NSX Logging and System Events

Update 6

VMware NSX Data Center for vSphere 6.4

vmware®

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

https://docs.vmware.com/

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

Copyright © 2010 - 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

NSX Logging and System Events

The *NSX Logging and System Events* document describes log messages, events, and alarms in the VMware NSX® Data Center for vSphere® system by using the VMware NSX® Manager™ user interface, the VMware vSphere® Web Client, and the VMware vSphere® Client™.

Important NSX for vSphere is now known as NSX Data Center for vSphere.

Intended Audience

This manual is intended for anyone who wants use or troubleshoot any problem for NSX Data Center for vSphere in a VMware vSphere® 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 vSphere, including VMware ESXi™, VMware vCenter Server®, and the vSphere Web Client.

Task Instructions

Task instructions in this guide are based on the vSphere Web Client. You can also perform some of the tasks in this guide by using the new vSphere Client. The new vSphere Client user interface terminology, topology, and workflow are closely aligned with the same aspects and elements of the vSphere Web Client.

Note Not all functionality of the NSX plug-in for the vSphere Web Client has been implemented for the vSphere Client in NSX 6.4. For an up-to-date list of supported and unsupported functionality, see https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/rn/nsx-vsphere-client-65-functionality-support.html.

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. In the vSphere Web Client, navigate to **Networking & Security > System > Events**.
2. Ensure that you are in the **Monitor** tab.
3. 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.

Setting the Logging Level of NSX Components

You can set the logging level for each NSX component.

The supported levels vary by component, as shown here.

```
nsxmgr> set
  hardware-gateway  Show Logical Switch Commands
  PACKAGE-NAME      Set log level
  controller        Show Logical Switch Commands
  host              Show Logical Switch Commands

nsxmgr> set hardware-gateway agent 10.1.1.1 logging-level
  ERROR
  WARN
  INFO
```

```
  DEBUG
  TRACE

nsxmgr-01a> set <package-name> logging-level
  OFF
  FATAL
  ERROR
  WARN
  INFO
  DEBUG
  TRACE

nsxmgr> set controller 192.168.110.31
  java-domain    Set controller node log level
  native-domain  Set controller node log level

nsxmgr> set controller 192.168.110.31 java-domain logging-level
  OFF
  FATAL
  ERROR
  WARN
  INFO
  DEBUG
  TRACE

nsxmgr> set controller 192.168.110.31 native-domain logging-level
  ERROR
  WARN
  INFO
  DEBUG
  TRACE

nsxmgr> set host host-28
  netcpa  Set host node log level by module
  vdl2    Set host node log level by module
  vdr     Set host node log level by module

nsxmgr> set host host-28 netcpa logging-level
  FATAL
  ERROR
  WARN
  INFO
  DEBUG

nsxmgr> set host host-28 vdl2 logging-level
  ERROR
  INFO
  DEBUG
  TRACE

nsxmgr> set host host-28 vdr logging-level
  OFF
  ERROR
  INFO
```

Enable Logging for IPSec VPN

You can enable logging of all IPSec VPN traffic.

By default, logging is enabled and is set to the WARNING level.

Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security > NSX Edges**.
3. Double-click an NSX Edge.
4. Click **Manage > VPN > IPSec VPN**.
5. Enable logging to log traffic flow between the local subnet and peer subnet.

NSX Version	Procedure
6.4.6 and later	a Next to **Logging Configuration**, click **Edit**. b Click the toggle switch to enable logging, and then select the logging level. c Click **Save**.
6.4.5 and earlier	a Next to **Logging Policy**, click ▶. b Select the **Enable logging** check box, and then select the logging level.

6. Click **Publish Changes**.

SSL VPN-Plus Logs

SSL VPN-Plus gateway logs are sent to the syslog server configured on the NSX Edge appliance.

The following table lists the locations on the remote user's computer where the SSL VPN-Plus client logs are stored.

Operating System	Location of Log File
Windows 8	`C:\Users\`*`username`*`\AppData\Local\VMware\vpn\svp_client.log`
Windows 10	`C:\Users\`*`username`*`\AppData\Local\VMware\vpn\svp_client.log`
Linux	System log files
Mac	Installation log file at `/tmp/naclient_install.log` System log files

Change SSL VPN-Plus Client Logs and Log Level

1. In the **SSL VPN-Plus** tab, click **Server Settings** from the left panel.
2. Go to the Logging Policy section and expand the section to view the current settings.
3. Click **Change**.
4. Select **Enable logging** check box to enable logging.

OR

Deselect **Enable logging** check box to disable logging.

5 Select the required log level.

Note SSL VPN-Plus client logs are enabled by default and log level is set to NOTICE.

6 Click **OK**.

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 In the vSphere Web Client, navigate to **Networking & Security > System > Events**.

2 Ensure that you are in the **Monitor** tab.

3 If multiple IP addresses are available in the **NSX Manager** drop-down menu, select an IP address, or keep the default selection.

The audit log details are displayed in the **Audit Logs** tab.

4 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.

5 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. NSX Manager supports five syslog servers.

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

Procedure

1 Log in to the NSX Manager virtual appliance.

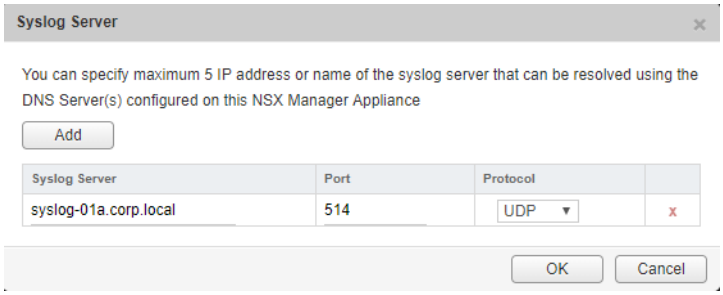
   In a Web browser, navigate to the NSX Manager appliance GUI at https://<nsx-manager-ip> or https://<nsx-manager-hostname>, and log in as **admin** or with an account that has the **Enterprise Administrator** role.

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

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

4 Specify 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 syslog server. If you have configured multiple syslog servers, logs are stored in all the configured syslog servers.

What to do next

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

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 > NSX Edges**.

3 Double-click an NSX Edge.

4 Navigate to configure syslog server settings.

Version	Procedure
NSX 6.4.4 and later	a Click **Manage > Settings > Appliance Settings**. b Next to Configuration, click ⚙, and then click **Change Syslog Configuration**.
NSX 6.4.3 and earlier	a Click **Manage > Settings > Configuration**. b In the **Details** pane, next to Syslog servers, click **Change**.

5 Type an IP address for both remote syslog servers.

6 Select a protocol, and click **OK**.

Configure DNS, NTP, and Syslog for the NSX Controller Cluster

You can configure DNS, NTP, and syslog servers for the NSX Controller cluster. The same settings apply to all NSX Controller nodes in the cluster.

Starting in NSX Data Center for vSphere 6.4.2, you can make these changes using the vSphere Web Client or vSphere Client. In earlier 6.4 versions, you can change NTP, and syslog settings using the API only. See the *NSX API Guide* for more information.

Important If you have an invalid configuration (for example, unreachable NTP servers), and then deploy a controller, the controller node deployment fails. Verify and correct the configuration and deploy the controller node again.

The NSX Controller cluster DNS settings override any DNS settings configured on the controller IP pool.

Procedure

1 Navigate to **Networking & Security > Installation and Upgrade > Management > NSX Controller Nodes**.

2 Select the NSX Manager that manages the NSX Controller nodes you want to modify.

3 Click the Common Controller Attributes **EDIT** link.

4 (Optional) Enter a comma-separated list of DNS servers, and optionally DNS suffixes.

DNS Setting	Example Values
DNS Servers	192.168.110.10, 192.168.110.11
DNS Suffixes	eng.example.com, corp.example.com, example.com

5 (Optional) Enter a comma-separated list of NTP servers.

You can enter the NTP servers as IPv4 addresses or fully qualified domain names (FQDN). If an FQDN is used, you must configure DNS so that the names can be resolved.

6 (Optional) Configure one or more syslog servers.

a In the Syslog Servers panel, click **ADD**.

b Enter the syslog server name or address.

You can enter the syslog servers as IPv4 addresses or fully qualified domain names (FQDN). If an FQDN is used, you must configure DNS so that the names can be resolved.

c Select the protocol.

If you select TLS, you must provide a PEM-encoded X.509 certificate.

Important Selecting TCP or TLS might result in extra consumption of memory for buffering that could negatively impact the performance of the controller. In extreme cases, this can stop controller processing until the buffered network log calls are drained.

a (Optional) Edit the port.

The default port for syslog, 6514, is entered by default.

b (Optional) Select the log level.

INFO is selected by default.

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.

You can collect the support bundle data for NSX components like NSX Manager, hosts, edges, and controllers using the **Support Bundle** collection tool. For details, refer to *NSX Administration Guide*.

Download Technical Support Logs for NSX

You can download NSX Manager system logs and Web Manager logs to your desktop. You can also collect the support bundle data for NSX Manager using the **Support Bundle** collection tool. For details, refer to *NSX Administration Guide*.

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 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. You can also collect the support bundle data for NSX Edge using the **Support Bundle** collection tool. For details, refer to *NSX Administration Guide*.

Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security > NSX Edges**.
3. Select an NSX Edge instance.
4. Click **Actions > Download Tech Support Logs**.
5. After the tech support logs are generated, click **Download**.

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. You can also collect the support bundle data for controllers using the **Support Bundle** collection tool. For details, refer to *NSX Administration Guide*.

To collect NSX Controller logs:

Procedure

1. Navigate to **Networking & Security > Installation and Upgrade > Management > NSX Controller Nodes**.
2. Select the controller for which you want to generate technical support logs.

   Caution Generate support logs for one controller at a time. An error might occur if you try to generate support logs for multiple controllers simultaneously.

3. Click **Support Logs** (or).

   NSX starts collecting the technical support logs. It takes several minutes for the log files to be generated. You can click **Cancel** at any time to abort the process and generate the support logs later.

4. After the support logs are generated, click **Download**.

   The support logs are saved on your computer in a compressed file with the `.tgz` 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.

NSX and Host Logs 2

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

You can collect the support bundle data for NSX components like NSX Manager, hosts, edges, and controllers using the **Support Bundle** collection tool. For details, refer to *NSX Administration Guide*.

This chapter includes the following topics:

About NSX Logs

You can configure the syslog server and view technical support logs for each NSX component. Management plane logs are available through NSX Manager and data plane logs are available through vCenter Server. Hence, it is recommended that you specify the same syslog server for the NSX component and vCenter Server in order to get a complete picture when viewing logs on the syslog server. For information on configuring a syslog server for hosts managed by a vCenter Server, see the appropriate version of vSphere documentation at https://docs.vmware.com.

Note Syslog or jump servers used to collect logs and access an NSX Distributed Logical Router (DLR) Control VM can't be on the logical switch that is directly attached to that DLR's logical interfaces.

Table 2-1. NSX Logs

Component	Description
ESXi Logs	These logs are collected as part of the VM support bundle generated from vCenter Server. For more information on ESXi log files, refer to vSphere documentation.
NSX Edge Logs	Use the `show log [follow | reverse]` command in the NSX Edge CLI. Download Technical Support Log bundle via NSX Edge UI.
NSX Manager Logs	Use the `show log` CLI command in the NSX Manager CLI. Download Technical Support Log bundle via the NSX Manager Virtual Appliance UI.
Routing Logs	See the *NSX Logging and System Events* Guide.

Table 2-1. NSX Logs (continued)

Component	Description
Firewall Logs	See *NSX Logging and System Events* Guide.
Guest Introspection Logs	See *NSX Logging and System Events* Guide.

NSX Manager

To specify a syslog server, see Configure a Syslog Server for NSX Manager.

To download technical support logs, see Download Technical Support Logs for NSX.

NSX Edge

To specify a syslog server, see Configure Syslog Servers for NSX Edge.

To download technical support logs, see Download Tech Support Logs for NSX Edge.

NSX Controller

To specify a syslog server, see Configure DNS, NTP, and Syslog for the NSX Controller Cluster.

To download technical support logs, see Download Technical Support Logs for NSX Controller.

Firewall

For more details, refer to Firewall Logs.

Firewall Logs

Firewall generates and stores log files, such as audit logs, rules message logs, and system event logs. You must configure a syslog server for each cluster that has enabled the firewall . The syslog server is specified in the `Syslog.global.logHost` attribute.

Recommendation To collect firewall audit logs on a syslog server, ensure that you have upgraded the syslog server to the recent version. Preferably, configure a remote syslog-ng server to collect the firewall audit logs.

Firewall generates logs as described in the following table.

Table 2-2. Firewall Logs

Log Type	Description	Location
Rules message logs	Include all access decisions such as permitted or denied traffic for each rule if logging was enabled for that rule. Contains DFW packet logs for the rules where logging has been enabled.	/var/log/dfwpktlogs.log
Audit logs	Include administration logs and Distributed Firewall configuration changes.	/home/secureall/secureall/logs/vsm.log

Table 2-2. Firewall Logs (continued)

Log Type	Description	Location
System event logs	Include Distributed Firewall configuration applied, filter created, deleted, or failed, and virtual machines added to security groups, and so on.	/home/secureall/secureall/logs/vsm.log
Data Plane/VMKernel logs	Capture activities related to a firewall kernel module (VSIP). It includes log entries for messages generated by the system.	/var/log/vmkernel.log
Message Bus Client/ VSFWD logs	Capture activities of a firewall agent.	/var/log/vsfwd.log

Note The *vsm.log* file can be accessed by running the `show log manager` command from the NSX Manager Command Line Interface (CLI) and performing *grep* for the keyword *vsm.log*. This file is accessible only to the user or user group having the *root* privilege.

Rules Message Logs

Rules message logs include all access decisions such as permitted or denied traffic for each rule, if logging was enabled for that rule. These logs are stored on each host in `/var/log/dfwpktlogs.log`.

Here are examples of firewall log message:

```
 # more /var/log/dfwpktlogs.log
2015-03-10T03:22:22.671Z INET match DROP domain-c7/1002 IN 242 UDP 192.168.110.10/138-
>192.168.110.255/138

# more /var/log/dfwpktlogs.log
2017-04-11T21:09:59.877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST
10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070
```

More examples:

```
2017-10-19T22:38:05.586Z 58734 INET match PASS domain-c8/1006 OUT 84 ICMP 172.18.8.121->172.18.8.119
RULE_TAG
2017-10-19T22:38:08.723Z 58734 INET match PASS domain-c8/1006 OUT 60 TCP 172.18.8.121/36485-
>172.18.8.119/22 S RULE_TAG
2017-10-19T22:38:18.785Z 58734 INET TERM domain-c8/1006 OUT ICMP 8 0 172.18.8.121->172.18.8.119 2/2
168/168 RULE_TAG
2017-10-19T22:38:20.789Z 58734 INET TERM domain-c8/1006 OUT TCP FIN 172.18.8.121/36484-
>172.18.8.119/22 44/33 4965/5009 RULE_TAG
```

In the following example:

- 1002 is the distributed firewall rule ID.
- domain-c7 is cluster ID in the vCenter managed object browser (MOB).
- 192.168.110.10/138 is the source IP address.

- 192.168.110.255/138 is the destination IP address.
- *RULE_TAG* is an example of the text that you add in the **Tag** text box while adding or editing the firewall rule.

The following example shows the results of a ping 192.168.110.10 to 172.16.10.12.

```
# tail –f /var/log/dfwpktlogs.log | grep 192.168.110.10

2015–03–10T03:20:31.274Z INET match DROP domain–c27/1002 IN 60 PROTO 1 192.168.110.10–>172.16.10.12
2015–03–10T03:20:35.794Z INET match DROP domain–c27/1002 IN 60 PROTO 1 192.168.110.10–>172.16.10.12
```

The following tables explain the text boxes in the firewall log message.

Table 2-3. Components of a log File Entry

Component	Value in example
Timestamp	2017-04-11T21:09:59
Firewall-specific portion	877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST 10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070

Table 2-4. Firewall-Specific Portion of log File Entry

Entity	Possible Values
Filter hash	A number that can be used to get the filter name and other information.
AF Value	INET, INET6
Reason	■ match: Packet matches a rule. ■ bad-offset: Datapath internal error while getting packet. ■ fragment: The non-first fragments after they are assembled to the first fragment. ■ short: Packet too short (for example, not even complete to include an IP header, or TCP/UDP header). ■ normalize: Malformed packets that do not have a correct header or a payload. ■ memory: Datapath out of memory. ■ bad-timestamp: Incorrect TCP timestamp. ■ proto-cksum: Bad protocol checksum. ■ state-mismatch: TCP packets that do not pass the TCP state machine check. ■ state-insert: Duplicate connection is found. ■ state-limit: Reached the maximum number of states that a datapath can track. ■ SpoofGuard: Packet dropped by SpoofGuard. ■ TERM: A connection is terminated.

Table 2-4. Firewall-Specific Portion of log File Entry (continued)

Entity	Possible Values
Action	■ PASS: Accept the packet. ■ DROP: Drop the packet. ■ NAT: SNAT rule. ■ NONAT: Matched the SNAT rule, but cannot translate the address. ■ RDR: DNAT rule. ■ NORDR: Matched the DNAT rule, but cannot translate the address. ■ PUNT: Send the packet to a service VM running on the same hypervisor of the current VM. ■ REDIRECT: Send the packet to network service running out of the hypervisor of the current VM. ■ COPY: Accept the packet and make a copy to a service VM running on the same hypervisor of the current VM. ■ REJECT: Reject the packet.
Rule set and rule ID	*rule set*/*rule ID*
Direction	IN, OUT
Packet length	*length*
Protocol	TCP, UDP, ICMP, or PROTO (protocol number) For TCP connections, the actual reason that a connection is terminated is indicated after the keyword TCP. If TERM is the reason for a TCP session, then an extra explanation appears in the PROTO row. The possible reasons for terminating a TCP connection include: RST (TCP RST packet), FIN (TCP FIN packet), and TIMEOUT (idle for too long) In the example above, it is *RST*. So it means that there is a *RST* packet in the connection that must be reset. For non-TCP connections (UDP, ICMP or other protocols), the reason for terminating a connection is only TIMEOUT.
Source IP address and port	*IP address*/*port*
Destination IP address and port	*IP address*/*port*
TCP flags	S (SYN), SA (SYN-ACK), A (ACK), P (PUSH), U (URGENT), F (FIN), R (RESET)
Number of packets	Number of packets. 22/14 - in packets / out packets
Number of bytes	Number of bytes. 7684/1070 - in bytes/ out bytes

To enable a rules message, log in to vSphere Web Client:

1 Navigate to **Networking & Security > Security > Firewall**.

2 Ensure that you are in the **General** tab.

3 Enable logging.

NSX Version	Procedure
NSX 6.4.1 and later	Click **More**>**Enable**>**Enable Rule Logs**
NSX 6.4.0	1 Enable the **Log** column on the page. 2 Enable logging for a rule by hovering over the Log table cell and clicking the pencil icon.

Note If you want customized text to be displayed in the firewall log message, you can enable the **Tag** column and add the required text by clicking the pencil icon.

Audit and System Event Logs

Audit logs include administration logs and Distributed Firewall configuration changes. These are stored in `/home/secureall/secureall/logs/vsm.log`.

System event logs include Distributed Firewall configuration applied, filter created, deleted, or failed, and virtual machines added to security groups, and so on. These logs are stored in `/home/secureall/secureall/logs/vsm.log`.

To view the audit and system event logs in the vSphere Web Client, navigate to **Networking & Security > System > Events**. In the **Monitor** tab, select the IP address of the NSX Manager.

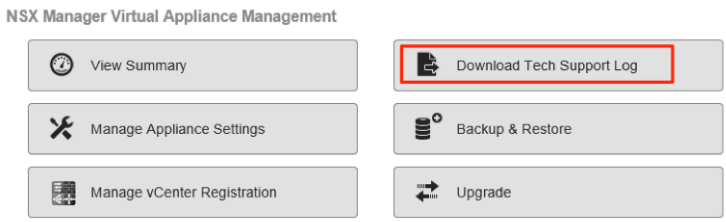
NSX Logs Relevant to Routing

The best practice is to configure all components of NSX to send their logs to a centralized collector, where they can be examined in one place.

If necessary, you can change the log level of NSX components. For more information, see "Setting the Logging Level of NSX Components" topic in *NSX Logging and System Events*.

NSX Manager Logs

- `show log` in the NSX Manager CLI
- Tech Support Log bundle, collected via the NSX Manager UI



The NSX Manager log contains information related to the management plane, which covers create, read, update, and delete (CRUD) operations.

Controller Logs

Controllers contain multiple modules, many with their own log files. Controller logs can be accessed using the `show log <log file> [ filtered-by <string> ]` command. The log files relevant to routing are as follows:

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log`: This log manages configuration and internal API server.
- `cloudnet/cloudnet.nsx-controller.log`: This is controller main process log.
- `cloudnet/cloudnet_cpp.log.nsx-controller.log`: This log manages clustering and bootstrap.
- `cloudnet/cloudnet_cpp.log.ERROR`: This file is present if any error occurs.

Controller logs are verbose and in most cases are required only for troubleshooting by VMware Customer Support.

In addition to the `show log` CLI, individual log files can be observed in real time as they are being updated, using the `watch log <logfile> [ filtered-by <string> ]` command.

The logs are included in the Controller support bundle that can be generated and downloaded by selecting a Controller node in the NSX UI and clicking the **Download tech support logs** icon.

ESXi Host Logs

NSX components running on ESXi hosts write several log files:

- VMkernel logs: `/var/log/vmkernel.log`
- Control Plane Agent logs: `/var/log/netcpa.log`
- Message Bus Client logs: `/var/log/vsfwd.log`

The logs can also be collected as part of the VM support bundle generated from vCenter Server. The log files are accessible only to the users or user groups having the *root* privilege.

ESG/DLR Control VM Logs

There are two ways to access log files on the ESG and DLR Control VMs—to display them using a CLI or to download the tech support bundle, using the CLI or UI.

The CLI command to display logs is `show log [ follow | reverse ]`.

To download tech-support bundle:

- From the CLI, enter `enable` mode, then run the `export tech-support <[ scp | ftp ]> <URI>` command.
- In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**. Select an Edge and click **Actions > Download Tech Support Logs**.

Other Useful Files and Their Locations

While not strictly logs, there are some files that can be helpful in understanding and troubleshooting NSX routing.

- The control plane agent configuration, `/etc/vmware/netcpa/config-by-vsm.xml` contains the information about the following components:
  - Controllers, IP addresses, TCP ports, certificate thumbprints, SSL enable/disable
  - dvUplinks on the DVS enabled with VXLAN (teaming policy, names, UUID)
  - DLR instances the host knows about (DLR ID, name)
- The control plane agent configuration, `/etc/vmware/netcpa/netcpa.xml` contains various configuration options for netcpa, including logging level (which by default is **info**).
- Control plane certificate files: `/etc/vmware/ssl/rui-for-netcpa.*`
  - Two files: host certificate and host private key
  - Used for authenticating host connections to Controllers

All these files are created by control plane agent using information it receives from NSX Manager via the message bus connection provided by vsfwd.

Guest Introspection Logs

There are several different logs you can capture to use while troubleshooting Guest Introspection.

ESX GI Module (MUX) Logs

If virtual machines on an ESXi host are not working with Guest Introspection, or if there are alarms on a host regarding communication to the SVA, then it could be a problem with the ESX GI Module on the ESXi host.

Log Path and Sample Message

MUX Log path
/var/log/syslog
var/run/syslog.log

ESX GI Module (MUX) messages follow the format of <timestamp>EPSecMUX<[ThreadID]>: <message>

For example:

```
2017-07-16T05:44:49Z EPSecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

In the above example

- [ERROR] is the type of message. Other types can be [DEBUG], [INFO]
- (EPSEC) represents that the messages are specific to Endpoint Security

Enabling and Viewing Log Files

To view the version of the ESX GI Module VIB installed on the host, run the `#esxcli software vib list | grep epsec-mux` command.

To turn on full logging, perform these steps on the ESXi host command shell:

1 Run the ps -c |grep Mux command to find the ESX GI Module processes that are currently running.

For example:

```
~ # ps -c | grep Mux
192223 192223 sh  /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t 1000000 /usr/lib/
vmware/vShield-Endpoint-Mux 900 -c 910
192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
```

2 If the service is not running, you can restart it with these commands:`/etc/init.d/vShield-Endpoint-Mux start` or `/etc//init.d/vShield-Endpoint-Mux restart`.

3 To stop the running ESX GI Module processes, including the watchdog.sh process, run the `~ # kill -9 192223 192233 192236` command.

Note that two ESX GI Module processes are spawned.

4 Start an ESX GI Module with a new -doption. Note that option -d does not exist for epsec-mux builds 5.1.0-01255202 and 5.1.0-01814505 `~ # /usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910`

5 View the ESX GI Module log messages in the `/var/log/syslog.log` file on the ESXi host. Check that the entries corresponding to the global solutions, solution ID, and port number are specified correctly.

Example: Sample muxconfig.xml File

```
<?xml version="1.0" encoding="UTF-8"?>

<EndpointConfig>

  <InstalledSolutions>

    <Solution>

      <id>100</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>

      <uuid>42383371-3630-47b0-8796-f1d9c52ab1d0</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/EndpointService (216)/EndpointService (216).vmx</
vmxPath>
```

```
    </Solution>
    <Solution>
      <id>102</id>
      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>
      <listenOn>ip</listenOn>
      <port>48651</port>
      <uuid>423839c4-c7d6-e92e-b552-79870da05291</uuid>
      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/apoon/EndpointSVM-alpha-01/EndpointSVM-alpha-01.vmx</
vmxPath>
    </Solution>
    <Solution>
      <id>6341068275337723904</id>
      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>
      <listenOn>ip</listenOn>
      <port>48655</port>
      <uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>
      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>
    </Solution>
  </InstalledSolutions>
  <DefaultSolutions/>
  <GlobalSolutions>
    <solution>
      <id>100</id>
      <tag></tag>
      <order>0</order>
    </solution>
    <solution>
      <id>102</id>
```

```
      <tag></tag>
      <order>10000</order>
    </solution>
    <solution>
      <id>6341068275337723904</id>
      <tag></tag>
      <order>10001</order>
    </solution>
  </GlobalSolutions>
</EndpointConfig>
```

GI Thin Agent Logs

The thin agent is installed on the VM Guest OS and detects user logon details.

Log Path and Sample Message

The thin agent consists of GI drivers – vsepflt.sys, vnetflt.sys, vnetwfp.sys (Windows 10 and later).

The thin agent logs are on the ESXi host, as part of the VCenter Log Bundle. The log path is `/vmfs/volumes/<datastore>/<vmname>/vmware.log` For example: `/vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log`

Thin agent messages follow the format of <timestamp> <VM Name><Process Name><[PID]>: <message>.

In the log example below `Guest: vnet or Guest:vsep`, indicate log messages related to the respective GI drivers, followed by debug messages.

For example:

```
2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
 vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore
```

Example: Enabling vShield Guest Introspection Thin Agent Driver Logging

Because the debug setting can flood the vmware.log file to the point that it throttles, we recommend you disable the debug mode as soon as you have collected all the required information.

This procedure requires you to modify the Windows registry. Before you modify the registry, ensure to take a backup of the registry. For more information on backing up and restoring the registry, see the Microsoft Knowledge Base article 136393.

To enable debug logging for the thin agent driver:

1 Click **Start > Run**. Enter regedit, and click **OK**. The Registry Editor window opens. For more information seen the Microsoft Knowledge Base article 256986.

2 Create this key using the registry editor: `HKEY_LOCAL_Machine\SYSTEM\CurrentControlSet\services\vsepflt\parameters`.

3 Under the newly created parameters key, create these DWORDs. Ensure that hexadecimal is selected when putting in these values:

```
Name: log_dest
Type: DWORD
Value: 0x2

Name: log_level
Type: DWORD
Value: 0x10
```

Other values for `log level` parameter key:

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

4 Open a command prompt as an administrator. Run these commands to unload and reload the vShield Endpoint filesystem mini driver:

- `fltmc unload vsepflt`
- `fltmc load vsepflt`

You can find the log entries in the vmware.log file located in the virtual machine.

Enabling vShield GI Network Introspection Driver Logging

Because the debug setting can flood the vmware.log file to the point that it can make it to throttle, we recommend you disable the debug mode as soon as you have collected all the required information.

This procedure requires you to modify the Windows registry. Before you modify the registry, ensure to take a backup of the registry. For more information on backing up and restoring the registry, see the Microsoft Knowledge Base article 136393.

1 Click **Start > Run**. Enter regedit, and click **OK**. The Registry Editor window opens. For more information seen the Microsoft Knowledge Base article 256986.

2 Edit the registry:

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest"  = DWORD: 0x00000001
```

3 Reboot the virtual machine.

vsepflt.sys and vnetflt.sys Log File Location

With the log_dest registry settings DWORD: 0x00000001, the Endpoint thin agent driver logs into the debugger. Run the debugger (DbgView from SysInternals or windbg) to capture the debug output.

Alternatively you can set the log_dest registry setting to DWORD:0x000000002, in which case the driver logs will be printed to vmware.log file, which is located in the corresponding virtual machine folder on the ESXi Host.

Enabling UMC logging

The Guest Introspection user-mode component (UMC) runs within the VMware Tools service in the protected virtual machine.

1 On Windows XP and Windows Server 2003, create a `tools config` file if it doesn't exist in the following path: `C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf`.

2 On Windows Vista, Windows 7 and Windows Server 2008, create a `tools config` file if it doesn't exist in the following path: `C:\ProgramData\VMWare\VMware Tools\tools.conf`

3 Add these lines in the `tools.conf` file to enable UMC component logging.

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

With the `vsep.handler = vmx` setting, the UMC component logs into the `vmware.log` file, which is located in the corresponding virtual machine folder on the ESXi host.

With the following setting logs, the UMC component logs will be printed in the specified log file.

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

GI EPSecLib and SVM Logs

The EPSecLib receives events from the ESXi host ESX GI Module (MUX).

Log Path and Sample Message

EPSecLib Log Path
/var/log/syslog
var/run/syslog

EPSecLib messages follow the format of <timestamp> <VM Name><Process Name><[PID]>: <message>

In the following example [ERROR] is the type of message and (EPSEC) represents the messages that are specific to Guest Introspection.

For example:

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
 [7203] Initializing EPSec library build: build-00000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

Collecting Logs

To enable debug logging for the EPSec library, which is a component inside GI SVM:

1 Log in to the GI SVM by obtaining the console password from NSX Manager.

2 Create `/etc/epseclib.conf` file and add:

`ENABLE_DEBUG=TRUE`

`ENABLE_SUPPORT=TRUE`

3 Change permissions by running the `chmod 644 /etc/epseclib.conf` command.

4 Restart the GI-SVM process by running the `/usr/local/sbin/rcusvm restart` command.

This enables debug logging for EPSecLib on the GI SVM. The debug logs can be found in /var/log/messages. Because the debug setting can flood the vmware.log file, disable the debug mode as soon as you have collected all the required information.

GI SVM Logs

Before you capture logs, determine the Host ID, or Host MOID:

- Run the `show cluster all` and `show cluster <cluster ID>` commands in the NSX Manager.

  For example:

```
nsxmgr-01a> show cluster all

No.  Cluster Name       Cluster Id              Datacenter Name   Firewall Status
1    RegionA01-COMP01   domain-c26              RegionA01         Enabled
```

```
2    RegionA01-MGMT01   domain-c71               RegionA01         Enabled

nsxmgr-01a> show cluster  domain-c26

Datacenter: RegionA01
Cluster: RegionA01-COMP01
No.  Host Name            Host Id                  Installation Status
1    esx-01a.corp.local   host-29                  Ready
2    esx-02a.corp.local   host-31                  Ready
```

1 To determine the current logging state, run this command:

`GET https://nsxmanager/api/1.0/usvmlogging/host-##/com.vmware.vshield.usvm`

`GET https://nsxmanager/api/1.0/usvmlogging/host-##/root`

2 To change the current logging state, run this command:

`POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel`

```
## Example to change root logger ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>

## Example to change com.vmware.vshield.usvm ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>com.vmware.vshield.usvm</loggerName>
<level>DEBUG</level>
</logginglevel>
```

3 To generate logs, run this command:

`GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs`

Select `Send` and `Download`.

Note that this command generates GI SVM logs and saves the file as `techsupportlogs.log.gz` file. Because the debug setting can flood the vmware.log file, disable the debug mode as soon as you have collected the required information.

System Events

3

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.
- To collect NSX Edge technical support logs, see Download Tech Support Logs for NSX Edge.
- 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*.
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.
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.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301035	Information or Major	No	`Firewall rules applied to host.`	A firewall ruleset is published successfully to the host. Starting in NSX 6.4.0, this system event is an "information" event. However, in all NSX 6.2.x and 6.3.x releases, it is a "major" event. Therefore, when you upgrade from NSX 6.2.x or 6.3.x to NSX 6.4.0 or later, this system event continues to be classified as a "major" event. In a fresh installation of NSX 6.4.0 or later, this event is an "information" event. If SNMP is used, an SNMP trap is triggered. Action: No action is required.
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.
301083	Critical	No	`Firewall Concurrent Connections threshold crossed.`	The maximum concurrent connections threshold for the host firewall agent is exceeded for the specified vNIC. Action: Reduce the amount of traffic on the vNIC.
301084	Critical	No	`Firewall Process Memory threshold crossed.`	The memory utilization threshold for the host firewall agent is exceeded. Action: Reduce the number of rules or security groups/containers in the firewall configuration. If the issue persists, a memory leak may have occurred. To recover from this condition, collect the technical support logs for NSX Manager and host, and contact VMware technical support.
301085	Critical	No	`Firewall CPU threshold cross cleared.`	CPU usage for the host firewall agent is below threshold level. Action: Information-only event. No action is required.
301086	Critical	No	`Firewall Heap Memory threshold cross cleared.`	The heap memory usage of the host firewall agent is below threshold level. Action: Information-only event. No action is required.
301087	Critical	No	`Firewall Connections per second threshold cross cleared.`	The connections per second (CPS) value for the host firewall agent is below the threshold level for the specified vNIC. Action: Information-only event. No action is required.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
301088	Critical	No	`Firewall Concurrent Connections threshold cross cleared.`	The maximum concurrent connections value for the host firewall agent is below threshold level for the specified vNIC. Action: Information-only event. No action is required.
301089	Critical	No	`Firewall Process Memory threshold cross cleared.`	The memory utilization of the host firewall agent is below the threshold level. Action: Information-only event. No action is required.
301098	Critical	No	`Firewall threshold configuration applied to host.`	The event thresholds for distributed firewall are applied successfully. Action: Information-only event. No action required.
301099	Critical	No	`Failed to apply firewall threshold configuration to host.`	The event thresholds for distributed firewall failed to be applied. Certain threshold values are unchanged. Contextual data provided with this event may indicate the cause of this failure. Action: If the issue persists, collect the technical support logs for the NSX Manager and host, and contact VMware technical support. Ensure that the host logs cover the period when the host received the firewall configuration update. After collecting the logs, force synchronize the firewall configuration to recover.
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.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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.
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 Upgrade** and select the Host Preparation tab. Verify that Firewall Status displays as green.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 Upgrade** 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.
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.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 and Upgrade > Host Preparation** and, under **Actions**, select **Force Sync Services**.
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 and Upgrade > 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 and Upgrade > 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.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 trigger 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 Managerreports that the NSX Edge VM is in 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.
30014	Major	N/A	`Failed to communicate with the NSX Edge VM.`	The NSX Manager communicates with NSX Edge Message Bus. This event indicates that NSX Manager has 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.

Event Code	Event Severity	Alarm Code	Event Message	Description
30033	High	130033	`NSX Edge VM (vmId : {#}) is not responding to NSX manager health check. Please check NSX manager logs for details.`	The NSX Edge VM is not responding to the health check sent by the NSX Manager. Action: Make sure that the NSX Edge VM is powered on, and investigate the NSX manager logs.
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.
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.
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.

Event Code	Event Severity	Alarm Code	Event Message	Description
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.
30157	Critical	130157	`NSX Edge (Edge ID} detected duplicate IP {IP address} with macAddress {MAC address}.`	An NSX Edge interface IP address is detected on another device on the network. Action: Investigate the network to locate the other device.
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.
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 a scenario, both the VMs 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.

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).
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	`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*.

Event Code	Event Severity	Alarm Code	Event Message	Description
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*.
30902	Critical	130902	`BGP Neighbor {Neighbor ID} is down.`	The state of an NSX Edge BGP neighbor has changed to down. Action: Use the Edge CLI to troubleshoot the routing or network condition.
30903	Critical	130903	`BGP Neighbor {Neighbor ID} AS Mismatch {AS Number} is not matching.`	The autonomous system (AS) number of the BGP neighbor does not match the AS number of the NSX Edge. Action: Make sure that the AS number that you have configured on the BGP neighbor matches the AS number on the NSX Edge.
30905	Critical	130905	`OSPF Neighbor is down. Source ip address:{IP address}, routerId: {ID}.`	The state of an NSX Edge OSPF neighbor relationship has changed to down. Action: Investigate the network or configuration issue.
30906	Critical	130906	`OSPF MTU mismatch. Source routerId: {Router ID}. Configured MTU: {Value}. Source MTU: {Value}.`	An NSX Edge OSPF neighbor relationship cannot be established because of MTU mismatch. Action: Check the MTU configured on both OSPF neighbors and make sure that the MTU matches.
30907	Critical	130907	`OSPF areaId mismatch. Source routerId:{ID}. Configured areaId: {Value}. Source areaId: {Value}.`	An NSX Edge OSPF neighbor relationship cannot be established because of mismatch in the OSPF area ID. Action: Check the area ID configured on both OSPF neighbors and make sure that the area ID matches.

Event Code	Event Severity	Alarm Code	Event Message	Description
30908	Critical	130908	`OSPF helloTimer mismatch. Source routerId:{ID}. Configured helloTimer: {Value}. Source helloTimer: {Value}.`	An NSX Edge OSPF neighbor relationship cannot be established because of mismatch in the OSPF hello interval. Action: Check the hello interval configured on both OSPF neighbors and make sure that the hello interval matches.
30909	Critical	130909	`OSPF deadTimer mismatch. Source routerId:{ID}. Configured deadTimer: {Value}. Source deadTimer: {Value}.`	An NSX Edge OSPF neighbor relationship cannot be established because of mismatch in the OSPF dead interval. Action: Check the dead interval configured on both OSPF neighbors and make sure that the dead interval matches.
31002	Critical	131002	`L2VPN tunnel for {user ID} and {server IP} is down. Failure message: {message}.`	This event is a client-side event. L2VPN client failed to establish tunnel with the L2VPN server. This event might be due to a misconfiguration issue, or the L2VPN server might not be reachable. Action: Try one of the following steps to resolve the problem: ■ Check whether the server address, server port, and encryption algorithm are configured correctly. ■ Make sure that the L2VPN Edge client has internet connectivity on the uplink port, and the L2VPN Edge server is reachable. ■ Make sure that port 443 is not blocked by the firewall.

Event Code	Event Severity	Alarm Code	Event Message	Description
31004	Critical	131004	`L2VPN tunnel to {site} is down. Failure message: {message}.`	This event is a server-side event and it occurs in the following situations: ■ You configured a site on the L2VPN server. ■ Tunnel with L2VPN client has gone down due to any reason. Action: Perform the following steps: 1 On the L2VPN client, check the reason for the tunnel failure. 2 Download the Tech Support Logs for the NSX Edge, and check the log files that are related to L2VPN. Typically, all the logs for the L2VPN server have the following format: `{Date}NSX-edge-1-0l2vpn:[local0:info]INFO: {MESSAGE}` 3 In all the L2VPN logs, check for any failure or error message.
31005	Critical	131005	`L2VPN tunnel to {site} with {client IP} got reconnected.`	This event is a server-side event and it occurs in the following situations: ■ Tunnel with the L2VPN client is up, and the client is restarted. ■ Network connection to client drops and is restored again within the timeout period. Action: No action is required.

Fabric System Events

The table explains system event messages for the Fabric system events.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
250000	Informational	No	`Deployment unit old operational status was {#} , new operational status is {#} and old progress state was {#}, new progress state is {#}. Check alarm string for root cause.`	Information-only event.
250001	Informational	No	`A deployment unit has been created.`	Information-only event.
250002	Informational	No	`A deployment unit in NSX has been updated. Fabric services will be updated on the cluster.`	Information-only event.
250003	Informational	No	`A deployment unit has been deleted from NSX.`	Information-only event.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
250004	High	Yes	`Failed to deploy service {#} on host {#} since datastore (#) is not connected to the host. Please verify that it is connected, or provide a different datastore.`	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 confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.`	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 confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.', Module:'Security Fabric'`. Action: Refer to *NSX Troubleshooting Guide*.
250006	Informational	No	`The fabric agent for network fabric services installed successfully on a host.`	Information-only event.
250007	Informational	No	`The fabric agent was removed successfully from a host.`	Information-only event.
250008	High	Yes	`Location of OVF / VIB files has changed. Service must be redeployed.`	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: Click the **Resolve**option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
250009	High	Yes	`Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.`	EAM has failed to access VIBs/OVFs from NSX during a host upgrade. In the vCenter system events table, you see: `Event Message:'Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.', Module:'Security Fabric'`. Action: Refer to *NSX Troubleshooting Guide*.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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. The solution may not be reachable/ responding. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be redeployed.`	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 `action=resolve` parameter in the `systemalarms` 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. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be redeployed.`	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 `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
250016	High	No	`Uninstallation of service failed. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.`	Uninstallation of service failed. Action: Ensure that solution URLs are accessible from NSX, and NSX is reachable from the solution. Use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
250017	High	Yes	`Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.`	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 `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
250018	High	Yes	`Error while notifying security solution before uninstall.Resolve to notify once again, or delete to uninstall without notification. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.`	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 `action=resolve` parameter in the `systemalarms` API to resolve the alarm.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
250019	High	Yes	`Server rebooted while security solution notification for uninstall was going on. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be uninstalled.`	Server was rebooted while security solution notification for uninstall was in progress. Action: Ensure that solution URLs are accessible from NSX. Use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm. Service will be uninstalled.
250020	High	Yes	`Server rebooted while security solution notification for upgrade was going on. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be redeployed.`	Server was rebooted while security solution notification for upgrade was in progress. Action: Ensure that solution URLs are accessible from NSX. Use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm. Service will be redeployed.
250021	Critical	No	`NSX Manager relies on the EAM service in vCenter for deploying/monitoring NSX vibs on ESX. The connection to this EAM service has gone down. This could be due to EAM service or vCenter restart/stop or an issue in the EAM service. Verify that vCenter is up, and the EAM service in vCenter is running. Further, we can look at EAM mob to verify that EAM is functioning as expected.`	NSX Manager relies on the EAM service in vCenter for deploying/monitoring NSX VIBs on ESX. The connection to this EAM service is down. This could be due to EAM service or vCenter has restarted/stoped or an issue in the EAM service. Action: Verify that vCenter is up and that the EAM service in vCenter is running. Verify that the EAM MOB URL **`http://{vCenter_IP}/eam/mob/`** is accessible and EAM is functioning as expected. For more information, refer to "Infrastructure Preparation" in the *NSX Troubleshooting Guide*.
250022	Critical	No	`NSX Manager relies on the EAM service in VC for deploying/monitoring NSX vibs on ESX. The connection to this EAM service has gone down. This could be due to EAM service or VC restart/stop or an issue in the EAM service. Verify that VC is up, and the EAM service in VC is running. Further, we can look at EAM mob to verify that EAM is functioning as expected.`	NSX Manager relies on the EAM service in vCenter for deploying/monitoring NSX VIBs on ESX. The connection to this EAM service is down. This could be due to EAM service or vCenter has restarted/stoped or an issue in the EAM service. Action: Verify that vCenter is up and that the EAM service in vCenter is running. Verify that the EAM MOB URL **`http://{vCenter_IP}/eam/mob/`** is accessible and EAM is functioning as expected. For more information, refer to "Infrastructure Preparation" in the *NSX Troubleshooting Guide*.
250023	High	Yes	`Pre Uninstall cleanup failed. Use resolve API to resolve the Alarm. Service will be removed.`	Internal cleanup tasks prior to uninstallation failed to complete. Action: Use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm. Service will be removed.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
250024	High	Yes	`The backing EAM agency for this deployment unit 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 unit 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	`This event is generated when an attempt is made to upgrade or uninstall NSX vibs on stateless host using EAM. All stateless host should be prepared using the auto deploy feature. Fix configuration using auto deploy feature, and use the resolve API to resolve the alarm.`	This event is generated when an attempt is made to upgrade or uninstall NSX VIBS 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 `action=resolve` parameter in the `systemalarms` API to resolve the alarm.

Deployment Plug-in System Events

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

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.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 and Upgrade > Host Preparation** tab. Action: For troubleshooting steps, refer to *NSX Troubleshooting Guide*.
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: For troubleshooting steps, refer to *NSX Troubleshooting Guide*.
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: For troubleshooting steps, refer to *NSX Troubleshooting Guide*.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
391002	Critical	No	`Messaging infrastructure down on host.`	Two or more heartbeat messages between NSX Manager and an NSX host were missed. Action: For troubleshooting steps, refer to *NSX Troubleshooting Guide*.
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. For troubleshooting steps, refer to *NSX Troubleshooting Guide*.

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. Resolve the alarm via Service Composer or use the `action=resolve` parameter in the `systemalarms` API to resolve the 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).

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 `action=resolve` parameter in the `systemalarms` API. See also "Troubleshooting issues with Service Composer in NSX 6.x" (http://kb.vmware.com/kb/2132612). Resolve the alarm via Service Composer or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
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 use the `action=resolve` parameter in the `systemalarms` 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 use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
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 use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
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 use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
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 use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.

GI SVM System Events

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

Event Code	Event Severity	Alarm Triggered	Event Message	Description
295002	Major			NSX Manager is not receiving heartbeats from the Guest Introspection USVM. Action: Collect the NSX Manager and USVM technical support logs and open a technical support request.
295003	Informational			NSX Manager is receiving heartbeats from the USVM. Action: Recovering event after event 295002 is reported.
295010	Informational			The connection between the USVM and the Guest Introspection host module is established. Action: Information-only event. No action required.

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 `action=resolve` parameter in the `systemalarms` 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.
360001	Critical	Yes (SNMP alert)	`Certificate {#} has expired.`	As certificate is now invalid, you may experience problems while performing operations in NSX. Renew certificate as per instructions provided by your certificate authority (CA).
360002	Critical	Yes (SNMP alert)	`Certificate {#} will expire on {#}.`	If you allow a certificate to expire, the certificate becomes invalid, , you may experience problems while performing operations in NSX. Renew certificate as per instructions provided by your certificate authority (CA).

Logical Network System Events

The table explains system event messages related to logical networking.

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 VMkernel NICs 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 VMkernel NICs 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*.
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 VMkernel NIC failed to be assigned a valid IP address. All VXLAN traffic through the VMkernel NIC 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).

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 VMkernel NIC is missing or deleted from the host. Traffic to and from the host will be affected. Action: To resolve the issue, click the **Resolve** button on the **Installation and Upgrade > 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 VMkernel NIC 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 VMkernel NIC and flags this event. After vCenter Server and the host finish rebooting, NSX Manager will check the VXLAN VMkernel NICs again and clear the event if everything is fine. Action: Resolve this issue if it is not transient by clicking the **Resolve** button on the **Installation and Upgrade > 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 Upgrade** 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** button on the **Installation and Upgrade > 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*.
1946	Informational	No	`All disk latency alerts on controller {0} are off.`	NSX Manager no longer detects high disk latency on a controller. Action: Information-only event. No action is required.
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 and Upgrade > Management** tab or call the API POST `https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate` to power on the controller VM.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
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 and Upgrade > 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.

Host Preparation System Events

The table explains all system event messages related to host preparation.

Note Multiple ESX Agent Manager events map to a single event on NSX.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	Informational	Yes	`A VIB module has been uploaded to the host {hostID}, but will not be fully installed until the host {hostID} has been put in maintenance mode.`	ESX Agent Manager puts host in the maintenance mode. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	Critical	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent virtual machine cannot be deployed because the vSphere ESX Agent Manager is unable to access the OVF package for the agent. This typically happens because the Web server providing the OVF package is down. The Web server is often internal to the solution that created the Agency.`	ESX Agent Manager redeploys the agent. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	Critical	Yes	`An agent VIB module is expected to be deployed on a host, but the VIM module cannot be deployed because the vSphere ESX Agent Manager is unable to access the VIB package for the agent. This typically happens because the Web server providing the VIB package is down. The Web server is often internal to the solution that created the Agency.`	ESX Agent Manager reinstalls the VIB module. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent could not be deployed because it was incompatible with the host {hostID}.`	vSphere ESX Agent Manager redeploys the agent . Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm. However, the problem is likely to persist until you upgrade either the host or the solution, so that the agent becomes compatible with the host.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	High	Yes	`An agent virtual machine is expected to be powered on, but there are no free IP addresses in the agent's pool of virtual machine IP addresses.`	Action: To resolve the issue, free some IP addresses or add some more IP addresses to the IP pool and then use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent virtual machine could not be deployed because the host {hostID} does not have enough free CPU or memory resources.`	ESX Agent Manager redeploys the agent virtual machine. However, the problem is likely to persist until enough CPU and memory resources are made available. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent virtual machine could not be deployed because the host's agent datastore did not have enough free space.`	ESX Agent Manager redeploys the agent virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm. However, the problem is likely to persist until either: You free-up space on the host's agent virtual machine datastore. -Or- Configure a new agent virtual machine datastore with enough free space.
270000	High	Yes	`An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off because there there are no IP addresses defined on the agent's virtual machine network.`	Action: Create an IP pool on the agent's virtual machine network and use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent datastore has not been configured on the host {hostID}.`	Action: You must configure the agent virtual machine datastore on the host.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent network has not been configured on the host.`	Action: You must configure the agent virtual machine network on the host.
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent network has not been configured on the host. The host needs to be added to one of the networks listed in customAgentVmNetwork.`	Action: You must add one of the *customAgentVmNetwork* networks to the host.
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent datastore has not been configured on the host. The host needs to be added to one of the datastores listed in customAgentVmDatastore.`	You must add one of the datastores named *customAgentVmDatastore* to the host.
270000	High	Yes	`The solution that created the agency is no longer registered with the vCenter server.`	ESX Agent Manager removes the agency. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`A dvFilter switch exists on a host but no agents on the host depend on dvFilter. This typically happens if a host is disconnected when an agency configuration changed.`	ESX Agent Manager removes the *dvFilterSwitch*. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	High	Yes	`An Agent virtual machine is expected to be provisioned on a host, but it failed to do so because the provisioning of the OVF package failed. The provisioning is unlikely to succeed until the solution that provides the OVF package has been upgraded or patched to provide a valid OVF package for the agent virtual machine.`	ESX Agent Manager attempts the OVF provisioning again. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine needs to be powered on, but an OVF property is either missing or has an invalid value.`	Action: Update the OVF environment in the agent configuration used to provision the agent virtual machine.
270000	High	Yes	`An agent virtual machine has been found in the vCenter inventory that does not belong to any agency in this vSphere ESX Agent Manager server instance.`	ESX Agent Manager powers off (if powered on) and deletes the agent virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`A VIB module requires the host to be in maintenance mode, but the vSphere ESX Agent Manager is unable to put the host in maintenance mode. This can happen if there are virtual machines running on the host that cannot be moved and must be stopped before the host can enter maintenance mode.`	ESX Agent Manager tries to put the host into maintenance mode. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm. However, the problem is likely to persist until you power off or move virtual machines to put the host into maintenance mode.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	Critical	Yes	`A VIB module is expected to be installed on a host, but it failed to install since the VIB package is in an invalid format. The installation is unlikely to succeed until the solution providing the bundle has been upgraded or patched to provide a valid VIB package.`	ESX Agent Manager attempts the VIB installation again. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`A VIB module is expected to be installed on a host, but it has not been installed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why the VIB module installation failed.`	ESX Agent Manager attempts the VIB installation again. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	informational	Yes	`A VIB module has been uploaded to the host, but will not be activated until the host is rebooted.`	ESX Agent Manager puts the host into maintenance mode and reboots it. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`A VIB module failed to install, but failed to do so because automatic installation by vSphere ESX Agent Manager is not allowed on the host.`	Action: Go to vSphere Update Manager and install the required bulletins on the host or add the bulletins to the host's image profile.For more details, refer to vSphere documentation.
270000	High	Yes	`A VIB module failed to uninstall, but failed to do so because automatic uninstallation by vSphere ESX Agent Manager is not allowed on the host.`	Action: Go to vSphere Update Manager and uninstall the required bulletins on the host or add the bulletins to the host's image profile.For more details, refer to vSphere documentation.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	High	Yes	`An agent virtual machine is corrupt.`	ESX Agent Manager deletes and re-provisions the agent virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm. To resolve the issue manually: Resolve the problem related to the missing file and power on the agent virtual machine.
270000	High	Yes	`An agent virtual machine is expected to be removed from a host, but the agent virtual machine has not been removed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why vSphere ESX Agent Manager was unable to remove the agent virtual machine, such as the host is in maintenance mode, powered off or in standby mode.`	ESX Agent Manager redeploys the agent. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is a virtual machine template.`	ESX Agent Manager converts the agent virtual machine template to a virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	High	Yes	`An agent virtual machine is expected to be deployed on a host, but the agent virtual machine has not been deployed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why vSphere ESX Agent Manager was unable to deploy the agent, such as being unable to access the OVF package for the agent or a missing host configuration. This issue can also happen if the agent virtual machine is explicitly deleted from the host.`	ESX Agent Manager redeploys the agent virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off.`	ESX Agent Manager powers on the agent virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be powered off, but the agent virtual machine is powered off.`	ESX Agent Manager powers off the agent virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be powered on, but the agent virtual machine is suspended.`	ESX Agent Manager powers on the agent virtual machine. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`An agent virtual machine is expected to be located in a designated agent virtual machine folder, but is found in a different folder.`	ESX Agent Manager moves the agent virtual machine back into the designated agent folder. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.

Event Code	Event Severity	Alarm Triggered	Event Message	Description
270000	High	Yes	`An agent virtual machine is expected to be located in a designated agent virtual machine resource pool, but is found in a different resource pool.`	ESX Agent Manager moves the agent virtual machine back into the designated agent resource pool. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.
270000	High	Yes	`EAM alarm received.`	ESX Agent Manager detected an NSX installation or upgrade issue with either NSX VIBs or service VMs. Action: Click the **Resolve** option on the **Host Preparation** tab, or use the `action=resolve` parameter in the `systemalarms` API to resolve the alarm.