

Focus Lab 12: FC-SP

Overview

Fabric Channel Security Protocol (FC-SP) provides switch-to-switch and host-to-switch authentication. In this lab you will learn how to perform switch-to-switch authentication using locally stored and remotely stored passwords. Remote authentication will be done using AAA server.

The following features are covered in this Focus Lab:

- FC-SP Fabric Security
- FC-SP with local authentication
- FC-SP with AAA authentication

ieMentor Storage VRACK support

Our VRACK is fully compliant with this lab.

Lab Tasks

12.1: Your manager is concerned that port-security and fabric-binding are not effective against WWN spoofing. Configure FC-SP authentication between MDS1 and MDS2:

- MDS1 password is `mds1password2`. MDS1 uses this password for authenticating only with MDS2.
- MDS2 password is `mds2password`. MDS2 uses this password for authenticating with any neighbor.
- MDS1 Port-Channel 1 initiates FC-SP challenge every half an hour. If MDS2 fails to respond, the link should stay up.
- MDS2 Port-Channel 1 does not require authentication, but supports it
- MDS1 fc1/8 – MDS2 fc1/8 link requires authentication. Re-authenticate every two hours.
- Disable authentication support on the MDS1 fc1/7 – MDS2 fc1/7 link
- MDS1 uses local authentication
- MDS2 should authenticate neighbors using remote TACACS+ running on WIN1 ACS server
- If TACACS+ server is not running, MDS2 should authenticate MDS1 using local database

12.2: Configure fabric security between MDS1 and MDS3:

- MDS1 password is `mds1password`. MDS1 uses this password for authentication with all neighbors.
- MDS3 password is `mds3password1`. This password is used for authentication with MDS1.
- MDS1 fc1/14 requires authentication. The link is brought down if no response is received within 20 seconds.
- MDS3 fc1/3 will never initiate authentication, but will respond to the DH-CHAP challenge
- MDS1 Port-Channel 2 attempts to authenticate with MDS3. If no FC-SP response is received, the Port-Channel should still come up.
- The first member of the MDS3 Port-Channel 2 requires FC-SP authentication
- The second member of the MDS3 Port-Channel 2 doesn't support FC-SP authentication
- MDS1 uses local authentication
- MDS3 must authenticate FC-SP challenges on the remote RADIUS server running on MGMT PC IAS server

12.3: Configure DH-CHAP authentication mechanism between MDS2 and MDS3:

- MDS2 password is `mds2password3`. The MD5 hash of this password must be sent to MDS3 only. SHA1 is not supported.
- MDS3 password is `mds3password2`. The SHA1 hash of this password must be sent to MDS2 only. Allow failover to MD5.
- Both sides of the MDS2 fc1/15 – MDS3 fc1/15 link support authentication, but never attempt to initiate it
- Both sides of the MDS2 fc1/14 – MDS3 fc1/14 link can bring up the link without authentication, but they still attempt to authenticate
- Disable authentication support on MDS2 Port-Channel 128
- Leave authentication support default on MDS3 Port-Channel 128
- MDS2 must authenticate DH-CHAP challenges using TACACS+ running on WIN1 ACS server
- MDS3 must authenticate DH-CHAP challenges using RADIUS running on MGMT PC IAS server

12.4: Make sure Diffie-Hellman 1536-bit is exchanged between MDS switches