

Recuperação de desastres de cluster de 3 nós do Cisco SDWAN Manager

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificação](#)

[Como verificar o nó líder de replicação?](#)

[Atualização da senha do Validator \(vBond\) após o registro da recuperação de desastres](#)

[Atualizar Senha do Validator \(vbond\)](#)

[Adicionando novo validador \(vBond\) à sobreposição após o registro de recuperação de desastres](#)

[Atualizar sobreposições de recuperação de desastres](#)

[Antes de Começar](#)

[Processo de atualização](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a natureza stateful do Cisco vManage e seu roteador designado (DR) principal/secundário, permitindo failover manual com replicação automática de dados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento dos clusters de 3 nós do vManage. 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 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 até a janela Tools > Rediscover Network no nó principal do Cisco vManage e redescubra os Cisco vBond Orchestrators.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Gerenciador: 20.12.5
- Validador: 20.12.5
- Controlador: 20.12.5
- Borda: 17.12.5

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.

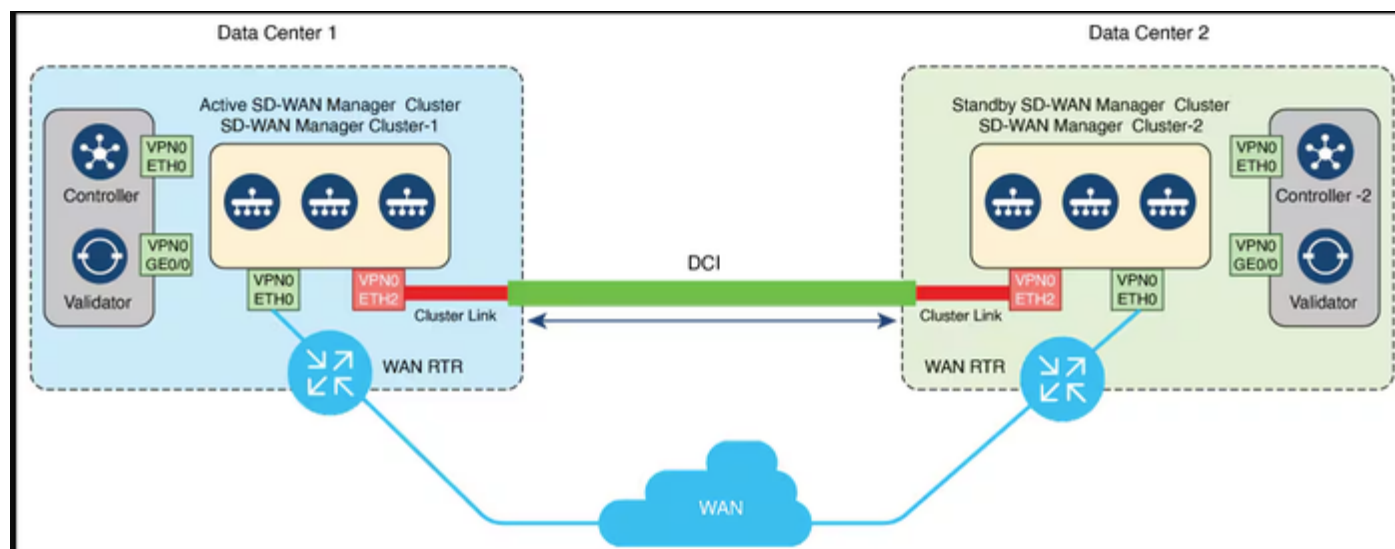
Informações de Apoio

A recuperação de desastres fornece um processo de failover acionado pelo administrador. Quando a recuperação de desastres é registrada, os dados são replicados automaticamente entre os clusters Cisco vManage primário e secundário. Você executa manualmente um failover para o cluster secundário, se necessário.

Configurar

Diagrama de Rede

Esta figura ilustra a arquitetura avançada da solução de recuperação de desastres com um cluster de três nós.



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.

```
vmanage2# show run system
system
host-name                vmanage2
system-ip                 11.11.11.2
site-id                   1001
admin-tech-on-failure
no vrrp-advt-with-physmac
sp-organization-name     AAMIR-405707
organization-name        AAMIR-405707
upgrade-confirm           15
vbond 10.105.60.104
```

```
vpn 0
interface eth0
ip address 10.105.60.102/24
ipv6 dhcp-client
tunnel-interface
no allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
allow-service ntp
no allow-service stun
no allow-service https
!
no shutdown
!
interface eth1
ip address 89.89.89.2/24
no shutdown
!
ip route 0.0.0.0/0 10.105.60.1
!
vpn 512
interface eth2
ip address 10.105.60.192/24
no shutdown
!
ip route 0.0.0.0/0 10.105.60.1
!
vmanage2# show interface
```

VPN	INTERFACE	AF	IP ADDRESS	IF ADMIN STATUS	IF OPER STATUS	IF TRACKER STATUS	ENCAP TYPE	PORT TYPE	MTU	HWADDR	SPEED MBPS	DUPLEX	TCP MSS ADJUST	UPTIME	RX PACKETS	TX PACKETS
0	eth0	ipv4	10.105.60.102/24	Up	Up	-	null	transport	-	00:0c:29:c0:37:03	1000	full	-	1:01:17:03	8806472	496731
0	eth1	ipv4	89.89.89.2/24	Up	Up	-	null	service	-	00:0c:29:c0:37:0d	1000	full	-	1:01:16:59	16382852	15748084
0	system	ipv4	11.11.11.2/32	Up	Up	-	null	loopback	-	-	1000	full	-	1:01:20:06	0	0
0	docker0	ipv4	-	Down	Down	-	null	service	-	02:42:fb:fd:d4:86	1000	full	-	-	9	21
0	cbr-vmanage	ipv4	-	Down	Up	-	-	-	-	02:42:c9:f5:28:c7	1000	full	-	-	-	-
512	eth2	ipv4	10.105.60.192/24	Up	Up	-	null	mgmt	-	00:0c:29:c0:37:17	1000	full	-	1:01:16:59	994009	11814

- 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

Select Resource Group

Administration • Cluster Management

Service Configuration

Service Reachability

Add Manager

Hostname	IP Address	Configure Status	Node Persona	UUID	
vmanage1	89.89.89.1	Ready	COMPUTE_AND_DATA	cb87a08e-079e-4394-81c3-e63c36ac22c0	...
vmanage2	89.89.89.2	Ready	COMPUTE_AND_DATA	8dc6c314-baca-40e7-a72c-94a3ebbe9d61	...
vmanage3	89.89.89.3	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	89.89.89.4	Ready	COMPUTE_AND_DATA	d78832e5-e6d3-4b6b-bf61-f923cf3c7282
DR-vmanage3	89.89.89.6	Ready	COMPUTE_AND_DATA	bf45f345-f2e-48ec-b8fd-0bb92427cc28
DR-vmanage2	89.89.89.5	Ready	COMPUTE_AND_DATA	c3e303a2-53d0-4525-901b-d96e9ce92875

- Navegue até Administração>Recuperação de desastres. Clique em Manage Disaster Recovery.

Cisco Catalyst SD-WAN

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.

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.

Manage Disaster Recovery

Connectivity Info

Validator Info

Recovery Mode

Replication Schedule

Active Cluster

IP*

89.89.89.1

Username*

admin

Password*

.....

Standby Cluster

IP*

89.89.89.4

Username*

admin

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 Register

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.

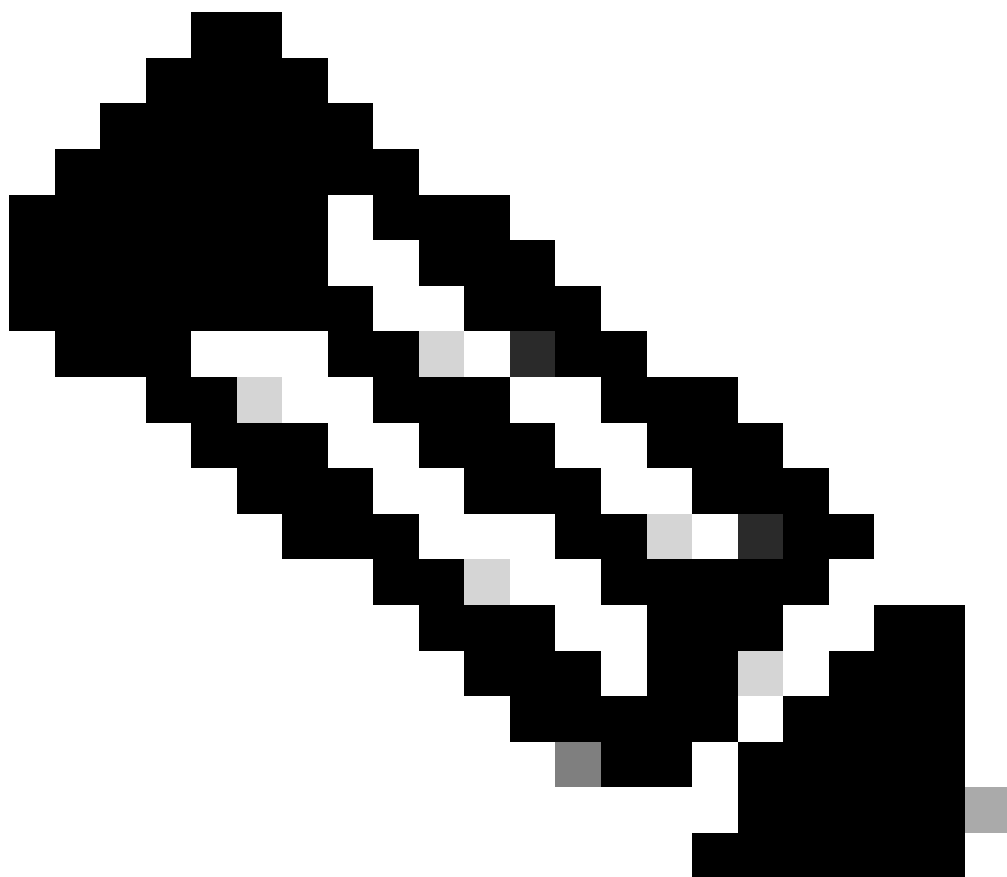
[4-Jul-2025 4:52:38 UTC] Vmanage 89.89.89.2 has successfully restarted.

[4-Jul-2025 4:52:40 UTC] 2 vmanages have successfully registered and restarted. Restarting current vmanage 89.89.89.1

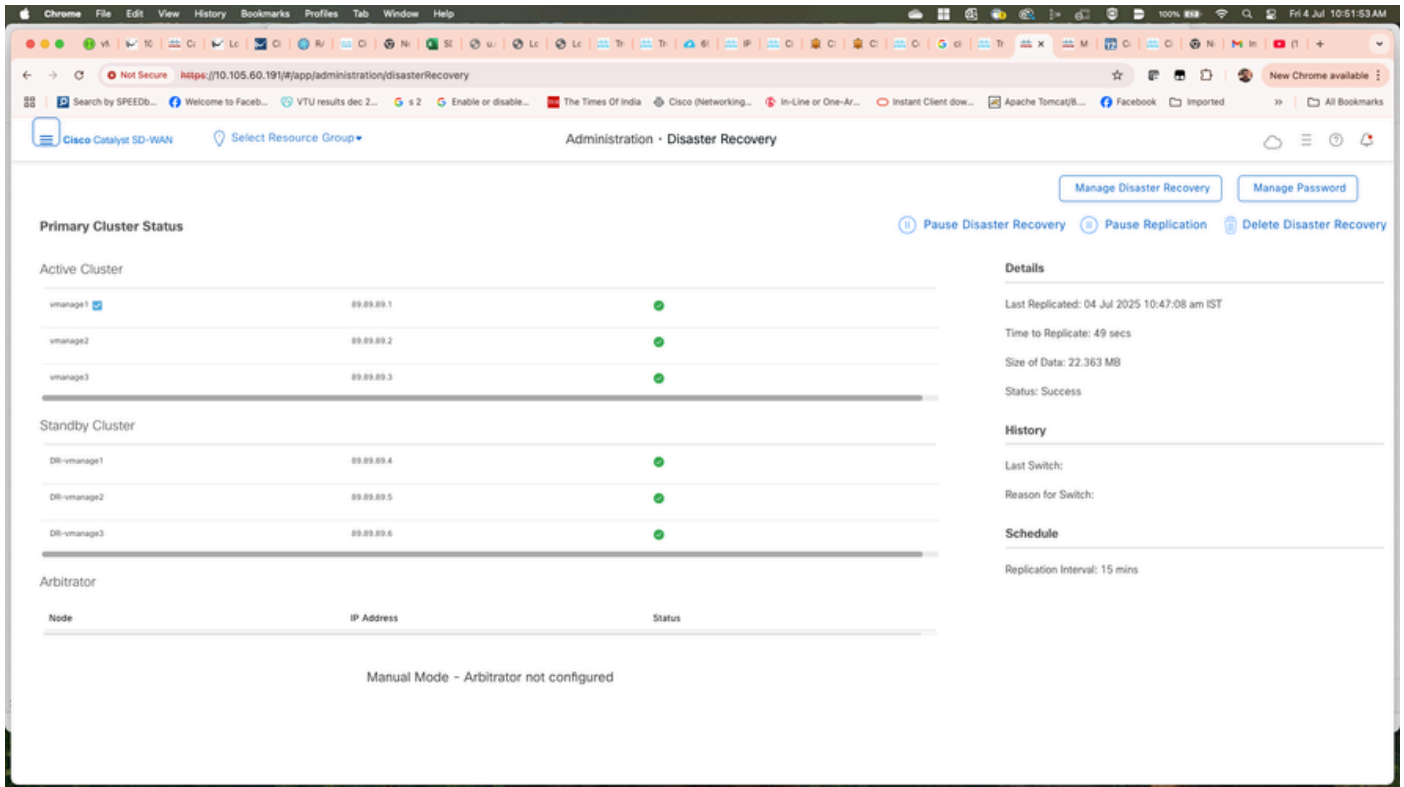
Close

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: Neste cenário, a replicação levou apenas 49 segundos, pois o ambiente de laboratório tem um pequeno banco de dados. No entanto, 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.



Verifique o log de recuperação de desastres em ambos os clusters.

DC-vmanage (9a15f979-d613-4d75-97bf-f7d4124bc687 is export ID)

```
vmanage1:/var/log/nms$ cat vmanage-disaster_recovery.log | grep 9a15f979-d613-4d75-97bf-f7d4124bc687
04-Jul-2025 05:17:08,297 UTC INFO [] [] [DataReplicationManager] (pool-232-thread-1) || Export ID Gener
04-Jul-2025 05:17:58,431 UTC INFO [] [] [DisasterRecoveryAlarmsDAO] (pool-232-thread-1) || AlarmsDAO::a
04-Jul-2025 05:17:58,722 UTC INFO [] [] [DataReplicationManager] (pool-232-thread-1) || Sending the imp
04-Jul-2025 05:17:59,081 UTC INFO [a17a50ae-e6d3-401c-9d34-7c9423a5dd5a] [vmanage1] [DisasterRecoveryRe
04-Jul-2025 05:21:06,515 UTC INFO [a456da19-9868-42e1-b3e7-9cb7ef3bdb81] [vmanage1] [DisasterRecoveryRe
vmanage1:/var/log/nms$
```

DR-Vmanage

```
DR-vmanage1:/var/log/nms$ cat vmanage-disaster_recovery.log | grep 9a15f979-d613-4d75-97bf-f7d4124bc687
04-Jul-2025 05:15:23,296 UTC INFO [] [] [DataReplicationManager] (Thread-366) || Payload received for d
04-Jul-2025 05:15:23,298 UTC INFO [] [] [DataReplicationManager] (Thread-366) || destinationURL dataserv
04-Jul-2025 05:15:24,040 UTC INFO [] [] [DisasterRecoveryAlarmsDAO] (Thread-366) || AlarmsDAO::addAlarm
04-Jul-2025 05:15:24,170 UTC INFO [] [] [DataReplicationManager] (Thread-366) || Downloaded replication
04-Jul-2025 05:15:24,171 UTC INFO [] [] [DisasterRecoveryManager] (Thread-366) || Sending rpc message t
04-Jul-2025 05:15:24,216 UTC INFO [] [] [DisasterRecoveryManager] (Thread-366) || Sending message to de
04-Jul-2025 05:15:24,245 UTC INFO [] [] [DisasterRecoveryManager] (Thread-366) || Waiting for copyRepli
04-Jul-2025 05:18:19,545 UTC INFO [] [] [DataReplicationWorker] (Thread-366) || Successfully Deleted Imp
04-Jul-2025 05:18:19,643 UTC INFO [] [] [DisasterRecoveryAlarmsDAO] (Thread-366) || AlarmsDAO::addAlarm
04-Jul-2025 05:18:19,707 UTC INFO [] [] [DataReplicationManager] (Thread-366) || Successfully imported
04-Jul-2025 05:18:19,716 UTC INFO [] [] [DisasterRecoveryManager] (Thread-366) || Sending rpc message t
04-Jul-2025 05:18:19,849 UTC INFO [] [] [DisasterRecoveryManager] (Thread-366) || Sending message to de
```

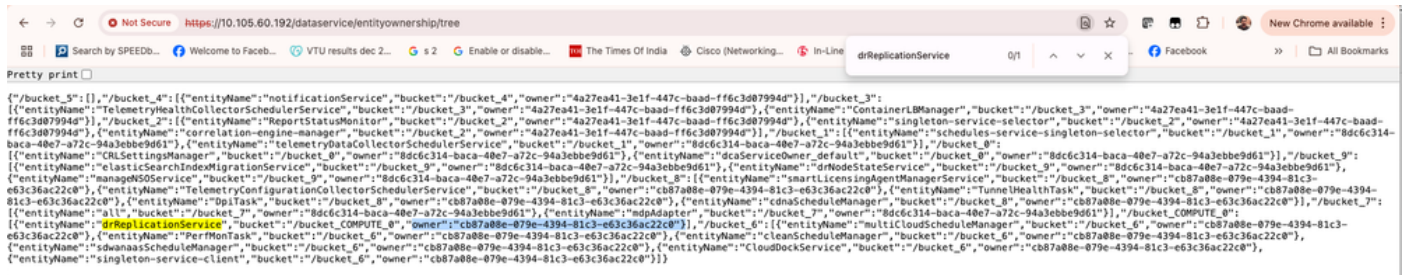
Como verificar o nó líder de replicação?

- Use a próxima API para descobrir o nó líder de replicação em ambos os clusters:

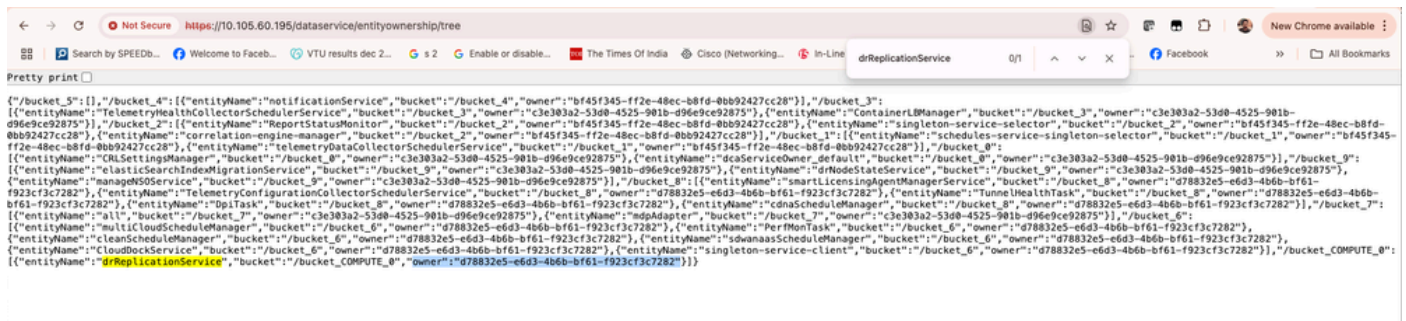
<https://<vmanage-ip>/data service/entity ownership/tree>.

Para cluster DC:

O nó de replicação é cb87a08e-079e-4394-81c3-e63c36ac22c0, que é o nó 1, verifique-o em show control local-properties.



Da mesma forma para o DR-vManage, o nó de replicação é d78832e5-e6d3-4b6b-bf61-f923cf3c7282.



Atualização da senha do Validator (vBond) após o registro da recuperação de desastres

Se você alterar a senha do vBond depois que o registro de recuperação de desastre estiver concluído, um switchover falha porque a senha do vBond não é atualizada no cluster secundário, que ainda mantém a senha antiga do vBond.

[04-July-2025 6:47:35 UTC] Unshut control tunnel on the standby vManage.

[04-July-2025 6:47:36 UTC] Sleeping for 10 seconds to ensure control tunnel is fully up and functional

[04-July-2025 6:47:55 UTC] Failed to activate the cluster. Vbond is unreachable

=====

04-July-2025 06:47:55,206 UTC ERROR [89b008fa-2c1b-4f78-b093-ed1fa1f06b71] [vManage20-14-DR] [DisasterR at com.viptela.vmanage.server.device.common.NetConfClient.connect(NetConfClient.java:255) ~[vmanage-ser at com.viptela.vmanage.server.device.common.NetConfClient.

(NetConfClient.java:114) ~[vmanage-server-1.0.0-SNAPSHOT.jar:?]

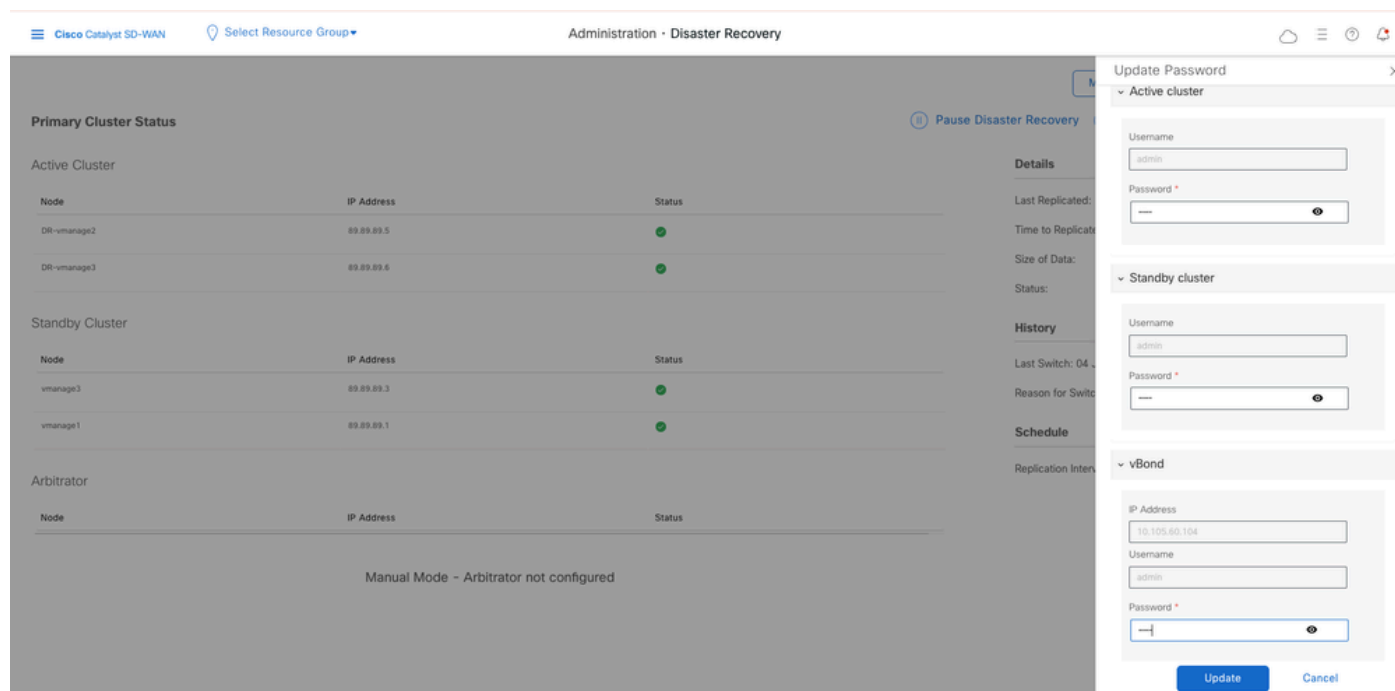
Atualizar Senha do Validador (vbond)

Certifique-se de atualizar a nova senha do vBond na página Recuperação de desastres e em Gerenciar senha:

Administração > Recuperação de desastres > Gerenciar senha > Atualizar senha do vBond.

Verifique se a replicação foi bem-sucedida após a atualização da senha. Tente um failover somente depois de confirmar a replicação bem-sucedida.

advertência: <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwn19224>.



The screenshot displays the Cisco Catalyst SD-WAN Administration interface for Disaster Recovery. The main panel shows the Primary Cluster Status, including Active, Standby, and Arbitrator clusters. The Active cluster table lists nodes DR-vmanage2 and DR-vmanage3. The Standby cluster table lists nodes vmanage3 and vmanage1. The Arbitrator section is in Manual Mode. An 'Update Password' modal is open on the right, showing fields for Username and Password for the Active cluster, Standby cluster, and vBond. The vBond section also includes an IP Address field.

Node	IP Address	Status
DR-vmanage2	89.89.89.5	●
DR-vmanage3	89.89.89.6	●

Node	IP Address	Status
vmanage3	89.89.89.3	●
vmanage1	89.89.89.1	●

Manual Mode - Arbitrator not configured

Adicionando novo validador (vBond) à sobreposição após o registro de recuperação de desastres

Não há suporte para a adição de um novo validador à sobreposição de SD-WAN após o registro de recuperação de desastre, pois a configuração de recuperação de desastre não está ciente dessas novas informações do validador, pois elas não foram atualizadas durante o registro.

Embora você possa adicionar o validador, um switchover falha.

Se precisar adicionar um novo validador, siga estas etapas:

1. Exclua a configuração de recuperação de desastre.
2. Adicione o novo validador à sobreposição de SD-WAN.
3. Reconfigure a recuperação de desastres.

Atualizar sobreposições de recuperação de desastres

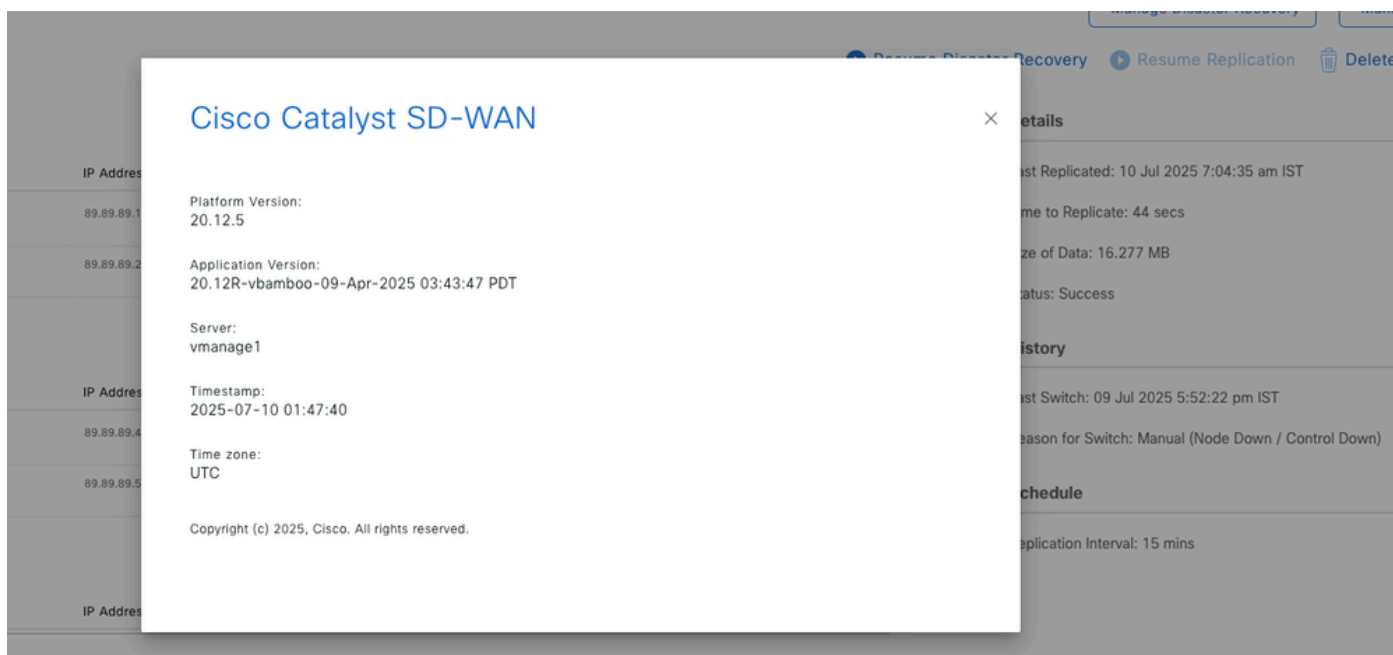
Antes de Começar

- Use o método CLI para atualizar os gerenciadores ativo e standby Cisco SD-WAN.
- Certifique-se de que o status da replicação na página Administração > Recuperação de desastres seja estável e não esteja em um estado transitório, como Importação pendente, Exportação pendente, ou Download pendente. Ele deve estar no estado Success antes de pausar a recuperação de desastres.
- Pause a recuperação de desastres usando Pausar recuperação de desastres em Administração > página Recuperação de desastres.

Processo de atualização

Nesse caso, você está atualizando o cluster vManage de 20.12.5 para 20.15.2. Use o método CLI para atualizar o cluster.

Antes de atualizar, verifique a versão e o status da replicação.



Pausar recuperação de desastres:

Primary Cluster Status

Active Cluster

Node	IP Address	Status
vmanage1	89.89.89.1	●
vmanage2	89.89.89.2	▲

Standby Cluster

Node	IP Address	Status
DR-vmanage1	89.89.89.4	●
DR-vmanage2	89.89.89.5	●

Arbitrator

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

Manage Disaster Recovery

Manage Password

Resume Disaster Recovery

Resume Replication

Delete Disaster Recovery

Details

Last Replicated: 10 Jul 2025 7:04:35 am IST

Time to Replicate: 44 secs

Size of Data: 16.277 MB

Status: Success

History

Last Switch: 09 Jul 2025 5:52:22 pm IST

Reason for Switch: Manual (Node Down / Control Down)

Schedule

Replication Interval: 15 mins

Após a atualização, certifique-se de que todos os serviços estejam em execução e que você possa fazer login em todos os nós do vManage (DC e DR) usando a GUI.

IP Address

89.89.89.2

89.89.89.3

89.89.89.1

IP Address

89.89.89.5

89.89.89.6

89.89.89.4

Cisco Catalyst SD-WAN

Platform Version:
20.15.2

Application Version:
20.15R-vbamboo-05-Mar-2025 01:53:17 PST

Server:
vmanage1

Timestamp:
2025-07-10 02:40:05

Time zone:
UTC

Copyright (c) 2025, Cisco. All rights reserved.

Close

Manage Disaster Recovery

Manage Password

Resume Disaster Recovery

Delete Disaster Recovery

Details

Last Replicated: 10 Jul 2025 7:04:35 AM GMT+5

Time to Replicate: 44 secs

Size of Data: 16.277 MB

Status: Success

History

Last Switch: 09 Jul 2025 5:52:22 PM GMT+05:30

Reason for Switch: Manual (Node Down / Control Down)

Schedule

Replication Interval: 15 mins

Retomar a recuperação de desastres; a replicação é iniciada, e o status da replicação deve ser exibido como sucesso.

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

Snooze

Disaster Recovery

Primary Cluster Status

Active Cluster (3)

Node	IP Address	Status
vmanage2	89.89.89.2	●
vmanage3	89.89.89.3	●
vmanage1	89.89.89.1	●

Standby Cluster (3)

Node	IP Address	Status
DR-vmanage2	89.89.89.5	●
DR-vmanage3	89.89.89.6	●
DR-vmanage1	89.89.89.4	●

Manage Disaster Recovery

Manage Password

Pause Disaster Recovery

Delete Disaster Recovery

Details

Last Replicated: 10 Jul 2025 8:32:37 AM GMT+5

Time to Replicate: 46 secs

Size of Data: 16.401 MB

Status: Success

History

Last Switch: 09 Jul 2025 5:52:22 PM GMT+05:30

Reason for Switch: Manual (Node Down / Control Down)

Schedule

Replication Interval: 15 mins

Informações Relacionadas

- <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/ha-scaling/ios-xe-17/high-availability-book-xe/m-disaster-recovery.html>
- [Suporte técnico e downloads da Cisco](#)

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.