Cisco SDWAN Manager Disaster Recovery für Cluster mit 3 Knoten

Inhalt

Einleitung

In diesem Dokument wird der Stateful-Status von Cisco vManage und des zugehörigen primären/sekundären Designated Routers (DR) beschrieben, der manuelles Failover mit automatischer Datenreplikation ermöglicht.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse von vManage Clustern mit drei Knoten verfügen. Zwei separate vManage-Cluster mit drei Knoten müssen konfiguriert und betriebsbereit sein, um mit der Notfallwiederherstellung fortfahren zu können. Auf dem aktiven Cluster müssen Validierungssteuerungen und Controller integriert sein. Falls sich der Validator und die Controller am DR-Standort befinden, müssen sie auch im aktiven Cluster und nicht im DR vManage-Cluster integriert werden.

Cisco empfiehlt, vor der Registrierung der Disaster Recovery die folgenden Anforderungen zu

erfüllen:

- Stellen Sie sicher, dass der primäre und der sekundäre Knoten über HTTPS über ein Transport-VPN (VPN 0) erreichbar sind.
- Stellen Sie sicher, dass die Cisco vSmart Controller und Cisco vBond Orchestrator der sekundären Einrichtung mit der primären Einrichtung verbunden sind.
- Stellen Sie sicher, dass auf dem primären und sekundären Cisco vManage-Knoten dieselbe Cisco vManage-Version ausgeführt wird.
- Out-of-Band-Cluster-Schnittstelle in VPN 0:
    - Für jede vManage-Instanz innerhalb eines Clusters ist neben den für VPN 0 (Transport) und VPN 512 (Management) verwendeten Schnittstellen eine dritte Schnittstelle (Cluster-Verbindung) erforderlich.
    - Diese Schnittstelle wird für die Kommunikation und Synchronisierung zwischen den vManage-Servern im Cluster verwendet.
    - Diese Schnittstelle muss mindestens 1 Gbit/s betragen und eine Latenz von maximal 4 ms aufweisen. Eine Schnittstelle mit 10 Gbit/s wird empfohlen.
    - Beide vManage-Knoten müssen sich über diese Schnittstelle erreichen können: sei es ein Layer-2-Segment oder durch Layer-3-Routing.
    - In jedem vManage muss diese Schnittstelle in der GUI als Cluster-Schnittstelle konfiguriert werden (Administration>Cluster Management - eigene Out-of-Band-Cluster-Schnittstellen-IP-Adresse, Benutzer und Kennwort angeben).
    - Damit Cisco vManage-Knoten über mehrere Rechenzentren hinweg miteinander kommunizieren können, aktivieren Sie die TCP-Ports 8443 und 830 auf den Firewalls Ihres Rechenzentrums.
- Stellen Sie sicher, dass alle Services (Anwendungsserver, Konfigurationsdatenbank, Messaging-Server, Koordinierungsserver und Statistikdatenbank) auf beiden Cisco vManage-Knoten aktiviert sind.
- Verteilung aller Controller, einschließlich Cisco vBond Orchestrator, auf primäre und sekundäre Rechenzentren Stellen Sie sicher, dass diese Controller über Cisco vManage-Knoten erreichbar sind, die über diese Rechenzentren verteilt sind. Die Controller sind nur mit dem primären Cisco vManage-Knoten verbunden.
- Stellen Sie sicher, dass im aktiven (primären) und im Standby-Knoten (sekundären) Cisco vManage keine weiteren Vorgänge ausgeführt werden. Stellen Sie beispielsweise sicher, dass keine Server aktualisiert oder Vorlagen an Geräte angehängt werden.
- Deaktivieren Sie den Cisco vManage HTTP/HTTPS-Proxyserver, wenn er aktiviert ist. Informationen zur Cisco vManage-Kommunikation mit externen Servern finden Sie unter HTTP/HTTPS-Proxy-Server. Wenn Sie den Proxyserver nicht deaktivieren, versucht Cisco vManage, eine Notfallwiederherstellungs-Kommunikation über die Proxy-IP-Adresse herzustellen, selbst wenn die Out-of-Band-Cluster-IP-Adressen von Cisco vManage direkt erreichbar sind. Sie können den Cisco vManage HTTP/HTTPS-Proxyserver nach Abschluss der Disaster Recovery-Registrierung erneut aktivieren.
- Bevor Sie mit der Registrierung für die Notfallwiederherstellung beginnen, navigieren Sie zum Fenster Extras > Netzwerk neu erkennen auf dem primären Cisco vManage-Knoten, und suchen Sie erneut nach den Cisco vBond Orchestrator.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Manager: 20.12.5
- Prüfer: 20.12.5
- Controller: 20.12.5
- cEdge: 17.12.5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

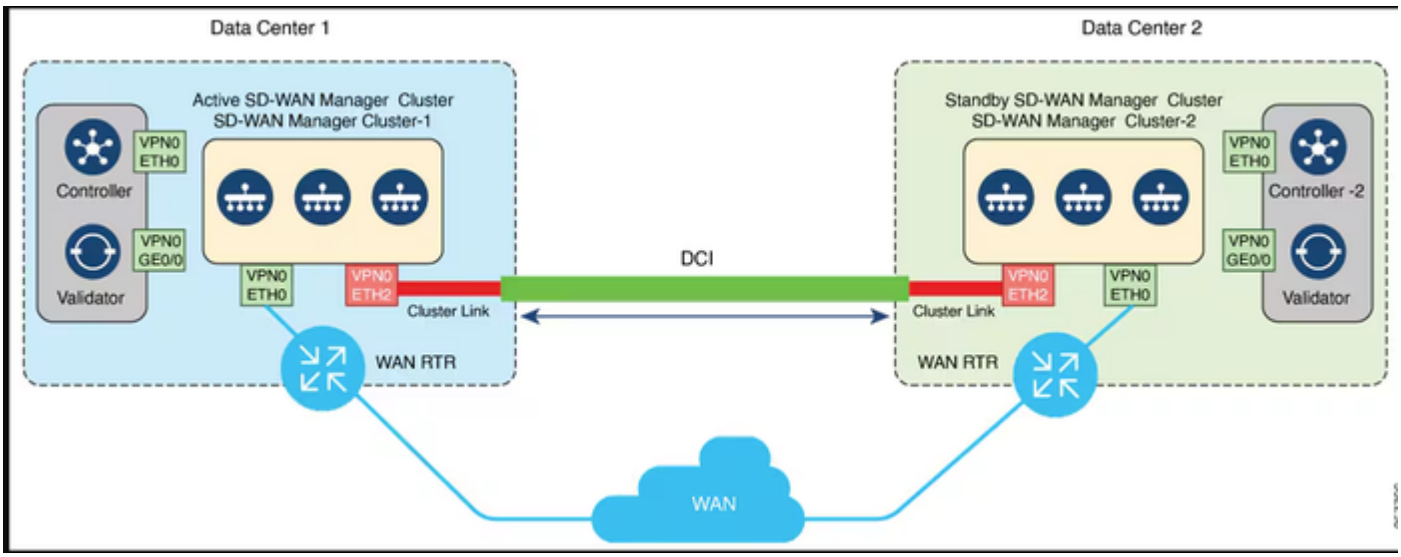
Hintergrundinformationen

Die Notfallwiederherstellung bietet einen vom Administrator ausgelösten Failover-Prozess. Wenn die Notfallwiederherstellung registriert wird, werden Daten automatisch zwischen dem primären und sekundären Cisco vManage-Cluster repliziert. Sie führen bei Bedarf manuell ein Failover auf den sekundären Cluster durch.

Konfigurieren

Netzwerkdiagramm

Diese Abbildung zeigt die High-Level-Architektur der Disaster Recovery-Lösung mit einem Cluster mit drei Knoten.



Konfigurationen

Weitere Informationen zu vManage Disaster Recovery finden Sie unter diesem Link.

Die beiden separaten Cluster mit drei Knoten wurden bereits erstellt. Dabei wird vorausgesetzt, dass jeder SD-WAN-Manager über die absolute Mindestkonfiguration verfügt und die

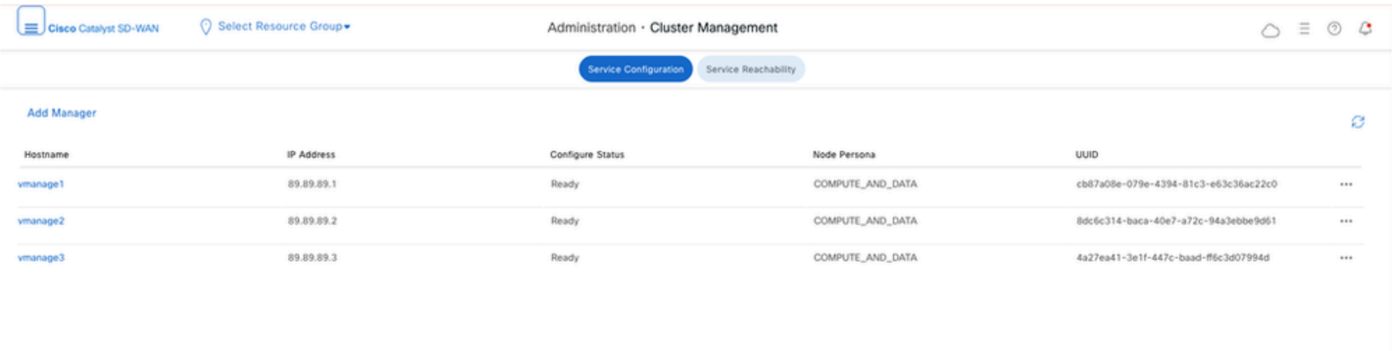
Zertifizierung abgeschlossen ist.

```
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
```

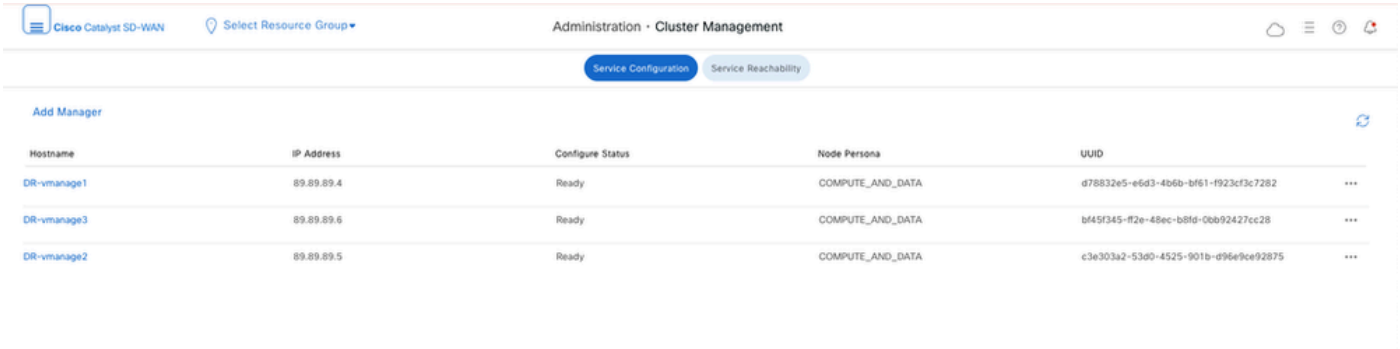
```
vpn 0
 interface eth0
  ip address 10.105.60.102/24
  ipv6 dhcp-client
  tunnel-interface
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service stun
   no allow-service https
  !
  no shutdown
 !
 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

                                            IF      IF      IF                                                                      TCP
                   AF                       ADMIN   OPER    TRACKER  ENCAP                                          SPEED           MSS                 RX        TX
VPN  INTERFACE     TYPE  IP ADDRESS         STATUS  STATUS  STATUS   TYPE   PORT TYPE  MTU  HWADDR             MBPS   DUPLEX  ADJUST  UPTIME      PACKETS   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
```

- Navigieren Sie zu Administration > Cluster Management auf beiden Clustern, und überprüfen Sie, ob alle Knoten bereit sind.

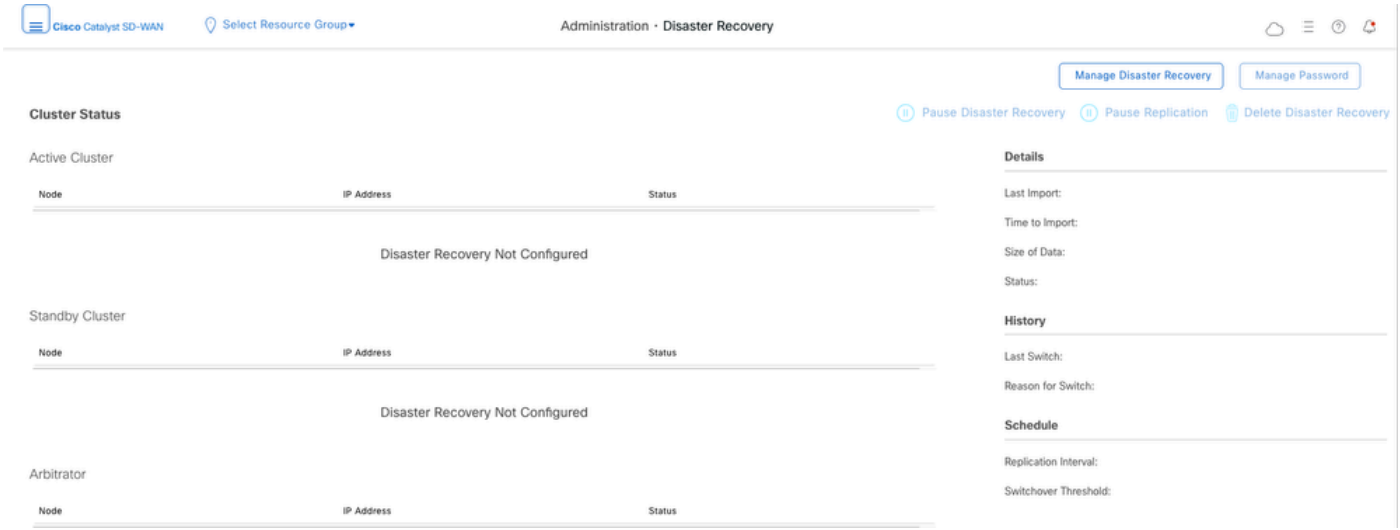
Rechenzentrums-vManager:



DR-vManager:



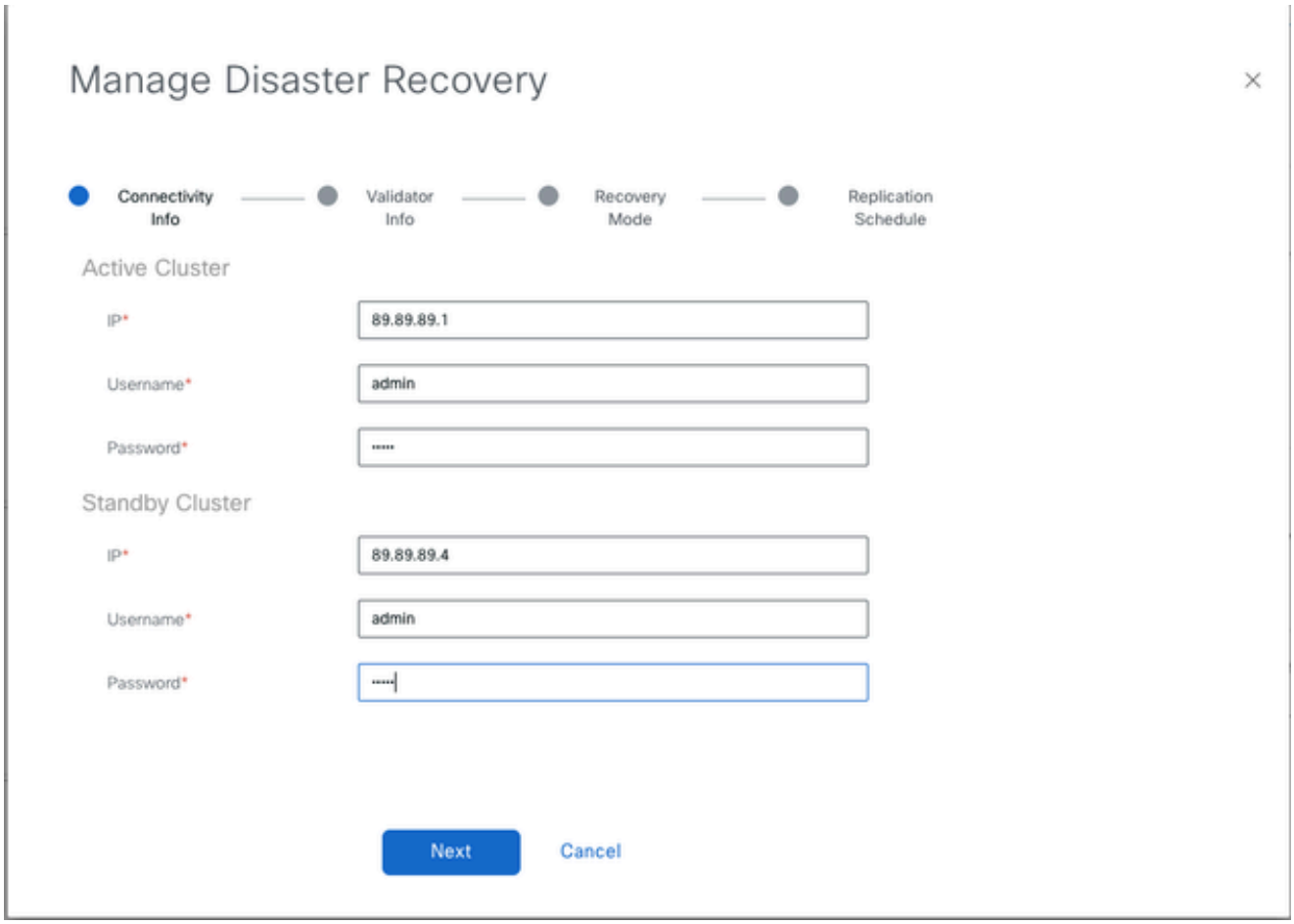
- Navigieren Sie zu Administration>Disaster Recovery. Klicken Sie auf Disaster Recovery verwalten.



- Geben Sie im Popup-Fenster die Details für den primären und sekundären vManage ein.

  Die anzuzeigenden IP-Adressen sind die IP-Adressen der Out-of-Band-Clusterschnittstellen.

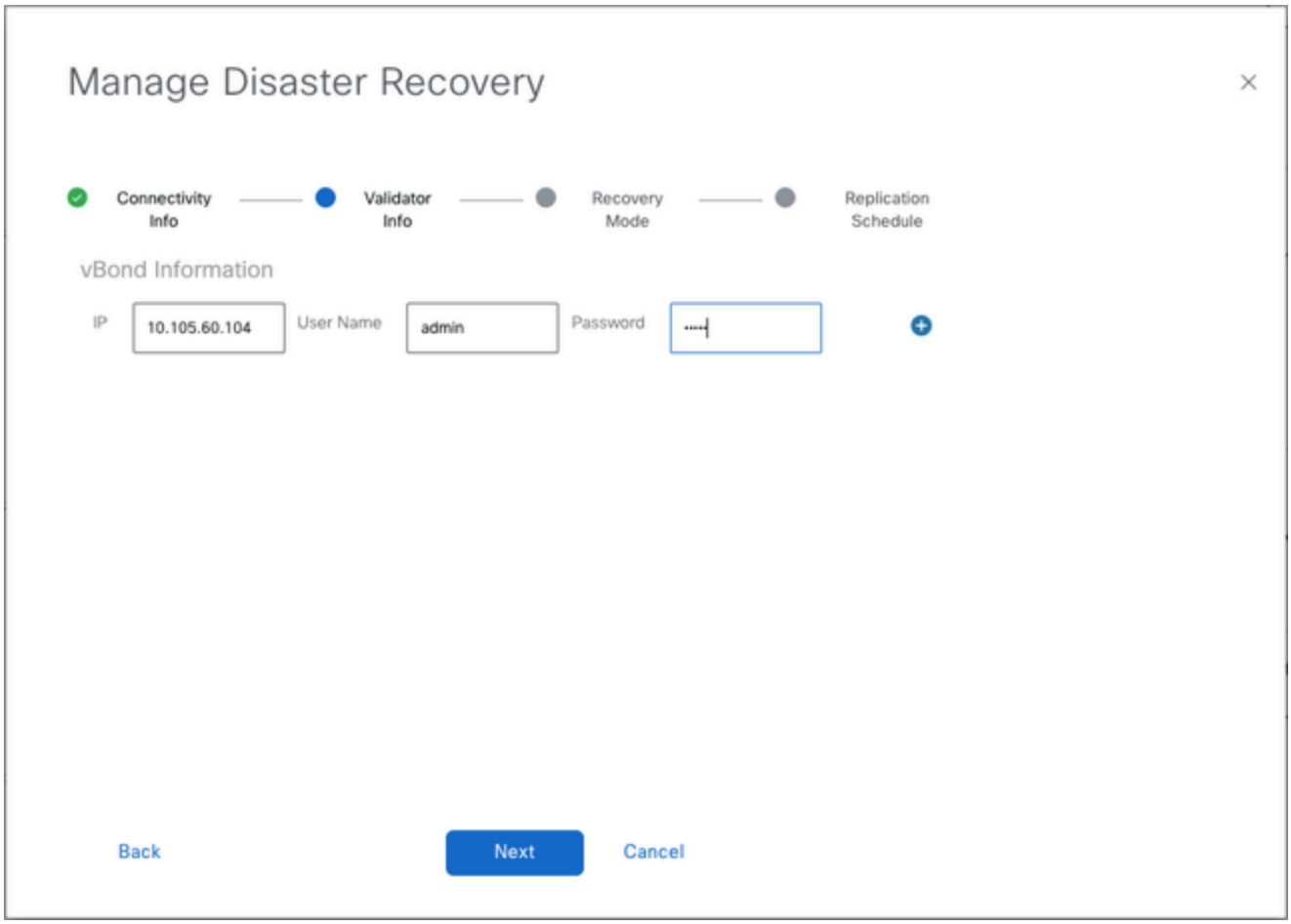
  Die Anmeldedaten müssen die eines netadmin-Benutzers sein. Sie dürfen nach der Konfiguration des DR nicht geändert werden, es sei denn, sie werden gelöscht.



Klicken Sie nach dem Ausfüllen auf Weiter.

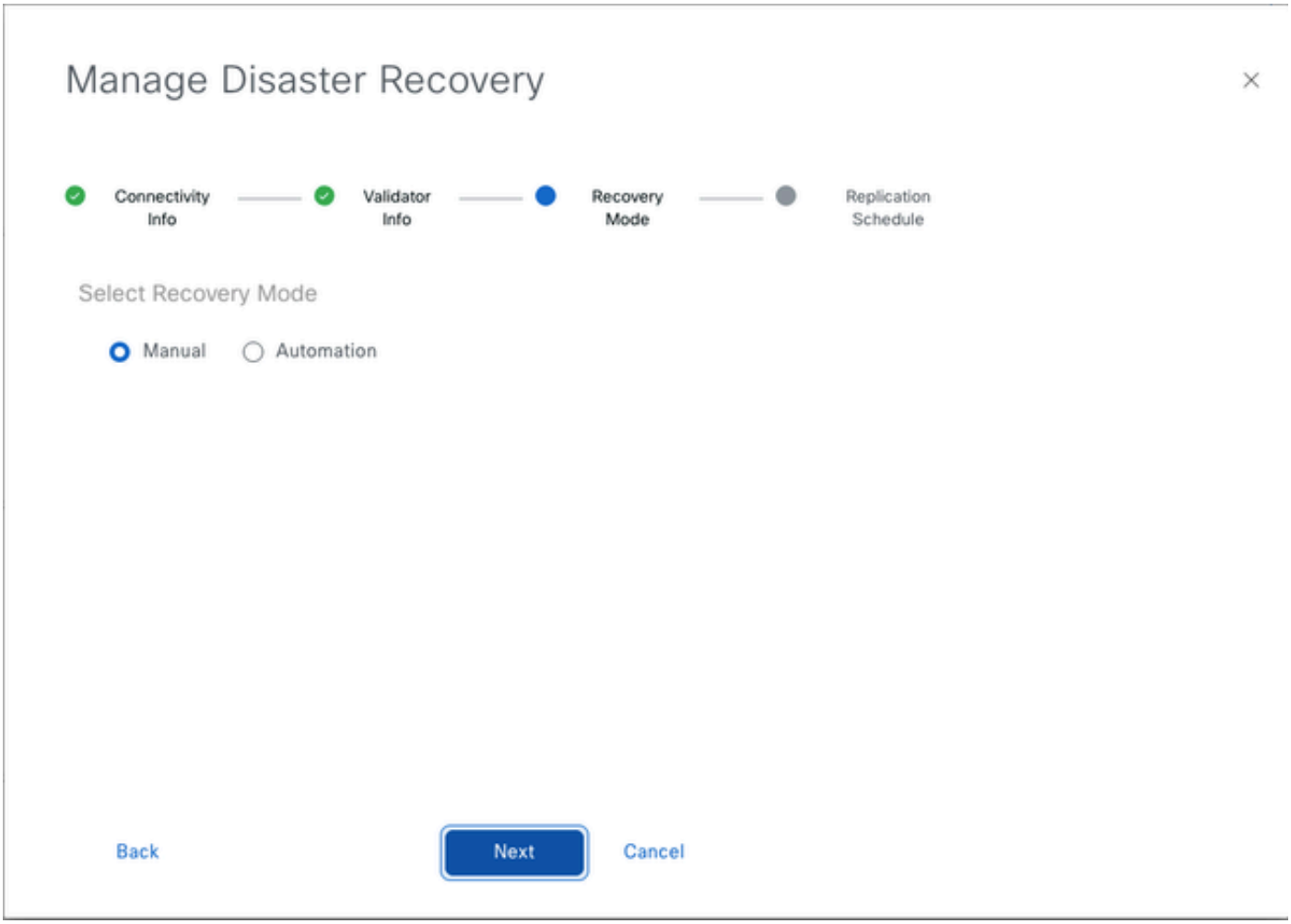
- Füllen Sie die Details der vBond-Controller aus.

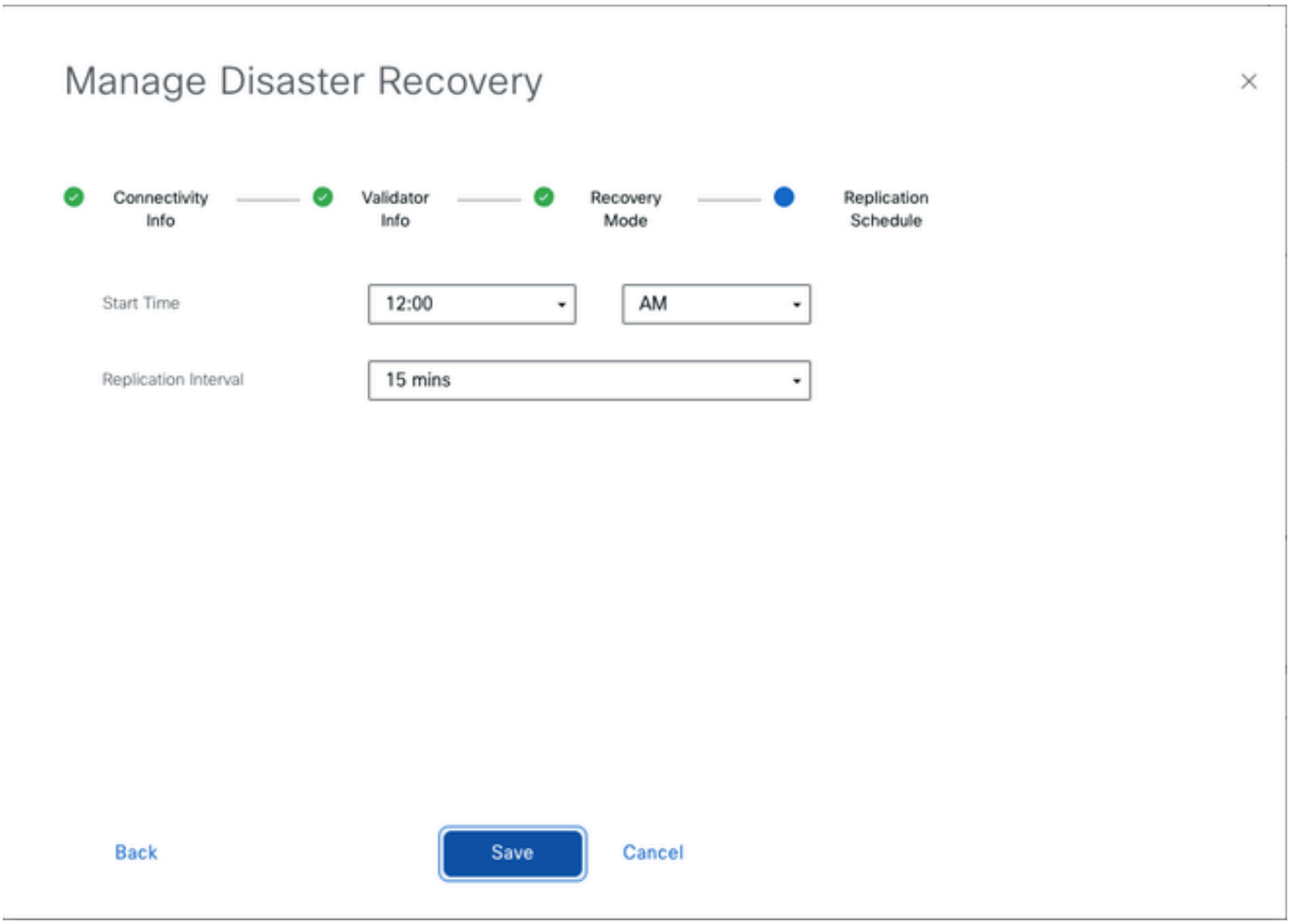
Die vBond-Controller müssen über Netconf in der angegebenen IP-Adresse erreichbar sein.



Klicken Sie nach dem Ausfüllen auf Weiter.

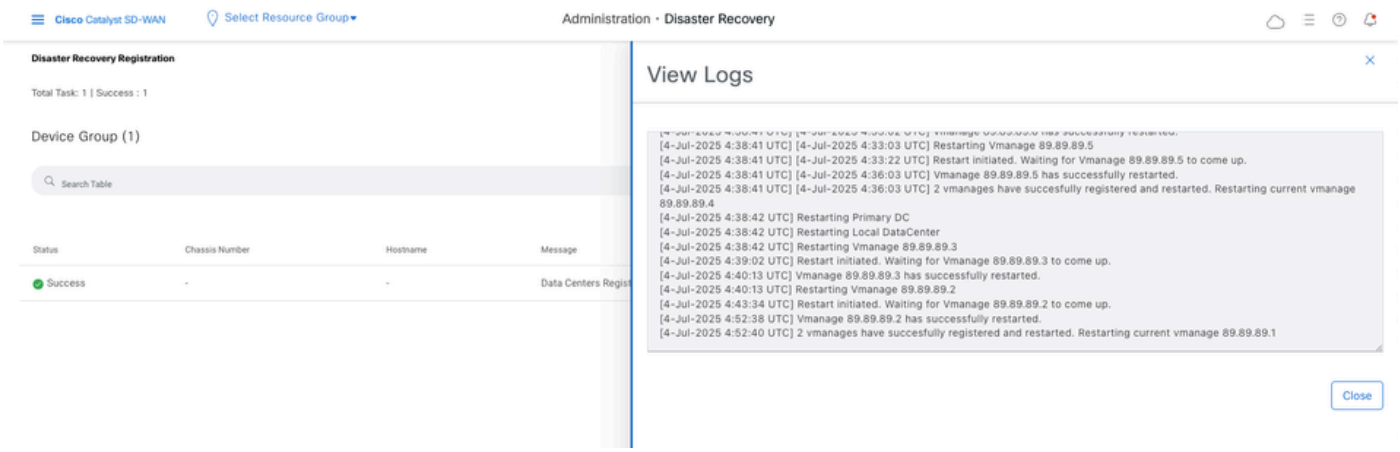
- Wählen Sie im Wiederherstellungsmodus die Option Manual (Manuell). Der Automatisierungsmodus ist veraltet. Klicken Sie auf Next (Weiter).


Manage Disaster Recovery
Connectivity Info
Validator Info
Recovery Mode
Replication Schedule
Select Recovery Mode
Manual
Automation
Back
Next
Cancel



Legen Sie den Wert fest, und klicken Sie auf Speichern.

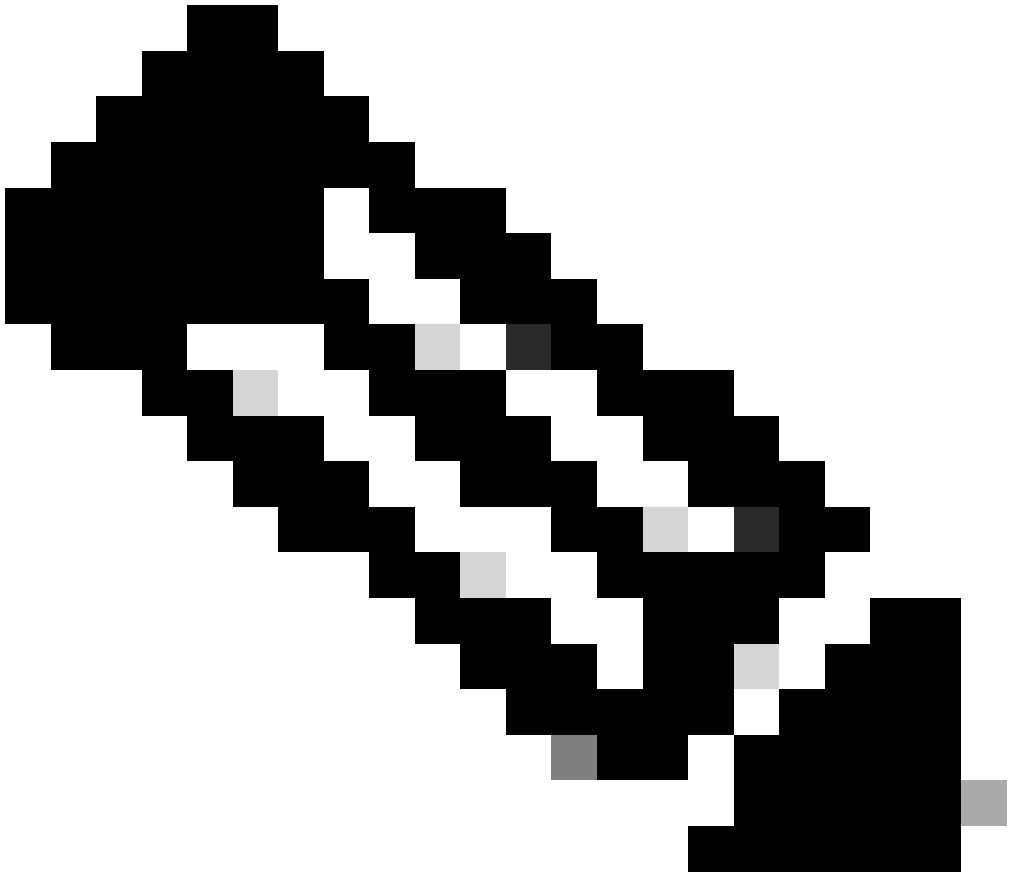
- Die DR-Registrierung beginnt jetzt. Klicken Sie auf die Aktualisierungsschaltfläche, um den Status und die Fortschrittsprotokolle manuell zu aktualisieren. Dieser Vorgang kann 20-30 Minuten dauern.



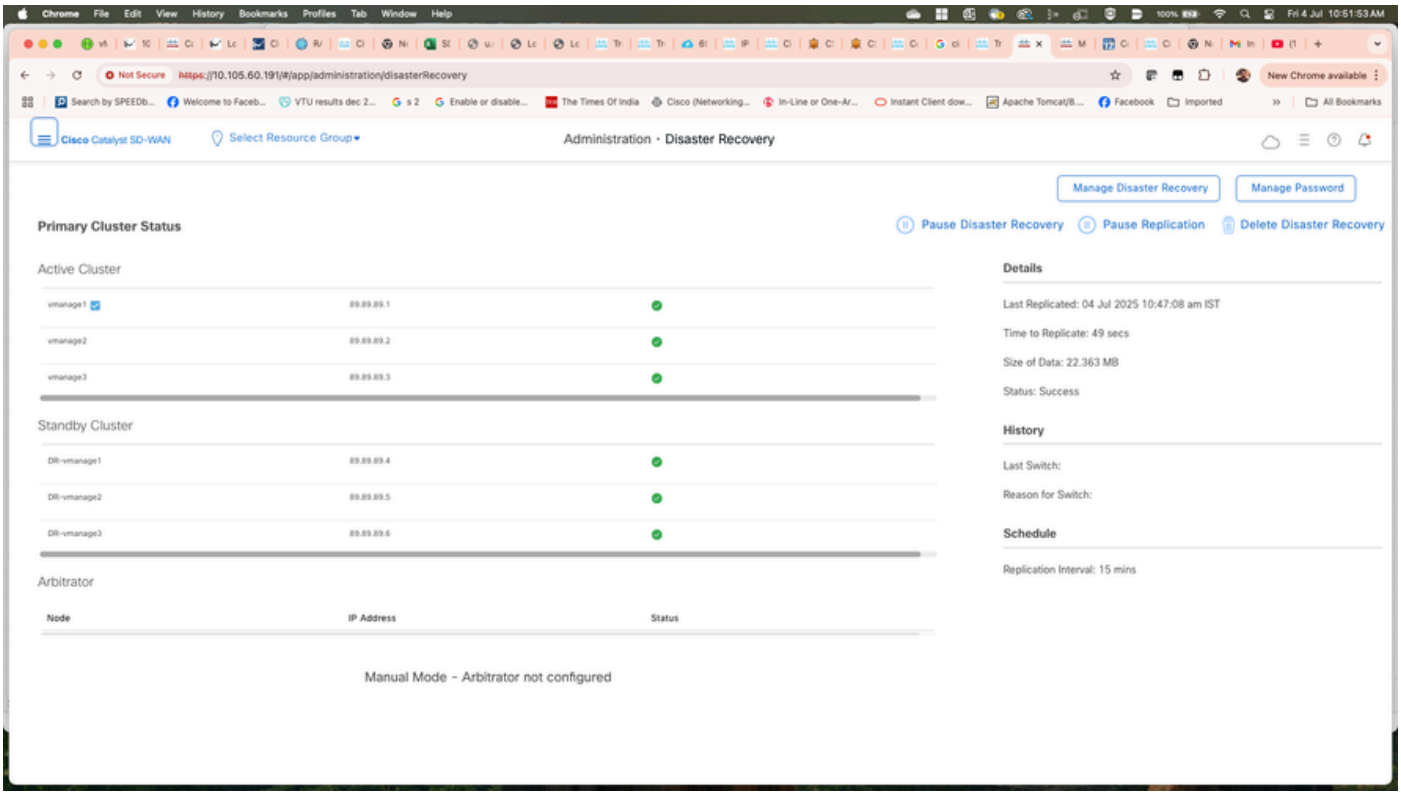
Verifizierung

- Navigieren Sie zu Administration>Disaster Recovery. um den Status der

Notfallwiederherstellung und den Zeitpunkt der letzten Replikation der Daten anzuzeigen.



Anmerkung: In diesem Szenario dauerte die Replikation nur 49 Sekunden, da die Laborumgebung über eine kleine Datenbank verfügt. Die Replikation kann je nach Datenbankgröße jedoch mehrere Stunden dauern. Außerdem kann es einige Zyklen dauern, bis die Replikation erfolgreich abgeschlossen ist.



Überprüfen Sie das Disaster Recovery-Protokoll in beiden Clustern.

```
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 da
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 Im
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
```

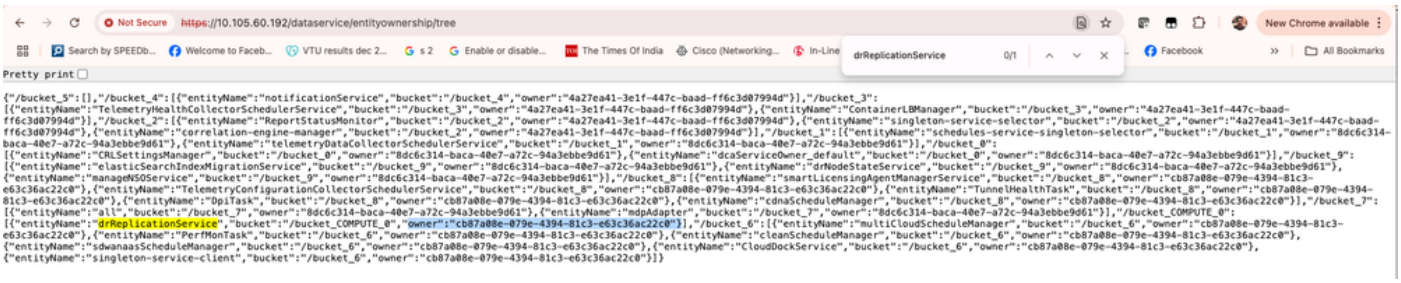
Wie wird der Replikations-Leader-Knoten überprüft?

- Verwenden Sie die nächste API, um den Replikations-Leader-Knoten auf beiden Clustern zu

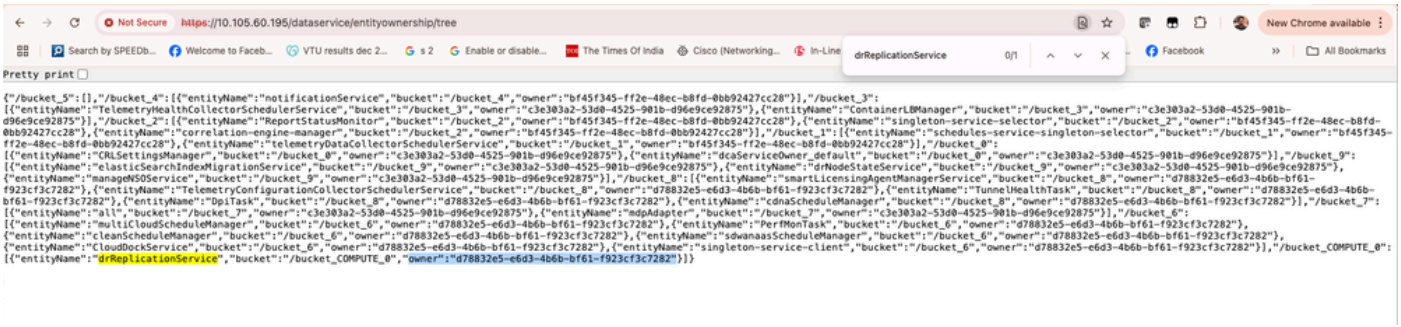
ermitteln:

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

Für DC-Cluster:
Der Replikationsknoten lautet cb87a08e-079e-4394-81c3-e63c36ac22c0, d. h. node1, überprüfen Sie ihn unter show control local-properties.



Ähnlich ist der Replikationsknoten für DR-vManage d78832e5-e6d3-4b6b-bf61-f923cf3c7282.



Kennwortaktualisierung bei Validator (vBond) nach Disaster Recovery-Registrierung

Wenn Sie das vBond-Kennwort nach Abschluss der Disaster Recovery-Registrierung ändern, schlägt ein Switchover fehl, da das vBond-Kennwort auf dem sekundären Cluster nicht aktualisiert wird, der weiterhin das alte vBond-Kennwort beibehält.

```
[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-serv
at com.viptela.vmanage.server.device.common.NetConfClient.

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

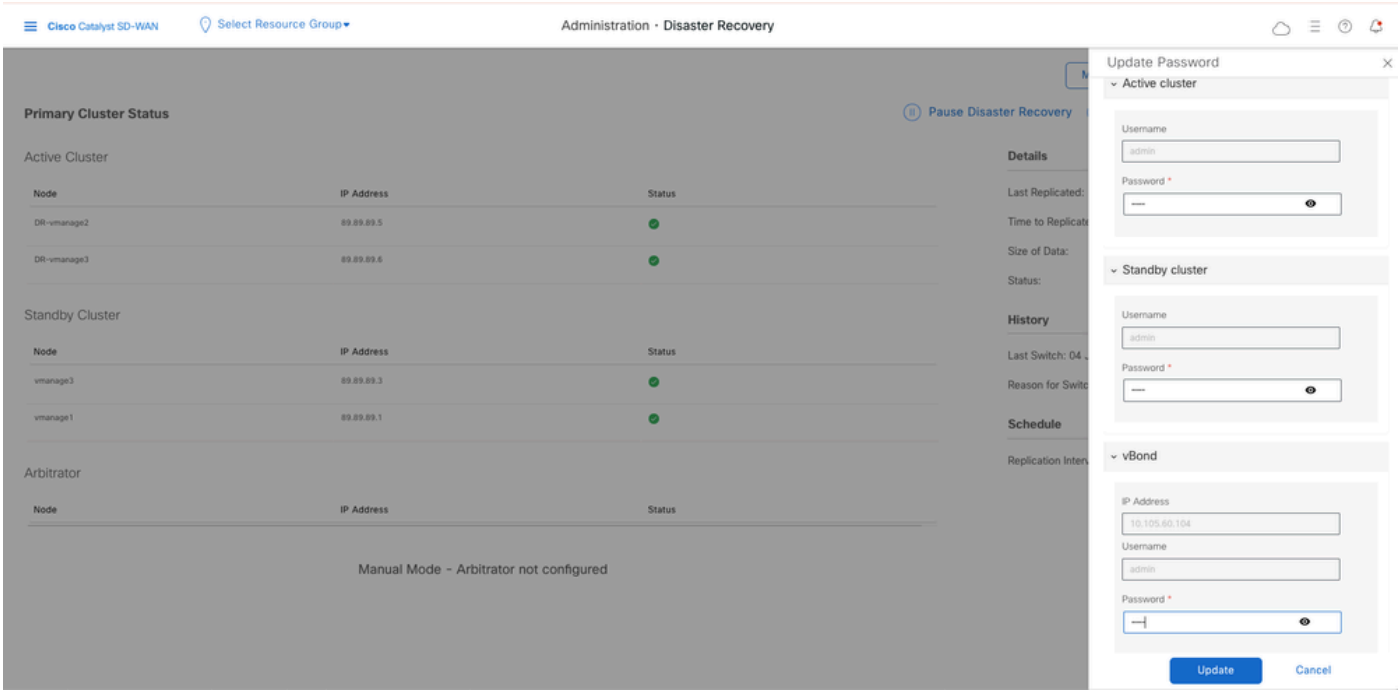
Kennwort des Validators aktualisieren (vbond)

Aktualisieren Sie das neue vBond-Kennwort sowohl auf der Seite Disaster Recovery als auch unter Manage Password:

Administration > Disaster Recovery > Manage Password > Update vBond password.

Stellen Sie sicher, dass die Replikation nach der Aktualisierung des Kennworts erfolgreich ist. Versuchen Sie erst nach Bestätigung der erfolgreichen Replikation, ein Failover durchzuführen.

caveat: https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwn19224.



Hinzufügen eines neuen Validators (vBond) zum Overlay nach der Disaster Recovery-Registrierung

Das Hinzufügen eines neuen Validierungssteuerelements zum SD-WAN-Overlay nach der Disaster Recovery-Registrierung wird nicht unterstützt, da das Disaster Recovery-Setup diese neuen Validierungsinformationen nicht kennt, da sie bei der Registrierung nicht aktualisiert wurden.

Obwohl Sie den Validator hinzufügen können, schlägt ein Switchover fehl.

Wenn Sie einen neuen Validator hinzufügen müssen, gehen Sie wie folgt vor:

1. Löschen Sie die Disaster Recovery-Konfiguration.

2. Fügen Sie den neuen Validator zum SD-WAN-Overlay hinzu.

3. Neukonfiguration der Notfallwiederherstellung

Disaster Recovery-Overlays aktualisieren

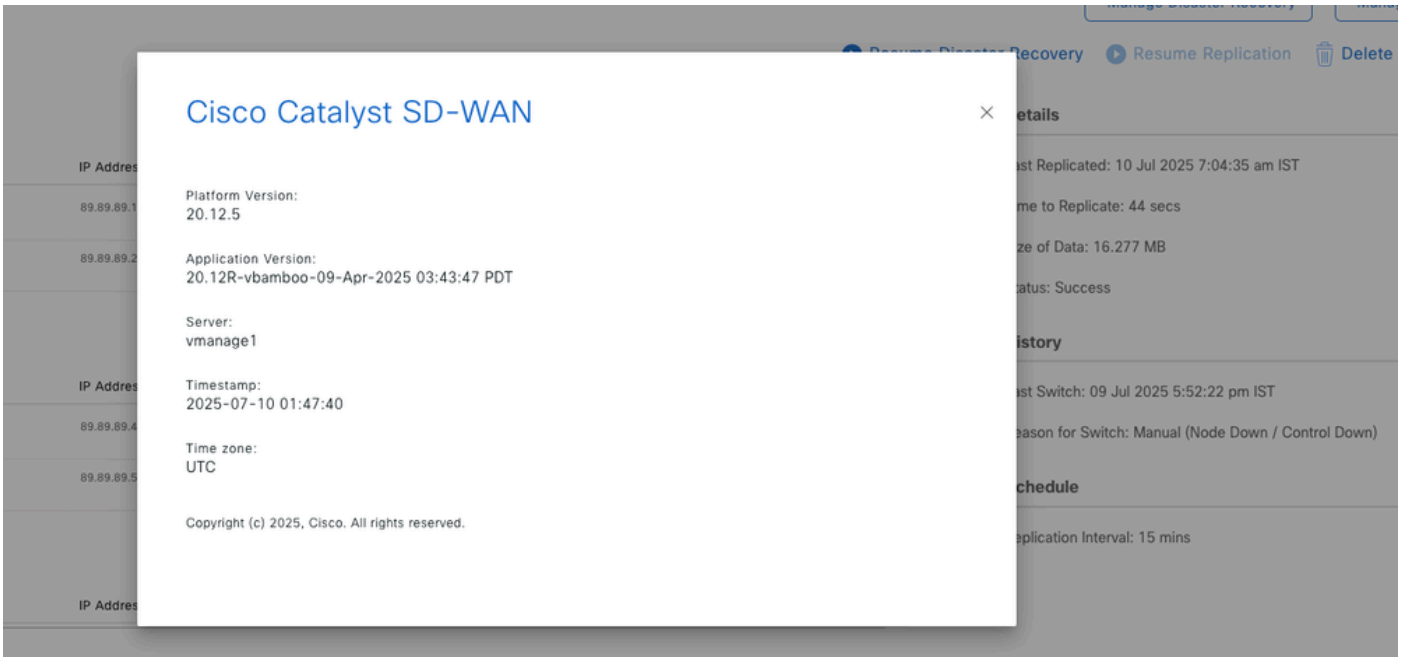
Vorbereitungen

- Verwenden Sie die CLI-Methode zum Upgrade des aktiven und des Standby-Cisco SD-WAN-Managers.
- Stellen Sie sicher, dass der Replikationsstatus auf der Seite Administration > Disaster Recover stabil ist und sich nicht in einem Übergangszustand befindet, wie z. B. Import Pending (Ausstehend), Export Pending (Ausstehend) oder Download Pending (Ausstehender Download). Der Status muss "Success" lauten, bevor die Notfallwiederherstellung angehalten werden kann.
- Unterbrechen Sie die Disaster Recovery mitDisaster Recovery unterbrechen unter Administration > Disaster Recovery Page.

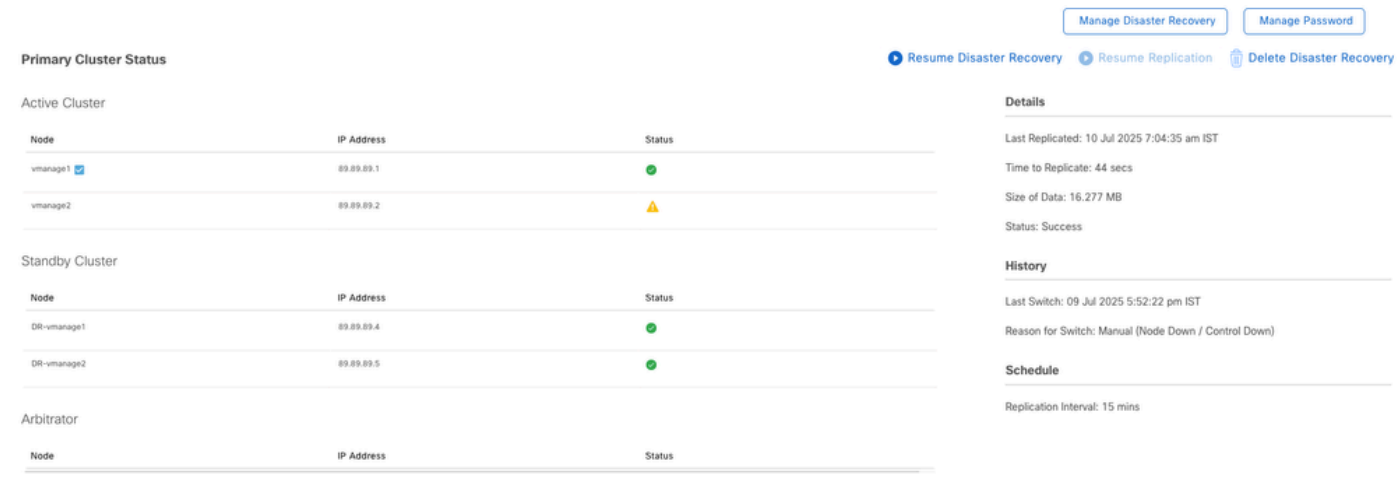
Upgrade-Prozess

In diesem Fall aktualisieren Sie den vManage-Cluster von 20.12.5 auf 20.15.2. Verwenden Sie die CLI-Methode, um den Cluster zu aktualisieren.

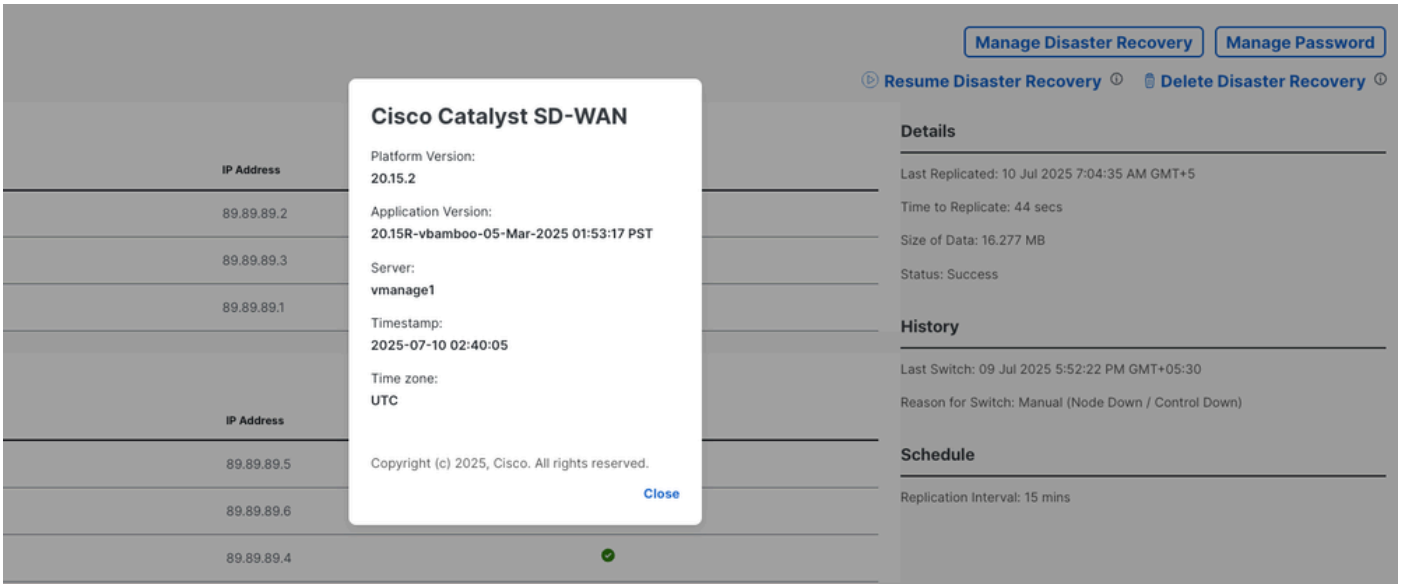
Überprüfen Sie vor dem Upgrade die Version und den Replikationsstatus.



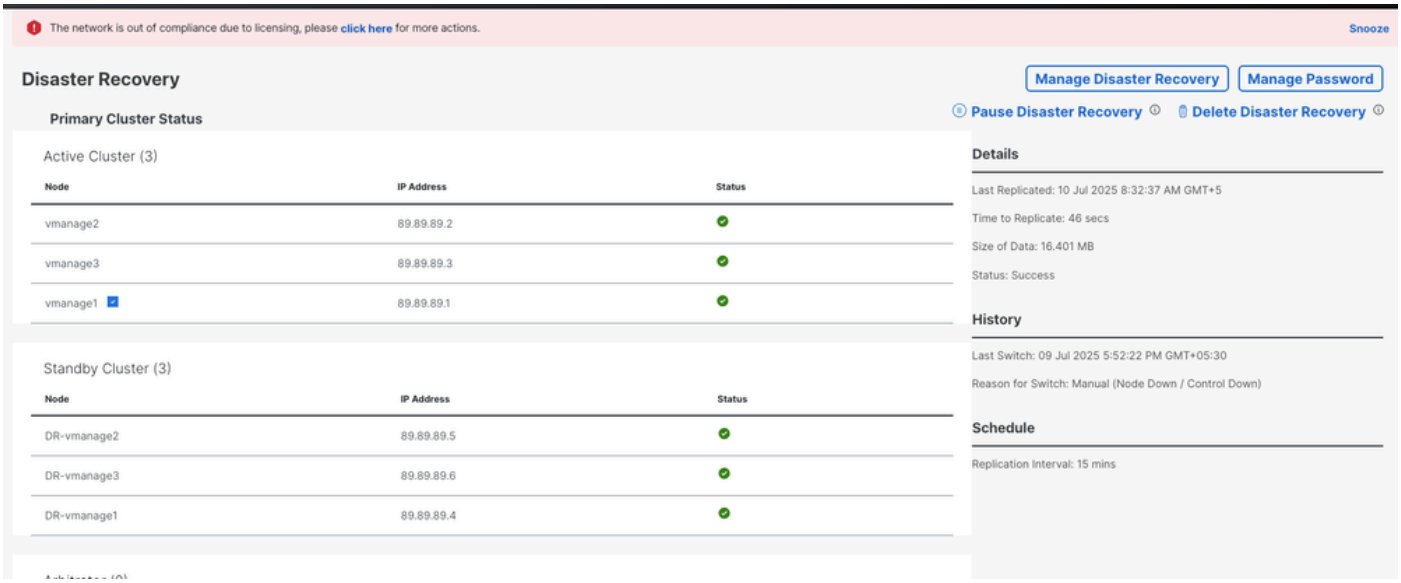
Disaster Recovery anhalten:



Stellen Sie nach dem Upgrade sicher, dass alle Dienste ausgeführt werden und dass Sie sich über die GUI bei allen vManage-Knoten (DC und DR) anmelden können.



die Notfallwiederherstellung fortsetzen; beginnt die Replikation, und der Replikationsstatus muss schließlich als erfolgreich angezeigt werden.



Zugehörige Informationen

- 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
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.