Dell EMC Integrated Data Protection Appliance (IDPA)

Version 2.1

Field Replacement Guide

302-003-913
REV 03

Published September 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

CONTENTS

FIGURES

TABLES

CHAPTER 1

Prepare the Integrated Data Protection Appliance for Hardware Replacement

This chapter includes the following topics:

Hardware replacement overview

Some hardware components of the Integrated Data Protection Appliance (IDPA) can be replaced without shutting down the system, and some hardware components require a system shutdown to replace.

The target audience for this document is Customer Support Services and partner personnel who are responsible for replacing IDPA components in the field.

The following table lists the IDPA components and whether it is required that they be shut down while being replaced. To replace one of these components, go to the required replacement procedure.

Table 1 IDPA component replacement shutdown requirements

Model	Component shutdown is not required	Component shutdown is required
Data Domain DD6300/DD6800/DD9300	• 2.5" disk drive • 3.5" disk drive • Power supply	• Chassis • DIMM • Fan • I/O module • NVRAM module • Rails • Storage processor (SP) module
Data Domain DD9800	• 2.5" solid state drive • Fan • Power supply	• Chassis • DIMM • I/O module • Management module • NVRAM module • Rails • SP module
Data Domain DS60	• 3.5" disk drive • Bezel (shelf and cable management assembly) • Fan • Link control card (LCC) • Power supply	• Cable management assembly • Chassis • Rails (shelf and cable management assembly)

Table 1 IDPA component replacement shutdown requirements (continued)

Model	Component shutdown is not required	Component shutdown is required
Data Domain ES30/FS15	• 3.5" disk drive • Bezel • LCC • Power/cooling module	• Chassis • Rails
Avamar Gen4T server	• 3.5" disk drive • Network switch • Power supply	• 2.5" solid state drive • Chassis • DIMM • Fan • I/O module • SP
Dell PowerEdge R630 server	• Disk drive • Power supply • Server chassis	Not applicable
Dell S4048-ON Ethernet switch	• Power supply • Fan • SFP	Complete switch replacement

Replacing a component of the Dell PowerEdge server requires that you connect to the Dell switch to access the VMware vSphere web Client, and the Dell server iDRAC interface. Connect to port 38 on the Dell switch. The switch port layout is displayed in the following table.

Table 2 Switch port layout

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

Identify the IDPA

The Data Domain system has an IDPA-specific serial number on its Product Serial Number Tag (PSNT). Before beginning any replacement activities on the IDPA, verify that the PSNT information on the Service Request matches the PSNT information on the Data Domain system.

Shut down the IDPA

Procedure

1. Use ssh to log in to AVE IP on the ACM dashboard. Use "admin" as user and the common password for the appliance.
2. From the root login, run the**/usr/local/avamar/bin/avinstaller.pl --checkPrcessingPackage** command to check if any package installation in progress on AVE or not. If it is, wait for package installation to complete.

```
root@xxxxxxx:/home/admin/#: /usr/local/avamar/bin/
avinstaller.pl --checkPrcessingPackage
roo@xxxxxxx:/home/admin
```

3. Run the **dpnctl status all** command. Examine the output and ensure that all important back up server services are up and running as shown in the following screen shot. If not, contact support.

```
admin@xxxxxxx~/>: dpcnt1 status all
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: gsan status: up
dpnctl: INFO: MCS status: up
dpnctl: INFO: emt status: up
dpnctl: INFO: Backup scheduler status: up
dpnctl: INFO: Maintenance windows scheduler status: enabled
dpnctl: INFO: Unattended startup status: disabled
dpnctl: INFO: avinstaller status: up
dpnctl: INFO: ConnectEMC status: up
dpnctl: INFO: ddrmaint-service status: up
```

4. Run the **mccli checkpoint show** command to check all the checkpoints available on the Avamar system. Please take a screen shot of the output from running this command. The screen shot will be helpful in the later stages of the shutdown procedure.

```
admin@xxxxxxx:/home/admin/>:mccli checkpoint show
0,23000,CLI command completed successfully
Tag                    Time                Validated  Deletable
cp. 20180523033106 2018-05-23 09:01:06 IST Validated   No
cp. 20180523033444 2018-05-23 09:04:44 IST             No
cp. 20180523054859 2018-05-23 11:18:59 IST             No
```

5. Run the **mccli checkpoint create--override_maintenance_scheduler** command to create a checkpoint on AVE.

```
admin@xxxxxxx:/home/admin/>mccli checkpoint
create --override_maintenance_scheduler
0,22624, Starting to create a server checkpoint.
```

6. After the previous command executes, run the **mccli checkpoint show** on the AVE again to see the checkpoint tag which was newly created and assigned to the checkpoint you initiated in the previous step. the entry may take some time to get reflected in the output of this command (you may need to repeat this command 2-3 times). The newly created checkpoint entry can be validated from the timestamp associated with the entries. In the following screen shot, cp.20180523033444 is the tag of the newly created checkpoint.

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Tag                    Time                Validated Deletable
```

```
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST              Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

7. Run the following command **mccli checkpoint validate --cptag=<cp_tag_of_new_checkpoint> --override_maintenance_scheduler** to validate the checkpoint.

```
admin@xxxxxxx:/home/admin/>: mccli
checkpoint validate --cptag=cp.20180523033444 --
override_maintenance_scheduler
0,22612,Starting to validate a server checkpoijnt
Attribute    Value
tag         cp. 20180523033444
type        Full
```

8. Run the **mccli checkpoint show** command to check the status of the validation process of the checkpoint. The screen will display **In Progress** for an extended period of time. Wait until the screen displays a **Validated** status for the checkpoint tag.

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Tag                  Time                Validated Deletable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST In Progress  Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Tag                  Time                Validated Deletable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST Validated    Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

9. From the root login , run the **avmaint hfscheckstatus <checkpoint_tag> --ava**command to check the status of the job. If necessary, run the **avmaint hfscheck --checkpoint=<checkpoint tag> --ava** to perform an hfscheck on the checkpoint. Wait until above hfscheck job status command gives a completed status.

```
root@xxxxxxx:/home/admin/#:avmaint hfscheckstatus cp.
20180524033103 --ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheckstatus
nodes-queried="1"
nodes-replied="1"
nodes-total="1"
checkpoint="cp.20180524033103"
status="waitcomplete"
type="full"
checks="full"
elapsed-time="114"
start-time="1527154524"
end-time="0"
check-start-time="1527154524"
check-end-time="1527154562"
generation-time="1527154565"
stripes-checking="31"
stripes-completed="31"
offline-stripes="0"
```

```
minutes-to-completion="100.00">
<hfscheckerrors/>
</hfscheckstatus>
root@xxxxxxx:/home/admin/#:
```

```
root@xxxxxxx:/home/admin/#:avmaint hfscheck cp.20180524033103 --
ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheck
checkpoint="cp.20180524033103"
status="waitcgsan"
type="full"
checks="full"
elapsed-time="73"
start-time="1527154451"
end-time="0"
check-start-time="0"
check-end-time="0"
generation-time="1527154524"
percent-complete="0.00">
<hfscheckerrors/>
</hfscheck>
```

```
root@xxxxxxx:/home/admin/#:avmaint hfscheckstatus cp.
20180524033103 --ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheckstatus
nodes-queried="1"
nodes-replied="1"
nodes-total="1"
checkpoint="cp.20180524033103"
status="completed"
result="OK"
type="full"
checks="full"
elapsed-time="103"
start-time="1527154451"
end-time="1527154554"
check-start-time="1527154524"
check-end-time="1527154554"
generation-time="1527154651"
stripes-checking="31"
stripes-completed="31"
offline-stripes="0"
percent completion="100.00">
<hfscheckerrors/>
</hfscheckstatus>
```

10. Run the **dpcntl stop sched** command to stop all the backup job that will be scheduled by AVE(current jobs will still continue to run).

```
admin@xxxxxxx:~/>: dpnctl stop sched
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: Suspending backup scheduler...
dpnctl: INFO: Backup scheduler suspended.
```

11. Run the **dpnctl stop maint**command to stop maintenance services running on Avamar.

```
admin@xxxxxxx:~/>: dpnctl stop maint
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: Suspending maintenance windows scheduler...
dpnctl: INFO: Maintenance windows scheduler suspended.
```

12. From the root login, run the **cplist** command and verify the following:

a. Check if hfschecked checkpoint is present within 36hrs of time.

b. Check whether there is a hfs entry for at least one checkpoint which was created within last 36hrs of time.

```
root@xxxxxxx://ust/local/avamar/bin/#: cplist
cp. 20180524033103 Thu May 24 09:01:03 2018 valid hfs --- nodes
1/1 stripes  32
cp. 20180524033441 Thu May 24 09:04:03 2018 valid hfs --- nodes
1/1 stripes  32
```

13. Run the **avmaint sessions** on AVE. This stops all active sessions on Avamar. It will list all the sessions currently running on AVE. To kill each session, select the **sessionid** and run the **avmaint kill <sessionid>' command**. Do this for every session until no session entries are found on AVE.

```
admin@xxxxxxx://>: avmaint sessions
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<nodesessionlist count="1">
<sessionlist
id="0.0"
count="1"
<session
numthreads="1"
type="avtarbackup"
ndispatchers="1"
expires="1532240626"
domain=""
workorderid="MOD-1527056601340"
pidnum="1001"
numconns="1"
path="/clients/acmpun059.lss.emc.com"
starttime="1527056651"
encrypt=="tls-sa"
dispatcher0="xxxxxxxxxxxxxx"
sessionid="9152705660134709"
root="/"
pluginid="Unix"
encrypt-strength="high"
clientid="86752318de80049804395b0756fde3fa034a9846"
user=""
clientip=xxxxxxxxxxxxx>
<host
numprocs="4"
speed="16777200"
osuser="root"
name="xxxxxxx"
memory="32175">
<build
msgversion="13-10"
time="06:46:59"
appname="avtar"
zlibversion="1.2.8"
lzoversion=1.08 Jul 12 2002"
date "Mar 22 2018"
appversion="7.5.101-101_HF294929"
processortype="x86_64"
osversion="SLES-64"
sslversion="TLSv1 OpenSSL 1.0.2a-fips 19 Mar 2015
osname="Linux"/>
```

```
admin@xxxxxxx://>: avmaint kill 9152705692533109
kill: killed 9152705692533109
```

```
admin@xxxxxxx:/home/admin/>: avmaint sessions
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<nodesessionlist count="1">
<sessionlist
id="0.0"
```

```
count="0"/>
</nodesessionlist>
```

14. From the Avamar root login, run the **avmaint cpstatus**to verify that no checkpoint is in progress. Verify that all the checkpoints listed are in a completed state. Wait for checkpoints to complete if they are running.

```
roor@xxxxxxx://#: avmaint cpstatus
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cpstatus
generation-time="1527099528"
tag="cp.20180523055705"
status="completed"
stripes-completed="32"
stripes-total="32"
start-time="1527055025"
end-time="1527055044"
result="OK"
refcount="1"/>
```

15. Run the **avmgr getb --path=/MC_BACKUPS --mr=1 --format=xml**to verify that the MCS has been flushed within the last 12 hours. You can check the actual time of the MCS flush by running the **t.pl <time_tag>** entry (execute in /usr/local/avamar/bin directory). If the MCS has not been flushed in the last 12 hours, run the **mcserver.sh- -flush**' to flush the MCS on AVE.

```
admin@xxxxxxx:~/>: avmgr getb  --path=/MC_BACKUPS --mr=1 --
format=xml
1 Request succeeded
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<backuplist version="3.0">
<backuplistrec flags="32768001" labelnum="418" label=""
created="157174902"
roothash="587c90ceea90e7523366025b3955a8ed142170f"
totalbytes="48514156.00"
ispresentbytes="0.00" pidnum="1001" percentnew"0" expires="0"
created_prectime="0x1d3f371fd3ffb5a" partial="0"
retentiontype="daily,weekly,monthly,yearly
backuptype="full" ddrindex="0" locked="1" direct_restore="1"
tier="0"
appconsistent="not_available"/>
</backuplist>
```

```
admin@xxxxxxx:~/>: mcserver.sh--flush
=== BEGIN === check.mcs (preflush)
check.mcs     passed
=== PASS === check.mcs PASSED OVERALL (preflush)
Flushing Administrator Server...
Adminstrator Server Flushed.
```

```
admin@xxxxxxx:~/>: avmgr getb  --path=/MC_BACKUPS --mr=1 --
format=xml
1 Request succeeded
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<backuplist version="3.0">
<backuplistrec flags="32768001" labelnum="419" label=""
created="157178362"
roothash="5876c90ceea90e7523366025b3955a8ed1422170f"
totalbytes="48514156.00"
ispresentbytes="0.00" pidnum="100" percentnew"0" expires="0"
created_prectime="0x1d3f371fd3ffb5a" partial="0"
retentiontype="daily,weekly,monthly,yearly
backuptype="full" ddrindex="0" locked="1" direct_restore="1"
tier="0"
appconsistent="not_available"/>
</backuplist>
```

```
admin@xxxxxxx:~/>:/usr/local/avamar/bin/>: t.pl 1527178362
local: Thu May 24 21:42:42 2018   gmt: Thu May 24 16:12:42 2018
```

```
admin@xxxxxxx:~/>: mcserver.sh--flush
=== BEGIN === check.ms (preflush)
check.mcs
===PASS === check.mcs PASSED OVERALL (preflush)
Flushing Administrator Server...
Administrator Server Flushed
```

16. In the /usr/local/avamar/bin directory, run the **hfscheck_kill** to kill the hfscheck jobs (if there are still any running).

```
admin@xxxxxxx:/usr/local/avamar/bin/#: hfscheck_kill
Using /usr/local/avamar/ver/probe.xml
```

17. Run the **avmaint gckill --ava** command to kill all garbage collector jobs.

```
admin@xxxxxxx:/usr/local/avamar/bin/#: avmaint gckill --ava
```

18. Run the **dpnctl shutdown --precheck** command to check whether all the shutdown requirements are satisfied.

```
admin@xxxxxxx:~/>: dpnctl shutdown --precheck
Identity added /home/admin/.ssh/admin_key)
dpnctl: INFO: Checking for validated checkpoint
dpnctl: INFO: found the most recently validated checkpoint: cp.
20180523033444 at
'Wed May 23 03:34:44 2018 UTC'
dpnctl: INFO: VALIDATED CHECKPOINT PASSED
dpnctl: INFO:
[###############-----------------------------------20%]
dpnctl: INFO: Starting MCS flush check
dpnctl: INFO: Last MCS flush at 'Wed May 23 15:45:02 2018'
dpnctl: INFO: LAST MCS PASSED
dpnctl: INFO:
[###############-----------------------------------30%]
dpnctl: INFO: Checking for file system and gsan percentage
dpnctl: INFO: FS/GSAN PERCENTAGE PASSED
dpnctl: INFO:
[###############-----------------------------------50%]
dpnctl: INFO: GSAN tasks: idle
dpnctl: INFO: Checking for hfscheck.
dpnctl: INFO: No hfsceck maintenance task is running.
dpnctl: INFO:
[###############-----------------------------------70%]
dpnctl: INFO: Checking for GC.
dpnctl: INFO: No GC task is running.
dpnctl: INFO:
[###############-----------------------------------80%]
dpnctl: INFO: Checking for active sessions (backup/restore).
dpnctl: INFO: No backup/restore is running.
dpnctl: INFO:
[###############-----------------------------------90%]
dpnctl: INFO: Checking for active checkpoint.
dpnctl: INFO: No checkpoint task is running.
dpnctl: INFO:
[###############-----------------------------------100%]
```

19. Perform file system cleaning by running the following CLI command on the Data Domain manager:

```
filesys clean status
```

20. Verify passwords are synchronized. Changing a password for a component causes the ACM UI to display the password out of sync error message. Ensure that all passwords are synchronized by checking each panel in the dashboard. If any password is not synchronized, the shutdown process cannot start. To allow the ACM to gather health information for the component, you must update the

stored password in the ACM UI to match. To update an unsynchronized password, click the error text.

21. On the dashboard **Home** tab, click the **Shutdown Appliance** icon.
22. Type the administrator password, click **Authenticate**, and then click **Yes**.
23. Click **Logout**.

⚠ CAUTION

It will a long time (estimated 45 minutes) between the ACM going down and the system physically powering off.

While the appliance is shutting down, the **Login** screen displays a message indicating shutdown is in progress. To view the status, Log into ESX to monitor the shutdown.

Troubleshooting shutdown

If any part of the shutdown process fails to complete automatically, resolve the problem by manually shutting down the IDPA on DP5300/DP5800 and DP8300/DP8800.

Stop the DP5300/DP5800

Procedure

1. Login to the Avamar server with SSH by using the Avamar IP address.
2. Create a checkpoint by running the following command:

   ```
   mccli checkpoint create --override_maintenance_scheduler
   ```

3. Stop all Avamar services by running the following command:

   ```
   dpnctl stop all
   ```

4. Log in to the Data Domain with SSH using the Data Domain IP address.
5. Shut down the Data Domain system by running the following command:

   ```
   system poweroff
   ```

6. Open the vCenter by typing the IP address in the browser.
7. Log in to vCenter by using the customer-specified username and password.
8. Power off the Data Protection virtual application.

   All virtual machines and virtual applications under the Data Protection virtual application are automatically shut down.
9. Shut down the IDPA Virtual Machine guest operating system, and power off the virtual machine.
10. Log in to the ESXi server on which the vCenter resides.
11. Log in to each ESXi host.
12. Place all of the ESXi hosts into maintenance mode by running the following command on each host:

    ```
    esxcli system maintenanceMode set -e true -m noAction
    ```

13. Use the vSphere Client or the ESXi host to shut down all of the ESXi hosts.

14. Go to the required component replacement procedure.

Stop the DP8300/DP8800

Procedure

1. Shut down the Avamar server by completing the following steps:
   a. Login to the Avamar server with SSH by using the Avamar IP address.
   b. Load the SSH keys by running the following commands:

      ```
      ssh-agent bash
      ssh-add ~admin/.ssh/admin_key
      ```

   c. Verify that no maintenance jobs are running on the Avamar server by using the following command:

      ```
      status.dpn
      ```

   d. Create a checkpoint by running the following command:

      ```
      mccli checkpoint create --override_maintenance_scheduler
      ```

   e. Stop all Avamar services by running the following command:

      ```
      dpnctl stop all
      ```

   f. When prompted, answer `yes` to the EMS question.
   g. Verify that the Avamar services are stopped by running the following command:

      ```
      dpnctl status
      ```

   h. Prepare the Avamar nodes for shut down by running the following commands:

      ```
      mapall --user=root --all 'touch /fastboot'
      mapall --user=root --all 'halt'
      ```

   i. Power off all nodes in the grid.
2. To log in to the Data Domain system, open a new SSH session.
3. Shut down the Data Domain system by running the following command:

   ```
   system poweroff
   ```

4. Open the vCenter by typing the IP address in the browser.
5. Log in to vCenter by using the customer-specified username and password.
6. Power off the Data Protection virtual application.

   All virtual machines and virtual applications under the Data Protection virtual application are automatically shut down.
7. Shut down the IDPA Virtual Machine guest operating system, and power off the virtual machine.
8. Log in to the ESXi server on which the vCenter resides.
9. Log in to each ESXi host.
10. Place all of the ESXi hosts into maintenance mode by running the following command on each host:

```
esxcli system maintenanceMode set -e true -m noAction
```

11. Use the vSphere Client or the ESXi host to shut down all of the ESXi hosts.
12. Go to the required component replacement procedure.

CHAPTER 2

Data Domain FRUs

This chapter includes the following topics:

Data Domain FRUs

Field replacement procedures for the following Data Domain systems and disk shelves are available from the Generator in Solve Desktop. Appropriate IDPA FRUs will be carried in the Solutions Generator.

- Data Domain DD6300 system
- Data Domain DD6800 system
- Data Domain DD9300 system
- Data Domain DD9800 system
- Data Domain DS60 shelf
- Data Domain ES30/FS15 shelf

Replace a Data Domain Ethernet cable

Connect to port 38 on the Dell switch. The switch port layout is displayed in Hardware replacement overview.

Procedure

1. Login to the Avamar with SSH using the Avamar IP address.
2. Stop all Avamar services.

   Run the following command:
   ```
   dpnctl stop all
   ```
3. Login to the Data Domain with SSH using the Data Domain IP address.
4. Identify the I/O module slot number where the failed cable connects to the Data Domain system.

   Run the following command:
   ```
   net show config
   ```

```
ethMa     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:A9
          inet addr:10.241.160.24  Bcast:10.241.160.255  Mask:
255.255.255.0
          inet6 addr: 2620:0:170:4140:260:16ff:fe5c:8ca9/64
Scope:Global
          inet6 addr: fe80::260:16ff:fe5c:8ca9/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500
Metric:1
          RX packets:1208361053 errors:0 dropped:92194 overruns:
0 frame:0
          TX packets:1366864848 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:683470101483 (636.5 GiB)  TX bytes:
897875829943 (836.2 GiB)
          Interrupt:17

ethMb     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:A8
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:16

ethMc     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:AB
```

```
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17

ethMd     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:AA
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:16

eth1a     Link encap:Ethernet  HWaddr 00:60:16:52:35:28
          inet addr:10.241.173.240  Bcast:10.241.173.255  Mask:
255.255.255.0
          inet6 addr: fe80::260:16ff:fe52:3528/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:9000
Metric:1
          RX packets:26978140 errors:0 dropped:3370236 overruns:
0 frame:0
          TX packets:1818896 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2450123730 (2.2 GiB)  TX bytes:642406163
(612.6 MiB)
          Interrupt:32 Memory:381c08000000-381c087fffff

eth1b     Link encap:Ethernet  HWaddr 00:60:16:52:35:29
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:36 Memory:381c07000000-381c077fffff

eth1c     Link encap:Ethernet  HWaddr 00:60:16:52:35:2A
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:36 Memory:381c06000000-381c067fffff

eth1d     Link encap:Ethernet  HWaddr 00:60:16:52:35:2B
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:37 Memory:381c05000000-381c057fffff
```

In this example, the failed cable is on the I/O module in slot 1.

5. Disable the all the network ports on the I/O module with the failed cable.

   Run the following commands:

   ```
   netconfig eth1a down
   netconfig eth1b down
   netconfig eth1c down
   netconfig eth1d down
   ```

6. Disconnect the failed cable from the switch.
7. Disconnect the failed cable from the Data Domain system.
8. Connect the new cable to the switch.

9. Connect the new cable to the Data Domain system.
10. Enable the all the network ports on the I/O module with the new cable.

    Run the following commands:

    ```
    netconfig eth1a up
    netconfig eth1b up
    netconfig eth1c up
    netconfig eth1d up
    ```

11. Start all Avamar services.

    Run the following command:

    ```
    dpnctl start
    ```

CHAPTER 3

Avamar FRUs

This chapter includes the following topics:

Avamar FRUs

Replacement procedures for the Avamar Data Store Gen4T are available from the Solutions Generator in Solve Desktop.

Replace an Avamar Ethernet cable

Complete the following steps to replace an Ethernet cable on an Avamar server.

Note

This procedure is only for the twinax cables connecting the Avamar server to the Dell switch. FRU replacement of the cables connected to the Brocade switches is not supported.

Procedure

1. Disconnect the failed cable from the switch.
2. Disconnect the failed cable from the Avamar server.
3. Connect the new cable to the switch.
4. Connect the new cable to the Avamar server.

CHAPTER 4

Dell PowerEdge R630 Server FRUs

WARNING

Whenever you need to lift the system, get others to assist you. To avoid injury, do not attempt to lift the system by yourself.

This chapter includes the following topics:

Replacing an Ethernet Cable

This procedure describes how to replace a failed Ethernet cable on a PowerEdge R630 server.

Replace a PowerEdge Ethernet cable

Complete the following steps to replace an Ethernet cable on a PowerEdge server.

Procedure

1. Disconnect the failed cable from the switch.
2. Disconnect the failed cable from the PowerEdge server.
3. Connect the new cable to the switch.
4. Connect the new cable to the PowerEdge server.

Replacing a Disk

This procedure describes how to replace a faulted disk in a PowerEdge R630 server.

Overview

The IDPA server contains three different disk types:

- SD disk: This disk contains the ESXi operating system. If this SD disk fails, perform the IDPA server replacement procedure. Replacing the SD disk without replacing the entire server is not supported.
- SSD disks: One SSD is present in the IDPA server for use as a caching device.
- HDD disks: Five HDDs are present in the IDPA server.

The disk replacement procedure consists of the following tasks:

1. Gather information about the faulty disk.It is important to note which type of disk has failed.
2. Remove the failed disk from the system.
3. Install the replacement disk.
4. Prepare the new disk.
5. Add the new disk to the system.
6. Verify there are no errors.

Prerequisites

Verify the following prerequisites are met before replacing an IDPA server disk.

General prerequisites

The following general prerequisites apply:

- Verify the IP address range, subnet, and gateway IP addresses for the BMC (iDRAC) port for all servers.
- Verify the root and administrator passwords for the server and BMC (iDRAC).

- Verify the service PC or laptop has a functional network port and an available IP address (and subnet and gateway) on the management network to connect via SSH/RDP.
- Verify all hardware is assembled as described in the *IDPA Hardware Installation Guide*

The following internet browsers are supported:

- Mozilla Firefox 30 or higher
- Microsoft Internet Explorer 8 or higher

Java requirements
The following Java requirements apply to the service computer used for this procedure:

The BMC (iDRAC) management client requires the latest update of Java 1.7.

In the internet browser, verify that pop-ups are enabled (or enabled only for Java console features).

Record disk information

Gather and record required information to use throughout the disk replacement process.

Table 3 Disk information

Parameter	Value
iDRAC IP address	• ESX 1: user definable • ESX 2: user definable • ESX 3: user definable
iDRAC root user password	• Default username: root • Default password: idpa_1234
ESX hostname	User defined value.
vSAN disk group of failed drive	Locate this information in vCenter. Select the cluster where the server resides, and select **Monitor** > **Physical disks**.
Failed drive slot	Run the `alerts show current` command to identify the location of the failed drive slot. Record the slot number of the failed drive.
Disk type (SSD or HDD)	Locate this information in vCenter. Select the cluster where the server resides, and select **Monitor** > **Physical disks**.

Locate and connect to the Dell switch

Replacing a component of the Dell PowerEdge server requires that you connect to the Dell switch to access the VMware vSphere Web Client, and the Dell server iDRAC interface. Connect to port 38 on the Dell switch. The switch port layout is displayed in Hardware replacement overview.

Procedure

1. Consult with the customer to get the values for IP address, subnet, and gateway for IDRAC.
2. Configure the service computer to connect with the IDPA.
   a. Open the **Control Panel**.
   b. Select **Networking** > **Change adapter settings**.
   c. Right-click **Local Area Connection**, and select **Properties**.
   d. Select **Internet Protocol Version 4 (TCP/IPv4)** > **Properties**.
   e. Specify the IP address as the IP address obtained from the customer.
   f. Specify the subnet mask as the subnet mask obtained from the customer.
   g. Click **OK**.
3. Locate the Dell switch in the cabinet.

   The switch location differs depending on the IDPA configuration:

   - For systems without an Avamar switch, the Dell switch is located above the three PowerEdge servers.
   - For systems with an Avamar switch in a single cabinet, the Dell switch is located above the Avamar switch.
   - For dual cabinet systems, the Dell switch is at the top of the cabinet containing the Data Domain controller.
4. Connect an RJ-45 Ethernet cable from the service computer to port 38 on the Dell switch.
5. Open a command propmt, and ping the IP address to test the connection.

   Run the following command:
   ```
   ping IP address
   ```
6. If the ping fails, verify the cable between the service computer and the Dell switch is fully seated and try again. Proceed with the component replacement once the ping succeeds.

Gather disk information

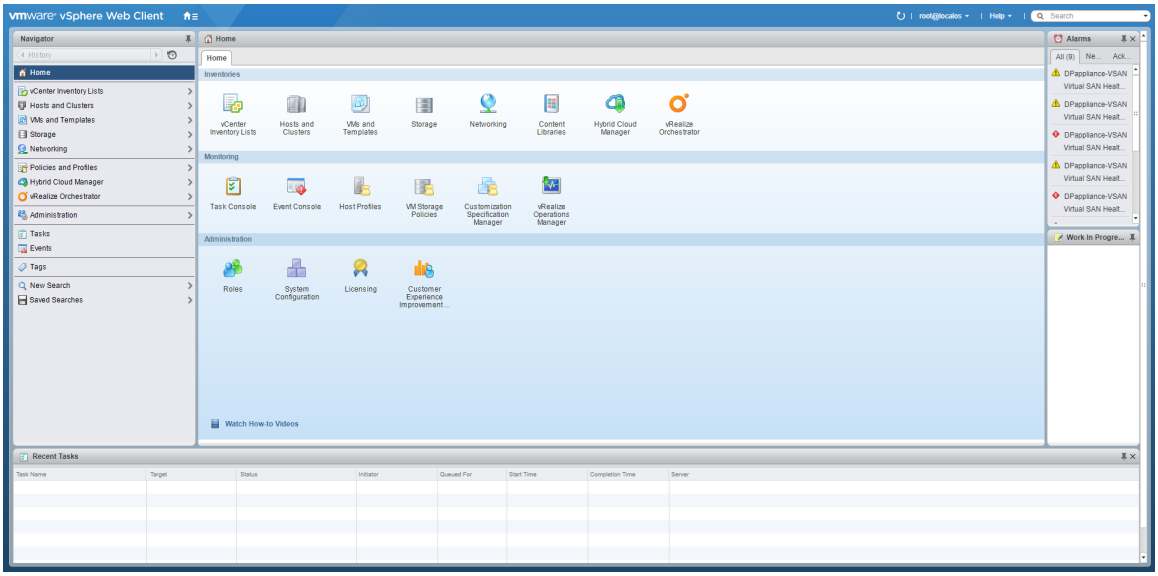
Before you begin

Connect an RJ-45 Ethernet cable between the Ethernet adapter on the service laptop, and port 38 on the IDPA top-of-rack switch.

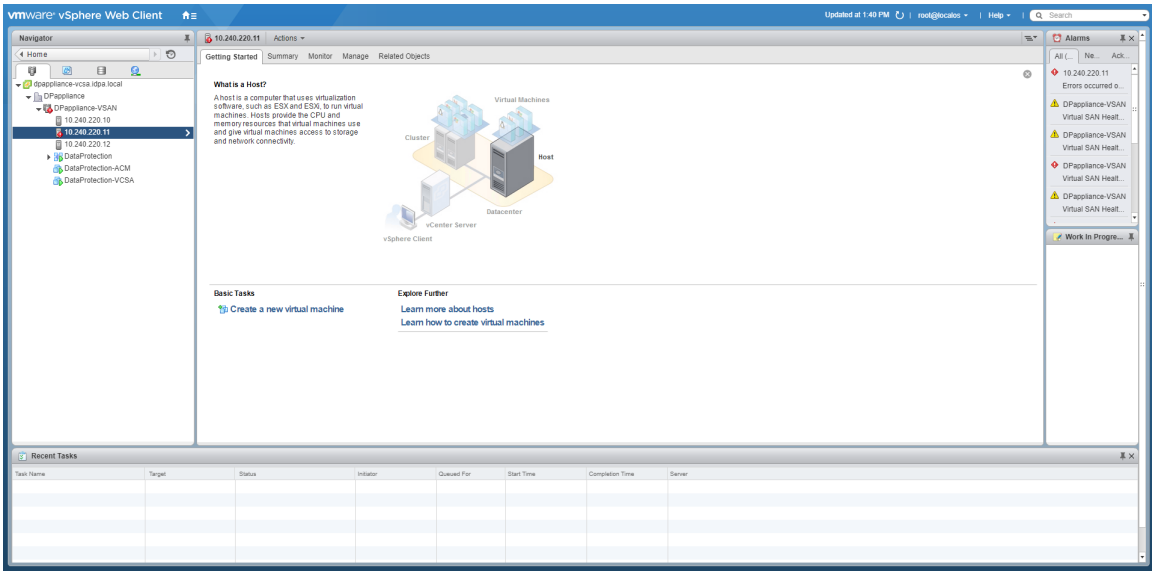
Gather the required information to use to replace the failed disk.

Procedure

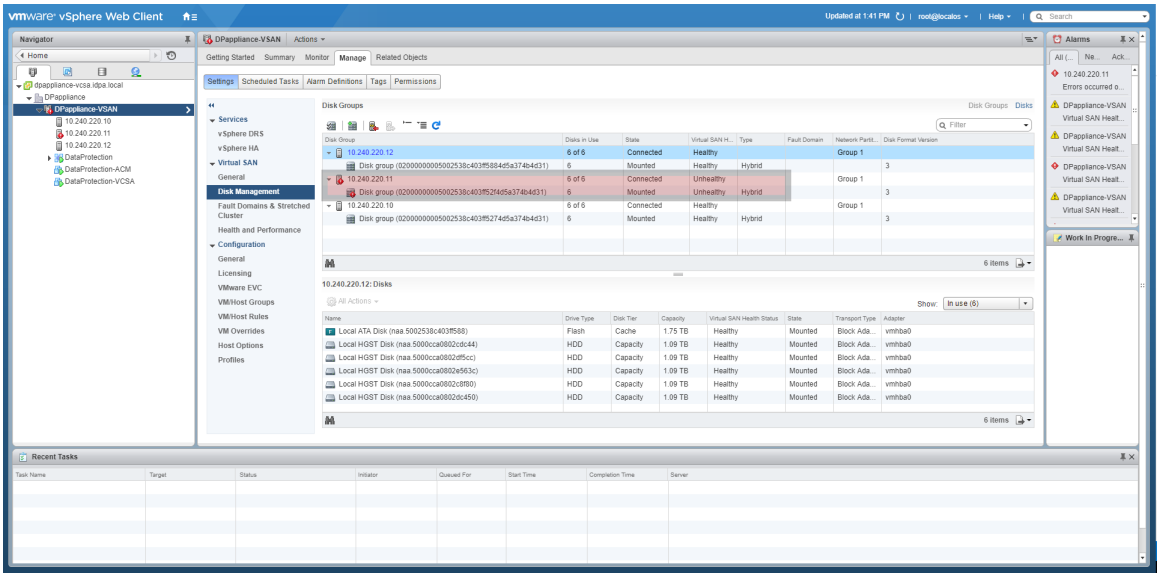
1. From an Internet browser, use the previously recorded IP address acquired from the customer to launch the VMware vSphere Web Client and access the IDPA vCenter Server.



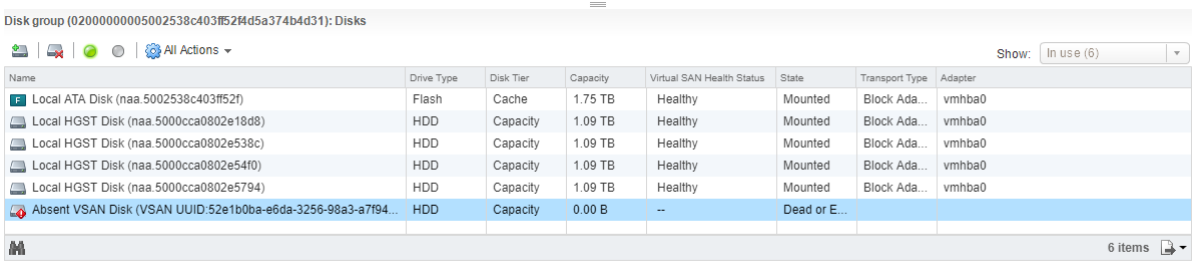
2. Respond to the security banners to add the required exception before connecting.
3. Modify the Windows hosts file on the service computer.
   a. Right-click the **Command Prompt** icon and select **Run as administrator**.
   b. Navigate to the hosts file in the `C:\windows\system32\drivers\etc` directory.
   c. Type `Notepad hosts` to open the hosts file in Notepad.
   d. Add the ip address to the file.
   e. Save the hosts file and exit Notepad.
   f. Exit the Command Prompt.
4. In the internet browser window, click **Log into vSphere Web client**, and use the previously recorded vSphere login information to login as the root user.
5. Respond to the security banners to add the required exception.
6. Select **Hosts and Clusters**.
7. Locate and select the ESX host with the failed drive.
   The node will have one or more alerts to indicate a drive has failed.



8. Select **DPappliance-VSAN** cluster.
9. Select **Manage** > **Settings** > **Virtual SAN** > **Disk Management**.



10. Locate and expand the ESX host with the failed drive, and record the disk group with Unhealthy status.
11. Select the unhealthy disk group, and select the drive with Failed or Error status.



12. Select **All Actions** > **Turn Locator LED on**.
13. Open a new browser window, and type in the iDRAC IP address to access the server iDRAC interface.
14. Accept any SSL certificate errors.
15. Log in as root with the customer-provided password.
16. Select **Storage** > **Physical disks**, and record the slot number of the failed disk.

After you finish

Do not disconnect the service computer from the network switch, and do not terminate the iDRAC or vCenter Server sessions. Additional steps are required to configure the replacement disk.

Prepare a failed SSD for replacement

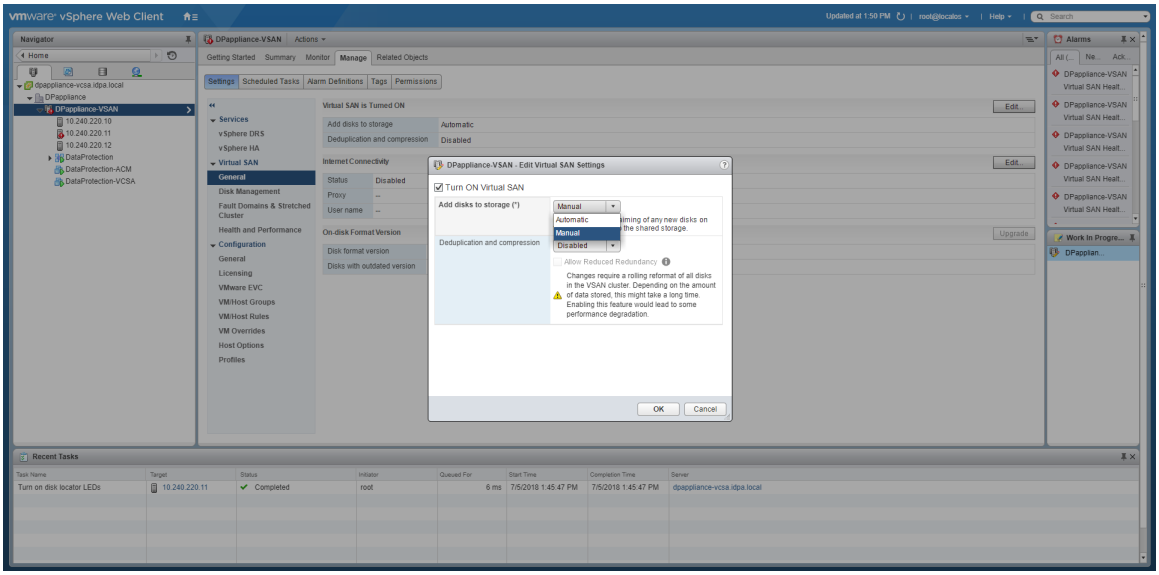
This task only applies to replacing a failed SSD. Skip this section when replacing an HDD. To prepare the SSD for replacement, complete the following steps.

Procedure

1. In the IDPA vCenter Server, select **Hosts and Clusters** > **DPappliance-VSAN**.
2. Select **Manage** > **Settings** > **Virtual SAN** > **General**.
3. Select **Edit**, and change the **Add disks to storage** value to **Manual**.

Note

There are two **Edit** buttons on the screen. Use the top button that is located across from `Virtual SAN is Turned ON`.



4. Select **OK**.
5. Select **Manage** > **Settings** > **Virtual SAN** > **Disk Management**.
6. Using the information that was previously gathered, select the disk group that contained the failed SSD, and select the failed SSD from the list. Select **All Actions**. From the pulldown menu, select **Remove Disks from Group**.
7. Click **Remove**.
8. Select **No data Migration**.
9. Click **Yes**, and allow some time for the removal operation to complete. Check the progress of the removal operation in the **Recent Tasks** pane at the bottom of the screen.

⚠ CAUTION

Removing the SSD destroys the vSAN group.

Drive status indicator codes

Table 4 Drive indicators

	1. Drive activity indicator 2. Drive status indicator 3. Drive

Table 5 Drive status indicator codes

Drive-Status Indicator Pattern	Condition
Flashes green twice per second	Identifying drive or preparing for removal.
Off	Drive ready for insertion or removal. **Note** The drive status indicator remains off until all hard drives are initialized after the system is turned on. Drives are not ready for insertion or removal during this time.
Flashes green, amber, and turns off	Predicted drive failure
Flashes amber four times per second	Drive failed
Steady green	Drive online
Flashes green for three seconds, amber for three seconds, and turns off after six seconds	Rebuild aborted

Locate the failed drive

After removing the bezel, locate the drive with the blinking LED.

The following table shows the disk layout. The slots are labeled on the server chassis.

Table 6 Disk layout

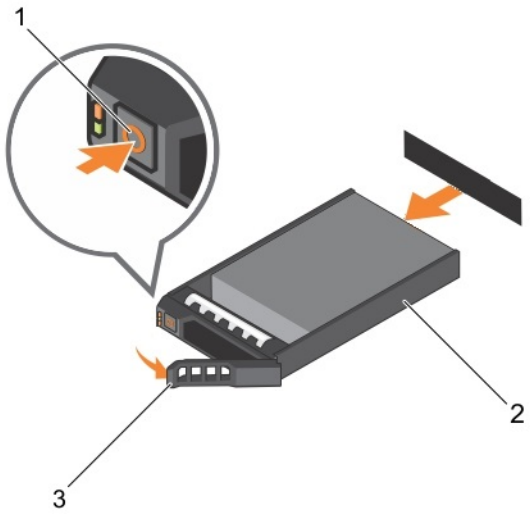
Front panel - No disks		Slot 2 - HDD	Slot 4 - HDD	Slot 6 - Blank
Slot 0 - HDD	Slot 1 - HDD	Slot 3 - HDD	Slot 5 - SSD	Slot 7 - Blank

Remove a disk drive

Procedure

1. Press the release button to open the disk drive carrier release handle.
2. Slide the disk drive carrier out of the hard drive slot.

Figure 1 Removing a hard drive



1. Release button
2. Disk/carrier
3. Drive carrier handle

Install a disk drive

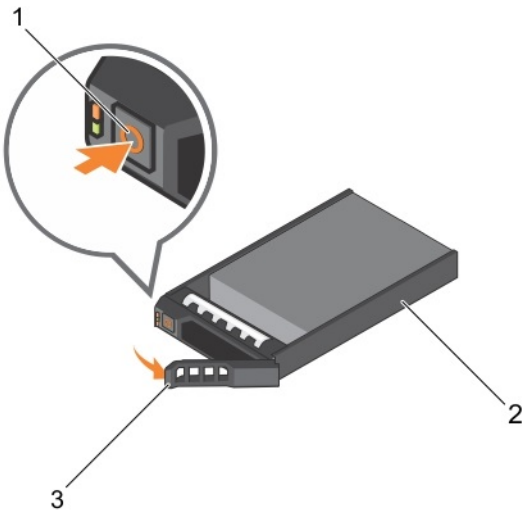
Note

Save the packing material to return the faulted disk drive.

Procedure

1. Press the release button on the front of the disk drive carrier and open the drive carrier handle.

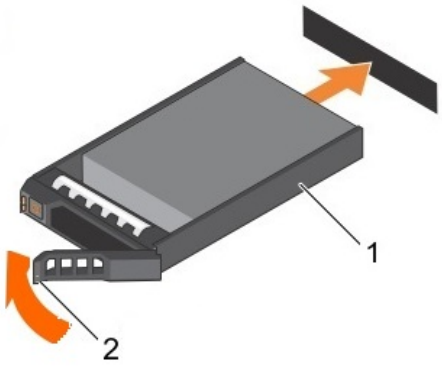
Figure 2 Open the disk drive carrier handle



1. Release button
2. Disk/carrier
3. Drive carrier handle

2. Insert the disk drive carrier into the disk drive slot until the carrier connects with the backplane.
3. Close the disk drive carrier handle to lock the disk drive in place.

Figure 3 Installing a disk drive



1. Disk/carrier
2. Drive carrier handle

Configure the replacement drive

Complete one of the following tasks to configure the replacement drive:

- Proceed to Configure the replacement SSD on page 39 to configure a new SSD.
- Proceed to Configure the replacement HDD on page 39 to configure a new HDD.

Configure the replacement SSD

Before you begin

If the existing iDRAC or IDPA vCetner Server session has been terminated, log in again.

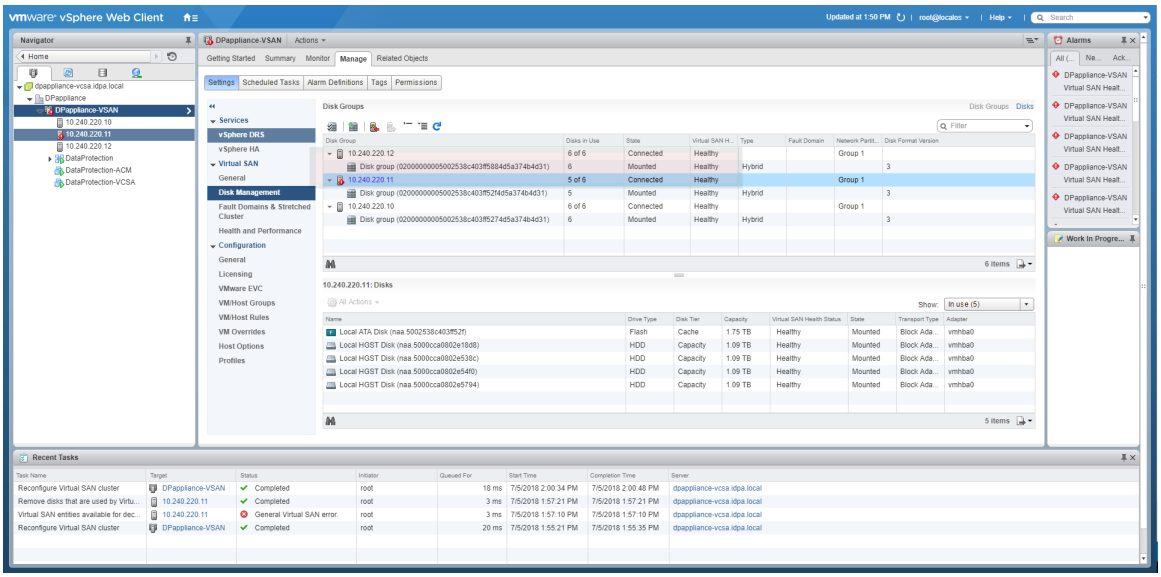
Complete the following steps after replacing an SSD.

Procedure

1. In the IDPA vCenter Server, select **Hosts and Clusters** > **DPappliance-VSAN**.
2. Select **Manage** > **Settings** > **Virtual SAN** > **General**.
3. Select **Edit**, and change the **Add disks to storage** value to **Manual**.

> **Note**
>
> There are two **Edit** buttons on the screen. Use the top button, across from `Virtual SAN is Turned ON`.

4. Select **Manage** > **Settings** > **Virtual SAN** > **Disk Management**.
5. Select the host where the failed drive was replaced.
6. Click the button to create a new disk group.



7. Select the SSD and the data disks.
8. Click **OK**.
9. Change Capacity Type to **Flash**.
10. Select **Monitor** > **Virtual SAN** > **Resynching Components** to monitor the progress of the resynching operation and verify it completes successfully.
11. Select **Edit**, and change the **Add disks to storage** value to **Automatic**.

Configure the replacement HDD

Before you begin

If the existing IDPA vCenter Server session has been terminated, log in again.

Complete the following steps after replacing an HDD.

Procedure

1. In the IDPA vCenter Server, select **Hosts and Clusters** > **DPappliance-VSAN**.
2. Select **Manage** > **Settings** > **Virtual SAN** > **General**.
3. Select **Edit**, and change the **Add disks to storage** value to **Manual**.

   Note

   There are two **Edit** buttons on the screen. Use the top button, across from `Virtual SAN is Turned ON`.

4. Select **Manage** > **Settings** > **Virtual SAN** > **Disk Management**.
5. Select the host and disk slot where the failed drive was replaced.
6. Using the information gathered earlier, select the disk group that contained the failed disk drive, and select the failed disk from the list.
7. Select **All Actions** > **Remove disk(s) from the disk group**.
8. Select **No data Migration**.
9. Click **Yes**, and allow some time for the removal operation to complete. Check the progress of the removal operation in the **Recent Tasks** pane at the bottom of the screen.
10. Select **All Actions** > **Add a disk**, select the checkbox for the new drive, and click **OK**.
11. Allow some time for the drive addition operation to complete. Monitor the status in the **Recent Tasks** window.
12. Select **Manage** > **Settings** > **Virtual SAN** > **General**.
13. Select **Edit**, and change the **Add disks to storage** value to **Automatic**.

Complete the procedure

Complete the following steps after the replacement component is installed and configured.

Procedure

1. Clear VMware Alarms.
   a. In the VMware web interface, select each virtual SAN alarm alert from the **Alarms** section.
   b. Right-click each alarm and select **Reset to Green**.
2. Clear the disk locator LED by selecting **All Action** and turn the LED to **OFF**.
3. Log out of all VMware and Dell interfaces.
4. Disconnect the service computer from the top-of-rack switch.

Replacing a server power supply

This procedure describes how to replace a faulted power supply in a PowerEdge R630 server.

Power supply units

The system supports two 750 W mixed mode PSUs which are installed in the rear panel. If two PSUs are used, they must be of the same maximum output power.

Note

Use only PSUs with the Extended Power Performance (EPP) label on the back. Mixing PSUs from previous generations of servers can result in a PSU mismatch condition or failure to power on.

Figure 4 PSUs location on rear panel

1. PSU 1
2. PSU 2

Power supply unit indicator codes

The PSUs have an illuminated translucent handle that serves as an indicator. The indicator shows whether power is present or a power fault has occurred.

Figure 5 PSU status indicator

1. PSU status indicator/handle

Table 7 PSU status indicator

Convention	Power Indicator Pattern	Condition
A	Green	A valid power source is connected to the PSU and the PSU is operational.
B	Flashing green	When the firmware of the PSU is being updated, the PSU handle flashes green.
C	Flashing green and turns off	When hot-swapping a PSU, the PSU handle flashes green five times at 4 Hz rate and turns off. The flashing green light that turns off after 5 flashes indicates a PSU efficiency mismatch for the feature set, health status, and supported voltage.
D	Flashing amber	Indicates a problem with the PSU.
E	Not lit	Power is not connected.

Identify the failed power supply unit

Identify the failed power supply unit by locating the PSU with its fault LED illuminated.

Removing a power supply unit

⚠ CAUTION

The system requires one PSU for normal operation. On power-redundant systems, remove and replace only one PSU at a time in a system that is powered on.

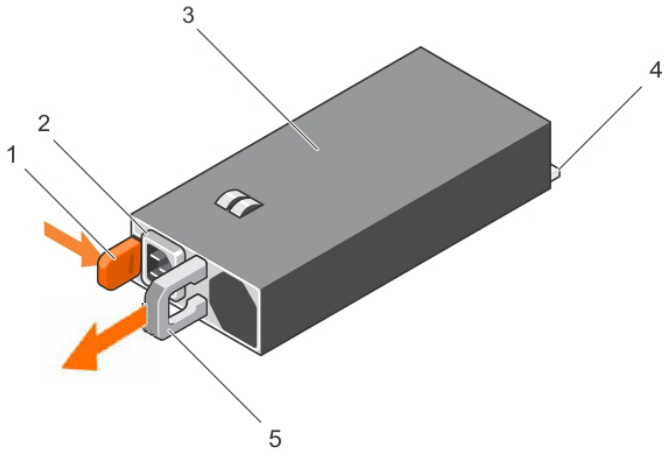
Note

You may have to unlatch and lift the optional cable management arm if it interferes with PSU removal. For information about the cable management arm, see the system's rack documentation.

Procedure

1. Disconnect the power cable from the power source and from the PSU you intend to remove, and remove the cable from the strap.
2. Press the release latch and slide the PSU out of the chassis.

Figure 6 Removing a PSU



1. Release latch
2. Power cable connector
3. PSU
4. Power connector
5. Handle

Installing a PSU

Note

Save the packing material to return the faulted PSU.

Procedure

1. Verify that the PSU being installed is of the same type and has the same maximum output power as the existing PSU.

   The maximum power output (shown in watts) is listed on the PSU label.

2. Slide the new PSU into the chassis until the PSU is fully seated and the release latch snaps into place.

   Note

   If you unlatched the cable management arm, re-latch it. For information about the cable management arm, see the system's rack documentation.

3. Connect the power cable to the PSU and plug the cable into a power outlet.

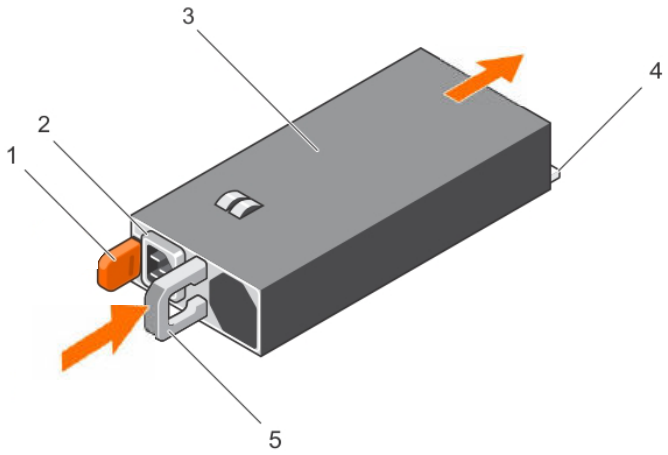
   CAUTION

   When connecting the power cable, secure the cable with the strap.

Note

Wait 15 seconds for the system to recognize the PSU and determine its status. The power supply redundancy may not occur until discovery is complete. Wait until the new PSU is discovered and enabled before you remove the other PSU. The PSU status indicator turns green to signify that the PSU is functioning properly.

Figure 7 Installing a PSU



1. Release latch
2. Power cable connector
3. Power supply unit
4. Power connector
5. Handle

Replacing a server

This procedure describes how to replace a faulted PowerEdge R630 server (IDPA node), and includes instructions to perform a full rebuild of the node .

Overview

The server replacement procedure consists of the following tasks:

1. Gather and record node information.
2. Prepare the node for replacement.
3. Remove the node from the system.
4. Install the replacement node.
5. Set up the new node.
6. Install the operating system.
7. Add the new node to the system.
8. Verify the new node functions correctly.

All logical configuration tasks in this procedure require a connection from the service computer to port 38 on the IDPA top-of-rack switch.

The replacement server chassis comes with fans and power supplies, but the disks must be transferred from the failed server to the new server.

Prerequisites

Verify the following prerequisites are met before replacing an IDPA server.

General prerequisites
The following general prerequisites apply:

- Verify the system identifiable information, which should be in the service request, including:
  - IDPA TLA/PSNT
  - Serial number of the part to be replaced.
- Verify the IP address range, subnet, and gateway IP addresses for the ESXi management interface on the node being replaced.
- Verify the root and administrator passwords for the server and BMC (iDRAC).
- Verify the service PC or laptop has a functional network port and an available IP address (and subnet and gateway) on the management network to connect via SSH/RDP.

The following internet browsers are supported:

- Mozilla Firefox 30 or higher
- Microsoft Internet Explorer 8 or higher

Java requirements
The following Java requirements apply:

The BMC (iDRAC) management client requires the latest update of Java 1.7.

In the internet browser, verify that pop-ups are enabled (or enabled only for Java console features).

Server FRU prerequisites
The following requirements apply when replacing a server:

The customer should provide the following information that was defined during the initial deployment process:

- The server username and password.
- The IP address of the BMC/iDRAC port on the server.

Install the operating system on the internal Dell ID SDM card, and configure IP addresses.

Record server information

Gather and record server information to use throughout the server replacement process. When you discover each piece of information, note it in the following table. Not all information is required for every configuration.

Default information is already included in the table. The remaining values are determined by the external customer network addresses.

Table 8 Server information

Item		**Value**
ACM	IP address	192.168.100.100
iDRAC	IP address/Subnet mask	• ESXi node 1: 192.168.100.110 / 255.255.255.224/27 • ESXi node 2: 192.168.100.111 / 255.255.255.224/27 • ESXI node 3: 192.168.100.112 / 255.255.255.224/27
	Default gateway	192.168.100.100
	Root user password, or username and password for a non-root user	
ESXi	Hostname	• ESXi node 1: esx1.dpappliance.local • ESXi node 2: esx2.dpappliance.local • ESXI node 3: esx3.dpappliance.local
	IP address/Subnet mask	• ESXi node 1: 192.168.100.101 / 255.255.255.224/27 • ESXi node 2: 192.168.100.102 / 255.255.255.224/27 • ESXI node 3: 192.168.100.103 / 255.255.255.224/27
	Host root password	Customer defined
vSphere	vSphere Web Client IP address	
	vSphere Web Client username	
	vSphere Web Client password	
DNS servers		
Domain		
Search Domain		
VMK0	IP address	
	Subnet mask	255.255.255.224
	IP default gateway	192.168.100.100
	VLAN	121
	Enabled services	• vMotion • Management traffic
	Network label assigned	DP-appliance-internal
VMK1	IP address	• ESXi node 1: 192.168.100.80 / 255.255.255.224/27

Table 8 Server information (continued)

Item		Value
		• ESXi node 2: 192.168.100.81 / 255.255.255.224/27 • ESXI node 3: 192.168.100.82 / 255.255.255.224/27
	Subnet mask	255.255.255.224
	VLAN	122
	Enabled Services	Virtual SAN traffic
	Network label assigned	DP-appliance-vsan
VMK2	IP address	Customer defined
	Subnet mask	
	IP default gateway	
	DNS server(s)	
	VLAN	123 **Note** 123 is the default value, but the customer may have changed it. Verify the VLAN ID with the customer.
	Enabled services	Management traffic
	Network label assigned	DP-appliance-external
vSwitch0 adapters assigned		vSwitch0: vmnic0, vmnic4
vSwitch1 adapters assigned		vSwitch1: vmnic2, vmnic6

Identify the failed server

Before beginning the procedure, compare the PSNT information on the Service Request to the PSNT information on each server to identify the failed server. The PSNT tag on each server is located in the lower right side of the enclosure, under disk drive slot number 1.

Locate and connect to the Dell switch

Replacing a component of the Dell PowerEdge server requires that you connect to the Dell switch to access the VMware vSphere Web Client, and the Dell server iDRAC interface. Connect to port 38 on the Dell switch. The switch port layout is displayed in Hardware replacement overview.

Procedure

1. Consult with the customer to get the values for IP address, subnet, and gateway for IDRAC.

2. Configure the service computer to connect with the IDPA.
   a. Open the **Control Panel**.
   b. Select **Networking** > **Change adapter settings**.
   c. Right-click **Local Area Connection**, and select **Properties**.
   d. Select **Internet Protocol Version 4 (TCP/IPv4)** > **Properties**.
   e. Specify the IP address as the IP address obtained from the customer.
   f. Specify the subnet mask as the subnet mask obtained from the customer.
   g. Click **OK**.
3. Locate the Dell switch in the cabinet.

   The switch location differs depending on the IDPA configuration:

   - For systems without an Avamar switch, the Dell switch is located above the three PowerEdge servers.
   - For systems with an Avamar switch in a single cabinet, the Dell switch is located above the Avamar switch.
   - For dual cabinet systems, the Dell switch is at the top of the cabinet containing the Data Domain controller.

4. Connect an RJ-45 Ethernet cable from the service computer to port 38 on the Dell switch.
5. Open a command propmt, and ping the IP address to test the connection.

   Run the following command:
   `ping IP address`
6. If the ping fails, verify the cable between the service computer and the Dell switch is fully seated and try again. Proceed with the component replacement once the ping succeeds.

Gather server information

Before you begin

Connect an RJ-45 Ethernet cable between the Ethernet adapter on the service laptop, and port 38 on the IDPA top-of-rack switch.

Gather the required information to use to restore the settings after replacing the server. If the server to be replaced is offline, most of the required information can be collected from one of the other servers. There is space to record this information in Record server information.

Procedure

1. From an Internet browser, use the previously recorded IP address to launch the VMware vSphere Web Client and access the IDPAvCenter Server.
2. Respond to the security banners to add the required exception before connecting.
3. Modify the Windows hosts file on the service computer.
   a. Open the Command Prompt as an administrator.
   b. Navigate to the hosts file in the `C:\windows\system32\driver\etc` directory.

c. Type `Notepad hosts` to open the hosts file in Notepad.

d. Add `192.168.100.99 dpappliance-vcsa.idpa.local` to the file.

e. Save the hosts file and exit Notepad.

f. Exit the Command Prompt.

4. In the internet browser window, click **Log into vSphere Web client**, and use the previously recorded vSphere login information.
5. Respond to the security banners to add the required exception.
6. Select **Hosts and Clusters**.
   a. Expand the DPAppliance cluster.
   b. Expand the DPappliance-VSAN to show the three host servers shown by IP address.
7. Locate and record the IP address of the server to be replaced.
8. In the right-hand pane, select the **Manage** tab.
9. Select **Networking** > **VMKernel Adapters**, and record the following information for VMK2.
   - IP address
   - Enabled services
   - DNS servers
   - Default gateway
   - VLAN ID
10. In the right-hand pane, select the default **System Stack**.
11. Select **DNS**, then scroll down and record the following information:
    - Domain
    - DNS servers
    - Search domain

After you finish

Do not disconnect the service computer from the network switch, and do not terminate the vCenter Server session. Additional steps are required to prepare and configure the replacement server.

Prepare the server for replacement

The required steps to prepare the server for replacement are different depending on whether the server is online or offline.

If the server is online, go to Prepare an online server for replacement on page 49.

If the server is offline, go to Prepare an offline server for replacement on page 50.

Prepare an online server for replacement

Before you begin

If the existing IDPA vCenter Server session has been terminated, log in again.

Complete the following steps to prepare an online server for replacement.

Procedure

1. In the IDPA vCenter Server, select **DPAppliance** > **DPAppliance-VSAN** and select the IP address of the ESX host to be replaced.
2. Right-click the host and select **Maintenance Mode** > **Enter Maintenance Mode**. Accept the confirmation pop-up.
   a. Verify the menu selection is **Ensure Accessibility**.
   b. Verify the checkbox is selected.
   c. Click **OK**, then click **OK** on the confirmation pop-up.
   d. Allow the system to move all virtual machines to other hosts using vMotion.

   Do not proceed to the next step until the ESXi host is in maintenance mode. Check the **Recent Tasks** panel at the bottom of the screen to verify the Enter Maintenance Mode task is complete. The host also appears with (Maintenance Mode) next to it in the left-hand pane.
3. Right-click the ESXi host and select **Power** > **Shutdown Host**.
4. In the window that appears, specify `IDPA FRU Procecdure` as the reason for shutting down the host, and select **OK**.
5. Allow some time for the host to shut down.

   Do not proceed to the next step until the host displays (Not Responding) in the left-hand pane where it previously displayed (Maintenance Mode).
6. Right-click the ESXi host and select **Remove from inventory**.
7. Click **OK** on the confirmation pop-up.

   The node changes to Disconnected, then disappears from the GUI.

Prepare an offline server for replacement

Before you begin

If the existing IDPA vCenter Server session has been terminated, log in again.

Complete the following steps to prepare an offline server for replacement.

Procedure

1. In the IDPA vCenter Server, locate and select the ESX host to be replaced.
2. Right-click the ESXi host and select **Remove from inventory**.

   The removal process takes some time. Allow for the host to be fully removed before proceeding with the physical removal and replacement of the server.
3. If the server is still powered on, power down the host from iDRAC or the front panel.

Remove the failed node from the virtual SAN cluster

Complete the following steps to remove the failed node from the virtual SAN cluster.

Procedure

1. From the vSphere Client, right-click on the failed node, and select **Remove from Inventory**.

   The failed node displays as Disconnected.

2. Click on the failed node and select **Manage** > **Settings** > **General**.
3. In the **Add disks to storage** list box, select **Manual**.

Disconnect power cords and I/O cables

This procedure is used to disconnect the power cords and I/O cables from the server.

Procedure

1. Label each cord and cable so you can easily identify them when you need to plug them into the replacement server.
2. Unplug power cords from the power supplies and disconnect I/O cables from the server.

Remove the server from the cabinet (sliding rails)

This procedure is used to remove the server (mounted on sliding rails) from the cabinet for replacement of a faulted server.

⚠ CAUTION

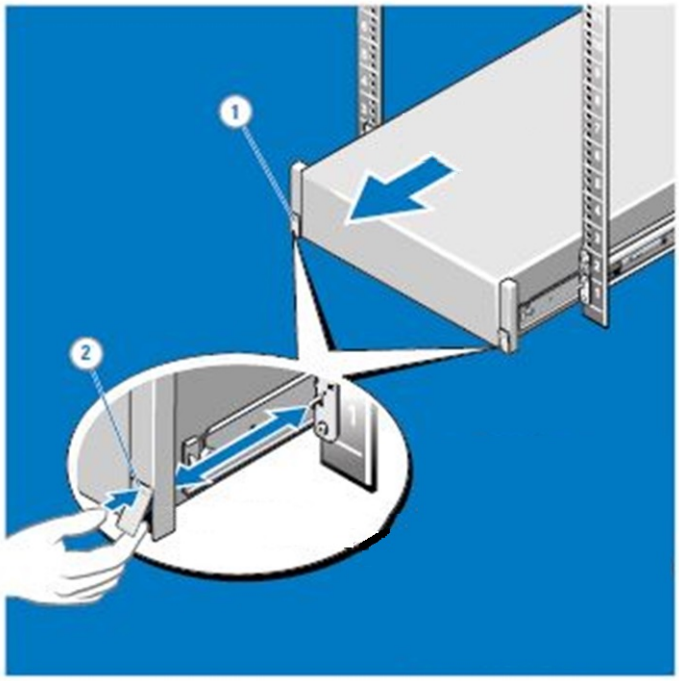
The server is heavy and should be removed from a cabinet by two people. To avoid personal injury and/or damage to the equipment, do not attempt to remove the server from a cabinet without a mechanical lift and/or help from another person.

The disk drives from the faulted server will be transferred to the replacement server. You will need suitable work surface(s), capable of supporting the weight of the servers while the transfer is accomplished.

Procedure

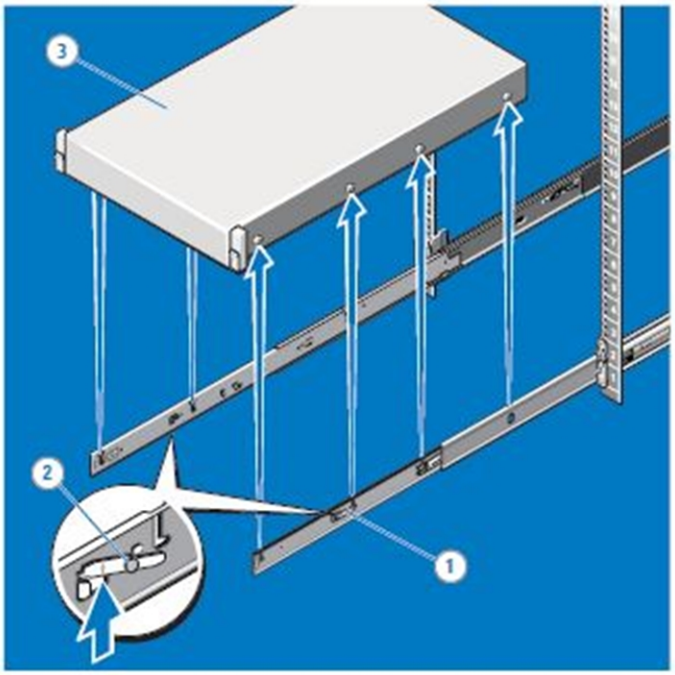
1. At front of the cabinet, locate the slam latch on either side of the server (1). Pull up the slam latches to release the server from the cabinet (2). Then, pull the server from cabinet until the rails lock in place.

Figure 8 Release the slam latches and extend server from cabinet



2. Locate the lock levers on the sides of the inner rails (1). Unlock each lever by rotating it up to its release position (2). Grasp the sides of the server (3) firmly and pull it forward until the server standoffs are at the front of the J-slots in the rails. Lift the server up and away from the rails.

Figure 9 Sliding server out of the cabinet to the locked position



3. Place the server on a suitable work surface. Ensure the work surface(s) is capable of supporting weight of the server and replacement server.

Unpack replacement server

⚠ CAUTION

The server is heavy and should be removed from the packing by two people. To avoid personal injury and/or damage to the equipment, do not attempt to unpack the server without help from another person.

The disk drives, SD module, and inner rails from the faulted server will be transferred to the replacement server. You will need suitable work surface(s), capable of supporting the weight of the servers while the transfer is accomplished.

Procedure

1. Unpack the replacement server.

   Note

   Save the packing material to return the faulted server.

2. Place the replacement server on a suitable work surface where the disk drives, SD module, and inner rails will be transferred from the faulted server to this server. Ensure the work surface(s) is capable of supporting weight of the servers.

PowerEdge disk layout

When transferring disks from the failed server to the replacement server, place the disk in the same slot in the replacement server where it resided in the failed server.

The following table shows the disk layout.

Table 9 Disk layout

Front panel - No disks		Slot 2 - HDD	Slot 4 - HDD	Slot 6 - Blank
Slot 0 - HDD	Slot 1 - HDD	Slot 3 - HDD	Slot 5 - SSD	Slot 7 - Blank

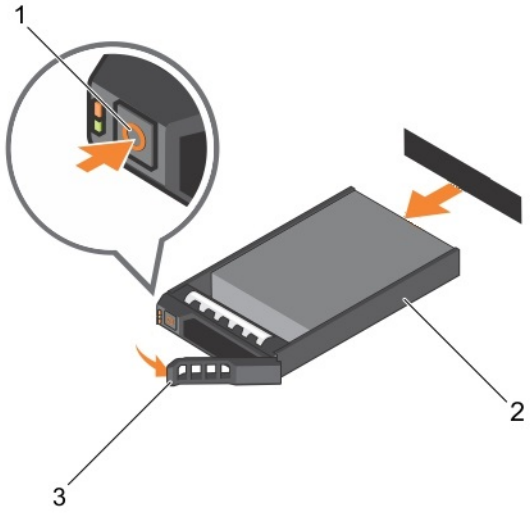
Place the old server chassis and the new server chassis side-by-side when moving disks, to ensure proper disk placement in the new server.

Transferring a disk drive for server replacement

Procedure

1. Press the release button to open the disk drive carrier release handle.
2. Slide the disk drive carrier out of the hard drive slot.

Figure 10 Removing a hard drive



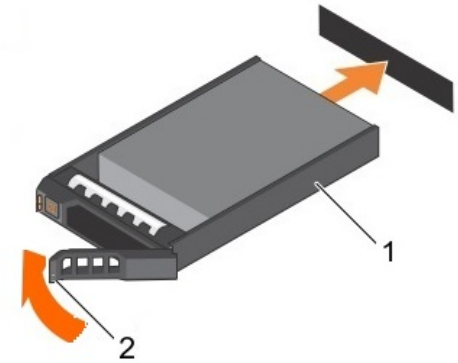
1. Release button
2. Disk/carrier
3. Drive carrier handle

⚠ CAUTION

You must transfer the disk drive tray to the exact corresponding slot in the replacement chassis that it was removed from.

3. Insert the disk drive carrier into the disk drive slot until the carrier connects with the backplane.
4. Close the disk drive carrier handle to lock the disk drive in place.

Figure 11 Installing a disk drive



1. Disk/carrier
2. Drive carrier handle

5. Repeat steps1 - 4 to transfer all remaining disks from the faulted server to the replacement server.

Install and secure the server in the cabinet (sliding rails)

This procedure is used to install the server (mounted on sliding rails) in the cabinet.

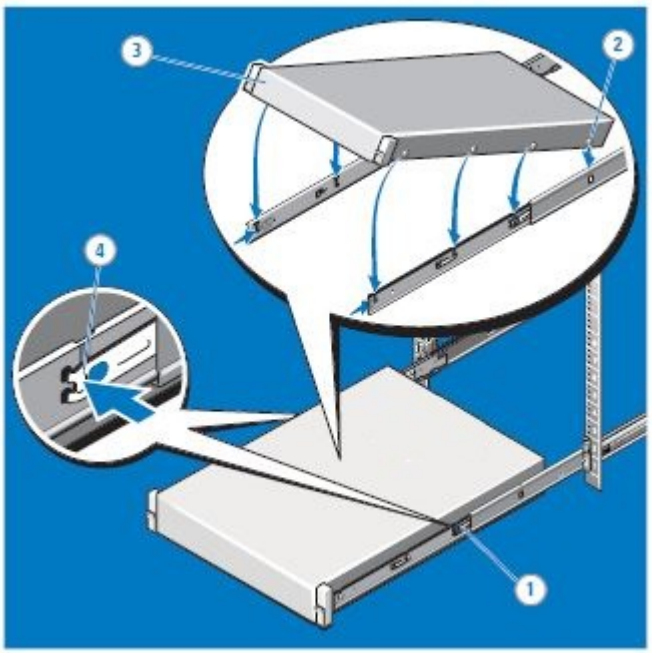
⚠ CAUTION

The server is heavy and should be installed in a cabinet by two people. To avoid personal injury and/or damage to the equipment, do not attempt to install the server in a cabinet without a mechanical lift and/or help from another person.

Procedure

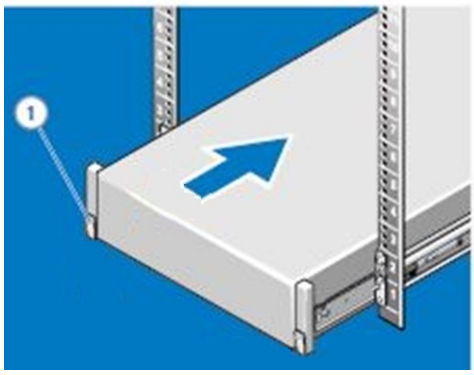
1. At front of the cabinet, pull the inner slide rails out of the rack until they lock into place (1). Locate the rear rail standoff on each side of the server and lower them into the rear J-slots on the slide assemblies (2). Rotate the system downward until all the rail standoffs are seated in the J-slots (3). Push the server inward until the lock levers click into place. Press the slide-release lock buttons on both rails and slide the system into the rack (4).

   Figure 12 Installing the server on the rails



2. Push the server into the cabinet. The latches (1) engage automatically as the system is pushed into the cabinet.

Figure 13 Sliding server into of the cabinet



Connect power cords and I/O cables

Procedure

1. Using the connection information recorded on the labels, connect the I/O cables to the server.

   The following table lists the connections between the Dell server iDRAC ports and the Dell switch.

   Table 10 iDRAC ports and Dell switch connections

Server	iDRAC port connection
Power EdgeR630 1	Dell switch port 37
Power EdgeR630 2	Dell switch port 36
Power EdgeR630 3	Dell switch port 35

   Note

   The lower row of Ethernet ports is not directly below the top row as shown in the table. The first and third ports from the left on both rows are cabled to the Dell switch.

   The following table lists the connections between the Dell server I/O ports and the Dell Switch.

   Table 11 Ethernet port layouts

Server	I/O port connections	
Power EdgeR630 1	Dell switch port 10	Dell switch port 12
	Dell switch port 9	Dell switch port 11
Power EdgeR630 2	Dell switch port 6	Dell switch port 8
	Dell switch port 5	Dell switch port 7
Power EdgeR630 3	Dell switch port 2	Dell switch port 4
	Dell switch port 1	Dell switch port 3

2. Plug the power cords into the power supplies.

3. Connect a serial cable between the service laptop and the new server.
4. Configure a Putty session to connect the service laptop to the new server.

   Use the following settings:

   - 115200 baud rate
   - No parity
   - 8 data bits
   - 1 stop bit
   - No flow control

5. Power on the server from the front power button.

Restore iDRAC settings

Once the new iDRAC server is installed, the settings must be restored.

Complete the following steps to restore the iDRAC settings after the new server is installed.

Procedure

1. Power on the server, and when prompted press `Esc + 2` to enter the Setup process.

   Use the username `root`, and the default password `calvin`.
   The username and password might differ depending on the information (root user password, or username and password for a non-root user) provided in Record server information.

2. From the main menu, select **iDRAC Settings** > **Network Settings**.
3. Use the arrow keys to select **Enable NIC**, and press the spacebar to toggle the value to Enabled.
4. Under **IPv4 Settings**, configure the settings using the details that were recorded prior to replacing the server.

   a. Enable **Enable NIC**.

   b. Disable **Enable DHCP**.

   c. In the **Static IP Address** field, specify the previously recorded IP address.

   d. In the **Static Gateway** field, specify the previously recorded gateway IP address.

   e. In the **Subnet Mask** field, specify the previously recorded subnet mask.
5. Under **IPv6 Settings**, disable IPv6.
6. Under **IPMI Settings**, enable **IPMI over LAN**.
7. Press `ESC` twice, press `Enter` to select **Yes** in the window that appears, then press `Enter` to select **OK** at the confirmation pop-up.
8. From the main menu, select **iDRAC Settings** > **User Configuration**.

   a. Enable **Enable User**.

   b. Verify the username is root.

   c. In the **Change Password** field, type the previously recorded customer iDRAC password and press `Enter`.

d. In the **Reenter Password** field, type the iDRAC password again and click **OK**.

e. Press `Esc`, then click **Yes** to save the changes.

9. Select **Advanced Controller Properties** to disable the storage controller cache.

a. Set **Disk Cache for Non-RAID** to `Disable`.

b. Select **Apply Changes** to save the settings.

c. Press `Esc` three times, then select **Yes** to exit.

10. Select **Device Settings** to set the hard drives in passthrough mode.

a. Select **Integrated RAID Controller 1: Dell PERC Configuration Utility**.

b. Select **Controller Management** > **Advanced Controller Management**.

c. Select **Switch to HBA Mode**.

d. Press `Esc`, then click **Yes** to exit.

Install ESXi

Before you begin

- Download the ISO and md5sum files for the latest version of VMware ESXi 6.0 update 2 to a folder on the service computer, or other location. Both files must be in the same directory.
- Open a command window and change the default directory to the folder containing the ISO and md5sum files.
- Use the md5sum file to verify the ISO file. Run the following command:
  `md5sum -c XXXX`
  The output for each command should be `Ok`.
- Connect an RJ-45 Ethernet cable betweentheEthernet adapter in the service laptop and port38in the IDPA top-of-rack switch. Assign the IP address 102.168.n.n to the service laptop's Ethernet adapter (to allow it to communicate with the set-in-manufcaturing addresses of the IDPA components.

Note

The 192.168.n.n address can be added to the service laptop's IP configuration without replacing the current static address).

To install ESXi on the replacement server, complete the following steps:

Procedure

1. To access the server iDRAC interface, open a browser window, and type in the iDRAC IP address.
2. Log in to iDRAC as root, with the previously recorded customer password.
3. To launch a Virtual Remote Console, click **Overview** > **Server** > **Virtual Console** > **Launch Virtual Console**
4. To continue, respond to the securtiy prompts.
5. Select **Virtual Media** > **Connect Virtual Media**.
6. Select **Virtual Media** > **Map CD/DVD**.

7. On the service computer, browse to the folder containing the ESXi ISO file.
8. Select the ISO file and click **Open**.
9. Click **Map Device**.
10. Click **Next Boot** > **Virtual CD/DVD ISO**, and click **OK** at the confirmation pop-up.
11. Click **Power** > **Reset System (warm boot)**.

    Allow some time for the ESXi 6.0 installer to load.
12. Select the ESXi installation option that corresponds to the server that was replaced:
    - **install esx-01**
    - **install esx-02**
    - **install esx-03**
13. To select the Installer image, press `Enter` and continue.

    The installation is silent and does not require any further input.

Configure ESXi

Complete the following steps to configure ESXi after installing it on the replacement server node.

Procedure

1. Connect to the new server with an SSH session.

   Use the 192.168.100.*<X>* IP address that corresponds to the position of the new server:
   - ESXi node 1: 192.168.100.101
   - ESXi node 2: 192.168.100.102
   - ESXI node 3: 192.168.100.103
2. Log in as root, using the previously recorded password.
3. Set the previously recorded customer IP address on the new server.

   Run the following command:
   ```
   esxcli network ip interface ipv4 set --interface-name=vmk2
   --ipv4=<customer-IP-address> --netmask=255.255.255.0 --
   type=static
   ```
4. Set the previously recorded customer gateway IP address on the new server.

   Run the following command:
   ```
   esxcfg-route -a default <customer-gateway-address>
   ```
5. Start the vSphere Client, and connect to the new server using the previously recorded username and password.
6. Select **Configuration** > **Time Configuration**.
7. Select **Properties** > **Options** > **NTP Settings**.
8. Click **Add**.
9. In the **Add NTP Server** dialog, specify the IP address or fully qualified domain name of the customer NTP server (customer supplied).

10. Click **OK**.

Add the ESXi host to vCenter

Complete the following steps to add the new ESXi host to vCenter.

Procedure

1. In an internet browser, launch the VMware vSphere Web Client and access the IDPA vCenter Server.
2. Select **Hosts and Clusters**.
3. Right-click the **DPAppliance-VSAN** icon and select **Add Host**.
   a. Specify the previously recorded server hostname and click **Next**.
   b. Specify `root` as the username, and type the previously recorded root password.
   c. In the **Certificate Error** window that appears, click **Yes**.
   d. At the **Host Summary**, click **Next**.
   e. Select the ESXi License Key, and click **Next**.
   f. Verify **Lockdown Mode** is disabled, and click **Next**.
   g. Select the option to pull a list of virtual machine rather than create a new pool, and click **Next**.
   h. Click **Finish**.
4. Select the DPalliance-VSAN Cluster, and expand it with the triangle icon.
5. Select the IDPA Cluster.
6. In the right-hand pane, select the **Manage** tab.
7. Select **Settings**.
8. Select **Disk Management**, and verify that the new ESXi host disk groups match the other ESXi hosts as follows:
   a. Verify the number of Disk Groups are the same.
   b. Verify the number of Disks per Group are the same.

   If the number of Disk Groups or Disks per Group do not match, call support.
9. Add the new server to the vSAN cluster.
   a. Using the previously recorded information, connect to one of the other ESXi hosts with SSH.
   b. Identify the vSAN Sub Cluster UUID.

      Run the following command:
      `esxcli vsan cluster get`
      Record the `Sub-Cluster UUID` value.

   c. Connect to the new ESXi host with SSH.
   d. Join the new ESXi host to the vSAN Sub Cluster

      Run the following command, using the recorded Sub Cluster ID:
      `esxcli vsan cluster join <sub-cluster-UUID>`

e. Verify the new ESXi host is joined to the vSAN cluster.

Run the following command:
```
esxcli vsan cluster get
```

f. From the vSphere Web Client, refresh the vSAN status to verify it displays as healthy.

Resolve cluster warning messages

Complete the following steps to resolve the warning message.

Procedure

1. Expand the cluster by selecting the triangle.
2. If the **Virtual SAN Disk Balance** displays a warning message, continue with this procedure. Contact support to resolve other error or warning messages.
3. Select **Virtual SAN Disk Balance**.
4. Select **Rebalance Disks**.

   The disk rebalance operation takes approximately three hours to complete.

Complete the procedure

Complete the following steps after the replacement component is installed and configured.

Procedure

1. Clear VMware Alarms.
   a. In the VMware web interface, select each virtual SAN alarm alert from the **Alarms** section.
   b. Right-click each alarm and select **Reset to Green**.
2. Clear the disk locator LED by selecting **All Action** and turn the LED to **OFF**.
3. Log out of all VMware and Dell interfaces.
4. Disconnect the service computer from the top-of-rack switch.

Update the Install Base

After replacing a Dell server or switch chassis, complete the following steps to update the Install Base with the serial number of the new hardware.

Procedure

1. In an internet browser, navigate to the Business Services Portal at http://emc.force.com/BusinessServices.
2. Under **Post Sales**, select **Install Base Group**.
3. In the **Case Subtype** list box, select **IB Status Change**, and click **Select**.
4. Specify your own contact name, email address, phone number, and theater.

Note

Add the email addresses of anyone else who needs to be notified of the Install Base change.

5. In the **Case Details** section, specify case details in the **Subject** and **Description** fields.

   Select the **Federal Case** checkbox if the support activity is at a federal site.

6. Select the Product Families that apply to the support activity.

   Family is defined as the TLA/Model product family for your request. If you have multiple product families in your request and one of them is listed here, choose that family, otherwise choose **All Other Families**.

7. Fill out the additional fields that are relevant to the support activity.

Note

For more than one Serial number, enter each value separated with a comma. If there is a large number of values, a Microsoft Excel spreadsheet can be attached. See help text. The Serial number used here is the Avamar UID obtained from "System ID" field of "mccli server show-prop" (Remove the colons and the '@'.)

8. In the **Remote Connection** field, specify the DialHome details.
9. Use the **Upload Documents** section to attach any relevant supporting documentation to the service request.
10. Click **Submit** to complete the service request.

    You will receive automated e-mail notifications to stay up-to-date on the progress of your request.

CHAPTER 5

Dell S4048-ON Switch FRUs

This chapter includes the following topics:

Replace an SFP+ or QSFP+ optic

The Dell S4048-ON switch has 48 ports that use SFP+ optics, and 6 ports that use QSFP+ optics. To replace a failed optic, complete the following steps.

⚠ CAUTION

If the components are mishandled, ESD damage can occur. Always wear an ESD-preventive wrist or heel ground strap when handling the S4048-ON and its components.

⚠ WARNING

When working with optical fibers, follow all the warning labels and always wear eye protection. Never look directly into the end of a terminated or unterminated fiber or connector as it can cause eye damage.

Procedure

1. Push the tab on the failed optic and slide it from the port.

   When removing optics with direct attach cables (DACs) from the port, pull the release tab firmly and steadily. Before pulling the release tab, you may need to gently push the optic into the port to ensure it is seated correctly. Do not jerk or tug repeatedly on the tab.
2. Position the optic so it is in the correct position. The optic has a key that prevents it from being inserted incorrectly.
3. Insert the optic into the port until it gently snaps into place.

   Note

   - Both rows of QSFP+ ports require that you install the 40GbE optics with the tabs facing up.
   - When you cable the ports, be sure not to interfere with the airflow from the small vent holes above and below the ports.

Replacing a Power Supply

This document describes how to replace a faulted power supply in a Dell S4048-ON network switch.

Location and description of power supply units

The S4048–ON switch contains two power supply units (PSU), designated PSU 1 and PSU 2. Each PSU has a connector for the AC power cord connection and a lever to release and extract the PSU from the switch.

Two PSUs are required for full redundancy, but the system can operate with a single PSU. When running with full redundancy (two power supplies installed and running), you can remove and replace one PSU without disrupting traffic.

When viewing the rear panel, PSU 1 is on the left side of the chassis; PSU 2 is on the right side of the chassis.

Figure 14 S4048–ON PSUs on the rear panel

1. PSU 1
2. PSU 2

Power supply units status indicators

Each PSU has a bi-color (amber and green) LED to indicate power supply status.

Figure 15 PSU LED location

1. PSU 1 LED
2. PSU 2 LED

Table 12 PSU LED behavior

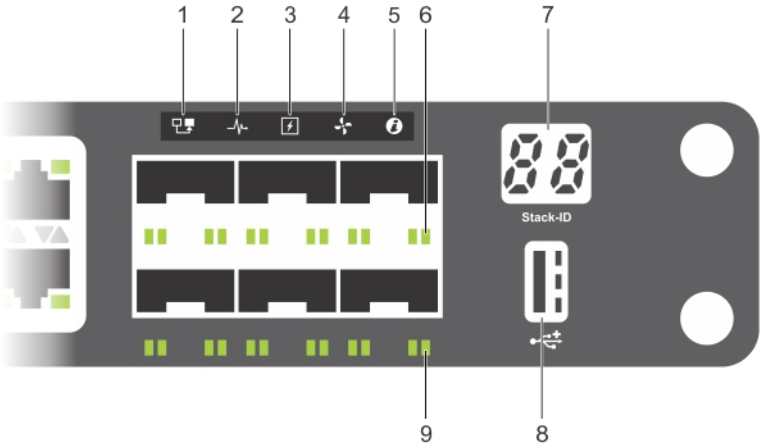
Power Supply Condition	LED State
Output ON and OK	Green
No AC power to both power supplies	Off
AC present / Only 12 VSB on (PSU off) or PSU in Smart on state	1 HZ blinking green
AC cord unplugged or AC power lost; with a second power supply in parallel still with AC input power	Amber
Power supply warning events where the PSU continues to operate; high temp, high power, high current, slow fan	1 HZ blinking amber
PSU critical event causing a shutdown; failure, OCP, OVP, fan fail	Amber
PSU firmware updating	2 HZ blinking green

S4048-ON front panel indicators

Note

Do not rely solely on the front panel indicators when checking the switch for proper operation. You must also check the indicators on the fans and power supplies (rear panel). Some fan and power supply conditions may not be indicated at the front panel.

Figure 16 S4048–ON front panel indicators



1. Master LED
2. System LED
3. Power LED
4. Fan LED
5. Locator LED
6. SFP+ link/activity LEDs
7. Stack LED
8. USB port LED
9. QSFP+ link/activity LEDs

Table 13 S4048–ON LED behavior

LED	Description
System Status/Health LED	• Solid green—Normal operation • Blinking green—Booting • Solid amber—Critical system error • Blinking amber—Non-critical system error, fan failure, or power supply failure
Power LED	• Off—No power

Table 13 S4048–ON LED behavior (continued)

LED	Description
	• Solid Green—Normal • Solid amber—POST is in process • Blinking amber—Power supply failed
MASTER LED	• Off—Switch is in Stacking Slave mode • Solid green—System is in Stacking Master or Standalone mode
FAN LED	• Solid green—fan powered and running at the expected RPM • Solid amber—fan failed including incompatible airflow direction when you insert the PSU or fan trays with differing airflows
PSU LED	• Solid green—Normal operation • Solid amber—Power supply critical event causing a shutdown • Blinking amber—Power supply warning event; power continues to operate.
LOCATOR LED	• Off—Locator function is disabled • Blinking blue—Locator function is enabled

Table 14 Management Ethernet port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 1 Gbps speed • Solid yellow—Link on 10/100 Mbps speeds

Table 15 SFP+ port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 10 Gbps speed • Solid Amber—Link on 1 Gbp speed **Note** If you are using 1x40G, one LED displays. If you are using 4x10G, four LEDs display.

Table 15 SFP+ port LEDs (continued)

LED	Description
Activity LED	• Off—No Link • Blinking green—Transmit/receive is active

Table 16 QSFP+ port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 40 Gbps speed • Solid amber—Link on 10 Gbps speeds

Storing and handling components

It is recommended to use these guidelines if you do not install replacement components immediately:

- Storage location temperature must remain constant ranging from -40° to 158°F (from -40°C to 70°C).
- Store on a dry surface or floor, away from direct sunlight, heat, and air conditioning ducts.
- Store in a dust-free environment.

⚠ CAUTION

ESD damage can occur when components are mishandled. Always wear an ESD-preventive wrist or heel ground strap when handling the S4048–ON and its accessories. After you remove the original packaging, place the S4048–ON and its components on an anti-static surface.

Replacing a power supply unit

The PSUs have an integrated fan, which you cannot replace. If the fan integrated in a PSU fails, you must replace the entire PSU.

⚠ WARNING

Disconnect the power cord before removing the PSU.

⚠ CAUTION

If components are mishandled, ESD damage can occur. Always wear an ESD-preventive wrist or heel ground strap when handling the S4048–ON and its components.

Note

If you use a single PSU, install a blank plate in the other PSU slot. If you are only using one PSU, install the power supply in the first slot (PSU 1) and install a blank plate in the second slot (PSU 2).

Procedure

1. Disconnect the power cable from the PSU.
2. Raise the handle on the PSU.
3. With your index finger over the PSU handle, press the orange lever to the left with your thumb. Pull the PSU out of the switch and place it on an anti-static surface.

   ⚠ WARNING

   Do not connect the power cord before inserting the PSU in the chassis.

   ⚠ CAUTION

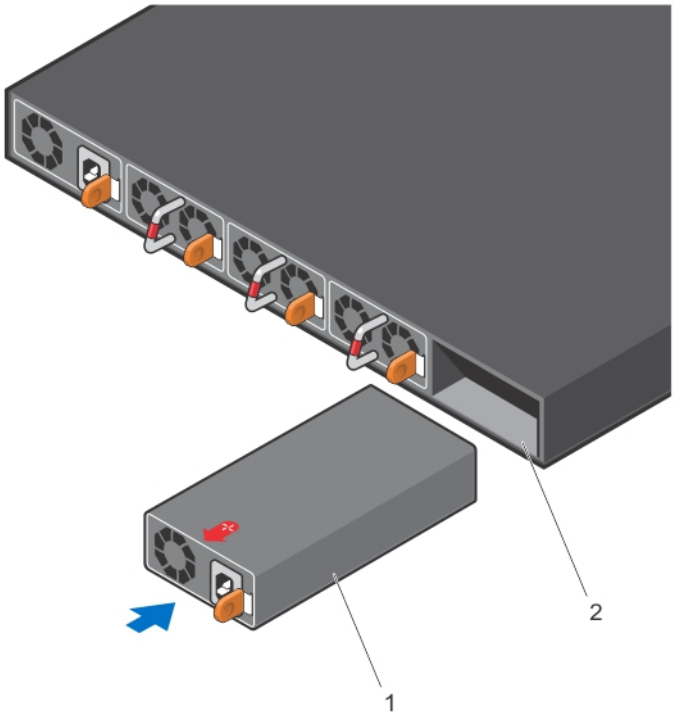
   The PSU slides into the slot smoothly. Do not force a PSU into a slot as this action may damage the PSU or the S4048–ON chassis.

4. Remove the replacement PSU from the electro-static bag.
5. Insert the PSU into the switch PSU slot. Insert the PSU exposed PCB edge connector first.

   The PSU slot is keyed so that the PSU can be fully inserted in one direction only.

6. Slide the PSU into the switch PSU slot until it snaps in place.

Figure 17 Install the PSU



1. PSU
2. PSU slot

7. Plug the power cord into the connector on the power supply unit.

   The PSU powers up as soon as the cable is connected.
8. Indicate that the PSU is operating normally by checking the LEDs on the PSU and the front panel.
9. Using the shipping materials that the replacement PSU shipped in, re-package the faulted PSU and prepare the package for return shipping.

Verify the replacement component

Verifying the component replacement requires connecting to the Dell switch to access the Dell switch management interface. Connect to port 38 on the Dell switch. The switch port layout is displayed in the following table.

Table 17 Switch port layout

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

Procedure

1. Log in to the Dell switch with the username admin, and the customer-provided password.
2. Verify the status of the replacement component is `up`.

   Run the following command:

```
show environment all
```

Replacing a Fan

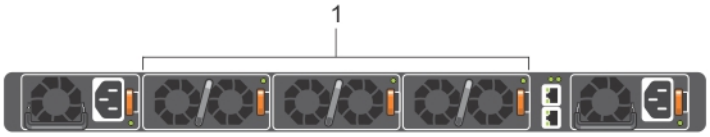
This document describes how to replace a faulted fan in a Dell S4048-ON network switch.

Location and description of the fan modules

The S4048-ON contains three fan modules. Module slot 1 is on the left side of the chassis, module slot 2 is in the middle of the chassis, and module slot 3 is on the right side of the chassis.

The fan speed increases when the internal temperature reaches 161.6°F (72°C) and decreases to normal speed when the temperature falls to 136.4°F (58°C). The S3048-ON never intentionally turns off the fans.

Figure 18 S4048–ON fan modules

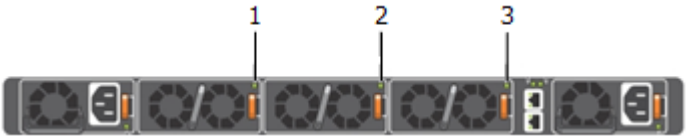


1. Fan modules

Fan module status indicator

Each fan module has a bi-color (green and amber) LED to indicate fan module operating status.

Figure 19 Fan module LED location



1. Fan module 1 LED
2. Fan module 2 LED
3. Fan module 3 LED

Table 18 Fan module LED behavior

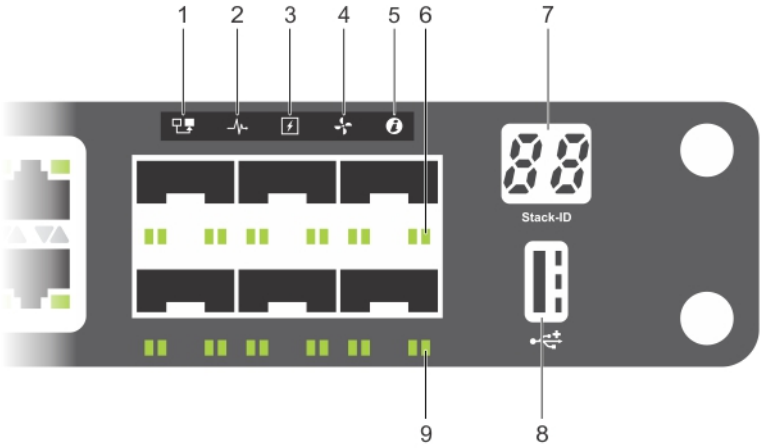
Fan Module Condition	LED State
No fault	Green
Fault	Amber

S4048-ON front panel indicators

Note

Do not rely solely on the front panel indicators when checking the switch for proper operation. You must also check the indicators on the fans and power supplies (rear panel). Some fan and power supply conditions may not be indicated at the front panel.

Figure 20 S4048–ON front panel indicators



1. Master LED
2. System LED
3. Power LED
4. Fan LED
5. Locator LED
6. SFP+ link/activity LEDs
7. Stack LED
8. USB port LED
9. QSFP+ link/activity LEDs

Table 19 S4048–ON LED behavior

LED	Description
System Status/Health LED	• Solid green—Normal operation • Blinking green—Booting • Solid amber—Critical system error • Blinking amber—Non-critical system error, fan failure, or power supply failure
Power LED	• Off—No power

Table 19 S4048–ON LED behavior (continued)

LED	Description
	• Solid Green—Normal • Solid amber—POST is in process • Blinking amber—Power supply failed
MASTER LED	• Off—Switch is in Stacking Slave mode • Solid green—System is in Stacking Master or Standalone mode
FAN LED	• Solid green—fan powered and running at the expected RPM • Solid amber—fan failed including incompatible airflow direction when you insert the PSU or fan trays with differing airflows
PSU LED	• Solid green—Normal operation • Solid amber—Power supply critical event causing a shutdown • Blinking amber—Power supply warning event; power continues to operate.
LOCATOR LED	• Off—Locator function is disabled • Blinking blue—Locator function is enabled

Table 20 Management Ethernet port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 1 Gbps speed • Solid yellow—Link on 10/100 Mbps speeds

Table 21 SFP+ port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 10 Gbps speed • Solid Amber—Link on 1 Gbp speed **Note** If you are using 1x40G, one LED displays. If you are using 4x10G, four LEDs display.

Table 21 SFP+ port LEDs (continued)

LED	Description
Activity LED	• Off—No Link • Blinking green—Transmit/receive is active

Table 22 QSFP+ port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 40 Gbps speed • Solid amber—Link on 10 Gbps speeds

Storing and handling components

It is recommended to use these guidelines if you do not install replacement components immediately:

- Storage location temperature must remain constant ranging from -40° to 158°F (from -40°C to 70°C).
- Store on a dry surface or floor, away from direct sunlight, heat, and air conditioning ducts.
- Store in a dust-free environment.

⚠ CAUTION

ESD damage can occur when components are mishandled. Always wear an ESD-preventive wrist or heel ground strap when handling the S4048–ON and its accessories. After you remove the original packaging, place the S4048–ON and its components on an anti-static surface.

Replacing a fan module

The S3048-ON supports two airflow direction options. Do not mix airflow types in a chassis; you can use only a single airflow direction in a chassis. If the airflow directions are mismatched, the S4048-ON powers down in one minute.

To run the system, the three fan module slots must have operating fan modules. If you do not install a module in each slot, the system shuts down in one minute.

⚠ CAUTION

ESD damage can occur if components are mishandled. Always wear an ESD-preventive wrist or heel ground strap when handling the S4048–ON and its components.

Procedure

1. Remove the replacement fan module from the electro-static bag and place it on an anti-static surface.

⚠ CAUTION

Complete steps 2 and 3 within one minute, or the system will power down.

2. With your index finger around the fan module handle, press the orange lever to the left with your thumb. Pull the fan module out of the fan module slot and place it on an anti-static surface.
3. Use the handle on replacement fan module to slide it into the fan module slot until it snaps in place.

   The fan begins to operate immediately.
4. Check that the fan module and the front panel LEDS indicate the fan module is operating normally.
5. Using the shipping materials that the replacement fan module shipped in, repackage the faulted fan module and prepare the package for return shipping.

Verify the replacement component

Verifying the component replacement requires connecting to the Dell switch to access the Dell switch management interface. Connect to port 38 on the Dell switch. The switch port layout is displayed in the following table.

Table 23 Switch port layout

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

Procedure

1. Log in to the Dell switch with the username admin, and the customer-provided password.
2. Verify the status of the replacement component is `up`.

   Run the following command:
   ```
   show environment all
   ```

Replacing a Switch

This document describes how to replace a Dell S4048-ON network switch.

Introduction

S4048-ON is a networking switch for campus aggregation and core switching 10 Gbps servers and 40 Gbps optical uplinks to the 40 Gbps switching fabric in the core.

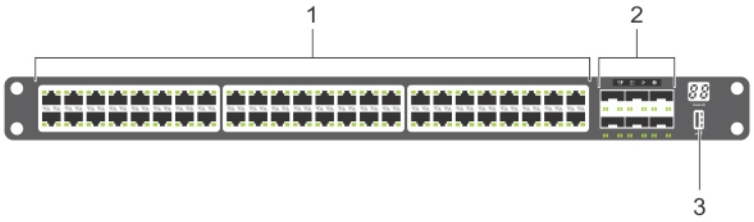
The S4048–ON has:

- Forty-eight ports of 10G SFP+ ports for a 1/10 Gbps transceiver
- Six 40 Gbps fixed QSFP+ optical ports for a 40 Gbps transceiver
- Serial RS 232 port, RJ-45, and MicroUSB
- RJ–45 management port

The S4048–ON I/O side includes:

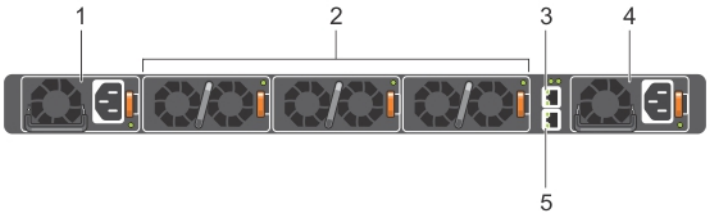
- Forty-eight fixed SFP+ and six fixed QSFP+ ports
- Management port
- USB 2.0 port
- Serial RS 232 port, RJ-45 and MicroUSB
- LED display for the system, fan, and power status

Figure 21 S4048–ON I/O-side view



1. SFP+ ports
2. QSFP+ ports
3. USB Type-A storage port

Figure 22 S4048–ON PSU-side view



1. Power supply unit 1
2. Fan module
3. Out-of-band management port
4. Power supply unit 2
5. RS-232 serial console port

Specifications

Table 24 Chassis physical design

Parameter	Specifications
Height	1.71 inches (43.5 mm)

Table 24 Chassis physical design (continued)

Parameter	Specifications
Width	17.09 inches (434 mm)
Depth	18.11 inches (460 mm)
Chassis weight with factory-installed components	21.7 lbs (9.86 kg)
Rack clearance required	Front: 5 inches (12.7 cm)
	Rear: 5 inches (12.7 cm)

Table 25 Environmental parameters

Parameter	Specifications
Operating temperature	32° to 113°F (0° to 45°C)
Operating humidity	5 to 85% (RH), non-condensing
Storage temperature	–40° to 158°F (–40° to 70°C)
Storage humidity	5 to 95%, non-condensing
Maximum thermal output	1153.265 BTU/hr
Maximum operational altitude	10,000 feet (3,048 meters)
Maximum non-operational altitude	No performance degradation to 35,000 feet (10,668 meters)
Shock	Meets Bellcore Zone 4 earthquake requirements (MIL-STD-810)

Table 26 AC power requirements

Parameter	Specifications
Power supply	100–240 VAC 50/60 Hz
Maximum current draw per system	5.8 A @ 398.02 watts/100vac
	2.9 A @ 398.02 watts/200vac
Maximum power consumption	460 Watts
Typical power consumption	338 Watts
Reliability	MTBF 355.178 hours

System status

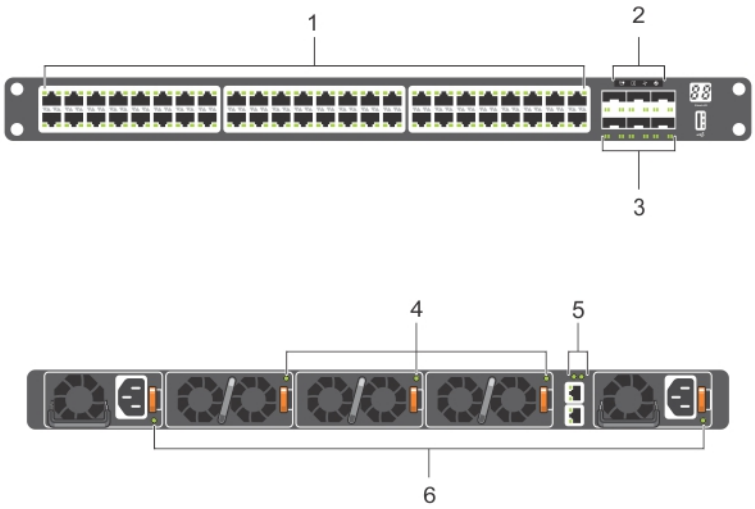
You can view S4048–ON status information using the light emitting diodes (LEDs).

LED displays

The S4048–ON includes LED displays on both the I/O Port and PSU side of the chassis, as shown.

For LED information, see your third-party operating software documentation.

Figure 23 S4048–ON LEDs

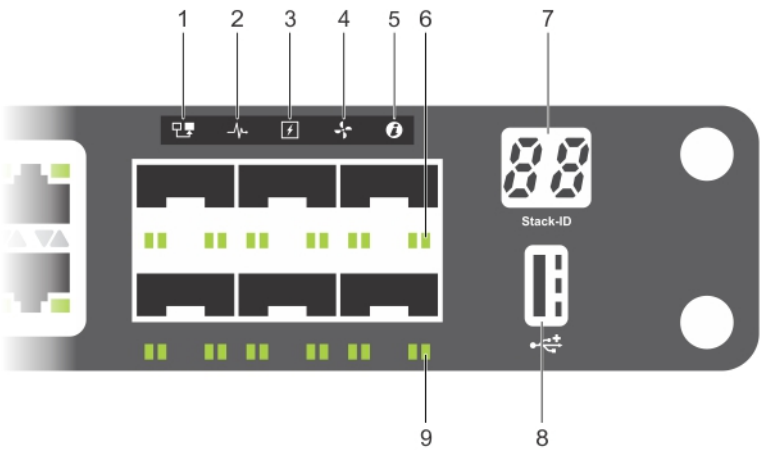


1. SFP+ port Link and activity LEDs
2. System LEDs
3. QSFP+ port LEDs
4. FAN LED
5. Management port LEDs
6. PSU LED

LED behavior

The following S4048–ON system LED behavior is seen during open networking installation environment (ONIE) operations:

Figure 24 S4048–ON LEDs



1. Master LED
2. System LED
3. Power LED
4. Fan LED
5. Locator LED
6. SFP+ link/activity LEDs
7. Stack LED
8. USB port LED
9. QSFP+ link/activity LEDs

Table 27 S4048–ON LED behavior

LED	Description
System Status/Health LED	• Solid green—Normal operation • Blinking green—Booting • Solid amber—Critical system error • Blinking amber—Non-critical system error, fan failure, or power supply failure
Power LED	• Off—No power • Solid Green—Normal • Solid amber—POST is in process • Blinking amber—Power supply failed
MASTER LED	• Off—Switch is in Stacking Slave mode • Solid green—System is in Stacking Master or Standalone mode
FAN LED	• Solid green—fan powered and running at the expected RPM • Solid amber—fan failed including incompatible airflow direction when you insert the PSU or fan trays with differing airflows
PSU LED	• Solid green—Normal operation • Solid amber—Power supply critical event causing a shutdown • Blinking amber—Power supply warning event; power continues to operate.
LOCATOR LED	• Off—Locator function is disabled • Blinking blue—Locator function is enabled

Table 28 Management Ethernet port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 1 Gbps speed • Solid yellow—Link on 10/100 Mbps speeds

Table 29 SFP+ port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 10 Gbps speed • Solid Amber—Link on 1 Gbp speed **Note** If you are using 1x40G, one LED displays. If you are using 4x10G, four LEDs display.
Activity LED	• Off—No Link • Blinking green—Transmit/receive is active

Table 30 QSFP+ port LEDs

LED	Description
Link LED	• Off—No Link • Solid green—Link on 40 Gbps speed • Solid amber—Link on 10 Gbps speeds

Storing and handling components

It is recommended to use these guidelines if you do not install replacement components immediately:

- Storage location temperature must remain constant ranging from -40° to 158°F (from -40°C to 70°C).
- Store on a dry surface or floor, away from direct sunlight, heat, and air conditioning ducts.
- Store in a dust-free environment.

⚠ CAUTION

ESD damage can occur when components are mishandled. Always wear an ESD-preventive wrist or heel ground strap when handling the S4048–ON and its accessories. After you remove the original packaging, place the S4048–ON and its components on an anti-static surface.

Unpack the replacement switch

Note

Before unpacking the system, inspect the container and immediately report any evidence of damage.

Procedure

1. Place the container on a clean, flat surface and cut all straps securing the container.
2. Open the container or remove the container top.
3. Carefully remove the switch from the container and place it on a secure, clean and static-free surface.
4. Remove all packing material.
5. Inspect the product and accessories for damage.
6. Retain the container and all packing material for repackaging and returning the faulted switch.

Prepare for switch replacement

Before you begin

The ACM, and all IDPA services and virtual machines must be stopped. If they are not stopped, stop them as described in Stop the data protection service and appliance.

Complete the following steps to disable the Data Domain network ports and stop the Avamar services.

Procedure

1. Log in to the Data Domain system.
2. Identify the I/O module slot number where the network traffic is occurring on the Data Domain system.

   Run the following command:
   `net show config`

```
ethMa     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:A9
          inet addr:10.241.160.24  Bcast:10.241.160.255  Mask:
255.255.255.0
          inet6 addr: 2620:0:170:4140:260:16ff:fe5c:8ca9/64
Scope:Global
          inet6 addr: fe80::260:16ff:fe5c:8ca9/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500
Metric:1
          RX packets:1208361053 errors:0 dropped:92194 overruns:
0 frame:0
          TX packets:1366864848 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:683470101483 (636.5 GiB)  TX bytes:
```

```
897875829943 (836.2 GiB)
          Interrupt:17

ethMb     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:A8
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:16

ethMc     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:AB
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17

ethMd     Link encap:Ethernet  HWaddr 00:60:16:5C:8C:AA
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:16

eth1a     Link encap:Ethernet  HWaddr 00:60:16:52:35:28
          inet addr:10.241.173.240  Bcast:10.241.173.255  Mask:
255.255.255.0
          inet6 addr: fe80::260:16ff:fe52:3528/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:9000
Metric:1
          RX packets:26978140 errors:0 dropped:3370236 overruns:
0 frame:0
          TX packets:1818896 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2450123730 (2.2 GiB)  TX bytes:642406163
(612.6 MiB)
          Interrupt:32 Memory:381c08000000-381c087fffff

eth1b     Link encap:Ethernet  HWaddr 00:60:16:52:35:29
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:36 Memory:381c07000000-381c077fffff

eth1c     Link encap:Ethernet  HWaddr 00:60:16:52:35:2A
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:36 Memory:381c06000000-381c067fffff

eth1d     Link encap:Ethernet  HWaddr 00:60:16:52:35:2B
          BROADCAST ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:37 Memory:381c05000000-381c057fffff
```

In this example, the network traffic is on the I/O module in slot 1.

3. Disable the all the network ports on the I/O module.

   Run the following commands:

```
netconfig eth1a down
netconfig eth1b down
netconfig eth1c down
netconfig eth1d down
```

Do not log out of the Data Domain system, as the network ports must be enabled after the switch replacement is complete.

4. Complete one of the following tasks to stop the Avamar services.

Stop the Avamar services for a DP5300/DP5800

Procedure

1. Login to the Avamar with SSH.
2. Stop all Avamar services.

   Run the following command:
   ```
   dpnctl stop all
   ```

Stop the Avamar services for a DP8300/DP8800

Procedure

1. Login to Avamar Administrator.
2. Navigate to the **Activity** screen.
3. Right-click each backup in progress and select **Cancel Activity**.
4. In Avamar Administrator, select**Server** > **Checkpoint Management**
5. Select a recent, validated checkpoint, or select **Actions** > **Create Checkpoint**.
6. Login to the Avamar Utility Node as the admin user.
7. Load the SSH keys as described in KB article 95614.
8. Verify that no maintenance jobs are running on the Avamar.

   Run the following command:
   ```
   status.dpn
   ```
9. If necessary, create a checkpoint.

   Run the following command:
   ```
   mccli checkpoint create --override_maintenance_scheduler
   ```
10. Shut down all Avamar services.

    Run the following command:
    ```
    dpnctl stop
    ```
11. Answer yes to the EMS question.
12. Verify the Avamar services are stopped.

    Run the following command:
    ```
    dpnctl status
    ```
13. Prepare the Avamar nodes for shut down.

    Run the following commands:
    ```
    mapall --user=root --all 'touch /fastboot'
    mapall --user=root --all 'halt'
    ```
14. Power down all nodes in the grid.

Disconnect network cables and power cords

Remove an optic by pushing the tab on the optic and sliding the optic from the port.

When removing optics with direct attach cables (DACs) from the port, pull the release tab firmly and steadily. Before pulling the release tab, you may need to gently push the optic into the port to ensure it is seated properly. Do not jerk or tug repeatedly on the tab.

Procedure

1. At the front of switch, label each network cable so you can easily identify them when you need to plug them into the replacement switch.

   NOTICE

   Disconnect the uplink cables first.

2. Disconnect uplink cables from ports on the front panel of the switch.
3. Disconnect remaining network cables from ports on the front of the switch.
4. Unplug the two power cords from the power supply unit connectors on rear of the switch.

Removing the switch from the cabinet

Procedure

1. At the rear of the cabinet, unfasten the two mounting screws that secure the switch to the rear of the cabinet.
2. Pull the switch out of the cabinet and place it on a clean, static-free surface.

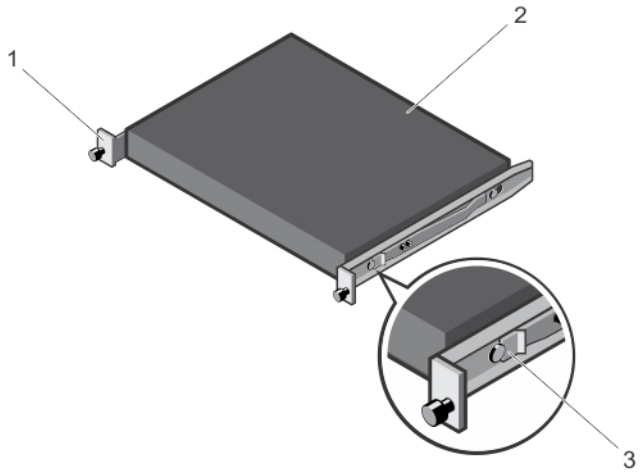
Transfer the inner rails

The two inner rails are transferred from the faulted switch to the replacement switch.

Procedure

1. On each side of the switch, pull outward on the rail locking tab (item 3 below) that secures the inner rail to the shoulder stud. Slide the inner rail forward to release it from the three shoulder posts on the switch.

Figure 25 Remove inner rails



1. Front standoff locking tab
2. Switch
3. Rail locking tab

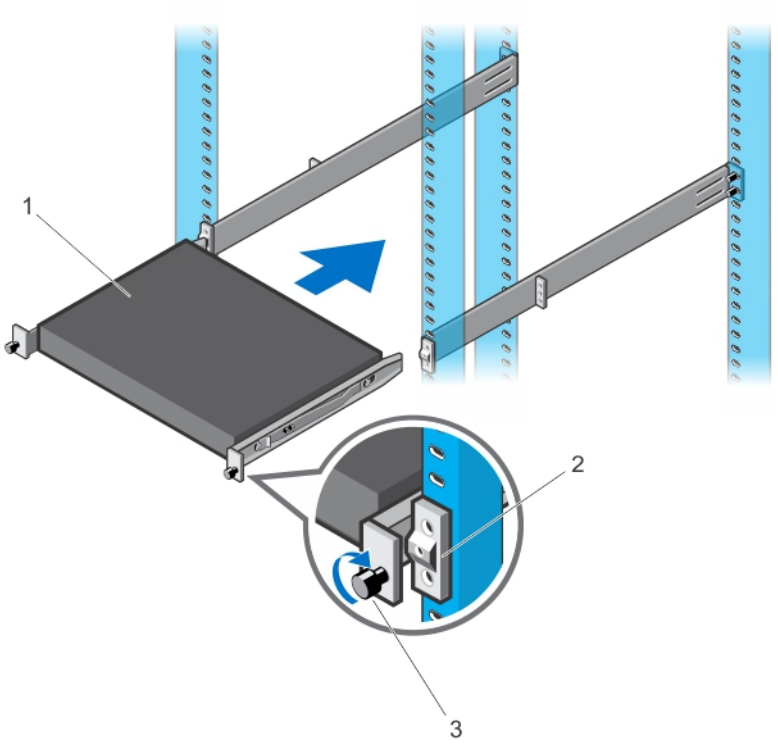
2. On each side of the replacement switch, align the inner rail over the shoulder studs on the switch.
3. Slide the inner rail rearward until the rail locking tab latches behind the front shoulder stud on the switch.

Install the replacement switch in the cabinet

Procedure

1. At the rear of the cabinet, line up the inner rails with the previously mounted Ready-Rails. Slide the switch in until it is flush with the rail bracket (item 2 below). About 3 inches before you fully insert your system, the rail locking feature engages to keep the switch from inadvertently sliding out of the rack and falling.
2. Tighten the two mounting screws to secure the switch to the rail brackets.

Figure 26 Install switch in cabinet



1. Switch
2. Rail bracket
3. Mounting screw

Connect power cords and network cables

Note

When working with optical fibers, follow all the warning labels and always wear eye protection. Never look directly into the end of a terminated or unterminated fiber or connector as it may cause eye damage.

Procedure

1. Connect the AC power cords to the PSU 1 and PSU 2 power connectors.

   Note

   When an AC power cord is connected to a PSU, the switch power is turned on.

2. Using the connection information that is recorded on the labels, connect the network and I/O cables to ports on the front of the switch.
   - Position the optic so it is in the correct position. The optic has a key that prevents it from being inserted incorrectly.
   - Insert the optic into the port until it gently snaps into place.

Note

- Both rows of QSFP+ ports require that you install the 40GbE optics with the tabs facing up.
- When you cable the ports, be sure not to interfere with the airflow from the small vent holes above and below the ports.

Copy the switch configuration file from a USB drive to a switch

Once the switch is replaced, the configuration file for the switch must be copied from a removable USB drive that is dedicated for this purpose.

⚠ CAUTION

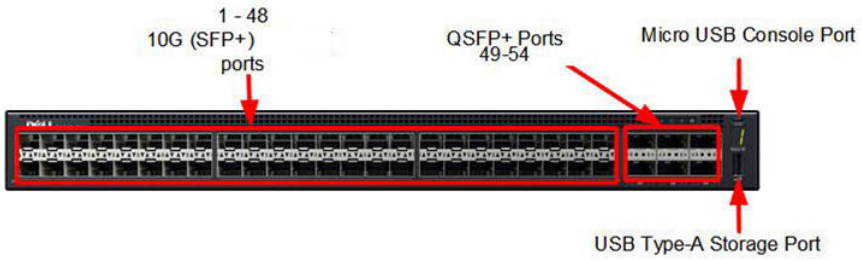
Only use a USB drive that is dedicated to copying and loading the switch configuration file to a system. Do not use any other USB drive, nor should you copy any other files onto the dedicated USB drive. Doing so may cause serious damage to the system.

The following tools are required to perform this procedure:

- RJ45 to serial cable
- USB to Serial adapter cable
- Dedicated USB thumbdrive

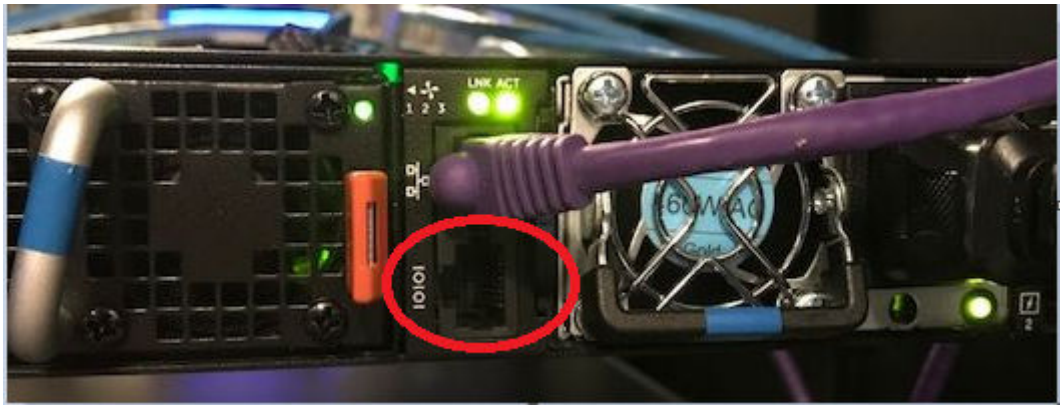
Procedure

1. Locate the USB port on the front of the switch, right side immediately below the stacking ID indicator is the USB Type-A connector.

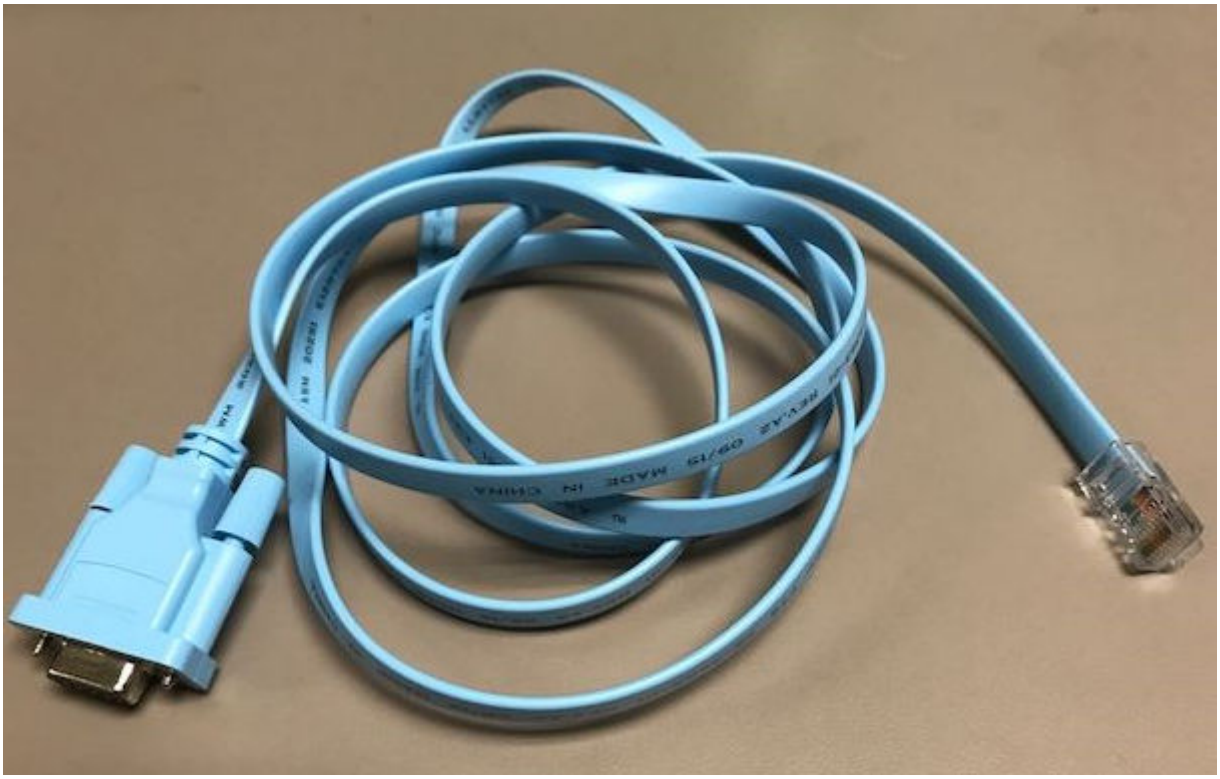


2. Insert the USB thumb drive into the USB port.

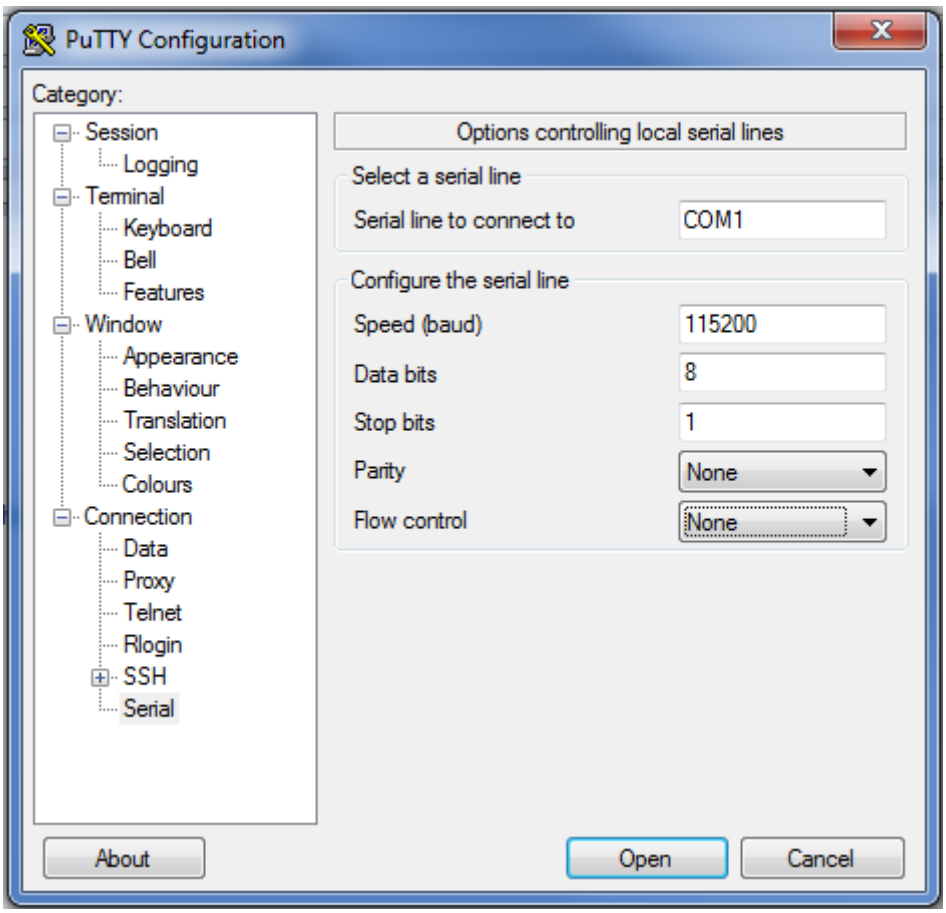
3. Connect the RJ45 end of the RJ45 to serial adapter cable to the switch console port.



4. Connect the serial end of the USB to serial adapter to the serial end of the RJ45 to serial adapter.



5. Connect the USB end of the USB to serial adapter to the laptop.



6. Start the Putty application, from the Category navigation tree, select Serial, and then configure the following options:
   a. Speed (baud): 115200
   b. Data bits: 8
   c. Stop bits: 1
   d. Parity: none
   e. Flow control: none
7. Start the EXEC function by typing
   `enable`
   .
   The password prompt appears.
8. Enter the password:
   `username admin password XXXXXXXXXXXX`
   (the default
   The screen displays a message similar to the following:

```
The SupportAssist EULA acceptance option has not been
selected. SupportAssist
 can be enabled once the SupportAssist EULA has been
accepted. Use the:
 'support-assist activate' command to accept EULA and enable
SupportAssist.

DPappliance-switch#
```

9. From the switch CLI prompt, copy the switch configuration file by entering the following command:

```
copy usbflash://< copy usbflash://<dell_sw_start_config>
startup-config >
```

   The screen displays the following:

```
Please do not remove usbflash, until the operation completes!!
File with same name already exist.
Proceed to copy the file [confirm yes/no]:
```

10. Type "yes" to confirm that you want to copy the file.
    The system copies the switch configuration from the USB drive to the switch.
11. When the system finishes copying the file, a message similar to the following is displayed.

```
12067 bytes successfully copied
```

12. The switch must be re-loaded for the new configuration to take effect. Re-load the switch by typing the command:
    `reload`
    The screen displays the following:

```
System configuration has been modified. Save? [yes/no]:
```

13. Type
    `no`

    The screen displays the following:

```
Proceed with reload [confirm yes/no]:
```

14. Type
    `yes`

    The system re-loads the switch and the switch now runs with the saved configuration file. The screen displays an output similar to the following:

```
Mar 12 23:08:23: %STKUNIT1-M:CP %CHMGR-5-RELOAD: User request
to reload the
chas
                                                    sis

syncing disks... done
unmounting file systems...
unmounting /f10/usbflash (/dev/sd0e)...
unmounting /f10/phonehome (tmpfs)...
unmounting /f10/flash (/dev/wd0e)...
unmounting /f10/ConfD/db (mfs:491)...
unmounting /usr/pkg (/dev/wd0i)...
unmounting /boot (/dev/wd0b)...
unmounting /usr (mfs:29)...
unmounting /force10 (mfs:24)...
unmounting /lib (mfs:21)...
unmounting /f10 (mfs:18)...
unmounting /tmp (mfs:9)...
unmounting /kern (kernfs)...
unmounting / (/dev/md0a)... done
rebooting...
```

15. Disconnect the thumbdrive and cables from the switch.
16. Connect Uplink port(s) to customer switch.
17. Connect Management port to customer management switch.
18. Verify the configuration file was copied successfully by validating the port-channel is up and has active members as follows:
    a. Start the EXEC privilege mode by typing the following command:
       `enable`
    b. At the Password prompt, type the password for the admin account.
    c. At the prompt, type: show interfaces port-channel.

       The port channel will be in the switch config file name ex.: Mot_PO3_RSTP. The following is an example:

```
DPappliance-switch#show interfaces port-channel 3
Port-channel 3 is up, line protocol is up
Created by LACP protocol
Description: 10GbeTwinax port channel used for customer
uplink
Hardware address is f4:8e:38:6f:1e:fe, Current address is
f4:8e:38:6f:1e:fe
Interface index is 1258292736
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f48e386f1efe
```

```
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 40000 Mbit
Members in this channel:  Te 1/13(U) Te 1/14(U)
```

The two highlighted information indicates the port channel is up and its members are up.

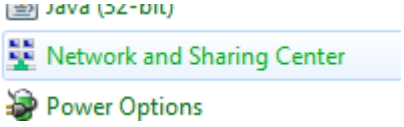
19. Contact the SA if the Line Protocol shows down and there are no active members. For example:

```
DPappliance-switch#show interfaces port-channel 3
Port channel 3 is up, line protocol is down (minimum links
not up)
Created by LACP protocol....
```

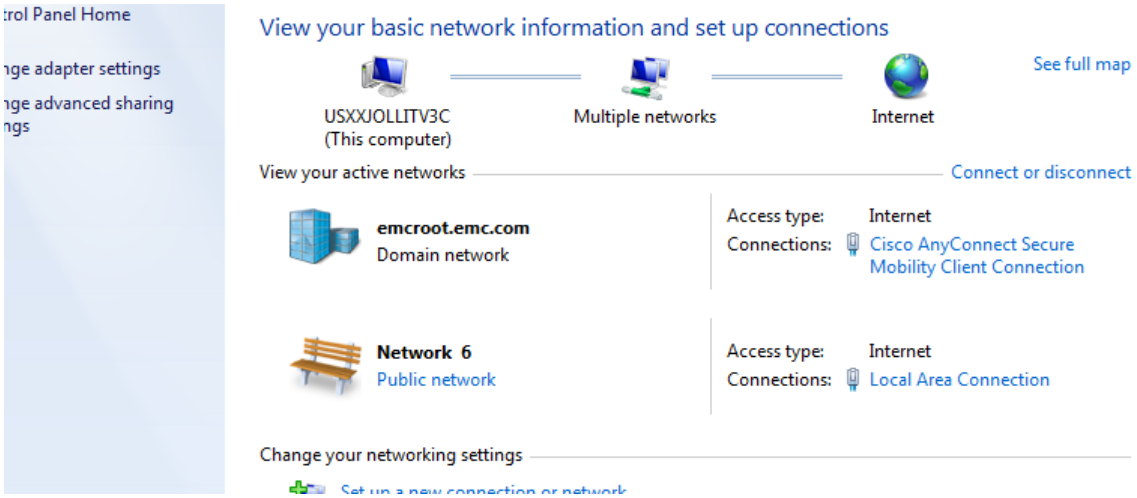
20. Create the management interface on the laptop as follows:

    a. Connect the RJ45 and Cat6 network cable from port 38 of the Dell switch to the laptop.

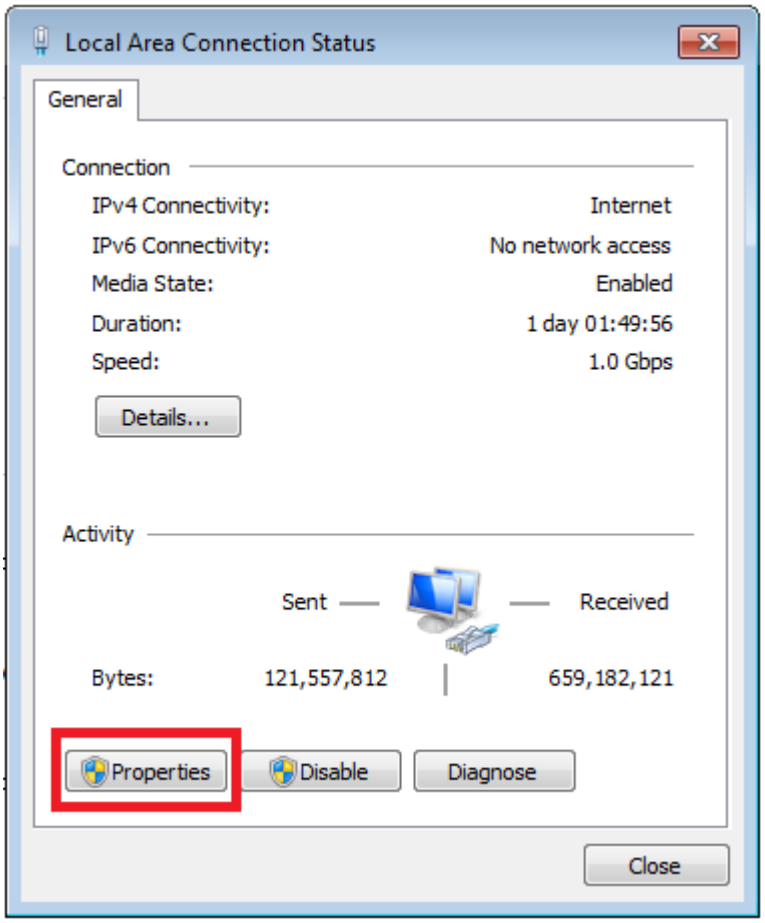
    b. On the laptop browse to Control Panel -> Network and Sharing Center.



    c. Open the Network Sharing Center and in the View your active networks section and open the Local Area Connection.



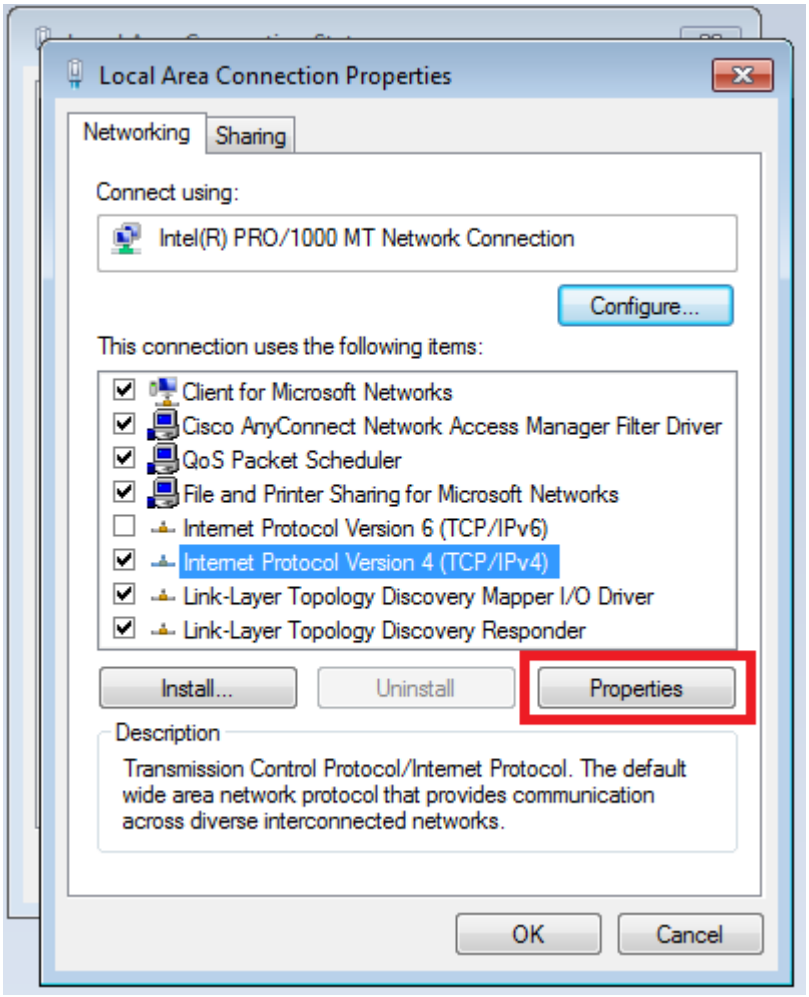
    d. Select Properties



e. Select Internet Protocol Version 4 (TCP/IPv4) and then click Properties.

f. On the General tab select Use the following IP address and then enter:

- IP Address: 192.168.100.98
- Subnet mask: 255.255.255.254
- Gateway: 192.168.100.100



g. Click OK to close the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.

h. Click OK to close the Local Area Connection Properties dialog box.

21. Create a putty session to the Data Domain at 192.168.100.109.

22. Configure the management interface by typing the following command (VLAN number will be in PEQ):

```
net create interface ethMa vlan vlan_number
```

Example: net create interface ethMa.123

23. Configure the management interface by typing the following command:

```
net config ethMa.vlan_number ip_address netmask mask
```

Example: net config ethMa.123 172.158.12.24 netmask 255.255.255.0

24. Configure the default gateway for the management interface by typing the following command gateway will be in PEQ:

```
net route set gateway gateway_ip_address
```

Example: net route set gateway 172.158.12.1.

25. Ping Default Gateway by typing the following command:

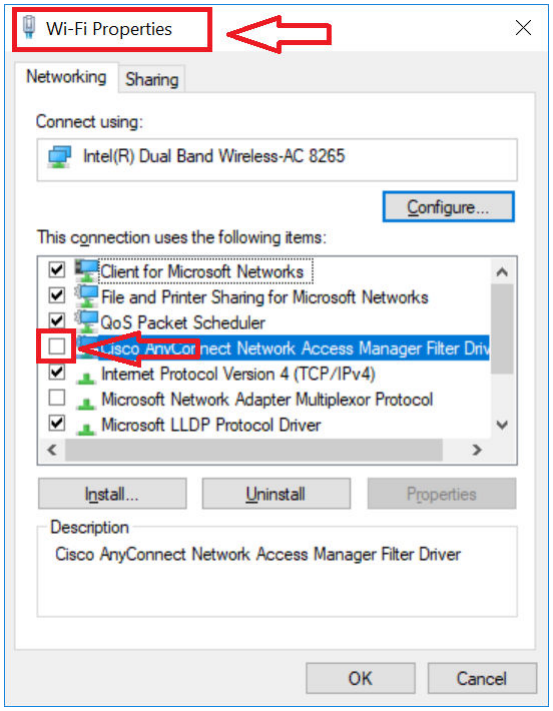
```
net ping gateway_ip
```

Example: net ping 172.158.12.1

If successful, continue by providing a WebEx for remote SA/IS. Contact SA if ping fails to respond.

Note

In order to be on the 192.168.100.x and a hotspot/WiFi network, disable the Cisco VPN Client on the Ethernet Adapter. At this point you should be able to connect to the Internal IPs of the equipment, and be on the wifi as well to accept the WebEx meeting invite.



Note

The SA/IS should send the WebEx invite to the customer as well as the CE. The CEs work is completed once the SA has established an external connection to the ACM VM and it is reachable on the customer external network. At that point the CE can leave the site, and the SA/IS will continue the WebEx with the Customer.

Management ports

Besides the 10 GbE and 40 GbE switch ports, the S4048–ON system provides several ports for management and storage.

RS-232 console port access

The RS-232 console port is on the PSU-side of the S4048-ON chassis, as shown.

Figure 27 S4048–ON RS–232 console ports

1. Ethernet management port
2. RS-232 console port

Note

Before starting this procedure, be sure that your PC has a 9-pin serial port and that you have a terminal emulation program installed and running on the PC. If the serial port cannot accept a female DB-9 connector, obtain a DB-9 male-to-male adaptor.

Procedure

1. Install the provided RJ-45 connector side of the provided cable into the S4048-ON console port.
2. Install the DB-9 female side of the provided copper cable into the serial port or into other data terminal equipment (DTE) server hardware that you intend to use.
3. Keep the default terminal settings on the console as follows:
   - 115200 baud rate—set the MicroUSB console port to 9600 baud rate
   - No parity
   - 8 data bits
   - 1 stop bit
   - No flow control

Enable Data Domain network ports

Before you begin

The SSH session with the Data Domain system should still be active. Log in again if the session has been terminated.

Complete the following steps to enable the Data Domain network ports after replacing the switch chassis.

Procedure

1. Enable the all the network ports on the I/O module that was disabled before.

Run the following commands:

```
netconfig eth1a up
netconfig eth1b up
netconfig eth1c up
netconfig eth1d up
```

2. Proceed to Powering on the appliance to restart the data protection service and appliance.

Update the Install Base

After replacing a Dell server or switch chassis, complete the following steps to update the Install Base with the serial number of the new hardware.

Procedure

1. In an internet browser, navigate to the Business Services Portal at http://emc.force.com/BusinessServices.
2. Under **Post Sales**, select **Install Base Group**.
3. In the **Case Subtype** list box, select **IB Status Change**, and click **Select**.
4. Specify your own contact name, email address, phone number, and theater.

   Note

   Add the email addresses of anyone else who needs to be notified of the Install Base change.

5. In the **Case Details** section, specify case details in the **Subject** and **Description** fields.

   Select the **Federal Case** checkbox if the support activity is at a federal site.

6. Select the Product Families that apply to the support activity.

   Family is defined as the TLA/Model product family for your request. If you have multiple product families in your request and one of them is listed here, choose that family, otherwise choose **All Other Families**.

7. Fill out the additional fields that are relevant to the support activity.

   Note

   For more than one Serial number, enter each value separated with a comma. If there is a large number of values, a Microsoft Excel spreadsheet can be attached. See help text. The Serial number used here is the Avamar UID obtained from "System ID" field of "mccli server show-prop" (Remove the colons and the '@'.)

8. In the **Remote Connection** field, specify the DialHome details.
9. Use the **Upload Documents** section to attach any relevant supporting documentation to the service request.
10. Click **Submit** to complete the service request.

    You will receive automated e-mail notifications to stay up-to-date on the progress of your request.

CHAPTER 6

Restart the IDPA

This chapter includes the following topics:

Start up the IDPA

Powering on the IDPA requires starting individual components in the correct order.

Procedure

1. Power on Data Domain system.
2. Power on the NDMP accelerator or accelerators if they are included in the configuration.

   Note

   Do not continue until both Data Domain and all NDMP accelerators are fully initialized.

3. For configurations with a physical Avamar implementation, power on the utility node and storage nodes.

   This step is not necessary for configurations with AVE.

   Note

   Do not continue until Avamar is fully initialized.

4. Power on each of the ESXi servers, moving from the bottom server to the top.

Results

The rest of the process finishes automatically. Once the ESXi servers are powered on, IDPA automatically starts vCenter, ACM, all DPSearch nodes, the DP Advisor nodes, DP Central, AVE, and Avamar Proxy.
For issues during startup, refer to Troubleshooting startup on page 100.

Troubleshooting startup

If one part of the startup process fails to complete automatically, the problem can be resolved manually to allow startup to continue.

Avamar does not start
If Avamar does not complete startup, connect to the Avamar server. If Avamar reports that GSAN did not shut down cleanly, select the option to roll back to the last checkpoint.

The ACM does not start
If the ACM service does not start within 2 hours and 15 minutes of powering on the appliance, one or more of the following components are not powered on or are not accessible on the network:

- Data Domain
- AVE

The Data Domain component must be powered on and accessible before the ESXi host is powered on.

1. Verify that the components that are required for the configuration are powered on.

2. Verify that the required components are accessible on the network. Resolve any connectivity issues that are encountered.
   - If the ACM loads successfully, skip the rest of this procedure. The DPSearch nodes, DP Advisor nodes, DP Central, AVE, and Avamar Proxy start automatically.
   - If all required components are powered on and accessible, but the ACM does not load, restart the ACM service:
3. Stop the `dataprotection_webapp` service:
   `service dataprotection_webapp stop`
4. Start the `dataprotection_webapp` service:
   `service dataprotection_webapp start`

The DPSearch nodes, DP Advisor nodes, DP Central, AVE, and Avamar Proxy start automatically.

The VMs do not start

When switch the power button on present on the Dell Server, the ACM internally executes `local.sh (/etc/init.d/local.sh)` and the VMs start automatically. To start the VMs manually:

1. Move ESXi out of maintenance mode manually.

   Note

   To do this, log in to ESX using **`idpauser`** and select **Exit maintenance mode**.

2. Start the DataProtection-VCSA by running the `/etc/init.d/local.sh` script on ESXi or power on the VM from the ESXi.
   DataProtection-ACM VM starts five minutes after the VCSA VM starts.
3. If DDVE VM is not up, click the **Power on** button to start the DDVE VM.
   Code waits filesystem status to show up and running.
4. If AVE is not started, start AVE VM from ESX UI.
5. login to AVE using admin credentials.
   ACM executes `dpnctl status all`, `dpnctl start all`, and `dpnctl start maint` commands.
6. If something goes wrong, execute the following in sequence and click the **Power on** button:
   - DataProtectionSearch Vapp
   - DPADatastoreServer VM
   - DPAApplicationServer VM
   - DataDomainCloudDR VApp
   - DataProtectionCentral VApp
   - AVProxy VM

   Note

   Check the status of DPA services by running `/opt/emc/dpa/services/bin/dpa.sh service status` command after logging in to Datastore server using its IP, OS user **`root`** and its password.

7. If DPS vApp does not started, start vApp.

8. Start the services of search by logging in to index master IP using OS root credentials and executing following commands:
   a. `service elasticsearch start`
   b. `service search-cis-core start`
   c. `service search-cis-schedule start`
   d. `service search-networker-worker start`
   e. `service search-networker-action start`
   f. `service search-avamar-worker start`
   g. `service search-avamar-action start`
   h. `service search-worker start`
   i. `service search-adminapi start`
   j. `service search-api start`
9. Login to VCSA using **`idpauser`**credentials, select **AVProxy** VM and click the **Power on** button.
10. After IDPA starts, start two services of Avamar using `dpnctl start emt`.