NSX Logging and System Events

Update 4
Modified on 10 AUG 2017
VMware NSX for vSphere 6.3

vmware®

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

https://docs.vmware.com/

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® for vSphere® system by using the NSX Manager user interface and the vSphere Web Client.

Intended Audience

This manual is intended for anyone who wants use or troubleshoot any problem for NSX in a VMware vCenter environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware vSphere, including VMware ESXi, vCenter Server, and the vSphere Web Client.

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.

Format of a System Event

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

These messages have a format similar to the message displayed below:

```
Jan 8 04:35:00 NSXMGR 2017-01-08 04:35:00.422 GMT+00:00
INFO TaskFrameworkExecutor-18 SystemEventDaoImpl:133 -
[SystemEvent] Time:'Tue Nov 08 04:35:00.410 GMT+00:00 2016',
Severity:'High', Event Source:'Security Fabric', Code:'250024',
Event Message:'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.', Module:'Security Fabric', Universal Object:'false
```

System event contains the following information.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Event Message: Text containing detailed information about the event.
Module: Event component. May be the same as event source.
Universal Object: Value displayed is True or False.
```

Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an object. Alarms, along with other alerts, are displayed on the NSX Dashboard and other screens on the vSphere Web Client UI.

You can use the `GET api/2.0/services/systemalarms` API to view alarms on NSX objects.

NSX supports two methods for an alarm:

- Alarm corresponds to a system event and has an associated resolver that will attempt to resolve the issue that triggers the alarm. This approach is designed for network and security fabric deployment (for example, EAM, Message Bus, Deployment Plug-In), and is also supported by Service Composer. These alarms use the event code as the alarm code. For more details, refer to *NSX Logging and System Events* document.
- Edge notifications alarms are structured as a triggering and resolving alarm pair. This method is supported by several Edge functions, including IPSec VPN, load balancer, high availability, health check, edge file system, and resource reservation. These alarms use a unique alarm code which is not the same as the event code. For more details, refer to *NSX Logging and System Events* document.

Generally, an alarm gets automatically deleted by the system when the error condition is rectified. Some alarms are not auto cleared on a configuration update. Once the issue is resolved, you have to clear the alarms manually.

Here is an example of the API that you can use to clear the alarms.

You can get alarms for a specific source, for example, cluster, host, resource pool, security group, or NSX Edge. View alarms for a source by *sourceId*:

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}
```

Resolve all alarms for a source by *sourceId*:

```
POST https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}?action=resolve
```

You can view NSX alarms, including Message Bus, Deployment Plug-In, Service Composer, and Edge alarms:

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms
```

You can view a specific NSX alarm by *alarmId*:

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
```

You can resolve a specific NSX alarm by *alarmId*:

```
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

For more information on API, refer to *NSX API Guide*.

Format of an Alarm

You can view format of an alarm through API.

The format of an alarm contains the following information.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Message: Text containing detailed information about the event.
Alarm ID: ID of an alarm.
Alarm Code: Event code which uniquely identifies the system alarm.
Alarm Source: Source where you should look to resolve the reported event.
```

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 100, 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.

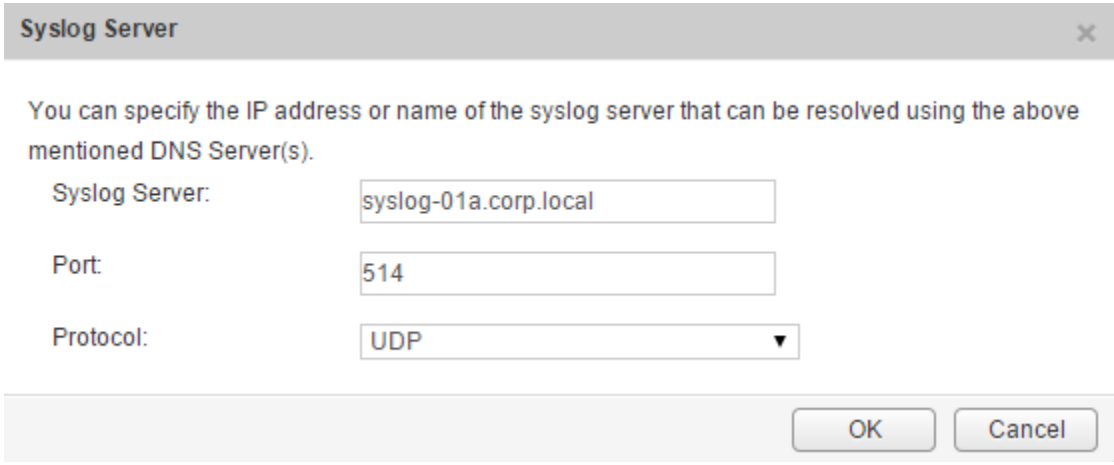
In a Web browser, navigate to the NSX Manager appliance GUI at https://<nsx-manager-ip> or https://<nsx-manager-hostname>, and log in as admin with the password that you configured during NSX Manager installation.

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 Technical Support Logs and Contacting VMware Support

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

- To collect NSX Manager technical support logs, see “Download Technical Support Logs for NSX,” on page 12.
- To collect NSX Edge technical support logs, see “Download Tech Support Logs for NSX Edge,” on page 13.
- To collect host technical 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 topics document system event messages of severity major, critical, or high from various components.

This chapter includes the following topics:

Security System Events

The table explains system event messages for security of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
11002	Critical	No	Unable to connect to vCenter Server. Bad username / password.	vCenter Server configuration failed. Action: Verify that the vCenter Server configuration is correct and the correct credentials are provided. 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	No	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*.
230000	Critical	No	SSO Configuration Task on NSX Manager failed.	Configuration of Single Sign On (SSO) failed. Reasons include invalid credentials, invalid configuration, or time out of sync. Action: Review the error message and configure SSO again. See "Configure Single Sign On" in the *NSX Administration Guide*. Also, see "Configuring the NSX SSO Lookup Service fails" in the *NSX Troubleshooting Guide*.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
230002	Critical	No	SSO STS Client disconnected.	Registering NSX Manager to the SSO 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 might also 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).
240000	Critical	No	Added an entry {0} to authentication black list.	A user with a specific IP address failed to log in for 10 consecutive times and is locked out for 30 minutes. Action: Investigate a potential security issue.

Distributed Firewall System Events

The table explains system event messages for distributed firewall of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301001	Critical	No	Filter config update failed on host.	Host failed to receive/parse filter configuration 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301002	Major	No	Filter config not applied to vnic.	Failed to apply filter configuration to vNIC. Possible cause: Failure in opening, parsing, or updating filter configuration. This error should not occur with distributed firewall but might occur in Network Extensibility (NetX) scenarios. Action: Collect technical support bundles for ESXi and NSX Manager, and contact VMware technical support.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301031	Critical	No	Firewall config update failed on host.	Failed to receive/parse/update firewall configuration. Key value will have context information such as generation number and other debug information. 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301032	Major	No	Failed to apply firewall rule to vnic.	Failed to apply firewall rules to 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 technical support logs for NSX Manager and host, and contact VMware technical support. Make sure that the host logs (*vmkernel.log* and *vsfwd.log*) includes the time period when the firewall configuration was being applied to the vNIC.
301041	Critical	No	Container configuration update failed on host.	An operation related to network and security container configuration failed. Key value will have context information 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 technical support logs for NSX Manager and host, and contact VMware technical support. Make sure that the host logs (*vmkernel.log* and *vsfwd.log*) includes the time period when the container configuration was being applied to the vNIC.
301051	Major	No	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 technical support logs for NSX Manager and host, and contact VMware technical support.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301061	Critical	No	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 technical support logs for NSX Manager and host, and contact VMware technical support. Make sure logs includes the time period when the host received the SpoofGuard configuration.
301062	Major	No	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 technical support logs for NSX Manager and host, and contact VMware technical support.
301064	Major	No	Failed to disable spoofguard for vnic.	SpoofGuard failed to be disabled for a vNIC. Action: Collect the technical support logs forNSX Manager and host, and contact VMware technical support.
301072	Critical	No	Failed to delete legacy App service vm.	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	No	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 technical support logs for NSX Manager and host, and contact VMware technical support.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301081	Critical	No	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 technical support logs for NSX Manager and host, and contact VMware technical support.
301082	Critical	No	Firewall ConnectionsPerSecond threshold crossed.	The threshold for firewall connections per second 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	No	Firewall configuration update version {version#} to host {hostID} timed out. Firewall configuration on host is synced upto version {version#}.	A host took more than two 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301502	Critical	No	Spoofguard configuration update number {number#} to host {hostID} timed out. Spoofguard configuration on host is synced upto version {version#}.	A host took more than two 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301503	Critical	No	Failed to publish firewall configuration version {version#} to cluster {clusterID}. 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301504	Critical	No	Failed to publish container updates to cluster {clusterID}. 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 technical support logs for NSX Manager and host, and contact VMware technical support.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301505	Critical	No	Failed to publish spoofguard updates to cluster {clusterID}. 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301506	Critical	No	Failed to publish exclude list updates to cluster {clusterID}. 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301508	Critical	No	Failed to sync host {hostID}. 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 technical support logs for NSX Manager and host, and contact VMware technical support.
301510	Critical	No	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 technical support logs for NSX Manager and host, and contact VMware technical support.
301512	Major	No	Firewall is installed on host {hostID}[{hostID}].	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	No	Firewall is uninstalled on host {hostID}[{hostID}].	The distributed firewall was uninstalled from a host. If the distributed firewall components fail to be uninstalled, collect the technical support logs for NSX Manager and host, and contact VMware technical support.
301514	Critical	No	Firewall is enabled on cluster {clusterID}.	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	No	Firewall is uninstalled on cluster {clusterID}.	The distributed firewall was uninstalled from a cluster. Action: If the distributed firewall components fail to be uninstalled, collect the technical support logs for NSX Manager and host, and contact VMware technical support.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301516	Critical	No	Firewall is disabled on cluster {clusterID}.	The distributed firewall was disabled on all hosts in a cluster. Action: None required.
301034	Major	No	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 technical support logs for NSX Manager and host, and contact VMware technical support.
301043	Critical	No	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 technical support logs for NSX Manager and host , and contact VMware technical support.
301044	Critical	No	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 technical support logs for NSX Manager and host, and contact VMware technical support.
301066	Major	No	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 technical support logs for NSX Manager and host , and contact VMware technical support.
301100	Critical	No	Firewall timeout configuration update failed on host.	The firewall session timer timeout configuration failed to be updated. Action: Collect the technical support logs for NSX Manager and host, 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**.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301101	Major	No	Failed to apply firewall timeout configuration to vnic.	The firewall session timer timeout configuration failed to be updated. Action: Collect the technical support logs for NSX Manager and host, and contact VMware technical 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	No	Failed to apply firewall timeout configuration to host.	The firewall session timer timeout configuration failed to be updated. Action: Collect the technical support logs for NSX Manager and host, and contact VMware technical 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	No	Application Rule Manager flow analysis started.	Application Rule Manager flow analysis started. Action: None required.
301201	Major	No	Application Rule Manager flow analysis failed.	Application Rule Manager flow analysis failed. Action: Collect the technical support logs for NSX Manager, and contact VMware technical support. Start a new monitoring session for the same vNICs as the failed session to attempt the operation again.
301202	Major	No	Application Rule Manager flow analysis completed.	Flow analysis for the Application Rule Manager is complete. Action: None required.

NSX Edge System Events

The table explains system event messages for NSX Edge of major, critical, or high severity. System events with informational severity are listed if such events triggers the alarm.

Event Code	Event Severity	Alarm Code	Event Message	Description
30011	High	N/A	None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.	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	130013	NSX Manager found NSX Edge VM (vmId : {#}) in bad state. Needs a force sync.	NSX Edge VM is reporting a bad state, and might not 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.

Event Code	Event Severity	Alarm Code	Event Message	Description
30014	Major	N/A	Failed to communicate with the NSX Edge 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 preparation is done or not at the time of edge deployment or re-deployment. This event indicates that NSX Manager lost communication with the NSX Edge. Action: See "Edge Appliance Troubleshooting" in the *NSX Troubleshooting Guide*.
30027	Informational	130027	NSX Edge VM (vmId : {#}) is powered off.	The NSX Edge VM was powered off. Action: Information-only event.
30032	High	130032	NSX Edge appliance with vmId : {#} not found in the vCenter inventory.	The NSX Edge VM was likely 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: Redeploy the edge or deploy a new edge.
30033	High	130033	NSX Edge VM (vmId : {#}) not found in the vCenter inventory.	The NSX Edge VM cannot be found in the vCenter inventory. Action: Check whether the VM was deleted accidentally. If confirmed, redeploy the edge.
30034	Critical	130034	None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.	The Edge VM is not responding to the health check sent by the NSX Manager. Action: Confirm the edge VM is powered on. Then collect the edge logs and contact VMware technical support.
30037	Critical	N/A	Edge firewall rule modified as {#} is no longer available for {#}.	An invalid GroupingObject (IPSet, securityGroup, and so on) is present in the firewall rule. Action: Revisit the firewall rule and make required updates.
30038	Critical	N/A	Powered-on NSX Edge appliance : {EdgeId #}, {vmName #} violates the virtual machine anti-affinity rule.	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 verify the anti-affinity rules.
30045	Critical	N/A	NSX Edge VM health check failing with critical vix errors. Further health check is disabled for vm. Please redeploy or forcesync vm to resume health check.	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 technical support logs if NSX Edge is responsive. Then do a force sync. If the problem persists, redeploy NSX Edge(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 deploy again.
30046	Critical	N/A	Pre rules publish failed on edge: {EdgeID#}, vm: {#} for generation number {#}. Refer logs for detail. It may need forcesync.	The NSX Edge firewall rules might be out of sync. This error is generated if the pre rules (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.

Event Code	Event Severity	Alarm Code	Event Message	Description
30100	Critical	N/A	NSX Edge was force synced.	The NSX Edge VM was force synced. Action: If the force sync does not resolve the problem, collect the technical support logs for NSX Manager and NSX Edge, and contact VMware technical support.
30102	High	130102	NSX Edge (vmId : {IP Address}) is in Bad State. Needs a force sync.	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	N/A	NSX Edge CPU usage has increased. {#} Top processes are: {#}.	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 technical support logs for NSX Manager and NSX Edge, and contact VMware technical support.
30153	Major	N/A	AESNI crypto engine is up.	AESNI crypto engine is up. Action: None required.
30154	Major	N/A	AESNI crypto engine is down.	AESNI crypto engine is down. Action: None required. This status is expected.
30155	High	130155	Insufficient CPU and/or Memory Resources available on Host or Resource Pool, during resource reservation at the time of NSX Edge deployment.	Insufficient CPU and/or memory resources on host or resource pool. You can view the available resources and reserved resources by navigating to the **Home > Hosts and Clusters > [Cluster-name]> Monitor > Resource Reservation**page. After checking the available resources, specify the resources as part of appliance configuration again, so that resource reservation limit succeeds.
30180	Critical	N/A	NSX Edge is out of memory. The Edge is rebooting in 3 seconds. Top 5 processes are: {#}.	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 technical support logs for NSX Manager and NSX Edge, and contact VMware technical support.
30181	Critical	130181	NSX Edge {EdgeID#} VM name {#} 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	N/A	NSX Edge {EdgeID#} HighAvailability switch over happened. VM {#} name {#} has moved 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	N/A	NSX Edge {EdgeID} HighAvailability switch over happened. VM {#} name {#} has moved 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.

Event Code	Event Severity	Alarm Code	Event Message	Description
30205	Critical	130205	Split Brain detected for NSX Edge {EdgeID} with HighAvailability.	Due to network failure, NSX Edge VM's configured for HA are unable to determine if the other VM is online. In such scenario, both the VM's think the other is not online and take on the ACTIVE state. This may cause network disruption. Action : Check network infrastructure (virtual and physical) to look for any failures, specially on the interfaces and the path configured for HA.
30302	Critical	130302	LoadBalancer virtualServer/pool : {virtualServerName]} Protocol : {#} serverIp : {IP Address} changed the state 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	N/A	LoadBalancer virtualServer/pool : {0} Protocol : {#} serverIp : {IP Address} changed to a wrong state.	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	130304	LoadBalancer pool : {0} Protocol : {#} serverIp : {IP address} changed to a warning state.	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	130402	IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to down.	An NSX Edge IPSec VPN channel is down. Action: Refer to the "Virtual Private Networks (VPN)" section in the *NSX Troubleshooting Guide*.
30404	Critical	130404	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: Refer to the "Virtual Private Networks (VPN)" section in the *NSX Troubleshooting Guide*.
30405	Major	N/A	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: Refer to the "Virtual Private Networks (VPN)" section in the *NSX Troubleshooting Guide*.
30406	Major	N/A	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: Refer to the "Virtual Private Networks (VPN)" section in the *NSX Troubleshooting Guide*.
30701	Critical	N/A	NSX Edge DHCP Relay service on edge {EdgeID} is disabled because there is no external DHCP server provided. Please check server IP or referenced grouping object.	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	Event Severity	Alarm Code	Event Message	Description
30206	Critical	N/A	Resolved Split Brain for NSX Edge {EdgeID} with HighAvailability.	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	N/A	Attempted Split Brain resolution for NSX Edge {EdgeID} with count {value}.	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

The table explains system event messages for fabric of major, critical, or high severity.

Few terms related to fabric system events are explained below:

- Fabric is a software layer in NSX Manager which interacts with ESX Agent Manager (EAM) to install network and security services on the host. Once NSX receives confirmation from EAM that the NSX VIBs have been installed successfully on a host, the fabric layer triggers message bus setup. You can view NSX fabric details are using the `/api/2.0/nwfabric/` API.
- ESX Agent Manager (EAM) Agency is the NSX Manager database of deployment units and the vCenter EAM database of EAM agencies must be in sync. An EAM agency is the object created in the vCenter EAM database to define an NSX service which relies on EAM for deployment. In rare cases, the two databases may not synchronize, and NSX provides events and alarms to notify the condition.

The following table documents system event messages of severity major, critical, or high for the Fabric system events.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
250004	High	Yes	Datastore {#} could not be configured on host, probably its not connected.	The datastore where you store security virtual machines for the host could not be configured. Action: Confirm the host can reach the datastore.
250005	High	Yes	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 vCenter 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).

Event Code	Event Severity	Alarm Triggered	Event Message	Description
250008	High	Yes	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: To resolve the alarm, click the **Resolve** link on the **Installation > Host Preparation** tab or use the `resolve` API to resolve the alarm.
250009	High	Yes	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 vCenter 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	Yes	Following service(s) need to be installed successfully for Service {#} to function: {#}.	The service being installed is dependent on another service that has not been installed yet. Action: Deploy the required service on the cluster.
250014	High	Yes	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.
250015	High	Yes	Did not receive callback from security solution for upgrade notification even after timeout.	Not received 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	No	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	Yes	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.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
250018	High	Yes	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	Yes	Server rebooted while security solution notification for uninstall was going on.	Server was rebooted while security solution notification for uninstall was in progress. Action: Ensure that solution URLs are accessible from NSX. Use the `resolve` API to resolve the alarm. Service will be uninstalled.
250020	High	Yes	Server rebooted while security solution notification for upgrade was going on.	Server was rebooted while security solution notification for uninstall was in progress. Action: Ensure that solution URLs are accessible from NSX. Use the resolve API to resolve the alarm. Service will be redeployed.
250021	Critical	No	Connection to EAM server failed.	The connection between NSX Manager and the vCenter EAM service is down. Action: Verify that vCenter 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*.
250023	High	Yes	Pre Uninstall cleanup failed.	Internal cleanup tasks prior to uninstallation failed to complete. Action: Use the `POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve` API with request body `SystemAlarmsDto` to resolve the alarm and remove the service.
250024	High	Yes	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.	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.
250025	High	Yes	VIB requires manual installation.	This event is generated when an attempt is made to upgrade or uninstall NSX BITS on the stateless host using EAM. All stateless host should be prepared using the Auto Deploy feature. Action: Fix configuration using the Auto Deploy feature, and use the `resolve` API to resolve the alarm.

Deployment Plugin System Events

The table explains system event messages for deployment plug-in of major, critical, or high severity.

Few terms related to deployment plug-in system events are explained below:

- Deployment plug-in is an additional code that is added to the NSX fabric to perform pre deployment and post deployment actions.
- Deployment unit is an object created in the NSX Manager database for every cluster. A deployment unit must be created before networking and security services are installed.

The following table documents system event messages of severity major, critical, or high for the deployment plug-in system events.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
280000	High	Yes	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	Yes	Deployment Plugin generic alarm.	Each service such as Guest Introspection 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	Yes	Deployment Plugin generic exception alarm.	Each service such as Guest Introspection 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 exception 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	Yes	VM needs to be rebooted for some changes to be made/take effect.	VM must be rebooted for some changes to be made or take effect. Action: Use the `resolve` API to resolve the alarm. This will reboot the VM.

Messaging System Events

The table explains system event messages related to messaging of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
390001	High	Yes	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	Yes	Host messaging connection reconfiguration failed.	In certain situations where NSX finds the RMQ broker details have changed, NSX tries to send the latest RMQ broker information to the host. If NSX fails to send the 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	Yes	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).
391002	Critical	No	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	No	Disabling messaging account {account #}. 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

The table explains system event messages for service composer of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
300000	Critical	Yes	Policy {#} 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.
300001	High	Yes	Policy is out of sync.	Service Composer encountered an error while attempting to enforce rules on this Service Policy. Action: See 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.
300002	High	Yes	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. Also, see "Troubleshooting issues with Service Composer in NSX 6.x" (http://kb.vmware.com/kb/2132612).
300003	High	Yes	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 is caused due to 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	Yes	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 is caused due to 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. Also, see "Troubleshooting issues with Service Composer in NSX 6.x" (http://kb.vmware.com/kb/2132612).
300005	High	Yes	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 using the `resolve` API.
300006	High	Yes	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 using the `resolve` API.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
300007	High	Yes	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 using the `resolve` API.
300008	High	Yes	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 using the `resolve` API.
300009	High	Yes	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 using the `resolve` API.
300010	High	Yes	Failure while initializing auto save drafts setting.	Service Composer encountered an error while initializing auto saved drafts settings. Action: Consult the error message to determine which policies and/or firewall sections to edit. Resolve the alarm via Service Composer or using the `resolve` API.

SVM Operations System Events

The table explains system event messages for service VM (SVM) operations of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
280002	High	Yes	Some of the events for this agent were missed by NSX. Probably reason could be reboot or temporary connectivity loss with Vcenter Server.Warning: Resolving the alarm will delete the VM and raise another indicating agent VM is missing. Resolving same will redeploy the VM.	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, and contact VMware technical support.
280003	High	Yes	Some of the events for this agent were missed by NSX. Probably reason could be reboot or temporary connectivity loss with vCenter Server.Warning: Resolving the alarm will restart the VM.	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 technical support.
280006	High	Yes	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 technical support.

Replication - Universal Sync System Events

The table explains system event messages for replication - universal sync of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
310001	Critical	No	Full sync failed for object type {#} on NSX Manager {#}.	Performing a full sync of universal objects on a secondary NSX Manager failed. Action: Collect the technical support logs for NSX Manager, and contact VMware technical support.
310003	Critical	No	Universal sync operation failed for the entity {#} on NSX Manager {#}.	Synchronizing a universal object to the secondary NSX Manager in a Cross-vCenter environment failed. Action: Collect the technical support logs for NSX Manager, and contact VMware technical support.

NSX Management System Events

The table explains system event messages for NSX Management of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
320001	Critical	No	The NSX Manager IP has been assigned to another machine with the MAC Address.	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

The table explains system event messages for VXLAN of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
814	Critical	No	Logical Switch {#} is no longer properly configured since some of the backing distributed virtual port groups were modified and/or removed.	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 is be shown on the Logical Switches page on thevSphere Web Client. Click the error to 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	No	VXLAN initialization failed on the host.	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`. Also, see the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.
1901	Critical	No	VXLAN port initialization failed on the host.	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`. Also, see the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.
1902	Critical	No	VXLAN instance does not exist on the host.	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`. Also, see the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
1903	Critical	No	Logical Switch {#} can't work properly since the backing IP interface couldn't join specific multicast group.	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`. Also, see the "Infrastructure Preparation" section in the *NSX Troubleshooting Guide*.
1905	Critical	No	Transport Zone may not be used since the backing IP interface can't acquire correct IP Address.	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	No	VXLAN overlay class is missing on DVS.	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	No	VXLAN Controller {#} has been removed due to the connection can't be built, please check controller IP configuration and deploy again.	The controller deployment failed. Action: Check that the assigned IP address is reachable. Also, see the "NSX Controller" section in the *NSX Troubleshooting Guide*.
1930	Critical	No	The controller {#} cannot establish the connection to the node {#}(active={#}). Current connection status = {#}.	Two controller nodes are disconnected, impacting controller to controller communication. Action: Refer to the "NSX Controller" section in the *NSX Troubleshooting Guide*.
1935	Critical	No	Host {#} information could not be sent to controllers as all controllers are inactive. Controller synchronization may be needed once controllers become active.	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	No	VXLAN vmknic {#} [PortGroup = {#}] is missing or deleted from host {#}.	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	No	VXLAN vmknic {#} [PortGroup = {#}] may have been deleted from the host {#} or the host-vCenter connection may have issues.	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 flags this event. After vCenter Server and the host finish rebooting, NSX Manager will check the VXLAN vmknics again and clear the event if everything is fine. Action: Resolve this issue if it is not transient by clicking the **Resolve** link on the **Installation > Logical Network Preparation > VXLAN Transport** tab.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
1941	Critical	No	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 Managerto 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	No	The backing portgroup [moid = {#}] of LogicalSwitch {#} is marked as missing.	NSX Manager detected a backing DV portgroup for an NSX logical switch is missing in Virtual Center. Action: Click the **Resolve** link on 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 port group.
1945	Critical	No	The device {#} on controller {#} has the disk latency alert on.	NSX Manager detected high disk latency for NSX Controller. Action: Refer to "NSX Controller" section in the *NSX Troubleshooting Guide*.
1947	Critical	No	Controller Virtual Machine is powered off on vCenter.	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 the **Resolve** button for the controller on 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	No	Controller Virtual Machine is deleted from vCenter.	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 on 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	No	The VXLAN portgroup [moid = dvportgroup-xx] and associated DVS have different teaming policies.	NSX Manager detected that a VXLAN port group's teaming policy is different from the teaming policy of the associated DVS. This can result in unpredictable behavior. Action: Configure the VXLAN port group or DVS again, so that they have the same teaming policy.

Identity Firewall System Events

The table explains system event messages for identity firewall (IDFW) of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
395000	Critical	No	SecurityLog on Domain Controller Eventlog Server is Full.	The security log in the Active Directory event log server is full. The IDFW, 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

The table explains system event messages for ESX Agent Manager (EAM) of major, critical, or high severity.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	High	Yes	EAM alarm received.	ESX Agent Manager (EAM) detected an NSX installation or upgrade issue with either NSX VIBs or service VMs. Action: To resolve the alarm, click the **Resolve** link on the **Installation > Host Preparation** tab, or by using the `resolve` API.

Index