

Cisco SDWAN Manager 3 Node - Ripristino di emergenza del cluster

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Come verificare il nodo principale della replica?](#)

[Aggiornamento della password di Convalida \(vBond\) dopo la registrazione del ripristino di emergenza](#)

[Aggiorna password di convalida \(vbond\)](#)

[Aggiunta di un nuovo validator \(vBond\) da sovrapporre dopo la registrazione del ripristino di emergenza](#)

[Aggiornamento delle sovrapposizioni del ripristino di emergenza](#)

[Operazioni preliminari](#)

[Processo di aggiornamento](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la natura di conservazione dello stato di Cisco vManage e del relativo router designato primario/secondario (DR), che consente il failover manuale con la replica automatica dei dati.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei cluster vManage a 3 nodi.

Per procedere con il ripristino di emergenza, è necessario configurare e utilizzare due cluster vManage a 3 nodi separati. Nel cluster attivo è necessario che le convalide e i controller siano integrati. Nel caso in cui si disponga di validator e controller sul sito DR, è necessario che questi siano installati anche sul cluster attivo e non sul cluster DR vManage.

Cisco consiglia di soddisfare i seguenti requisiti prima di registrare il disaster recovery:

- Verificare che il nodo primario e il nodo secondario siano raggiungibili da HTTPS su una VPN di trasporto (VPN 0).
- Verificare che i Cisco vSmart Controller e i Cisco vBond Orchestrator sull'installazione secondaria siano collegati all'installazione primaria.
- Verificare che il nodo primario e il nodo secondario Cisco vManage eseguano la stessa versione di Cisco vManage.
- Interfaccia cluster fuori banda nella VPN 0:
 - Per ogni istanza vManage all'interno di un cluster, è necessaria una terza interfaccia (collegamento cluster) oltre alle interfacce utilizzate per VPN 0 (trasporto) e VPN 512 (gestione).
 - Questa interfaccia viene utilizzata per la comunicazione e la sincronizzazione tra i server vManage all'interno del cluster.
 - Questa interfaccia deve essere di almeno 1 Gbps e avere una latenza di 4 ms o inferiore. Si consiglia un'interfaccia di 10 Gbps.
 - Entrambi i nodi vManage devono essere in grado di raggiungere l'uno l'altro tramite questa interfaccia: che si tratti di un segmento di livello 2 o di un instradamento di livello 3.
 - In ogni vManage, questa interfaccia deve essere configurata nella GUI come interfaccia cluster (Amministrazione > Gestione cluster - indicare l'indirizzo IP, l'utente e la password dell'interfaccia cluster fuori banda).
 - Per consentire ai nodi Cisco vManage di comunicare tra loro nei data center, abilitare le porte TCP 8443 e 830 sui firewall del data center.
- Verificare che tutti i servizi (application-server, configuration-db, messaging server, coordination server e statistics-db) siano abilitati su entrambi i nodi Cisco vManage.
- Distribuire tutti i controller, inclusi i Cisco vBond Orchestrator, nei centri dati principali e secondari. Verificare che questi controller siano raggiungibili dai nodi Cisco vManage distribuiti nei centri dati. I controller si connettono solo al nodo Cisco vManage primario.
- Verificare che non siano in corso altre operazioni nel nodo Cisco vManage attivo (primario) e in standby (secondario). Verificare, ad esempio, che nessun server stia aggiornando o collegando modelli ai dispositivi.
- Disabilitare il server proxy HTTP/HTTPS Cisco vManage, se abilitato. Vedere [Server proxy HTTP/HTTPS per la comunicazione Cisco vManage con server esterni](#). Se non si disabilita il server proxy, Cisco vManage tenta di stabilire la comunicazione per il ripristino di emergenza tramite l'indirizzo IP proxy, anche se gli indirizzi IP dei cluster fuori banda di Cisco vManage sono raggiungibili direttamente. È possibile riattivare il server proxy Cisco vManage HTTP/HTTPS al termine della registrazione del ripristino di emergenza.
- Prima di avviare il processo di registrazione del ripristino di emergenza, passare alla finestra Strumenti > Riconosci rete sul nodo Cisco vManage principale e individuare nuovamente i Cisco vBond Orchestrator.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Responsabile: 20.12.5
- Convalida: 20.12.5

- Controller: 20.12.5
- Bordo: 17.12.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

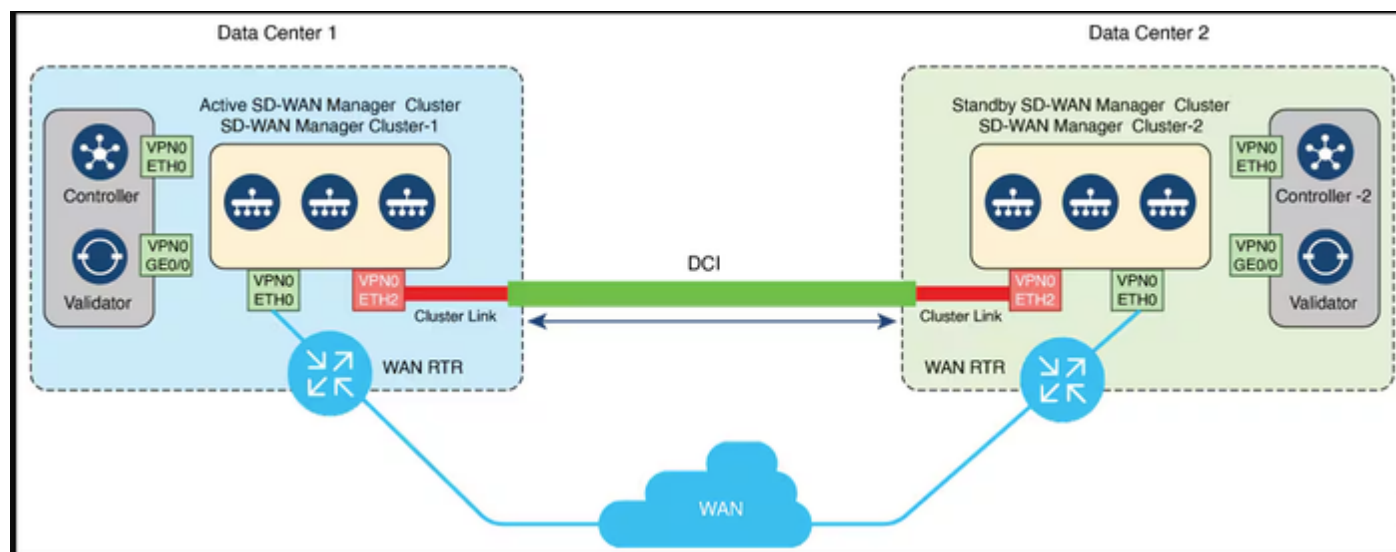
Premesse

Il disaster recovery fornisce un processo di failover avviato dall'amministratore. Quando viene registrato il ripristino di emergenza, i dati vengono replicati automaticamente tra i cluster Cisco vManage primario e secondario. Se necessario, è possibile eseguire manualmente un failover sul cluster secondario.

Configurazione

Esempio di rete

La figura mostra l'architettura di alto livello della soluzione di disaster recovery con un cluster a tre nodi.



Configurazioni

Per ulteriori informazioni su vManage Disaster Recovery, fare riferimento a [questo](#) collegamento.

I due cluster a 3 nodi separati sono già stati creati, presupponendo che ciascun gestore SD-WAN disponga della configurazione minima e che la parte di certificazione sia stata completata.

```
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

- Passare a Amministrazione > Gestione cluster in entrambi i cluster e verificare che tutti i nodi siano in stato 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-bf61-1923cf3c7282
DR-vmanage3	89.89.89.6	Ready	COMPUTE_AND_DATA	bf45f345-ff2e-48ec-b8fd-0bb92427cc28
DR-vmanage2	89.89.89.5	Ready	COMPUTE_AND_DATA	c3e303a2-53d0-4525-901b-d96e9ce92875

- Passare a Amministrazione>Disaster Recovery. Fare clic su Gestione ripristino di emergenza.

Cisco Catalyst SD-WAN

Select Resource Group

Administration · Disaster Recovery

Manage Disaster Recovery

Manage Password

Pause Disaster Recovery

Pause Replication

Delete 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

Details

Last Import:

Time to Import:

Size of Data:

Status:

History

Last Switch:

Reason for Switch:

Schedule

Replication Interval:

Switchover Threshold:

- Nella finestra popup, immettere i dettagli per vManage principale e secondario.

Gli indirizzi IP da indicare sono gli indirizzi IP delle interfacce cluster fuori banda.

Le credenziali devono essere quelle di un utente netadmin e non devono essere modificate una volta configurato il DR, a meno che non venga eliminato.

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

Una volta completate le impostazioni, fare clic su Avanti.

- Specificare i dettagli dei controller vBond.

I controller vBond devono essere raggiungibili nell'indirizzo IP specificato tramite Netconf.

Manage Disaster Recovery

Connectivity Info

Validator Info

Recovery Mode

Replication Schedule

vBond Information

IP10.105.60.104

User Nameadmin

Password

Back

Next

Cancel

Una volta completate le impostazioni, fare clic su Avanti.

- In Modalità di ripristino, scegliere Manuale. La modalità di automazione è deprecata. Fare clic su Next (Avanti).

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

Impostare il valore e fare clic su Salva.

- La registrazione del ripristino di emergenza inizia ora. Fare clic sul pulsante Aggiorna per aggiornare manualmente lo stato e i registri di stato. Questo processo può richiedere fino a 20-30 minuti.

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.

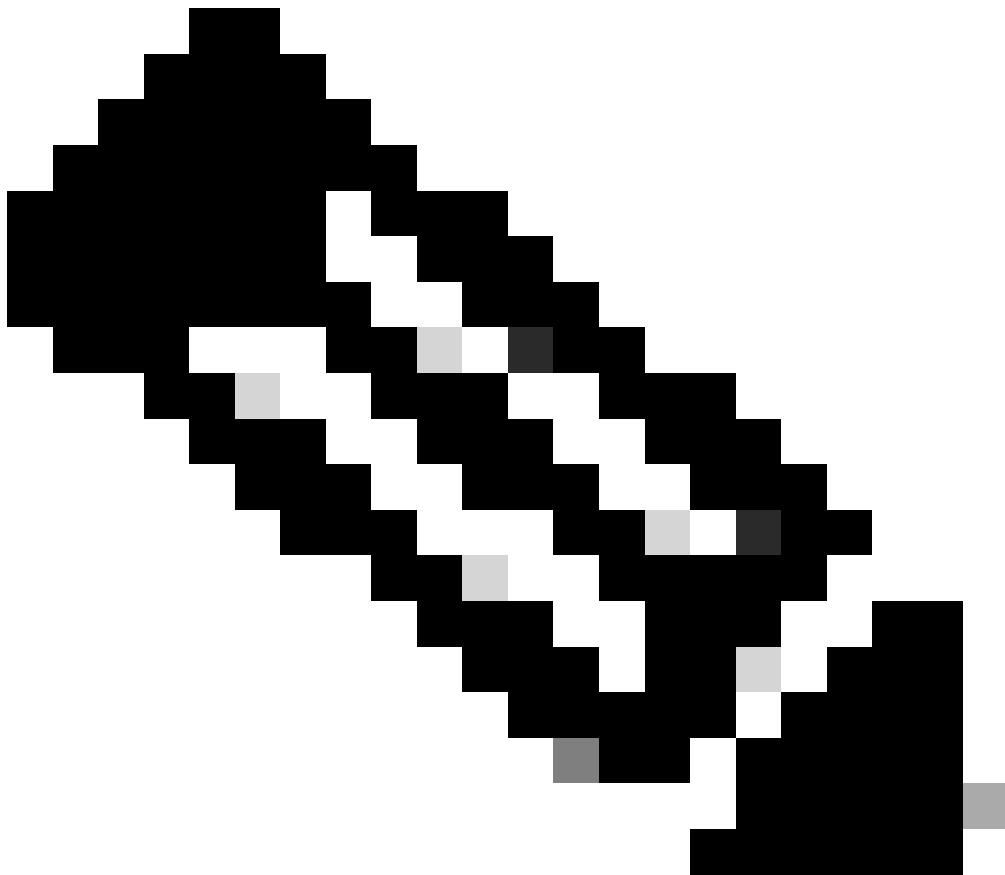
[4-Jul-2025 4:52:40 UTC] 2 vmanages have successfully registered and restarted. Restarting current vmanage 89.89.89.1

Close

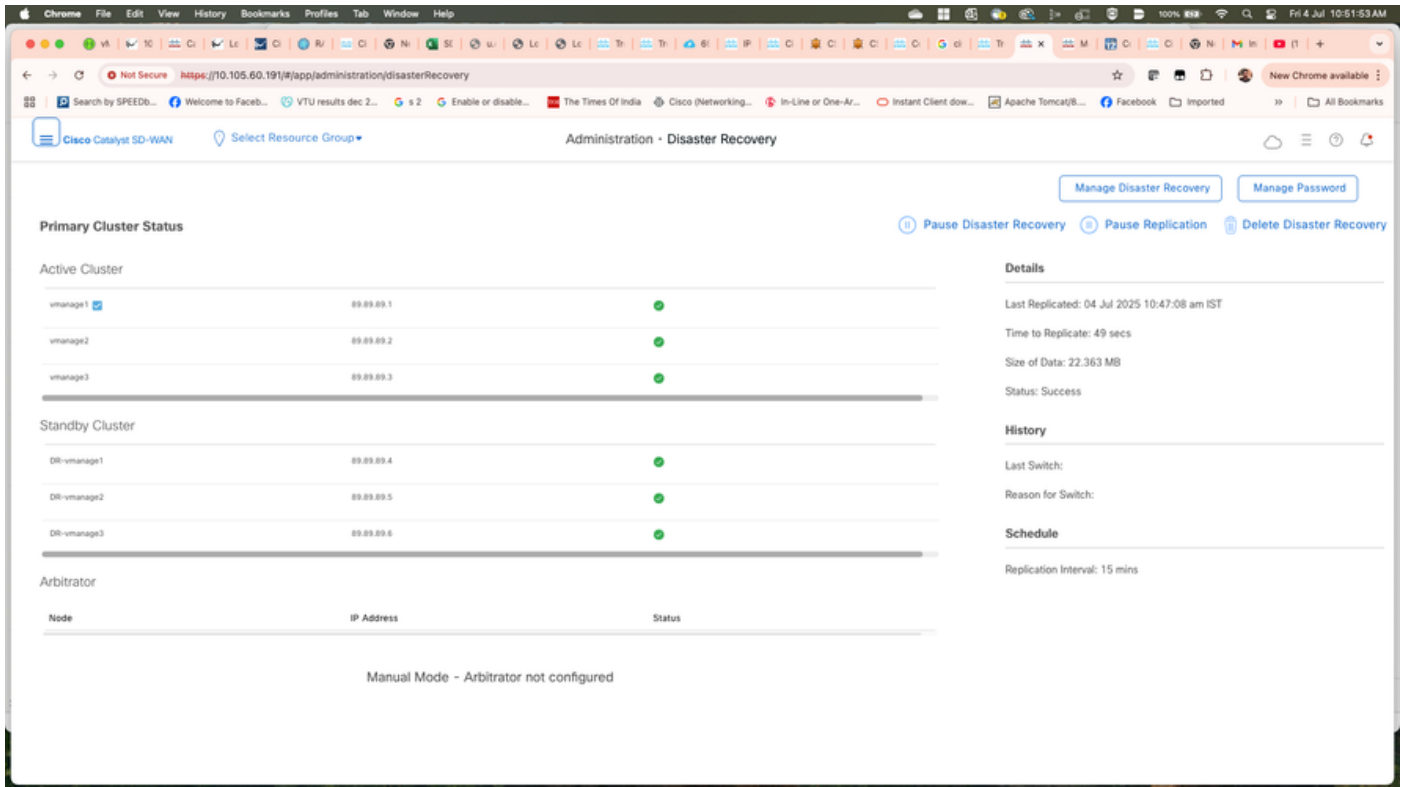
Verifica

- Passare a Amministrazione>Disaster Recovery per verificare lo stato del ripristino di

emergenza e la data dell'ultima replica dei dati.



Nota: In questo scenario, la replica ha richiesto solo 49 secondi perché l'ambiente lab dispone di un database di dimensioni ridotte. Tuttavia, la replica può richiedere diverse ore a seconda delle dimensioni del database. Inoltre, può richiedere alcuni cicli per ottenere una replica corretta.



Verificare il registro di disaster recovery in entrambi i cluster.

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
```

Come verificare il nodo principale della replica?

- Utilizzare l'API successiva per individuare il nodo della linea guida della replica in entrambi i

cluster:

<https://<vmanage-ip>/servizio dati/proprietà entità/albero>.

Per il cluster di controller di dominio:

Il nodo di replica è `cb87a08e-079e-4394-81c3-e63c36ac22c0` che è `node1`, verificare da `show control local-properties`.

Search by SPEED... Welcome to Face... VTU results dec 2... s 2 Enable or disable... The Times Of India Cisco (Networking... In-Line dReplicationService 0/1 Facebook New Chrome available...

```

{"bucket_size":1,"bucket_4":{"entityName":"notificationService","bucket1":"/bucket_4","owner":"4a27e4d1-3e1f-447c-baad-f6fc3087994d"},"bucket_3":{"entityName":"TelemetryHealthCollectorSchedulerService","bucket1":"/bucket_3","owner":"4a27e4d1-3e1f-447c-baad-f6fc3087994d"},"bucket_2":{"entityName":"ReportStatusMonitor","bucket1":"/bucket_2","owner":"4a27e4d1-3e1f-447c-baad-f6fc3087994d"},"entityName":"Singleton-service-selector","bucket1":"/bucket_2","owner":"4a27e4d1-3e1f-447c-baad-f6fc3087994d"},"bucket_1":{"entityName":"elasticSearchIndexingService","bucket1":"/bucket_1","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"entityName":"telemetryDataCollectorSchedulerService","bucket1":"/bucket_1","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"bucket_0":{"entityName":"CRISettingManager","bucket1":"/bucket_0","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"entityName":"dataServiceOwner.default","bucket1":"/bucket_0","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"bucket_9":{"entityName":"ElasticSearchIndexingService","bucket1":"/bucket_9","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"entityName":"drIdoService","bucket1":"/bucket_9","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"bucket_8":{"entityName":"managementService","bucket1":"/bucket_8","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"bucket_8":{"entityName":"smartLinkSingletonManagerService","bucket1":"/bucket_8","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"TelemetryConfigurationCollectorSchedulerService","bucket1":"/bucket_8","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"TunnelHealthTask","bucket1":"/bucket_8","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"DpiTask","bucket1":"/bucket_8","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"cdnsCacheManager","bucket1":"/bucket_8","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"bucket_7":{"entityName":"all","bucket1":"/bucket_7","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"entityName":"mdpAdapter","bucket1":"/bucket_7","owner":"8d6c313a-b4ca-4b67-972c-94a3eb9b9d61"},"bucket_COMPUTE_0":{"entityName":"dReplicationService","bucket1":"/bucket_COMPUTE_0","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"bucket_6":{"entityName":"multiCloudScheduleManager","bucket1":"/bucket_6","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"PerfMonTask","bucket1":"/bucket_6","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"cleanScheduleManager","bucket1":"/bucket_6","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"cdnsCacheManager","bucket1":"/bucket_6","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"Singleton-service-client","bucket1":"/bucket_6","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"entityName":"cloudBackupService","bucket1":"/bucket_6","owner":"c8b7888e-079e-4394-81c3-6e336ac22c08"},"

```

Analogamente, per DR-vManage, il nodo di replica è d78832e5-e6d3-4b6b-bf61-f923cf3c7282.

```

{"@version": 1, "buckets": [{"@type": "notification-engine", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "bucket_3": "1", "entityName": "elasticSearchCollectorService", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "ContainerManager", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "bucket_2": "1", "entityName": "ReportStatusMonitor", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "singleton-service-selector", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "correlation-engine-manager", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "bucket_1": "1", "entityName": "schedules-service-singleton-selector", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "CRMSettingsManager", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "dDataServiceOwner_default", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "elasticSearchIndexMigrationService", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "dNodeStateManager", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "managementService", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "bucket_8": "1", "entityName": "smartLinkingManagerService", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "TelemetryConfigurationCollectorService", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "DpiTask", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "cdnsScheduleManager", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "mail", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "mpAdapter", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "cleanSchedulerManager", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "sdwannaasScheduleManager", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "cloudDocService", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "entityName": "singleton-service-client", "bucket": "1", "owner": "b4f5345-f72e-48bc-bf0d-8bb9247cc28b", "bucket_COMPUTE": "0"}]}

```

Aggiornamento della password di Convalida (vBond) dopo la registrazione del ripristino di emergenza

Se si modifica la password vBond dopo la registrazione del ripristino di emergenza, lo switchover non riesce perché la password vBond non viene aggiornata nel cluster secondario, che conserva comunque la vecchia password 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) ~[vmange-ser
at com.viptela.vmanage.server.device.common.NetConfClient.
```

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

Aggiorna password di convalida (vbond)

Assicurarsi di aggiornare la nuova password vBond sia nella pagina Disaster Recovery che in Gestione password:

Amministrazione > Disaster Recovery > Gestisci password > Aggiorna password vBond.

Verificare che la replica sia stata eseguita correttamente dopo l'aggiornamento della password. Tentare un failover solo dopo aver confermato la corretta replica.

avvertimento: <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, which is divided into three sections: Active Cluster, Standby Cluster, and Arbitrator. Each section contains a table with columns for Node, IP Address, and Status. The Active Cluster table lists DR-vmanage2 and DR-vmanage3. The Standby Cluster table lists vmanage3 and vmanage1. The Arbitrator section is currently empty, with a note indicating 'Manual Mode - Arbitrator not configured'. On the right side, there is a sidebar with tabs for Details, History, and Schedule. An 'Update Password' modal is open, showing fields for Username and Password for the Active cluster, Standby cluster, and vBond. The vBond section includes an IP Address field (10.105.60.104) and Username and Password fields.

Aggiunta di un nuovo validator (vBond) da sovrapporre dopo la registrazione del ripristino di emergenza

L'aggiunta di un nuovo validator alla sovrapposizione SD-WAN dopo la registrazione del disaster recovery non è supportata, in quanto la configurazione del disaster recovery non è a conoscenza di queste nuove informazioni di validator poiché non sono state aggiornate durante la registrazione.

Sebbene sia possibile aggiungere la convalida, il passaggio non riesce.

Se è necessario aggiungere un nuovo validator, attenersi alla seguente procedura:

1. Eliminare l'impostazione di ripristino di emergenza.
2. Aggiungere il nuovo validator alla sovrapposizione SD-WAN.
3. Riconfigurare il ripristino di emergenza.

Aggiornamento delle sovrapposizioni del ripristino di emergenza

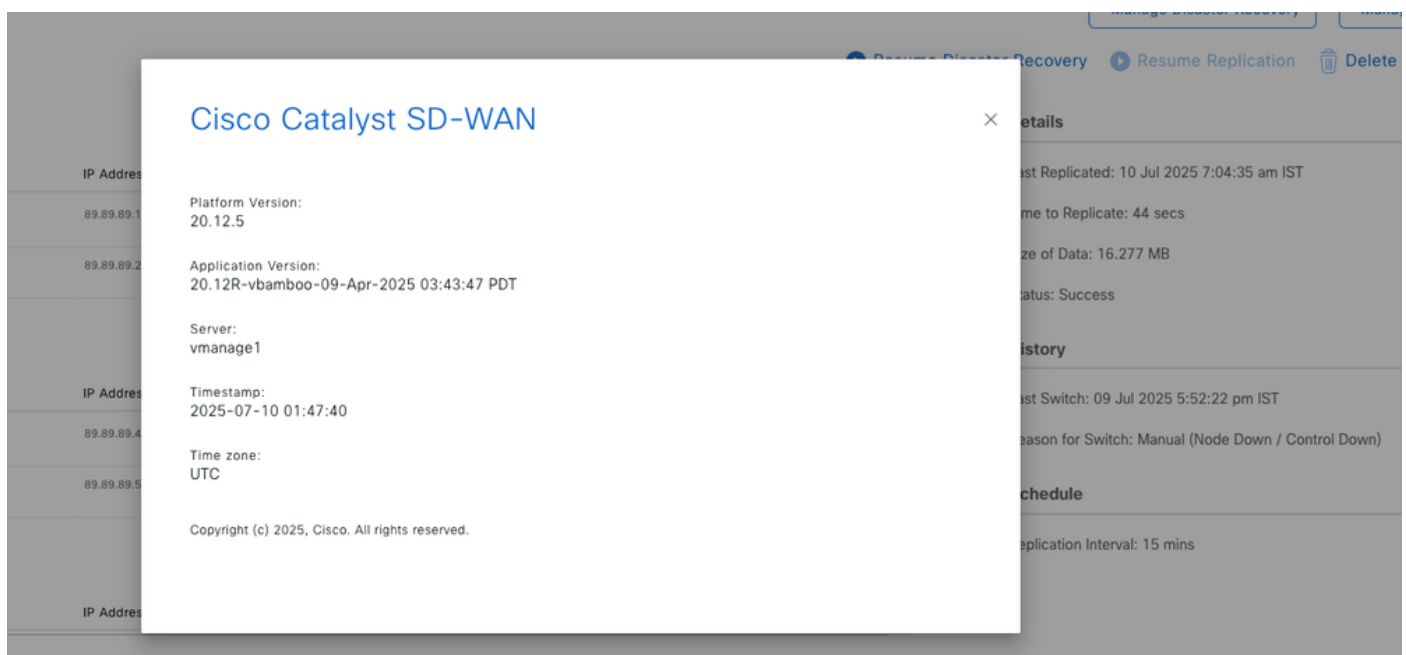
Operazioni preliminari

- Usare il metodo CLI per aggiornare i manager Cisco SD-WAN attivi e in standby.
- Verificare che lo stato di replica nella pagina Amministrazione > Ripristino di emergenza sia stabile e non in uno stato transitorio, ad esempio Importazione in sospeso, Esportazione in sospeso, o Download in sospeso. Deve essere in stato Riuscito prima di sospendere il ripristino di emergenza.
- Sospendere il ripristino di emergenza utilizzando Sospendi ripristino di emergenza nella pagina Amministrazione > Ripristino di emergenza.

Processo di aggiornamento

In questo caso si sta aggiornando il cluster vManage dalla versione 20.12.5 alla 20.15.2. Utilizzare il metodo CLI per aggiornare il cluster.

Prima di eseguire l'aggiornamento, verificare la versione e lo stato della replica.



Sospendi ripristino di emergenza:

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

Dopo l'aggiornamento, verificare che tutti i servizi siano in esecuzione e che sia possibile accedere a tutti i nodi vManage (controller di dominio e ripristino di emergenza) utilizzando la 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

Riprendere il ripristino di emergenza; la replica viene avviata e lo stato della replica deve risultare corretto.

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

Informazioni correlate

- <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>
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).