



IP switch maintenance and replacement

ONTAP MetroCluster

NetApp
December 14, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap-metrocluster/maintain/task_replace_an_ip_switch.html on December 14, 2022. Always check docs.netapp.com for the latest.

Table of Contents

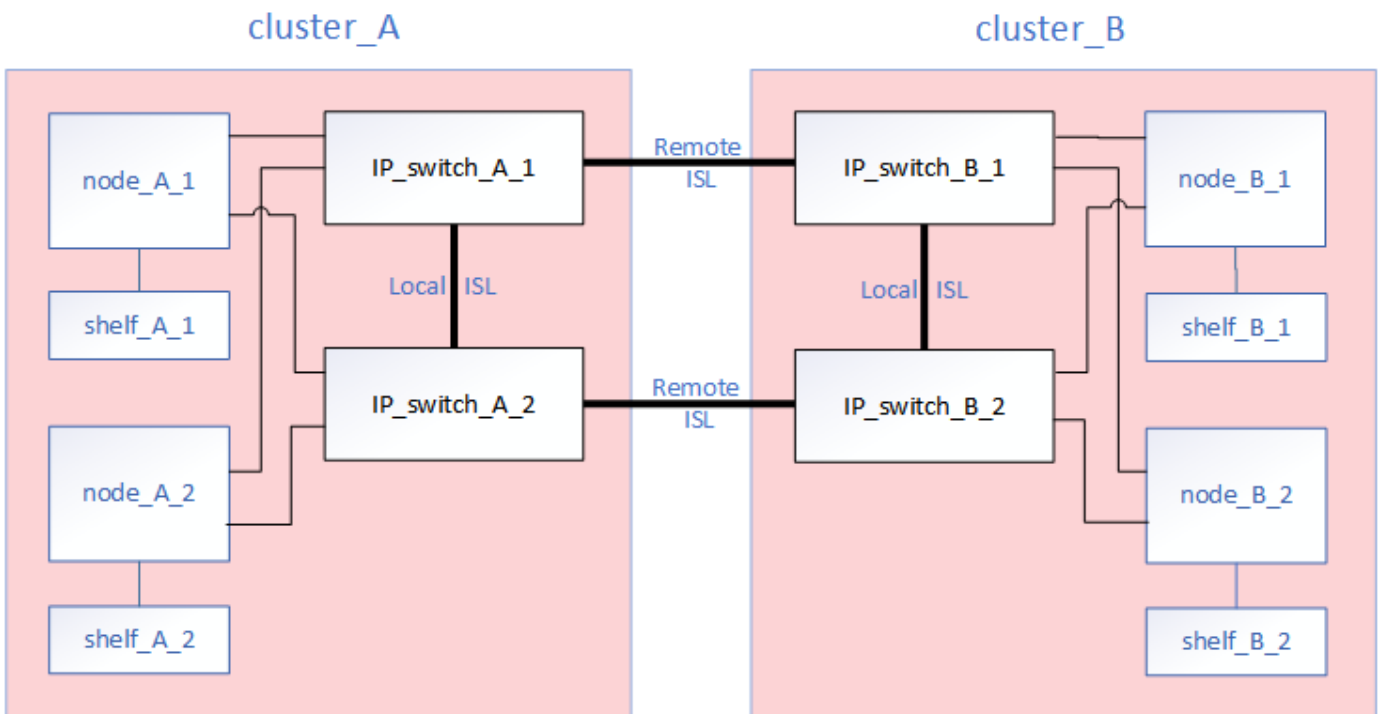
- IP switch maintenance and replacement 1
 - Replacing an IP switch 1
 - Upgrading firmware on MetroCluster IP switches 4
 - Upgrade RCF files on MetroCluster IP switches 6
 - Upgrade RCF files on Cisco IP switches using CleanUpFiles 8
 - Renaming a Cisco IP switch. 14

IP switch maintenance and replacement

Replacing an IP switch

You might need to replace a failed switch, or upgrade or downgrade a switch. The new switch can be the same as the old switch when a switch has failed, or you can change the switch type (upgrade or downgrade the switch).

If you want to replace a failed switch with the same type of switch, you only need to replace the failed switch. If you want to upgrade or downgrade a switch, you need to adjust two switches that are in the same network. Two switches are in the same network if they are connected with an inter-switch link (ISL) and are not located at the same site. For example, Network 1 includes IP_switch_A_1 and IP_switch_B_1. Network 2 includes IP_switch_A_2 and IP_switch_B_2 as shown in the diagram below:



This procedure applies when you are using NetApp-validated switches. If you are using MetroCluster-compliant switches, refer to the switch vendor.

If you upgrade or downgrade the networks, you must repeat this procedure for the second network.

Steps

1. Check the health of the configuration.
 - a. Check that the MetroCluster is configured and in normal mode on each cluster: **metrocluster show**

```
cluster_A::> metrocluster show
```

Cluster	Entry Name	State
Local: cluster_A	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		
Remote: cluster_B	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
disaster		

- b. Check that mirroring is enabled on each node: **metrocluster node show**

```
cluster_A::> metrocluster node show
```

DR	Group	Cluster	Node	Configuration State	DR	Mirroring Mode
	1	cluster_A	node_A_1	configured	enabled	normal
		cluster_B	node_B_1	configured	enabled	normal

2 entries were displayed.

- c. Check that the MetroCluster components are healthy: **metrocluster check run**

```
cluster_A::> metrocluster check run
```

```
Last Checked On: 10/1/2014 16:03:37
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok

4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

d. Check that there are no health alerts: **system health alert show**

2. Configure the new switch before installation.



If you are upgrading or downgrading the switches, you must configure all the switches in the network.

Follow the steps in the section *Configuring the IP switches* in the [MetroCluster IP installation and configuration](#).

Make sure that you apply the correct RCF file for switch _A_1, _A_2, _B_1 or _B_2. If the new switch is the same as the old switch, you need to apply the same RCF file.

If you upgrade or downgrade a switch, apply the latest supported RCF file for the new switch.

3. Run the port show command to view information about the network ports:

```
network port show
```

4. Disconnect the ISL connections from the remote switch that connect to the old switch.

You should disconnect the ISL connections from the ports on the IP_switch_A_1 that connect to IP_switch_B_1.

5. Power off the switch, remove the cables and physically remove IP_switch_B_1.

6. Install the new switch.

Cable the new switch first (including the ISLs) according to the steps in the *Cabling the IP switches* section in the [MetroCluster IP installation and configuration](#).



The used ports might be different from those on the old switch if the switch type is different. If you are upgrading or downgrading the switches, do **NOT** cable the local ISLs. Only cable the local ISLs if you are upgrading or downgrading the switches in the second network and both switches at one site are the same type.

7. Power up the switch or switches.

If the new switch is the same, power up the new switch. If you are upgrading or downgrading the switches, then power up both switches. The configuration can operate with two different switches at each site until the second network is updated.

8. Verify that the MetroCluster configuration is healthy by repeating step 1.

If you are upgrading or downgrading the switches in the first network, you might see some alerts related to local clustering.



If you upgrade or downgrade the networks, then repeat all of the steps for the second network.

Upgrading firmware on MetroCluster IP switches

You might need to upgrade the firmware on a MetroCluster IP switch.

You must repeat this task on each of the switches in succession.

Steps

1. Check the health of the configuration.

- Check that the MetroCluster is configured and in normal mode on each cluster:

```
metrocluster show
```

```
cluster_A::> metrocluster show
Cluster              Entry Name              State
-----
Local: cluster_A     Configuration state      configured
                      Mode                      normal
                      AUSO Failure Domain      auso-on-cluster-
disaster
Remote: cluster_B     Configuration state      configured
                      Mode                      normal
                      AUSO Failure Domain      auso-on-cluster-
disaster
```

- Check that mirroring is enabled on each node:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
```

DR	Group	Cluster	Node	Configuration	DR	Mirroring	Mode
				State			
	-----			-----			
1		cluster_A					
			node_A_1	configured		enabled	normal
		cluster_B					
			node_B_1	configured		enabled	normal

2 entries were displayed.

c. Check that the MetroCluster components are healthy:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
```

Last Checked On: 10/1/2014 16:03:37

Component	Result
-----	-----
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok

4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

d. Check that there are no health alerts:

```
system health alert show
```

2. Install the software on the first switch.



You must install the switch software on the switches in the following order: switch_A_1, switch_B_1, switch_A_2, switch_B_2.

Follow the steps for installing switch software in the relevant topic of the *MetroCluster IP Installation and Configuration* information depending on whether the switch type is Broadcom or Cisco:

- [Downloading and installing the Broadcom switch EFOS software](#)
- [Downloading and installing the Cisco switch NX-OS software](#)

3. Repeat the previous step for each of the switches.
4. Repeat Step 1 to check the health of the configuration.

Upgrade RCF files on MetroCluster IP switches

You might need to upgrade an RCF file on a MetroCluster IP switch. For example, an ONTAP upgrade or a switch firmware upgrade both require a new RCF file.

Ensure that the RCF file is supported

If you are changing the ONTAP version running on the switches, you should ensure that you have an RCF file that is supported for that version. If you use the RCF generator, the correct RCF file will be generated for you.

Steps

1. Use the following commands from the switches to verify the version of the RCF file:

From this switch...	Issue this command...
Broadcom switch	(IP_switch_A_1) # show clibanner
Cisco switch	IP_switch_A_1# show banner motd

For either switch, find the line in the output that indicates the version of the RCF file. For example, the following output is from a Cisco switch, which indicates the RCF file version is “v1.80”.

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. To check which files are supported for a specific ONTAP version, switch, and platform, use the RcfFileGenerator. If you can generate the RCF file for the configuration that you have or that you want to upgrade to, then it is supported.
3. To verify that the switch firmware is supported, refer to the following:
 - [Hardware Universe](#)
 - [NetApp Interoperability](#)

Upgrade RCF files

If you are installing new switch firmware, you must install the switch firmware before upgrading the RCF file.

About this task

This procedure disrupts traffic on the switch where the RCF file is upgraded. Traffic will resume once the new RCF file is applied.

Steps

1. Verify the health of the configuration.

- a. Verify that the MetroCluster components are healthy:

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

The operation runs in the background.

- a. After the `metrocluster check run` operation completes, run `metrocluster check show` to view the results.

After approximately five minutes, the following results are displayed:

```
-----
::*> metrocluster check show

Last Checked On: 4/7/2019 21:15:05

Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates         warning
clusters           ok
connections        not-applicable
volumes            ok
7 entries were displayed.
```

- b. Check the status of the running MetroCluster check operation:

```
metrocluster operation history show -job-id 38
```

- c. Verify that there are no health alerts:

```
system health alert show
```

2. Prepare the IP switches for the application of the new RCF files.

Follow the steps for your switch vendor:

- [Resetting the Broadcom IP switch to factory defaults](#)
- [Resetting the Cisco IP switch to factory defaults](#)

3. Download and install the IP RCF file, depending on your switch vendor.



Update the switches in the following order: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2

- [Downloading and installing the Broadcom IP RCF files](#)
- [Downloading and installing the Cisco IP RCF files](#)



If you have an L2 shared or L3 network configuration, you might need to adjust the ISL ports on the intermediate/customer switches. The switchport mode might change from 'access' to 'trunk' mode. Only proceed to upgrade the second switch pair (A_2, B_2) if the network connectivity between switches A_1 and B_1 is fully operational and the network is healthy.

Upgrade RCF files on Cisco IP switches using CleanUpFiles

You might need to upgrade an RCF file on a Cisco IP switch. For example, an ONTAP upgrade or a switch firmware upgrade both require a new RCF file.

About this task

Beginning with RcfFileGenerator version 1.4a, there is a new option to change (upgrade, downgrade, or replace) the switch configuration on Cisco IP switches without the need to perform a 'write erase'.

Before you begin

You can use this method if your configuration meets the following requirements:

- The standard RCF configuration is applied.
- The [RcfFileGenerator](#) must be able to create the same RCF file that is applied, with the same version and configuration (platforms, VLANs).
- The RCF file that is applied was not provided by NetApp for a special configuration.
- The RCF file was not altered before it was applied.
- The steps to reset the switch to factory defaults were followed before applying the current RCF file.
- No changes were made to the switch(port) configuration after the RCF was applied.

If you do not meet these requirements, then you cannot use the CleanUpFiles that are created when generating the RCF files. However, you can leverage the function to create generic CleanUpFiles — the cleanup using this method is derived from the output of `show running-config` and is best practice.



You must update the switches in the following order: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2. Or, you can update the switches Switch_A_1 and Switch_B_1 at the same time followed by switches Switch_A_2 and Switch_B_2.

Steps

1. Determine the current RCF file version, and which ports and VLANs are used: `IP_switch_A_1# show banner motd`



You need to get this information from all four switches and complete the following information table.

```

* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*
#
IP_switch_A_1#

```

From this output, you must collect the information shown in the following two tables.

Generic information	MetroCluster	Data
RCF file version		1.81
Switch type		NX9336
Network typology		L2 Networks, direct ISL
Storage type		SAS storage
Platforms	1	AFF A400
	2	FAS9000

VLAN information	Network	MetroCluster configuration	Switchports	Site A	Site B
VLAN local cluster	Network 1	1	1, 2	111	222
		2	3, 4	151	251
	Network 2	1	1, 2	111	222
		2	3, 4	151	251
VLAN MetroCluster	Network 1	1	9, 10	119	119
		2	11, 12	159	159
	Network 2	1	9, 10	219	219
		2	11, 12	259	259

2. Create the RCF files and CleanUpFiles, or create generic CleanUpFiles for the current configuration.

If your configuration meets the requirements outlined in the prerequisites, select **Option 1**. If your configuration does **not** meet the requirements outlined in the prerequisites, select **Option 2**.

Option 1: Create the RCF files and CleanUpFiles

Use this procedure if the configuration meets the requirements.

Steps

- a. Use the RcfFileGenerator 1.4a (or later) to create the RCF files with the information that you retrieved in Step 1. The new version of the RcfFileGenerator creates an additional set of CleanUpFiles that you can use to revert some configuration and prepare the switch to apply a new RCF configuration.
- b. Compare the banner motd with the RCF files that are currently applied. The platform types, switch type, port and VLAN usage must be the same.



You must use the CleanUpFiles from the same version as the RCF file and for the exact same configuration. Using any CleanUpFile will not work and might require a full reset of the switch.



The storage type might be different — SAS storage or direct storage.



The ONTAP version the RCF file is created for is not relevant. Only the RCF file version is important.



The RCF file (even it is the same version) might list fewer or more platforms. Make sure that your platform is listed.

Option 2: Create generic CleanUpFiles

Use this procedure if the configuration does **not** meet all the requirements.

Steps

- a. Retrieve the output of `show running-config` from each switch.
- b. Open the RcfFileGenerator tool and click 'Create generic CleanUpFiles' at the bottom of the window
- c. Copy the output that you retrieved in Step 1 from 'one' switch into the upper window. You can remove or leave the default output.
- d. Click 'Create CUF files'.
- e. Copy the output from the lower window into a text file (this file is the CleanUpFile).
- f. Repeat Steps c, d, and e for all switches in the configuration.

At the end of this procedure, you should have four text files, one for each switch. You can use these files in the same way as the CleanUpFiles that you can create by using Option 1.

3. Create the 'new' RCF files for the new configuration. Create these files in the same way that you created the files in the previous step, except choose the respective ONTAP and RCF file version.

After completing this step you should have two sets of RCF files, each set consisting of twelve files.

4. Download the files to the bootflash.

- a. Download the CleanUpFiles that you created in [Create the RCF files and CleanUpFiles, or create generic CleanUpFiles for the current configuration](#)



This CleanUpFile is for the current RCF file that is applied and **NOT** for the new RCF that you want to upgrade to.

Example CleanUpFile for Switch-A1: Cleanup_NX9336_v1.81_Switch-A1.txt

- b. Download the 'new' RCF files that you created in [Create the 'new' RCF files for the new configuration.](#)

Example RCF file for Switch-A1: NX9336_v1.90_Switch-A1.txt

- c. Download the CleanUpFiles that you created in [Create the 'new' RCF files for the new configuration.](#) This step is optional — you can use the file in future to update the switch configuration. It matches the currently applied configuration.

Example CleanUpFile for Switch-A1: Cleanup_NX9336_v1.90_Switch-A1.txt



You must use the CleanUpFile for the correct (matching) RCF version. If you use a CleanUpFile for a different RCF version, or a different configuration then the cleanup of the configuration might not work correctly.

The following example copies the three files to the bootflash:

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_XXX_XXX_XXX_XXX/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_XXX_XXX_XXX_XXXNX9336_v1.90//NX933
6_v1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_XXX_XXX_XXX_XXXNX9336_v1.90//Clean
up_NX9336_v1.90_Switch-A1.txt bootflash:
```



You are prompted to specify Virtual Routing and Forwarding (VRF).

5. Apply the CleanUpFile or generic CleanUpFile.

Some of the configuration is reverted and switchports go 'offline'.

- a. Confirm that there are no pending changes to the startup configuration: `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. If you see system output, save the running configuration to the startup configuration: `copy running-config startup-config`



System output indicates that the startup configuration and running configuration are different and pending changes. If you do not save the pending changes, you are unable to roll back using a reload of the switch.

- a. Apply the CleanUpFile:

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```



The script might take a while to return to the switch prompt. No output is expected.

7. View the running configuration to verify that the configuration is cleared: `show running-config`

The current configuration should show:

- No class maps and IP access lists are configured
- No policy maps are configured
- No service policies are configured
- No port-profiles are configured
- All Ethernet interfaces (except mgmt0 which should not show any configuration, and only VLAN 1 should be configured).

If you find that any of the above items are configured, you might not be able to apply a new RCF file configuration. However, you can revert to the previous configuration by reloading the switch **without** saving the running configuration to the startup configuration. The switch will come up with the previous configuration.

8. Apply the RCF file and verify that the ports are online.

- a. Apply the RCF files.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```



Some warning messages appear while applying the configuration. Error messages are not expected.

- b. After the configuration is applied, verify that the cluster and MetroCluster ports are coming online with one of the following commands, `show interface brief`, `show cdp neighbors`, or `show lldp neighbors`



If you changed the VLAN for the local cluster and you upgraded the first switch at the site, then cluster health monitoring might not report the state as 'healthy' because the VLANs from the old and new configurations do not match. After the second switch is updated, the state should return to healthy.

If the configuration is not applied correctly, or you do not want to keep the configuration, you can revert to the previous configuration by reloading the switch **without** saving the running configuration to startup configuration. The switch will come up with the previous configuration.

9. Save the configuration and reload the switch.

```
IP_switch_A_1# copy running-config startup-config  
  
IP_switch_A_1# reload
```

Renaming a Cisco IP switch

You might need to rename a Cisco IP switch to provide consistent naming throughout your configuration.

In the examples in this task, the switch name is changed from `myswitch` to `IP_switch_A_1`.

1. Enter global configuration mode:

configure terminal

The following example shows the configuration mode prompt. Both prompts show the switch name of `myswitch`.

```
myswitch# configure terminal  
myswitch(config)#
```

2. Rename the switch:

switchname new-switch-name

If you are renaming both switches in the fabric, use the same command on each switch.

The CLI prompt changes to reflect the new name:

```
myswitch(config)# switchname IP_switch_A_1  
IP_switch_A_1(config)#
```


3. Exit configuration mode:

exit

The top-level switch prompt is displayed:

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. Copy the current running configuration to the startup configuration file:

copy running-config startup-config

5. Verify that the switch name change is visible from the ONTAP cluster prompt.

Note that the new switch name is shown, and the old switch name (myswitch) does not appear.

- a. Enter advanced privilege mode, pressing **y** when prompted:

set -privilege advanced

- b. Display the attached devices:

network device-discovery show

- c. Return to admin privilege mode:

set -privilege admin

The following example shows that the switch appears with the new name, IP_switch_A_1:

```
cluster_A::storage show> set advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.

Do you want to continue? {y|n}: y

```
cluster_A::storage show*> network device-discovery show
```

Node/ Protocol Platform	Local Port	Discovered Device	Interface	

node_A_2/cdp				
	e0M	LF01-410J53.mycompany.com (SAL18516DZY)	Ethernet125/1/28	N9K-
C9372PX				
	e1a	IP_switch_A_1 (FOC21211RBU)	Ethernet1/2	N3K-
C3232C				
	e1b	IP_switch_A_1 (FOC21211RBU)	Ethernet1/10	N3K-
C3232C				
.				
.				
.			Ethernet1/18	N9K-
C9372PX				
node_A_1/cdp				
	e0M	LF01-410J53.mycompany.com (SAL18516DZY)	Ethernet125/1/26	N9K-
C9372PX				
	e0a	IP_switch_A_2 (FOC21211RB5)	Ethernet1/1	N3K-
C3232C				
	e0b	IP_switch_A_2 (FOC21211RB5)	Ethernet1/9	N3K-
C3232C				
	e1a	IP_switch_A_1 (FOC21211RBU)		
.				
.				
.				

16 entries were displayed.

Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.