SAN configurations in a MetroCluster environment

ONTAP 9

NetApp
March 21, 2023

Table of Contents

SAN configurations in a MetroCluster environment

SAN configurations in a MetroCluster environment

You must be aware of certain considerations when using SAN configurations in a MetroCluster environment.

- MetroCluster configurations do not support front-end FC fabric “routed” vSAN configurations.
- Beginning with ONTAP 9.12.1, four-node MetroCluster IP configurations are supported on NVMe/FC. MetroCluster configurations are not supported for NVMe prior to ONTAP 9.12.1.
- Other SAN protocols such as iSCSI, FC, and FCoE are supported on MetroCluster configurations.
- When using SAN client configurations, you must check whether any special considerations for MetroCluster configurations are included in the notes that are provided in the NetApp Interoperability Matrix Tool (IMT).
- Operating systems and applications must provide an I/O resiliency of 120 seconds to support MetroCluster automatic unplanned switchover and Tiebreaker or Mediator-initiated switchover.
- The MetroCluster is using the same WWPNs on both sides of the front-end SAN.

Related information

Understanding MetroCluster data protection and disaster recovery

For further MetroCluster-specific host information, refer to the following NetApp Knowledge Base articles:

What are AIX Host support considerations in a MetroCluster configuration?

Solaris host support considerations in a MetroCluster configuration

Prevent port overlap between switchover and switchback

In a SAN environment, you can configure the front-end switches to avoid overlap when the old port goes offline and the new port comes online.

During switchover, the FC port on the surviving site might log in to the fabric before the fabric has detected that the FC port on the disaster site is offline and has removed this port from the name and directory services.

If the FC port on the disaster is not yet removed, the fabric login attempt of the FC port at the surviving site might be rejected due to a duplicate WWPN. This behavior of the FC switches can be changed to honor the login of the previous device and not the existing one. You should verify the effects of this behavior on other fabric devices. Contact the switch vendor for more information.

Choose the correct procedure according to your switch type.

Example 1. Steps

Cisco switch

1. Connect to the switch and log in.
2. Enter configuration mode:

```
switch# config t
switch(config)#
```

3. Overwrite the first device entry in the name server database with the new device:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. In switches that are running NX-OS 8.x, confirm that the flogi quiesce timeout is set to zero:
   a. Display the quiesce timerval:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. If the output in the previous step does not indicate that the timerval is zero, then set it to zero:

   ```
   switch(config)# flogi scale enable

   switch(config)$ flogi quiesce timeout 0
   ```

Brocade switch

1. Connect to the switch and log in.
2. Enter the `switchDisable` command.
3. Enter the `configure` command, and press `y` at the prompt.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Choose setting 1:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Respond to the remaining prompts, or press **Ctrl + D**.

6. Enter the `switchEnable` command.

Related information

Performing switchover for tests or maintenance

Copyright information

Trademark information