

Cisco SDWAN Manager 3 Node Cluster Disaster Recovery

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Comment vérifier le noeud principal de réplication ?](#)

[Mise à jour du mot de passe Validator \(vBond\) après enregistrement de reprise après sinistre](#)

[Mettre à jour le mot de passe du validateur \(vbond\)](#)

[Ajout d'un nouveau validateur \(vBond\) à la superposition après l'enregistrement de reprise après sinistre](#)

[Mise à niveau des superpositions de reprise après sinistre](#)

[Avant de commencer](#)

[Processus de mise à niveau](#)

[Informations connexes](#)

Introduction

Ce document décrit la nature avec état de Cisco vManage et de son routeur désigné (DR) principal/secondaire, permettant un basculement manuel avec réplication automatique des données.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance des clusters vManage 3 noeuds. Deux clusters à 3 noeuds vManage distincts doivent être configurés et opérationnels pour poursuivre la reprise après sinistre. Sur le cluster actif, vous devez avoir des validateurs et des contrôleurs intégrés. Si vous avez des validateurs et des contrôleurs sur le site DR, ils doivent également être intégrés sur le cluster actif et non sur le cluster vManage DR.

Cisco recommande de respecter les conditions suivantes avant d'enregistrer une reprise après

sinistre :

- Assurez-vous que le noeud principal et le noeud secondaire sont accessibles par HTTPS sur un VPN de transport (VPN 0).
- Assurez-vous que les contrôleurs Cisco vSmart et les orchestrateurs Cisco vBond de la configuration secondaire sont connectés à la configuration principale.
- Assurez-vous que le noeud principal et le noeud secondaire Cisco vManage exécutent la même version de Cisco vManage.
- Interface de cluster hors bande dans VPN 0 :
 - Pour chaque instance vManage d'un cluster, une troisième interface (liaison de cluster) est requise en plus des interfaces utilisées pour VPN 0 (transport) et VPN 512 (gestion).
 - Cette interface est utilisée pour la communication et la synchronisation entre les serveurs vManage du cluster.
 - Cette interface doit être d'au moins 1 Gbit/s et avoir une latence de 4 ms ou moins. Une interface 10 Gbit/s est recommandée.
 - Les deux noeuds vManage doivent être en mesure de se joindre via cette interface : qu'il s'agisse d'un segment de couche 2 ou du routage de couche 3.
 - Dans chaque vManage, cette interface doit être configurée dans l'interface utilisateur graphique comme interface de cluster (Administration > Gestion de cluster - indiquez votre propre adresse IP, votre propre utilisateur et votre propre mot de passe d'interface de cluster hors bande).
 - Afin de permettre aux noeuds Cisco vManage de communiquer entre eux à travers les data centers, activez les ports TCP 8443 et 830 sur les pare-feu de votre data center.
- Assurez-vous que tous les services (application-server, configuration-db, messaging server, coordination server et statistics-db) sont activés sur les deux noeuds Cisco vManage.
- Distribuez tous les contrôleurs, y compris les orchestrateurs Cisco vBond, dans les data centers principal et secondaire. Assurez-vous que ces contrôleurs sont accessibles par les noeuds Cisco vManage distribués dans ces data centers. Les contrôleurs se connectent uniquement au noeud Cisco vManage principal.
- Assurez-vous qu'aucune autre opération n'est en cours dans le noeud Cisco vManage actif (principal) et en veille (secondaire). Par exemple, assurez-vous qu'aucun serveur n'est en cours de mise à niveau ou d'association de modèles à des périphériques.
- Désactivez le serveur proxy HTTP/HTTPS Cisco vManage s'il est activé. Voir [Serveur proxy HTTP/HTTPS pour Cisco vManage Communication with External Servers](#). Si vous ne désactivez pas le serveur proxy, Cisco vManage tente d'établir une communication de reprise après sinistre via l'adresse IP proxy, même si les adresses IP de cluster hors bande Cisco vManage sont directement accessibles. Vous pouvez réactiver le serveur proxy HTTP/HTTPS Cisco vManage une fois l'enregistrement de la reprise après sinistre terminé.
- Avant de commencer le processus d'enregistrement de reprise après sinistre, accédez à la fenêtre Outils > Redécouvrir le réseau sur le noeud principal Cisco vManage et retrouvez les orchestrateurs Cisco vBond.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Responsable : 20.12.5
- Valideur : 20.12.5
- Contrôleur : 20.12.5
- cEdge : 17.12.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

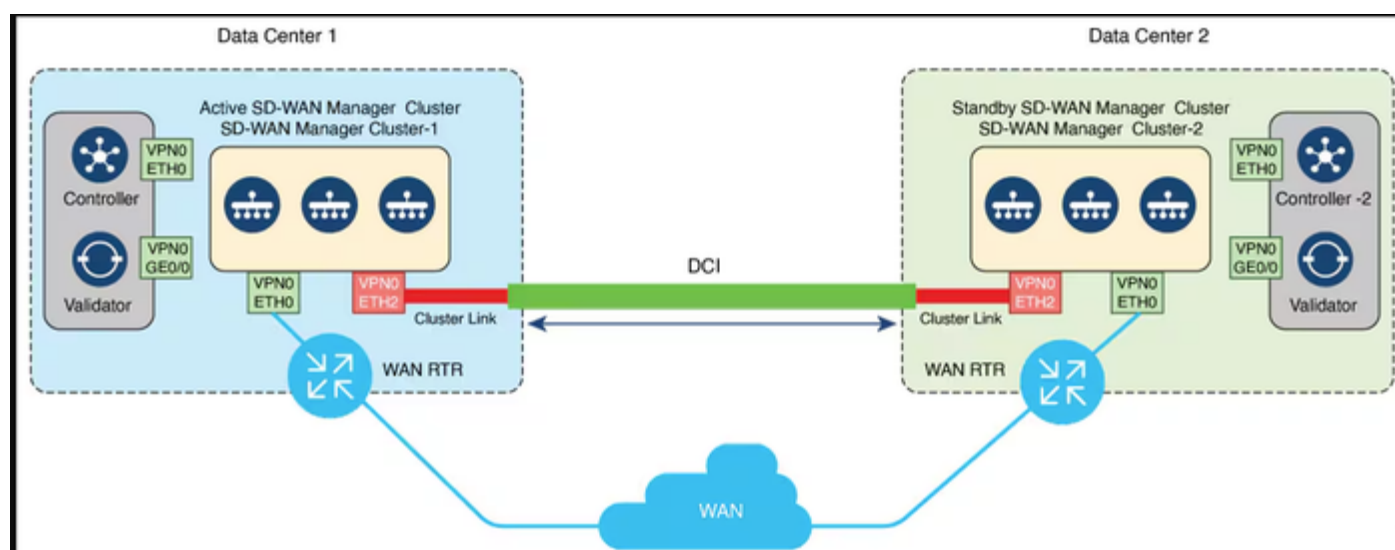
Informations générales

La reprise après sinistre fournit un processus de basculement déclenché par l'administrateur. Lorsque la reprise après sinistre est enregistrée, les données sont répliquées automatiquement entre les clusters Cisco vManage principal et secondaire. Vous effectuez manuellement un basculement vers le cluster secondaire si nécessaire.

Configurer

Diagramme du réseau

Cette figure illustre l'architecture de haut niveau de la solution de reprise après sinistre avec un cluster à trois nœuds.



Configurations

Pour plus d'informations sur vManage Disaster Recovery, consultez [ce lien](#).

Les deux clusters à 3 nœuds distincts sont déjà créés, à condition que chaque gestionnaire SD-WAN dispose d'une configuration minimale et que la partie certification soit terminée.

```
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-phymac
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

- Accédez à Administration > Cluster Management sur les deux clusters et vérifiez que tous les noeuds sont à l'état Prêt.

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-e63c36ac22e0	...
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-bf61-1923cf3c7282
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

- Accédez à Administration>Reprise après sinistre. Cliquez sur Gérer la reprise après sinistre.

Cisco Catalyst SD-WAN Administration · Disaster Recovery				
Manage Disaster Recovery Manage Password				
Cluster Status Active Cluster Standby Cluster Arbitrator				
Node IP Address Status Disaster Recovery Not Configured Node IP Address Status Disaster Recovery Not Configured Node IP Address Status				
Details History Schedule Last Import: Time to Import: Size of Data: Status: Last Switch: Reason for Switch: Replication Interval: Switchover Threshold:				

- Dans la fenêtre contextuelle, renseignez les détails de vManage principal et secondaire.

Les adresses IP à indiquer sont les adresses IP des interfaces de cluster hors bande.

Les informations d'identification doivent être celles d'un utilisateur netadmin et ne doivent pas être modifiées une fois que le DR est configuré, à moins qu'il ne soit supprimé.

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

Une fois rempli, cliquez sur Next.

- Renseignez les détails des contrôleurs vBond.

Les contrôleurs vBond doivent être accessibles dans l'adresse IP spécifiée 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

Une fois rempli, cliquez sur Next.

- Dans le champ Recovery Mode, sélectionnez Manual. Le mode Automation est déconseillé. Cliquez sur Next (Suivant).

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

Définissez la valeur et cliquez sur Save.

- L'enregistrement du DR commence maintenant. Cliquez sur le bouton Actualiser pour actualiser manuellement l'état et les journaux de progression. Ce processus peut prendre de 20 à 30 minutes.

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.

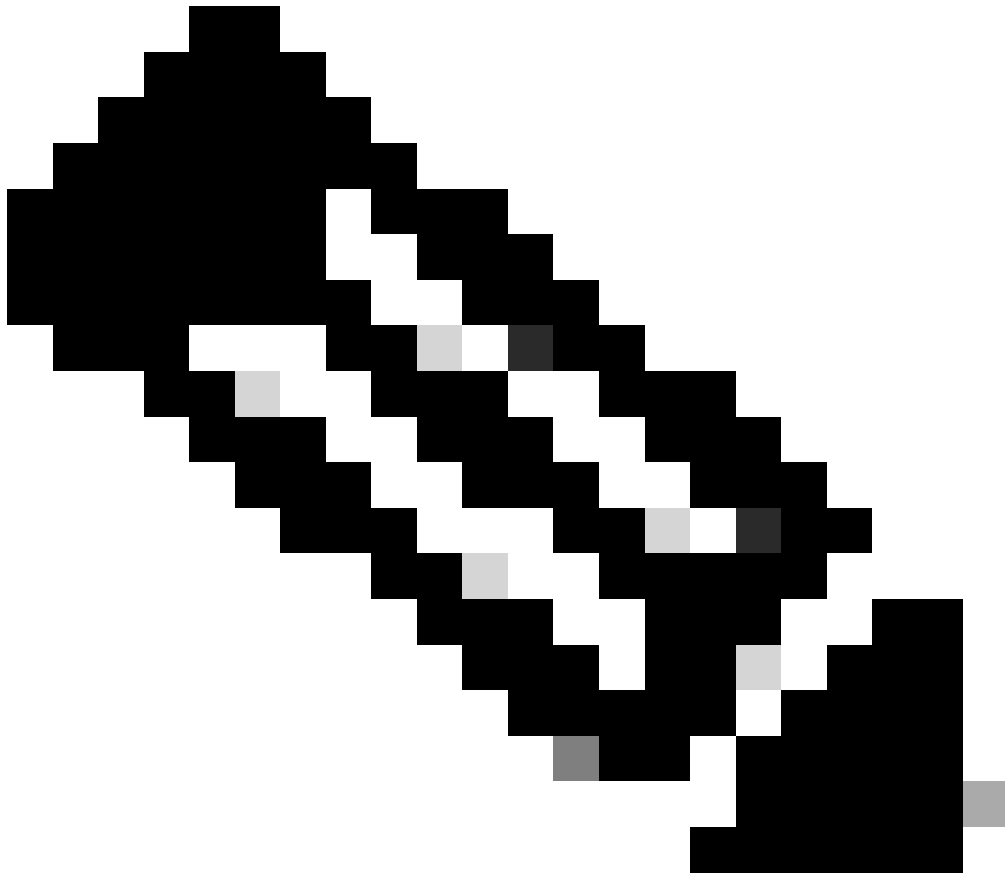
[4-Jul-2025 4:52:40 UTC] 2 vmanages have successfully registered and restarted. Restarting current vmanage 89.89.89.1

Close

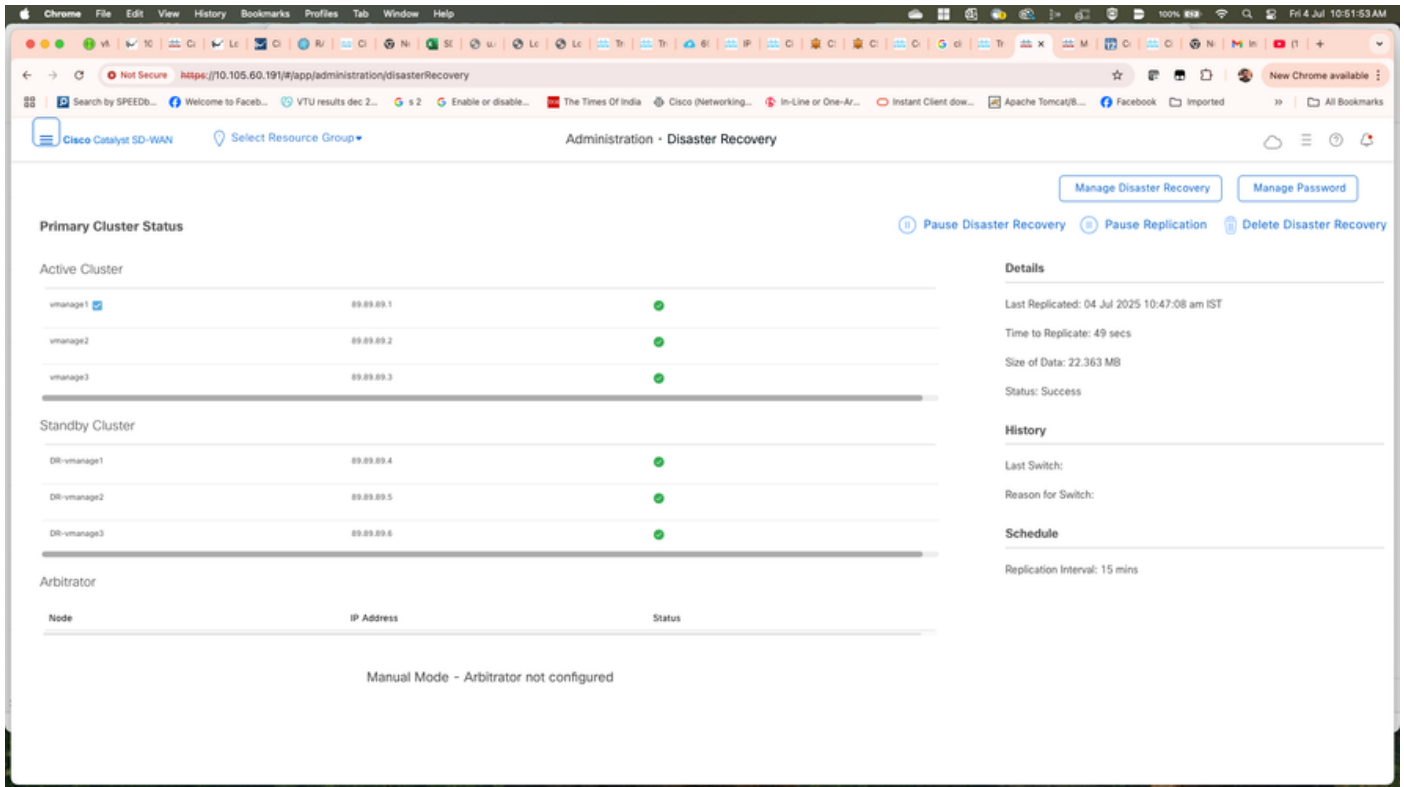
Vérification

- Accédez à Administration>Reprise après sinistre afin de voir l'état de reprise après sinistre

et quand les données ont été répliquées la dernière fois.



Remarque : Dans ce scénario, la réplication n'a pris que 49 secondes, car l'environnement des travaux pratiques comporte une petite base de données. Cependant, la réplication peut prendre plusieurs heures en fonction de la taille de la base de données. En outre, quelques cycles peuvent être nécessaires pour réussir la réplication.



Vérifiez le journal de reprise après sinistre dans les deux 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 dataser
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
```

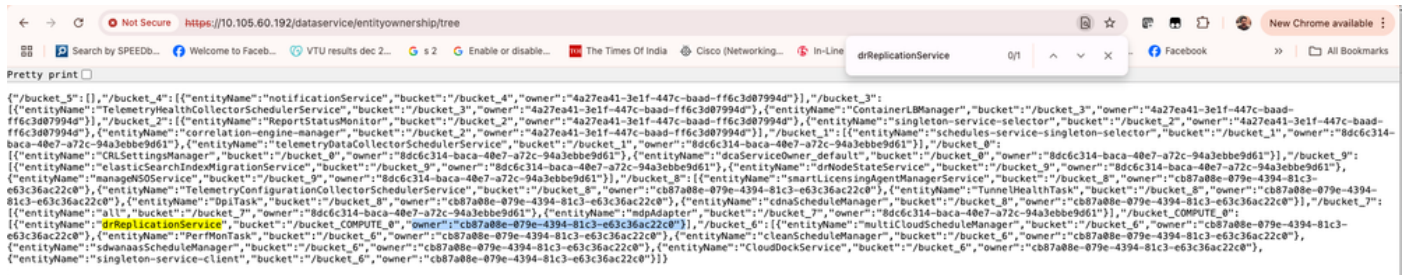
Comment vérifier le noeud principal de réplication ?

- Utilisez l'API suivante afin de trouver le noeud principal de réplication sur les deux clusters :

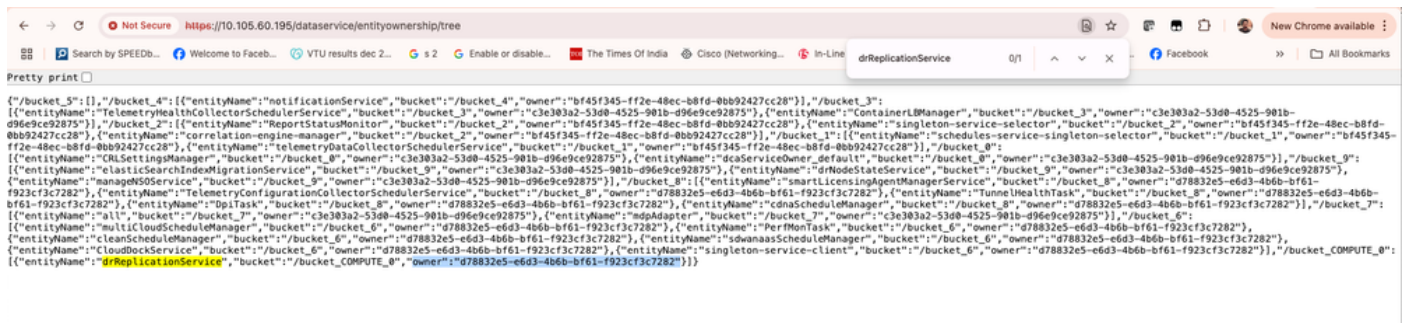
<https://<vmanage-ip>/service/de/donnees/propriete/d'entite/arborescence>.

Pour le cluster CC :

Le noeud de réplication est cb87a08e-079e-4394-81c3-e63c36ac22c0 qui est node1, vérifiez-le à partir de show control local-properties.



De même pour DR-vManage, le noeud de réplication est d78832e5-e6d3-4b6b-bf61-f923cf3c7282.



Mise à jour du mot de passe Validator (vBond) après enregistrement de reprise après sinistre

Si vous modifiez le mot de passe vBond après l'enregistrement de la reprise après sinistre, une commutation échoue car le mot de passe vBond n'est pas mis à jour sur le cluster secondaire, qui conserve toujours l'ancien mot de passe 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:?]

Mettre à jour le mot de passe du validateur (vBond)

Assurez-vous de mettre à jour le nouveau mot de passe vBond à la fois sur la page Reprise après sinistre et sous Gérer le mot de passe :

Administration > Reprise après sinistre > Gérer le mot de passe > Mettre à jour le mot de passe vBond.

Assurez-vous que la réplication réussit après la mise à jour du mot de passe. Tentative de basculement uniquement après confirmation de la réplication réussie.

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

The screenshot displays the Cisco Catalyst SD-WAN Administration interface, specifically the Disaster Recovery section. The main content area shows the 'Primary Cluster Status' with two tables: 'Active Cluster' and 'Standby Cluster'. The 'Active Cluster' table lists nodes DR-vmanage2 and DR-vmanage3 with their respective IP addresses and green status indicators. The 'Standby Cluster' table lists nodes vmanage3 and vmanage1, also with green status indicators. Below these tables, it indicates 'Manual Mode - Arbitrator not configured'. On the right side, a sidebar provides details such as 'Last Replicated', 'Time to Replicate', 'Size of Data', 'Status', 'History', 'Last Switch', 'Reason for Switch', 'Schedule', and 'Replication Interval'. Overlaid on the right is a modal window titled 'Update Password'. This modal contains three sections: 'Active cluster', 'Standby cluster', and 'vBond'. Each section has a 'Username' field (pre-filled with 'admin') and a 'Password *' field. The 'vBond' section also includes an 'IP Address' field (pre-filled with '10.105.60.104'). At the bottom of the modal, there are 'Update' and 'Cancel' buttons.

Ajout d'un nouveau validateur (vBond) à la superposition après l'enregistrement de reprise après sinistre

L'ajout d'un nouveau validateur à la superposition SD-WAN après l'enregistrement de la reprise après sinistre n'est pas pris en charge, car la configuration de la reprise après sinistre ne connaît pas ces nouvelles informations de validateur car elles n'ont pas été mises à jour pendant l'enregistrement.

Bien que vous puissiez ajouter le validateur, une commutation échoue.

Si vous devez ajouter un nouveau validateur, observez ces étapes :

1. Supprimez la configuration de reprise après sinistre.
2. Ajoutez le nouveau validateur à la superposition SD-WAN.
3. Reconfigurez la reprise après sinistre.

Mise à niveau des superpositions de reprise après sinistre

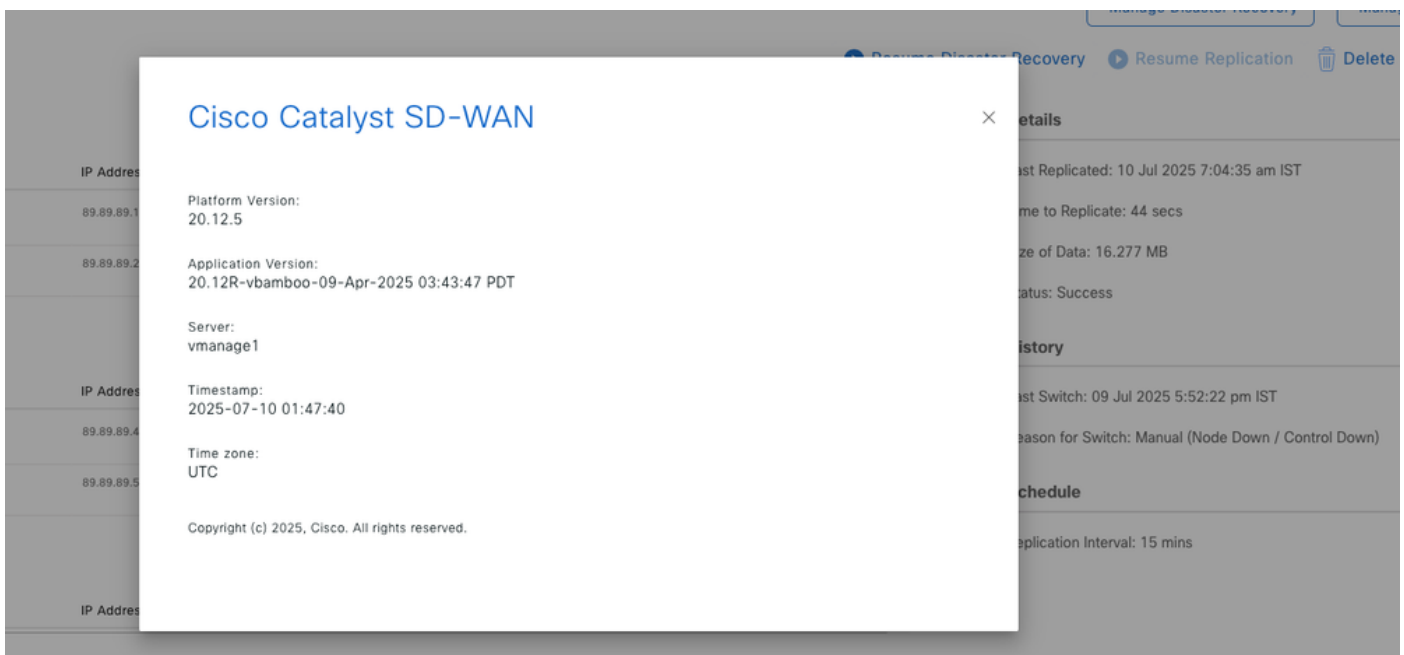
Avant de commencer

- Utilisez la méthode CLI pour mettre à niveau les gestionnaires SD-WAN Cisco actifs et en veille.
- Assurez-vous que l'état de réplication sur la page Administration > Récupération après sinistre est stable et qu'il n'est pas dans un état transitoire comme Importation en attente, Exportation en attente, ou Téléchargement en attente. Il doit être à l'état Success (Réussite) avant de suspendre la reprise après sinistre.
- Suspendez la reprise après sinistre en utilisant Suspendre la reprise après sinistre sous Administration > page Reprise après sinistre.

Processus de mise à niveau

Dans ce cas, vous mettez à niveau le cluster vManage de 20.12.5 vers 20.15.2. Utilisez la méthode CLI afin de mettre à niveau le cluster.

Avant de procéder à la mise à niveau, vérifiez la version et l'état de réplication.



Suspendre la reprise après sinistre :

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

Après la mise à niveau, assurez-vous que tous les services sont en cours d'exécution et que vous pouvez vous connecter à tous les noeuds vManage (DC et DR) à l'aide de l'interface utilisateur graphique.

IP Address

89.89.89.2

89.89.89.3

89.89.89.1

89.89.89.5

89.89.89.6

89.89.89.4

IP Address

89.89.89.2

89.89.89.3

89.89.89.1

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

Reprise après sinistre ; la réplication démarre et l'état de la réplication doit apparaître comme réussi.

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

Informations connexes

- <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>
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.