# Upgrade Checker Tool

*Master Document*

# Table of Contents

## Contents

# Document Control

| **Document Title** | | | Upgrade Checker Tool Master Document |
|---|---|---|---|
| **STATUS** | | **REVISION** | **2.8** |

| Version | Description | Date |
|---|---|---|
| v1 | Initial release.<br><br>Supports 6.0.1 Patch 4 – 6.0.1 Patch 6 for GenU option.<br><br>The following checks were implemented:<br><br>✓ WAN COM Event History<br>✓ FE & BE Event History<br>✓ portLayout File Permissions Issue on VS2<br>✓ Non-Standard Port WWN Format on VS2<br>✓ Warning for VPN Connectivity Issue After GenU IP Swap<br>✓ VPlexPlatformHealthCheck on VS6<br>✓ portRoles File With All Ports OFF on VS6<br>✓ GeoSynchrony Version Warning | 12/22/2017 |
| v1.1 | Added support for 6.0.1 Patch 7 for GenU option. | 2/16/2018 |
| v2.1 | Added support for 6.1 for GenU option.<br><br>Integrated the Firmware Log Analysis Tool (FLAT) for analyzing firmware events (replacing WAN COM & FE/BE Event History checks).<br><br>The following new checks were implemented:<br><br>✓ Check CST Lockbox<br>✓ Check Enabled Ports' RX/TX Power<br>✓ Check VPN status<br>✓ Check certificate status<br>✓ Check for Disabled VS6 WAN Ports<br>✓ Check for 'Up' VS6 WAN Ports<br>✓ Check for IPv6 on the WAN COM ports<br>✓ Check for IPv6 on the management-server eth3 port<br>✓ VS6 SLIC-4 Check | 8/31/2018 |
| V2.2 | Added support for 6.1 Patch 1 for GenU option. | 1/18/2019 |

| | | |
|---|---|---|
| | The following new checks were implemented:<br><br>• Check for 'down' VS2 FE Ports | |
| V2.3 | Added support for 6.1 Patch 2 for GenU option. | 3/18/2019 |
| V2.4 | Added support for 6.2 GA. | 1/22/2020 |
| V2.5 | Added support for:<br>6.2 Patch 2<br>6.2 Patch 3 | 5/22/2020 |
| V2.6 | The following new check was implemented for the NDU option:<br>• Check for Memory Fragmentation | 7/2/2020 |
| V2.7 | Fixed a Defect involving the failed import of the VPlexUpgradeCheckerCli script on a busy management-server, which caused the UCT to hang indefinitely. | 7/29/2020 |
| V2.8 | Added support for 6.2 Patch 4<br>NDU option of the tool was enhanced. | 2/5/2021 |

# GenU Checks

# Overview

The tool will perform the GenU pre-checks listed below depending on the hardware platform (VS2 or VS6), and as long as the VPLEX cluster is running a GeoSynchrony release supported by the tool (refer to the Release Notes for supported versions).

If the tool detects that any of the below issues are present they will be reported in the 'Issues Summary Report', which is printed on the console, and at the end of the log file produced by the tool (file named C*x*_<*last4TLA*>.log – where x = cluster-1/cluster-2 and last4TLA = the last 4 digits of the VPLEX TLA).

## Tool Exits due to Unreachable Directors

If there are unreachable directors detected in VPlexcli, the VPlexcli 'version –a' command will display the 'Product version' as 'mixed' (or potentially 'Version mismatch' if the SMS is running a different version from the reachable directors), and one or more directors will be listed with a version of 'n/a'.

This can occur if a director has gone down, or has some physical connectivity issue, or if the VPN between two clusters in a Metro is down. The tool will report this condition and automatically exit if the genu option is specified, as it can't continue with the unreachable directors connected in VPlexcli.

If the issue causing the unreachable directors can't be resolved before the tool needs to be run then the unreachable directors must be disconnected from VPlexcli in order for the tool to proceed. To do this use the 'disconnect' command in VPlexcli and specify the unreachable directors (see example below).

However, if this is done the disconnected/unreachable directors will not be analyzed and reported on. In the case where VPN is down between two VS2 clusters in a Metro be sure to run the tool separately on each management-server to ensure that all directors are analyzed.

In the following example the VPN is down between two clusters in a VS2 Metro:

```
VPlexcli:/> version -a
What                                          Version      Info
--------------------------------------------  -----------  ------------------------------------------------
Product Version                                    mixed       the connected directors have different versions
SMSv2                                          D50.40.2.0.0  -
Mgmt Server Base                                    D50.40.2.1    -
Mgmt Server Software                                D50.40.2.4    -
/engines/engine-1-1/directors/director-1-1-A  7.5.129.4.0   -
/engines/engine-1-2/directors/director-1-2-B  7.5.129.4.0   -
/engines/engine-2-1/directors/director-2-1-A  n/a         Unable to retrieve version information
/engines/engine-2-2/directors/director-2-2-A  n/a         Unable to retrieve version information
/engines/engine-1-1/directors/director-1-1-B  7.5.129.4.0   -
/engines/engine-2-2/directors/director-2-2-B  n/a         Unable to retrieve version information
/engines/engine-1-2/directors/director-1-2-A  7.5.129.4.0   -
/engines/engine-2-1/directors/director-2-1-B  n/a         Unable to retrieve version information

VPlexcli:/> disconnect -n director-2-1-A, director-2-1-B, director-2-2-A, director-2-2-B
Disconnected from remote systems director-2-1-A, director-2-1-B, director-2-2-A, director-2-2-B.

VPlexcli:/> version -a
What                                          Version       Info
--------------------------------------------  --------------  ----
Product Version                                    6.0.1.07.00.04  -
SMSv2                                          D50.40.2.0.0    -
Mgmt Server Base                                    D50.40.2.1     -
Mgmt Server Software                                D50.40.2.4     -
/engines/engine-1-1/directors/director-1-1-A  7.5.129.4.0    -
/engines/engine-1-2/directors/director-1-2-B  7.5.129.4.0    -
/engines/engine-1-1/directors/director-1-1-B  7.5.129.4.0    -
/engines/engine-1-2/directors/director-1-2-A  7.5.129.4.0    -
```

# VS2 GenU Checks

## VS2 portLayout File Permissions Check

Susceptible Versions: 6.0.1 Patch 4 and earlier

Fixed Version(s): 6.0.1 Patch 5

VPLEX CQ/Jira #: CQ 44372

VPLEX Hardware Checked: VS2

**Issue:**

During GenU from VS2 to VS6, if the 'portLayout' file exists on the VS2, then Upgrade Manager can fail with an error like the following:
"Unable to determine director-1-1-A WWN compatibility: {u'code': -32603, u'data': u"[Errno 13] Permission denied: '/var/opt/zephyr/flashDir/portLayout'", u'message': u'Internal error'}" while checking for VS1 style WWNs."

The reason for this failure is that due to a bug the 'portLayout' file does not have read permission for the 'service' account user.

This issue is fixed in 6.0.1 P5 and above releases by providing read permission for all the groups, including the 'service' account user belonging to a root group.

**Workaround/Next Steps:**

Upgrade to 6.0.1 Patch 5 or higher prior to the GenU to avoid this issue.

Otherwise, if the GenU must be performed at 6.0.1 Patch 4 or lower a Customer Engineer (CE) must implement the following workaround prior to the GenU:

Log into the VPlex management-server. Execute the following steps from the Linux prompt of the management-server:

For each of the directors called out as needing the permissions fixed:

1. SSH to the director
    a. eg. to SSH to director-1-1-A: ssh root@128.221.252.35
2. Execute the following command to fix the permissions:
   chmod a+r /var/opt/zephyr/flashDir/portLayout

## Check for Non-Standard WWNs on a VS2

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS2

**Issue:**

A generational upgrade of VS2 to VS6 is not supported on VPLEX clusters that have non-standard configurations, such as:

- Clusters that have a non-EMC World Wide Name (WWN) seed.
- VS2 clusters that were upgraded from VS1.

If this issue is reported it typically means that the director(s) have non-standard port WWNs, which need to be addressed prior to the GenU.

**Workaround/Next Steps:**

If this issue is reported a Customer Engineer (CE) should follow KBA 487310, and engage a VPLEX Field Support Specialist (FSS) if needed, to convert the non-standard WWPNs to standard WWPNs prior to the GenU.

NOTE: Non-standard port WWNs can be reported on a VS2 Local system with standard port WWNs if WAN COM SLICs had previously been installed and subsequently removed. If standard port WWNs are found on the system then reference KBA 524514 “VPLEX: Nonstandard port WWNs flagged on VPLEX Local with standard port WWNs”.

## Warning for VPN Connectivity Issue After GenU IP Swap

Susceptible Versions: All

Fixed Version(s): TBD

VPLEX CQ/Jira #: CQ 44825

VPLEX Hardware Checked: VS2

**Issue:**

The GenU script delegates to the 'management-server set-ip -i <ip/netmask> -g gateway -p eth3' command to change the VS2 and VS6 public IPs. That command takes the input IP/netmask and gateway and calculates a set of new routes to add. However, it also reads and preserves the current set of routes in /etc/sysconfig/network/ifroute-eth3 (skipping over the default route).

This causes issues in the case of GenU IP swap when the VS2 and VS6 are on different subnets, as the old routing can interfere with network traffic between the cluster management servers when the remote management server is on the same subnet as the original VS2.

**Workaround/Next Steps:**

Professional Services should discuss this potential issue with the customer prior to the GenU to determine the best course of action to take. If the VS2 & VS6 are on different subnets it's recommended to skip the automated IP swap option to prevent this issue.

Following the completion of the GenU the SolVe Desktop procedure "Change IP addresses-VPLEX Metro (VS6)" can be used to manually swap the IP addresses after ensuring the VS2 system(s) is no longer on the network. Also, prior to the GenU the /etc/sysconfig/network/ifroute-eth3 file on the VS2 can be checked for any old routes that could potentially cause a conflict.

## Check CST Lockbox

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS2

**Issue:**

If there are problems with the CST Lockbox it will cause a GenU to fail during the preparation phase. The following three issues are checked for:

1. CST lockbox service is not running
2. CST lockbox permissions are incorrect
3. CST VPLEX-PAM-Authority is invalid

**Workaround/Next Steps:**

If any of these issues are reported a Customer Engineer (CE) should follow KBA 457268 to correct the CST lockbox on the management server. The CE should engage a Field Support Specialist (FSS) or VPLEX Remote Support if assistance is needed.

**NOTE:** CST lockbox corruption can be verified by attempting to log into the GUI. If the CST lockbox is corrupted the login to the GUI will fail.

**NOTE:** If CST file permission/ownership issues are reported along with invalid VPLEX-PAM-Authority then the CST file permission/ownership issues should be resolved first by following the instructions in the 'CST lockbox permissions are incorrect' section above, before following the KBA.

## Check Enabled Ports' RX/TX Power

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS2

**Issue:**

This check is performed to verify if any of the enabled VPLEX ports have low RX or TX power levels (defined as <=200uW). Low RX or TX power issues could result in connectivity issues that could potentially impact the GenU procedure, so if these issues are reported they should be investigated and resolved prior to the GenU.

**Workaround/Next Steps:**

If this issue is reported a Customer Engineer (CE) should reference KBA 336564 for steps to troubleshoot this issue.

## Check certificate status

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS2

**Issue:**

If the security certificates expire just prior to the GenU it could result in delays to the procedure. This check verifies the expiration date of all security certificates on the VS2. If any are set to expire within 30 days a warning is reported, or if any have already expired an error is reported.

**Workaround/Next Steps:**

If this issue is reported the Customer Engineer (CE) should work with the customer to renew the security certificates prior to the GenU. The procedure 'Renew Security Certificates' in VPLEX SolVe Desktop should be followed to perform the renewal.

## Check VPN status

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS2

**Issue:**

If VPN is down between the clusters of a VS2 Metro it can delay or impact the GenU procedure. This VPN status check is performed on VS2 Metro clusters in order to warn if the VPN is down, so that it can be brought up prior to the GenU.

**Workaround/Next Steps:**

If this issue is reported the Customer Engineer (CE) should work with the customer by following KBA 448400 'VPLEX: After an IP network outage VPN is down' to troubleshoot the VPN connectivity issue.

**NOTE:** If the above 'Check certificate status' check is also reported for an expired VPN certificate, then the expired VPN certificate is likely the root cause for why the VPN is down. The certificate should be renewed, and then the customer or Customer Engineer (CE) can re-check the VPN status by logging into VPlexcli and executing the 'vpn status' command.

## Check for IPv6 on the management-server eth3 port

Susceptible Versions: 6.0.1 Patch 4 – 6.0.1 Patch 7

Fixed Version(s): 6.1

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS2

**Issue:**

GeoSynchrony 6.0.x releases have not been qualified for generational hardware upgrade (GenU) if IPv6 is used for management-connectivity (on any Local/Metro). This check analyzes if IPv6 is in use on the eth3 port of the management-server, and prints a warning if detected.

**Workaround/Next Steps:**

If this issue is reported it's recommended to upgrade the VPLEX clusters to GeoSynchrony 6.1, where GenU with IPv6 in use has been qualified, and is supported.

## Check for IPv6 on the WAN COM ports

Susceptible Versions: 6.0.1 Patch 4 – 6.0.1 Patch 7

Fixed Version(s): 6.1

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS2

**Issue:**

GeoSynchrony 6.0.x releases have not been qualified for generational hardware upgrade (GenU) if IPv6 is used for WAN COM connectivity (on Metro-IP). This check analyzes if IPv6 is in use on the WAN COM ports, and prints a warning if detected.

**Workaround/Next Steps:**

If this issue is reported it's recommended to upgrade the VPLEX clusters to GeoSynchrony 6.1, where GenU with IPv6 in use has been qualified, and is supported.

## Check for 'down' VS2 FE Ports

Susceptible Versions: 6.0.1 Patch 4 – 6.1 Patch 1

Fixed Version(s): N/A

VPLEX CQ/Jira #: VPLEX-8873

VPLEX Hardware Checked: VS2

**Issue:**

During the GenU, the state/settings of the VS2 (including that of the FE ports) is transferred to the VS6, and then during the I/O Transfer Phase, when the VS6 director is being brought up, the FE ports are enabled. If one or more VS2 FE ports are in a 'down' state (disabled) prior to the GenU, and especially if those ports can't be enabled in the VPlexcli, it can lead to the I/O Transfer Phase failing, as the step of enabling the FE ports on the VS6 director will silently fail, and then a subsequent step waiting for all FE ports to have the 'enabled' state (on the VS6 director) will fail due to a timeout error.

This check checks the state of all FE ports in both VPlexcli, and sxport. It will report any FE ports found that are in 'down' state in VPlexcli, and/or any with a disabled sxport state.

**Workaround/Next Steps:**

If FE (front-end) ports are reported as 'down' in VPlexcli a CE should:

1. Log into VPlexcli
2. Check the FE port status by using the following command, and check if the FE port(s) are still down (disabled):

   **VPlexcli:/> ll /engines/*/directors/*/hardware/ports**

   In the following example (skipping the output from 1-1-A & 1-2-B):
   - director-1-1-B B0-FC02 is 'down' (disabled)
   - on director-1-2-A all FE ports are enabled
     - FC00 & FC01 ports are 'up' (enabled and have connectivity)
     - FC02 & FC03 ports are in 'no-link' (enabled but no connectivity) state

```
/engines/engine-1-1/directors/director-1-1-B/hardware/ports:
Name    Address          Role      Port Status
------- ---------------- --------- -----------
B-CMI00 2                -         down
B0-FC00 0x50001442902a0a00 front-end  up
B0-FC01 0x50001442902a0a01 front-end  up
B0-FC02 0x0000000000000000 front-end  down
B0-FC03 0x50001442902a0a03 front-end  no-link
B1-FC00 0x50001442902a0a10 back-end   up
B1-FC01 0x50001442902a0a11 back-end   up
B1-FC02 0x50001442902a0a12 back-end   no-link
B1-FC03 0x50001442902a0a13 back-end   no-link
B2-FC00 0x50001442902a0a20 wan-com    up
B2-FC01 0x50001442902a0a21 wan-com    up
B2-FC02 0x50001442902a0a22 wan-com    no-link
B2-FC03 0x50001442902a0a23 wan-com    no-link
B3-FC00 0x50001442902a0a30 local-com  up
B3-FC01 0x50001442902a0a31 local-com  up
B3-FC02 0x0000000000000000 -          down
B3-FC03 0x0000000000000000 -          down

/engines/engine-1-2/directors/director-1-2-A/hardware/ports:
Name    Address          Role      Port Status
------- ---------------- --------- -----------
A-CMI00 1                -         down
```

**A0-FC00 0x5000144260750100 front-end up**
**A0-FC01 0x5000144260750101 front-end up**
**A0-FC02 0x5000144260750102 front-end no-link**
**A0-FC03 0x5000144260750103 front-end no-link**
A1-FC00 0x5000144260750110 back-end up
A1-FC01 0x5000144260750111 back-end up
A1-FC02 0x5000144260750112 back-end no-link
A1-FC03 0x5000144260750113 back-end no-link
A2-FC00 0x5000144260750120 wan-com up
A2-FC01 0x5000144260750121 wan-com up
A2-FC02 0x5000144260750122 wan-com no-link
A2-FC03 0x5000144260750123 wan-com no-link
A3-FC00 0x5000144260750130 local-com up
A3-FC01 0x5000144260750131 local-com up
A3-FC02 0x0000000000000000 - down
A3-FC03 0x0000000000000000 - down

3. If any FE ports are down, attempt to enable them by using the VPlexcli command 'set enabled true'.

   First, cd into the context of the FE port in question, example:
   **VPlexcli:/> cd /engines/engine-1-1/directors/director-1-1-B/hardware/ports/B0-FC02**

   Then issue the 'set enabled true' command, example:

   **VPlexcli:/engines/engine-1-1/directors/director-1-1-B/hardware/ports/B0-FC02> set enabled true**

   Issue command 'cd ..' to change to the 'ports' context of the director, and then run a long listing 'll' command to check the state of the port again:

   **VPlexcli:/engines/engine-1-1/directors/director-1-1-B/hardware/ports/B0-FC02> cd ..**
   **VPlexcli:/engines/engine-1-1/directors/director-1-1-B/hardware/ports> ll**
   Name Address Role Port Status
   ------- ------------------ --------- -----------
   B-CMI00 2 - down
   B0-FC00 0x50001442902a0a00 front-end up
   B0-FC01 0x50001442902a0a01 front-end up
   **B0-FC02 0x0000000000000000 front-end down**
   B0-FC03 0x50001442902a0a03 front-end no-link

4. If the FE port now shows in 'up' or 'no-link' state then the enable was successful. However, if it remains in 'down' (disabled) state (like in the example above) it indicates the port is disabled in sxport, and therefore can't be enabled in VPlexcli. The CS Recovery Team in VPLEX Remote Support will need to execute internal commands to correct this. Engage the VPLEX Remote Support team and reference KBA 529368.

If the tool reports that FE ports are disabled in sxport, and it's unclear whether the ports identified are the same as those reported in 'down' state in VPlexcli, the following command can be used to check the UUID of the directors in order to map which director the ports belong to:

**VPlexcli:/> connectivity director –n <director-x-x-x>**

Example output produced by the UCT in the Issues Summary Report:

The following ports were found to have a disabled sxport state:

TPort: P00000000**47202A0A-A0-FC02**.0

Running the 'connectivity director –n director-1-1-A' command shows that the above noted FE port (A0-FC02) belongs to director-1-1-A, as it has UUID 47202a0a:

VPlexcli:/> connectivity director -n director-1-1-A

Directors discovered by director-1-1-A, **UUID** 0x00000000**47202a0a**:

# VS6 GenU Checks

## VPlexPlatformHealthCheck Analysis

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS6

**Issue:**

When run on a VS6, the tool prints the output of the 'VPlexPlatformHealthCheck –v' command to the log file (named C*x*_<*last4TLA*>.log). If errors are detected in the output of the command this will be noted in the Issues Summary Report (which is printed to the console and the end of the log file).

**Workaround/Next Steps:**

A Customer Engineer (CE) should review the output of the command (it's printed to the log file named C*x*_<*last4TLA*>.log) to see the errors reported. The command can also be run again manually on the management-server (Linux prompt) to verify if the errors persist. The CE should work with the customer (and engage a Field Support Specialist as needed) to resolve the errors prior to the GenU.

**NOTE:** Errors regarding the A4/B4 I/O Module should be ignored since these are only present during the duration of the generational upgrade (due to the extra COM SLIC having been installed on the VS6 directors).

**NOTE:** If the VPlexPlatformHealthCheck reports that the ECOM process is not running on one or more VS6 directors then the CE or Professional Services should follow KBA 519163 to work around this issue. Warning: not following the recommended steps can potentially lead to continuous firmware crashes on the VS6 directors.

## Check VS6 for portRoles with all ports set to off

Susceptible Versions: 6.0.1 Patch 4 – 6.0.1 Patch 7

Fixed Version(s): 6.1

VPLEX CQ/Jira #: CQ 44829

VPLEX Hardware Checked: VS6

**Issue:**

If the VS6 directors are initially powered on with a firmware version older than 6.0.1 P1, the 'portRoles' file will be generated with all ports = "off". If left in this state it will cause the GenU to fail during the IO transfer phase.

**Workaround/Next Steps:**

If this issue is reported Professional Services should implement the workaround documented in KBA 515617 "VPLEX: Un-configured VS6 portRoles file has all roles 'off'".

## Check for Disabled VS6 WAN Ports

Susceptible Versions: 6.0.1 Patch 5 – 6.0.1 Patch 7

Fixed Version(s): 6.1

VPLEX CQ/Jira #: VPLEX-2682

VPLEX Hardware Checked: VS6

**Issue:**

In GeoSynchrony 6.0.1 Patch 5 the step to automatically enable the VS6 WAN COM ports was removed from the 'genu-setup' command. After running the 'genu-setup' command, if none of the VS6 ports (FE/BE/Local/WAN) are enabled this can subsequently lead to a failure when the 'hardware-upgrade prepare-vs6 --apply-settings' command is executed. The error returned is "Expected argument after -c, but got -a."

Example:

VPlexcli:/> hardware-upgrade prepare-vs6 --apply-settings
Applying settings from GenU-VS2-Settings-backup-2018-03-20_18-24-23.tar.gz
Applying VS2 cluster settings on VS6: ....DONE
Configuring cache on VS6: .DONE
Stopping VPN: .DONE
Disabling ports: .ERROR
Expected argument after -c, but got -a.
hardware-upgrade prepare-vs6: Evaluation of <<hardware-upgrade prepare-vs6 --apply-settings>> failed.
cause: Command execution failed.
cause: **Expected argument after -c, but got -a.**

This issue occurs due to a bug, where if all ports are already disabled the wait command (an internally run command to wait for the return status from the port disabling command) isn't passed a value for the '-c' option, which results in the failure.

**Workaround/Next Steps:**

The recommended workaround is to manually enable the WAN COM ports on the VS6 to ensure that some of the ports are enabled during the –apply-settings phase in order to avoid this failure.

A Customer Engineer (CE) or Professional Services can manually enable the WAN COM ports on the VS6 directors by logging into VPlexcli and using the following command:

VPlexcli:/> set engines/*/directors/*/hardware/ports/[A|B]2*::enabled true

Verify the WAN COM ports are enabled using command:

VPlexcli:/> ll engines/*/directors/*/hardware/ports

**NOTE** – Since the VS6 is un-configured at the stage when the tool is typically run the product type (Local vs. Metro) can't be determined. Therefore this check is done on all VS6 clusters. If there's no WAN COM SLIC installed this issue will not be detected/reported.

## Check for 'Up' VS6 WAN Ports

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS6

**Issue:**

During the VS2 to VS6 GenU procedure the cabling for the WAN COM ports should not be performed until prompted to by the Upgrade Manager script. Therefore, this check is performed to determine if the cabling has been done too early (prior to the start of the procedure). The tool looks for VS6 WAN COM ports with 'Up' status, which indicates they have connectivity (are cabled). The VS6 WAN COM ports should have 'no-link' status prior to the GenU.

**Workaround/Next Steps:**

If this issue is reported the Customer Engineer (CE) should remove the cabling from the VS6 WAN COM ports, and then verify the ports are displayed in VPlexcli with 'no-link' status. This can be verified by logging into VPlexcli and issuing this command:

VPlexcli:/> ll engines/*/directors/*/hardware/ports

## GeoSynchrony Version Warning

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS6

**Issue:**

The VS2 and VS6 clusters must have the same GeoSynchrony software version running prior to the start of the GENU.

The tool prints the GeoSynchrony version found on the VS6 cluster to the log along with the following warning:

*WARNING: The VS2 and VS6 need to be running the same GeoSynchrony version prior to the GENU*

**Workaround/Next Steps:**

Ensure the VS2 and VS6 clusters involved in the GENU are running the same GeoSynchrony version prior to the start of the GENU. Use the VPlexcli command 'version –a' to check the version.

## VS6 SLIC-4 Check

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS6

**Issue:**

In the preparatory phase, when configuring a VS6 cluster for a generational upgrade procedure, the temporary FC IO Modules need to be inserted in SLOT-4 of the VS6 directors.

If this isn't done before the VS6 directors are powered up, and the temporary FC IO Modules are inserted after the directors are brought up, then the temporary FC IO Module port entries won't be populated in the directors' portRoles files. This leads to the generational upgrade failing.

**Workaround/Next Steps:**

If this issue is reported a Customer Engineer (CE) needs to follow KBA 524376 "VPLEX: Temporary IO Module (SLIC-4) Not Detected on Un-configured VS6 Preparing for/Undergoing GenU".

## Check for IPv6 on the management-server eth3 port

Susceptible Versions: 6.0.1 Patch 4 – 6.0.1 Patch 7

Fixed Version(s): 6.1

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: VS6

**Issue:**

GeoSynchrony 6.0.x releases have not been qualified for generational hardware upgrade (GenU) if IPv6 is used for management-connectivity (on any Local/Metro). This check analyzes if IPv6 is in use on the eth3 port of the management-server, and prints a warning if detected.

**Workaround/Next Steps:**

If this issue is reported it's recommended to upgrade the VPLEX clusters to GeoSynchrony 6.1, where GenU with IPv6 in use has been qualified, and is supported.

# NDU Checks

# Overview

The tool will perform the following checks for the ndu option. If the tool detects that any of the below issues are present they will be reported in the 'Issues Summary Report', which is printed on the console and at the end of the log file produced by the tool (file named C*x*_<*last4TLA*>.log – where x = cluster-1/cluster-2 and the last 4 digits of the VPLEX TLA).

## Check Enabled Ports' RX/TX Power

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: All

**Issue:**

This check is performed to verify if any of the enabled VPLEX ports have low RX or TX power levels (defined as <=200uW). Low RX or TX power issues could result in connectivity issues that could potentially impact the NDU, so if these issues are reported they should be investigated and resolved prior to the NDU.

**Workaround/Next Steps:**

If this issue is reported a Customer Engineer (CE) should reference KBA 336564 for steps to troubleshoot this issue.

## Check certificate status

Susceptible Versions: All

Fixed Version(s): N/A

VPLEX CQ/Jira #: N/A

VPLEX Hardware Checked: All

**Issue:**

If the security certificates expire just prior to the NDU it could result in delays to the procedure. This check verifies the expiration date of all security certificates. If any are set to expire within 30 days a warning is reported, or if any have already expired an error is reported.

**Workaround/Next Steps:**

If this issue is reported the Customer Engineer (CE) should work with the customer to renew the security certificates prior to the NDU. The procedure 'Renew Security Certificates' in VPLEX SolVe Desktop should be followed to perform the renewal.

## Check for Memory Fragmentation

Susceptible Versions: 6.0.x and 6.1.x versions

Fixed Version(s): 6.2

VPLEX CQ/Jira #: VPLEX-16703

VPLEX Hardware Checked: All

**Issue:**

There's a known memory fragmentation issue that can impact NDU on VS6 Metros running GeoSynchrony 6.1.x releases, which is documented in KBA 538517. This memory fragmentation issue is fixed in GeoSynchrony 6.2 and higher releases, but NDU to 6.2 can still potentially be impacted or delayed if memory fragmentation occurs. In 6.2 Patch 2 and higher a memory fragmentation pre-check is added to the VPlexcli 'ndu pre-check' command, which becomes available once the management-server is upgraded to 6.2 Patch 2 or higher. If it detects memory fragmentation the VPLEX Remote Support team needs to be engaged to clear the memory fragmentation prior to starting the director

firmware upgrade. As this can potentially delay the start of the NDU (director firmware upgrade) the same memory fragmentation check is now available in the Upgrade Checker Tool (UCT) so that it can be run prior to the management-server upgrade as well. It's executed by the UCT if the GeoSynchrony version is 6.1.x or 6.0.x (VS2 or VS6).

NOTE: Memory fragmentation is unlikely to be detected on 6.0.x versions, but possible. If it occurs, it is not caused by the same issue that's documented in KBA 538517.

**Workaround/Next Steps:**

This memory fragmentation is triggered by workload changes and can appear/disappear within hours as the workload fluctuates, meaning the memory fragmentation could still reoccur just prior to the director firmware upgrade. It's recommended to perform NDU during off-peak hours, particularly when read-intensive workloads are minimal (if possible) to avoid disruption or a delay to the NDU. If the memory fragmentation check is detected by the UCT prior to the management-server upgrade there is a greater chance that it will also be detected again just prior to the NDU. The memory fragmentation could be cleared, and then potentially re-occur just prior to the NDU (director firmware upgrade).

In this case GS should prepare extra time prior to the NDU (director firmware upgrade) in order for the VPLEX Remote Support team to reboot the directors with memory fragmentation one by one (each reboot takes ~20 minutes to complete (including health/verification checks), so estimate 20 minutes * # directors for max time). Note that instances have been seen where memory fragmentation is cleared on an initial set of directors, and then after running the 'ndu pre-check' again the check detected it on a second set of directors requiring another round of director reboots (requiring even more time to clear).

If memory fragmentation is reported on 6.0.x engage the VPLEX Remote Support team to investigate to verify that it is persisting and clear it if needed (typically requiring a director OS reboot) prior to the NDU (director firmware upgrade).

# Firmware Log Analysis (FLAT)

## Overview

The Firmware Log Analysis Tool (FLAT), which is run by the Upgrade Checker Tool, analyzes the firmware logs present on the VPLEX management-server. It checks for a number of firmware events that could indicate a persistent or intermittent issue on the VPLEX, or in the VPLEX environment, which could potentially cause a VPLEX NDU or GenU to fail.

FLAT is called when the tool is run with the ndu option (with CCA option 'SolVeCCAReview'), or if the genu option is run on a VS2. FLAT is NOT called when the genu option is run on a VS6 (as the VS6 is un-configured).

The FLAT will first check for the presence of the firmware.log files from the VPLEX cluster's management-server, and determine if they contain the last 3 days of event history. If the firmware.logs aren't found, or don't contain 3 days of history they will not be used and the FLAT will instead use the nsfw logs from each director to analyze the firmware events.

On a Metro the nsfw.logs from the directors of both clusters will be analyzed as long as the remote directors can be reached. It's expected that the Upgrade Checker Tool (and thus FLAT) will be run on both clusters in a Metro if there are (or have been in the recent past) VPN connectivity issues, or other issues that prevent access to the remote directors.

If the nsfw.logs from the directors don't contain 3 days of event history an additional warning will be printed to make the user aware of this. Regardless of the time span of the nsfw.logs the FLAT will continue to analyze the nsfw.logs.

The report summary on the firmware analysis will be printed to the log file FirmwareReportSummary.txt. If events are noted this file can be shared with the customer, and the descriptions and instruction summaries for the event(s) should be reviewed in order to further investigate the event(s).

## Potential Issues

### Can't Use Firmware Logs

If the firmware.logs can't be used, then the sms firmware events will not be checked (as they are only contained in the firmware.logs from the management-server, and not the nsfw.logs). If this occurs a warning regarding this will be printed to the console:

*WARNING: Either the firmware.log(s) from the management-server wasn't found, or it doesn't go back 3 days, so the nsfw.logs from the directors will be used to analyze the firmware events. Due to this the SMS related events can't be checked. Please use VPlexcli command 'director uptime' to check if any directors firmware has restarted recently. If this is the case, and the cause is unknown, engage the VPLEX Remote Support team to investigate as soon as possible.*

To check this, log into VPlexcli and issue the command 'director uptime':

VPlexcli:/> director uptime

Example:

VPlexcli:/> director uptime
Director director-1-1-B: 3 days, 5 hours, 10 minutes, 44 seconds.
Director director-2-1-A: 9 days, 12 hours, 38 minutes, 40 seconds.
Director director-2-1-B: 9 days, 12 hours, 38 minutes, 9 seconds.
Director director-1-1-A: 9 days, 12 hours, 51 minutes, 40 seconds.

If one or more directors have an uptime that indicates the firmware restarted in the recent past, and the cause of the firmware restart is unknown (a NDU did not take place recently), then the VPLEX Remote Support team should be engaged to investigate the cause.

**NOTE:** The VPLEX Remote Support team will need a collect-diagnostics (including the extended collect-diagnostics) from the VPLEX in order to troubleshoot director firmware restarts. The VPlexcli command 'collect-diagnostics' should be executed in order to collect this.

## Can't Use Firmware or NSFW Logs

The FLAT could potentially print a range of error messages if it's unable to obtain the required firmware or nsfw logs, or if a failure is encountered in parsing them. If this occurs, it's recommended to manually check the firmware.logs for events that could potentially indicate a persistent or intermittent problem on the VPLEX, or in the VPLEX environment, which could impact a planned activity.

NOTE: A Customer Engineer (CE) should review the below instructions, and if unsure about the analysis engage a Field Support Specialist (FSS) for assistance.

The Linux 'grep' command can be used to manually search the firmware.logs for the event IDs listed in the following table (which are analyzed by FLAT).

From the Linux command prompt on the management-server or MMCS-A cd to the /var/log/VPlex/cli directory:

service@sms:~> cd /var/log/VPlex/cli

To view the firmware.logs use the command 'ls -ltr firmware.log*', eg.:

```
service@sms:/var/log/VPlex/cli> ls -ltr firmware.log*
-rw-r--r-- 1 service users    3048 Aug 10 04:17 firmware.log_20180810040718
-rw-r--r-- 1 service users  299434 Aug 13 15:43 firmware.log_20180812121554
```

To check the current date & time, use the 'date' command, eg.:

```
service@sms: /var/log/VPlex/cli> date

Mon Aug 13 16:04:04 UTC 2018
```

Then use the grep command with 'wc –l' to search for, and determine the counts of the events within the last 3 days.

Example searching for the com/21 event indicates none have logged in the last 3 days:

```
service@sms:/var/log/VPlex/cli> grep "com/21" firmware.log* | grep "2018/08/1[1,2,3]" | wc -l

0
```

Example searching for the sms/1 event, where 17 were logged in the last 3 days:

```
service@sms:/var/log/VPlex/cli> grep "sms/1" firmware.log* | grep "2018/08/1[1,2,3]" | wc -l

17
```

If concerning events are found VI can be used to manually parse through the firmware.log and analyze them in greater detail. Other variations of the above 'grep' command can also be used to narrow the events down to particular time ranges, and/or objects (volumes, wwns, etc.) printed in the event message. Reference 'grep –help' for more details.

## NSFW Logs Don't Contain 3 Days of History

If the firmware logs on the management-server can't be used, the FLAT will use the nsfw.logs from the directors to analyze the events. If the available nsfw.logs don't go back 3 days in time the following warning will be printed to the console & report:

*WARNING: The nsfw.logs from the directors don't go back 3 days, analyzing <3 days of event history.*

As the nsfw.logs are rotated on the directors, the older files are compressed, leaving only a single nsfw.log file which can be analyzed by FLAT, making this issue potentially likely to occur. The nsfw.logs can be analyzed manually, but as they're printed in TCL format, it's more challenging to do so.

Therefore, if this is encountered it's recommended to manually check the firmware.logs on the management-server, see if they go back 3 or more days, and try to manually analyze at least 3 days of event history using the instructions given in the section above 'Can't Use Firmware or NSFW Logs'.

# List of Firmware Events

The FLAT checks for the following events, and if found according to the corresponding threshold it reports them in the FirmwareReportSummary.txt file.

| Event ID | Threshold for Reporting the Event | Description | Instruction Summary |
|---|---|---|---|
| com/21 | Any number in last 3 days | A COM IO took >900 ms to complete, potentially indicating high Local COM or WAN COM latency. | If the events persist, and the VPLEX is a Metro begin by checking for signs of high WAN COM latency from the VPLEX performance statistics. If the WAN COM latency is in the expected range engage Customer Service to investigate the latency on the LOCAL COM links. Otherwise, on a VPLEX Local if the events persist engage Customer Service to investigate the latency on the LOCAL COM links. |
| fsmon/0 | Any number in last 3 days | Unable to retrieve the filesystem status of one of the filesystems. The filesystem may have gone into a read-only state. | Engage Customer Service (VPLEX Remote Support) for investigation. |
| fsmon/1 | Any number in last 3 days, including some in last 24 hours | A filesystem on the director has exceeded its usage threshold and is getting low on free space. | The filesystem likely needs to be cleaned up. If uncertain which files to remove engage VPLEX Customer Service for investigation. |
| splitter/1 | Any number in last 3 days | VPlex sent a write to RecoverPoint RPAs, and the RPAs failed to complete it, the volume(s) was moved into MOH mode. If this occurs during the VPLEX NDU it will cause the NDU to fail and rollback. | Investigate the fabrics between the VPLEX BE ports & RPAs, and engage RecoverPoint support to investigate the RPAs health to determine why the writes failed to be protected on the RPAs. |
| amf/249 | Any number in last 3 days | The average I/O latency on a disk has exceeded the acceptable limit (default of 200 msec). | Investigate the backend array and fabrics to determine why there are poor response times for the storage-volume. |

| | | | |
|---|---|---|---|
| stdf/10 (Abort Task) | >20 in last 3 days, including some in last 24 hours | Large numbers of SCSI Task Management Functions (TMF) from host initiators have been processed. | Determine if the hosts have experienced performance impact, and if so investigate the performance of the VPLEX. |
| stdf/10 + stdf/13 | >20 in last 3 days, including some in last 24 hours | A SCSI Task Management Function (TMF) has been processed for which no active task on the nexus could be found. | These events typically indicate frames are being dropped in the FE fabrics. Investigate fabrics between involved VPLEX FE ports & host HBAs. |
| nmg/50 | Any number in last 3 days | The nmg/50 event has logged indicating a cluster departed in the recent past. This could mean both clusters departed each other due to a failure in WAN COM connectivity, or only one cluster may have departed due to an issue on that cluster (power loss, etc.) | Investigate the WAN COM fabrics for link failures and check for problems on the remote cluster, such as a power outage. Verify stability of the WAN COM links prior to proceeding with NDU. |
| sms/1 | Any number in last 3 days | A network connection from the management server to a director failed. This could be due to a hardware problem on one side of the management network or an unresponsive director (the director firmware may have restarted at the time). | Engage Customer Service to investigate why the director was unresponsive. If it was due to a firmware crash, investigate if this poses any risk to the NDU. |
| sms/500 | Any number in last 3 days, including some in last 24 hours | The VPN tunnel between this management server and the remote management server is down. | Check the connection with the VPlexcli command "vpn status". If the ipsec connection is down, restart it with "vpn start" command from VPlexcli. If problems still occur, ping remote site's management server and ensure it can be reached. Also, please verify if there are any issues in the network between the management servers. If problem persists engage Customer Service for investigation. |

| | | | |
|---|---|---|---|
| sms/506 | Any number in last 3 days, including some in last 24 hours | A partition on the Management Server has exceeded a critical capacity threshold. | 1. You will need to back up critical data. Run "sudo /tmp/VPlexInstallPackages/VPlex-MS-install --pre-reimage -v -l /var/log/install.log. Move this file to a destination off of the Management Server and delete the local copy. 2. You will need to collect any diagnostic data. Run "collect-diagnostics". Move this file to a destination off of the Management Server and delete the local copy. 3. Find the largest files in the partition by running du -s [partition]> \| sort -n. Remove the largest files as needed. This can be confirmed with du -sh [partition]. If uncertain which files to remove engage Customer Service. |
| sms/507 | Any number in last 3 days, including some in last 24 hours | A partition on the Management Server has reached a high capacity. | 1. You will need to back up critical data. Run "sudo /tmp/VPlexInstallPackages/VPlex-MS-install --pre-reimage -v -l /var/log/install.log. Move this file to a destination off of the Management Server and delete the local copy. 2. You will need to collect any diagnostic data. Run "collect-diagnostics". Move this file to a destination off of the Management Server and delete the local copy. 3. Find the largest files in the partition by running du -s [partition]> \| sort -n. Remove the largest files as needed. This can be confirmed with du -sh [partition]. If uncertain which files to remove engage Customer Service. |
| scsi/27 | >20 in last 3 days, including some in last 24 hours | A SCSI command was returned from a BE array with SCSI sense data (typically a check condition). | Investigate the BE array to determine why it returned the check condition for the volume. |

| | | | |
|---|---|---|---|
| scsi/92 | Any number in last 3 days | The VPLEX director specified lost a path to a Logical Unit from the specified BE initiator port to the specified target port on the BackEnd array. If this didn't occur during an activity of deprovisioning the Logical Unit from the VPLEX, then there is/was a problem with the masking or physical connectivity between the array and the VPLEX BE port. There could also potentially be an intermittent connectivity problem. | If the issue persists, check the masking/mapping from the array for the LU. If in good standing, investigate the health of the connectivity between the specified VPLEX port and BE array port, including the cables and switches. Analyze the switch logs for signs of errors, and test/replace hardware as needed to resolve the issue. |
| scsi/93 | Any number in last 3 days | The second to last FibreChannel connection was lost between a VPLEX director's BE port (the initiator) and a target port on a BackEnd array for a particular Logical Unit. If this didn't occur during an activity of deprovisioning the Logical Unit from the VPLEX, then there is/was a problem with the masking or physical connectivity between the array and the VPLEX BE port. There could also potentially be an intermittent connectivity problem. | If the issue persists, check the masking/mapping from the array for the LU. If in good standing, investigate the health of the connectivity between the specified VPLEX port and BE array port, including the cables and switches. Analyze the switch logs for signs of errors, and test/replace hardware as needed to resolve the issue. |
| scsi/138 | >20 in last 3 days, including some in last 24 hours | A reservation conflict has been detected on a storage-volume. | If these events are still logging investigate the BE array to determine which initiator is holding the reservation and release it. |
| scsi/140 | >20 in last 3 days, including some in last 24 hours | The BE array did not respond to a SCSI command from VPLEX in the timeout interval of 10 seconds. This could indicate a performance or other problem on the array. | Investigate BE array to determine why it wasn't responding to IO within 10 seconds. |
| scsi/148 | Any number in last 3 days | The reported IT nexus on the VPLEX BackEnd failed a reliability test and is/was considered failing. The IT nexus was banished (meaning the VPLEX will no longer use the BackEnd path until the reliability of the connection improves). | If the issue persists, the cause of the failure for the IT nexus must be determined. Investigate the switch logs to help pinpoint the cause of the failure. Check for faulty hardware along the path, verify the health of the cable(s), and SFPs on the VPLEX, switch(es) and array. |
| scsi/153 | >20 in last 3 days, including some in last 24 hours | A SCSI command to a BE array failed with an error status. | Investigate the BE array to determine why the SCSI command(s) failed. |

| | | | |
|---|---|---|---|
| scsi/154 | Any number in last 3 days, including some in last 24 hours | The array has reported the logical unit as being BUSY more often than is normal and this may impact performance. | Investigate the BE array to determine why it was responding to IO with BUSY. |
| scsi/155 | >20 in last 3 days, including some in last 24 hours | A SCSI command submission (from the VPLEX BE to an array) failed with the listed error status. | If these are logging along with splitter/1 events then investigate the connectivity to the RPAs along with the health of the RPAs. Otherwise, investigate the BE connectivity. If the events persist and unable to determine the cause engage VPLEX Customer Service. |
| ipc/19 | Any number in last 3 days | Link went down on a port, depending on the port role, a physical path to the local or remote cluster has been lost. These events are more frequently seen for WAN COM connectivity loss. | Perform the following steps: 1. Check the state of the port and ensure that it is enabled. 2. Check the cable and the SFP, and ensure they are properly plugged in. 3. Check the switch if applicable, and ensure it is operational and the corresponding port is enabled. 4. If the link remains down, contact VPLEX Customer Service. |
| ipc/22 | Any number in last 3 days | A WAN COM connection is degraded. The link path between two directors is experiencing high packet loss, high latency or a degraded bandwidth problem. | Investigate the switch logs for the specified path(s) to determine the cause of the high latency, degraded bandwidth or connectivity issue. |
| ipc/24 | Any number in last 3 days | A SFP on a VPLEX WAN COM port was detected as missing, inserted incorrectly, or faulty as it is/was not responding. | If the issue persists apply the following measures until the issue is resolved: 1. Identify the physical port specified in the event. 2. If the SFP is missing, insert a new DELL EMC-approved SFP and connect the appropriate cable (engage a DELL EMC field representative (CE). 3. Re-seat the SFP. 4. Engage a DELL EMC field representative (CE) to replace the SFP. 5. If all else fails a DELL EMC field representative (CE) should replace the IO SLIC. |
| ipc/26 | Any number in last 3 days | The port was detected to be equipped with an SFP which is not approved by DELL EMC. | Engage a DELL EMC field representative (CE) to replace the SFP for the port(s) in question. |

| | | | |
|---|---|---|---|
| ipc/28 | Any number in last 3 days | No incoming laser had been detected on a VPLEX ethernet port. This is typically logged for VPLEX WAN COM ports when there's a connectivity problem between the VPLEX port and the switch. | Apply the following measures until the issue is resolved: 1. Identify the physical port mentioned in this event. 2. Check if the optical cable had been inserted into the SFP on the VPLEX port, plug in cable if needed. 3. Reseat the SFP on the VPLEX port. 4. Follow the optical cable to the switch, write down the switch/port information. 5. Inspect the switch side cabling/SFP, and replace hardware as needed. 6. Verify the switch port configuration and determine if any changes are needed. |
| ipc/34 | Any number in last 3 days | Attempts to establish a WAN COM link is failing continuously. Possibly due to improper switch MTU settings. | Verify the MTU settings are correct on each device within the path. Check for other connectivity issues that could cause the path to not establish. If the issue persists and unable to determine the cause engage VPLEX Customer Service. |
| ipc/42 | Any number in last 3 days | The expected ID for a packet received over the IP WAN COM network does not match with the packet ID. The received packet may be corrupted. The connection is being reset. | Investigate the IP WAN COM networks to determine what could be causing the corrupted packets. If the issue persists engage Customer Service for investigation. |
| ipc/46 | Any number in last 3 days | The WAN COM path from the specified director to the specified remote IP address is the last path remaining between the two directors. If this last available path is lost, there will be a site departure between the clusters. | Investigate the IP WAN-COM switches and the links between them to determine why the link is down. Check the cables and the SFPs, make sure they are properly plugged in. Check the relevant switches and make sure they are operational and the corresponding switch ports are enabled. If the issue persists and unable to determine the cause engage VPLEX Customer Service. |

| | | | |
|---|---|---|---|
| comscsi/17 | Any number in last 3 days | A WAN COM path is degraded due to the specified condition. | Depends on the degradation condition: 1). RTT_TOO_BIG: the path might be congested, when the congestion resolves, the degrade condition will resolve by itself; If the path does have a longer RTT compared to the other path, then it will not be used unless it is the last usable path. 2). IO_ERROR: some IO errors will trigger this condition, these IO errors are usually caused by faulty hardware on the IO path. Try to identify the common point of failure and remove the faulty condition. The degrade condition will be removed once no more IO errors are noticed for some time. 3). LINK_FLAP: the link had been flapping too often, fix the connectivity issue which caused the flapping and the condition will be resolved. |
| comscsi/25 | Any number in last 3 days | The last redundant FC WAN COM path to the specified remote director is down. If the last path is lost between the directors there will be a site partition between the clusters. | Investigate the FC WAN-COM switches and the links between them to determine why the link is down. Check the cables and the SFPs, make sure they are properly plugged in. Check the related switches (if applicable), and make sure they are operational and the corresponding switch ports are enabled. Check the switch logs for indications of connectivity issues. |
| comscsi/27 | Any number in last 3 days | Stuck IO had been detected on the FC port(s) in the specified IT nexus. | Stuck IO had been detected and automatically resolved by resetting the FC COM port. Please contact VPLEX Remote Support to investigate this issue. |
| comscsi/28 | Any number in last 3 days | The immediate data probe on an inter-director (WAN COM) FC path failed. This typically happens when fast-write/write-acceleration is enabled on the WAN COM switches, and this conflicts with the VPLEX short-write feature. | Check the configuration on the WAN COM switch(es) and disable fast-write/write-acceleration if enabled. |

| | | | |
|---|---|---|---|
| comscsi/29 | Any number in last 3 days | Large numbers of IOs have timed out on this connection in the past one minute. | Please investigate the health of the switch(es), cables and SFPs in the connection identified as having a high timeout count. Please rectify any bad hardware found. If the connection with a high timeout count is a local COM path (between directors in one cluster) please contact VPLEX Customer Service for investigation. |
| tach/20 | >20 in last 3 days, including some in last 24 hours | IO failures have occurred on the specified IT nexus due to frame drops. The frame drop threshold has been exceeded. | If the port is a BE port check the target storage device specified by the event, as this is usually caused by the target device port being unable to handle the amount of IO generated by the VPLEX initiator port(s). Otherwise, an over-subscribed switch in the IO path could also cause this symptom. Check the switch logs for any sign of over-subscription, or other connectivity issues. |
| tach/21 | >20 in last 3 days, including some in last 24 hours | IO failures have occurred on the specified IT nexus due to frame time outs. The frame time out threshold has been exceeded. | There might be faulty hardware close to the port. Take the following steps in order: 1. Identify the physical port specified in the event, follow the cable and find the switch port it connects to (or target device). 2. Clean and re-seat the cable; 3. Replace the SFP on both ends; 4. try to use a different switch port if available; 5. Contact VPLEX Customer Service to replace the IO SLIC. |
| tach/31 | Any number in last 3 days | An SFP is missing, inserted incorrectly, or faulty. | Engage Customer Service for investigation. |
| tach/48 | Any number in last 3 days | An FC chip detected persistent PCI error. The SLIC corresponding to the specified port needs to be replaced. | Engage VPLEX Customer Service to replace the IO SLIC. |
| tach/52 | >20 in last 3 days, including some in last 24 hours | A Fibre Channel port has observed frames with an EOFa (End of Frame Abort) delimiter in the last minute. | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |

| | | | |
|---|---|---|---|
| tach/53 | >20 in last 3 days, including some in last 24 hours | A Fibre Channel port has discarded frames in the last minute. | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |
| tach/54 | >20 in last 3 days, including some in last 24 hours | A Fibre Channel port has observed frames with CRC error in the last minute | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |
| tach/55 | >20 in last 3 days, including some in last 24 hours | A Fibre Channel port has observed frames with protocol error in the last minute. | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |
| tach/60 | >20 in last 3 days, including some in last 24 hours | An FC port had IO failed due to out of order frames. | Investigate the switch logs for the respective ports to determine what's causing the out of order frames. |
| tach/61 | >20 in last 3 days, including some in last 24 hours | An FC port reset the link to recover from no BB_credit. | Investigate the switch logs for the respective ports to determine if there's a slow drain device in the fabric. Investigate the cause for the slow drain. |
| io-port/19 | >20 in last 3 days, including some in last 24 hours | An IO port observed high IO failure counts on an IO path. IO exchange timeout threshold exceeded. Common cause is faulty hardware (dirty cable, faulty SFP, etc). | Engage VPLEX Customer Service to check for faulty hardware with the following steps: 1. Identify the IO path specified by the event. 2. Clean and re-seat the cables on the path. 3. If applicable, check switch stats to see if any switch in the path is over-subscribed 4. Replace SFPs on the IO path. 5. Check the target storage device to see if it is over-subscribed, if so, add more target ports to serve IO. |
| io-port/20 | >20 in last 3 days, including some in last 24 hours | An IO port observed a high IO failure rate due to dropped frames on the IO path. | Check the target storage device specified by the event. This is usually caused by the target device port being unable to handle the amount of IO generated by the initiator ports. Or an over-subscribed switch in the IO path could also cause the |

| | | | |
|---|---|---|---|
| | | | symptom. Check the switch logs for any sign of over-subscription. |
| io-port/21 | >20 in last 3 days, including some in last 24 hours | An IO port observed high IO failure rate due to frames timing out on the IO path. | There might be faulty hardware close to the specified port. Take the following steps in order: 1. Identify the physical port specified in the event, follow the cable and find the switch port it connects to (or target device). 2. Clean and re-seat the cable; 3. Replace the SFP on both ends; 4. try to use a different switch port if available; 5. Contact VPLEX Customer Service to replace the IO SLIC. |
| io-port/24 | >20 in last 3 days, including some in last 24 hours | An IO port is continuously toggling between linkup and linkdown. There might be faulty hardware at the port. | There might be faulty hardware close to the specified port. Take the following steps in order: 1. Identify the physical port specified in the event, follow the cable and find the switch port it connects to (or target device). 2. Clean and re-seat the cable; 3. Replace the SFP on both ends; 4. try to use a different switch port if available; 5. Contact VPLEX Customer Service to replace the IO SLIC. |
| io-port/48 | Any number in the last 3 days. | An IO chip detected persistent PCI error. This SLIC needs to be replaced. | Engage VPLEX Customer Service to check if the indicated IO SLIC is healthy and has full connectivity. If the IO SLIC is unhealthy, or the errors persist, it should be replaced. |
| io-port/49 | Any number in the last 3 days. | An IO chip detected an uncorrectable SLIC error. This SLIC needs to be replaced. | Engage VPLEX Customer Service to check if the indicated IO SLIC is healthy and has full connectivity. If the IO SLIC is unhealthy, or the errors persist, it should be replaced. |
| io-port/52 | >20 in last 3 days, including some in last 24 hours | An IO port received frames with EOFa (End of Frame Abort) delimiter in the last minute. There might be faulty hardware on the IO path. | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |

| | | | |
|---|---|---|---|
| io-port/53 | >20 in last 3 days, including some in last 24 hours | An IO port discarded frame(s) in the last minute. There might be faulty hardware on the IO path. | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |
| io-port/54 | >20 in last 3 days, including some in last 24 hours | An IO port received frames with CRC error in the last minute. There might be faulty hardware on the IO path. | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |
| io-port/55 | >20 in last 3 days, including some in last 24 hours | An IO port received frames with protocol error in the last minute. There might be faulty hardware on the IO path. | There might be faulty hardware on the IO path. Engage VPLEX Customer Service to: 1. Clean and re-seat the cables connecting to the interface; 2. Replace SFPs on the interface. |
| io-port/60 | >20 in last 3 days, including some in last 24 hours | An IO port has IO failed due to out of order frames. | Investigate the switch logs for the respective ports to determine what's causing the out of order frames. |
| io-port/61 | >20 in last 3 days, including some in last 24 hours | An IO port reset the link to recover from a lack of buffer-to-buffer credits. | Investigate the switch logs for the respective ports to determine if there's a slow drain device in the fabric. Investigate the cause for the slow drain. |
| scsi/170 | Any number in last 3 days | An array returned Unit Attention 6/38/07h THIN_PROVISIONING_SOFT_THRESHOLD_REACHED for a storage-volume on a VPLEX write. The thin pool on the array is/was running out of space. | Add additional block resources to the thin pool on the array from which the storage-volume is provisioned. |
| scsi/171 | Any number in last 3 days with at least 1 in the last 24 hours | The Logical unit inventory reported from an array is invalid. The array is reporting that it has a greater number of logical units than what VPLEX requested. The number does not match what the array actually transferred in the response data buffer, and does not match what the array actually has in its masking-view/storage-group for VPLEX. | VPLEX will retry getting logical unit inventory. If the issue persists, collect VPLEX and Array logs and traces and contact EMC Customer support. |

| | | | |
|---|---|---|---|
| scsi/172 | Any number in last 3 days with at least 1 in the last 24 hours | The Logical unit inventory reported from an array is invalid. The array is reporting that it has less logical units than what VPLEX requested. The number does not match what the array actually transferred in the response data buffer, and does not match what the array actually has in its masking-view/storage-group for VPLEX. | VPLEX will retry getting logical unit inventory. If the issue persists, collect VPLEX and Array logs and traces and contact EMC Customer support. |
| scsi/173 | Any number in last 3 days with at least 1 in the last 24 hours | Logical unit inventory, from an array, is invalid. The number of LUs reported by the array is not equal to the number of LUs VPLEX requested. | VPLEX will retry getting logical unit inventory. If the issue persists, collect VPLEX and Array logs and traces and contact EMC Customer support. |
| scsi/174 | Any number in last 3 days with at least 1 in the last 24 hours | Retry limit on successfully processing logical unit inventory exceeded on an IT Nexus. VPLEX proceeds with processing as many logical units as it can. Failure to successfully process logical unit inventory could be be due to one of the following: 1. The array is reporting that it has a greater number of logical units than what VPLEX requested. The number does not match what the array actually transferred in the response data buffer, and does not match what the array actually has in its masking-view/storage-group for VPLEX. 2. The array is reporting that it has less logical units than what VPLEX requested. The number does not match what the array actually transferred in the response data buffer, and does not match what the array actually has in its masking-view/storage-group for VPLEX. | The retry limit is exhausted, VPLEX is proceeding with processing as many LUs as it can. If all LUs, from the array masking-view/storage-group from VPLEX, are not discovered, perform array re-discover. Collect VPLEX and Array logs and traces and contact EMC Customer support. |
| fc/7 | Any number in last 3 days | A diagnostic dump for the given interface could not be written. This could indicate a full or corrupt director filesystem or a hardware issue with the director's internal storage. | Contact VPLEX Remote Support to investigate this issue. |
| fc/8 | Any number in last 3 days | This port is connected to a switch and link is up. However, the port is not in any configured switch zone. This might be an oversight of switch configuration, which could impact connectivity. | Analyze the zones enabled in the effective configuration for the switch in question, and add the zone for the port(s) in question. |
| fc/9 | Any number in last 3 days | An interface operating in a direct-connect topology received an unexpected command. Normal function of the connection may be affected. | Contact VPLEX Remote Support to investigate this issue. |

| | | | |
|---|---|---|---|
| fc/10 | Any number in last 3 days | An interface operating in a direct-connect topology received an unexpected command. Normal function of the connection may be affected. | Contact VPLEX Remote Support to investigate this issue. |
| fc/11 | Any number in last 3 days | An interface operating in a direct-connect topology received an unexpected command. Normal function of the connection may be affected. | Contact VPLEX Remote Support to investigate this issue. |
| fc/12 | Any number in last 3 days | An interface operating in a direct-connect topology received an unexpected command. Normal function of the connection may be affected. | Contact VPLEX Remote Support to investigate this issue. |
| fc/13 | Any number in last 3 days | When connecting to a switch, the port received a non-spec-compliant response indicating that the switch does not support any protocol version that VPLEX supports. Because this response is non-spec-compliant, VPLEX is unable to report on which version of the spec that the switch does support. VPLEX is unable to register with the switch or perform fabric discovery. | Check the VPLEX ESSM to verify the switch model & firmware version is supported. If it is, engage VPLEX Support to investigate. |
| fc/16 | Any number in last 3 days | When connecting to a switch, the port received a response indicating that the switch does not support any protocol version that VPLEX supports. This switch is likely not compatible with VPLEX. | Check the VPLEX ESSM to verify the switch model & firmware version is supported. If it is, engage VPLEX Support to investigate. |
| fc/17 | Any number in last 3 days | The indicated interface has encountered an internal error and has dumped diagnostics for chip vendor analysis. | If it hasn't already been done, issue collect-diagnostics (with extended collect-diagnostics), which will collect the chip dump. Engage the VPLEX Remote Support team for investigation. Consult with VPLEX Remote Support to determine if it's safe to proceed with any change control (NDU or GenU) if one is planned. |

| | | | |
|---|---|---|---|
| fc/23 | Any number in last 3 days | The link has been lost, likely due to local or remote port disablement or loss of physical connection. This could also potentially have logged following the director firmware having restarted, if the director experienced a director firmware restart or an OS reboot at the time. | Check the director port in VPlexcli to determine if the link is still down. If it is and the issue persists, analyze the switch logs to check for signs of errors that will help determine where the problem lies. If the physical connection is down test/replace the physical hardware (cables/SFPs) as needed until the issue is resolved. If the link is back up, the VPlexcli command 'director uptime' can be used to check if the director firmware restarted around the time this event logged. |
| fc/24 | Any number in last 3 days | An attempt to communicate with the switch has timed out. This likely indicates either a physical communication issue with the switch or a misbehaving switch. | Check for SFP & cable health issues on the path(s) in question. Check the switch logs for health and frame loss. Contact VPLEX Support if the issues persist and unable to determine the cause. |
| fc/25 | Any number in last 3 days | An internal command on this interface has failed unexpectedly. | Engage VPLEX Remote Support. Consult with VPLEX Remote Support to determine if it's safe to proceed with any change control (NDU or GenU) if one is planned. |
| fc/29 | Any number in last 3 days | The chip underlying the specified interface (VPLEX port) has encountered an error condition and requires a manual reset from DELL EMC Customer Service. Reference KBA 522334. | Engage VPLEX Remote Support to verify if the issue has already been rectified or not. Consult with VPLEX Remote Support to determine if it's safe to proceed with any change control (NDU or GenU) if one is planned. |
| fc/30 | Any number in last 3 days | The chip has encountered an error condition and no automated recovery is possible. The chip may now be unresponsive resulting in stuck IO. The chip needs to be manually reset by DELL EMC Customer Service, and if that fails the director needs to be rebooted to recover from this issue. Reference KBA 522334. | Engage VPLEX Remote Support to verify if the issue has already been rectified or not. Consult with VPLEX Remote Support to determine if it's safe to proceed with any change control (NDU or GenU) if one is planned. |
| febefc/400 | Any number in last 3 days | This port attempted to log in to or handle a login from a remote endpoint but doesn't have any login resources remaining. | It is likely that this port has been exposed to more endpoints than are supported by VPLEX. Check configuration to see if it's within limits (compare with Release Notes). If it is, engage the VPLEX Remote Support team for further investigation. Toggling the port (disabling and re-enabling via |

| | | | |
|---|---|---|---|
| | | | VPlexcli) may workaround the issue. |
| febefc/402 | Any number in last 3 days | This port attempted to initiate or handle an I/O to/from a remote endpoint but doesn't have any I/O resources remaining. This has occurred for many I/O in the indicated period. Either a large increase in IOPS has occurred on the FE of the director, there are frame drop issues on the fabric, or there is an internal issue in the VPLEX. | Engage VPLEX Support if there is an outage or extreme performance issues. Check the performance stats to determine if there was a large increase in incoming IO on the director at the time of the issue. Ensure that the switch logs do not indicate a large number of frame drops or other errors that would indicate a problem. If unable to determine the root cause and the issue persists engage VPLEX Support. |
| febefc/403 | Any number in last 3 days | This port is experiencing a high I/O failure rate with multiple remote endpoints. | Check the switch logs from the fabric for frame drop issues or other errors that could indicate a problem. Check the health of the SFPs on the port and the switch, for both VPLEX and the indicated endpoint. Engage VPLEX Support if the issue persists and unable to determine the cause. |
| febefc/501 | Any number in last 3 days | This port is experiencing a high I/O failure rate with the indicated remote endpoint. | Check the fabric for frame drop issues. Check the health of the SFPs on the port and the switch, for both VPLEX and the indicated endpoint. Engage VPLEX Support if the issue persists and unable to determine the cause. |
| stdf/65 | Any number in last 3 days with at least 1 in the last 24 hours | VPLEX is unable to format the volume with zeroes for an IBM iSeries D910 host | Investigate why the zeroing of the volume is failing. Investigate if there are any backend issues for the storage-volume(s) in question. Once resolved, try the format again. |

| | | | |
|---|---|---|---|
| amf/269 | >10 in last 3 days, including some in last 24 hours | The average I/O latency on a remote device has exceeded the acceptable limit | 1. Use the VPLEX Unisphere performance monitoring stats to verify if there is high average I/O latency on the WAN COM links, or high average backend I/O latency on the cluster where the remote device resides, and investigate further as needed. 2. Create storage-volume performance monitors in Vplexcli to investigate individual storage-volume latency stats as needed to further investigate the cause of the performance degradation. 3. Compare the storage-volume latency stats to the latency on the storage array for the volume(s) in question. If the latency on the array isn't as high investigate the fabrics between the storage array and VPLEX. 4. If the issue persists and unable to determine the cause engage DELL EMC Customer Service. |
| floor/35 | Any number in last 3 days | The director firmware has been reset to recover from an unexpected internal firmware error. | DELL EMC will receive call-homes for the firmware restart and will determine the cause. If the system doesn't have call-home enabled to DELL EMC, then report this event to the VPLEX Remote Support team in Customer Service. Verify the root cause and any required workarounds before proceeding with a software or hardware upgrade on the system. |
| disk/1007 | >10 in last 3 days | A storage volume encountered an I/O failure due to retry exhaustion after multiple consecutive I/O completions. | Verify reported array's BE disk health and LUN masking. Check array configuration and physical connection between (a) the director (VPLEX BE Port) and the backend switch and (b) backend switch and the array. |
| disk/1008 | >10 in last 3 days | A storage volume encountered sustained I/O failures due to retry exhaustion. | Verify reported array's BE disk health and LUN masking. Check array configuration and physical connection between (a) the director (VPLEX BE Port) and the backend switch and (b) backend switch and the array. |

| | | | |
|---|---|---|---|
| bepm/1 | >10 in last 3 days | A back-end IT nexus is experiencing poor performance and has been marked degraded. VPLEX has automatically stopped using the ITL paths on this IT nexus for host-based I/O until performance improves. Run VPlexcli command 'back-end degraded list' to check all currently degraded ITs and LUs. | Investigate the related switch logs and array performance for the IT nexus to determine the cause for the degraded performance. Once the performance improves the VPLEX will automatically restore the use of ITLs that were taken out of service. Ensure the root cause for the performance degradation is understood and the issue is resolved before proceeding with a hardware or software upgrade. |
| bepm/4 | >10 in last 3 days | A back-end IT nexus has been continuously cycling between degraded and un-degraded. The IT nexus is now considered unstable and will continue to be marked this way for a default time of 4 hours. Run VPlexcli command 'back-end degraded list' to check all currently degraded ITs and LUs. | Investigate the related switch logs and array performance for the IT nexus to determine the cause for the intermittent poor performance. The I-T path will be marked "Isolated due to unstable performance" until the user manually restores the use of the I-T path via VPlexcli command 'back-end degraded recover', or the default 4 hour threshold is reached, after which the IT nexus will then be marked "performance degraded" while the recovery process checks its health before un-degrading it. If the intermittent latency issue continues on the I-T path, and the user is unable to address the root cause quickly then it is advised to engage Dell EMC Customer Service to manually isolate the IT nexus path to remove it from use until the underlying issue can be resolved. Ensure the root cause for the performance degradation is understood and the issue is resolved before proceeding with a hardware or software upgrade. |
| tcpcom/ 111 | Any number in last 3 days | The local WAN COM port received an invalid header from the remote port (CRC check failed) | The system should recover automatically. However, the underlying network and hardware needs to be investigated to determine the source of the corrupt packet. Please contact Dell EMC support for assistance and ensure the root cause of the issue is |

| | | | |
|---|---|---|---|
| | | | understood and resolved before proceeding with a hardware or software upgrade. |
| tcpcom/ 201 | Any number in last 3 days | A WAN COM path has been indicted due to a received packet failing a CRC check. | The system should recover automatically. However, the underlying network and hardware needs to be investigated to determine the cause of the CRC errors. Please contact DELL EMC Customer Service for assistance and ensure the root cause of the issue is understood and resolved before proceeding with a hardware or software upgrade. |
| tcpcom/ 202 | Any number in last 3 days | A WAN COM path has been indicted due to a received packet having an invalid message length. | The system should recover automatically. However, the underlying network and hardware needs to be investigated to determine the cause of the CRC errors. Please contact DELL EMC Customer Service for assistance and ensure the root cause of the issue is understood and resolved before proceeding with a hardware or software upgrade. |
| tcpcom/ 203 | Any number in last 3 days | A WAN COM path has been indicted due to a timeout. | The system should recover automatically. However, the underlying network and hardware needs to be investigated to determine the cause of the timeout. Please contact DELL EMC Customer Service for assistance and ensure the root cause of the issue is understood and resolved before proceeding with a hardware or software upgrade. |
| febefc/4 04 | Any number in last 3 days | This port has outstanding IO but failed to make progress for over 60s. A chip dump will be initiated, and the directors' firmware will restart to clear any stuck IO. | A call-home should have been sent for this event if call-home was enabled on the system and created a Service Request for the VPLEX Remote Support team. The chip dump will need to be investigated by VPLEX Engineering to determine the cause. Consult with the VPLEX Remote Support team to verify |

| | | | |
|---|---|---|---|
| | | | that the cause and any required mitigations are understood before proceeding with a hardware or software upgrade. |
| sfp/7 | Any number in last 3 days | The SFP is either missing, inserted incorrectly, or faulty. | A call-home should have been sent for this event if call-home was enabled on the system. DELL EMC Customer Service needs to either replace the SFP or verify that it's been inserted properly and now functioning correctly. Verify that DELL EMC Customer Service has verified the health of the SFP or replaced it prior to proceeding with a hardware or software upgrade. |
| sfp/8 | Any number in last 3 days | The port is equipped with an SFP with an unrecognized part-number. | DELL EMC Customer Service needs to replace the SFP with an approved part. A call-home should have been sent for this event if call-home was enabled on the system. Verify that DELL EMC Customer Service has replaced the SFP before proceeding with a hardware or software upgrade. |
| sfp/9 | Any number in last 3 days | The port is equipped with an SFP which is not approved by DELL EMC. | DELL EMC Customer Service needs to replace the SFP with an approved part. A call-home should have been sent for this event if call-home was enabled on the system. Verify that DELL EMC Customer Service has replaced the SFP before proceeding with a hardware or software upgrade. |
| sfp/11 | Any number in last 3 days | An FC port's RX/TX power has surpassed the warning threshold. | 1] For RX power issues the hardware attached to this port needs to be carefully investigated, and the switch port SFP and cable need to be re-seated, cleaned, and swapped as needed. 2] For TX power issues contact DELL EMC Customer Service to replace the SFP. If call-home is enabled on the system a call-home should have been sent for this event. Verify that DELL EMC Customer Service has |

| | | | |
|---|---|---|---|
| | | | addressed it prior to proceeding with a hardware or software upgrade. |
| sfp/12 | Any number in last 3 days | An FC port's RX/TX power has surpassed the alarm threshold. | 1] For RX power issues the hardware attached to this port needs to be carefully investigated, and the switch port SFP and cable need to be re-seated, cleaned, and swapped as needed. 2] For TX power issues contact DELL EMC Customer Service to replace the SFP. If call-home is enabled on the system a call-home should have been sent for this event. Verify that DELL EMC Customer Service has addressed it prior to proceeding with a hardware or software upgrade. |

# Other Tool Functions

## GenU CCA Command Collection

DELL EMC Global Services requires a set of commands be run on a VS2 system for the GenU Change Control Authorization (CCA) process. The output of these commands is to be reviewed by the CCA reviewer prior to the GenU.

The tool automates the collection of the command output, and prints it to the log file produced by the tool (file named C*x*_<*last4TLA*>.log – where x = cluster-1/cluster-2, and last4TLA = the last 4 digits of the VPLEX TLA). The following will be printed to the log file, followed by the output of the commands:

*Collecting the output of the commands required for the GenU CCA Process for a VS2…*

## NDU CCA Command Collection

DELL EMC Global Services requires a set of VPlexcli commands be run for the NDU Change Control Authorization (CCA) process. The output of these commands is to be reviewed by the CCA reviewer prior to the NDU. A smaller set of VPlexcli commands is also required to be collected on the day of the scheduled NDU. Review the README for the CCA command collection options and the lists of VPlexcli commands related to each.

The tool automates the collection of the command output, and prints it to the log file produced by the tool (file named C*x*_<*last4TLA*>.log – where x = cluster-1/cluster-2, and last4TLA = the last 4 digits of the VPLEX TLA). The following will be printed to the log file, followed by the output of the commands:

*Collecting the output of the commands required for the NDU CCA process:*

**NOTE:** All commands are executed regardless of the platform/product configuration type, so some commands may expectedly fail (such as 'vpn status' on a VPLEX Local), or produce no output. Problems with director connectivity can also result in command failures.