



Observação: na produção real, se o IP da interface usado para reautenticar for o IP da interface do túnel, será necessário garantir que o serviço NETCONF seja permitido na interface do túnel do vManage, vSmart e vBond e também nos firewalls ao longo do caminho. A porta de firewall a ser aberta é a porta TCP 830 como regra bidirecional do cluster DR para todos os vBonds e vSmarts .

Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers

- Clique nos três pontos próximos a cada controlador e clique em Editar

The screenshot shows the Cisco Catalyst SD-WAN Manager interface. The top navigation bar includes 'Cisco Catalyst SD-WAN', 'Select Resource Group', and 'Configuration - Devices'. Below this, there are tabs for 'WAN Edge List' and 'Controllers'. The 'Controllers' tab is active, displaying a table with 5 controllers. To the right of the table is an 'Edit' form with fields for IP Address, Username, and Password.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	System-ip	Draft Mode	Certificate Status	Policy Name	Policy Version
vbond	SITE_300	vedge	No	Unmanaged	In Sync	3.3.3.3	Disabled	Installed	-	-
vmanage	SITE_300	vmanage1-20121	No	Unmanaged	In Sync	1.1.1.1	Disabled	Installed	-	-
vmanage	SITE_300	vmanage2-20121	No	Unmanaged	In Sync	1.1.1.2	Disabled	Installed	-	-
vmanage	SITE_300	vmanage3-20121	No	Unmanaged	In Sync	1.1.1.3	Disabled	Installed	-	-
vsmart	SITE_300	vsmart	No	Unmanaged	In Sync	2.2.2.2	Disabled	Installed	-	-

- Substitua ip-address (system-ip do controlador) pelo endereço ip transport vpn 0(tunnel interface) .Insira o nome de usuário e a senha e clique em save
- Faça o mesmo para todos os novos controladores na malha

Sincronizar a cadeia de certificados raiz

Depois que todos os controladores estiverem integrados, conclua esta etapa:

Em qualquer servidor Cisco SD-WAN Manager no cluster recém-ativo, execute estas ações:

Digite este comando para sincronizar o certificado raiz com todos os dispositivos Cisco Catalyst SD-WAN no cluster recém-ativo:

<https://vmanage-url/dataservice/system/device/sync/rootcertchain>

Digite este comando para sincronizar o UUID do Cisco SD-WAN Manager com o Cisco SD-WAN Validator:

<https://vmanage-url/dataservice/certificate/syncvbond>

Depois que a estrutura for restaurada e as sessões de controle e bfd estiverem ativas para todas as bordas e controladores na estrutura, precisamos invalidar os controladores antigos (vmanage/vsmart/vbond) da interface do usuário

- Na interface do usuário do vmanage, clique em Configuration > Devices > Certificates
- Clique em Controladores
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em invalidar
- Clique em enviar para vbond
- Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em Excluir.

Passo 6: Pós-cheques



Note: Continue com a seção Post Checks mostrada aqui, que é comum a todas as combinações de implantação.

Combinação 4: vManage Cluster + DR manual/em espera fria

O que é DR em espera manual/a frio? O servidor de backup do SD-WAN Manager ou o cluster do SD-WAN Manager é mantido desligado no estado de espera a frio.

São feitos backups regulares do banco de dados ativo e, se o cluster principal do SD-WAN Manager ou do SD-WAN Manager for desativado, o cluster do SD-WAN Manager ou do SD-WAN Manager em standby será ativado manualmente e o banco de dados de backup será restaurado nele.

Instâncias necessárias:

- 3 ou 6 vManage (cluster principal)
- 3 ou 6 vManage (cluster em standby de recuperação de desastres)
- 1 ou mais vBond (distribuídos entre data centers principais e de DR)
- 1 ou mais vSmart (distribuída entre data centers principais e de recuperação de desastres)

Etapas:

1. Ativar todas as instâncias usando as Etapas Comuns
2. Verificações prévias
3. Configurar a interface do usuário, os certificados e os controladores integrados do vManage
4. Construir cluster vManage
5. Configuração de cluster DR em standby frio
6. Backup/restauração de config-db
7. Pós-cheques

Passo 1: Pré-verificações

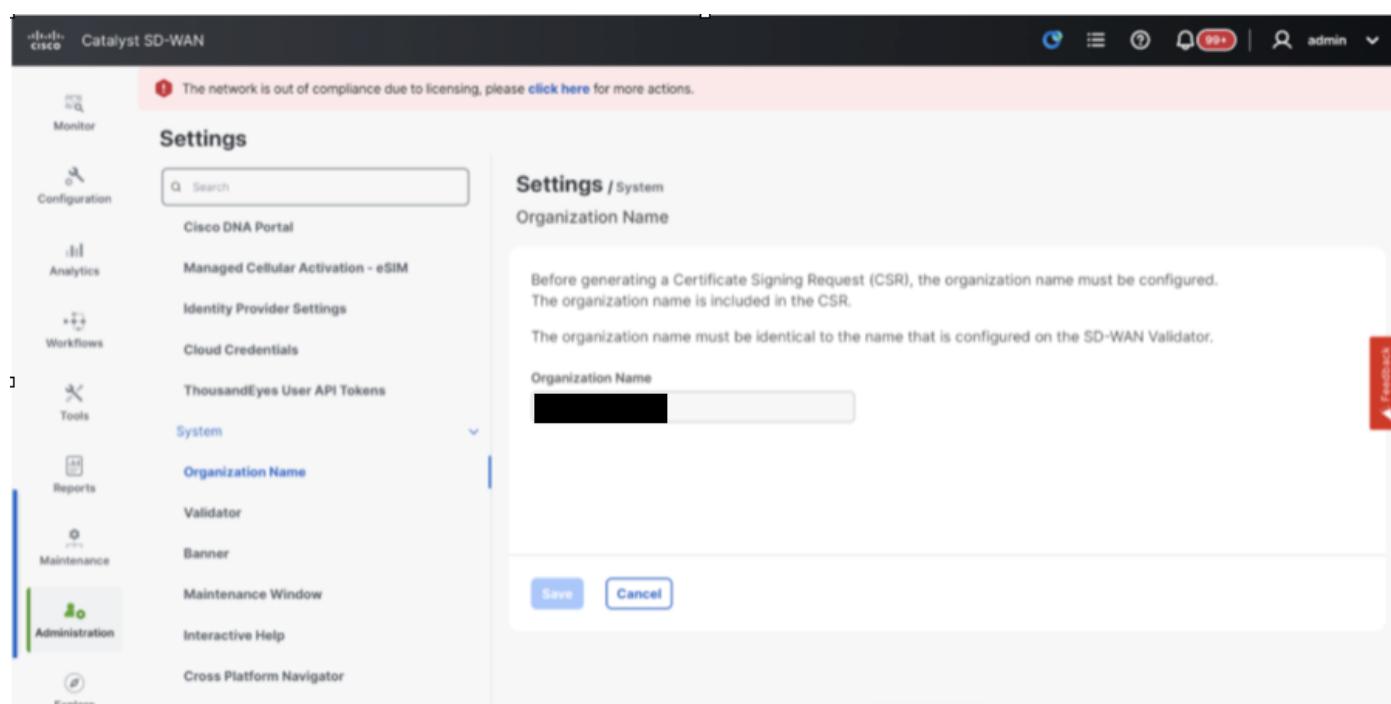
- Certifique-se de que o número das instâncias do gerenciador Cisco SD-WAN ativas seja idêntico ao número das instâncias do gerenciador recém-instaladas do Cisco SD-WAN .

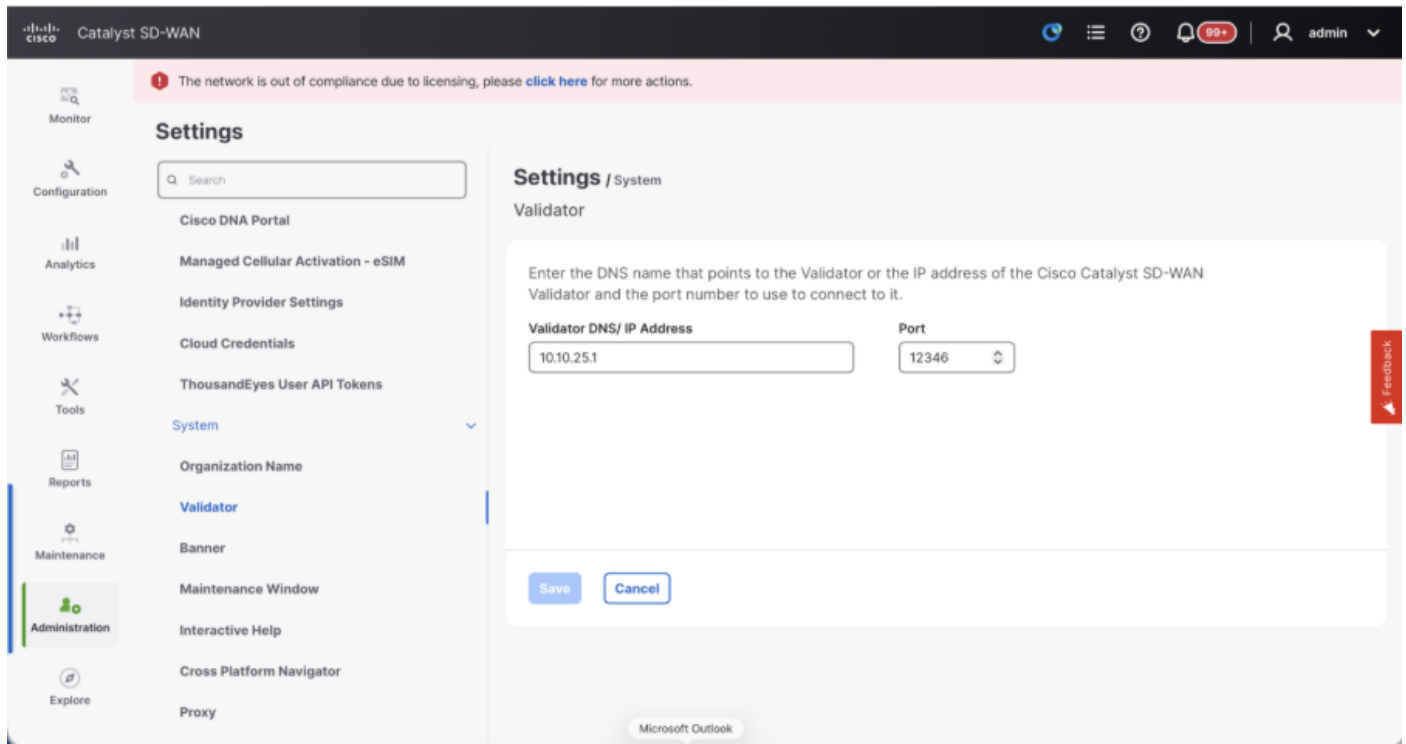
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager executem a mesma versão de software.
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager possam acessar o endereço IP de gerenciamento do Cisco SD-WAN Validator.
- Verifique se os certificados foram instalados nas instâncias recém-instaladas do Cisco SD-WAN Manager.
- Certifique-se de que os relógios em todos os dispositivos Cisco Catalyst SD-WAN, incluindo as instâncias recém-instaladas do Cisco SD-WAN Manager, estejam sincronizados.
- Verifique se um novo conjunto de IPs do sistema e IDs do local está configurado nas instâncias do Cisco SD-WAN Manager recém-instalado, juntamente com a mesma configuração básica do cluster ativo.

Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage

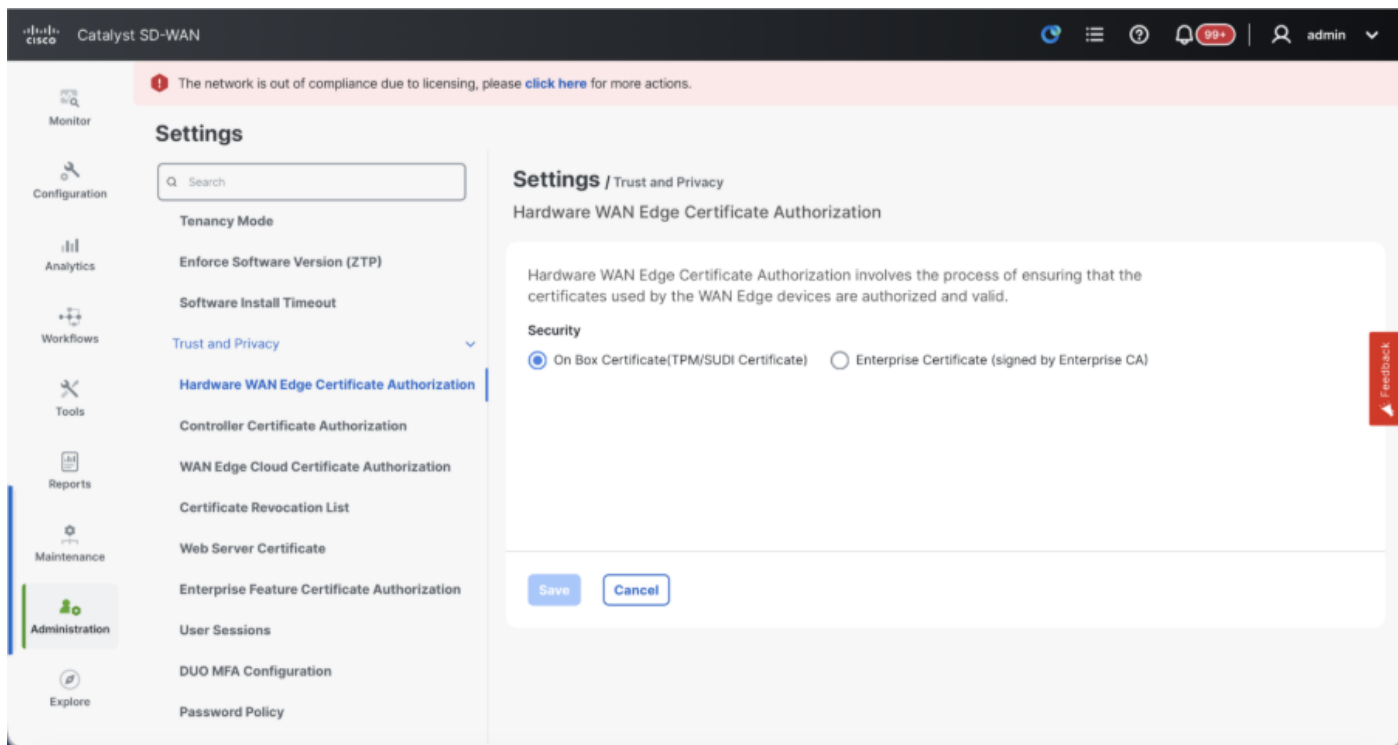
Atualizar as configurações na interface do usuário do vManage

- Depois que as configurações na Etapa 1 forem adicionadas à CLI de todos os controladores, poderemos acessar a webUI do vManage, usando o URL `https://<vmanage-ip>` em seu navegador. Use o endereço IP VPN 512 dos respectivos nós do vManage. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue até Administration > Settings e conclua estas etapas.
- Configure o nome da organização e o endereço IP/URL do validador/vBond. Configure o mesmo valor da CLI do nó do vManage.
- No vManage 20.15/20.18, essas configurações estão disponíveis na seção Sistema.



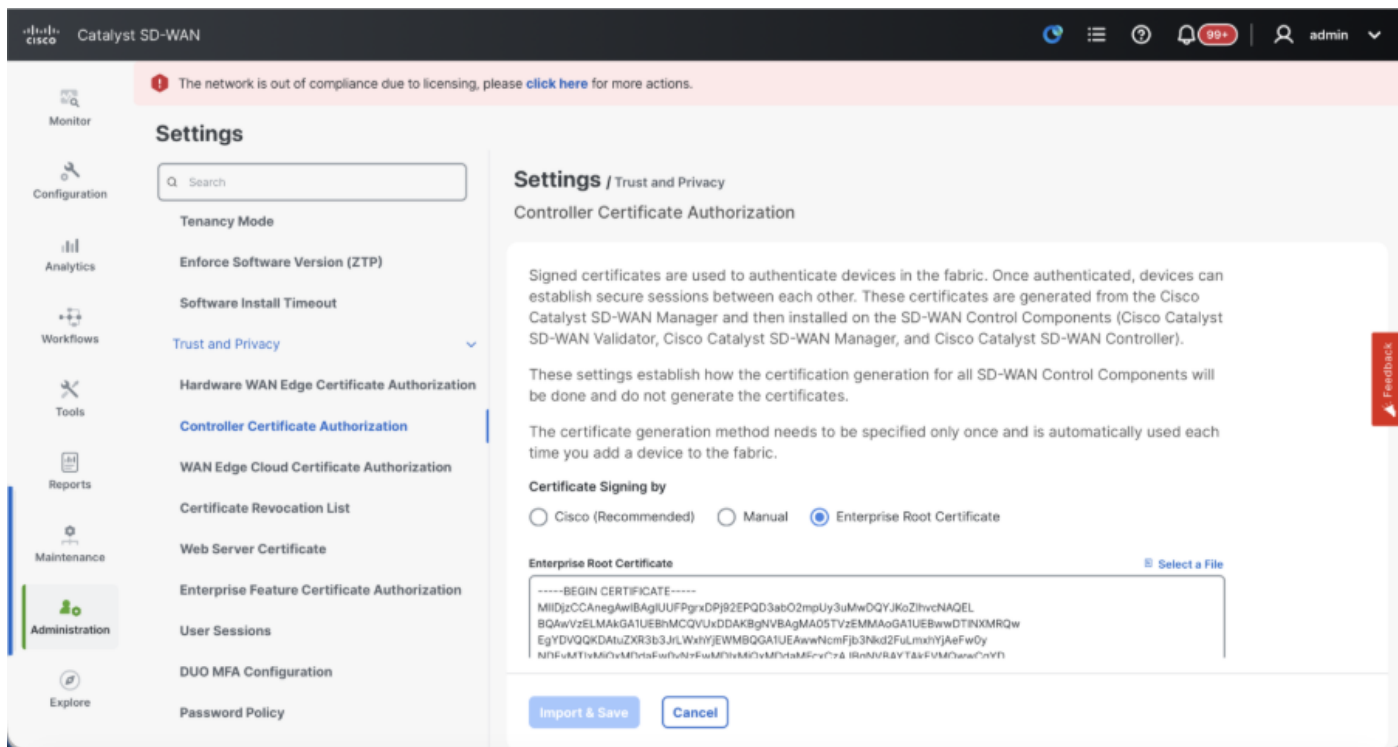


- Verifique as configurações da CA (Certificate Authorization, Autorização de Certificado), que decide a autoridade de certificação usada para assinar os certificados. Podemos ver 3 opções aqui:
1. Autorização do certificado de borda da WAN de hardware - decide a CA para os roteadores de borda da SD-WAN de hardware.
 - On Box Certificate (TPM/SUDI Certificate) - Com essa opção, o certificado pré-instalado no hardware do roteador é usado para estabelecer as conexões de controle (conexões TLS/DTLS)
 - Certificado corporativo (assinado pela autoridade de certificação corporativa) - Com essa opção, os roteadores usam certificados assinados pela autoridade de certificação corporativa da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



2. Controller Certificate Authorization - Decide a CA para controladores SD-WAN.

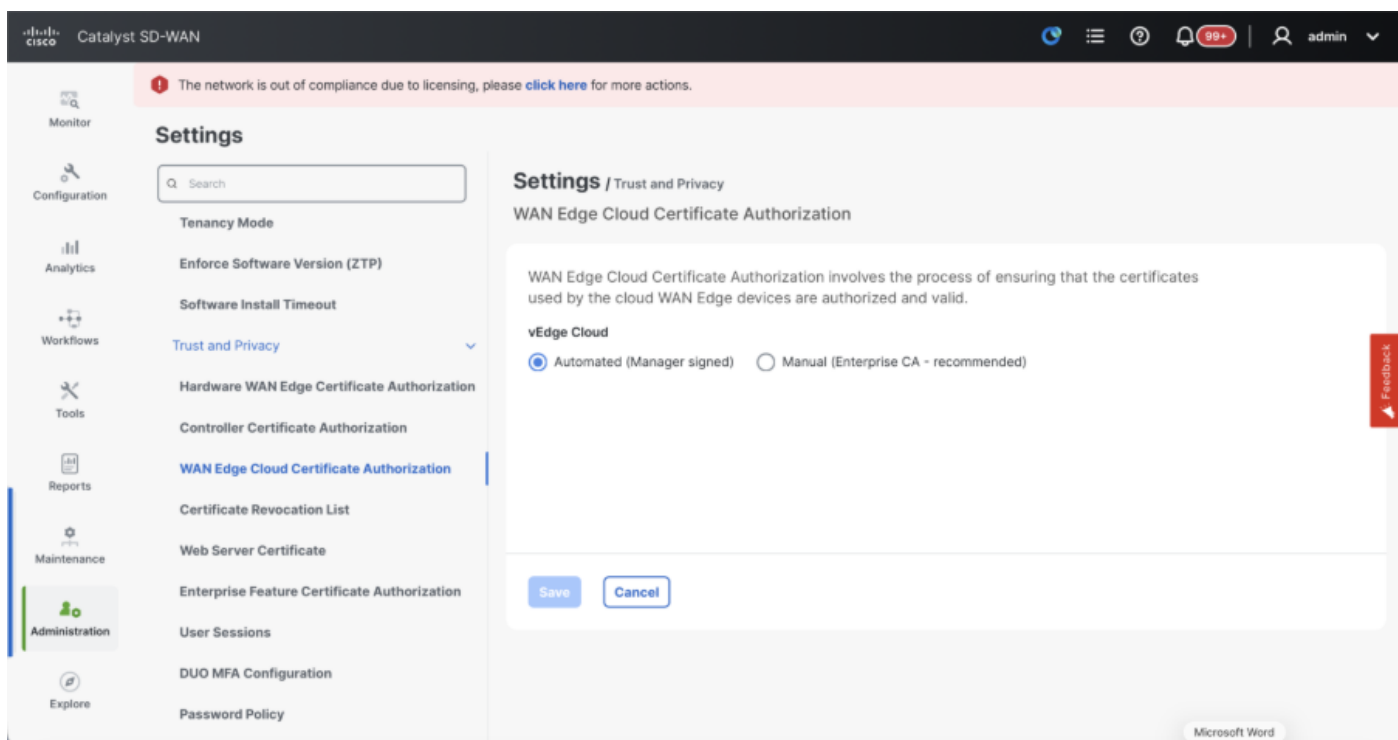
- Cisco (Recomendado) - Os controladores usam os certificados assinados pelo Cisco PKI. O vManage entra em contato automaticamente com o portal PNP usando as credenciais de Smart Account configuradas no vManage e obtém o certificado assinado e é instalado no controlador.
- Manual - Os controladores usam os certificados assinados pela PKI da Cisco. Assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Certificado raiz empresarial - com esta opção, os roteadores usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



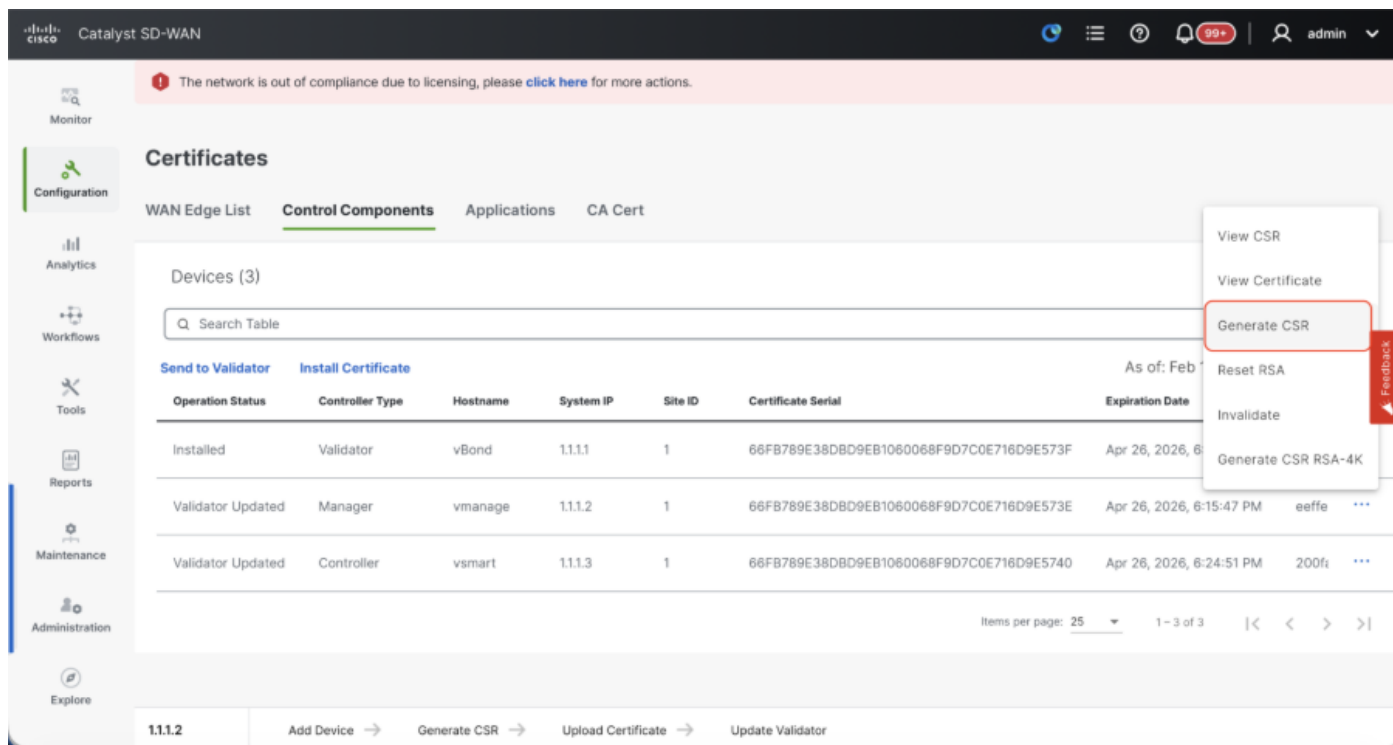
3. Autorização de certificado de nuvem de borda de WAN - decide a CA para roteadores de borda de SD-WAN virtuais (CSR1000v, C8000v, nuvem vEdge)

- Automatizado (vManage assinado) - O vManage assina automaticamente o CSR para os roteadores de borda virtual e instala o certificado no roteador.
- Manual (CA empresarial - recomendado) - Os roteadores virtuais usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.

Caso estejamos usando nossa própria CA, autoridade de certificação empresarial, escolha Empresa.



- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores
- Clique em ... para Gerente/vManage e clique em Gerar CSR.



- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.

Integração do vBond/Validator e vSmart/Controller ao vManage

Navegue para Configuration > Devices > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Onboarding vBond/Validador

- Clique em Add vBond no caso de 20.12 vManage ou Adicionar validador no caso de 20.15/20.18 vManage. Um pop-up é aberto, insira o IP de transporte VPN 0 de vBond que pode ser acessado a partir do vManage.
- Verifique a acessibilidade usando ping se permitido a partir do CLI de vManage to vBond IP.

- Insira as credenciais de usuário do vBond.



Observação: Precisamos usar credenciais de administrador de VoBond ou uma parte do usuário de netadmingroup. Você pode verificar isso no CLI do vBond. Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vBond



Note: Se o vBond estiver por trás de um dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vBond está traduzido para um IP público. Se o IP da interface VPN 0 não estiver acessível no vManage, use o endereço IP público da interface VPN 0 nesta etapa

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. On the left, there is a navigation sidebar with options like Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main area displays the 'Control Components' section, which includes a table with 3 components. A red box highlights the 'Add Validator' button. On the right, the 'Add Validator' dialog box is open, showing fields for Validator Management IP Address, Username, Password, and a dropdown for Generate CSR (set to No). A red 'Feedback' button is visible on the right side of the dialog.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sync
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se a Cisco (recomendada) for escolhida, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, será instalado no vBond automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver várias vBonds, repita as mesmas etapas.

vSmart/controlador integrado:

- Clique em Add vSmart no caso do vManage 20.12 ou Add Controller no caso do vManage 20.15/20.18.
- Um pop-up é aberto, insira o IP de transporte VPN 0 do vSmart que pode ser acessado no vManage.
- Verifique a acessibilidade usando ping se permitido do CLI do vManage para o vSmart IP.
- Insira as credenciais de usuário do vSmart. Observe que precisamos usar credenciais de administrador do vSmart ou uma parte do usuário do grupo netadmin.
- Você pode verificar isso na CLI do vSmart.
- Defina o protocolo como TLS, se pretendemos usar TLS para roteadores para estabelecer conexões de controle com vSmart. Essa configuração também precisa ser configurada na CLI dos nós vSmarts e vManage.
- Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vSmart.



Observação: se o vSmart estiver por trás do dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vSmart está convertido em um IP público e se o IP da interface VPN 0 não pode ser acessado do vManage, use o endereço IP público do IP da interface VPN 0 nesta etapa.

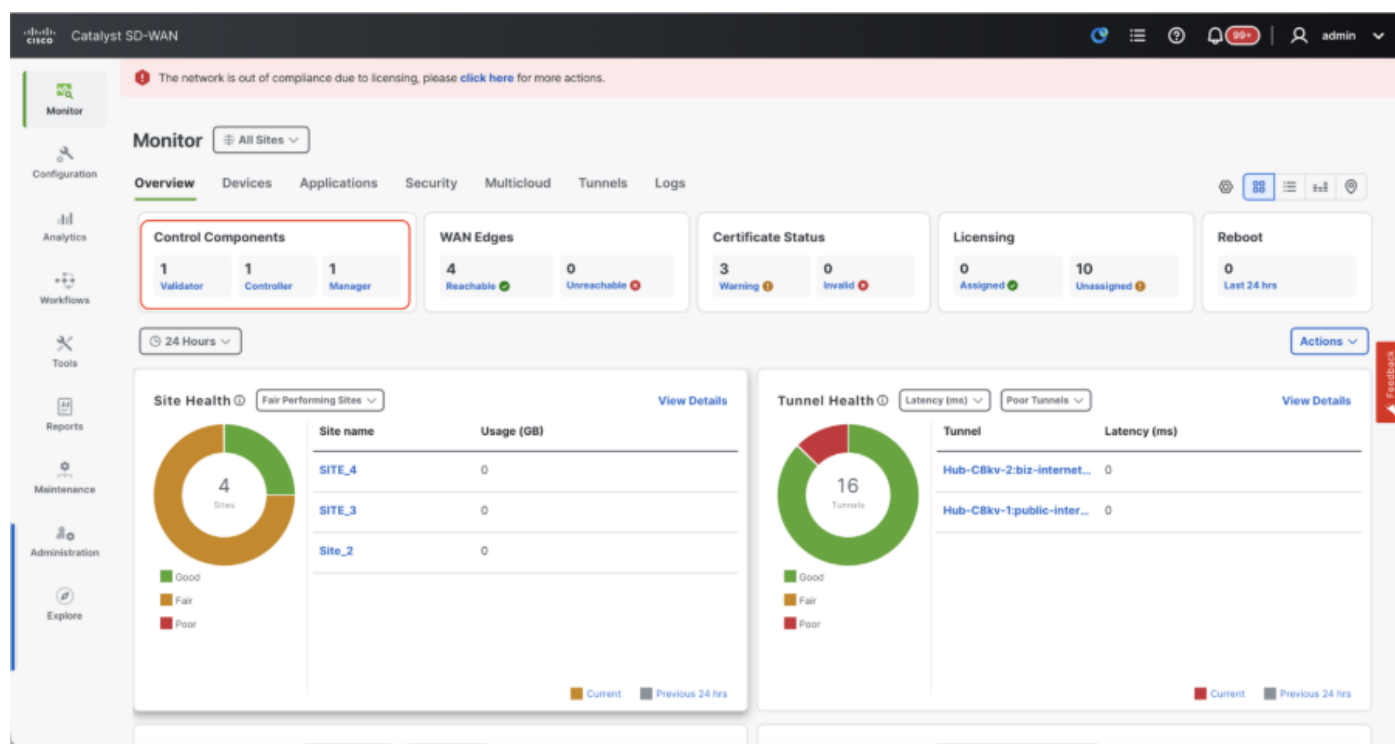
The screenshot shows the Cisco Catalyst SD-WAN vManage interface. The main panel displays the 'Devices' section with a table of 'Control Components (3)'. The table has columns for Controller Type, Site Name, Hostname, Config Locked, Managed By, Device Status, and Sy. The table lists three components: a Validator (vBond), a Manager (vmanage), and a Controller (vsmart). The 'Add Controller' modal is open on the right, showing fields for Controller Management IP Address, Username, Password, Protocol (set to DTLS), Port, and Generate CSR (set to No). A red 'Feedback' button is visible on the right side of the modal.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sy
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

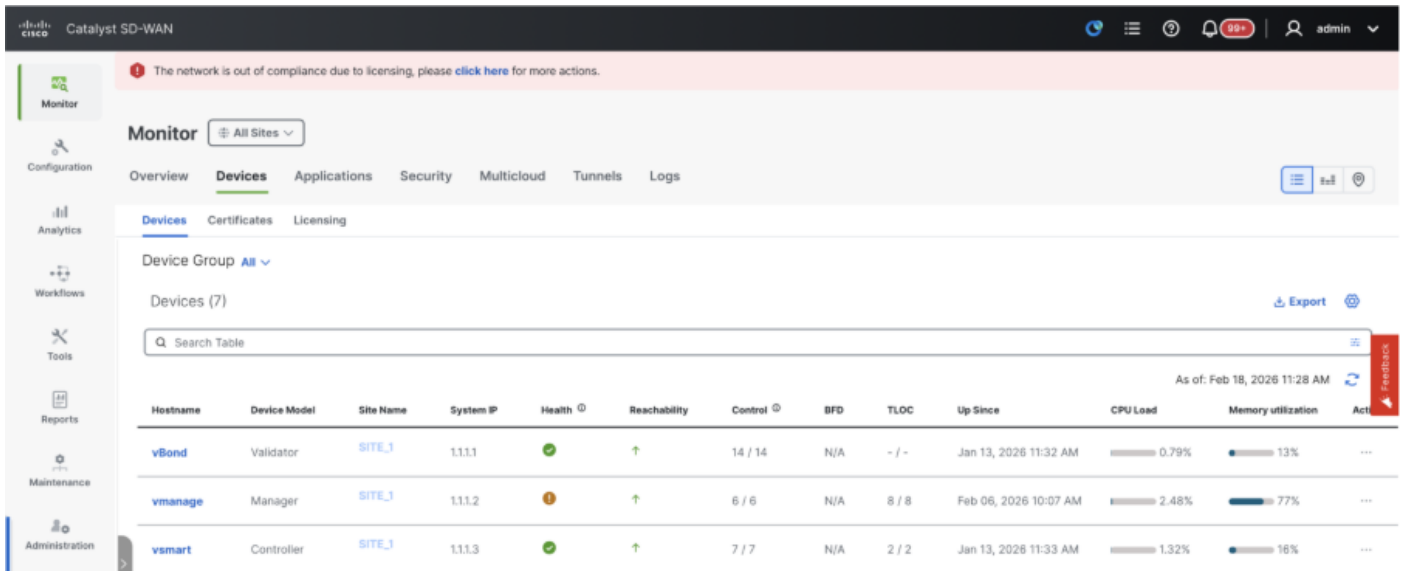
- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vSmart automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver vários vSmarts, repita as mesmas etapas.

Verificação

Após concluir todas as etapas, verifique se todos os componentes de controle estão acessíveis em Monitor>Dashboard



- Clique nos respectivos componentes de controle e confirme se todos estão acessíveis.
- Navegue até Monitor > Devices e confirme se todos os componentes de controle estão acessíveis.



The screenshot shows the Catalyst SD-WAN Monitor interface. A notification at the top states: "The network is out of compliance due to licensing, please [click here](#) for more actions." The main section is titled "Monitor" and includes a "Device Group" dropdown set to "All". Below this, a table lists 7 devices. The table has columns for Hostname, Device Model, Site Name, System IP, Health, Reachability, Control, BFD, TLOC, Up Since, CPU Load, Memory utilization, and Actions. The devices listed are vBond (Validator), vmanage (Manager), and vsmart (Controller), all associated with SITE_1.

Hostname	Device Model	Site Name	System IP	Health	Reachability	Control	BFD	TLOC	Up Since	CPU Load	Memory utilization	Act
vBond	Validator	SITE_1	1.1.1.1	✓	↑	14 / 14	N/A	- / -	Jan 13, 2026 11:32 AM	0.79%	13%	...
vmanage	Manager	SITE_1	1.1.1.2	⚠	↑	6 / 6	N/A	8 / 8	Feb 06, 2026 10:07 AM	2.48%	77%	...
vsmart	Controller	SITE_1	1.1.1.3	✓	↑	7 / 7	N/A	2 / 2	Jan 13, 2026 11:33 AM	1.32%	16%	...

Passo 3: Construir cluster vManage

Estrutura SD-WAN integrada com um cluster vManage na sobreposição SD-WAN



Observação: o vManage Cluster pode ser configurado com 3 nós do vManage ou 6 nós do vManage, dependendo do número de locais integrados à malha SD-WAN

Integre todos os controladores SD-WAN com um único nó vManage

Continue com as etapas compartilhadas em "Controladores SD-WAN integrados com um único nó vManage na sobreposição SD-WAN" para ativar primeiro a estrutura SD-WAN com um nó vManage e integrar todos os Validadores (vBond) e Controladores (vSmart) necessários.

Configure as configurações CLI de todos os nós do vManage que fazem parte do cluster

- Configure o restante dos nós do vManage. No caso de um cluster de 3 nós, você tem 2 nós restantes para configurar, no caso de um cluster de 6 nós, você tem 5 nós para configurar.
- Configure as configurações do sistema conforme mostrado:

```
config t
system
host-name
```

```
system-ip
```

site-id

organization-name

vbond

commit



Observação: se estamos usando URL como endereço vBond, certifique-se de configurar os endereços IP do servidor DNS na configuração VPN 0 ou de garantir que eles possam ser resolvidos.

Essas configurações são necessárias para ativar a interface de transporte usada para estabelecer conexões de controle com os roteadores e o restante dos controladores.

```
config t
vpn 0
  dns
```

```
    primary
  dns
```

```
    secondary
interface eth1
  ip address
```

```
tunnel-interface
  allow-service all
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service stun
  allow-service https
!
no shutdown
!
ip route 0.0.0.0/0
```

```
commit
```

Configure também a interface de gerenciamento VPN 512 para permitir o acesso de gerenciamento fora de banda ao controlador.

```
Conf t
vpn 512
  interface eth0
    ip address

    no shutdown
  !
  ip route 0.0.0.0/0
```

```
!
Commit
```

Configuração opcional:

- Você pode consultar as configurações da sua controladora existente e, se a configuração listada aqui estiver presente, poderá adicionar essa configuração às novas controladoras.
- Configure o protocolo de controle como TLS somente se houver um requisito para que os roteadores estabeleçam conexões de controle seguras com os nós do vManage que usam TLS. Por padrão, todos os controladores e roteadores estabelecem uma conexão de controle usando DTLS. Essa é uma configuração opcional necessária apenas nos nós vSmart e vManage, dependendo de sua necessidade.

```
Conf t
security
  control
    protocol tls
commit
```

Configurar a interface de serviço em todos os nós do vManage

Configure a interface de serviço em todos os vManageEnodes, incluindo o vManage-1, que já foi integrado. Essa interface é usada para comunicação de cluster, o que significa comunicação entre os vManagenodes no cluster.

```
conf t
interface eth2
  ip address
```

```
no shutdown
commit
```

Certifique-se de que a mesma sub-rede IP seja usada para a interface de serviço em todos os nós no cluster vManagern.

Configurar credenciais do cluster

Podemos usar as mesmas credenciais de administrador dos modosv para configurar o cluster do gerenciamento. Caso contrário, podemos configurar uma nova credencial de usuário que faz parte de netadmin group. As configurações para configurar a credencial do novo usuário são as mostradas

```
conf t
system
aaa
user
```

```
password
```

```
group netadmin
commit
```

Certifique-se de configurar as mesmas credenciais de usuário em todos os nós vManagenodesque fazem parte do cluster. Se decidirmos usar credenciais de administrador, ele deverá ter o mesmo nome de usuário/senha em todos os nós vManagenodes.

Instalar o certificado do dispositivo em todos os nós do vManage

- Faça login na vManageUI de todos os nós de gerenciamento usando a URL <https://<vmanage-ip>> em seu navegador. Use o endereço IP VPN 512 dos respectivos vManagenodes. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Clique em ... para Gerente/vManage e clique em Gerar CSR.

The screenshot shows the Cisco Catalyst SD-WAN web interface. At the top, there's a notification: "The network is out of compliance due to licensing, please [click here](#) for more actions." The left sidebar contains navigation options: Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main content area is titled "Certificates" and has tabs for WAN Edge List, Control Components (selected), Applications, and CA Cert. Under "Control Components", there's a "Devices (3)" section with a search bar. Below this is a table with columns: Operation Status, Controller Type, Hostname, System IP, Site ID, Certificate Serial, and Expiration Date. The table lists three devices. A context menu is open over the table, showing options: View CSR, View Certificate, Generate CSR (highlighted with a red box), Reset RSA, Invalidate, and Generate CSR RSA-4K. The bottom navigation bar shows the path: 1.1.1.2 > Add Device > Generate CSR > Upload Certificate > Update Validator.

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Conclua esta etapa em todos os nós do vManage que fazem parte do cluster.

Prepare-se para criar o cluster vManage

- Na webUI do vManage-1, navegue para Administração > Gerenciamento de cluster, clique em ... em Ações para vManage-1, escolha Editar.
- A persona do nó é escolhida automaticamente com base na persona que escolhemos enquanto a VM estava ativada.



Note: Para um cluster de 3 nós, todos os 3 nós do vManage são ativados com computação+dados como persona.

- Para um cluster de 6 nós, 3 nós do vManage são ativados com computação+dados como o persona e 3 nós do vManage são ativados com dados como o persona.
- No menu suspenso do endereço IP do gerente, certifique-se de escolher o IP da interface de serviço do vManage.
- Insira o nome de usuário e a senha que desejamos usar para habilitar o cluster vManage, que é conhecido como credenciais de cluster.
- Como mencionado anteriormente, as mesmas credenciais devem ser configuradas em todos os nós do vManage e devem ser usadas ao adicionar todos os nós ao cluster.

Configuração opcional:

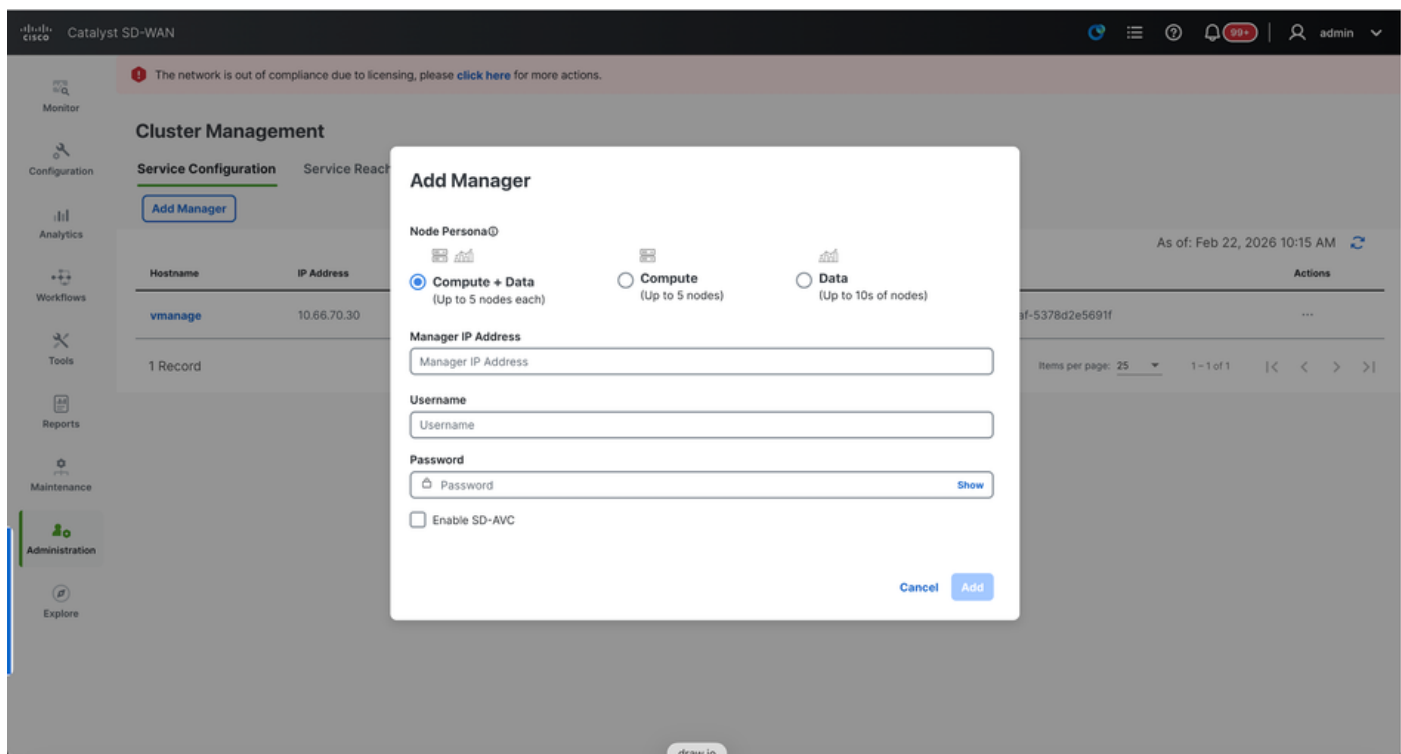
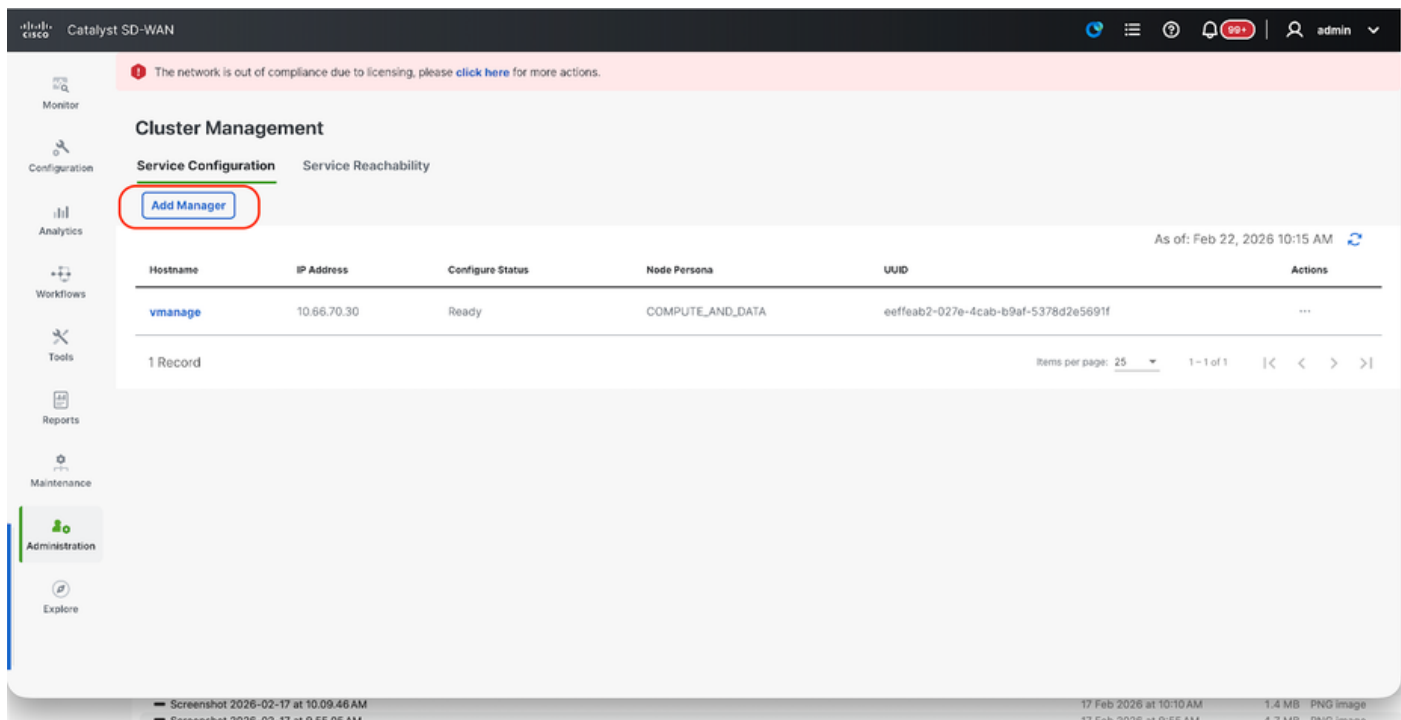
Consulte essa configuração no cluster existente para Habilitar SDAVC - Só precisa ser verificado se for necessário e só é necessário em um nó vManage do cluster.

Clique em Atualizar.

- Depois disso, o serviço vManage NMS é reiniciado em segundo plano e a interface do usuário não fica disponível por alguns minutos, em torno de 5 a 10 minutos. Durante esse período, o acesso do vManage via CLI estará disponível.
- Quando a interface do usuário do vManage-1 estiver acessível, navegue para Administração > Gerenciamento de cluster, certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona é refletido corretamente. Alterne para a seção Alcançabilidade do serviço na mesma página e certifique-se de que todos os serviços estejam acessíveis.
- Se algum dos serviços ainda não estiver acessível, aguarde. Geralmente leva em torno de 20 a 30 minutos.

Construir o cluster vManage

- Na webUI do vManage-1, navegue para Administração > Gerenciamento de cluster, na seção Configuração de serviço,
- Clique em Add Manager, uma janela pop-up será exibida:



- Escolha o Node persona com base nas configurações personalizadas feitas enquanto o nó do vManage - 2 foi girado.
- Insira o IP da interface de serviço do vManage-2 em Endereço IP do gerente
- Insira o nome de usuário e a senha, que são as mesmas credenciais usadas na Etapa 6.
- Ativar SDAVC - Para ser deixado desmarcado, pois já o habilitaríamos no vManage-1
- Clique em Adicionar.
- Depois disso, os serviços NMS do vManage são reiniciados em segundo plano para os nós 1 e 2 do vManage. A interface do usuário não está disponível por alguns minutos, em torno de 5 a 10 minutos, para o vManage 1 e 2.
- Durante esse período, o acesso via CLI do vManage 1 e 2 estará disponível.

- Quando a interface do usuário do vManage-1 estiver acessível, navegue para Administração > Gerenciamento de cluster, certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona esteja refletido corretamente.
- Alterne para a seção Alcance do serviço na mesma página e verifique se todos os serviços estão acessíveis para ambos os nós do vManage.
- Se algum dos serviços ainda não estiver acessível, aguarde. Geralmente leva cerca de 5 a 10 minutos.
- Você pode verificar o status do processo de adição de cluster na lista de tarefas disponível no canto superior direito da interface do usuário do vManage.

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. The top navigation bar includes a menu icon (circled in red), a help icon, a notification bell with '99+', and a user profile 'admin'. A red banner at the top states: 'The network is out of compliance due to licensing, please click here for more actions.' The main content area is titled 'Cluster Management' and has two tabs: 'Service Configuration' (active) and 'Service Reachability'. Under 'Service Configuration', there is an 'Add Manager' button. Below this is a table with columns: Hostname, IP Address, Configure Status, Node Persona, UUID, and Actions. The table contains one record for 'vmanage' with IP 10.66.70.30, status 'Ready', and persona 'COMPUTE_AND_DATA'. The bottom of the table shows '1 Record' and pagination controls.

- Você pode procurar a lista de tarefas Ativas e, se a tarefa ainda estiver listada nessa lista, isso indica que a tarefa ainda não foi concluída.
- Você pode clicar na tarefa para verificar o andamento da mesma. Se a tarefa não estiver listada na lista de tarefas Ativas, alterne para Concluído e verifique se a tarefa foi concluída com êxito.
- Somente depois que esses pontos forem validados, vá para a próxima etapa.

Esses pontos precisam ser levados em consideração antes de adicionar o próximo nó ao cluster:

Verifique esses pontos em todas as IUs dos nós do vManage que foram adicionados ao cluster até o momento:

- Navegue para Monitor > Overview da interface do usuário do vManage e verifique se o número de nós do vManage está refletido corretamente e pode ser visto como acessível, dependendo do número de nós adicionados ao cluster.
- Navegue para Administração > Gerenciamento de cluster e certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona esteja refletido corretamente.

- Alterne para a seção Alcance do serviço na mesma página e verifique se todos os serviços estão acessíveis para ambos os nós do vManage.
- Cada vez que um nó é adicionado ao cluster, os serviços NMS de todos os nós no cluster são reiniciados, portanto, a interface do usuário de todos esses nós fica inacessível por algum tempo.
- Dependendo do número de nós no cluster, pode levar mais tempo para que a interface do usuário seja copiada e todos os serviços sejam acessíveis.
- Você pode monitorar a tarefa na Lista de tarefas disponível no canto superior direito da interface do usuário do vManage.
- Na interface do usuário do vManage de cada nó adicionado ao cluster, precisamos ver todos os roteadores, modelos e políticas, se estiverem disponíveis no vManage-1.
- Se essas configurações não estiverem presentes no vManage-1, os vBonds e vSmarts que foram adicionados ao vManage-1 e também Administration > Settings para Organization-name, vBond, Certificate Authorization devem ser refletidos no restante dos nós do vManage adicionados ao cluster.
- Repita as mesmas etapas para o restante dos nós do vManage.

Passo 4: Configuração de cluster DR em standby frio

Configuração de cluster DR em standby frio

Você pode ativar um ou mais clusters do vManage usando as etapas descritas na Etapa 4:

Construir cluster vManage. Postagem que conclua as etapas descritas na Etapa 6:

Backup/Restauração do Config-db para restaurar o backup do config-db no cluster em standby.

Passo 5: Backup/Restauração do Config-db

Coletar backup e restauração do banco de dados de configuração do vManage em outro nó do vManage

Coletar backup do BD de configuração:

- Na estrutura SD-WAN atualmente em uso, é possível gerar backup de configuração-db a partir do cluster vManage.
- Observe que devemos gerar o backup do configuration-db apenas em um nó do cluster vManage, que é o líder do configuration-db.
- No caso do vManage autônomo, o próprio vManage é o líder do banco de dados de configuração.
- No cluster do vManage, identifique o nó do líder configuration-db usando o comando `request nms configuration-db diagnostics`. Você pode executar esse comando em todos os nós do cluster vManage de 3 nós.
- Em um cluster de 6 nós, certifique-se de executar esse comando nos nós vManage onde configuration-db está habilitado para identificar o nó líder. Navegue até Administração > Gerenciamento de cluster para verificar o mesmo:

- Como vemos na captura de tela, os nós configurados com persona COMPUTE_AND_DATA têm configuration-db em execução.

Você pode verificar o mesmo usando o comando requestnmsconfiguration-dbstatus no vManageCLI. A saída é a mostrada

```
vmanage# request nms configuration-db status
NMS configuration database
  Enabled: true
  Status: running PID:32632 for 1066085s
  Native metrics status: ENABLED
  Server-load metrics status: ENABLED
vmanage#
```

- Depois de executar o comando solicite o diagnóstico nms configuration-db nesses nós, a saída é a seguinte:
- Procure o campo destacado para "IsLeader". Se estiver definido como 1, indica que o nó é o nó líder e podemos coletar backup configuration-db a partir dele.

```
vManage-3# request nms configuration-db diagnostics
NMS configuration database
Checking cluster connectivity for ports 7687,7474 ...
Pinging vManage node 0 on 169.254.1.5:7687,7474...
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2026-02-18 12:41 UTC
SENT (0.0013s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (0.0022s) Handshake with 169.254.1.5:7474 completed
SENT (1.0024s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (1.0028s) Handshake with 169.254.1.5:7687 completed
SENT (2.0044s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (2.0050s) Handshake with 169.254.1.5:7474 completed
SENT (3.0064s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (3.0072s) Handshake with 169.254.1.5:7687 completed
SENT (4.0083s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (4.0091s) Handshake with 169.254.1.5:7474 completed
SENT (5.0106s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (5.0115s) Handshake with 169.254.1.5:7687 completed
Max rtt: 0.906ms | Min rtt: 0.392ms | Avg rtt: 0.724ms
TCP connection attempts: 6 | Successful connections: 6 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 5.01 seconds
Pinging vManage node 1 on 169.254.2.5:7687,7474...
===== SNIP =====
Connecting to 10.10.10.3...
```

type	row	attributes[row]["value"]
"StoreSizes"	"TotalStoreSize"	85828934
"PageCache"	"Flush"	4268666
"PageCache"	"EvictionExceptions"	0
"PageCache"	"UsageRatio"	0.09724264705882353
"PageCache"	"Eviction"	2068
"PageCache"	"HitRatio"	1.0
"ID Allocations"	"NumberOfRelationshipIdsInUse"	2068
"ID Allocations"	"NumberOfPropertyIdsInUse"	56151

"ID Allocations"	"NumberOfNodeIdsInUse"	7561	
"ID Allocations"	"NumberOfRelationshipTypeIdsInUse"	31	
"Transactions"	"LastCommittedTxId"	214273	
"Transactions"	"NumberOfOpenTransactions"	1	
"Transactions"	"NumberOfOpenedTransactions"	441742	
"Transactions"	"PeakNumberOfConcurrentTransactions"	11	
"Transactions"	"NumberOfCommittedTransactions"	414568	
"Causal Cluster"	"IsLeader"	1	>>>>>>>>>
"Causal Cluster"	"MsgProcessDelay"	0	
"Causal Cluster"	"InFlightCacheTotalBytes"	0	

18 rows
ready to start consuming query after 388 ms, results consumed after another 13 ms
Completed
Connecting to 10.10.10.3...
Displaying the Neo4j Cluster Status

name	aliases	access	address	role	requestedStatus	currentStatus
"neo4j"	[]	"read-write"	"169.254.3.5:7687"	"leader"	"online"	"online"
"neo4j"	[]	"read-write"	"169.254.2.5:7687"	"follower"	"online"	"online"
"neo4j"	[]	"read-write"	"169.254.1.5:7687"	"follower"	"online"	"online"
"system"	[]	"read-write"	"169.254.3.5:7687"	"follower"	"online"	"online"
"system"	[]	"read-write"	"169.254.2.5:7687"	"follower"	"online"	"online"
"system"	[]	"read-write"	"169.254.1.5:7687"	"leader"	"online"	"online"

6 rows
ready to start consuming query after 256 ms, results consumed after another 3 ms
Completed
Total disk space used by configuration-db:
60M .

Use esse comando para coletar o backup configuration-db do nó vManage líder configuration-db identificado.

```
request nms configuration-db backup path /opt/data/backup/
```

A saída esperada é a seguinte:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Anote as credenciais do configuration-db se ele tiver sido atualizado.
- Se você não souber as credenciais do configuration-db, entre em contato com o TAC para recuperar as credenciais do configuration-db dos nós vManage existentes.
- As credenciais padrão do configuration-db são nome de usuário: neo4j e senha: senha

Restaurar backup do banco de dados de configuração para outro nó do vManage

Copie o backup do configuration-db para o diretório /home/admin/ do vManage usando SCP.

Exemplo de saída do comando scp:

```
XXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1
```

```
(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Para restaurar o backup do configuration-db, primeiro precisamos configurar as credenciais do configuration-db. Se suas credenciais de configuração-db forem default (neo4j/password), podemos pular esta etapa.

Para configurar as credenciais do configuration-db, use o comando request nms configuration-db update-admin-user. Use o nome de usuário e a senha de sua escolha.

Observe que o servidor de aplicativos do vManage é reiniciado. Devido ao qual a interface do usuário do vManage fica inacessível por um curto período.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same op
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Post que podemos continuar para restaurar o backup do configuration-db:

Podemos usar o comando request nms configuration-db restore path /home/admin/< >para restaurar o configuration-db para o novo vManage:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Resetting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Depois que o configuration-db for restaurado, verifique se a interface do usuário do vManage está acessível. Aguarde cerca de 5 minutos e tente acessar a interface do usuário.

Depois de fazer login na interface do usuário com êxito, verifique se a lista de roteadores de borda, o modelo, as políticas e todas as configurações presentes na interface do usuário do vManage anterior ou existente estão refletidas na nova interface do usuário do vManage.

Passo 6: Reautenticação de controladores e invalidação de controladores antigos

Depois que o configuration-db for restaurado, precisamos autenticar novamente todos os novos controladores (vmanage/vsmart/vbond) na malha



Observação: na produção real, se o IP da interface usado para reautenticar for o IP da interface do túnel, será necessário garantir que o serviço NETCONF seja permitido na interface do túnel do vManage, vSmart e vBond e também nos firewalls ao longo do caminho. A porta de firewall a ser aberta é a porta TCP 830 como regra bidirecional do cluster DR para todos os vBonds e vSmarts .

Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers

- Clique nos três pontos próximos a cada controlador e clique em Editar

The screenshot shows the Cisco Catalyst SD-WAN Configuration - Devices page. The 'WAN Edge List' tab is selected, displaying a table of controllers. On the right, the 'Edit' form is open, showing fields for IP Address, Username, and Password.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	System-ip	Draft Mode	Certificate Status	Policy Name	Policy Version
vbond	SITE_300	vedge	No	Unmanaged	In Sync	3.3.3.3	Disabled	Installed	-	-
vmanage	SITE_300	vmanage1-20121	No	Unmanaged	In Sync	1.1.1.1	Disabled	Installed	-	-
vmanage	SITE_300	vmanage2-20121	No	Unmanaged	In Sync	1.1.1.2	Disabled	Installed	-	-
vmanage	SITE_300	vmanage3-20121	No	Unmanaged	In Sync	1.1.1.3	Disabled	Installed	-	-
vsmart	SITE_300	vsmart	No	Unmanaged	In Sync	2.2.2.2	Disabled	Installed	-	-

- Substitua ip-address (system-ip do controlador) pelo endereço ip transport vpn 0(tunnel interface) .Insira o nome de usuário e a senha e clique em save
- Faça o mesmo para todos os novos controladores na malha

Sincronizar a cadeia de certificados raiz

Depois que todos os controladores estiverem integrados, conclua esta etapa:

Em qualquer servidor Cisco SD-WAN Manager no cluster recém-ativo, execute estas ações:

Digite este comando para sincronizar o certificado raiz com todos os dispositivos Cisco Catalyst SD-WAN no cluster recém-ativo:

<https://vmanage-url/dataservice/system/device/sync/rootcertchain>

Digite este comando para sincronizar o UUID do Cisco SD-WAN Manager com o Cisco SD-WAN Validator:

<https://vmanage-url/dataservice/certificate/syncvbond>

Depois que a estrutura for restaurada e as sessões de controle e bfd estiverem ativas para todas as bordas e controladores na estrutura, precisamos invalidar os controladores antigos (vmanage/vsmart/vbond) da interface do usuário

- Na interface do usuário do vmanage, clique em Configuration > Devices > Certificates
- Clique em Controladores
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em invalidar
- Clique em enviar para vbond
- Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em Excluir

Passo 7: Pós-cheques



Note: Continue com a seção Post Checks mostrada aqui, que é comum a todas as combinações de implantação.

Combinação 5: vManage Cluster + DR ativado

Instâncias necessárias:

- 3 ou 6 vManage (cluster principal)
- 3 ou 6 vManage (cluster em standby de recuperação de desastres)
- 1 ou mais vBond (distribuídos entre data centers principais e de DR)
- 1 ou mais vSmart (distribuída entre data centers principais e de recuperação de desastres)

Etapas:

1. Ativar todas as instâncias usando as Etapas Comuns
2. Verificações prévias
3. Configurar a interface do usuário, os certificados e os controladores integrados do vManage
4. Construir cluster vManage
5. Configuração de cluster DR em standby frio
6. Backup/restauração de config-db
7. Pós-cheques

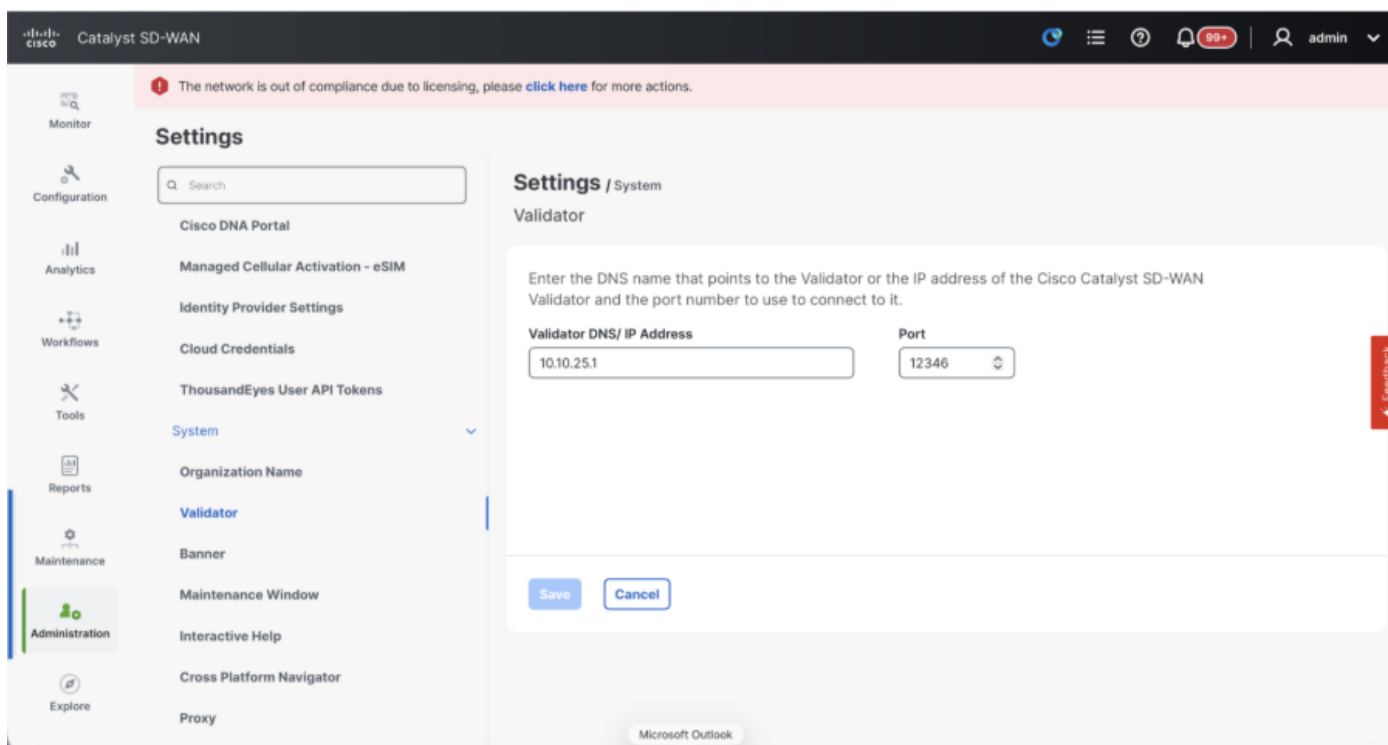
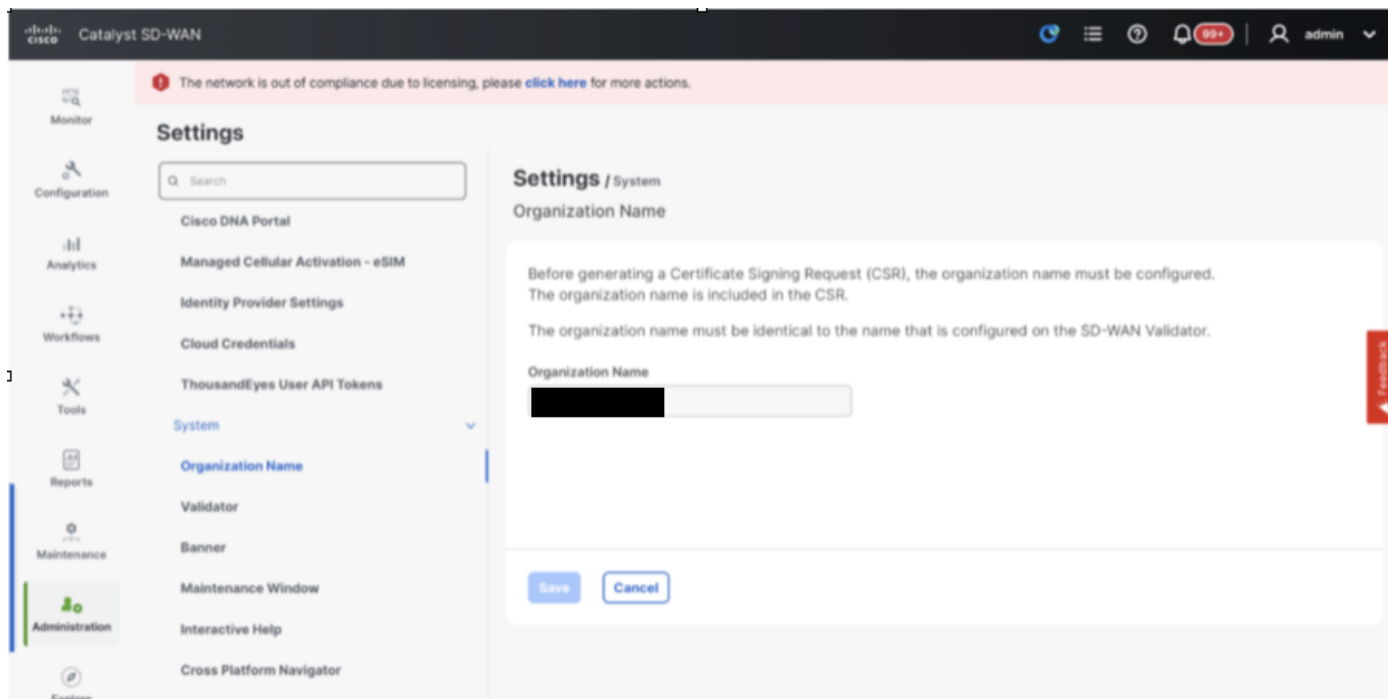
Passo 1: Pré-verificações

- Certifique-se de que o número das instâncias do gerenciador Cisco SD-WAN ativas seja idêntico ao número das instâncias do gerenciador recém-instaladas do Cisco SD-WAN .
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager executem a mesma versão de software.
- Certifique-se de que todas as instâncias novas e ativas do Cisco SD-WAN Manager possam acessar o endereço IP de gerenciamento do Cisco SD-WAN Validator.
- Verifique se os certificados foram instalados nas instâncias recém-instaladas do Cisco SD-WAN Manager.
- Certifique-se de que os relógios em todos os dispositivos Cisco Catalyst SD-WAN, incluindo as instâncias recém-instaladas do Cisco SD-WAN Manager, estejam sincronizados.
- Verifique se um novo conjunto de IPs do sistema e IDs do local está configurado nas instâncias do Cisco SD-WAN Manager recém-instalado, juntamente com a mesma configuração básica do cluster ativo.

Passo 2: Configurar a interface do usuário, os certificados e os controladores integrados do vManage

Atualizar as configurações na interface do usuário do vManage

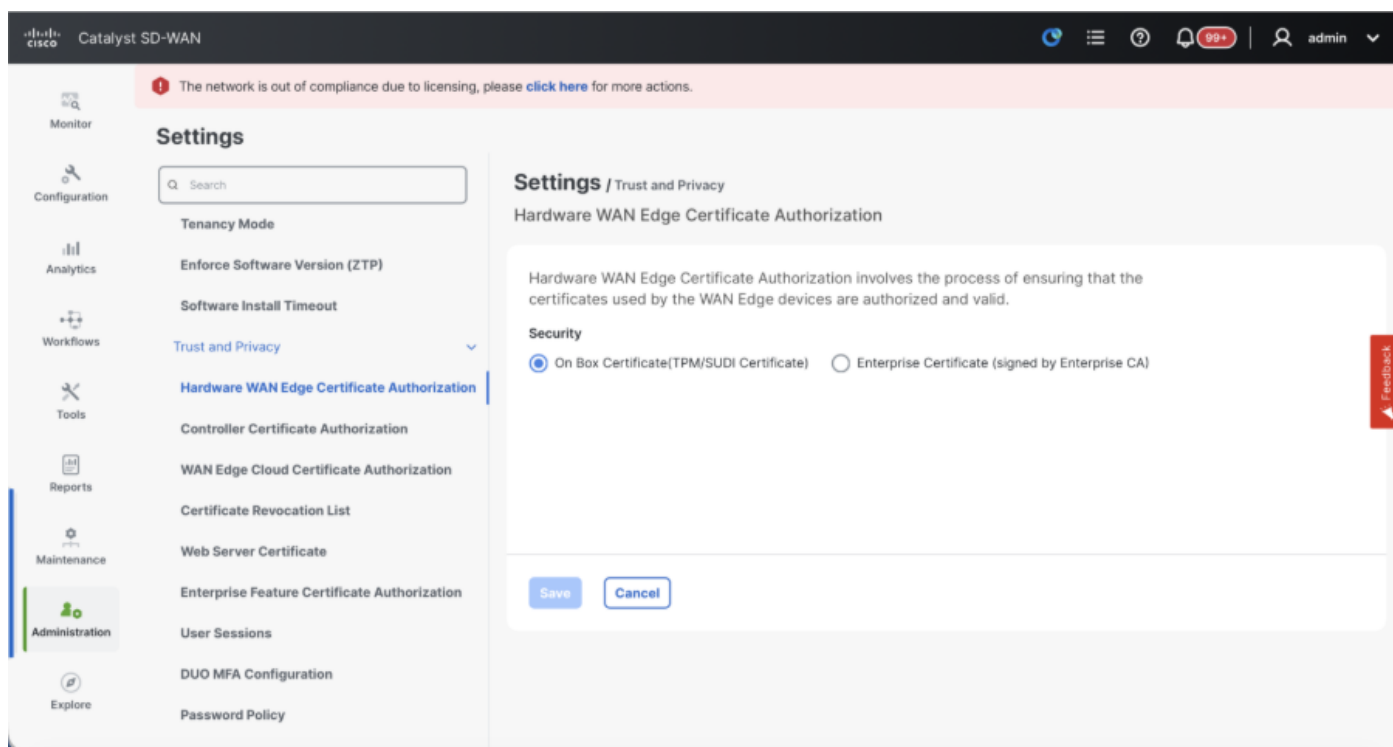
- Depois que as configurações na Etapa 1 forem adicionadas à CLI de todos os controladores, poderemos acessar a webUI do vManage, usando o URL `https://<vmanage-ip>` em seu navegador. Use o endereço IP VPN 512 dos respectivos nós do vManage. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue até Administration > Settings e conclua estas etapas.
- Configure o nome da organização e o endereço IP/URL do validador/vBond. Configure o mesmo valor da CLI do nó do vManage.
- No vManage 20.15/20.18, essas configurações estão disponíveis na seção Sistema.



- Verifique as configurações da CA (Certificate Authorization, Autorização de Certificado), que decide a autoridade de certificação usada para assinar os certificados. Podemos ver 3 opções aqui:

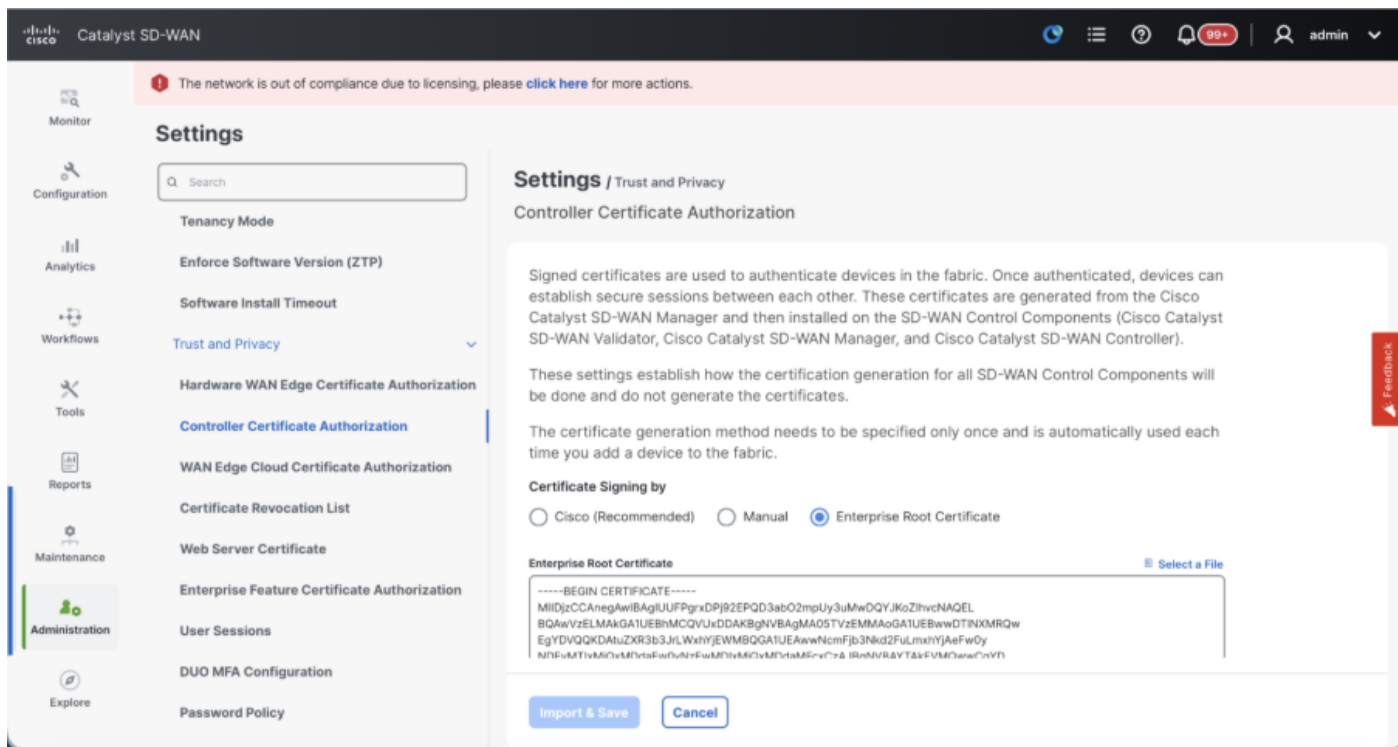
1. Autorização do certificado de borda da WAN de hardware - decide a CA para os roteadores de borda da SD-WAN de hardware.

- On Box Certificate (TPM/SUDI Certificate) - Com essa opção, o certificado pré-instalado no hardware do roteador é usado para estabelecer as conexões de controle (conexões TLS/DTLS)
- Certificado corporativo (assinado pela autoridade de certificação corporativa) - Com essa opção, os roteadores usam certificados assinados pela autoridade de certificação corporativa da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



2. Controller Certificate Authorization - Decide a CA para controladores SD-WAN.

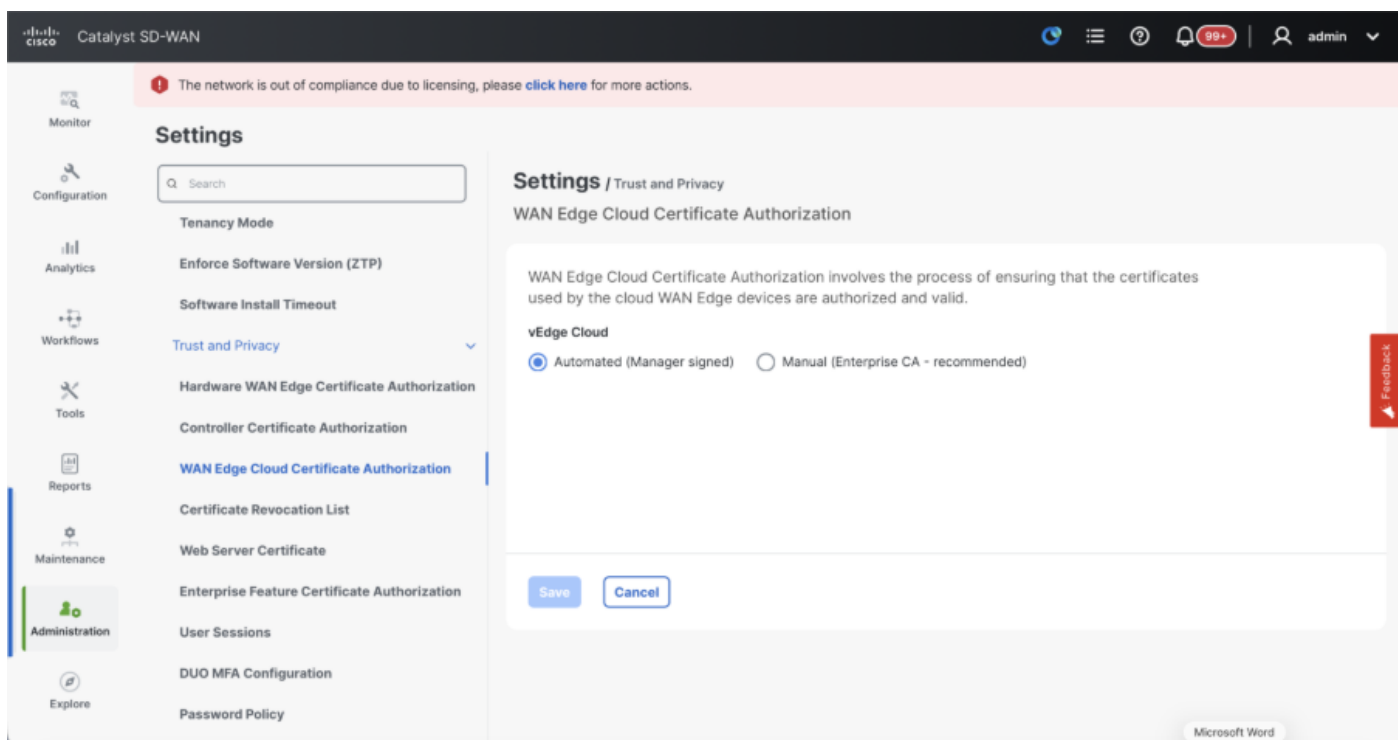
- Cisco (Recomendado) - Os controladores usam os certificados assinados pelo Cisco PKI. O vManage entra em contato automaticamente com o portal PNP usando as credenciais de Smart Account configuradas no vManage e obtém o certificado assinado e é instalado no controlador.
- Manual - Os controladores usam os certificados assinados pela PKI da Cisco. Assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Certificado raiz empresarial - com esta opção, os roteadores usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.



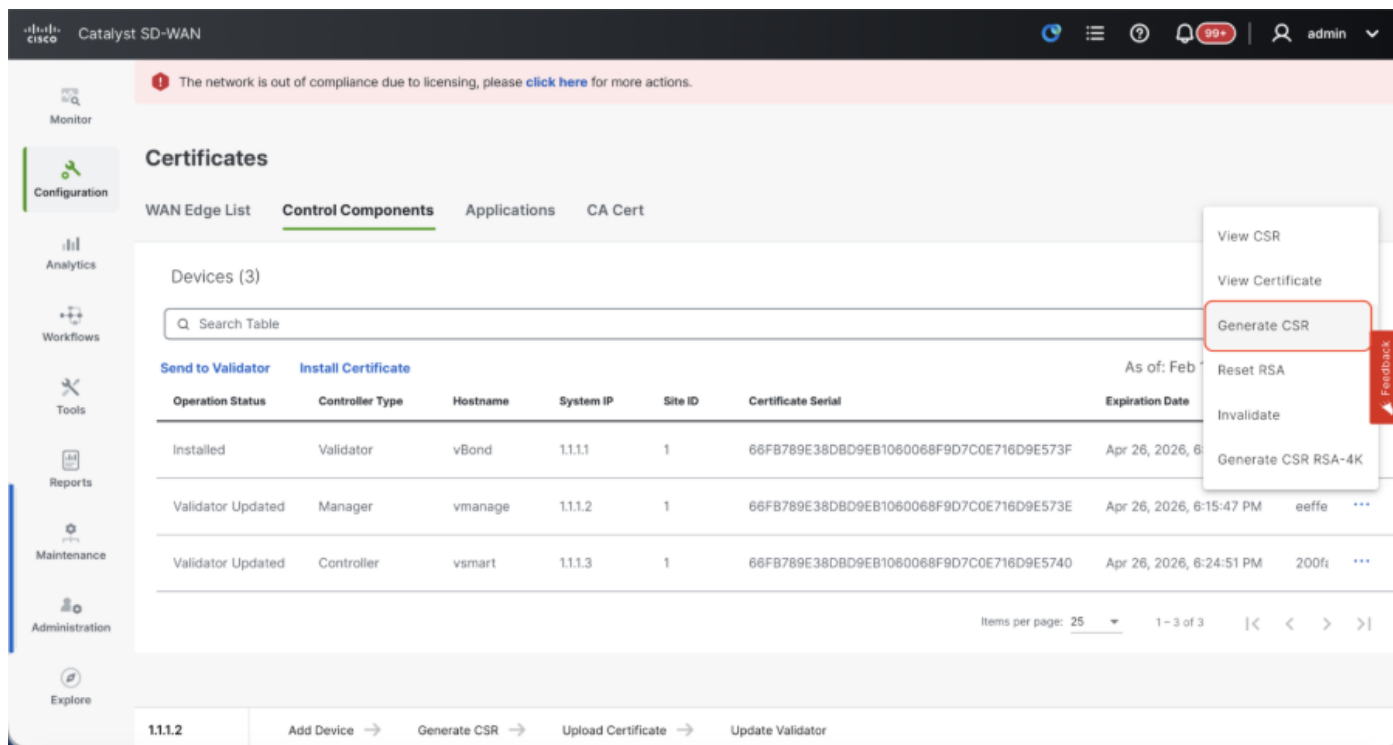
3. Autorização de certificado de nuvem de borda de WAN - decide a CA para roteadores de borda de SD-WAN virtuais (CSR1000v, C8000v, nuvem vEdge)

- Automatizado (vManage assinado) - O vManage assina automaticamente o CSR para os roteadores de borda virtual e instala o certificado no roteador.
- Manual (CA empresarial - recomendado) - Os roteadores virtuais usam certificados assinados pela autoridade de certificação empresarial da sua organização. Ao escolher esta opção, o certificado raiz da CA Corporativa deve ser atualizado aqui.

Caso estejamos usando nossa própria CA, autoridade de certificação empresarial, escolha Empresa.



- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores
- Clique em ... para Gerente/vManage e clique em Gerar CSR.



- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.

Integração do vBond/Validator e vSmart/Controller ao vManage

Navegue para Configuration > Devices > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Onboarding vBond/Validador

- Clique em Add vBond no caso de 20.12 vManage ou Adicionar validador no caso de 20.15/20.18 vManage. Um pop-up é aberto, insira o O IP de transporte VPN 0 de vBond que pode ser acessado a partir do vManage.
- Verifique a acessibilidade usando ping se permitido a partir do CLI de vManage to vBond IP.

- Insira as credenciais de usuário do vBond.



Observação: Precisamos usar credenciais de administrador de VoBond ou uma parte do usuário de netadmingroup. Você pode verificar isso no CLI do vBond. Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vBond



Note: Se o vBond estiver por trás de um dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vBond está traduzido para um IP público. Se o IP da interface VPN 0 não estiver acessível no vManage, use o endereço IP público da interface VPN 0 nesta etapa

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. On the left is a navigation sidebar with options like Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main area is titled 'Devices' and has tabs for 'WAN Edge List', 'Control Components', and 'Unclaimed WAN Edges'. The 'Control Components' tab is active, showing a table with 3 components. A red box highlights the 'Add Validator' button. On the right, the 'Add Validator' dialog box is open, showing fields for 'Validator Management IP Address', 'Username', 'Password', and a 'Generate CSR' dropdown menu set to 'No'. There are 'Cancel' and 'Add' buttons at the bottom right of the dialog.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sync
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se a Cisco (recomendada) for escolhida, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, será instalado no vBond automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN. Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o. O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver várias vBonds, repita as mesmas etapas.

vSmart/controlador integrado:

- Clique em Add vSmart no caso do vManage 20.12 ou Add Controller no caso do vManage 20.15/20.18.
- Um pop-up é aberto, insira o IP de transporte VPN 0 do vSmart que pode ser acessado no vManage.
- Verifique a acessibilidade usando ping se permitido do CLI do vManage para o vSmart IP.
- Insira as credenciais de usuário do vSmart. Observe que precisamos usar credenciais de administrador do vSmart ou uma parte do usuário do grupo netadmin.
- Você pode verificar isso na CLI do vSmart.
- Defina o protocolo como TLS, se pretendemos usar TLS para roteadores para estabelecer conexões de controle com vSmart. Essa configuração também precisa ser configurada na CLI dos nós vSmarts e vManage.
- Escolha Sim no menu suspenso de "Gerar CSR" se precisarmos instalar um novo certificado para vSmart.



Observação: se o vSmart estiver por trás do dispositivo NAT/Firewall, verifique se o IP da interface VPN 0 do vSmart está convertido em um IP público e se o IP da interface VPN 0 não pode ser acessado do vManage, use o endereço IP público do IP da interface VPN 0 nesta etapa.

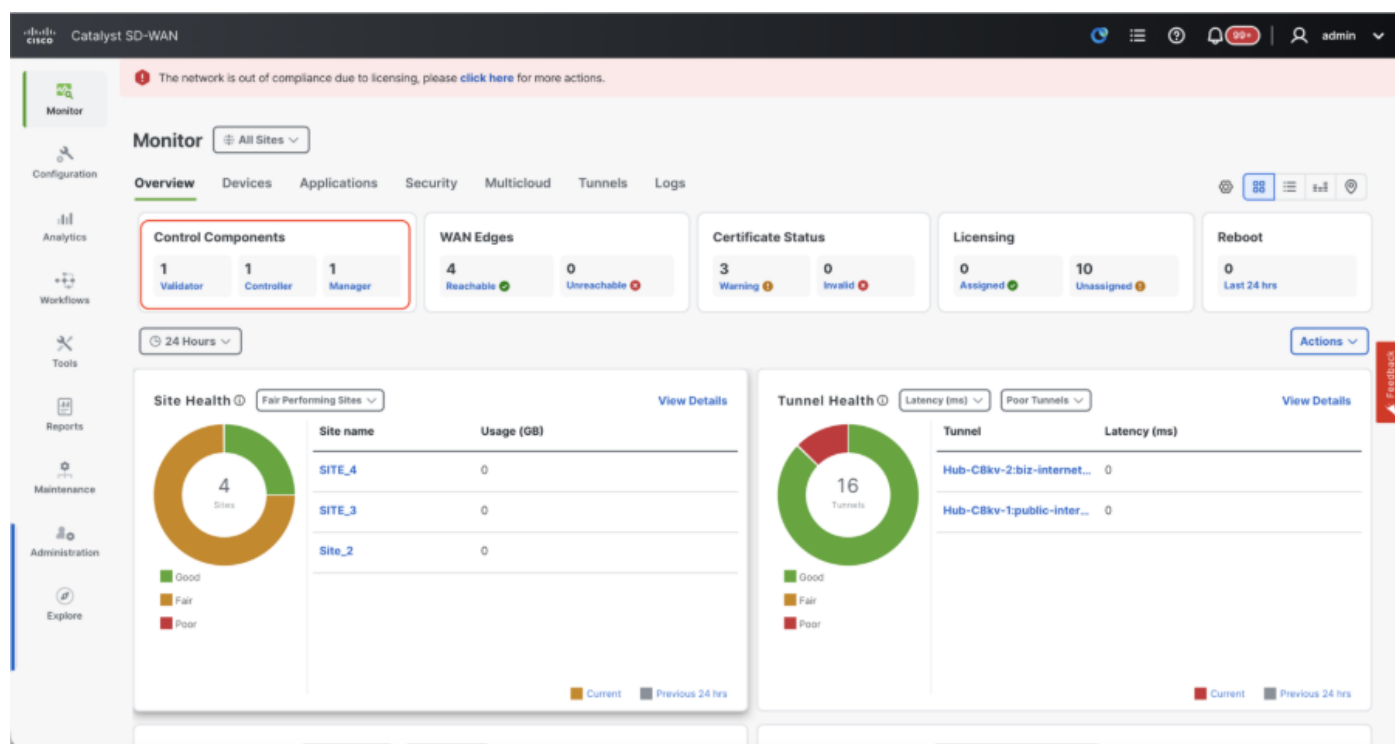
The screenshot displays the Cisco Catalyst SD-WAN vManage interface. The main panel shows the 'Devices' section with a table of 'Control Components (3)'. The table lists three components: a Validator (vBond), a Manager (vmanage), and a Controller (vsmart). The vsmart component is highlighted, showing it is managed by 'Template vSmart-template' and is 'In Sync'. A modal window titled 'Add Controller' is open on the right, allowing the user to configure a new controller. The modal includes fields for 'Controller Management IP Address', 'Username', 'Password', 'Protocol' (set to DTLS), 'Port', and 'Generate CSR' (set to No). A red 'Feedback' button is visible on the right side of the modal. The interface also shows a navigation sidebar on the left with options like Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. A top banner indicates a compliance issue: 'The network is out of compliance due to licensing, please click here for more actions.'

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	Sync
Validator	SITE_1	vBond	No	Unmanaged	In Sync	1.1
Manager	SITE_1	vmanage	No	Unmanaged	In Sync	1.1
Controller	SITE_1	vsmart	Yes	Template vSmart-template	In Sync	1.1

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vSmart automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Se houver vários vSmarts, repita as mesmas etapas.

Verificação

Após concluir todas as etapas, verifique se todos os componentes de controle estão acessíveis em Monitor>Dashboard



- Clique nos respectivos componentes de controle e confirme se todos estão acessíveis.
- Navegue até Monitor > Devices e confirme se todos os componentes de controle estão acessíveis.

The screenshot shows the Catalyst SD-WAN Monitor interface. A notification at the top states: "The network is out of compliance due to licensing, please [click here](#) for more actions." The left sidebar contains navigation options: Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, and Administration. The main content area is titled "Monitor" and shows a "Devices" tab with a "Device Group" dropdown set to "All". Below this is a "Devices (7)" section with a search bar. A table displays the following data:

Hostname	Device Model	Site Name	System IP	Health	Reachability	Control	BFD	TLOC	Up Since	CPU Load	Memory utilization	Act
vBond	Validator	SITE_1	1.1.1.1	✓	↑	14 / 14	N/A	- / -	Jan 13, 2026 11:32 AM	0.79%	13%	...
vmanage	Manager	SITE_1	1.1.1.2	⚠	↑	6 / 6	N/A	8 / 8	Feb 06, 2026 10:07 AM	2.48%	77%	...
vsmart	Controller	SITE_1	1.1.1.3	✓	↑	7 / 7	N/A	2 / 2	Jan 13, 2026 11:33 AM	1.32%	16%	...

Passo 3: Construir cluster vManage

Estrutura SD-WAN integrada com um cluster vManage na sobreposição SD-WAN



Observação: o vManage Cluster pode ser configurado com 3 nós do vManage ou 6 nós do vManage, dependendo do número de locais integrados à malha SD-WAN

Integre todos os controladores SD-WAN com um único nó vManage

Continue com as etapas compartilhadas em "Controladores SD-WAN integrados com um único nó vManage na sobreposição SD-WAN" para ativar primeiro a estrutura SD-WAN com um nó vManage e integrar todos os Validadores (vBond) e Controladores (vSmart) necessários.

Configure as configurações CLI de todos os nós do vManage que fazem parte do cluster

- Configure o restante dos nós do vManage. No caso de um cluster de 3 nós, você tem 2 nós restantes para configurar, no caso de um cluster de 6 nós, você tem 5 nós para configurar.
- Configure as configurações do sistema conforme mostrado:

```
config t
system
host-name
```

```
system-ip
```

site-id

organization-name

vbond

commit



Observação: se estamos usando URL como endereço vBond, certifique-se de configurar os endereços IP do servidor DNS na configuração VPN 0 ou de garantir que eles possam ser resolvidos.

Essas configurações são necessárias para ativar a interface de transporte usada para estabelecer conexões de controle com os roteadores e o restante dos controladores.

```
config t
vpn 0
  dns
```

```
    primary
  dns
```

```
    secondary
interface eth1
  ip address
```

```
tunnel-interface
  allow-service all
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service stun
  allow-service https
!
no shutdown
!
ip route 0.0.0.0/0
```

```
commit
```

Configure também a interface de gerenciamento VPN 512 para permitir o acesso de gerenciamento fora de banda ao controlador.

```
Conf t
vpn 512
  interface eth0
    ip address

    no shutdown
  !
  ip route 0.0.0.0/0
```

```
!
Commit
```

Configuração opcional:

- Você pode consultar as configurações da sua controladora existente e, se a configuração listada aqui estiver presente, poderá adicionar essa configuração às novas controladoras.
- Configure o protocolo de controle como TLS somente se houver um requisito para que os roteadores estabeleçam conexões de controle seguras com os nós do vManage que usam TLS. Por padrão, todos os controladores e roteadores estabelecem uma conexão de controle usando DTLS. Essa é uma configuração opcional necessária apenas nos nós vSmart e vManage, dependendo de sua necessidade.

```
Conf t
security
  control
    protocol tls
commit
```

Configurar a interface de serviço em todos os nós do vManage

Configure a interface de serviço em todos os vManageEnodes, incluindo o vManage-1, que já foi integrado. Essa interface é usada para comunicação de cluster, o que significa comunicação entre os vManagenodes no cluster.

```
conf t
interface eth2
ip address
```

```
no shutdown
commit
```

Certifique-se de que a mesma sub-rede IP seja usada para a interface de serviço em todos os nós no cluster vManagern.

Configurar credenciais do cluster

Podemos usar as mesmas credenciais de administrador dos modosv para configurar o cluster do gerenciamento. Caso contrário, podemos configurar uma nova credencial de usuário que faz parte de netadmin group. As configurações para configurar a credencial do novo usuário são as mostradas

```
conf t
system
aaa
user
```

```
password
```

```
group netadmin
commit
```

Certifique-se de configurar as mesmas credenciais de usuário em todos os nós vManagenodesque fazem parte do cluster. Se decidirmos usar credenciais de administrador, ele deverá ter o mesmo nome de usuário/senha em todos os nós vManagenodes.

Instalar o certificado do dispositivo em todos os nós do vManage

- Faça login na vManageUI de todos os nós de gerenciamento usando a URL <https://<vmanage-ip>> em seu navegador. Use o endereço IP VPN 512 dos respectivos vManagenodes. Você pode fazer login com o nome de usuário e a senha do administrador.
- Navegue para Configuration > Certificates > Control Components no caso de nós 20.15/20.18 vManage. No caso das versões 20.9/20.12, Configuração > Dispositivos > Controladores

Clique em ... para Gerente/vManage e clique em Gerar CSR.

The screenshot displays the Cisco Catalyst SD-WAN web interface. At the top, a notification states: "The network is out of compliance due to licensing, please [click here](#) for more actions." The left sidebar contains navigation icons for Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, and Administration. The main content area is titled "Certificates" and includes tabs for WAN Edge List, Control Components (selected), Applications, and CA Cert. Below the tabs is a search bar and a table of certificates. A context menu is open over the table, showing options: View CSR, View Certificate, Generate CSR (highlighted with a red box), Reset RSA, Invalidate, and Generate CSR RSA-4K. The table has columns: Operation Status, Controller Type, Hostname, System IP, Site ID, Certificate Serial, and Expiration Date. The bottom of the interface shows a breadcrumb trail: 1.1.1.2 > Add Device > Generate CSR > Upload Certificate > Update Validator.

- Depois que o CSR for gerado, você poderá fazer o download do CSR e obtê-lo assinado com base na autoridade de certificado escolhida para os controladores. Você pode verificar essa configuração em Administration > Settings > Controller Certificate Authorization. Se Cisco (recomendado) for escolhido, o CSR será automaticamente carregado no portal PNP pelo vManage e, uma vez assinado o certificado, ele será instalado no vManage automaticamente.
- Se Manual for escolhido, assine manualmente o CSR usando o portal PNP da Cisco navegando até a Smart Account e a Virtual Account da respectiva sobreposição SD-WAN.
- Quando o certificado estiver disponível no portal PNP, clique em instalar certificado na mesma seção do vManage, carregue o certificado e instale-o.
- O mesmo procedimento é aplicável se estivermos usando Digicert e Enterprise Root Certificate.
- Conclua esta etapa em todos os nós do vManage que fazem parte do cluster.

Prepare-se para criar o cluster vManage

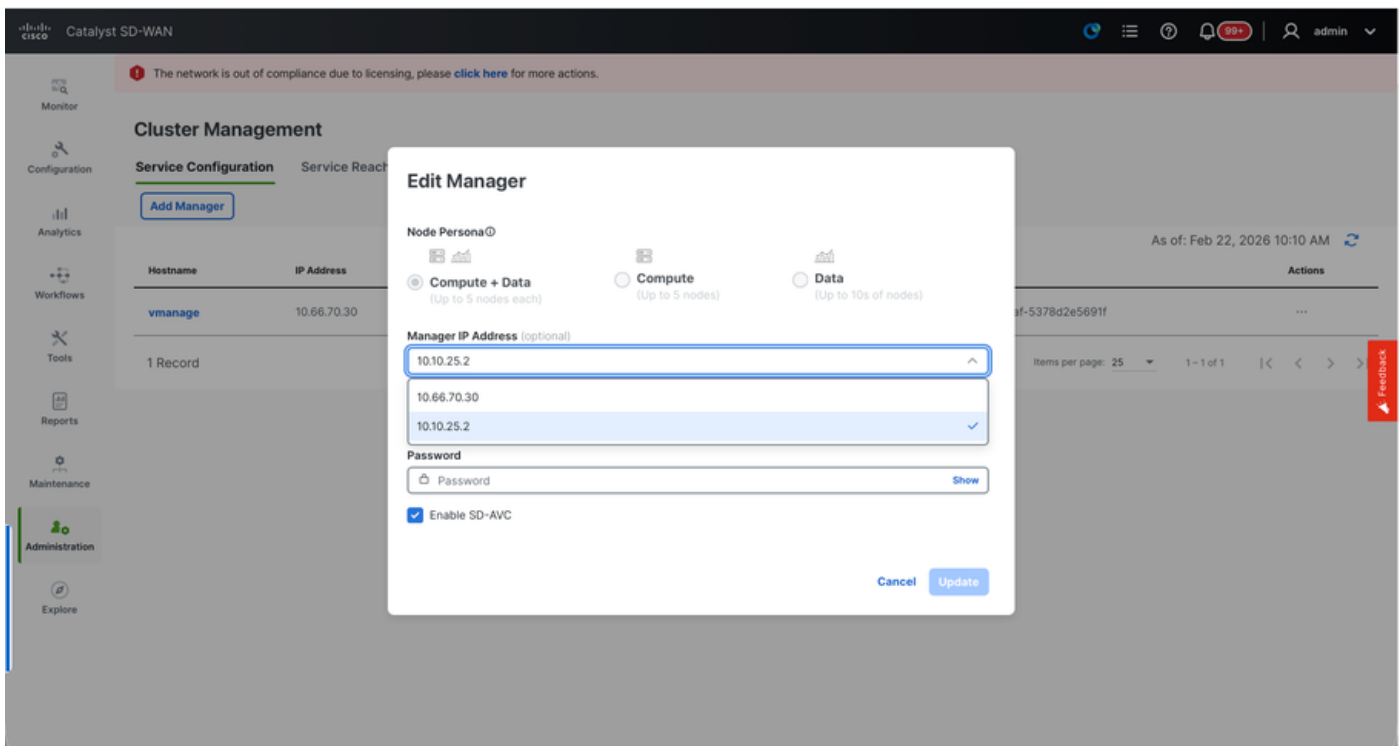
- Na webUI do vManage-1, navegue para Administração > Gerenciamento de cluster, clique em ... em Ações para vManage-1, escolha Editar.
- A persona do nó é escolhida automaticamente com base na persona que escolhemos enquanto a VM estava ativada.



Note: Para um cluster de 3 nós, todos os 3 nós do vManage são ativados com computação+dados como persona. Para um cluster de 6 nós, 3 nós do vManage são

ativados com computação+dados como o persona e 3 nós do vManage são ativados com dados como o persona.

- No menu suspenso do endereço IP do gerente, certifique-se de escolher o IP da interface de serviço do vManage.



- Insira o nome de usuário e a senha que desejamos usar para habilitar o cluster vManage, que é conhecido como credenciais de cluster.
- Como mencionado anteriormente, as mesmas credenciais devem ser configuradas em todos os nós do vManage e devem ser usadas ao adicionar todos os nós ao cluster.

Configuração opcional:

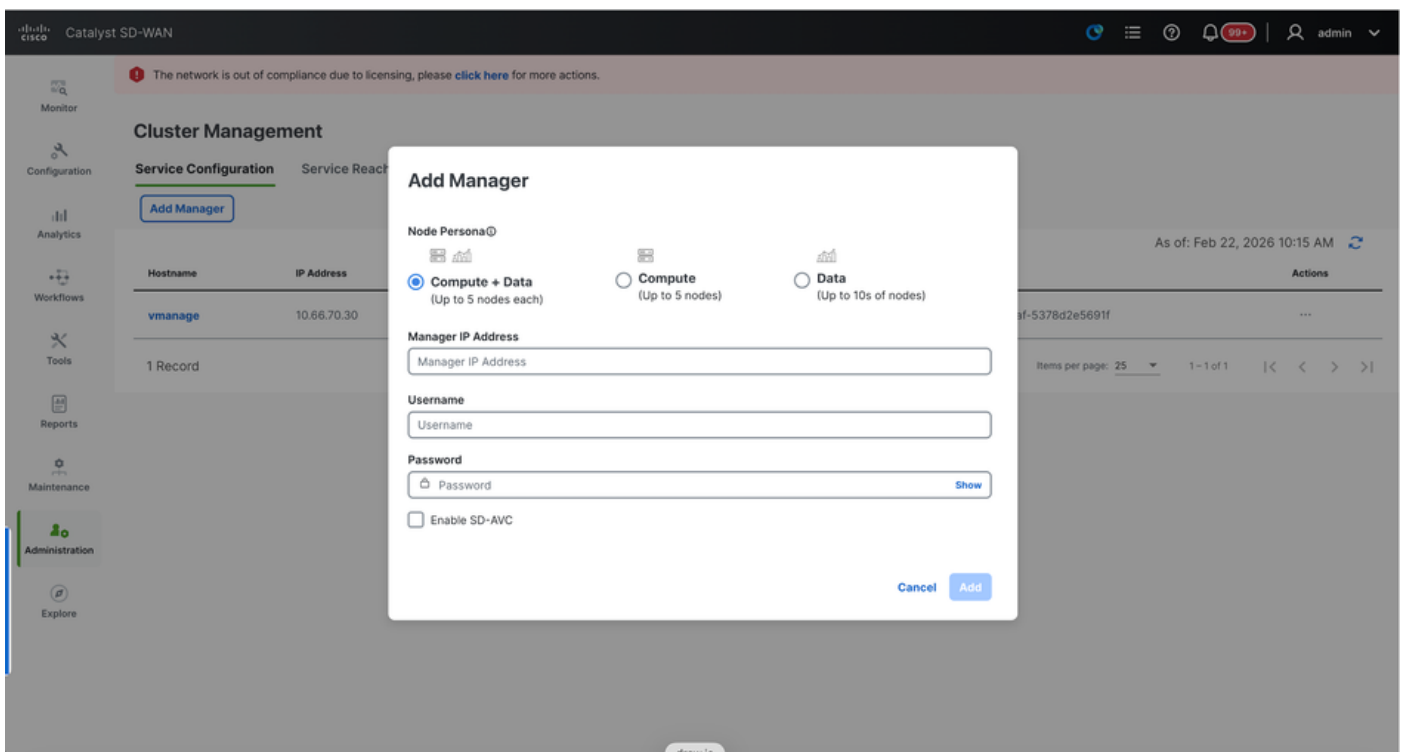
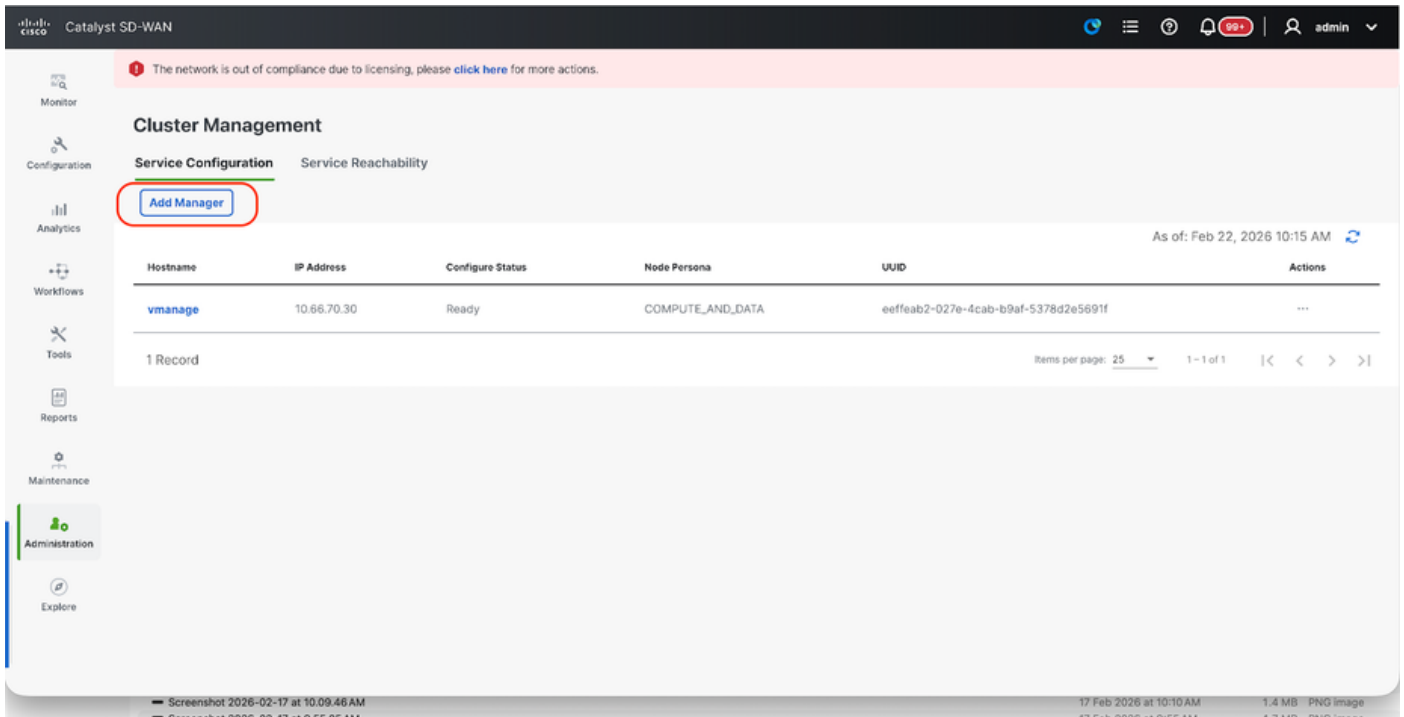
Consulte essa configuração no cluster existente para Habilitar SDAVC - Só precisa ser verificado se for necessário e só é necessário em um nó vManage do cluster.

Clique em Atualizar.

- Depois disso, o serviço vManage NMS é reiniciado em segundo plano e a interface do usuário não fica disponível por alguns minutos, em torno de 5 a 10 minutos. Durante esse período, o acesso do vManage via CLI estará disponível.
- Quando a interface do usuário do vManage-1 estiver acessível, navegue para Administração > Gerenciamento de cluster, certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona é refletido corretamente. Alterne para a seção Alcançabilidade do serviço na mesma página e certifique-se de que todos os serviços estejam acessíveis.
- Se algum dos serviços ainda não estiver acessível, aguarde. Geralmente leva em torno de 20 a 30 minutos.

Construir o cluster vManage

- Na webUI do vManage-1, navegue para Administração > Gerenciamento de cluster, na seção Configuração de serviço,
- Clique em Add Manager, uma janela pop-up será exibida:



- Escolha o Node persona com base nas configurações personalizadas feitas enquanto o nó do vManage - 2 foi girado.
- Insira o IP da interface de serviço do vManage-2 em Endereço IP do gerente
- Insira o nome de usuário e a senha, que são as mesmas credenciais usadas na Etapa 6.

- Ativar SDAVC - Para ser deixado desmarcado, pois já o habilitaríamos no vManage-1
- Clique em Adicionar.
- Depois disso, os serviços NMS do vManage são reiniciados em segundo plano para os nós 1 e 2 do vManage. A interface do usuário não está disponível por alguns minutos, em torno de 5 a 10 minutos, para o vManage 1 e 2.
- Durante esse período, o acesso via CLI do vManage 1 e 2 estará disponível.
- Quando a interface do usuário do vManage-1 estiver acessível, navegue para Administração > Gerenciamento de cluster, certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona esteja refletido corretamente.
- Alterne para a seção Alcance do serviço na mesma página e verifique se todos os serviços estão acessíveis para ambos os nós do vManage.
- Se algum dos serviços ainda não estiver acessível, aguarde. Geralmente leva cerca de 5 a 10 minutos.
- Você pode verificar o status do processo de adição de cluster na lista de tarefas disponível no canto superior direito da interface do usuário do vManage.

The screenshot shows the Cisco Catalyst SD-WAN vManage interface. The top navigation bar includes a red circle around the 'Menu' icon. A red banner at the top states: "The network is out of compliance due to licensing, please click here for more actions." The main content area is titled "Cluster Management" with tabs for "Service Configuration" and "Service Reachability". Under "Service Configuration", there is an "Add Manager" button. Below is a table with columns: Hostname, IP Address, Configure Status, Node Persona, UUID, and Actions. The table contains one record for "vmanage" with IP 10.66.70.30 and status "Ready". The bottom of the table shows "1 Record" and pagination controls.

Hostname	IP Address	Configure Status	Node Persona	UUID	Actions
vmanage	10.66.70.30	Ready	COMPUTE_AND_DATA	eeffea2-027e-4cab-b9af-5378d2e5691f	...

- Você pode procurar a lista de tarefas Ativas e, se a tarefa ainda estiver listada nessa lista, isso indica que a tarefa ainda não foi concluída.
- Você pode clicar na tarefa para verificar o andamento da mesma. Se a tarefa não estiver listada na lista de tarefas Ativas, alterne para Concluído e verifique se a tarefa foi concluída com êxito.
- Somente depois que esses pontos forem validados, vá para a próxima etapa.

Esses pontos precisam ser levados em consideração antes de adicionar o próximo nó ao cluster:

Verifique esses pontos em todas as IUs dos nós do vManage que foram adicionados ao cluster até o momento:

- Navegue para Monitor > Overview da interface do usuário do vManage e verifique se o

número de nós do vManage está refletido corretamente e pode ser visto como acessível, dependendo do número de nós adicionados ao cluster.

- Navegue para Administração > Gerenciamento de cluster e certifique-se de que o IP da interface de serviço do vManage esteja refletido no endereço IP, Configure Status is Ready e node persona esteja refletido corretamente.
- Alterne para a seção Alcance do serviço na mesma página e verifique se todos os serviços estão acessíveis para ambos os nós do vManage.
- Cada vez que um nó é adicionado ao cluster, os serviços NMS de todos os nós no cluster são reiniciados, portanto, a interface do usuário de todos esses nós fica inacessível por algum tempo.
- Dependendo do número de nós no cluster, pode levar mais tempo para que a interface do usuário seja copiada e todos os serviços sejam acessíveis.
- Você pode monitorar a tarefa na Lista de tarefas disponível no canto superior direito da interface do usuário do vManage.
- Na interface do usuário do vManage de cada nó adicionado ao cluster, precisamos ver todos os roteadores, modelos e políticas, se estiverem disponíveis no vManage-1.
- Se essas configurações não estiverem presentes no vManage-1, os vBonds e vSmarts que foram adicionados ao vManage-1 e também Administration > Settings para Organization-name, vBond, Certificate Authorization devem ser refletidos no restante dos nós do vManage adicionados ao cluster.
- Repita as mesmas etapas para o restante dos nós do vManage.

Passo 4: Backup/Restauração do Config-db

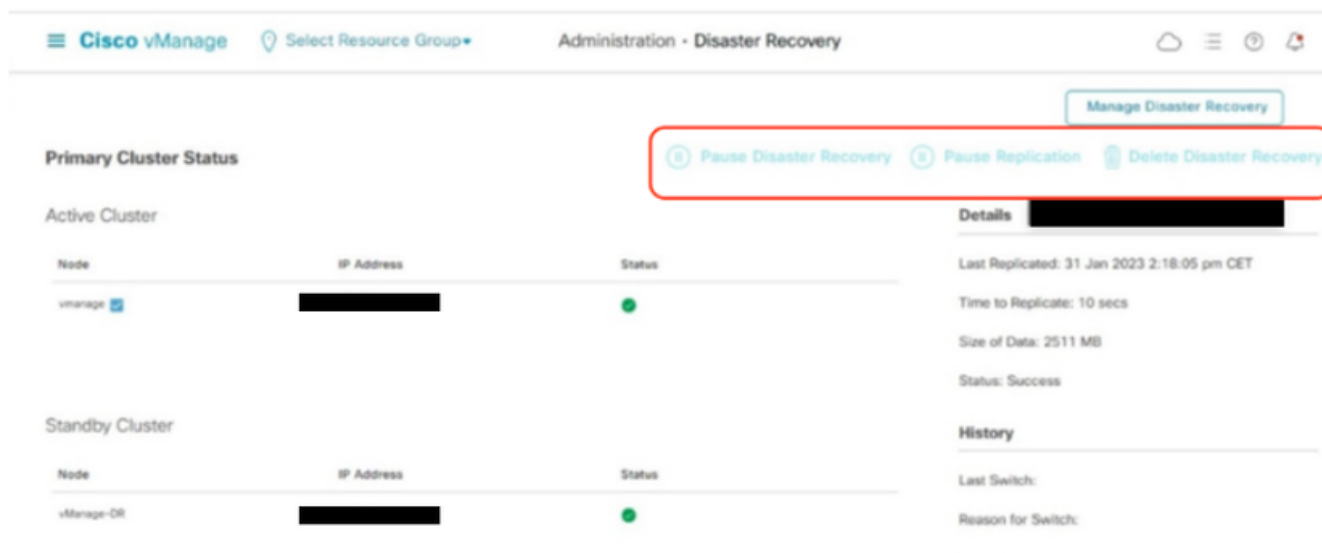
Coletar backup e restauração do banco de dados de configuração do vManage em outro nó do vManage



Note: Ao coletar o backup do banco de dados de configuração do cluster vManage existente que tem a recuperação de desastres ativada, certifique-se de que ele seja coletado após a recuperação de desastres nesse nó ser pausada e excluída.

Confirme se não há replicação de recuperação de desastres em andamento. Navegue até Administração > Recuperação de desastres e verifique o status Sucesso e não em um estado transitório, como Importação pendente, Exportação pendente ou Download pendente. Se o status não for sucesso, entre em contato com o Cisco TAC e certifique-se de que a replicação seja bem-sucedida antes de continuar a pausar a recuperação de desastres.

Primeiro, pause a recuperação de desastres e certifique-se de que a tarefa esteja concluída. Em seguida, exclua a recuperação de desastre e confirme se a tarefa foi concluída.



Entre em contato com o Cisco TAC para garantir que a recuperação de desastres seja limpa com êxito.

Coletar backup do BD de configuração:

- Na estrutura SD-WAN atualmente em uso, é possível gerar backup de configuração-db a partir do cluster vManage.
- Observe que devemos gerar o backup do configuration-db apenas em um nó do cluster vManage, que é o líder do configuration-db.
- No caso do vManage autônomo, o próprio vManage é o líder do banco de dados de configuração.
- No cluster do vManage, identifique o nó do líder configuration-db usando o comando `request nms configuration-db diagnostics`. Você pode executar esse comando em todos os nós do cluster vManage de 3 nós.
- Em um cluster de 6 nós, certifique-se de executar esse comando nos nós vManage onde configuration-db está habilitado para identificar o nó líder. Navegue até Administração > Gerenciamento de cluster para verificar o mesmo:
- Como vemos na captura de tela, os nós configurados com persona COMPUTE_AND_DATA têm configuration-db em execução.

Você pode verificar o mesmo usando o comando `request nms configuration-db status` no vManageCLI. A saída é a mostrada

```
vmanage# request nms configuration-db status
NMS configuration database
  Enabled: true
  Status: running PID:32632 for 1066085s
  Native metrics status: ENABLED
  Server-load metrics status: ENABLED
vmanage#
```

- saída é a seguinte:

```
===== SNIP =====
Connecting to 10.10.10.3...
```

type	row	attributes[row]["value"]
"StoreSizes"	"TotalStoreSize"	85828934
"PageCache"	"Flush"	4268666
"PageCache"	"EvictionExceptions"	0
"PageCache"	"UsageRatio"	0.09724264705882353
"PageCache"	"Eviction"	2068
"PageCache"	"HitRatio"	1.0
"ID Allocations"	"NumberOfRelationshipIdsInUse"	2068
"ID Allocations"	"NumberOfPropertyIdsInUse"	56151
"ID Allocations"	"NumberOfNodeIdsInUse"	7561
"ID Allocations"	"NumberOfRelationshipTypeIdsInUse"	31
"Transactions"	"LastCommittedTxId"	214273
"Transactions"	"NumberOfOpenTransactions"	1
"Transactions"	"NumberOfOpenedTransactions"	441742
"Transactions"	"PeakNumberOfConcurrentTransactions"	11
"Transactions"	"NumberOfCommittedTransactions"	414568
"Causal Cluster"	"IsLeader"	1 >>>>>>>>
"Causal Cluster"	"MsgProcessDelay"	0
"Causal Cluster"	"InFlightCacheTotalBytes"	0

18 rows

```
ready to start consuming query after 388 ms, results consumed after another 13 ms
```

Completed

Connecting to 10.10.10.3...

Displaying the Neo4j Cluster Status

name	aliases	access	address	role	requestedStatus	currentStatus
"neo4j"	[]	"read-write"	"169.254.3.5:7687"	"leader"	"online"	"online"

"neo4j"	[]	"read-write"	"169.254.2.5:7687"	"follower"	"online"	"online"
"neo4j"	[]	"read-write"	"169.254.1.5:7687"	"follower"	"online"	"online"
"system"	[]	"read-write"	"169.254.3.5:7687"	"follower"	"online"	"online"
"system"	[]	"read-write"	"169.254.2.5:7687"	"follower"	"online"	"online"
"system"	[]	"read-write"	"169.254.1.5:7687"	"leader"	"online"	"online"

```

+-----+
6 rows
ready to start consuming query after 256 ms, results consumed after another 3 ms
Completed
Total disk space used by configuration-db:
60M

```

Use esse comando para coletar o backup configuration-db do nó vManage líder configuration-db identificado.

```
request nms configuration-db backup path /opt/data/backup/
```

A saída esperada é a seguinte:

```

vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#

```

- Anote as credenciais do configuration-db se ele tiver sido atualizado.
- Se você não souber as credenciais do configuration-db, entre em contato com o TAC para recuperar as credenciais do configuration-db dos nós vManage existentes.
- As credenciais padrão do configuration-db são nome de usuário: neo4j e senha: senha

Restaurar backup do banco de dados de configuração para outro nó do vManage

Copie o backup do configuration-db para o diretório /home/admin/ do vManage usando SCP.

Exemplo de saída do comando scp:

```

XXXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1

```

```
(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Para restaurar o backup do configuration-db, primeiro precisamos configurar as credenciais do configuration-db. Se suas credenciais de configuração-db forem default (neo4j/password), podemos pular esta etapa.

Para configurar as credenciais do configuration-db, use o comando `request nms configuration-db update-admin-user`. Use o nome de usuário e a senha de sua escolha.

Observe que o servidor de aplicativos do vManage é reiniciado. Devido ao qual a interface do usuário do vManage fica inacessível por um curto período.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operation on other nodes)
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Post que podemos continuar para restaurar o backup do configuration-db:

Podemos usar o comando `request nms configuration-db restore path /home/admin/< >` para restaurar o configuration-db para o novo vManage:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Resetting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
```

```
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Depois que o configuration-db for restaurado, verifique se a interface do usuário do vManage está acessível. Aguarde cerca de 5 minutos e tente acessar a interface do usuário.

Depois de fazer login na interface do usuário com êxito, verifique se a lista de roteadores de borda, o modelo, as políticas e todas as configurações presentes na interface do usuário do vManage anterior ou existente estão refletidas na nova interface do usuário do vManage.

Passo 5: Ativar a recuperação de desastres em um cluster vManage

Pré-verificações importantes

Dois clusters de três nós do vManage separados devem ser configurados e estar operacionais para prosseguir com a recuperação de desastres. No cluster ativo, você deve ter validadores e controladores integrados. Caso você tenha o validador e os controladores no local do DR, eles também devem ser integrados no cluster ativo e não no cluster do DR vManage.

A Cisco recomenda que, antes de registrar a recuperação de desastres, estes requisitos devem ser atendidos:

- Certifique-se de que o nó primário e o secundário estejam acessíveis por HTTPS em uma VPN de transporte (VPN 0).
- Certifique-se de que os Cisco vSmart Controllers e Cisco vBond Orchestrators na configuração secundária estejam conectados à configuração principal.
- Verifique se o nó primário e o nó secundário do Cisco vManage estão executando a mesma versão do Cisco vManage.
- Interface de cluster fora de banda (interface de serviço) na VPN 0.
- Para cada instância do vManage em um cluster, é necessária uma terceira interface (link de cluster) além das interfaces usadas para VPN 0 (transporte) e VPN 512 (gerenciamento).
- Essa interface é usada para comunicação e sincronização entre os servidores vManage no cluster.
- Essa interface deve ter pelo menos 1 Gbps e uma latência de 4 ms ou menos. Recomenda-se uma interface de 10 Gbps.
- Ambos os nós do vManage devem ser capazes de alcançar um ao outro por meio dessa interface: seja um segmento da camada 2 ou através do roteamento da camada 3.
- Em cada vManage, essa interface deve ser configurada na GUI como uma interface de cluster (Administração > Gerenciamento de cluster- indique o próprio endereço IP, usuário e

senha da interface de cluster fora da banda).

- Para permitir que os nós do Cisco vManage se comuniquem entre si em data centers, ative as portas TCP 8443 e 830 em seus firewalls de data center.
- Verifique se todos os serviços (servidor de aplicativos, configuração-db, servidor de mensagens, servidor de coordenação e estatística-db) estão habilitados em ambos os nós do Cisco vManage.
- Distribua todos os controladores, incluindo os Cisco vBond Orchestrators, em data centers primários e secundários. Verifique se esses controladores podem ser acessados pelos nós do Cisco vManage que estão distribuídos nesses data centers. Os controladores se conectam apenas ao nó principal do Cisco vManage.
- Certifique-se de que nenhuma outra operação esteja em andamento no nó ativo (principal) e no nó standby (secundário) do Cisco vManage. Por exemplo, certifique-se de que nenhum servidor esteja no processo de atualização ou anexação de modelos aos dispositivos.
- Desative o servidor proxy HTTP/HTTPS do Cisco vManage se ele estiver ativado. Consulte [Servidor Proxy HTTP/HTTPS para Comunicação do Cisco vManage com Servidores Externos](#). Se você não desativar o servidor proxy, o Cisco vManage tentará estabelecer comunicação de recuperação de desastres por meio do endereço IP do proxy, mesmo que os endereços IP do cluster fora de banda do Cisco vManage sejam diretamente acessíveis. Você pode reativar o servidor proxy HTTP/HTTPS do Cisco vManage após a conclusão do registro de recuperação de desastres.
- Antes de iniciar o processo de registro de recuperação de desastres, navegue para a janela Tools > Rediscover Network no nó principal do Cisco vManage e redescubra os Cisco vBond Orchestrators.

Configurações

Para obter mais informações sobre o vManage Disaster Recovery, consulte [este](#) link.

Os dois clusters de 3 nós separados já foram criados, supondo que cada gerenciador de SD-WAN tenha uma configuração mínima e que a parte de certificação esteja concluída.

Navegue para Administração > Gerenciamento de cluster em ambos os clusters e verifique se todos os nós estão no estado pronto.

DC vManage

Cisco Catalyst SD-WAN Administration - Cluster Management				
Service Configuration Service Reachability				
Add Manager				
Hostname	IP Address	Configure Status	Node Persona	UUID
vmanage1		Ready	COMPUTE_AND_DATA	cb87a08e-079e-4394-81c3-e63c36ac22c0
vmanage2		Ready	COMPUTE_AND_DATA	86c6c314-baca-40e7-a72c-94a3e6be9d61
vmanage3		Ready	COMPUTE_AND_DATA	4a27ea41-3e1f-447c-baad-f6c3d07994d

DR vmanage

Cisco Catalyst SD-WAN Administration - Cluster Management				
Service Configuration Service Reachability				
Add Manager				
Hostname	IP Address	Configure Status	Node Persona	UUID
DR-vmanage1		Ready	COMPUTE_AND_DATA	d78832e5-e6d3-4b6b-bf61-f923cf3c7282
DR-vmanage3		Ready	COMPUTE_AND_DATA	b4f5f345-f2e-48ec-b8f0-0be92427cc28
DR-vmanage2		Ready	COMPUTE_AND_DATA	c3e303a2-53d0-4525-901b-d96e9ce92875

Navegue até Administração>Recuperação de desastres do vManage Cluster principal. Clique em Manage Disaster Recovery.

Select Resource Group ▾

Administration • Disaster Recovery

Cluster Status

Active Cluster

Node	IP Address	Status
Disaster Recovery Not Configured		

Standby Cluster

Node	IP Address	Status
Disaster Recovery Not Configured		

Arbitrator

Node	IP Address	Status
------	------------	--------

Manage Disaster Recovery

Manage Password

Pause Disaster Recovery

Pause Replication

Delete Disaster Recovery

Details

Last Import:

Time to Import:

Size of Data:

Status:

History

Last Switch:

Reason for Switch:

Schedule

Replication Interval:

Switchover Threshold:

Na janela pop-up, preencha os detalhes do vManage principal e secundário.

Os endereços IP a serem indicados são os endereços IP das interfaces de cluster fora da banda. De preferência, use o endereço IP da interface de serviço VPN 0 do vManage-1 em cada um dos clusters.

As credenciais devem ser as de um usuário netadmin e não devem ser alteradas após a configuração do DR, a menos que ele seja excluído. Uma credencial de usuário local do vManage separada para recuperação de desastres pode ser usada. Precisamos verificar se o usuário local do vManage faz parte do grupo netadmin. Até mesmo as credenciais de

administrador podem ser usadas aqui.

Manage Disaster Recovery ×

● Connectivity Info

● Validator Info

● Recovery Mode

● Replication Schedule

Active Cluster

IP*

Username*

Password*

Standby Cluster

IP*

Username*

Password*

Next

Cancel

Depois de preenchido, clique em Avançar.

- Preencha os detalhes dos controladores vBond.

Os controladores vBond devem estar acessíveis no endereço IP especificado via Netconf.

Manage Disaster Recovery

Connectivity Info

Validator Info

Recovery Mode

Replication Schedule

vBond Information

IP10.105.60.104

User Nameadmin

Password

Back

Next

Cancel

Depois de preenchido, clique em Avançar.

- No Modo de recuperação, escolha Manual. O modo de Automação foi preterido. Clique em Next.

Manage Disaster Recovery



Select Recovery Mode

- ☒ Manual ☐ Automation

[Back](#)

[Next](#)

[Cancel](#)

Manage Disaster Recovery

✓ Connectivity Info
✓ Validator Info
✓ Recovery Mode
● Replication Schedule

Start Time

12:00

AM

Replication Interval

15 mins

Back
Save
Cancel

Defina o valor e clique em Salvar.

- O registro do DR começa agora. Clique no botão atualizar para atualizar manualmente o estado e os logs de andamento. Esse processo pode levar de 20 a 30 minutos.

Cisco Catalyst SD-WAN
Select Resource Group
Administration - Disaster Recovery

Disaster Recovery Registration
Total Task: 1 | Success: 1
Device Group (1)
Search Table

Status	Chassis Number	Hostname	Message
Success	-	-	Data Centers Regist

View Logs

[4-Jul-2025 4:38:41 UTC] [4-Jul-2025 4:33:03 UTC] Restarting Vmanage 89.89.89.5
[4-Jul-2025 4:38:41 UTC] [4-Jul-2025 4:33:22 UTC] Restart initiated. Waiting for Vmanage 89.89.89.5 to come up.
[4-Jul-2025 4:38:41 UTC] [4-Jul-2025 4:36:03 UTC] Vmanage 89.89.89.5 has successfully restarted.
[4-Jul-2025 4:38:41 UTC] [4-Jul-2025 4:36:03 UTC] 2 vmanages have successfully registered and restarted. Restarting current vmanage 89.89.89.4
[4-Jul-2025 4:38:42 UTC] Restarting Primary DC
[4-Jul-2025 4:38:42 UTC] Restarting Local DataCenter
[4-Jul-2025 4:38:42 UTC] Restarting Vmanage 89.89.89.3
[4-Jul-2025 4:39:02 UTC] Restart initiated. Waiting for Vmanage 89.89.89.3 to come up.
[4-Jul-2025 4:40:13 UTC] Vmanage 89.89.89.3 has successfully restarted.
[4-Jul-2025 4:40:13 UTC] Restarting Vmanage 89.89.89.2
[4-Jul-2025 4:43:34 UTC] Restart initiated. Waiting for Vmanage 89.89.89.2 to come up.
[4-Jul-2025 4:52:36 UTC] Vmanage 89.89.89.2 has successfully restarted.
[4-Jul-2025 4:52:40 UTC] 2 vmanages have successfully registered and restarted. Restarting current vmanage 89.89.89.1

Close

Verificação

Navegue até Administração>Recuperação de desastres para ver o status da Recuperação de desastres e quando os dados foram replicados pela última vez.



Note: A replicação pode levar várias horas, dependendo do tamanho do banco de dados. Além disso, pode exigir alguns ciclos para obter uma replicação bem-sucedida.

Passo 6: Reautenticação de controladores e invalidação de controladores antigos

Depois que o configuration-db for restaurado, precisamos autenticar novamente todos os novos controladores (vmanage/vsmart/vbond) na malha



Observação: na produção real, se o IP da interface usado para reautenticar for o IP da interface do túnel, será necessário garantir que o serviço NETCONF seja permitido na interface do túnel do vManage, vSmart e vBond e também nos firewalls ao longo do caminho. A porta de firewall a ser aberta é a porta TCP 830 como regra bidirecional do cluster DR para todos os vBonds e vSmarts .

Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers

- Clique nos três pontos próximos a cada controlador e clique em Editar

The screenshot shows the Cisco Catalyst SD-WAN Configuration - Devices page. The 'WAN Edge List' tab is active, displaying a table of controllers. On the right, the 'Edit' form is open, showing fields for IP Address, Username, and Password.

Controller Type	Site Name	Hostname	Config Locked	Managed By	Device Status	System-ip	Draft Mode	Certificate Status	Policy Name	Policy Version
vbond	SITE_300	vedge	No	Unmanaged	In Sync	3.3.3.3	Disabled	Installed	-	-
vmanage	SITE_300	vmanage1-20121	No	Unmanaged	In Sync	1.1.1.1	Disabled	Installed	-	-
vmanage	SITE_300	vmanage2-20121	No	Unmanaged	In Sync	1.1.1.2	Disabled	Installed	-	-
vmanage	SITE_300	vmanage3-20121	No	Unmanaged	In Sync	1.1.1.3	Disabled	Installed	-	-
vsmart	SITE_300	vsmart	No	Unmanaged	In Sync	2.2.2.2	Disabled	Installed	-	-

- Substitua ip-address (system-ip do controlador) pelo endereço ip transport vpn 0(tunnel interface) .Insira o nome de usuário e a senha e clique em save
- Faça o mesmo para todos os novos controladores na malha

Sincronizar a cadeia de certificados raiz

Depois que todos os controladores estiverem integrados, conclua esta etapa:

Em qualquer servidor Cisco SD-WAN Manager no cluster recém-ativo, execute estas ações:

Digite este comando para sincronizar o certificado raiz com todos os dispositivos Cisco Catalyst SD-WAN no cluster recém-ativo:

<https://vmanage-url/dataservice/system/device/sync/rootcertchain>

Digite este comando para sincronizar o UUID do Cisco SD-WAN Manager com o Cisco SD-WAN Validator:

<https://vmanage-url/dataservice/certificate/syncvbond>

Depois que a estrutura for restaurada e as sessões de controle e bfd estiverem ativas para todas as bordas e controladores na estrutura, precisamos invalidar os controladores antigos (vmanage/vsmart/vbond) da interface do usuário

- Na interface do usuário do vmanage, clique em Configuration > Devices > Certificates
- Clique em Controladores
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em invalidar
- Clique em enviar para vbond
- Na interface do usuário do vmanage, clique em Configuration > Devices > Controllers
- Clique nos três pontos próximos ao controlador (vmanage/vsmart/vbond) da estrutura antiga. Clique em Excluir

Pós-cheques

Essas pós-verificações se aplicam a todas as combinações de implantação.

Reativar roteadores de Borda da nuvem:

- Se o C8000v fizer parte da sobreposição e tiver o vmanaged assinado, ele precisará ser autenticado novamente, ou seja:

```
request platform software sdwan vedge_cloud activate chassis-number
```

token

- Confirmar se as conexões de controle e as sessões BFD estão ativas
- Confirme se o tráfego do aplicativo está fluindo de ponta a ponta
- Se foram feitas alterações no port-hop antes da reconstrução da estrutura nas bordas, elas devem ser revertidas
- Verifique se os itens aparecem como esperado:
 - Modelos
 - Políticas
 - Página Dispositivo (ambas as guias)Lista de WAN vEdgeControladores

vManage pós-verificações

- Aplicável para nós vManage:

Verificações de Configuration-DB(Neo4j):

Execute o comando "request nms configuration-db diagnostics" em todos os nós do vManage:

1. Verificar o status do Nó on-line e de Liderança:(não disponível para todas as versões)

Displaying the Neo4j Cluster Status

name	aliases	access	address	role	requestedStatus	currentStatus	error	default	home
"neo4j"	[""]	"read-write"	"169.254.1.5:7687"	"leader"	"on-line"	"on-line"	""	TRUE	TRUE
"neo4j"	[""]	"read-write"	"169.254.3.5:7687"	"follower"	"on-line"	"on-line"	""	TRUE	TRUE
"neo4j"	[""]	"read-write"	"169.254.2.5:7687"	"follower"	"on-line"	"on-line"	""	TRUE	TRUE
"system"	[""]	"read-write"	"169.254.1.5:7687"	"follower"	"on-line"	"on-line"	""	FALSE	FALSE
"system"	[""]	"read-write"	"169.254.3.5:7687"	"follower"	"on-line"	"on-line"	""	FALSE	FALSE
"system"	[""]	"read-write"	"169.254.2.5:7687"	"leader"	"on-line"	"on-line"	""	FALSE	FALSE

"Neo4j" deve mostrar 3 nós online e 1 líder e 2 seguidores. "system" também deve mostrar 3 nós on-line e 1 líder e 2 seguidores, no entanto, como este não é o Db padrão, o sinalizador padrão é false. Se houver menos de 3 entradas em cada neo4j e o sistema significa que o nó caiu do cluster. Entre em contato com o TAC da Cisco para solucionar o mesmo problema.

2. Verifique se algum nó está em "quarentena".

```
#####
#####
Running quarantine check
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Check if Neo4j Nodes are Quarantined
None of the neo4j nodes is quarantined
None of the neo4j nodes is quarantined
None of the neo4j nodes is quarantined
#####
```

Nenhum dos nós deve estar em estado de quarentena.

3. A validação do esquema deve ser "bem-sucedida".

```
#####
Running schema violation pre-check script
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Validating Schema from the configuration-db
Successfully validated configuration-db schema
written to file /opt/data/containers/mounts/upgrade-coordinator/schema.json
Contents of /opt/data/containers/mounts/upgrade-coordinator/schema.json:
{
  "check_name": "Validating configuration-db admin names",
  "check_result": "SUCCESSFUL",
  "check_analysis": "Successfully validated configuration-db schema",
  "check_action": ""
}
#####
#####
```

4. Colete um backup configuration-db usando o comando "request nms configuration-db diagnostics" e certifique-se de que ele seja bem-sucedido.

```
vmanage_2013# request nms configuration-db backup path /opt/data/backup/9thSepBackup.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/9thSepBackup.tar.gz.tar.gz
sha256sum: 9d43addcf6c43f18c32b833295a6318fa0a63a7bf7456965140dcb9a61118b5e
Removing the temp staging dir :/opt/data/backup/staging
vmanage_2013# █
```

Se houver qualquer inconsistência ou erro, entre em contato com o TAC da Cisco para solucionar problemas.

Como alternativa, podemos executar essas chamadas de API para confirmar o status do nó vmanage de um cluster (para todos os nós COMPUTE+DATA) - funciona somente na versão 20.12 e posterior

```
go to vshell of the vmanage node ( to be done on all vmanages)
=====
curl -u
```

:

```

-H "Content-Type: application/json" -d '{"statements":[{"statement":"call dbms.cluster.over
:7474/db/neo4j/tx/commit | jq -r
curl -u
:

```

```

-H "Content-Type: application/json" -d '{"statements":[{"statement":"show databases"}]}'
:7474/db/neo4j/tx/commit | jq -r

```

Certifique-se de que em um cluster tenha apenas um líder para o neo4j e o sistema e resto como seguidores .Certifique-se de que todos os nós estão on-line .Se você tem cluster de 3 nós (todos os três são COMPUTE+DATA),deve haver apenas um líder para o neo4j e o sistema .Qualquer desvio, você deve entrar em contato com o TAC

5. Verifique se há erros de disco, memória e E/S em /var/log/kern.log. Isso precisa ser verificado em todos os nós do vManage.

6. Verifique a etapa ao formar um cluster novo para vmanage que não tem CC entre cada nó Execute ssh como vmanage-admin do nó 1 para o ip do cluster de outros nós e vice-versa, para verificar se a chave pública é trocada e a senha menos ssh está funcionando [O token de consentimento é necessário para as etapas mostradas aqui]

```
DR-vManage-1:~# ssh -i /etc/viptela/.ssh/id_dsa -p 830 vmanage-admin@
```

```
The authenticity of host '[192.168.50.5]:830 ([192.168.50.5]:830)' can't be established.
ECDSA key fingerprint is SHA256:rSpscoYCVc+yiFUMHVT1xtjqmyrZSFg93msFdoSUieQ.
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.50.5]:830' (ECDSA) to the list of known hosts.
viptela 20.9.3.0.31
```

Password:

Caso a saída solicite a inserção da senha, entre em contato com o TAC

Verificações de post do controlador:

Aplicável a todos os controladores SD-WAN (vBond, vManage, vSmart):

Execute os comandos em todos os controladores na sobreposição e confirme se o vManage UUID e os números de série vistos são válidos para a estrutura atual:

Comandos vBond:

```
show orchestrator valid-vsmarts
```

```
show orchestrator valid-vmanage-id
```

Comandos vManage/vSmart:

```
show control valid-vsmarts
```

```
show control valid-manage-id
```

Observe que a saída de `show control valid-vsmarts` inclui os números de série dos nós vSmarts e vManage.

Compare-o com os vistos na interface do usuário do vManage. Navegue até a seção Configuração > Certificados > Controladores.

Se forem vistas entradas adicionais para o UUID/número de série que não estão atualmente integrados à estrutura, devemos excluí-los. Você pode entrar em contato com o TAC da Cisco para o mesmo.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.