Cisco SDWAN Manager 3 Node Cluster Disaster Recovery

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

- Diagrama de la red
- Configuraciones

Verificación

¿Cómo se verifica el nodo de líder de replicación?

Actualización de contraseña de validador (vBond) tras el registro de recuperación ante desastres

- Contraseña del validador de actualización (vbond)
- Adición de un nuevo validador (vBond) a la superposición después del registro de recuperación ante desastres

Actualizar superposiciones de recuperación ante desastres

- Antes de comenzar
- Proceso de actualización

Información Relacionada

Introducción

Este documento describe la naturaleza stateful de Cisco vManage y su router designado (DR) principal/secundario, que permite la conmutación por fallo manual con replicación automática de datos.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de los clústeres de 3 nodos de vManage.
Se deben configurar y poner en funcionamiento dos clústeres independientes de 3 nodos de vManage para continuar con la recuperación ante desastres. En el clúster activo debe tener validadores y controladores incorporados. En caso de que tenga un validador y controladores en el sitio DR, también deben estar incorporados en el clúster activo y no en el clúster DR vManage.

Cisco recomienda que, antes de registrar la recuperación ante desastres, se cumplan estos

requisitos:

- Asegúrese de que el nodo principal y el secundario estén accesibles mediante HTTPS en una VPN de transporte (VPN 0).
- Asegúrese de que Cisco vSmart Controllers y Cisco vBond Orchestrators de la configuración secundaria estén conectados a la configuración principal.
- Asegúrese de que el nodo principal y el nodo secundario de Cisco vManage ejecutan la misma versión de Cisco vManage.
- Interfaz de clúster fuera de banda en VPN 0:
  - Para cada instancia de vManage de un clúster, se requiere una tercera interfaz (enlace de clúster) además de las interfaces utilizadas para VPN 0 (transporte) y VPN 512 (gestión).
  - Esta interfaz se utiliza para la comunicación y la sincronización entre los servidores vManage del clúster.
  - Esta interfaz debe tener al menos 1 Gbps y una latencia de 4 ms o menos. Se recomienda una interfaz de 10 Gbps.
  - Ambos nodos de vManage deben poder comunicarse entre sí a través de esta interfaz: ya sea un segmento de capa 2 o a través del routing de capa 3.
  - En cada vManage, esta interfaz se debe configurar en la GUI como una interfaz de clúster(Administration>Cluster Management- indica su propia dirección IP, usuario y contraseña de la interfaz de clúster fuera de banda).
  - Para permitir que los nodos de Cisco vManage se comuniquen entre sí en los Data Centers, habilite los puertos TCP 8443 y 830 en los firewalls de los Data Centers.
- Asegúrese de que todos los servicios (application-server, configuration-db, messaging server, coordinator server y statistics-db) estén habilitados en ambos nodos de Cisco vManage.
- Distribuya todos los controladores, incluidos los Cisco vBond Orchestrators, entre los Data Centers principales y secundarios. Asegúrese de que los nodos de Cisco vManage que se distribuyen por estos Data Centers puedan acceder a estos controladores. Los controladores solo se conectan al nodo principal de Cisco vManage.
- Asegúrese de que no hay otras operaciones en proceso en el nodo activo (principal) y en el nodo de Cisco vManage en espera (secundario). Por ejemplo, asegúrese de que ningún servidor esté en proceso de actualizar o adjuntar plantillas a los dispositivos.
- Desactive el servidor proxy HTTP/HTTPS de Cisco vManage si está activado. Consulte Servidor proxy HTTP/HTTPS para Cisco vManage Communication con servidores externos. Si no desactiva el servidor proxy, Cisco vManage intenta establecer la comunicación de recuperación ante desastres a través de la dirección IP del proxy, incluso si las direcciones IP del clúster fuera de banda de Cisco vManage son directamente accesibles. Puede volver a habilitar el servidor proxy HTTP/HTTPS de Cisco vManage una vez finalizado el registro de recuperación ante desastres.
- Antes de iniciar el proceso de registro de recuperación ante desastres, vaya a la ventana Tools > Rediscover Network del nodo principal de Cisco vManage y vuelva a descubrir Cisco vBond Orchestrators.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Administrador: 20.12.5
- Validador: 20.12.5
- Controlador: 20.12.5
- Perímetro: 17.12.5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

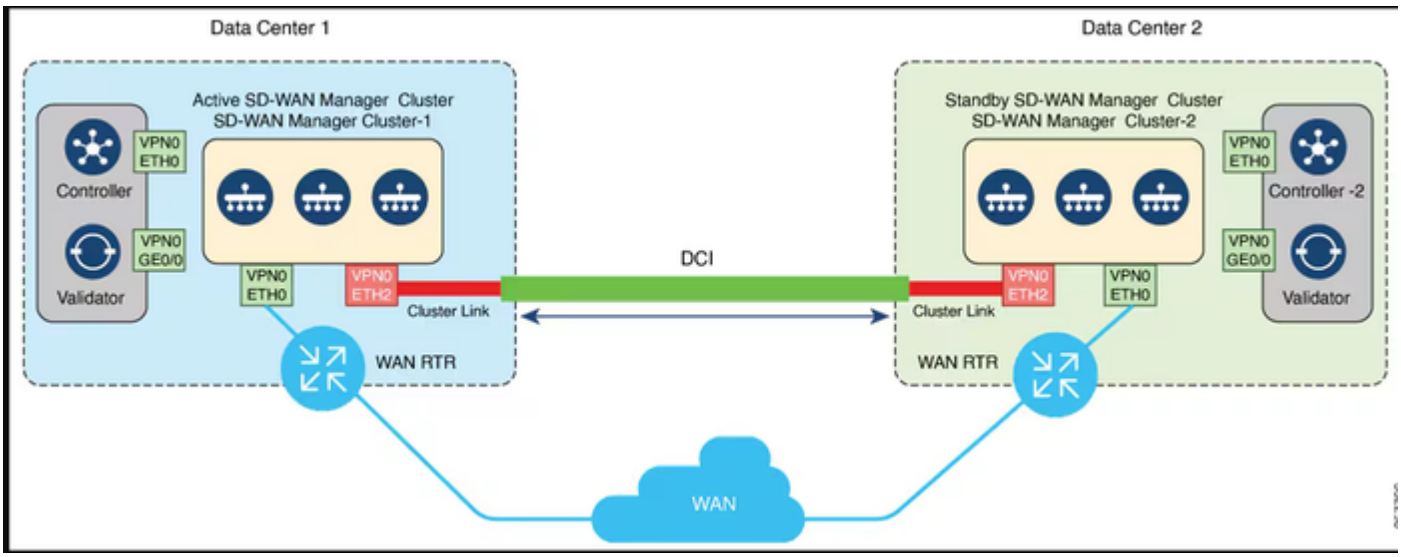
Antecedentes

La recuperación ante desastres proporciona un proceso de recuperación ante fallos activado por el administrador. Cuando se registra la recuperación ante desastres, los datos se replican automáticamente entre los clústeres de Cisco vManage principal y secundario. Si es necesario, se realiza manualmente una conmutación por error al clúster secundario.

Configurar

Diagrama de la red

Esta figura ilustra la arquitectura de alto nivel de la solución de recuperación ante desastres con un clúster de tres nodos.



Configuraciones

Para obtener más información sobre vManage Disaster Recovery, consulte este enlace.

Ya se han creado los dos clústeres de 3 nodos independientes, suponiendo que cada administrador de SD-WAN tiene una configuración mínima y que se ha completado la parte de

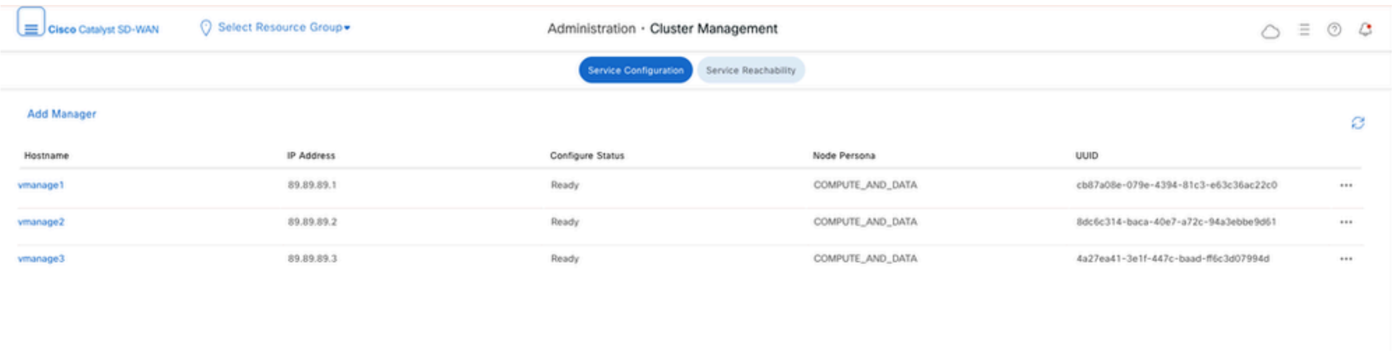
certificación.

```
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
```

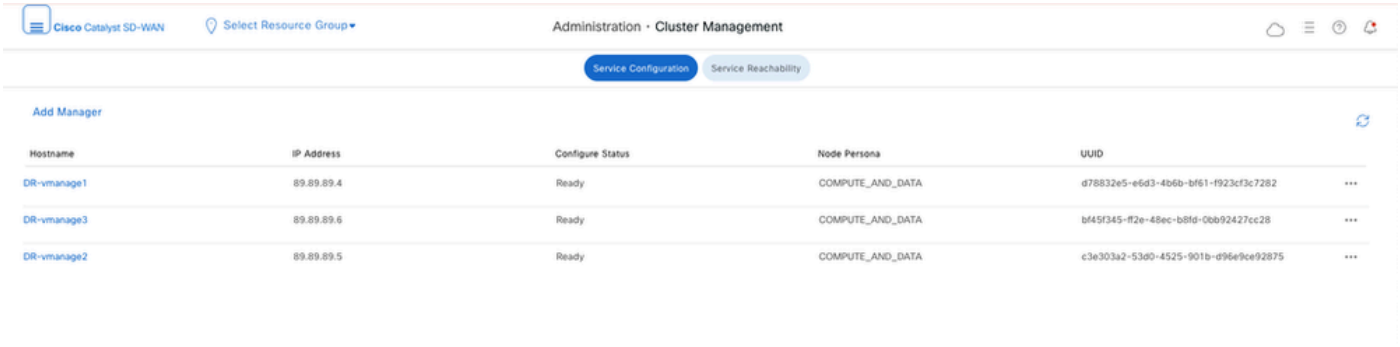
```
vpn 0
 interface eth0
  ip address 10.105.60.102/24
  ipv6 dhcp-client
  tunnel-interface
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service stun
   no allow-service https
  !
  no shutdown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

- Vaya a Administration > Cluster Management en ambos clústeres y verifique que todos los nodos estén en estado Ready.

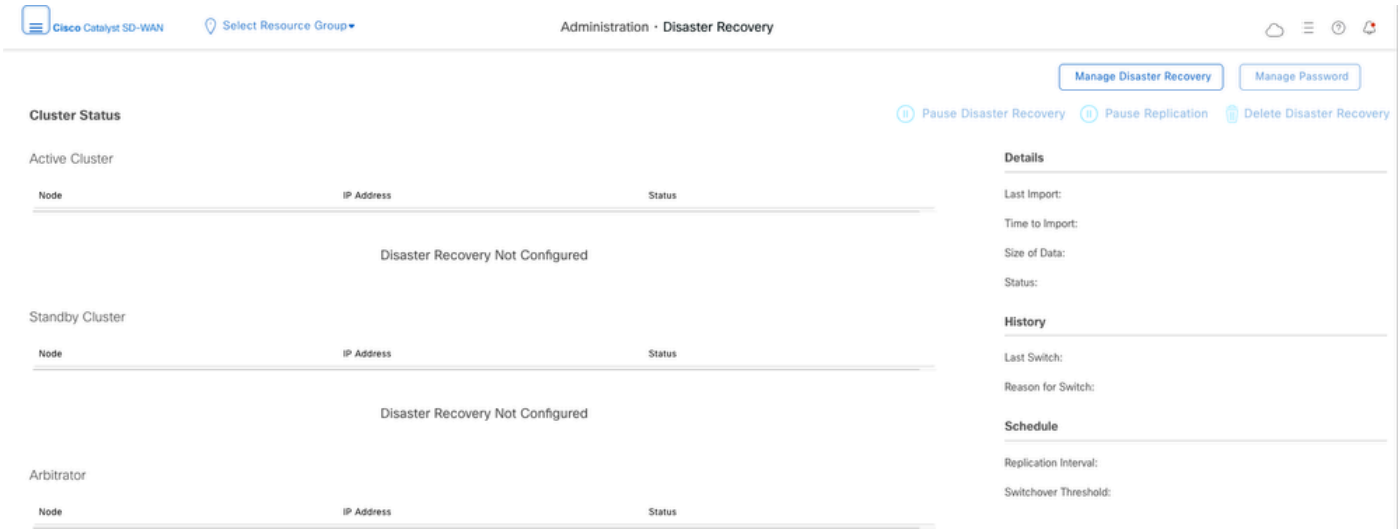
vManage de DC:



DR-vManage:



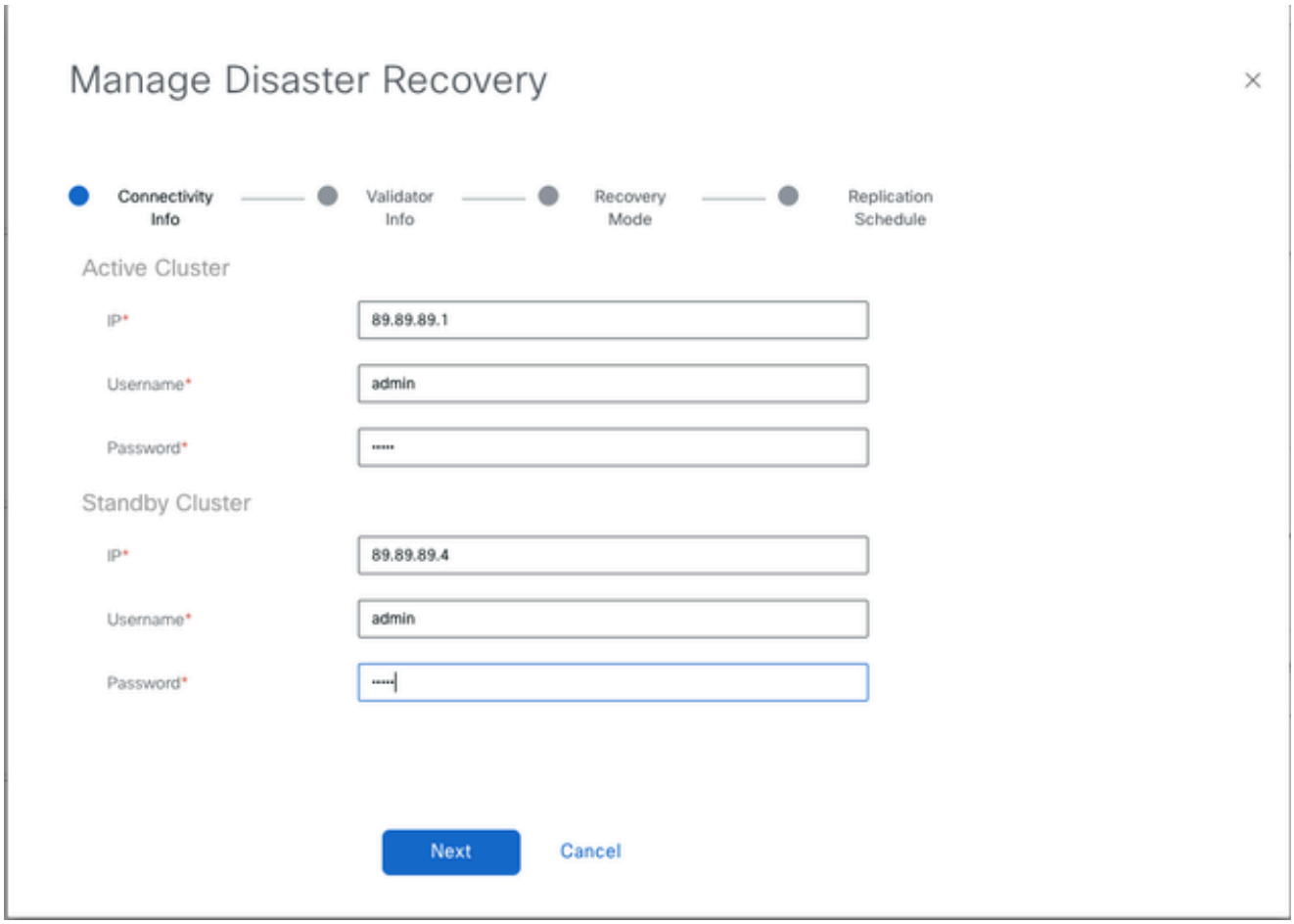
- Vaya a Administración>Recuperación ante desastres. Haga clic en Administrar recuperación ante desastres.



- En la ventana emergente, rellene los detalles de vManage principal y secundaria.

  Las direcciones IP que se deben indicar son las direcciones IP de las interfaces de clúster fuera de banda.

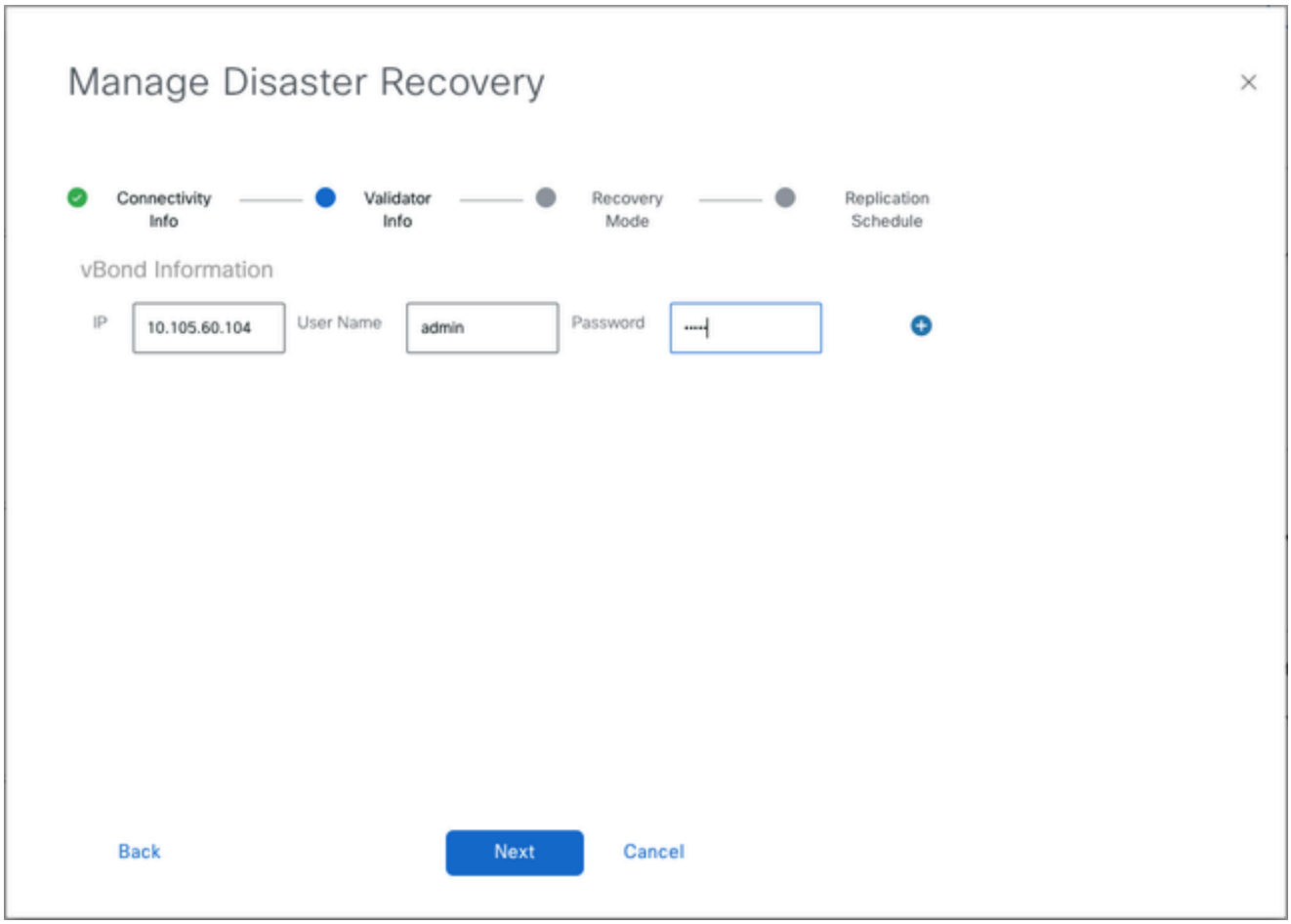
  Las credenciales deben ser las de un usuario netadmin y no deben cambiarse una vez configurado el DR, a menos que se elimine.



Una vez rellenado, haga clic en Next.

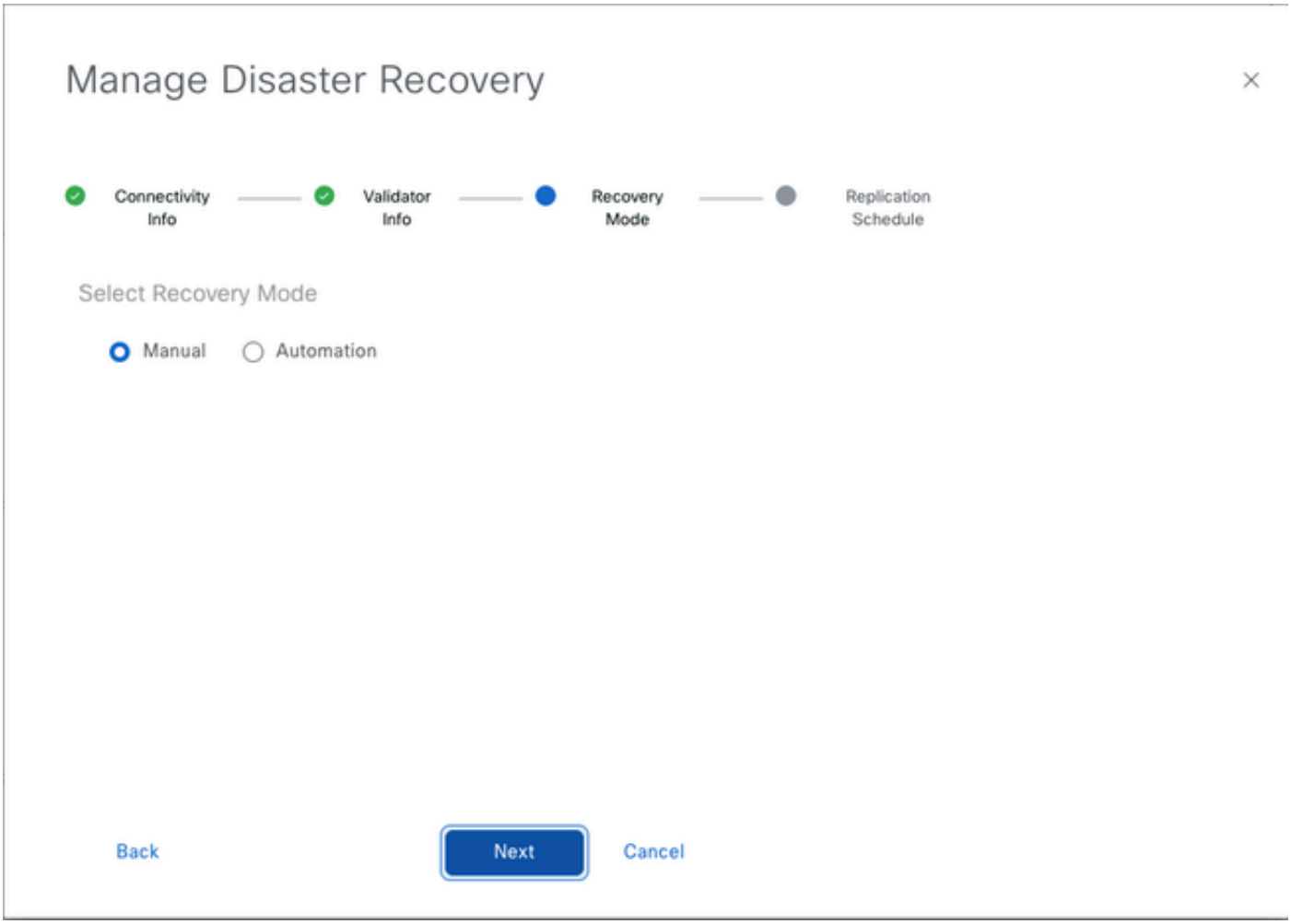
- Rellene los detalles de los controladores de vBond.

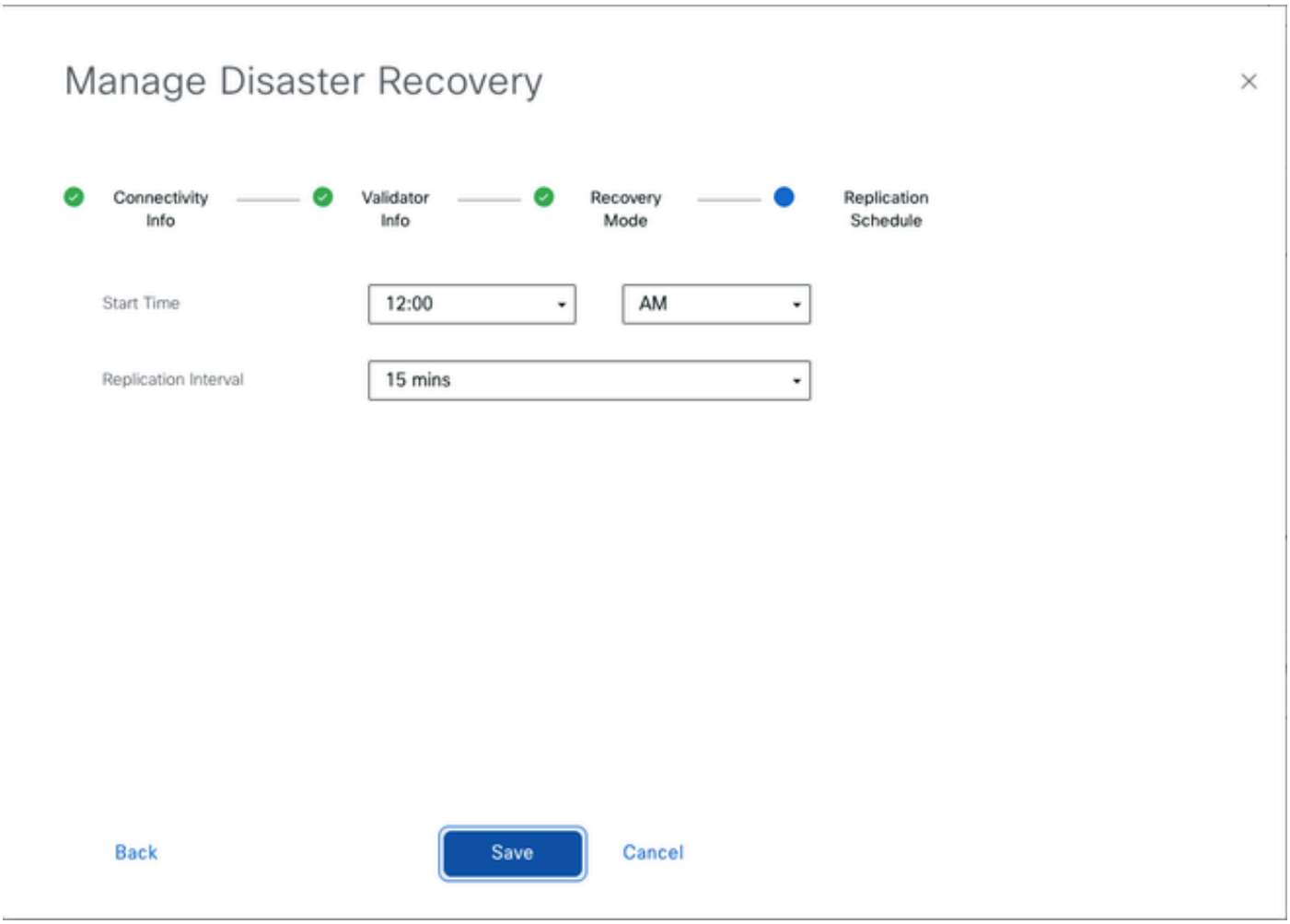
Los controladores vBond deben ser accesibles en la dirección IP especificada a través de Netconf.



Una vez rellenado, haga clic en Next.

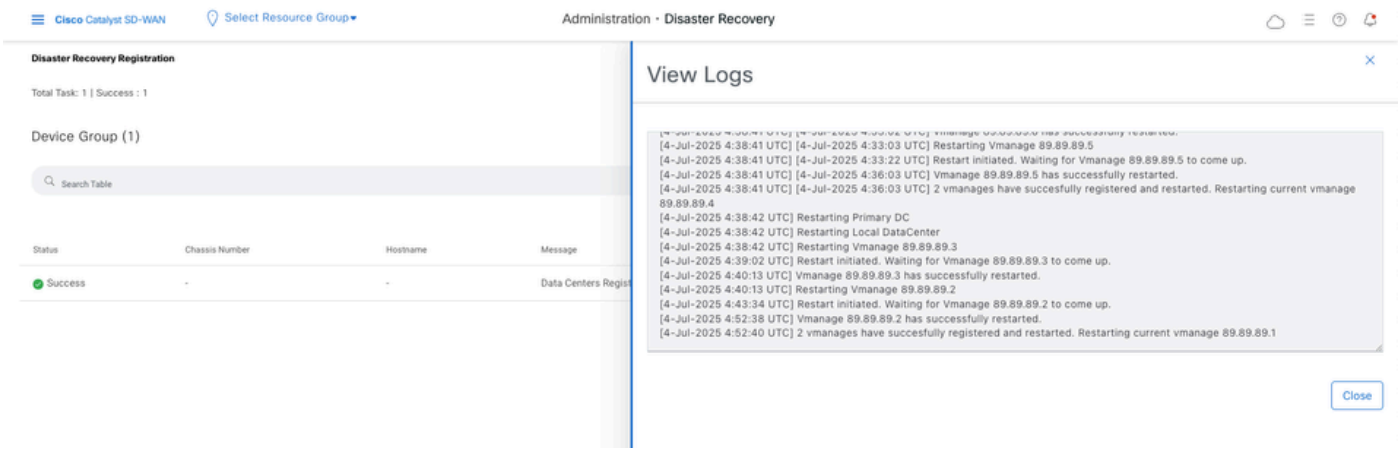
- En el modo de recuperación, seleccione Manual. El modo de automatización está obsoleto. Haga clic en Next (Siguiente).


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



Establezca el valor y haga clic en Guardar.

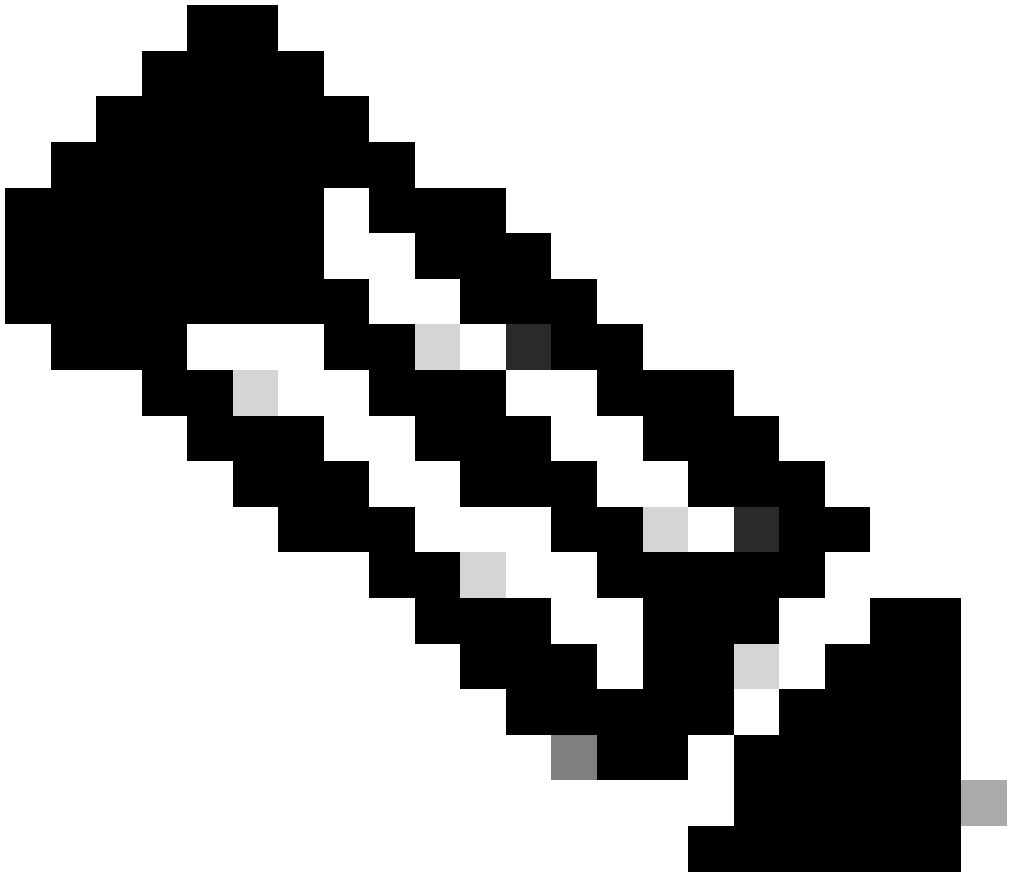
- El registro de DR comienza ahora. Haga clic en el botón Actualizar para actualizar manualmente el estado y los registros de progreso. Este proceso puede tardar hasta 20-30 minutos.



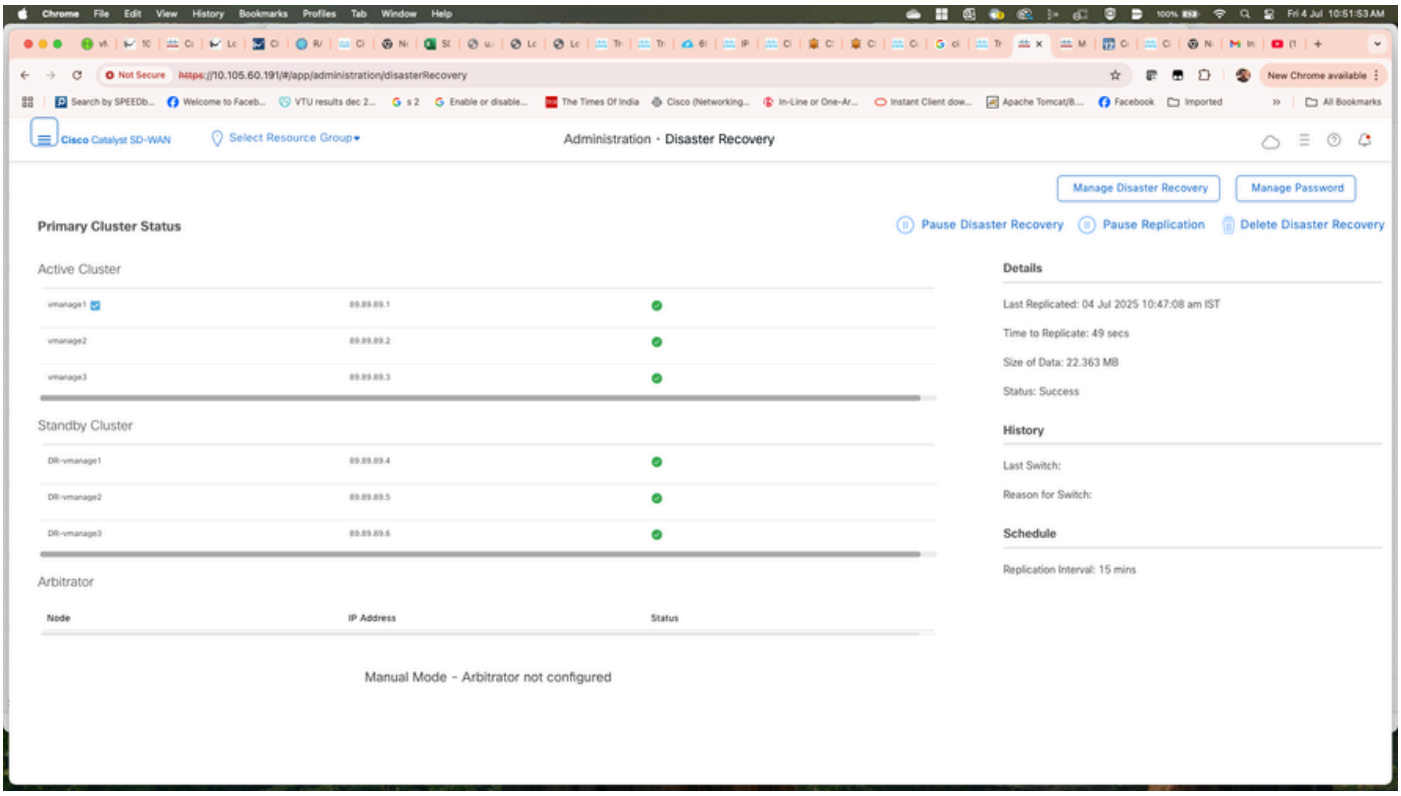
Verificación

- Vaya a Administración>Recuperación ante desastres para ver el estado de Recuperación

ante desastres y cuándo se replicaron los datos la última vez.



Nota: En esta situación, la replicación tardó sólo 49 segundos porque el entorno de laboratorio tiene una base de datos pequeña. Sin embargo, la replicación puede tardar varias horas en función del tamaño de la base de datos. Además, puede requerir algunos ciclos para lograr una replicación correcta.



Verifique el registro de recuperación ante desastres en ambos clústeres.

```
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 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
```

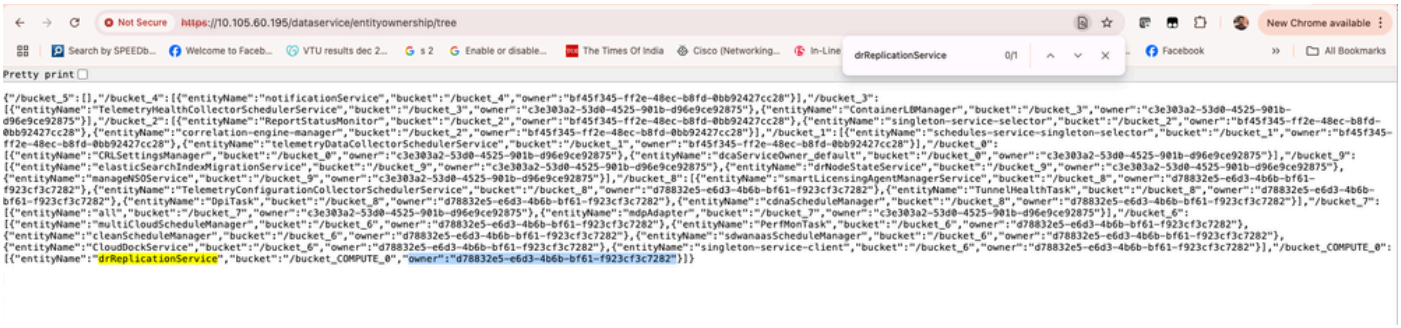
¿Cómo se verifica el nodo de líder de replicación?

- Utilice la siguiente API para averiguar el nodo de líder de replicación en ambos clústeres:

https://<vmanage-ip>/servicio de datos/propiedad de entidad/árbol.

Para el clúster de DC:
El nodo de replicación es cb87a08e-079e-4394-81c3-e63c36ac22c0, que es node1, verifíquelo desde show control local-properties.

De forma similar para DR-vManage, el nodo de replicación es d78832e5-e6d3-4b6b-bf61-f923cf3c7282.



Actualización de contraseña de validador (vBond) tras el registro de recuperación ante desastres

Si cambia la contraseña de vBond después de completar el registro de recuperación ante desastres, se produce un error en el switchover porque la contraseña de vBond no se actualiza en el clúster secundario, que aún conserva la contraseña de vBond antigua.

```
[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:?]
```

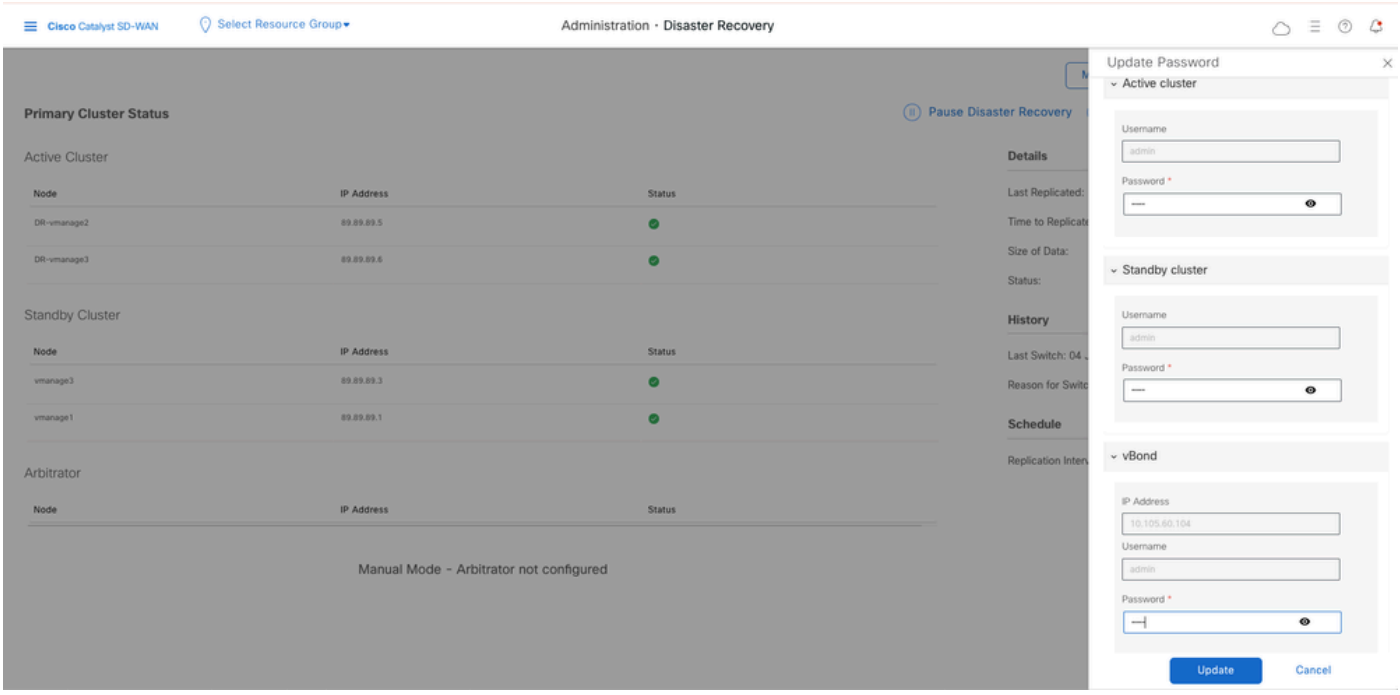
Contraseña del validador de actualización (vbond)

Asegúrese de actualizar la nueva contraseña de vBond tanto en la página Recuperación en caso de error como en Administrar contraseña:

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

Asegúrese de que la replicación se realice correctamente después de actualizar la contraseña. Intente una conmutación por error sólo después de confirmar que la replicación se ha realizado correctamente.

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



Adición de un nuevo validador (vBond) a la superposición después del registro de recuperación ante desastres

No se admite la adición de un nuevo validador a la superposición de SD-WAN después del registro de recuperación ante desastres, ya que la configuración de recuperación ante desastres no conoce esta nueva información del validador, ya que no se actualizó durante el registro.

Aunque puede agregar el validador, un switchover falla.

Si necesita agregar un nuevo validador, siga estos pasos:

1. Elimine la configuración de recuperación ante desastres.

2. Agregue el nuevo validador a la superposición SD-WAN.

3. Reconfigure la recuperación ante desastres.

Actualizar superposiciones de recuperación ante desastres

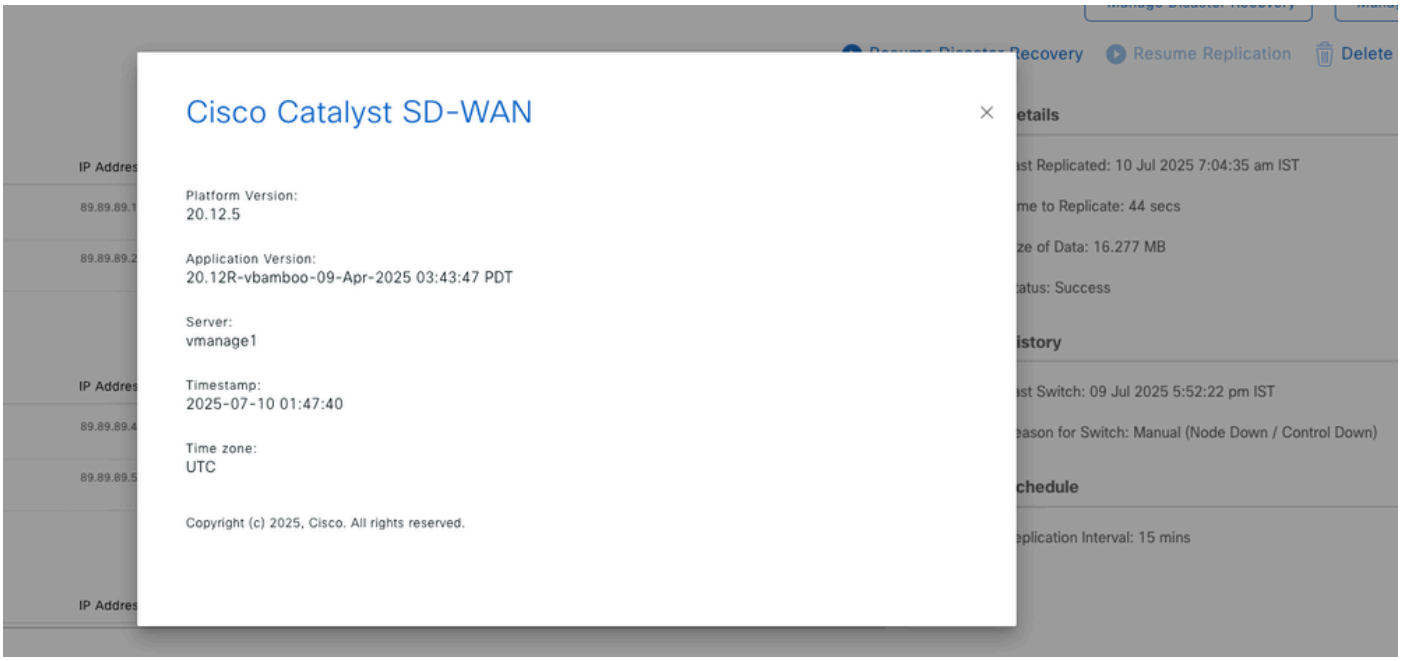
Antes de comenzar

- Utilice el método CLI para actualizar los Cisco SD-WAN Managers activos y en espera.
- Asegúrese de que el estado de replicación en la páginaAdministration > Disaster Recoverypage sea estable y no se encuentre en un estado transitorio comoImport Pending,Export Pending o Download Pending. Debe estar en el estado Correcto antes de pausar la recuperación ante desastres.
- Pause la recuperación ante desastres usandoPause Disaster Recovery bajo Administration > Disaster Recoverypage.

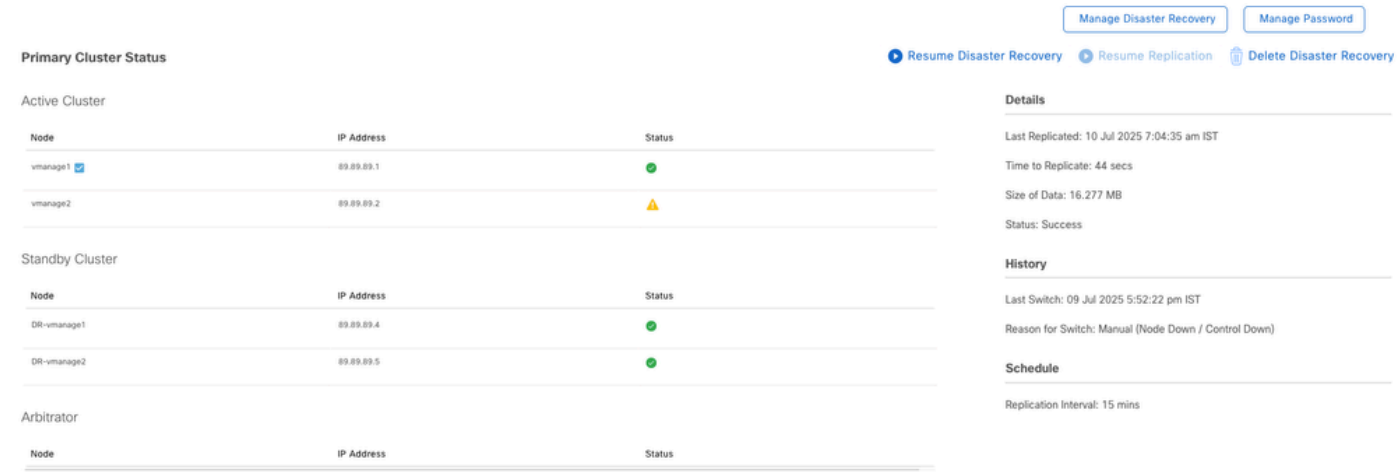
Proceso de actualización

En este caso, está actualizando el clúster de vManage de 20.12.5 a 20.15.2. Utilice el método CLI para actualizar el clúster.

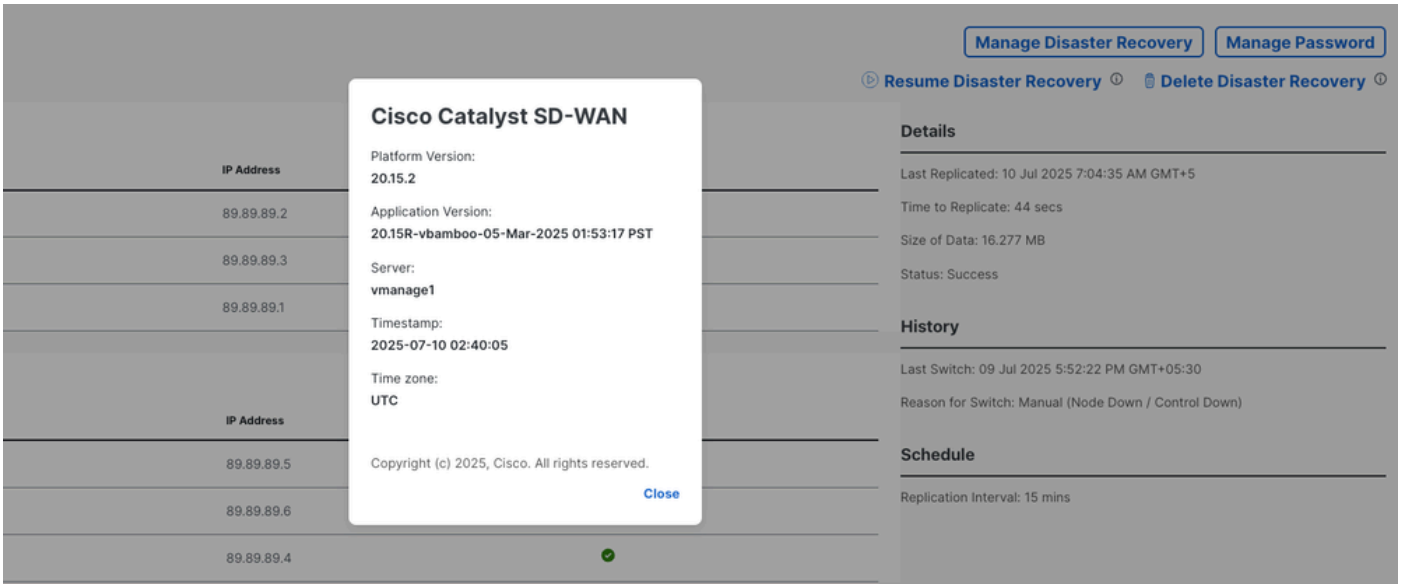
Antes de realizar la actualización, compruebe el estado de la versión y la replicación.



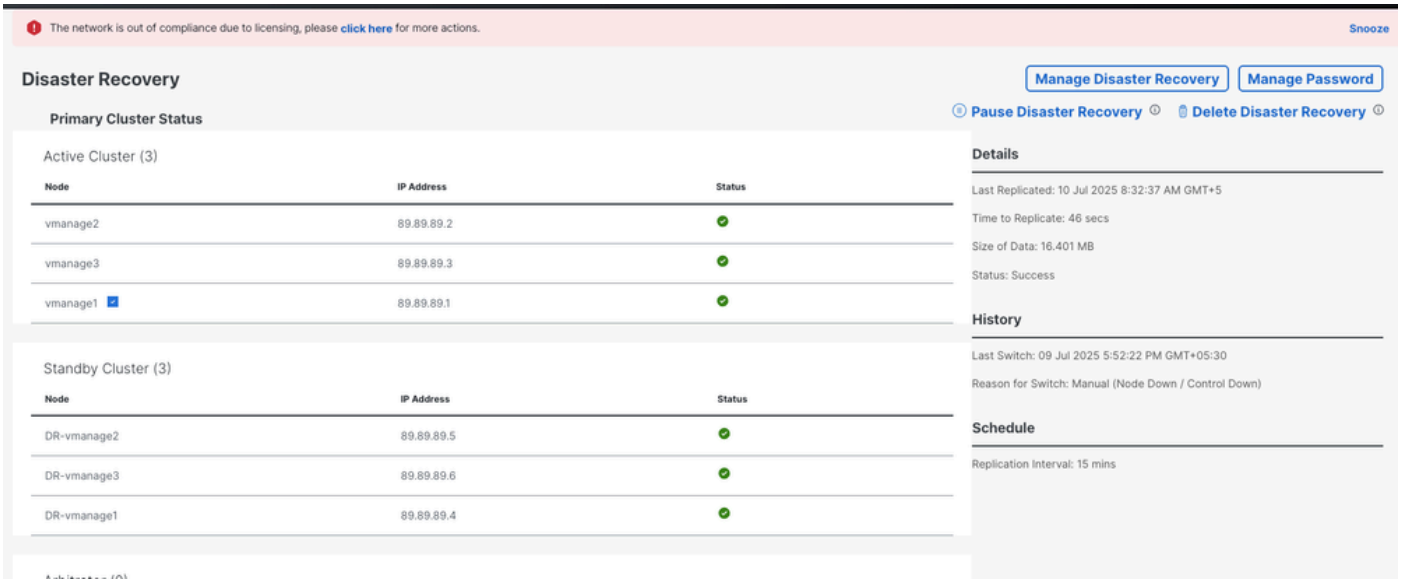
Pausar la recuperación ante desastres:



Después de la actualización, asegúrese de que todos los servicios se están ejecutando y de que puede iniciar sesión en todos los nodos de vManage (DC y DR) mediante la GUI.



Reanudar la recuperación ante desastres; la replicación se inicia y el estado de la replicación debe mostrarse como correcto.



Información Relacionada

- 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
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).