

Dell EMC Metro node 8.0 Events and Alerts

Reference Guide

8.0

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: Events and Alerts.....	4
UI overview.....	4
Platform alerts.....	4
Hardware alerts.....	6
iDRAC alerts.....	6
Monitor alerts.....	7
Alert states.....	8
Scope of the events.....	8
Sorting and filtering alerts.....	9
Download .csv.....	9
Default and hidden columns	9
Live alerts.....	9
Alerts roll-up.....	10
Historical alerts.....	10
Alerts on remote director.....	11
Configure alerts.....	11
Disable or enable platform alerts.....	11
Disable or enable hardware alerts.....	12
Disable or enable alerts based on the component group.....	12
Disabling notifications.....	13
Service Monitoring Alert.....	14
Test alerts for platform, monitor, and SMS.....	14
Heartbeat alerts.....	15
Mail notification.....	15
Configure emailing notification.....	16
Test email alert.....	16
Supported events.....	17
Supported platform event.....	17
Supported metro node monitor events.....	67
Supported iDRAC events.....	67
Index.....	70

Events and Alerts

Topics:

- [UI overview](#)
- [Platform alerts](#)
- [Hardware alerts](#)
- [Alert states](#)
- [Scope of the events](#)
- [Sorting and filtering alerts](#)
- [Download .csv](#)
- [Default and hidden columns](#)
- [Live alerts](#)
- [Alerts roll-up](#)
- [Historical alerts](#)
- [Alerts on remote director](#)
- [Configure alerts](#)
- [Service Monitoring Alert](#)
- [Test alerts for platform, monitor, and SMS](#)
- [Heartbeat alerts](#)
- [Mail notification](#)
- [Configure emailing notification](#)
- [Test email alert](#)
- [Supported events](#)

UI overview

Events provide information about changes happening to the system, and it indicates that there is a problem with the system. Alerts are events that require attention from the System Administrator or User. Most alerts indicate that there is a problem with the system, and it must be rectified to attain the best performance from the system. In the dashboard, the metro node notifications system displays live and historical alerts for Platform and Hardware that requires attention from the user, and it also helps through monitoring the state of the various components, triage, and troubleshooting issues. On the **Notification** tab, there are two tabs:

- Platform Alerts
- Hardware Alerts

Platform alerts

You can monitor the status of metro node platform, and it includes alerts at director level and cluster level. You can view alerts that were created during the last 48 hours (by default).

The metro node alerts are of two types: Operational and Alarms.

Information associated with a platform alert

See the following information:

Column	Description
Severity	<p>Indicates the urgency of alert:</p> <ul style="list-style-type: none"> ● CRITICAL-A condition has occurred that can obstruct the functionality or can lead to failure of the other components. ● ERROR-An error has occurred that has a significant impact on the system and must be rectified immediately. ● WARNING-An error has occurred that you should be aware of but does not have a significant impact on the system. For example, a component is working, but its performance may not be optimum. ● INFO-An event has occurred that does not impact system functions. No action is required. ● CLEAR-When a corresponding clear event is generated for the raised alert which represents the issue is resolved at the system level.
State	<p>Represents the state of the alert-OPEN, CLOSED, or ACK state.</p> <p>OPEN-The alert is active and no action has been taken on it. The alert generating condition still persists in the system. If the system administrator wants to reopen to pay attention to that event, the alert status can also be changed to open from acknowledge state.</p> <ul style="list-style-type: none"> ● To reopen an alert: Select the checkbox corresponding to the alert, and then click OPEN. <p>ACK-After you view an alert and understand its contents, you can acknowledge that you have read through the alert message.</p> <ul style="list-style-type: none"> ● To acknowledge an alert: Select the checkbox corresponding to the alert, and then click ACKNOWLEDGE . <p>CLOSED-Once, the problem condition is resolved, the event state is updated as closed. Once closed the alerts cannot be reopened.</p> <ul style="list-style-type: none"> ● To close an alert: Select the checkbox corresponding to the alert, and then click CLOSE.
Message	Indicates the cause of an event for which the alert is generated.
Alert ID	Represents the unique ID assigned to each alert.
Description	Describes the platform alert.
Corrective Action	Action to eliminate the cause of event.
Scope	Represents the level of alert-Cluster or Director.
Condition ID	Indicates Unique ID of all defined alert definitions.
Component	System component that caused the event. Intended for service personnel.
Event Source	Represents the context of the event. For example, Virtual Volume.
Event Source ID	Unique ID for the source of the event. Helps to narrow down to the final component.
Resource	Represents the actual resource for which the issue has occurred.
Count	It represents the number of times the same alert is generated over the selected period. This column is available for historical alerts only.
Creation Date (UTC)	Date and time when the alert got generated.
Last Updated (UTC)	Date and time when the status of the alert is last changed.
External RCA	Represents the external Root Cause Analysis of the issue.
Additional Details	Display more data received along with the alert.
User Note	It shows the notes which are added through user.

Platform alerts contains two type of data-Static and Dynamic. The static data are read from `firmware_event.yaml(/etc/opt/dell/vplex)` and the dynamic data read from payload.

Hardware alerts

iDRAC alerts

For a corresponding iDRAC or hardware event, the notification service generates alert.

You can monitor the status of metro node hardware that includes alerts that are generated at hardware level. You can view alerts that were created during the last 48 hours (default).

In the details of each alert, you can see more information including Severity, Message, and other properties. This information is useful in troubleshooting scenarios and allows users to remediate issues seen on the system. For more information about a particular iDRAC alert, log in to appropriate iDRAC. To log in to iDRAC UI, either you can click the **iDRAC GUI** button available below the main title bar or you can directly log in to the iDRAC UI.

Information associated with a iDRAC Alert

See the following information:

Column	Description
Severity	Indicates the urgency of alert: <ul style="list-style-type: none">● CRITICAL- An error has occurred that has a significant impact on the system and must be rectified immediately. For example, a component is missing or failed, and recovery may not be possible.● WARNING-An error has occurred that you should be aware of but does not have a significant impact on the system. For example, a component is working, but its performance may not be optimum.
State	Represents the state of the alert-OPEN, CLOSED, or ACK state. OPEN -The alert is active and no action has been taken on it. The alert generating condition still persists in the system. If the system administrator wants to reopen to pay attention to that event, the alert status can also be changed to open from acknowledge state. <ul style="list-style-type: none">● To reopen an alert: Select the checkbox corresponding to the alert, and then click OPEN. ACK -After you view an alert and understand its contents, you can acknowledge that you have read through the alert message. <ul style="list-style-type: none">● To acknowledge an alert: Select the checkbox corresponding to the alert, and then click ACKNOWLEDGE . CLOSED -Once, the problem condition is resolved, the event state is updated as closed. Once closed the alerts cannot be reopened. <ul style="list-style-type: none">● To close an alert: Select the checkbox corresponding to the alert, and then click CLOSE.
Message	Indicates the cause of an event for which the alert is generated.
Severity code	It represents the numerical code for the corresponding severity of the alert.
Version	Indicates certificate version.
Category	Indicates event category. For example, System.
Message ID	Indicates ID of the event record.
Condition ID	Indicates Unique ID of all defined alert definitions.
Count	It represents the number of times the same alert is generated over the selected period. This column is available for historical alerts only.
App Name	It represents the device or application that originated the message.
Host Name	It represents IP address or network name of the remote host.
Creation Date (UTC)	Date and time when the alert got generated.

Column	Description
Last Updated (UTC)	Date and time when the status of the alert is last changed.
User Note	It shows the notes which are added through user.

Monitor alerts

Monitor alerts alert the customer if there are specific use cases. These alerts are there to keep a watch on the hardware functionality. Monitor alerts are generated for the following scenarios:

- If any of the storage partitions becomes 80% full.
- If any of the storage partitions becomes 90% full.
- If the peer node is not pingable.
- If the iDRAC is unresponsive.
- If the system clock of any node deviates by more than three seconds.
- If the NSFW crashes.

Information associated with a Monitor Alert

See the following information:

Column	Description
Severity	<p>Indicates the urgency of alert:</p> <ul style="list-style-type: none"> • CRITICAL- An error has occurred that has a significant impact on the system and must be rectified immediately. For example, a component is missing or failed, and recovery may not be possible. • WARNING-An error has occurred that you should be aware of but does not have a significant impact on the system. For example, a component is working, but its performance may not be optimum.
State	<p>Represents the state of the alert-OPEN, CLOSED, or ACK state.</p> <p>OPEN-The alert is active and no action has been taken on it. The alert generating condition still persists in the system. If the system administrator wants to reopen to pay attention to that event, the alert status can also be changed to open from acknowledge state.</p> <ul style="list-style-type: none"> • To reopen an alert: Select the checkbox corresponding to the alert, and then click OPEN. <p>ACK-After you view an alert and understand its contents, you can acknowledge that you have read through the alert message.</p> <ul style="list-style-type: none"> • To acknowledge an alert: Select the checkbox corresponding to the alert, and then click ACKNOWLEDGE . <p>CLOSED- Once the problem condition is resolved, the event state is updated as closed. After it is closed, the alerts cannot be reopened.</p> <ul style="list-style-type: none"> • To close an alert: Select the checkbox corresponding to the alert, and then click CLOSE.
Message	Indicates the cause of an event for which the alert is generated.
Severity code	Represents the numerical code for the corresponding severity of the alert.
Version	Indicates certificate version.
Category	Indicates event category. For example, System.
Message ID	Indicates ID of the event record.
Condition ID	Indicates Unique ID of all defined alert definitions.
Count	Represents the number of times the same alert is generated over the selected period. This column is available for historical alerts only.

Column	Description
App Name	Represents the device or application that originated the message.
Host Name	Represents the IP address or network name of the remote host.
Creation Date (UTC)	The date and time when the alert got generated.
Last Updated (UTC)	The date and time when the status of the alert is last changed.
User Note	Shows the notes which are added through user.

Alert states

The alerts can be in any of the following states:

OPEN

It represents the state when an alert has been raised. When the alert is raised, the state remains open until the user closes or acknowledges it from the UI, or the system generates a clear event that represents the issue has been resolved.

CLOSED

The user can move an alert to closed state after resolving the issue, or the system generates a clear event that represents the issue has been resolved.

If the alert is closed from the UI, then its state changes to CLOSED, and the Last Updated time is updated but the severity remains the same.

If the platform alert is closed through a system-generated event, then its severity changes to CLEAR along with the state change to CLOSED, and the Last Updated time is updated.

The Operational Alerts are closed automatically after four hours. If node or director reboots, or NDU is performed within this four hours interval, then Operational Alerts remain open even after four hours.

The Hardware alerts state change to closed state after moving to historical alerts.

ACK

Once the user feels that the message has been checked and there are no functional consequences because of the issue, then the user can move an OPEN alert to the ACK state. Acknowledging an alert does not indicate that the issue has been resolved, but it means that the user is aware to bear the consequences caused through the underlying issue with that alert.

Scope of the events

This property is limited to the platform alerts, and the scope of the events is categorized as:

- Director Scope
- Cluster Scope

Cluster scope-The cluster scope events are published only through one director which is the publisher. So, the cluster scope alerts are seen only on the publisher at both the clusters. It means that only one director at each cluster shows these cluster level alerts. If the publisher faces a node restart, then the other node becomes the publisher, and continue to serve as publisher even after the previous node comes up.

Director scope-The director scope alerts can be seen on any of the nodes with respective director names as the component.

Change of publisher

There is a unique ID assigned to each of the directors and cluster. It is internally termed as scope incarnation.

For Platform alerts, whenever there is a change in scope incarnation value for the events, then all the director scope alerts with the previous scope incarnation value are closed on that node.


Scope Incarnation value for director changes when the node of the metro node or firmware is restarted. The cluster scope incarnation values change when both the nodes are restarted on the cluster.

- If there is change in scope incarnation for alert with scope as **DIRECTOR**, then all the alerts (**OPEN** or **ACK**) with scope **DIRECTOR** are closed on the node after the first supported event with the new incarnation value reaches the notification service.
- If there is a change in scope incarnation for alert with scope as **CLUSTER**, then all the alerts (**OPEN** or **ACK**) with scope **CLUSTER** are closed on the node after the first supported event with the new incarnation value reaches the notification service.

Sorting and filtering alerts

To make the search easier among the listed alerts, the user has been provided with sorting on all the columns where the user can sort the alerts in ascending or descending order that is based on the type of that column.

To make the search easier, the filter operation is also provided. The user can filter the alerts depending on the type of columns except for the date columns. The date filter operation is part of historical alerts, and there you can have various filter operations on date.

 **NOTE:** The filter operation is case-sensitive.

Download .csv

The notifications service provides an option to the user to download the listed alerts in a .csv file.

The user can also apply filters on the listed alerts and get only the filtered alerts in the .csv file.

Default and hidden columns

By default, only the major fields are added to the alerts grid, but the user has the option to add all the columns or any of the hidden columns.

The user can also reset the columns to default where only the default columns can be seen.

Live alerts

Live alerts represent the alerts that are generated within the window of last 48 hours. The records are up to 48 hours, but an hour buffer window is taken which is then doubled through the timescale. So, it becomes a two-hour buffer window.

Live Platform Alerts- At any time, there is only one alert in UI related to a particular resource for a given **condition_id** associated with the type of alert.

Live Hardware Alerts- There is a separate entry for each hardware alert generated. The Last updated is not updated for hardware alerts.

Live alerts retention

The Live alerts are retained for an interval of 48 hours before adding to the historical alerts.

Alerts roll-up

Alerts roll-up is the process of consolidating the alerts based on the circumstances that are possessed at the time of generation of platform alerts and at the time of moving the live alerts to historical alerts. As of now, the roll-up is applicable only for the platform alerts.

The roll-ups are at two different places:

Live alerts roll-up for platform alerts

The roll-up of alerts happens if there are multiple alerts that are generated for the same condition ID within a span of 30 sec interval. In 30 seconds window, the initial five events generate as many alerts, and the later events are rolled up and generate a single alert depicting the number of times the event occurred.

Closing of rolled-up alerts (automatically through system)-If the clear rolled-up alerts generate for these rolled-up alerts, then these rolled-up alerts can be closed. If system generated clear events are received more than five within the 30 seconds window, then clear roll-up alert is generated.

Alerts roll-up if the notifications service was down

If the notification service is down momentarily, and some events are generated gradually during that time, then on the service restart, it processes all the events, and the same roll-up logic is applied as the events are consumed through the service from broker within 30 seconds.

Historical alerts

Historical alerts provide a view to the user to look into the occurrences of the particular alerts in the past. Historical alerts contain the consolidated data of the generated alerts over a period of last six months. The alerts are aggregated and stored in the historical table. The user has been provided with default filters for the 7 Days, 14 Days, and 30 Days. These filters include the data for the number of days in the filters along with the current day data. For example, Last 7 Days data contains the data for last 7 days and the current days.

Customized date filter

The custom dates filter is provided where user can get data for a customized interval. That customized date filter contains the data from 00:00:00 hours start date to 23:59:59 hours end date. For example, if the start date is selected as 1 Jul 2020 and end date as 15 Jul 2020, then user sees the alerts from Jul 1 00:00:00 hours to Jul 15 23:59:59 hours.

Aggregation for alerts

While adding to the historical alerts, the platform alerts with the same Condition ID, Resource and State are aggregated as one with the addition of a column **Count** which represents the number of times that particular alert is generated in the time window filter which the user has applied.

The hardware alerts are aggregated based on the Message ID field with the addition of a column **Count** which represents the number of times that particular alert is generated. The logs field in the properties panel contains the creation date and last updated date for these occurrences. The rolled-up live alerts are stored as in historical alerts table as these alerts are already rolled-up.

A single row represents an alert with its particular state (OPEN or CLOSED), number of occurrences on a given day, and whether it is enabled or disabled.

So, based on this scenario, a particular **condition_id** can have the following entries for the historical alerts:

- Enabled-OPEN rolled-up historical alert
- Enabled-CLOSED rolled-up historical alert
- Disabled-OPEN rolled-up historical alert

- Disabled-CLOSED rolled-up historical alert
- Entries for the Live alerts which got rolled-up

Alerts on remote director

User has option to view the alerts on the remote directors also. The director selection can be done from the drop-down option available on the alerts listing page.

These alerts on the remote director can be viewed, and the state change operation can also be performed on them.

The user can also disable the alert on the remote director. To disable the alert, selecting the alert on the alerts listing page, and then click the **Disable Alerts** button from the **MORE** drop-down.

Configure alerts

A feature is provided in the UI where user can configure the platform alerts that are to be received as per the requirement. The user can choose at multiple levels like for which component or condition Id the user wants to see the alerts.

Disable or enable platform alerts

A user can disable or enable alerts at multiple levels:

- Condition ID level
- Component level
- Disabling Notifications

Disabling the alerts from UI means that the user does not want to see the alerts in the UI, but it does not mean that the generation of the alert is stopped. The alerts keep on generating and are stored in the database.

Condition ID level

The alerts can be disabled at the condition ID level which means that the future alerts that are associated with that particular condition ID are not displayed in the UI.

Steps:

1. In the UI, go to the **Settings**.
2. Select **Notifications** from drop-down. The **Configure Alerts** page is displayed.
3. To select the alert configuration from the list, select the check box .
4. Select the **Disable Alerts** from the **MORE** drop-down.
5. A **Disable Alert Confirmation** window is displayed, click **YES** to disable the selected alert.

If user enables it again, then it starts showing up future alerts that are associated with the condition ID in the UI.

Component level

The alerts can be disabled at the component level which means that the future alerts that are associated with that particular component are not displayed in the UI.

Steps:

1. In the UI, go to the **Settings**.
2. Select **Notifications** from drop-down. The **Configure Alerts** page is displayed.
3. Click the **CONFIGURE NOTIFICATIONS** button. A **Configure Notification** window is displayed.
4. In the **Platform Alerts** section, to disable the particular component, switch the button, and then click **CLOSE** to close the window.

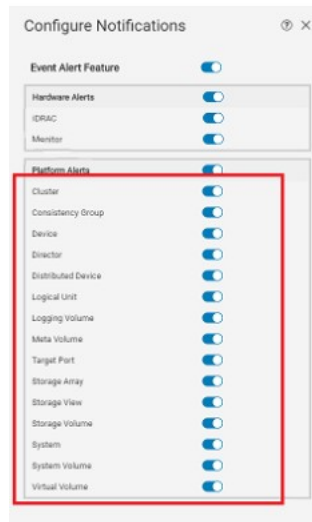


Figure 1. Disabling particular component of platform alerts

If user enables it again, then it starts showing up future alerts that are associated with the component level in the UI.

Disable or enable hardware alerts

In hardware alerts, user can disable the entire iDRAC alerts or Monitor alerts or both.

Steps:

1. In the UI, go to the **Settings**.
2. Select **Notifications** from drop-down. The **Configure Alerts** page is displayed.
3. Click the **CONFIGURE NOTIFICATIONS** button. A **Configure Notification** window is displayed.
4. In the **Hardware Alerts** section, to disable the particular component, switch the button, and then click **CLOSE** to close the window.

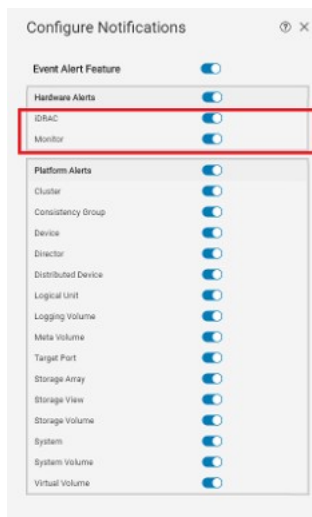


Figure 2. Disabling particular component of hardware alerts

If user enables it again, then it starts showing up future alerts that are associated with the hardware alerts in the UI.

Disable or enable alerts based on the component group

The alerts can be disabled at the component group level which means that the alerts associated with all components of that component group are not displayed in the UI.

There are two component groups: Platform alerts and Hardware alerts. The user can disable either of them or both as well.

Steps:

1. In the UI, go to the **Settings**.
2. Select **Notifications** from drop-down. The **Configure Alerts** page is displayed.
3. Click the **CONFIGURE NOTIFICATIONS** button. A **Configure Notification** window is displayed.
4. To disable the **Platform Alerts** or **Hardware Alerts** or both, switch **Platform Alerts** button, or **Hardware Alerts** button, or both buttons as shown in the following figure, and then click **CLOSE** to close the window.

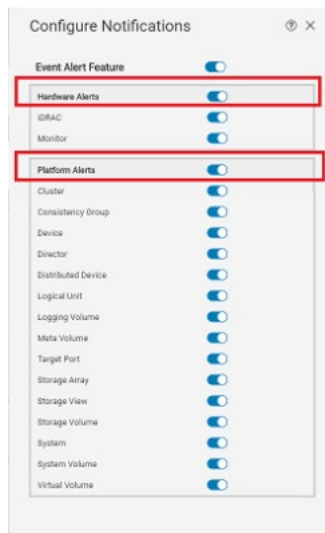


Figure 3. Disabling alerts

If user enables it again, then it starts showing up future alerts that are associated with the hardware alerts and platform alerts in the UI.

Disabling notifications

The entire notifications can be disabled, and user cannot see any future alerts in the UI.

Steps:

1. In the UI, go to the **Settings**.
2. Select **Notifications** from drop-down. The **Configure Alerts** page is displayed.
3. Click the **CONFIGURE NOTIFICATIONS** button. A **Configure Notification** window is displayed.
4. To disable the entire notifications, switch the **Event Alert Feature** button as shown in the following figure, and then click **CLOSE** to close the window.



Figure 4. Disabling entire notifications

If user enables it again, then it starts showing up future alerts that are associated with the hardware alerts and platform alerts in the UI.

Service Monitoring Alert

If any monitoring service is stopped or failed at any given time, the service monitoring alert is generated. Under Notifications, this alert is displayed in the monitor window of metro node inside. Initially, the severity of the alert is **Warning**. If the service is down for more than 5 minutes, then the severity is changed to Critical.

This alert has following states:

- OPEN- If the service is inactive, then the state of alert is OPEN.
- CLOSED-If the service is activated, then the state is changed to CLOSED and severity is changed to CLEAR.

Enable monitoring service

To enable monitoring of any service, follow these steps:

1. Create a <service_name>.yaml file along with the RPM and put it into /etc/opt/dell/vplex/monitoring folder.

The format of the configuration file is as follows:

```
telegraf:
  id: SM-TELEGRAF
  name: telegraf
  corrective_action: 'Please check the logs for more details.'
  enabled: true
  is_notification_stack: false
```

To generate the alerts, the field **enabled** must be true.

If the field **is_notification_stack** is false, only then the event is sent to the kafka else it logs only into the journalctl. For now, it is true for kafka, notification, and postgresql services.

2. Before starting the **vplex-service-monitor.service**, put the configuration file into the folder.
3. To verify the **vplex-service-monitor.service** has picked up the configuration file and started monitoring, see the file **services.yaml** under **/etc/opt/dell/vplex/**. If the file contains the service details, then the service is monitored.

Test alerts for platform, monitor, and SMS

Test alerts confirm the functionality of the notifications service. When user clicks the **Test Alerts** button, then three type of test alerts (Platform, Monitor, and SMS) generate, and that confirms the flow of the events to alerts.

The user has been provided with the option to disable the test alerts. If one of the test alerts is disabled, then that alert is not displayed in the UI, but it is stored in the database.

If both the alerts are disabled, then none of the test alerts are generated. If SMTP is configured, then TEST mail is also generated to the provided email address.

Steps to generate Test Alerts

1. In the UI, go to the **Settings**.
2. Select **Notifications** from drop-down. The **Configure Alerts** page is displayed.
3. Select the **Test Alerts** from **MORE** drop-down.

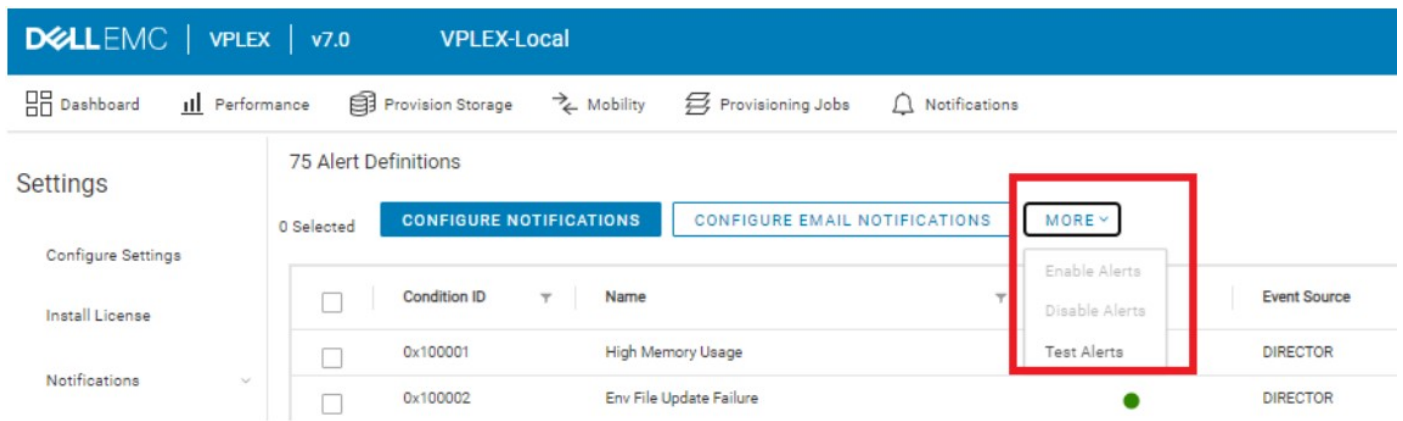


Figure 5. Selecting the Test Alerts

4. A confirmation window is displayed, select the type of alert-Platform, Monitor, and SMS.
5. A **Test Alert Result** window is displayed, click the **CLOSE** to close the window.

Ensure that when you generate the test alerts, the previous test alerts are closed. If the previous test alerts are not closed, then those alerts can be closed from the live alerts listing page.

If you view the remote director's alert from UI and you go to **Configuration Alerts** page and generate test alerts, then it generates the test alerts only for the director IP you are logged on to and NOT on the remote director.

Heartbeat alerts

Heartbeat alerts are generated in an interval of every 5 minutes if no communication from the director or any of the components of the working stack is failed. Heartbeat alerts are of **CRITICAL** severity and have **0x0000** condition ID.

Disabling the notification service does not display the heartbeat alert in the UI.

It generates in three conditions:

1. Kafka down
2. Nsfw down
3. Telegraf down

SupportAssist heartbeat

- **conditionId 0x0001**-This alert generates if DC is not communicating with notifications for more than 5 minutes. This alert is with severity **CRITICAL**.
- **conditionId 0x0002**-This alert generates if DC is configured and the payload validation fails (in all condition except `current_connection_state=enabled & last_five_min_success_rate >= threshold & last_hour_min_success_rate >= threshold`) .

If the **current_connection_state** is enabled and the heartbeat is 0, then there is no requirement to create any alert. This alert is with severity **ERROR**.

Threshold value is configured, and the configuration file is present under `/etc/opt/dell/vplex/notification/` folder. This file `notification.conf` gets installed along with notification RPM in all the nodes.

After changing the value from next alert, it considers the new value as the threshold. No service restart is required.

If the configured value is invalid or the file is not present, then the default value 0.5 is used as the threshold.

Mail notification

The notification service provides users to receive the email messages for the generated alerts. So, it is more accessible to get the alerts at odd times also. The mail is sent for all raised alerts, and there is not any mail that is generated for the closed

alert. User can also send the alert notifications to a specified email or SMTP server. To configure SMTP server, see *System Configuration guide* available at SolVe (<https://solve.dell.com/solve/home/30>).

Configure emailing notification

You can disable the notification emailing as a whole, or you can also disable the Email notifications for platform, iDRAC, or monitor alerts individually.

Under **Configure Alerts** page, this configuration is provided where you can enable the mails only for the required alerts.

Procedure to disable email notifications

Follow these steps:

1. In the UI, click the **Settings**.
2. Select **Notifications** from the drop-down.
3. Click the **CONFIGURE EMAIL NOTIFICATIONS** as shown in the following figure:

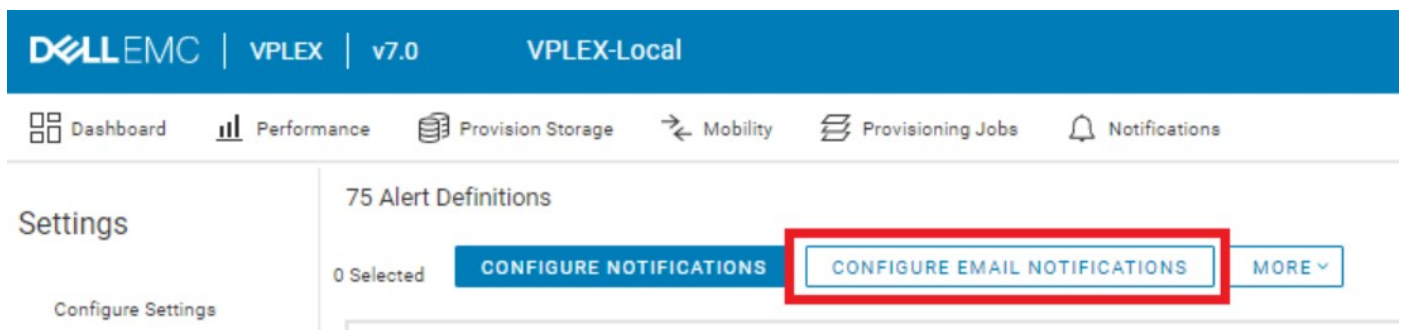


Figure 6. Configure email notifications

4. To disable the email notifications for required component, switch the button of that component. You can disable the entire emailing feature through switching the **Email Notification Feature** button.

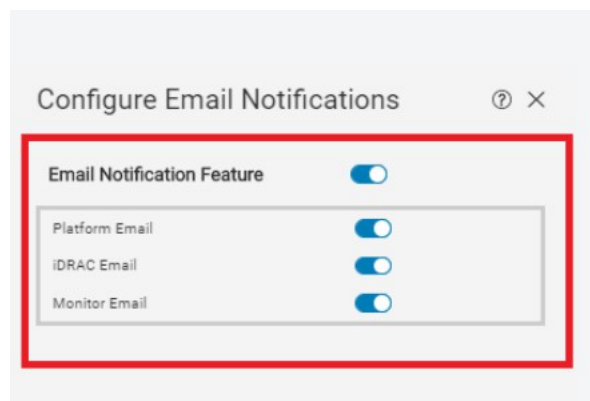


Figure 7. Disable email notifications feature

Test email alert

Test email alert confirms the functionality of the email notification feature of the notifications service. Once the Test Email Alert option is clicked, then an email alert goes to the respective configured email ID.

NOTE: If **Email Notification** feature is not enabled, then selection of **Test Email Alert** is disabled for a user.

1. From the UI, go to the **Settings > Notifications** or go to the **Notifications > Platform Alerts > MORE > Configure Alerts**. The **Configure alerts** page is displayed.
2. Select **MORE > Test Email Alert**. An email alert is sent to the respective configured email ID.

Supported events

Supported platform event

See the following table:

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x100001	floor/31	0x8a18901f	CRITICAL	True	High Memory Usage	Memory usage on this director exceeds the threshold.	Either a memory leak has occurred or the VPLEX has exceeded its configuration limits.	Contact Dell EMC Customer Support.	DIRECTOR	Operational
0x100002	floor/32	0x8a186020	ERROR	True	Env File Update Failure	An update to an internal environment file failed.	An update to an internal environment file failed.	Contact Dell EMC Customer Support.	DIRECTOR	Operational
0x10001	--	--	CRITICAL	True	Director Scope Test Alarm	TEST: This is an example director scope alarm message.	This is an example RCA for the director-scope test alarm.	This is an example external remedy for the director-scopetest alarm.	DIRECTOR	Alarm
0x10006	--	--	CRITICAL	True	Director level Test Operational Alert	TEST: This is an example director scope alarm message.	This is an example RCA for the director-scope operational test event.	This is an example external remedy for the director-scope operational test event.	DIRECTOR	Operational
0x110001	ipc/18, ipc/19, ip/2, ip/3	0x8a450012, 0x8a450013	WARNING	True	IP Interface State Change	The IP port state has changed.	Link went down on a port. Depending on the port role, a physical path to local or remote cluster has been lost.	Link went down on a port. Depending on the port role, a physical path to the local or remote cluster has been lost. Perform the following steps: 1. Check the state of the port, and ensure that it is enabled. 2.	IPPORT	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								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 Dell EMC Customer Support.		
0x20001	scsi/156, scsi/157	0x8a2d609c, 0x8a2d009d	CRITICAL	False	Array No Access	Storage Array is not seen by this director.	Storage Array is not reachable by this director.	Check for faulty hardware: verify the health of the cables, backends and switches and array. Contact Dell EMC Customer Support if the problem persists	ARRAY	Alarm
0x20002	scsi/72, scsi/73	0x8a2d0048, 0x8a2d0049	ERROR	False	Unreliable ITNexus Banished	The IT nexus has been automatically taken out of service (banished) due to poor reliability in order to prevent performance impact.	The Initiator-Target connection is failing and is out of service. Once the reliability improves the VPLEX will automatically resume using it.	Check for faulty hardware: verify the health of the cables, backends and switches and array. Contact Dell EMC Customer Support if the problem persists	ITNEXUS	Alarm
0x20003	--	--	CRITICAL	False	Array Cluster Wide Redundant Access Loss	The storage array is not accessible either from n-1 (or) n directors.	The storage array is not accessible from all directors in the cluster.	Check for faulty hardware: verify the health of the cables, backends and switches	ARRAY	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								and array. Contact Dell EMC Customer Support if the problem persists		
0x20004	scsi/154, scsi/166	0x8a2d309A, 0x8a2d00a6	WARNING	False	Unit Busy Condition	The logical unit is busy more often than is normal and may impact performance.	The array has returned the SCSI BUSY status to VPLEX IO requests for this storage volume more often than what is considered acceptable.	The cause of busy condition on the storage array should be investigated. Investigate the health of the storage array, backend fabric and VPLEX backend port to determine the source of the issue. Contact Dell EMC Customer Support if there are performance problems.	LOGICAL UNIT	Alarm
0x20005	scsi/126	0x8a2d307e	WARNING	False	Unit ALUA Support Inconsistent	ALUA support is incorrectly configured on LU.	An inconsistent ALUA support level has been detected for logical unit.	Check the ALUA configuration on the array. All paths to logical unit should be configured with the same failover mode.	LOGICAL UNIT	Alarm
0x20006	scsi/71	0x8a2d6047	ERROR	False	Unit Path Type Inconsistent	A Logical Unit reported an inconsistent path type for the array. Recovery attempts failed and the unit has been banished.	A logical unit has inconsistent path types. Exhausted attempts to correct this via refresh and have banished the unit.	Engage the array vendor or Dell EMC Customer Support to investigate why the logical unit has inconsistent path types.	LOGICAL UNIT	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x20007	scsi/79	0x8a2d304f	WARNING	False	Array Not Supported SPC Version	Array supports an SPC version NOT matching 2, 3 or 4.	Target device advertised a behavior which is not supported by the VPLEX initiator.	Switch the target device into a supported mode following VPLEX best practices for this device, do not use this target device, or the device may be less highly available than is recommended for normal operation.	ARRAY	Alarm
0x20008	scsi/91	0x8a2d605b	ERROR	False	Array Exceeds Max Controller	Array exceeds maximum number of controllers allowed.	Logical Unit already has maximum controllers allowed on this array. Extra controller is being attempted to be added.	Check Array configuration. If problem persists, contact Dell EMC Customer Support.	ARRAY	Alarm
0x2000a	scsi/158	0x8a2d309e	WARNING	False	Array Serial Number Unexpected	Storage Array returned an unexpected serial number.	The storage array reported an unexpected serial number.	Before using this array, check the storage-arrays context to ensure that multiple entries do not have the same identifier, and that this array does not present multiple identifiers. If either of these conditions occur, do not use this array. The array name and version number should be	ARRAY	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								reported to Dell EMC Customer support. Continuing to use the array could lead to Data Unavailability and Data Loss conditions and unreliable array behavior.		
0x2000b	scsi/147	0x8a2d6093	ERROR	False	Logical Unit Changed	Logical Unit mapping change detected. For this ITL, a different Logical Unit is reported than what was reported earlier.	LU mapping on the storage array had changed. Depending on the state of the system (host I/Os running or not), either Data Unavailable, Data Loss or Data Corruption might have already happened or might happen in future.	The system will automatically run a refresh to destroy the stale ITL to the old LUID and re-discover the ITL to the new LUID. Always follow the 'Remove Disk or Array' procedure in the VPLEX Solve Desktop when de-provisioning storage-volumes and/or re-provisioning storage-volumes to VPLEX to ensure an 'array re-discover' is run in between changes in order to prevent LUN swapping from occurring.	ITL NEXUS	Alarm
0x2000c	apf/15	0x8a04900f	ERROR	False	Array No Failover	No suitable executor director to	This is likely indicative of severely	Check the backend switches,	ARRAY	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
					Executor Director	perform the failover of a group of Logical Units to a specific array controller.	degraded hardware and/or fabric condition. Restore connectivity to the array controllers for all directors.	and engage the array vendor to investigate why the failover to the array controller could not succeed. Contact Dell EMC Customer Support if problem persists.		
0x2000d	scsi/138	0x8a2d608A	ERROR	False	Unit Reservation Conflict	Reservation conflict response for command sent to the logical unit on a specific IT.	The logical unit is reserved by another initiator.	Contact your storage administrator to remove the reservation of the logical unit from either the initiator(s) or storage array.	LOGICAL UNIT	Alarm
0x2000e	scsi/167	0x8a2d60a7	ERROR	False	Scsi Deferred IO Error	Received deferred error from a specific target for a previous command.	VPLEX received deferred error from the specified target which indicates exception condition occurred on the target during processing of some previous command for which status was already returned. This can lead to Data Unavailability /Data Loss.	Determine which backend storage array the target corresponds to, and then engage the storage array vendor's Customer Support to determine the cause of the deferred error and to correct the exception condition on the target.	TARGET	Alarm
0x2000f	scsi/161	0x8a2d30a1	ERROR	False	Inquiry Not Ready	INQUIRY data not yet ready. Skipping discovery on itlNexus.	An array returned empty INQUIRY data. Device not ready for discovery.	Run array re-discover for this array. New LUNs will now be listed.	LOGICAL UNIT	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x20010	scsi/162	0x8a2d30a2	WARNING	False	VPD Parameters Outside Scope	The array did not return a VPD peripheral qualifier status of Connected. Device may be not ready for discovery.	The array did not return a VPD peripheral qualifier status of 'Connected'. Device may be not ready for discovery.	Run array re-discover for this array. New LUNs will now be listed. If this event is persistent, engage the array support team to investigate why it did not return a VPD peripheral qualifier status of 'Connected' in the Inquiry Response.	LOGICAL UNIT	Operational
0x20011	scsi/122	0x8a2d607a	ERROR	False	New Device Type Reported	New device type reported for LU type was oldPdType, now reported as newPdType.	Unexpected change in device type for a backend Logical Unit.	Verify if the associated storage-volume is operational on the VPLEX, and investigate the cause of the unexpected change in type from the storage array. If the issue persists and unable to determine the cause engage Dell EMC Customer Service.	LOGICAL UNIT	Operational
0x20012	scsi/70	0x8a2d6046	ERROR	True	Scsi Memory Alloc Failure	Memory allocation failure of object in function.	Firmware memory allocation failure. Running out of memory resources.	Run the collect-diagnostics utility to collect system information to determine why an internal firmware memory	TARGET	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								allocation failure occurred. Please contact Dell EMC Customer Support.		
0x20013	scsi/169	0x8a2d90a9	CRITICAL	True	Scsi Thin Volume No Space On Write	Space allocation failed on scsi vol.	Allocation has failed on the thin-enabled storage-volume. There are no more available storage blocks on the BE array to map to the address to which the host has issued a write command.	The host administrator can try reclaiming storage using the scsi UNMAP command from the host. If reclaimed storage is not sufficient, the storage administrator must add free block storage to the BE storage array to increase the space available to the thin-enabled storage-volume. Once additional space is available host administrators can restart the hosts that are suspended/stopped.	TARGET	Operational
0x20014	scsi/36	0x8a2d0024	INFO	False	ITNexus Ready	IT Nexus is ready.	The scsi layer found an IT Nexus connection indicated by the tuple.	Contact Dell EMC Customer Support.	ARRAY	Operational
0x20015	scsi/68	0x8a2d3044	WARNING	False	Renew Retry Exceeded	Report luns command failing to get logical unit	The repeated failure could be due to any one of	Check if the array is a Hitachi, HP, SUN or HDS array, and if	ARRAY	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
						inventory on an IT Nexus.	the following:1. The director was unable to allocate any more memory,2. Attempts to get logical unit inventory were unable to complete.3. The REPORTLUNS command failed as there is no LUNID 0 provisioned to the VPLEX on the path from a Hitachi, HP, SUN or HDS array.	it is verify that each path from the array has a LUNID 0 exported to VPLEX. Reference the 'Configure Arrays' procedure in the VPLEX Solve Desktop. Investigate the health of the BE array. If the issue persists contact Dell EMC Customer Service.		
0x20016	scsi/146	0x8a203092	WARNING	False	Path Count Above Limit	The number of active paths on this director for the specified LogicalUnit is above the recommended limit.	The number of active paths on this director for the specified Logical Unit is above the recommended limit.	Reduce the number of paths to the recommended limit. Reference the VPLEX Best Practices document, available via the VPLEX Solve Desktop.	LOGICAL UNIT	Operational
0x20017	scsi/43, scsi/44	0x8a2d302b, 0x8a2d302c	WARNING	False	Port link is down	Port link is down.	The link is down between the specified VPLEX BE port and the switch.	Check the SFP, cable, and switch attached to this back-end port, especially anything that has been changed recently. Reseat/clean/replace the hardware as needed to	INTERFACE	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								resolve the problem. If the problem persists and unable to determine the cause contact Dell EMC Customer Support.		
0x20018	scsi/93	0x8a2d305d	WARNING	False	Single Path For LU	Path to a backend storage volume of an array is lost. VPLEX director has only one path to the LUN on the backend storage device.	VPLEX lost a path to a LUN from one director to an array. There is one path remaining. There might be a faulty hardware (cable, backend switch, array).	Verify reported array's BE disk health, LUN masking, array configuration and physical connection. If problem persists, contact Dell EMC Customer Support.	ARRAY	Operational
0x20019	scsi/80	0x8a2d9050	CRITICAL	False	Array Dev Type Not Interoperable	Storage Array has registered a Peripheral Device Type which is not interoperable with VPLEX.	The target device advertised a behavior which doesn't work with the VPLEX initiator.	Follow the 'Configure Arrays' procedure in the VPLEX Solve Desktop to ensure the storage is provisioned in a manner supported by VPLEX.	ARRAY	Operational
0x2001a	scsi/164	0x8a2d30a4	WARNING	False	Inquiry Peripheral Invalid	The array did not return a STD INQ peripheral qualifier of Connected. Device may be not ready for discovery.	The SCSI target device may be in the Unavailable state or not be capable of accessing the addressed logical unit from the addressed SCSI target port.	Run array re-discover for this array. New LUNs will now be listed. If this event is persistent, engage the array support team to investigate why the array did not return a STD INQ	ARRAY	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								peripheral qualifier of 'Connected'.		
0x2001b	scsi/170	0x8a2d30aa	WARNING	True	Thin Threshold Reached	A storage volume reported a Thin Provisioning Soft Threshold Reached error on a VPLEX write.	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 running out of space.	Add additional block resources to the thin pool on the array from which the storage-volume is provisioned.	LOGICAL UNIT	Operational
0x2001c	scsi/174	0x8a2d30ae	WARNING	False	Report Luns Retry Exhausted	Retry limit on successfully processing REPORT LUNS SCSI command response exceeded on an IT Nexus. VPLEX proceeds with processing as many LUs as it can.	Failure to successfully process REPORT LUNS SCSI command response could 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	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 Dell EMC Customer support.	ARRAY	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							VPLEX. 2. The array is reporting that it has fewer LUs 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.			
0x2001d	scsi/171, scsi/172, scsi/173	0x8a2d30ab, 0x8a2d30ac, 0x8a2d30ad	WARNING	False	Report Luns Data Mismatch	A specific IT Nexus reported specific number of logical units which did not match the total number of logical units.	The Logical unit inventory reported from an array is invalid. There is a mismatch between number of LUs that the array is reporting and the number of LUs that the VPLEX requested.	VPLEX will retry getting logical unit inventory. Collect VPLEX and Array logs and traces and contact Dell EMC Customer support.	ARRAY	Operational
0x30003	--	--	CRITICAL	True	Virtual Volume Redundancy Loss	Virtual Volume redundancy has changed.	One or more factors have contributed to changing the redundancy of the given virtual volume.	Contact Dell EMC Customer Support for assistance with restoring the redundancy of the virtual volume.	VIRTUAL VOLUME	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x30004	amf/45, amf/96, amf/97, amf/98, amf/99, amf/100, amf/101, amf/223	0x8a02302d, 0x8a029060, 0x8a029061, 0x8a026062, 0x8a026063, 0x8a020064, 0x8a020065, 0x8a0230df	WARNING	True	Storage Volume Unreachable	Storage Volume accessibility has changed.	A storage volume attached to the system can no longer service I/O.	If the storage volume is unreachable see Troubleshooting_Unreachable_Storage_Volumes.	STORAGE VOLUME	Alarm
0x30005	--	--	CRITICAL	True	System Device Redundancy Loss	The system device has regained full redundancy.	One or more factors have contributed to changing the redundancy of the given system device.	Contact Dell EMC Customer Support for assistance with restoring the redundancy of the system device.	METAVOLUME	Alarm
0x30006	--	--	CRITICAL	True	Virtual Volume Suspended	Virtual volume has been suspended for more than 10 seconds.	A suspension of I/O applied to a virtual volume has lasted longer than a preconfigured threshold.	Contact Dell EMC Customer Support for analysis of the factors contributing to the extended suspension.	VIRTUAL VOLUME	Alarm
0x30007	amf/20, amf/24	0x8a020014, 0x8a020018	INFO	False	Device Rebuild On going	The given device is undergoing a rebuild on one or more of its mirrors.	Rebuilding work has begun on the given device in order to restore it to full redundancy.	No user action is required.	DEVICE	Alarm
0x30009	amf/126	0x8a02307e	WARNING	True	Logging Volume Write Failed	Write failed to logging volume. The mirror will be marked out of date.	The system has lost access to the logging-volume device on which it was maintaining a list of changes to the reported distributed	Check the accessibility of the logging-volume component and check the accessibility of the underlying storage-volume of	LOGGING VOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							device. The specified mirror of the distributed device will be marked out of date and completely rebuilt when possible.	the mirror that is marked out of date. Take corrective action, if necessary, to reconnect the inaccessible storage volumes. Contact Dell EMC Customer Support for assistance.		
0x3000a	amf/146	0x8a029092	CRITICAL	True	All Mirrors Out of Date	All mirrors of the distributed device are out of date, choosing one mirror as up to date to allow access to the device.	All of the mirrors of the specified distributed device had been marked out of date. In order to restore access to the device, and to minimize data loss, the specified mirror was marked as up to date.	Contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational
0x3000b	amf/111	0x8a02606f	ERROR	True	Device Name Conflict	Name conflict detected between two devices, renaming the second occurrence.	Two discovered devices reported the same device name. This can occur if configuration changes are made when one or more storage volumes are unreachable, if storage devices from separate VPLEX systems with existing devices are merged into one VPLEX	Manual intervention is required. Contact Dell EMC Customer Support to resolve the conflict.	DEVICE	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							system or if a device becomes visible to both clusters and happens to have the same name as a cluster-local device on the other cluster.			
0x3000c	amf/181	0x8a0260b5	ERROR	True	Virtual Volume Name Conflict	Name conflict detected between two virtual volumes, renaming these second occurrence.	Two discovered virtual volumes reported the same name. This can occur if configuration changes are made when one or more storage volumes are unreachable, if storage devices from separate VPLEX systems with existing devices are merged into one VPLEX system or if a virtual volume becomes visible to both clusters and happens to have the same name as a cluster-local virtual volume on the other cluster.	Manual intervention is required. Contact Dell EMC Customer Support to resolve the conflict.	VIRTUAL VOLUME	Operational
0x3000e	amf/158	0x8a02609e	ERROR	True	Hide Storage Volume Provisioned To	Hiding storage volume at the local cluster as this	A storage volume has been provisioned to this cluster, even	Reconfigure the zoning and/or masking on the back-end so that	STORAGE VOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
					Other Cluster	storage volume is also provisioned at the remote cluster.	though the storage volume logically belongs to the other cluster. This message likely indicates a back-end zoning or masking problem, because a storage volume should be provisioned to only one cluster.	each cluster can see only its local storage volumes. Run the 'array re-discover' command to remove the remote storage volumes.		
0x3000f	amf/221	0x8a0290dd	CRITICAL	True	Storage Volume Claimed From Multiple	Storage volume is claimed at both the local and remote clusters.	The same storage volume has been not only presented to both clusters, but claimed at both clusters as well. If more than one cluster is doing I/O to the storage volume, data corruption is extremely likely.	1. Choose one cluster at which the storage volume should be used. 2. Tear down all configurations involving the storage volume at the other cluster. 3. Remove visibility to the storage volume from the other cluster.	STORAGE VOLUME	Operational
0x30010	amf/141	0x8a02308d	WARNING	True	Mirror Marked Out Of Date	A mirror of a raid-1 device has been marked fully out of date.	A write to a raid-1 device was successful to some mirrors, but not the one in question. That mirror is being marked as fully out of date, so that a subsequent rebuild can bring the	If the mirror is not still showing as out of date, it has likely auto-corrected. If it is still marked out of date, investigate the backend issues. Once they have been resolved, the rebuild should initiate	METAVOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							mirror back up today.	automatically . This could take time depending on the number of active rebuilds on the system at the time. Contact Dell EMC Customer Support if the condition persists.		
0x30011	amf/197	0x8a0290c5	CRITICAL	True	Metadata Volume Write Failed	A write to a metadata volume was unsuccessful.	A write to the specified metadata volume has failed. The changes are preserved in memory, but if the entire cluster fails or is shut down before the access to the metadata volume is restored and the changes can be written successfully to disk, the changes will be lost. The system configuration information associated with those metadata writes not written to the disk may be lost.	1. Fix the unhealthy or failed metadata volume, or underlying storage volumes by checking fabric connectivity and the storage array(s). 2. If the metadata volume cannot be restored to an 'ok' state, create and move to a new metadata volume as soon as possible.	METAVOLUME	Operational
0x30012	amf/233	0x8a0230e9	WARNING	True	Metadata Volume Becoming Full	A metadata volume has reached a preconfigured percentage of its capacity.	The metadata volume is running out of available space. This event does not indicate an	Refer to the troubleshooting entry for the issue in the Generator.	METAVOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							immediate metadata volume failure.			
0x30013	amf/251	0x8a0230fb	WARNING	True	Storage Volume Latency Events Suppressed	Generation of storage volume I/O latency events stopped to prevent event flooding.	Generation of I/O latency events has been stopped after emitting the maximum allowed number of events, to prevent event flooding.	1. Use the VPLEX Unisphere performance monitoring stats to verify if there is still high average I/O latency on the backend. 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	CLUSTER	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								Customer Service.		
0x30014	amf/267		CRITICAL	True	Device Detach Full Rebuild	A complex sequence of failures has led to marking one mirror of a distributed device fully out of date, and to the temporary suspension of I/O on that distributed device.	A combination of failures involving metadata and disks offline at cluster followed by cluster partition and failed writes to a logging volume has led to temporary condition where the distributed device can no longer process I/O. Once this condition is resolved, a full rebuild will occur. This condition is necessary to avoid data corruption.	A full rebuild will be started automatically once the clusters re-join. Investigate why the clusters are partitioned and take any required actions to restore the WAN COM connectivity so the clusters can re-join.	DISTRIBUTED DEVICE	Operational
0x30015	amf/34, amf/35, amf/51, amf/52, amf/53, amf/54, amf/55, amf/56, amf/57, amf/58, amf/59, amf/60, amf/61, amf/62, amf/63, amf/64, amf/69, amf/70, amf/71, amf/72, amf/73, amf/75,	0x8a029022, 0x8a029023, 0x8a029033, 0x8a029034, 0x8a029035, 0x8a029036, 0x8a029037, 0x8a029038, 0x8a029039, 0x8a02903a, 0x8a02903b, 0x8a02903c,	CRITICAL	True	Device Bad Config	Metadata persisted to the metadata volume relating to the device or storage volume in question has been detected to be inconsistent. Access to the device or storage volume has been disabled until the problem can be	VPLEX has detected an inconsistency in the persisted information relating to the configuration of the given device or disk. This may indicate a problem with the persisted information, or may simply be the result of a timing issue upon cluster or system bringup.	Contact Dell EMC Customer Support for analysis and remedy of the problem.	DEVICE	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
	amf/76, amf/77, amf/78, amf/79, amf/80, amf/ 81,amf/ 82, amf/91, amf/92, amf/ 122, amf/ 123, amf/ 230	0x8a0290 3d, 0x8a0290 3e, 0x8a0290 3f, 0x8a0290 40, 0x8a0290 45, 0x8a0290 46, 0x8a0290 47, 0x8a0290 48, 0x8a0290 49, 0x8a0290 4b, 0x8a0290 4c, 0x8a0290 4d, 0x8a0290 4e, 0x8a0290 4f, 0x8a0290 50, 0x8a0290 51, 0x8a0290 52, 0x8a0290 5c, 0x8a0290 7a, 0x8a0290 7b, 0x8a0290 e6				examined and remedied.				
0x30016	amf/ 215, amf/ 216	0x8a0290 d7, 0x8a0290 d8	CRITICAL	True	Virtual Volume Capacity Shrunk	The capacity of a virtual volume has shrunk below the capacity withwhich it was created.	The capacity of a virtual volume has shrunk below the capacity withwhich it was created.	1. Examine the back-end arrays to determine why the storage hasshrunk.2. Resize the required back-end devices to their original size.3. Contact Dell EMC Customer Support.	VIRTUAL VOLUME	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x30017	amf/215, amf/216	0x8a0290d7, 0x8a0290d8	CRITICAL	True	System Device Capacity Shrunk	The capacity of a system device (metadata or logging) has shrunk below the capacity with which it was created.	The capacity of a system device (metadata or logging) has shrunk below the capacity with which it was created.	1. Examine the back-end arrays to determine why the storage has shrunk.2. Resize the required back-end devices to their original size.3. Contact Dell EMC Customer Support.	METAVOLUME	Alarm
0x30018	amf/162	0x8a0290a2	CRITICAL	True	Active Metadata Volume Unhealthy	The active metadata volume has become unhealthy and is at risk.	The active meta-volume has become unhealthy and is at risk. It is in cache only, and needs to be written to storage volume.	The active meta-volume has become unhealthy. Either resolve the problem on the back end, or create another meta-volume using 'meta-volume create' as soon as possible, and then run the 'meta-volume move' command to save the cache data to the newly created meta-volume. Contact Dell EMC Customer Support.	STORAGE VOLUME	Alarm
0x30019	amf/226	0x8a0230e2	WARNING	True	Active Metadata Volume Missing	Timed out waiting for the active metadata volume to arrive.	A fixed time has passed after the local cluster last booted, and the active metadata volume has	Fix the problem with the active metadata volume, or activate a backup if no configuration changes have taken	METAVOLUME	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							not yet been detected.	place since the backup. If there have been configuration changes, contact Dell EMC Customer Support to restore from the backup.		
0x3001a	amf/249, amf/250	0x8a0230f9, 0x8a0230fa	WARNING	True	Storage Volume Latency Degraded	Storage volume I/O latency has increased above an acceptable threshold.	The average I/O latency on a storage volume has exceeded the acceptable limit, likely due to increased latency on the backend storage array or fabrics between the VPLEX and storage array.	1. Analyze the latency stats from the storage array for the volume in question at the time of the event to determine if it reported the same high latency. Engage the storage array vendor as needed. 2. If the storage array did not report the same latency at the time of the issue for the volume then investigate the fabrics between the VPLEX and storage array. 3. If the issue persists and the cause cannot be determined engage DELL EMC Customer Service.	STORAGE VOLUME	Alarm
0x3001b	amf/250, amf/270	0x8a0230fa	WARNING	True	Remote Device Latency Degraded	Remote device I/O latency has increased above an acceptable threshold.	The average I/O latency on a remote device has exceeded the acceptable limit due to	1. Use the VPLEX Unisphere performance monitoring stats to verify if there	DISTRIBUTED DEVICE	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							possible issues on the back-end or WAN link.	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 the cause cannot be determined engage DELL EMC		

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								Customer Service.		
0x3001c	amf/244, amf/245, amf/246	0x8a0290f4, 0x8a0290f5, 0x8a0290f6	CRITICAL	True	Mirror Isolated	A mirror of a raid-1 device has been isolated due to severe performance degradation of its storage volume components.	All of the storage volumes supporting this mirror are performing very poorly, causing severe degradation in the RAID-1 performance. To improve the RAID-1 performance through the healthy legs, the IOs to the poorly performing mirror leg have been blocked.	Determine the cause of the storage volume's poor performance by referring to the troubleshooting entry related to degraded disks and isolated mirrors in the normal operation section of Solve Procedure Generator ("Recovery -> Troubleshooting -> Problems during normal operation -> Degraded disks and isolated mirrors problems"). If the underlying issues cannot be fixed in a timely manner, consider detaching the unhealthy mirror from the RAID-1 device and attaching a mirror based on healthy storage volume(s) to reinstate redundancy. Contact Dell EMC Customer	METAVOLUME	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								Support if the problem persists.		
0x3001d	amf/203	0x8a0200cb	INFO	False	Metadata Copy Succeeded	Successfully copied in-memory metadata to a metadata volume.	All in-memory metadata has been written out to the given metadata volume.	This is an informational event only. No action is required.	METAVOLUME	Operational
0x3001e	amf/201, amf/206, amf/219	0x8a0290c9, 0x8a0290ce, 0x8a0290db	CRITICAL	False	Metadata Copy Failed	Failed to copy in-memory metadata to a metadata volume.	An attempt to write out all in-memory metadata to a metadata volume failed.	Examine the metadata volume to see if there are any problems that can be corrected, contacting Dell EMC Customer Service for assistance if needed.	METAVOLUME	Operational
0x3001f	amf/205	0x8a0200cd	INFO	False	Metadata Move Succeeded	Successfully copied in-memory metadata to a metadata volume, which is now the active metadata volume.	All in-memory metadata has been written out to the given metadata volume, which is now the active metadata volume.	This is an informational event only. No action is required.	METAVOLUME	Operational
0x30020	amf/202, amf/207, amf/220	0x8a0290ca, 0x8a0290cf, 0x8a0290dc	CRITICAL	False	Metadata Move Failed	Failed to copy in-memory metadata to a metadata volume, and therefore the metadata volume has not been activated.	An attempt to write out all in-memory metadata to a metadata volume failed, and therefore that metadata volume has not been activated.	Examine the metadata volume to see if there are any problems that can be corrected, contacting Dell EMC Customer Service for assistance if needed.	METAVOLUME	Operational
0x30021			WARNING	False	Bitmap Log At Expansion Limit	An internal limit relating to expansion of a distributed device has	A distributed device has reached an expansion limit internal to VPLEX. Further	Logging for the distributed device must be recreated. Contact Dell	DISTRIBUTED DEVICE	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
						been reached.	attempts to expand this device will fail without corrective action.	EMC Customer Service for assistance.		
0x40001	com/11	0x8a0a300b	WARNING	True	Other Director Has Different Sw Version	Director running a different version of the software detected.	Local directors are running different versions of software.	Contact Dell EMC Customer Support.	DIRECTOR	Operational
0x40002	com/40	0x8a0a3028	WARNING	True	Fewer Active Paths Than Expected	The number of COM paths to remote director is smaller than expected in a standard configuration.	Fewer than expected paths to remote director.	Check the state of the COM port, making sure it is enabled. Check the cable, making sure it is properly plugged in. Check the switch if applicable, making sure it is operational and the corresponding port is enabled. Contact Dell EMC Customer Support if this event persists.	DIRECTOR	Operational
0x40003	com/52	0x8a0a6034	ERROR	True	Crc Status Initialization Failed	The system failed to read an internal setting.	The system failed to read an internal setting. This will prevent the director from fully booting, thereby preventing it from processing I/O	Contact Dell EMC Customer Support.	DIRECTOR	Operational
0x60001	nmg/49, nmg/50, nmg/59	0x8a260031, 0x8a266032,	ERROR	True	Cluster Partition	Cluster has partitioned.	The last director with the given cluster id has	The last director with the given cluster ID has	CLUSTER	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
		0x8a26303b					departed. This marks the loss of the indicated cluster from the point of view of the reporting cluster.	departed. This marks the loss of the indicated cluster from the point of view of the reporting cluster. Check that the distributed-devices and consistency-groups are running on the winning cluster. A winner may need to be manually chosen. 1. Check for problems with the network link to the indicated cluster. 2. Check the equipment at the indicated cluster for malfunctions.		
0x60002	nmg/100	0x8a266064	ERROR	True	Witness Com Node Untrustworthy	'Memberships connection to {remoteDirector}/{remoteDirectorId}untrustworthy : {qualifier} operational for {secondsSinceOperational}seconds.'	This failure exposes the cluster to a Data Unavailability condition in certain director failure/inter-director link failure scenarios.	Check the management network cables and the corresponding management modules.	DIRECTOR	Operational
0x60003	nmg/56, nmg/57	0x8a269038, 0x8a269039	CRITICAL	True	Stonith Call Failed for remote director	Stonith call failed for {remoteDirector}/{remoteDirectorId}	This director tried to kill the identified director, but the call to do that has failed.	Contact Dell EMC Customer Support.	DIRECTOR	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x60004	nmg/64, nmg/65, nmg/66, nmg/67	0x8a266040, 0x8a266041, 0x8a266042, 0x8a266043	ERROR	True	Director Running Different Firmware	Director running a different version of the software detected.	A director with a different version of firmware may have been inserted into the cluster. Also a communications link could have been brought up by mistake, allowing a cluster of a different version to be visible.	If this situation arose because a director with a different version of firmware was inserted into the cluster and booted, then shut down that director. If the situation arose because a communications link has been brought up by mistake, then take down that communications link.	CLUSTER	Operational
0x60005	nmg/96	0x8a263060	WARNING	True	Witness Com Node From Foreign Site	Unexpected membership arrival uuid {directorId} appears from foreign cluster {foreignClusterId}.	A director from a foreign VPLEX cluster was unexpectedly discovered by this cluster.	Contact Dell EMC Customer Support to check if there has been a mis-configuration done between clusters in the environment	CLUSTER	Operational
0x70001	nmg/107, nmg/108, nmg/109	0x8a26006b, 0x8a26006c, 0x8a26006d	WARNING	False	Cluster Witness Disabled	Cluster Witness is disabled.	This event is generated when Cluster Witness is administratively disabled.	If the Cluster Witness was disabled in error, re-enable it	CLUSTER	Alarm
0x70002	nmg/105, nmg/106	0x8a269069, 0x8a26906a	ERROR	True	Cluster Witness Server Connection Lost	Cluster Witness Server Connection Lost	The cluster reporting this event has been unable to establish communication with Cluster Witness Server. This may be due to the failure	Check network connectivity between the local cluster and Cluster Witness Server. Check whether Cluster Witness	CLUSTER	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							of the server or loss of network connectivity.	Server VM is running.If connectivity is lost from both clusters, disable the Cluster Witness Server via VPLEXCLI until connectivity can be restored inorder to prevent data unavailability on cluster partition. If the Problem persists, contact Dell EMC Customer Support.		
0x70003	nmg/112, nmg/117	0x8a263070, 0x8a260075	WARNIN G	False	CW Cluster Partition Guidance	Communication between clusters is broken.	Cluster Witness Server has detected and reported an inter-cluster partition. This marks the loss of connectivity between the remote cluster and the reporting cluster. This may be due to physical failure or congestion of the inter-cluster network.	If the Cluster Witness Server is present and enabled, it should have provided guidance to continue IO on the winning cluster. If the Cluster Witness Server is not present, check that the distributed devices and consistency groups are running on the winning cluster.If the problem persists, contact Dell EMC Customer Support.	CLUSTER	Alarm
0x70004	nmg/113,	0x8a263071,	WARNIN G	False	CW Remote	CW Remote	Cluster Witness	Verify the state of the	CLUSTER	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
	nmg/117	0x8a260075			Cluster Failure Or Isolation Guidance	Cluster Failure Or Isolation Guidance	Server detected that the remote cluster has either failed or become isolated. This could be due to site disaster or due to dual failure of inter-cluster and management networks.	remote cluster. Also, check the state of inter-cluster network as well as the management network connecting the remote cluster to Cluster Witness Server. If the problem persists, contact Dell EMC Customer Support.		
0x70005	nmg/116, nmg/117	0x8a260074, 0x8a260075	ERROR	True	CW Cluster Isolation Guidance Or No Guidance	CW Cluster Isolation Guidance Or No Guidance	The cluster reporting this event has been unable to receive any guidance from the Cluster Witness Server for the last 10 seconds. This may be due to failure of the Cluster Witness Server or loss of network connectivity.	A winner needs to be manually chosen for all suspended synchronous consistency-groups using the VPLEXcli command "consistency-group choose-winner" in order to resume I/O at the desired cluster. Once this is complete, check network connectivity between the local cluster and Cluster Witness Server. Check whether Cluster Witness Server VM is running. If the problem persists, contact Dell	CLUSTER	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								EMC Customer Support.		
0x70006	nmg/120	0x8a266078	Critical	True	CW Inconsistent State Message Received	CW Inconsistent State Message Received	There are no known causes for this condition. Please contact Dell EMC Customer Support for assistance.	Please contact Dell EMC Customer Support for assistance.	CLUSTER	Operational
0x70007	nmg/127, nmg/128	--	ERROR	True	Cluster Witness Connection Lost	Cluster Witness Connection Lost	The director reporting this event is unable to establish communication with Cluster Witness Server. This may be due to the failure of the server or loss of network connectivity.	Check network connectivity between the director and Cluster Witness Server. Check whether Cluster Witness Server is running. If connectivity is lost from other directors, disable the Cluster Witness Server until connectivity is restored in order to prevent data unavailability on cluster partition. If the problem persists, contact Dell EMC Customer Support.	DIRECTOR	Alarm
0x70008	nmg/129, nmg/130	--	WARNING	True	Cluster Witness Intermittent Communication	Cluster Witness Intermittent Communication	This event is generated when Cluster Witness is unable to send requests or receive responses	Check network connectivity or network bandwidth between the director and Cluster Witness Server.	DIRECTOR	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							from Cluster Witness server.			
0x90001	stdf/32	0x8a346020	ERROR	True	SCSI Target Reset received for host IT Nexus	SCSI Target Reset received for host IT Nexus.	Host initiator has issued target reset due to slow I/O processing.	Check I/O processing statistics. Identify the reason for the host to issue Target Reset and resolve it. If the problem is with the host, unzone the initiator in question from the fabric to prevent potential performance impact to other hosts until the issue can be resolved. Contact Dell EMC Customer Support if problem persists.	TARGET PORT	Operational
0x90002	stdf/53	0x8a349035	CRITICAL	True	Possible Stuck IO detected on virtual volume	Possible Stuck IO detected on virtual volume.	An IO failed to complete or be properly aborted and cleaned up.	Contact Dell EMC Customer Support for assistance.	VIRTUAL VOLUME	Operational
0x90003	stdf/59	0x8a34603b	ERROR	True	Unmap Command Buffer Allocation Failed	SCSI UNMAP command failed on virtual volume due to an internal memory allocation issue.	A Scsi Unmap command could not be processed because of an internal firmware memory allocation failure.	Run the collect-diagnostics utility to collect system information to determine why an internal firmware memory allocation failure occurred. Please contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x90004	stdf/25	0x8a346019	ERROR	True	Compare And Write Insufficient Resources	SCSI Compare And Write command failed on virtual volume due to an internal memory allocation issue.	The VPLEX director had insufficient memory resources to process theScsi Compare and Write Command.	Run collect-diagnostics utility to collect system information to determine why an internal firmware memory allocation failure occurred. Please contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational
0x90005	stdf/29	0x8a34601d	ERROR	True	Write Same 16 Insufficient Resources	SCSI Write Same (16) command failed on virtual volume due to an internal memory allocation issue.	The VPLEX director had insufficient memory resources to process theScsi Write Same Command.	Run the collect-diagnostics utility to collect system information to determine why an internal firmware memory allocation failure occurred. Please contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational
0x90006	stdf/39	0x8a346027	ERROR	True	Xcopy Insufficient Resources	Run the collect-diagnostics utility to collect system information to determine why an internal firmware memory allocation failure occurred. Please contact Dell EMC	The VPLEX director had insufficient memory resources to process theScsi Xcopy Command.	Run the collect-diagnostics utility to collect system information to determine why an internal firmware memory allocation failure occurred. Please contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
						Customer Support.				
0x90007	stdf/26	0x8a34601a	ERROR	True	Compare And Write Processing Failure	SCSI Compare and Write command failed on virtual volume it couldnot be processed by internal layers.	The attempt to start a transaction for a Scsi Compare and Write command failed as it could not be processed by the internal layers.	Please contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational
0x90008	stdf/30	0x8a34301e	WARNING	True	Write Same16 Processing Failure	SCSI Write Same (16) command failed on virtual volume as it couldnot be processed by the internal layers.	The attempt to start a transaction for a Scsi Write Same command failed as it could not be processed by the internal layers.	Consult the Troubleshooting Entry related to VAAI in VPLEX Solve Desktop. If it does not resolve, please contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational
0x90009	stdf/23	0x8a343017	WARNING	True	Compare And Write Invalid Block Count	SCSI Compare and Write command failed on volume due to an invalidblock count.	The host application or OS requested an invalid transfer size on a Scsi Compare and Write Command.	This is a host side issue. Investigate why the host application or OS is not respecting the maximum transfer size advertised by the VPLEX. Consult the Troubleshooting Entry in the VAAI section of Solve Desktop for this event. If problem persists, contact Dell EMC Customer Support.	VIRTUAL VOLUME	Operational
0x9000a	stdf/24	0x8a343018	WARNING	True	Compare And	SCSI Compare	The host application	This is a host side issue.	VIRTUAL VOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
					Write Bad LBA	and Write command failed on volume due to a bad Logical Block Address.	or OS specified an out of range Logical Block Address on a Scsi Compare and Write Command.	Investigate why the host application or OS is not respecting the maximum size of the volume. If problem persists, contact Dell EMC Customer Support.		
0x9000b	stdf/56	0x8a343038	WARNING	True	Volume Not Thin Enabled For Unmap	SCSI UNMAP command received on volume which is not Thin enabled.	Scsi Unmap command processing is rejected by VPLEX because the volume is not thin capable or thin enabled.	Use the VPLEXcli command "virtual-volume set-thin-enabled true-v volume_name" to enable the thin-enabled property for the virtual volume.	VIRTUAL VOLUME	Operational
0x9000c	stdf/34	0x8a343022	WARNING	True	Xcopy Failed	Failed to process a SCSI Xcopy command on volume as xcopy-enable attribute on the storage view is disabled.	Scsi xcopy command processing is disabled on VPLEX.	Use the CLI command and set the xcopy-enabled attribute for the corresponding storage view to true. Refer to the VPLEX CLI guide.	STORAGE VIEW	Operational
0x9000d	stdf/31	0x8a34301f	WARNING	True	Write Same 16 Failed	Failed to process a Write Same (16) command on volume as write-same-16-enabled attribute is disabled on the storage view.	Scsi Write Same command processing is disabled on VPLEX.	Use the CLI command and set the write-same-16-enabled attribute for the corresponding storage view to true. Refer to the VPLEX CLI guide.	STORAGE VIEW	Operational
0x9000e	stdf/19	0x8a343013	WARNING	True	Unintentional	Unintentional Link	An enabled FE port has	1. Check the FE port	TARGET PORT	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
					Front End Port Link Down	Down seen for Front End Target Port.	gone down as a result of FC cable pull, switch reboot or disabling switch port.	status in the 'ports' context of VPLEXcli / clusters/ cluster-*/ directors/ **/ports/to verify if it's still in 'no-link' state. If it is, proceed to next steps.2. Check the switch and ensure it's operational, check the switch logs for errors that will indicate the root cause of the issue.3. Check the cabling and SFPs along the path, clean/reset/replace as needed.		
0xa0000	sfp/8, sfp/9	--	Critical	True	SFP Unsupported	The installed SFP is not a Dell EMC approved part for this interface.	The part number of the SFP is not approved. It is required to use Dell EMC approved SFPs.	Contact Dell EMC Customer Support to replace the SFP with an approved part.	INTERFAC	Alarm
0xa0001	sfp/7	--	Critical	True	SFP Absent	SFP is absent or malfunctioning.	An SFP is missing, inserted incorrectly, or faulty.	Contact Dell EMC Customer Support to check/replace the SFP.	INTERFAC	Alarm
0xa0002	sfp/11, sfp/12	--	Critical	True	SFP Rx Power Low	A port RX power is below the warning or alarm threshold.	A port's RX power is below the warning or alarm threshold.	The hardware attached to this port needs to be carefully investigated, and the switch port SFP	INTERFAC	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								and cable should be re-seated, cleaned, and swapped as needed.		
Oxa0003	sfp/11, sfp/12	--	Critical	True	SFP Rx Power High	A port RX power is above the warning or alarm threshold	A port's RX power is above the warning or alarm threshold.	The hardware attached to this port needs to be carefully investigated, and the switch port SFP and cable should be re-seated, cleaned, and swapped as needed.	INTERFA CE	Alarm
Oxa0004	sfp/11, sfp/12	--	Critical	True	SFP Tx Power Low	A port TX power is below the warning or alarm threshold.	A port's TX power is below the warning or alarm threshold.	Contact Dell EMC Customer Support to replace the SFP.	INTERFA CE	Alarm
Oxa0005	sfp/11, sfp/12	--	Critical	True	SFP Tx Power High	A port TX power is above the warning or alarm threshold.	A port's TX power is above the warning or alarm threshold.	Contact Dell EMC Customer Support to replace the SFP.	INTERFA CE	Alarm
Oxb0001	dios/20	--	WARNING	True	Recovery From One Director Failure Took Too Long	Recovery from the failure of a single director took too long	Recovery from the failure of a single director took too long.	If the host application experienced a DU, confirm that all VPLEX volumes used by that application are in a healthy state. The applications affected will need to go through their recovery process.	SYSTEM	Operational
Oxb0002	dios/13	--	INFO	True	All Failure Recovery Complete	Failure recovery has completed for all volumes.	Failure recovery has completed for all volumes.	This is an informational event only. No further action is required.	SYSTEM	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0xc0001	utl/16	0x8a3a6010	ERROR	True	Too Many Instances of given command running at once	There are too many instances of the given command running at once.	There are already the maximum number of instances of the given management command currently running, and another one cannot be started. The previous instances of the command may be stuck, and the cause of this needs to be investigated.	Contact Dell EMC Customer Support.	DIRECTOR	Operational
0xd0001	vmg/1, vmg/2, vmg/3	0x8a523001, 0x8a523002, 0x8a523003	WARNING	True	Invalid Persisted Consistency Group Record	A persisted record relating to a consistency group had a format unrecognized by the system. The record is thus being ignored.	A persisted record relating to a consistency group had a format unrecognized by the system. The record is thus being ignored.	Check for any missing consistency groups, and reconstruct these as required. Contact Dell EMC Customer Support for assistance.	DIRECTOR	Operational
0xd0002	vmg/29	0x8a52601d	ERROR	True	Automatic Detach On Consistency Group Failed	Following a link or cluster failure, the configured winner settings on a consistency group were not able to come into effect, and I/O remains suspended on both clusters.	The system disallowed the automatic detach on the given consistency group, in order to preserve consistency on the volumes in the set and avoid losing data. Cluster detach is disallowed when the cluster configured	If I/O needs to resume, then all required links should be brought up.	CONSISTENCYGROUP	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							to become the winner needs data from the other cluster, and the necessary rebuild has not yet been completed.			
0xe0001	ndu/3	0x8a250003	INFO	False	NDU started	NDU has started.			DIRECTOR	Operational
0xf0001	nvol/5	0x8a276005	ERROR	True	Scan Failed	Non-volatile storage filesystem corruption detected.	The non-volatile file system has been corrupted and must be repaired.	Contact Dell EMC Customer Support.	METAVOLUME	Operational
0xf0002	nvol/6	0x8a276006	ERROR	True	Header Read Failed	Couldn't read metavolume header - nvol not ready.	The non-volatile file system is either not configured or has been corrupted.	The file system should be reconfigured. Contact Dell EMC Customer Support.	METAVOLUME	Operational
0xf0003	nvol/7	0x8a276007	ERROR	True	Compact Failed	An operation on the meta-volume has failed due to lack of space.	The non-volatile file system is not large enough to handle the amount of information that needs to be persisted.	Create a larger meta-volume. Contact Dell EMC Customer Support for assistance.	METAVOLUME	Operational
0xf0004	nvol/9	0x8a276009	ERROR	True	Write Error	A write error occurred and data was not written to the non-volatile file system	A write error occurred to the non-volatile file system and data was not written to disk.	Investigate why writing to the meta-volume failed. If the failure cannot be corrected, create a new meta-volume and copy the in-memory data to the new meta-volume. Contact Dell EMC Customer	METAVOLUME	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								Support for assistance if necessary.		
0x120003	udcom/3	0x8a649003	CRITICAL	True	Path Disconnected	A communications path has been disconnected.	A communications path has been disconnected due to network connectivity issues.	Check the WAN COM or LOCAL COM path that was disconnected, then check the switch logs for errors that will help pinpoint the root cause. If errors point to hardware issue check/clean/replace the cables and SFPs along the path. Engage Dell EMC Customer Support if unable to determine the root cause.	COMMUNICATIONSPATH	Operational
0x13006f	tcpcom/111	0x8a69606f	ERROR	True	Discover Header CRC Error	The local port received an invalid header from the remote port (CRC check failed).	A tcpcom connection header failed to pass CRC checks.	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 Customer Support for assistance.	PORT	Operational
0x1300c8	tcpcom/200	0x8a6960c8	ERROR	True	Path Indictment	A tcpcom path has been indicted.	A tcpcom path has been indicted.	The system should recover automatically. However,	COMMUNICATIONSPATH	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								the underlying network and hardware needs to be investigated to determine the cause of the error. Please contact DELL EMC Customer Support for assistance.		
0x1300c9	tcpcom/201	0x8a6960c9	ERROR	True	Path Indictment CRC	A tcpcom path has been indicted due to a received packet failing a CRC check.	A tcpcom 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 Support for assistance.	COMMUNICATION PATH	Operational
0x1300ca	tcpcom/202	0x8a6960ca	ERROR	True	Path Indictment Message Length	A tcpcom path has been indicted due to a received packet having an invalid message length.	A tcpcom 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 invalid packets. Please contact DELL EMC Customer Support for assistance.	COMMUNICATION PATH	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x1300cb	tcpcom/203	0x8a6960cb	ERROR	True	Path Indictment Timeout	A tcpcom path has been indicted due to a timeout.	A tcpcom 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 Support for assistance.	COMMUNICATION PATH	Operational
0x150001	fc/1	0x8a660001	INFO	False	Discovery Starting	Fabric discovery is starting due to successful fabric login.	Fabric discovery is starting due to successful fabric login.	No user action is required.	VIRTUAL PORT	Operational
0x150008	fc/8	0x8a666008	ERROR	True	Unzoned Port	A Fibre Channel port came online, but is unzoned.	Fibre Channel port is connected to a switch, but the port isn't in any zone yet.	Please verify: 1. That the port is cabled correctly. 2. That the switch zoning is complete and correct. Additionally, some switches need to enable the zoning configuration one more time to make the just-changed zoning configuration apply. If unable to resolve the issue engage Dell EMC Customer Support.	VIRTUAL PORT	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
0x15000d	fc/13	0x8a66600d	ERROR	True	GS Same Revision Rejected	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.	This switch is likely not compatible with VPLEX. VPLEX is unable to register with the switch or perform fabric discovery. Because this response is non-spec-compliant, VPLEX is unable to report on which version of the spec the switch does support.	Check the connectivity support matrix from E-Lab Navigator to verify if the switch model and firmware is supported by Dell EMC. If assistance is needed engage Dell EMC Customer Support.	VIRTUAL PORT	Operational
0x15000e	fc/14	0x8a66600e	INFO	False	GS Same Revision Rejected Default	When connecting to a switch using the default protocol version, the port received a non-spec-compliant response indicating that the switch does not support the default protocol version that VPLEX supports.	Because this response is non-spec-compliant, VPLEX is unable to determine which version of the spec that the switch does support. VPLEX will try a protocol version that is known to work with some switches that act in this way.	No user action is required. VPLEX is attempting to automatically recover from this issue. A different event will be emitted if further problems are encountered.	VIRTUAL PORT	Operational
0x15000f	fc/15	0x8a66600f	INFO	False	GS Revision Rejected Supported	When connecting to a switch, the port received a response indicating that the switch does not support	VPLEX will attempt to use the specified protocol version to communicate with the switch.	No user action is required.	VIRTUAL PORT	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
						the default protocol version that VPLEX supports. However, the switch responded with an older protocol version that VPLEX does support.				
0x150010	fc/16	0x8a666010	ERROR	True	GS Revision Rejected Unsupported	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. VPLEX is unable to register with the switch or perform fabric discovery.	Check the connectivity support matrix from E-Lab Navigator to verify if the switch model and firmware is supported by Dell EMC. If assistance is needed engage Dell EMC Customer Support.	VIRTUAL PORT	Operational
0x150011	fc/17	0x8a666011	CRITICAL	True	Chip Dump Detected	The indicated interface has encountered an internal error and has dumped diagnostics for chip vendor analysis.	The indicated interface has encountered an internal error and has dumped diagnostics for chip vendor analysis.	Contact Dell EMC Customer Support.	INTERFACE	Operational
0x150018	fc/24	0x8a663018	WARNING	True	Discovery Timeout	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 the physical paths to the switch and verify good connectivity through reset/clean/replacement	VIRTUAL PORT	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								of cables/SFPs as needed. Check the switch logs for indications of frame drops or other problems. If unable to determine the cause engage Dell EMC Customer Support.		
0x150019	fc/25	0x8a669019	CRITICAL	True	Chip Operation Failed	An internal command on this interface has failed unexpectedly.	An internal command on this interface has failed unexpectedly.	Contact Dell EMC Customer Support.	INTERFACE	Operational
0x15001d	fc/29	0x8a66901d	CRITICAL	True	Chip Reset Needed	Chip error requires manual reset from Dell EMC Customer Support.	The chip underlying the specified interface (VPLEX port) has encountered an error condition and requires a manual reset from Dell EMC Customer Support.	Contact Dell EMC Customer Support to manually reset the chip.	INTERFACE	Operational
0x15001e	fc/30	0x8a66901e	CRITICAL	True	Chip Unrecoverable Error Detected	Unrecoverable chip error requires manual reset from Dell EMC Customer Support.	The chip has encountered an error condition and no automated recovery is possible. The chip may now be unresponsive resulting in stuck I/O. The chip needs to be manually reset by Dell EMC Customer	Contact Dell EMC Customer Support to manually reset the chip.	INTERFACE	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							Support, and if that fails the director needs to be rebooted to recover from this issue.			
0x170192	febefc/402	0x8a673192	WARNING	True	Port No IO Resources Warning	{vportName}: In the last {seconds} seconds there were a high number of I/O allocation failures {initiatorIO} {targetIO} {targetResponses}	Either a large I/O spike has occurred, there are frame drop issues on the fabric, or there is an internal issue in the VPLEX.	Engage Dell EMC Customer Service immediately if there is an outage or extreme performance issues. Check the switch logs from the fabric to determine if it's logged a large number of frame drops, in which case further investigation of the fabric is needed. Toggling the VPLEXport(s) in question one at a time by disabling and re-enabling the port in the /clusters/cluster-x/directors/director-x/ports context of VPLEXcli may relieve the issue.	VirtualPort	Operational
0x170193	febefc/403	0x8a673193	WARNING	True	Port High IO Error Rate	{vportName}: In the last {seconds} seconds at least {numLogins} logins observed a	Either there are frame drop issues on the fabric or there is an internal issue in the VPLEX.	Check the physical paths to the switch and verify good connectivity through reseal/clean/replacement	VirtualPort	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
						high I/O failure rate		of cables/SFPs as needed. Check the switch logs for indications of frame drops or other problems. If unable to determine the cause, engage Dell EMC Customer Service.		
0x170194	febefc/404		CRITICAL	True	Port Detected Wedged	{vportName} has outstanding activity but made no progress in the last {seconds} seconds. Initiating chip dump and firmware abort.	This port has outstanding IO but failed to make progress for over 60s, likely due to an internal issue.	Issue extended collect-diagnostics to collect the chip dump. Engage Dell EMC Customer Service.	VirtualPort	Operational
0x1701f5	febefc/501	0x8a6731f5	WARNING	True	Login High IO Error Rate	{vportName}: In the last {seconds} seconds {errorPercent}% of I/O failed on login (npid {npid}, wwpn {wwpn})	Either there are frame drop issues on the fabric or there is an internal issue in the VPLEX.	Check the physical paths to the switch and verify good connectivity through reset/clean/replacement of cables/SFPs as needed, including the connectivity of the VPLEX port. Check the switch logs for indications of frame drops or other problems. If unable to determine the cause	VirtualPort	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								engage Dell EMC Customer Service.		
0x180001	disk/1007	0x8a0e33ef	ERROR	True	One Disk Hw After Sustained Success	A storage volume encountered an I/O failure due to retry exhaustion after multiple consecutive I/O completions.	Multiple successive I/Os to a given disk failed after retryexhaustion. There might be faulty hardware (cable, backendswitch, array).	Verify reported array's BE disk health, LUN masking, array configuration and physical connection. If the problem persists,contact Dell EMC Customer Support.	DiskId	Operational
0x180002	disk/1008	0x8a0e63f0	ERROR	True	Sustained Disk Hw	A storage volume encountered sustained I/O failures due to retry exhaustion.	Multiple successive I/Os to a given disk failed after retryexhaustion. There might be faulty hardware (cable, backend switch,array).	Verify reported array's BE disk health, LUN masking, array configuration and physical connection. If the problem persists,contact Dell EMC Customer Support.	DiskId	Operational
0x190001	scsidisk/201	0x8a2e60c9	ERROR	True	Io Busy Threshold Reached	The given storage volume reached the limit for the number of consecutive busy responses returned.	The storage volume returned too many busy responses, and may be marked dead in VPLEX as a result, if the devices above have redundancy.	Engage array vendor in determining the cause of the returned SCSI busies. If the storage volume has been marked dead, it will be automatically resurrected by VPLEX once the array begins processing I/O for the storage	DiskId	Operational

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								volume again.		
0x1a0001	bepm/3, bepm/4	0x8a6b9004	ERROR	True	IT Flap Degraded	Marking IT flap degraded.	The back-end IT path was found cycling between degraded and un-degraded five times within a 40 minute period due to intermittent poor performance , and is now considered "flap degraded".	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 "flap degraded" until the user manually restores the use of the I-T path via VPLEXcli command 'back-enddegraded 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	ARRAY	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
								Service to manually isolate the IT nexus path to remove it from use until the underlying issue can be resolved.		
0x1a0002	bepm/7, bepm/8	--	ERROR	False	Unit Degraded	Marking LU degraded.	All ITLs to a logical-unit on this director are experiencing poor performance , so the logical-unit is marked degraded.	Investigate the related switch logs and array performance for the logical-unit to determine the cause for the performance degradation. Once the performance improves the VPLEX will automatically restore the default outstanding IO count to the logical-unit.	LOGICAL UNIT	Alarm
0x1a0003	bepm/1, bepm/2	0x8a6b9001	ERROR	True	IT Degraded	Marking IT degraded.	A critical number of ITLs (20 by default, but possibly fewer if fewer than 20 ITLs exist or the threshold was manually changed) on this IT nexus have had multiple IOs experience IO latency of 1 second or greater and all ITLs on that IT have been taken out of service. The IT nexus is	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.	ARRAY	Alarm

Condition ID	Component	ID	Severity	Call home	Alert name	Description	RCA	Corrective action	Event source	Alert type
							now marked degraded.			

Supported metro node monitor events

See the following table:

Message ID	Severity	App name	Description
HWM-PRT101	WARNING	vplex_partition_monitor	The space that is occupied is 80% of the different partitions of the disk.
HWM-PRT102	CRITICAL	vplex_partition_monitor	The space that is occupied is 90% of the different partitions of the disk.
HWM-HRT102	CRITICAL	vplex-peer-heartbeat	Peer is not pingable from MC-00 or MC-01.
-	CRITICAL	vplex_idrac_monitor	iDRAC is unresponsive.
HWM-NC101	ERROR	vplex-nsfw-crash	Metro node firmware has failed with a core dump.
HWM-NC102	ERROR	vplex-nsfw-crash	Metro node firmware has failed with a signal.

Supported iDRAC events

Supported hardware Ports to metro node port-mapping events

The following table is generated through pulling out the cables from the system in real time. For more details about iDRAC alerts, see <https://qrl.dell.com/#/lookup>.

Condition ID (Platform Alerts)	HW Label	PortRole	UDEV (metro node)	VS5 EndUser (UI/CLI) PortName	Physical Port location (Controller ID)	Physical Port location (Port ID)	Message
FC102	FC1	front-end	-	IO-00	FC.Slot.1-1	1	The Fibre Channel in Slot 1 port 1 link is not functioning either because the FC cable is not connected or the FC device is not functioning.
FC102	FC2	front-end	-	IO-01	FC.Slot.1-2	2	The Fibre Channel in Slot 1 port 2

Condition ID (Platform Alerts)	HW Label	PortRole	UDEV (metro node)	VS5 EndUser (UI/CLI) PortName	Physical Port location (Controller ID)	Physical Port location (Port ID)	Message
							link is not functioning either because the FC cable is not connected or the FC device is not functioning.
FC102	FC3	back-end	-	IO-03	FC.Slot.2-2	2	The Fibre Channel in Slot 2 port 2 link is not functioning either because the FC cable is not connected or the FC device is not functioning.
FC102	FC4	back-end	-	IO-02	FC.Slot.2-1	1	The Fibre Channel in Slot 2 port 1 link is not functioning either because the FC cable is not connected or the FC device is not functioning.
0x110001	LCOM1	local-com	LC-00	LC-00	NIC.Integrate d.1-1-1	1	The Integrated NIC 1 Port 1 network link is down.
0x110001	LCOM2	local-com	LC-01	LC-01	NIC.Integrate d.1-2-1	2	The Integrated NIC 1 Port 2 network link is down.
0x110001	WAN1	wan-com	WC-00	WC-00	NIC.Integrate d.1-3-1	3	-
0x110001	WAN2	wan-com	WC-01	WC-01	NIC.Integrate d.1-4-1	4	-
0x110001	MGMT1	mgmt-com	MC-00	MC-00	NIC.Slot.3-1-1	1	The NIC in Slot 3 Port 1 network link is down.

Condition ID (Platform Alerts)	HW Label	PortRole	UDEV (metro node)	VS5 EndUser (UI/CLI) PortName	Physical Port location (Controller ID)	Physical Port location (Port ID)	Message
0x110001	MGMT2	mgmt-com	MC-01	MC-01	NIC.Slot.3-2-1	2	The NIC in Slot 3 Port 2 network link is down.
-	SVC	svc	EC-00	EC-00	NIC.Slot.3-3-1	3	-
0x110001	CUST	cust	EC-01	EC-01	NIC.Slot.3-4-1	4	The NIC in Slot 3 Port 4 network link is down.

Supported SMS events

Condition ID	Severity	Call home	Alert name	Description	Event source
sms/22	Info	False	AMP Unreachable	An AMP registered is unreachable.	ARRAY
sms/00	Warning	True	Test SMSEvent	This is a warning TEST Event.	TEST
0x8A00010E	Warning	True	Sms Automated BackupConfig Details Missing	Meta-volume backup has not been configured. Run configuration and try again.	METAVOLUME
0x8A00010F	Error	True	Sms Automated Backup Config Reserved SV Used Error	Automated backup cannot proceed.	METAVOLUME
0x8A000110	Error	True	Sms Automated Backup Config Details Error	Detected incorrect number of storage-volumes configured for meta-volume backup: two are required, {noOfConfiguredVolumes} detected.	METAVOLUME
0x8A000111	Error	True	Sms Automated Meta Volume Backup Failed	The automated backup of the meta-volume could not be completed: {exception}.	METAVOLUME
0x8A4a61F6	Error	True	SMS_HOST_CERTIFICATE_30_DAYS_UNTIL_EXPIRATION	The host certificate expires within a month.	CERTIFICATES
0x8A4a61F7	Error	True	SMS_CA_CERTIFICATE_30_DAYS_UNTIL_EXPIRATION	The host certificate expires within a month.	CERTIFICATES
0x8A4a91F8	Critical	True	SMS_CA_CERTIFICATE_HAS_EXPIRED	Your CA certificate is expired.	CERTIFICATES
0x8A4a91F9	Critical	True	SMS_HOST_CERTIFICATE_30_DAYS_UNTIL_EXPIRATION	Your host certificate is expired.	CERTIFICATES

Index

H

hardware ports [67](#)

M

monitor alerts [7](#)

monitor events [67](#)