NSX Logging and System Events

VMware NSX for vSphere 6.3

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002451-02

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

NSX Logging and System Events

The *NSX Logging and System Events* document describes log messages, events, and alarms in the VMware® NSX™ product.

Intended Audience

This information is intended for administrators of NSX.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

1 System Events, Alarms and Logs

You can use system events, alarms, and logs to monitor the health and security of the NSX environment and troubleshoot problems.

This chapter includes the following topics:

System Events

System events are records of system actions. Each event has a severity level, such as informational or critical, to indicate how serious the event is. System events are also pushed as SNMP traps so that any SNMP management software can monitor NSX system events..

View the System Event Report

From vSphere Web Client you can view the system events for all the components that are managed by NSX Manager.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then under **Networking & Security Inventory** click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Monitor** tab.

4 Click the **System Events** tab.

You can click the arrows in the column headers to sort events, or use the **Filter** text box to filter events.

About the Syslog Format

If you specify a syslog server, NSX Manager sends all system events to the syslog server. Each message has the following format:

```
syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter '::' (double colons)
Each name/value pair separated by delimiter ';;' (double semi-colons)
```

The fields and types of the system event contain the following information.

```
Event ID :: 32 bit unsigned integer
Timestamp :: 32 bit unsigned integer
Application Name :: string
Application Submodule :: string
Application Profile :: string
Event Code :: integer
Severity :: string (possible values: INFORMATIONAL, LOW, MEDIUM, MAJOR, CRITICAL, HIGH)
Message ::
```

Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an object. Each alarm generates a system event and has an associated resolver that will attempt to resolve the issue that triggers the alarm.

Guest Introspection Alarms

Alarms signal the vCenter Server administrator about Guest Introspection events that require attention. Alarms are automatically cancelled in case the alarm state is no longer present.

vCenter Server alarms can be displayed without a custom vSphere plug-in. See the *vCenter Server Administration Guide* on events and alarms.

Upon registering as a vCenter Server extension, NSX Manager defines the rules that create and remove alarms, based on events coming from the three Guest Introspection components: SVM, Guest Introspection module, and thin agent. Rules can be customized. For instructions on how to create new custom rules for alarms, see the vCenter Server documentation. In some cases, there are multiple possible causes for the alarm. The tables that follow list the possible causes and the corresponding actions you might want to take for remediation.

Host Alarms

Host alarms are generated by events affecting the health status of the Guest Introspection module.

Table 1-1. Errors (Marked Red)

Possible Cause	Action
The Guest Introspection module has been installed on the host, but is no longer reporting status to the NSX Manager.	1 Ensure that Guest Introspection is running by logging in to the host and typing the command `/etc/init.d/vShield-Endpoint-Mux start`. 2 Ensure that the network is configured properly so that Guest Introspection can connect to NSX Manager. 3 Reboot the NSX Manager.

SVM Alarms

SVM alarms are generated by events affecting the health status of the SVM.

Table 1-2. Red SVM Alarms

Problem	Action
There is a protocol version mismatch with the Guest Introspection module	Ensure that the Guest Introspection module and SVM have a protocol that is compatible with each other.
Guest Introspection could not establish a connection to the SVM	Ensure that the SVM is powered on and that the network is configured properly.
The SVM is not reporting its status even though guests are connected.	Internal error. Contact your VMware support representative.

NSX and Host Logs

You can use logs that are in the various NSX components and on the hosts to detect and troubleshoot problems.

For the list of NSX and host log files, see "Infrastructure Preparation" in the *NSX Troubleshooting Guide*.

Audit Logs

The audit logs record all actions by users who log in to NSX Manager.

View the Audit Log

The **Audit Logs** tab provides a view into the actions performed by all NSX Manager users. The NSX Manager retains up to 1,000, 000 audit logs.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then under **Networking & Security Inventory** click **NSX Managers**.

3 In the **Name** column, click an NSX server and then click the **Monitor** tab.

4 Click the **Audit Logs** tab.

5 When details are available for an audit log, the text in the **Operation** column for that log is clickable. To view details of an audit log, click the text in the **Operation** column.

6 In the **Audit Log Change Details**, select **Changed Rows** to display only those properties whose values have changed for this audit log operation.

Configuring a Syslog Server

You can configure a syslog server to be a repository of logs from NSX components and hosts.

Configure a Syslog Server for NSX Manager

If you specify a syslog server, NSX Manager sends all audit logs and system events to the syslog server.

Syslog data is useful for troubleshooting and reviewing data logged during installation and configuration.

NSX Edge supports two syslog servers. NSX Manager and NSX Controllers support one syslog server.

Procedure

1 Log in to the NSX Manager virtual appliance.

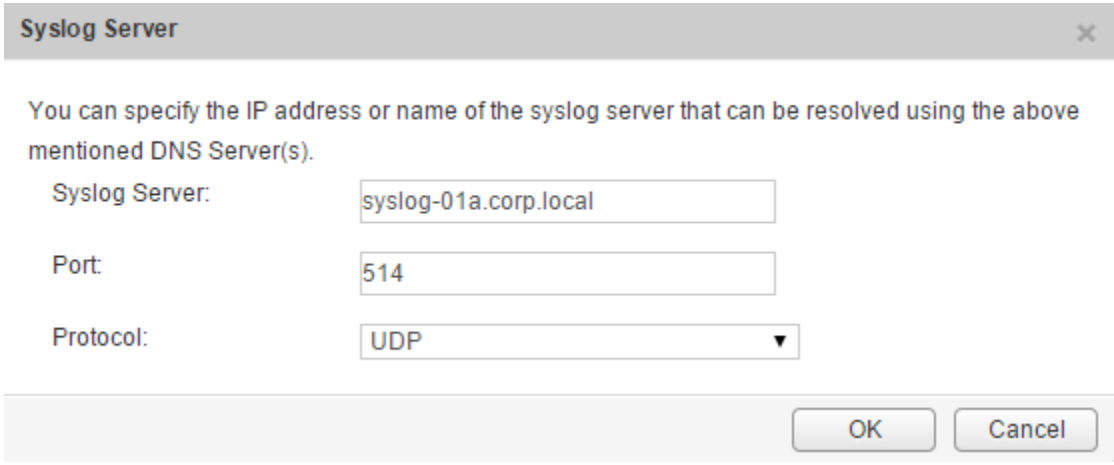
In a Web browser, navigate to the NSX Manager appliance GUI at https://<nsx-manager-ip> or https://<nsx-manager-hostname>, and log in as admin with the password that you configured during NSX Manager installation.

2 From the home page, click **Manage Appliance Settings > General** .

3 Click **Edit** next to **Syslog Server**.

4 Type the IP address or hostname, port, and protocol of the syslog server.

For example:



5 Click **OK**.

NSX Manager remote logging is enabled, and logs are stored in your standalone syslog server.

Configure Syslog Servers for NSX Edge

You can configure one or two remote syslog servers. NSX Edge events and logs related to firewall events that flow from NSX Edge appliances are sent to the syslog servers.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click a NSX Edge.

4 Click the **Manage** tab, and then click the **Settings** tab.

5 In the **Details** panel, click **Change** next to Syslog servers.

6 Type the IP address of both remote syslog servers and select the protocol.

7 Click **OK** to save the configuration.

Collecting Technical Support Logs

On occasions, you might need to collect technical support logs from the NSX components and the hosts to report an issue to VMware.

To collect host tech support logs, run the command `export host-tech-support` (see "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*).

Download Technical Support Logs for NSX

You can download NSX Manager system logs and Web Manager logs to your desktop.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under Appliance Management, click **Manage Appliance Settings**.

3 Click  and then click **Download Tech Support Log**.

4 Click **Download**.

5 After the log is ready, click the **Save** to download the log to your desktop.

The log is compressed and has the file extension `.gz`.

What to do next

You can open the log using a decompression utility by browsing for **All Files** in the directory where you saved the file.

Download Technical Support Logs for NSX Controller

You can download technical support logs for each NSX Controller instance. These product specific logs contain diagnostic information for analysis.

To collect NSX Controller logs:

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security**, and then click **Installation**.

3 Under **Management**, select the controller that you want to download logs from.

4 Click **Download tech support logs**.

5 Click **Download**.

The NSX Manager starts downloading the NSX Controller log and acquires the lock.

Note Download one NSX Controller log at a time. Once the first one completes, start downloading the other. An error might occur if you download logs from multiple controllers simultaneously.

---

6 After the log is ready, click **Save** to download the log to your desktop.

The log is compressed and has `.gz` file extension .

You can now analyze the downloaded logs.

What to do next

If you want to upload diagnostic information for VMware technical support, refer to the Knowledge Base article 2070100.

Download Tech Support Logs for NSX Edge

You can download technical support logs for each NSX Edge instance. If high availability is enabled for the NSX Edge instance, support logs from both NSX Edge virtual machines are downloaded.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Select an NSX Edge instance.

4 Click the **More Actions** () icon and select **Download Tech Support Logs**.

5 After the tech support logs are generated, click **Download**.

6 In the Select location for download dialog box, browse to the directory where you want to save the log file.

7 Click **Save**.

8 Click **Close**.

System Events 2

All components in NSX report system events. These events can help in monitoring the health and security of the environment and troubleshooting problems.

Each event message has the following information:

- Unique event code
- Severity level
- Description of the event and, if appropriate, recommended actions.

Collecting Tech Support Logs and Contacting VMware Support

For some events, the recommended action includes collecting tech support logs and contacting VMware support.

- To collect NSX Manager tech support logs, see "Download Technical Support Logs for NSX," on page 11.
- To collect NSX Edge tech support logs, see "Download Tech Support Logs for NSX Edge," on page 12.
- To collect host tech support logs, run the command `export host-tech-support` (see "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*).
- To contact VMware support, see "How to file a Support Request in My VMware" (http://kb.vmware.com/kb/2006985).

Performing a Force Sync on NSX Edge

For some events, the recommended action includes performing a force sync on NSX Edge. For more information, see "Force Sync NSX Edge with NSX Manager in the *NSX Administration Guide*. Force sync is a disruptive operation and reboots the NSX Edge VM.

System Event Severity Level

Each event has one of the following severity levels:

- Informational
- Low
- Medium
- Major
- Critical

- High

The following tables document system event messages of severity major, critical, or high from various components.

Security System Events

Event Code	Severity	Log Message	Description
240000	Critical	INFO log: adding <user>@<ip> to the blacklist System event log: eventcode.240000.name=Added an IP to authentication black list	A user fails to log in 10 consecutive times. The user cannot log in from the same IP address for 30 minutes. Action: This is a potential security problem and might require an investigation.
230000	Critical	vsm log: errorcode.4010=Invalid SSO Configuration. errorcode.4011=Invalid Lookup service url. errorcode.4012=Invalid NSX Manager Solution Name. errorcode.4013=Invalid Certificate store id. vsmvam log: errorcode.150715=Invalid Lookup Service IP or Port.	Configuration of Single Sign On (SSO) failed. Reasons include invalid credentials, invalid configuration, or time out of sync. Action: Review the error message and re-configure SSO. See "Configure Single Sign On" in the NSX Administration Guide. See also "Configuring the NSX SSO Lookup Service fails" (http://kb.vmware.com/kb/2102041).
11002	Critical	vsmvam log: errorcode.151100=VC Configuration failed. Either wrong credentials provided or vCenter details are not correct	vCenter Server configuration failed. Action: Verify that the vCenter Server configuration is correct. See "Register vCenter Server with NSX Manager" in the *NSX Administration Guide* and "Connecting NSX Manager to vCenter Server" in the *NSX Troubleshooting Guide*
11006	Critical	INFO log: Connection to VC lost System event log: eventcode.11006.name=Lost vCenter Server connectivity	Connection to vCenter Server was lost. Action: Investigate any connectivity problem with vCenter Server. See "Connecting NSX Manager to vCenter Server" and "Troubleshooting NSX Manager Issues" in the NSX Troubleshooting Guide.
230002	Critical	System event log: eventcode.230002.name=SSO STS Client disconnected. eventcode.230002.fullFormat=SSO STS Client disconnected.	Registering NSX Manager to the Single Sign-On service failed or connectivity to the SSO service was lost. Action: Check for configuration issues, such as invalid credentials, out of sync issues, and network connectivity issues. This event also might occur due to specific VMware technical issues. See KB articles "SSL certificate of the STS service cannot be verified" (http://kb.vmware.com/kb/2121696) and "Registering NSX Manager to Lookup Service with External Platform Service Controller (PSC) fails with the error: server certificate chain not verified" (http://kb.vmware.com/kb/2132645).

Distributed Firewall System Events

Event Code	Severity	Log Message	Description
301002	Major	Filter config not applied to vnic	Failed to apply filter config to vNIC. Possible cause: failure in opening, parsing, or updating filter config. This error should not occur with DFW but might occur in Netx scenarios. Action: Collect ESXi and NSX Manager tech support bundles and contact VMware tech support."
301031	Critical	Firewall config update failed on host	Failed to receive/parse/Update firewall config. Key value will have context info such as generation number and also other debug info. Action: Verify that the host preparation procedure was followed. Log in to the host and collect the `/var/log/vsfwd.log` file and then force sync the firewall configuration with the API https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id> (see "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*). If the distributed firewall configuration still fails to be updated on the host, collect the NSX Manager and host tech support logs, and contact VMware support.
301032	Major	Failed to apply firewall rule to vnic	Firewall rules failed to be applied to a vNIC. Action: Verify that vsip kernel heaps have enough free memory (see "View Firewall CPU and Memory Threshold Events" in the *NSX Administration Guide*.) If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support. Make sure that the host logs (vmkernel.log and vsfwd.log) cover when the firewall configuration was being applied to the vNIC.
301041	Critical	Container configuration update failed on host	An operation related to network and security container configuration failed. Key value will have context info such as container name and generation number. Action: Verify that vsip kernel heaps have enough free memory (see "View Firewall CPU and Memory Threshold Events" in the *NSX Administration Guide*.) If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support. Make sure that the host logs (vmkernel.log and vsfwd.log) cover when the container configuration was being applied to the vNIC.
301051	Major	Flow missed on host	Flow data for one or more sessions to and from protected virtual machines was dropped, failed to be read or failed to be sent to NSX Manager. Action: Verify that vsip kernel heaps have enough free memory and that vsfwd memory consumption is within resource limits (see "View Firewall CPU and Memory Threshold Events" in the *NSX Administration Guide*.) If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301061	Critical	Spoofguard config update failed on host	A configuration operation related to SpoofGuard failed. Action: Verify that the host preparation procedure was followed. Log in to the host and collect the `/var/log/vsfwd.log` file and then force sync the firewall configuration with the API https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id> (see "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*). If the SpoofGuard configuration still fails, collect the NSX Manager and host tech support logs, and contact VMware support. Make sure the logs cover when the host received the SpoofGuard configuration.

Event Code	Severity	Log Message	Description
301062	Major	Failed to apply spoofguard to vnic	SpoofGuard failed to be applied to a vNIC. Action: Verify that the host preparation procedure was followed. Log in to the host and collect the `/var/log/vsfwd.log` file and then force sync the firewall configuration with the API https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id> (see "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*). If the SpoofGuard configuration still fails, collect the NSX Manager and host tech support logs, and contact VMware support.
301064	Major	Failed to disable spoofguard for vnic	SpoofGuard failed to be disabled for a vNIC. Action: Collect the NSX Manager and host tech support logs, and contact VMware support.
301072	Critical	Failed to delete legacy App service vm: {0}	The vShield App service VM for vCloud Networking and Security failed to be deleted. Action: Verify that the procedure "Upgrade vShield App to Distributed Firewall" in the *NSX Upgrade Guide* was followed.
301080	Critical	Firewall CPU threshold crossed	vsfwd CPU usage threshold value was crossed. Action: See the "View Firewall CPU and Memory Threshold Events" section in the *NSX Administration Guide*. You might need to reduce host resource utilization. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301081	Critical	Firewall memory threshold crossed	vsfwd memory threshold value was crossed. Action: See the "View Firewall CPU and Memory Threshold Events" section in the *NSX Administration Guide*. You might need to reduce host resource utilization, including reducing the number of configured firewall rules or network and security containers. To reduce the number of firewall rules, use the `appliedTo` capability. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301082	Critical	Firewall ConnectionsPerSecond threshold crossed	The firewall connections per second threshold was crossed. Action: See the "View Firewall CPU and Memory Threshold Events" section in the *NSX Administration Guide*. You might need to reduce host resource utilization, including reducing the number of active connections to and from VMs on the host.
301501	Critical	Firewall configuration update version {0} to host {1} timed out. Firewall configuration on host is synced upto version {2}.	A host took more than 2 minutes to process a firewall configuration update, and the update timed out. Action: Verify that vsfwd is functioning and that rules are being published to hosts. See "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301502	Critical	Spoofguard configuration update number {0} to host {1} timed out. Spoofguard configuration on host is synced upto version {2}	A host took more than 2 minutes to process a SpoofGuard configuration update, and the update timed out. Action: Verify that vsfwd is functioning and that rules are being published to hosts. See "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301503	Critical	Failed to publish firewall configuration version {1} to cluster {0}. Refer logs for details	Publishing firewall rules has failed for a cluster or one or more hosts. Action: See "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.

Event Code	Severity	Log Message	Description
301504	Critical	Failed to publish container updates to cluster {0}. Refer logs for details.	Publishing network and security container updates failed for a cluster or one or more hosts. Action: See "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301001	Critical	Filter config update failed on host	Host failed to receive/parse filter config or open device /dev/dvfiltertbl. Action: See the key-value pair for context and failure reason, which might include VIB version mismatch between NSX Manager and prepared hosts and unexpected upgrade issues. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301505	Critical	Failed to publish spoofguard updates to cluster {0}. Refer logs for details	Publishing SpoofGuard updates has failed for a cluster or one or more hosts. Action: See "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301506	Critical	Failed to publish exclude list updates to cluster {0}. Refer logs for details	Publishing exclude list updates has failed for a cluster or one or more hosts. Action: See "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301508	Critical	Failed to sync host {0}. Refer logs for details	A firewall force sync operation via the API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> failed. Action: See "Troubleshooting Distributed Firewall" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301512	Major	Firewall is installed on host {0}[{1}]	The distributed firewall was installed successfully on a host. Action: In vCenter Server, navigate to **Home > Networking & Security > Installation**and select the Host Preparation tab. Verify that Firewall Status displays as green.
301513	Major	Firewall is uninstalled on host {0}[{1}]	The distributed firewall was uninstalled from a host. If the distributed firewall components fail to be uninstalled, collect the NSX Manager and host tech support logs, and contact VMware support.
301514	Critical	Firewall is enabled on cluster {0}	The distributed firewall was installed successfully on a cluster. Action: In vCenter Server, navigate to **Home > Networking & Security > Installation**and select the Host Preparation tab. Verify that Firewall Status displays as green.
301515	Critical	Firewall is uninstalled on cluster {0}	The distributed firewall was uninstalled from a cluster. Action: If the distributed firewall components fail to be uninstalled, collect the NSX Manager and host tech support logs, and contact VMware support.
301516	Critical	Firewall is disabled on cluster {0}	The distributed firewall was disabled on all hosts in a cluster. Action: None required.
301510	Critical	Force sync operation failed for the cluster	A firewall force sync operation via the API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> failed. Action: Collect the NSX Manager and host tech support logs, and contact VMware support.

Event Code	Severity	Log Message	Description
301034	Major	Failed to apply Firewall rules to host	A distributed firewall rule section failed to be applied. Action: Verify that vsip kernel heaps have enough free memory (see "View Firewall CPU and Memory Threshold Events" in the *NSX Administration Guide*.) If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301043	Critical	Failed to apply container configuration to vnic	A network or security container configuration failed to be applied. Action: Verify that vsip kernel heaps have enough free memory (see "View Firewall CPU and Memory Threshold Events" in the *NSX Administration Guide*.) If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301044	Critical	Failed to apply container configuration to host	A network or security container configuration failed to be applied. Action: Verify that vsip kernel heaps have enough free memory (see "View Firewall CPU and Memory Threshold Events" in the *NSX Administration Guide*.) If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301066	Major	Failed to apply Spoofguard configuration to host	Failed to apply all SpoofGuard to the vnics. Action: Verify that vsip kernel heaps have enough free memory (see "View Firewall CPU and Memory Threshold Events" in the *NSX Administration Guide*.) If the problem persists, collect the NSX Manager and host tech support logs, and contact VMware support.
301100	Critical	Firewall timeout configuration update failed on host	The firewall session timer timeout configuration failed to be updated. Action: Collect the NSX Manager and host tech support logs, and contact VMware support. After you have collected the logs, force sync the firewall configuration with the REST API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> or by going to **Installation > Host Preparation** and, under **Actions**, select **Force Sync Services**.
301101	Major	Failed to apply firewall timeout configuration to vnic	The firewall session timer timeout configuration failed to be updated. Action: Collect the NSX Manager and host tech support logs, and contact VMware support. After you have collected the logs, force sync the firewall configuration with the REST API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> or by going to **Installation > Host Preparation** and, under **Actions**, select **Force Sync Services**.
301103	Major	Failed to apply firewall timeout configuration to vnic	The firewall session timer timeout configuration failed to be updated. Action: Collect the NSX Manager and host tech support logs, and contact VMware support. After you have collected the logs, force sync the firewall configuration with the REST API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> or by going to **Installation > Host Preparation** and, under **Actions**, select **Force Sync Services**.
301200	Major	Application Rule Manager flow analysis started	Application Rule Manager flow analysis started. Action: None required.

Event Code	Severity	Log Message	Description
301201	Major	Application Rule Manager flow analysis failed	Application Rule Manager flow analysis failed. Action: Collect the NSX Manager tech support logs, and contact VMware support. Start a new monitoring session for the same vNICs as the failed session to attempt the operation again.
301202	Major	Application Rule Manager flow analysis completed	Application Rule Manager flow analysis completed. Action: None required.

NSX Edge System Events

Event Code	Severity	Log Message	Description
30011	High	**Note** 30011 is passed from VSE. No specific log in NSX.	The NSX Edge VMs should recover automatically from this state. Check for a trap with event code 30202 or 30203. Action: See "Edge Appliance Troubleshooting" in the *NSX Troubleshooting Guide*.
30013	Critical	1 Empty status file returned by VIX agent. 2 SysEvent-Detailed-Message : (Kept only in logs) :: VSE_OPERATION_TIMEDOUT 3 populateSystemEvent parameters : sourceName {}, morefIdOfObjectOnVc {}, moduleName {}, eventCode {}, severity {}, messageParams {} eventMetaData {}"	NSX Edge VM is reporting a bad state, and might be functioning correctly. Action: An automatic force sync is triggered when a problematic state is detected. If the automatic force sync fails, try a manual force sync.
30014	Major	1 Rpc request to vm: vmId on host hostId timed out 2 publishToVm failed for vmId. Continue for other vm. [If publish has succeeded at least on one VM]	The NSX Manager communicates with NSX Edge through the VIX or Message Bus. The communication channel is selected by the NSX Manager on the basis of whether Host prep is done or not at the time of edge deploymentor redeployment. Action: See "Edge Appliance Troubleshooting" in the *NSX Troubleshooting Guide*.
30032	High	1 INFO Failed to find vm with ID = '{}' in the inventory. 2 INFO Discovering Vm with vmId : '{}' having VC uuid '{}' 3 ERROR Failed to discover the vm : '{}' using vcUuId = '{}'	The NSX Edge VM likely was deleted directly from vCenter Server. This is not a supported operation as NSX-managed objects must be added or deleted from the vSphere Web Client interface for NSX. Action: Re-deploy the Edge or deploy a new Edge.
30034	Critical	**Note** 30033 is also raised EDGE_VM_HEALTHCHECK_NO_PULSE 30034 EDGE_GATEWAY_HEALTHCHECK_NO_PULSE Event Message:'NSX Edge VM (vmId : vmId) not responding to health check.'	Communication issues between manager and edge. Action: Perform log analysis to root cause the issue. Check if edge VM is powered on.

Event Code	Severity	Log Message	Description
30037	Critical	INFO {0} dropped from {1} firewall addressList. It is not found or is not in scope. (Where 0=groupingObjectId and 1=edgeId) or INFO {0} dropped from {1} firewall applicationList. It is not found or is not in scope. (Where 0=groupingObjectId and 1=edgeId)	NSX Edge firewall rule modified as {0} is no longer available for {1}. This is generated when an invalid GroupingObject (IPSet, securityGroup, etc) is present in the firewallRule. Action: Revisit the firewall rule and make required updates.
30038	Critical	Disable cluster anti affinity rule for Edge {}, primaryResourcePoolMoId: {}, secondaryResourcePoolMoId: {}, primaryEdgeMoId: {}, secondaryEdgeMoId: {} ClusterAntiAffinityRuleUtils:234 - About to configure anti affinity rule for edge edge-Id	NSX Edge High Availability applies anti-affinity rules to vSphere hosts automatically so that the active and standby Edge VMs are deployed on different hosts. This event indicates that these anti-affinity rules were removed from the cluster and that both Edge VMs are running on the same host. Action: Go to vCenter Server and check the anti-affinity rules.
30045	Critical	VIX Exception Error Code VIX_AGENT_VIX_ERROR(10013)	The network environment might be causing repeated communication failures to the Edge VM over the VIX channel. Action: Collect the NSX Manager and NSX Edge tech support logs if NSX Edge is responsive. Then do a force sync. If the problem persists, collect the tech support logs if not able to do so before the force sync, and do a redeploy (see "Redeploy NSX Edge" in the *NSX Administration Guide*). **Note** Redeploying is a disruptive action. It is recommended that you first do a force sync and if the issue is not resolved, then redeploy.
30046	Critical	ERROR Pre rule update failed: generation generation number {0}, edge {1}} , vm {2} (Where 0=generationNumber as per DFW, 1=edgeId, 2=edgeVm's VcUuid	The NSX Edge firewall rules might be out of sync. This error is generated if the preRules (configured from DFW UI/API) fails. Action: If the problem is not resolved automatically by the built-in recovery process, do a manual force sync.
30100	Critical	vShield Edge was force synced	The NSX Edge VM was force synced. Action: If the force sync does not resolve the problem, collect the NSX Manager and NSX Edge tech support logs, and contact VMware support.
30102	High	vShield Edge is in System Bad state	The NSX Edge VM is experiencing an internal error. Action: If the problem is not resolved automatically by the built-in recovery process, try a manual force sync.
30148	Critical	vShield Edge CPU over used	The NSX Edge VM CPU utilization is high for sustained periods. Action: Refer to "Edge Appliance Troubleshooting" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and NSX Edge tech support logs, and contact VMware support.
30153	Major	AESNI crypto engine is up	AESNI crypto engine is up. Action: None required.
30154	Major	AESNI crypto engine is down	AESNI crypto engine is down. Action: None required. This status is expected.

Event Code	Severity	Log Message	Description
30180	Critical	OOM happened, system rebooting in 3 seconds...	The NSX Edge VM has run out of memory. A reboot was initiated to recover. Action: Refer to "Edge Appliance Troubleshooting" in the *NSX Troubleshooting Guide*. If the problem persists, collect the NSX Manager and NSX Edge tech support logs, and contact VMware support.
30181	Critical	File system is read only	There is connectivity issue with the storage device backing the NSX Edge VM. Action: Check and correct any connectivity issue with the backing datastore. You might need to execute a manual force sync after the connectivity issue is resolved.
30202	Major	vShield Edge HighAvailability switch over happens: move to ACTIVE state	An HA failover has occurred, and the secondary NSX Edge VM has transitioned from the STANDBY to ACTIVE state. Action: No action is required.
30203	Major	vShield Edge HighAvailability switch over happens: move to STANDBY state	An HA failover occurred, and the primary NSX Edge VM transitioned from the ACTIVE to STANDBY state. Action: No action is required.
30302	Critical	LoadBalancer pool/member status is changed to down	A virtual server or pool on the NSX Edge load balancer is down. Action: Refer to the "Load Balancing" section in the *NSX Troubleshooting Guide*.
30303	Major	LoadBalancer pool/member status is changed to unknown	A virtual server or pool on the NSX Edge load balancer is experiencing an internal error. Action: Refer to the "Load Balancing" section in the *NSX Troubleshooting Guide*.
30304	Major	LoadBalancer pool/member status is changed to warning	An NSX Edge load balancer pool changed its state to warning. Action: Refer to the "Load Balancing" section in the *NSX Troubleshooting Guide*.
30402	Critical	IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to down	An NSX Edge IPSec VPN channel is down. Action: See KB article "Troubleshooting IPSec VPN in NSX for vSphere 6.x" (http://kb.vmware.com/kb/2123580).
30404	Critical	EDGE IPSEC TUNNEL DOWN : IPsec Tunnel from localSubnet : {subnet} to peerSubnet : {subnet} changed the status to down.	An NSX Edge IPSec VPN channel is down. Action: See KB article "Troubleshooting IPSec VPN in NSX for vSphere 6.x" (http://kb.vmware.com/kb/2123580).
30405	Major	IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown	An NSX Edge IPSec VPN channel's status cannot be determined. Action: See KB article "Troubleshooting IPSec VPN in NSX for vSphere 6.x" (http://kb.vmware.com/kb/2123580).
30406	Major	IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown	An NSX Edge IPSec VPN channel's status cannot be determined. Action: See KB article "Troubleshooting IPSec VPN in NSX for vSphere 6.x" (http://kb.vmware.com/kb/2123580).
30701	Critical	Edge DHCP relay service is disabled.	The NSX Edge DHCP Relay service is disabled. Possible reasons: (1) The DHCP Relay process is not running. (2) There is no external DHCP server. This might be caused by the deletion of grouping object referenced by the relay. Action: See "Configuring DHCP Relay" in the *NSX Administration Guide*.

Event Code	Severity	Log Message	Description
30206	Critical	System event: Split Brain recovered on edge id edgeId . AutoHeal Counter : count	The two NSX Edge HA appliances are able to communicate with each other and have re-negotiated active and standby status. Action: Refer to "Troubleshooting NSX Edge High Availability (HA) issues: (http://kb.vmware.com/kb/2126560).
30207	Critical	Recovery from Split Brain for vShield Edge edgeId attempted with count	The two NSX Edge HA appliances are attempting to re-negotiate and recover from a split brain condition. Note: The recovery mechanism reported by this event occurs only in NSX Edge releases earlier than 6.2.3. Action: Refer to "Troubleshooting NSX Edge High Availability (HA) issues: (http://kb.vmware.com/kb/2126560).

Fabric System Events

Event Code	Severity	Log Message	Description
250004	High	Datastore {0} could not be configured on host, probably its not connected.	The datastore where you will store security virtual machines for the host could not be configured. Action: Confirm the host can reach the datastore.
250005	High	Installation of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.	ESXi host failed to access VIBs/OVFs from NSX during an NSX service installation on host. In the VC system events table, you see: Event Message:'Installation of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.', Module:'Security Fabric'. Action: Refer to "Troubleshooting vSphere ESX Agent Manager (EAM) with NSX" (http://kb.vmware.com/kb/2122392).
250008	High	Service will need to be redeployed as the location of the OVF / VIB bundles to be deployed has changed.	NSX VIBs and OVFs are available via a URL which differs across NSX versions. To find the correct VIBs, you must go to https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties. If the NSX Manager IP address changes, the NSX OVF or VIB may need to be redeployed. Action: Resolve the alarm by clicking the **Resolve** link in the **Installation > Host Preparation** tab or by using the resolve API.
250009	High	Upgrade of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.	EAM has failed to access VIBs/OVFs from NSX during a host upgrade. In the VC system events table, you see: Event Message:'Installation of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.', Module:'Security Fabric'. Action: Refer to "Troubleshooting vSphere ESX Agent Manager (EAM) with NSX" (http://kb.vmware.com/kb/2122392).
250012	High	Following service(s) need to be installed successfully for Service {0} to function: {1}	The service being installed is dependent on another service that has not yet been installed. Action: Deploy the required service on the cluster.
250014	High	Error while notifying security solution before upgrade	Error while notifying security solution before upgrade. The solution may not be reachable/responding. Action: Ensure that solution URLs are accessible from NSX. Use the resolve API to resolve the alarm. Service will be redeployed.

Event Code	Severity	Log Message	Description
250015	High	Did not receive callback from security solution for upgrade notification even after timeout	Did not receive callback from security solution for upgrade notification even after timeout. Action: Ensure that solution URLs are accessible from NSX, and NSX is reachable from the solution. Use the resolve API to resolve the alarm. Service will be redeployed.
250016	High	Did not receive callback from security solution for uninstall notification even after timeout	Uninstallation of service failed. Action: Ensure that solution URLs are accessible from NSX, and NSX is reachable from the solution. Use the resolve API to resolve the Alarm. Service will be removed.
250017	High	Uninstallation of service failed	Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. Action: Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use the resolve API to resolve the alarm. Service will be removed.
250018	High	Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification.	Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. Action: Ensure that solution URLs are accessible from NSX, and NSX is reachable from the solution. Use the resolve API to resolve the Alarm. Service will be removed.
250019	High	Server rebooted while security solution notification for uninstall was going on	Server rebooted while security solution notification for uninstall was going on. Action: Ensure that solution urls are accessible from NSX. Use the resolve API to resolve the alarm. Service will be uninstalled.
250020	High	Server rebooted while security solution notification for upgrade was going on	Server rebooted while security solution notification for uninstall was going on. Action: Ensure that solution urls are accessible from NSX. Use the resolve API to resolve the alarm. Service will be redeployed.
250021	Critical	Connection to EAM server failed	The connection between NSX Manager and the Virtual Center EAM service has gone down. Action: Verify that Virtual Center is up and that the EAM service is running. Verify that the URL http://{VC_IP}/eam/mob/ is accessible. For more information, refer to "Infrastructure Preparation" in the *NSX Troubleshooting Guide* and "Troubleshooting vSphere ESX Agent Manager (EAM) with NSX" (http://kb.vmware.com/kb/2122392).
250023	High	Pre Uninstall cleanup failed	Internal pre-uninstallation cleanup tasks failed to complete. Action: Use the `POST /2.0/services/alarms?action=resolve` API with request body `SystemAlarmsDto` to resolve the alarm and remove the service.
250024	High	The backing EAM agency for this deployment could not be found. It is possible that the VC services may still be initializing. Please try to resolve the alarm to check existence of the agency. In case you have deleted the agency manually, please delete the deployment entry from NSX.	vSphere ESX Agent Manager (EAM) deploys VIBs onto ESXi hosts. An EAM agency is installed on each NSX-prepared cluster. If this agency cannot be found, the vCenter Server services may be initializing or the agency was deleted manually in error. Action: See "Infrastructure Preparation" in the *NSX Troubleshooting Guide*, and "Troubleshooting vSphere ESX Agent Manager (EAM) with NSX" (2122392)."

Deployment Plugin System Events

Event Code	Severity	Log Message	Description
280000	High	Deployment plugin Ip pool exhausted alarm	An IP address failed to be assigned to an NSX Service VM as the source IP pool has been exhausted. Action: Add IP addresses to the pool.
280001	High	Deployment plugin generic alarm	Each service such as Guest Introspection or Trend has a set of plug-ins to configure the service on each host. Any problem in the plug-in code is reported as a generic alarm. The service will turn green only after all the plug-ins for the service are successful. This event captures a subset of possible exceptions. Action: Use the resolve API to resolve the alarm. Service will be deployed.
280004	High	Deployment plugin generic exception alarm	Each service such as Guest Introspection or Trend has a set of plug-ins to configure the service on each host. Any problem in the plug-in code is reported as a generic alarm. The service will turn green only after all the plug-ins for the service are successful. This event captures all possible exceptions. Action: Use the resolve API to resolve the alarm. Service will be deployed.
280005	High	VM needs to be rebooted for some changes to be made/take effect	VM needs to be rebooted for some changes to be made/take effect. Action: Use the resolve API to resolve the alarm. This will reboot the VM.

Messaging System Events

Event Code	Severity	Log Message	Description
390001	High	Host messaging configuration failed.	The NSX message bus is set up after host preparation once ESX Agent Manager (EAM) has notified NSX that NSX VIBs have been successfully installed on an ESXi host. This event indicates that the message bus setup on the host failed. Starting with NSX 6.2.3, a red error icon is shown next to the affected host on the Installation > Host Preparation tab. Action: Refer to the troubleshooting steps in "Understanding and troubleshooting Message Bus in VMware NSX for vSphere 6.x" (http://kb.vmware.com/kb/2133897).
390002	High	NSX tried to send latest RMQ broker information to Host via VC and it failed	In certain situations where NSX finds the RMQ broker details have changed, it tries to send the latest RMQ broker information to the host. If it fails to send this information, this alarm is raised. Action: Refer to the troubleshooting steps in "Understanding and troubleshooting Message Bus in VMware NSX for vSphere 6.x" (http://kb.vmware.com/kb/2133897).
390003	High	Host messaging configuration failed and notifications were skipped.	NSX will try to set up messaging channel again when a prepared host connects back to vCenter Server. This event indicates that setup failed and that other NSX modules dependent on the messaging channel were not notified. Action: Refer to the troubleshooting steps in "Understanding and troubleshooting Message Bus in VMware NSX for vSphere 6.x" (http://kb.vmware.com/kb/2133897).

Event Code	Severity	Log Message	Description
391002	Critical	Messaging infrastructure down on host.	Two or more heartbeat messages between NSX Manager and an NSX host were missed. Action: Refer to the troubleshooting steps in "Understanding and troubleshooting Message Bus in VMware NSX for vSphere 6.x" (http://kb.vmware.com/kb/2133897).
321100	Critical	Disabling messaging account uw-host-11. Password has expired.	An ESXi host, NSX Edge VM, or USVM acting as a message bus client has not changed its rabbit MQ password within the expected period of two hours after initial deployment or host preparation. Action: Investigate a communication issue between NSX Manager and the message bus client. Verify the client is running. Before performing a re-sync or redeploy, collect the appropriate logs. Refer to the troubleshooting steps in "Understanding and troubleshooting Message Bus in VMware NSX for vSphere 6.x" (http://kb.vmware.com/kb/2133897).

Service Composer System Events

Event Code	Severity	Log Message	Description
300001	High	Policy is out of sync	Service Composer encountered an error while attempting to enforce rules on this Service Policy. Action: Consult the error message for inputs on which rules to change in the Policy. Use either Service Composer or the resolve API to resolve this alarm.
300000	Critical	Policy {0} is deleted as a result of explicit deletion of its dependent SecurityGroup	A service policy was deleted when a dependent security group was deleted. Action: Investigate creating the security policy again.
300002	High	Firewall rules on this Policy are out of sync. No Firewall related changes from this policy will be pushed, until this alarm is resolved.	This error was caused by an issue with the firewall configuration. Action: Consult the error message for details of the policy (and possibly the rules) that caused the error. Ensure that you resolve the alarm to synchronize the policy using Service Composer or the resolve API. See also "Troubleshooting issues with Service Composer in NSX 6.x" (http://kb.vmware.com/kb/2132612).
300003	High	Network Introspection rules on this Policy are out of sync. No Network Introspection related changes from this policy will be pushed, until this alarm is resolved.	This error was caused by an issue with the network introspection configuration. Action: Consult the error message for details of the policy (and possibly the rules) which caused the error. Ensure that you resolve the alarm to synchronize the policy using Service Composer or the resolve API. See also "Troubleshooting issues with Service Composer in NSX 6.x" (http://kb.vmware.com/kb/2132612).
300004	High	Guest Introspection rules on this Policy are out of sync. No Guest Introspection related changes from this policy will be pushed, until this alarm is resolved.	This error was caused by an issue with the guest introspection configuration. Action: Consult the error message for details of the policy (and possibly the rules) which caused the error. Ensure that you resolve the alarm to synchronize the policy using Service Composer or the resolve API. See also "Troubleshooting issues with Service Composer in NSX 6.x" (http://kb.vmware.com/kb/2132612).

Event Code	Severity	Log Message	Description
300005	High	Service Composer is out of sync. No changes from Service Composer will be pushed to Firewall/Network Introspection.	Service Composer encountered an error when synchronizing a policy. No changes will be sent to the firewall or network introspection services. Action: Consult the error message to determine which policies and/or firewall sections to edit. Resolve the alarm via Service Composer or via the resolve API.
300006	High	Service Composer is out of sync due to failure on sync on reboot operation.	Service Composer encountered an error when synchronizing a policy on reboot. No changes will be sent to the firewall or network introspection services. Action: Consult the error message to determine which policies and/or firewall sections to edit. Resolve the alarm via Service Composer or via the resolve API.
300007	High	Service Composer is out of sync due to rollback of drafts from Firewall. No changes from Service Composer will be pushed to Firewall/Network Introspection	Service Composer encountered a synchronization error when reverting firewall rule sets to an earlier draft. No changes will be sent to the firewall or network introspection services. Action: Resolve the alarm via Service Composer or via the resolve API.
300008	High	Failure while deleting section corresponding to the Policy.	Service Composer encountered an error when deleting the firewall rules section for the policy. This issue will occur when the manager for a third-party service with NSX Service Insertion is not reachable. Action: Investigate a connectivity issue to the third-party service manager. Resolve the alarm via Service Composer or via the resolve API.
300009	High	Failure while reordering section to reflect precedence change.	Service Composer encountered an error when synchronizing a policy on reboot. No changes will be sent to the firewall or network introspection services. Action: Consult the error message to determine which policies and/or firewall sections to edit. Resolve the alarm via Service Composer or via the resolve API.
300010	High	Failure while initializing auto save drafts setting.	Service Composer encountered an error while initializing autosaved drafts settings. Action: Consult the error message to determine which policies and/or firewall sections to edit. Resolve the alarm via Service Composer or via the resolve API.

SVM Operations System Events

Event Code	Severity	Log Message	Description
280002	High	Inconsistent SVM alarm	A deployed service VM experienced an internal error. Action: Resolving the alarm deletes the VM and reports a second alarm about the deletion. Resolving the second alarm reinstalls the VM. If redeploying the VM fails, the original alarm is again reported. If the alarm reappears, collect the SVM logs using the procedure in KB http://kb.vmware.com/kb/2144624.
280003	High	SVM restart alarm	A deployed service VM has been restarted. Action: Resolving the alarm restarts the VM. If the restart fails, the alarm reappears. Collect the SVM logs using the procedure in KB http://kb.vmware.com/kb/2144624 and contact VMware support.
280006	High	Failed to mark agent as available.	An internal error occurred while marking the ESX agent VM as available. Action: Resolve the alarm using the resolve API. If the alarm cannot be resolved, collect the SVM logs using the procedure in KB http://kb.vmware.com/kb/2144624 and contact VMware support.

Replication - Universal Sync System Events

Event Code	Severity	Log Message	Description
310001	Critical	eventcode.310001.name=Full sync failed. eventcode. 310001.description=Full sync failed for object type {0} on NSX manager {1}.	Performing a full sync of universal objects on a secondary NSX Manager failed. Action: Collect the NSX Manager technical support logs and contact VMware support.
310003	Critical	eventcode. 310003.description=Universal sync operation failed for the entity {0} on NSX manager {1}.	Synchronizing a universal object to the secondary NSX Manager in a Cross-vCenter environment failed. Action: Collect the NSX Manager technical support logs and contact VMware support.

NSX Management System Events

Event Code	Severity	Log Message	Description
320001	Critical	eventcode.320001.name=Duplicate NSX Manager IP detected eventcode.320001.description=The NSX Manager IP {0} has been assigned to another machine with the MAC Address {1}.	The NSX Manager management IP address has been assigned to a VM on the same network. Prior to 6.2.3, a duplicate NSX Manager IP address is not detected or prevented. This can cause data path outage. In 6.2.3 and later, this event is raised when a duplicate address is detected. Action: Resolve the duplicate address problem.

VXLAN System Events

Event Code	Severity	Log Message	Description
814	Critical	The status of virtualwire [{}] changed [{} -> {}].	One or more DVS port groups backing an NSX logical switch have been modified or deleted, or changing the logical switch control plane mode has failed. Action: If the event was triggered by deleting or modifying a port group, an error will be shown on the Logical Switches page in the vSphere Web Client. Clicking on the error will create the missing DVS port groups. If the event was triggered because changing the control plane mode failed, perform the update again. Refer to "Update Transport Zones and Logical Switches" in the *NSX Upgrade Guide*.
1900	Critical	Failed to create VXLAN IP vmknic on port[XXXXX] of VDS[XXXXX]	VXLAN initialization failed as the vmknics failed to be configured for the required number of VTEPs. NSX prepares the DVS selected by the user for VXLAN and creates a DV port group for VTEP vmknics to use. The teaming, load balancing method, MTU, and VLAN ID is chosen during VXLAN configuration. The teaming and load balancing methods must match the configuration of the DVS selected for the VXLAN. Action: Review the vmkernel.log. See also the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.
1901	Critical	VDL2PortPropSet:XXX: Failed to set control plane property for port[XXXXX] on VDS[XXXXX] : Would block	VXLAN failed to be configured on the associated DV port, and the port has been disconnected. NSX prepares the DVS selected by the user for VXLAN and creates a DV port group for each configured logical switch to use. Action: Review the vmkernel.log. See also the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.
1902	Critical	failed to install overlay instance vxlan: Not found	The VXLAN configuration was received for a DV port when the DVS on the ESXI host is not yet enabled for VXLAN. Action: Review the vmkernel.log. See also the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.
1903	Critical	Failed to join mcast group[XXXX] in VLAN[XXX] on VDS[XXXX] . Not always seen, will need to look at vsi stats of VTEP FRP filter.	The VTEP interface failed to join the specified multicast group. Traffic to certain hosts will be impacted until the issue is resolved. NSX uses a periodic retry mechanism (every five seconds) for joining the multicast group. Action: Review the vmkernel.log. See also the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.
1905	Critical	Host prep fails with "Insufficient IP addresses in IP pool."	The VTEP vmknic failed to be assigned a valid IP address. All VXLAN traffic through the vmknic will be dropped. Action: Confirm DHCP is available on VXLAN transport VLANs if you are using DHCP for IP assignment for VMKNics. See "NSX host preparation fails with error: Insufficient IP addresses in IP pool" (http://kb.vmware.com/kb/2137025).
1906	Critical	VDL2PortPropSet:XXX: Failed to set control plane property for port[XXXXX] on VDS[XXXXX] : Would block	NSX VIBs were not installed when the DVS was configured for VXLAN. All VXLAN interfaces will fail to connect to the DVS. Action: See "Network connectivity issues after upgrade in NSX/VCNS environment" (http://kb.vmware.com/kb/2107951).
1920	Critical	(from vsm) Timeout on building connection between VSM and new deployed controller {}, then remove it	The controller deployment failed. Action: Check that the assigned IP address is reachable. Also see "Troubleshooting NSX for vSphere 6.x Controllers" (http://kb.vmware.com/kb/2125767).

Event Code	Severity	Log Message	Description
1930	Critical	WARN org.apache.zookeeper.server.quorum.QuorumCnxManager - Connection broken for id X, my id = X	Two controller nodes are disconnected, impacting controller to controller communication. Action: Refer to "Troubleshooting NSX for vSphere 6.x Controllers" (http://kb.vmware.com/kb/2125767). For known issues, refer to http://kb.vmware.com/kb/2146973 and http://kb.vmware.com/kb/2127655.
1935	Critical	(from vsm) Add host key on the controller operation [for {}] failed	Host certificate information failed to be sent to the NSX controller cluster. The communication channel between the host and the controller cluster may behave unexpectedly. Action: Confirm the NSX controller cluster status is normal before preparing an ESXi host. Use the controller sync API to resolve this issue.
1937	Critical	Vxlan vmknic {} [PortGroup = {}] does not appear in the host {}, remove it from database.	The VXLAN vmknic is missing or deleted from the host. Traffic to and from the host will be affected. Action: Resolve this issue by clicking on the **Resolve** link in the **Installation > Logical Network Preparation > VXLAN Transport** tab.
1939	Critical	Vxlan vmknic {} [PortGroup = {}] does not appear on the host {}, mark it as missingOnHost.	NSX Manager detected that a VXLAN vmknic is missing on Virtual Center. This can be caused by vCenter Server to host communication issues. Also, when vCenter Server or a host is rebooted, there will be a brief period when NSX Manager cannot detect the VXLAN vmknic and raises this event. After vCenter Server and the host finish rebooting, NSX Manager will recheck the VXLAN vmknics and clear the event if everything is fine. Action: Resolve this issue if it is not transient by clicking on the **Resolve** link in the **Installation > Logical Network Preparation > VXLAN Transport** tab.
1941	Critical	Host Connection Status Changed: Event Code: {}, Host: {} (ID: {}), NSX Manager - Firewall Agent: {}, NSX Manager - Control Plane Agent: {}, Control Plane Agent - Controllers: {}.	NSX Manager detected a down status for one of the following connections: NSX Manager to host firewall agent, NSX Manager to host control plane agent, or host control plane agent to NSX controller. Action: If the NSX Manager to host firewall agent connection is down, check the NSX Manager and firewall agent log (/var/log/vsfwd.log) or send the POST https://NSX-Manager-IP-Address/api/2.0/nwfabric/configure?action=synchronize REST API call to re-synchronize the connection. If the NSX Manager to control plane agent is down, check the NSX Manager and control plane agent log (/var/log/netcpa.log). If the control plane agent to NSX controller connection is down, navigate to **Networking & Security > Installation** and check the host connection status.
1942	Critical	Marked backing [{}] as [missingOnVc = {}] on VirtualWire {}.	NSX Manager detected a backing DV portgroup for an NSX logical switch is missing in Virtual Center. Action: Click the **Resolve** link in the **Installation > Logical Network Preparation > VXLAN Transport** tab, or use the REST API (POST https://<vsm-ip>/api/2.0/vdn/virtualwires/<vw-id>/backing?action=remediate) to recreate the portgroup.

Event Code	Severity	Log Message	Description
1945	Critical	[/var/log/cloudnet/run/iostat/iostat_alert.log] r_await(or w_await) XXX.X avg XX.X True / [syslog]: WARN org.apache.zookeeper.server.persistence.FileTxnLog - fsync-ing the write ahead log in SyncThread:X took XXXXms which will adversely effect operation latency. See the ZooKeeper troubleshooting guide	NSX Manager detected high disk latency for NSX controllers. Action: Refer to "Troubleshooting NSX for vSphere 6.x Controllers" (http://kb.vmware.com/kb/2125767)."
1947	Critical	(from vsm) Updating controller {} vm status to power off	NSX Manager detected an NSX controller VM was powered off from Virtual Center. The controller cluster status may become disconnected, impacting any operation which requires a working cluster. Action: Click on the **Resolve** button for the controller in the **Installation > Management** tab or call the API POST https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate to power on the controller VM.
1948	Critical	(from vsm) Updating controller {} vm status to vm deleted	NSX Manager detected an NSX controller VM was deleted from Virtual Center. The controller cluster status may become disconnected, impacting any operation which requires a working cluster. Action: Click the **Resolve** button for the controller in the **Installation > Management** tab or call the API POST https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate to remove the state of the controller in the NSX Manager database."
1952	Critical	The VXLAN portgroup [moid = dvportgroup-xx] and associated DVS have different teaming policies.	NSX Manager detected that a VXLAN portgroup's teaming policy is different from the teaming policy of the associated DVS. This can result in unpredictable behavior. Action: Reconfigure the VXLAN portgroup or the DVS so that they have the same teaming policy.

vmwNsxMLogserver System Events

Event Code	Severity	Log Message	Description
395000	Critical	SecurityLog on Domain Controller Eventlog Server is Full.	The security log in the Active Directory event log server is full. The ID firewall, when configured to use log scraping, will stop functioning. Action: Contact the Active Directory server administrator and increase the size of the security log, clear the security log, or archive the security log.

EAM System Events

Event Code	Severity	Log Message	Description
270000	High	Eam generic alarm	ESX Agent Manager (EAM) detected an NSX installation or upgrade issue with either NSX VIBs or service VMs. Action: Resolve the alarm by clicking the **Resolve** link in the **Installation > Host Preparation** tab or by using the resolve API.

Index