NSX-Protokollierung und -Systemereignisse

Update 5
Geändert am 16. November 2017
VMware NSX for vSphere 6.3

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

NSX-Protokollierung und -Systemereignisse

Im Dokument *NSX-Protokollierung und -Systemereignisse* werden Protokollmeldungen, Ereignisse und Alarme des VMware NSX® for vSphere®-Systems mithilfe der NSX Manager-Benutzeroberfläche und des vSphere Web Client beschrieben.

Zielgruppe

Dieses Handbuch ist für alle Benutzer gedacht, die NSX in einer VMware vCenter-Umgebung nutzen oder eine Fehlerbehebung dafür durchführen möchten. Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb virtueller Datencenter vertraut sind. Dieses Handbuch setzt voraus, mit VMware vSphere, einschließlich VMware ESXi, vCenter Server und dem vSphere Web Client vertraut zu sein.

VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

Systemereignisse, Alarme und Protokolle

1

Mit Systemereignissen, Alarmen und Protokollen können Sie die Integrität und die Sicherheit der NSX-Umgebung überwachen sowie Probleme beheben.

Dieses Kapitel behandelt die folgenden Themen:

Systemereignisse

Systemereignisse sind Aufzeichnungen von Systemaktionen. Für jedes Ereignis gilt eine Schweregrad wie z. B. „Zur Information“ oder „Kritisch“, um anzuzeigen, wie schwerwiegend das Ereignis ist. Systemereignisse werden auch als SNMP-Traps übertragen, sodass jede SNMP-Verwaltungssoftware in der Lage ist, NSX-Systemereignisse zu überwachen.

Anzeigen des Systemereignisberichts

In vSphere Web Client können Sie alle Systemereignisse für die von NSX Manager verwalteten Komponenten anzeigen lassen.

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
3. Klicken Sie auf einen NSX Manager in der Spalte **Name** und anschließend auf die Registerkarte **Überwachen**.

4 Klicken Sie auf die Registerkarte **Systemereignisse**.

Sie können die Ereignisse durch Klicken auf die Pfeile in der Spaltenüberschrift sortieren oder mithilfe des Textfeldes **Filter** filtern.

Format von Systemereignissen

Wenn Sie einen Syslog-Server angeben, sendet NSX Manager alle Systemereignisse an den Syslog-Server.

Das Format dieser Meldungen ähnelt dem folgenden:

```
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
```

Das Systemereignis enthält die folgenden Informationen.

```
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.
```

Alarme

Alarme sind Benachrichtigungen, die als Reaktion auf ein Ereignis, einen Satz von Bedingungen oder den Status eines Objekts aktiviert werden. Alarme werden zusammen mit anderen Warnungen im NSX-Dashboard und auf anderen Bildschirmen in der vSphere Web Client-Benutzeroberfläche angezeigt.

Sie können die `GET api/2.0/services/systemalarms`-API verwenden, um Alarme für NSX-Objekte anzuzeigen.

NSX unterstützt zwei Methoden für einen Alarm:

- Der Alarm generiert ein Systemereignis und verfügt über einen zugeordneten Lösungsmechanismus, mit dem versucht wird, das Problem zu lösen, das den Alarm ausgelöst hat. Dieser Ansatz ist auf die Fabric-Bereitstellung für Netzwerk und Sicherheit (z. B. EAM, Nachrichtenbus, Bereitstellungs-Plugin) ausgelegt und wird von Service Composer unterstützt. Für diese Alarme wird der Ereigniscode als Alarmcode verwendet. Weitere Informationen finden Sie im Dokument *NSX-Protokollierung und -Systemereignisse*.

- Edge-Benachrichtigungen/Alarme sind als Alarmpaar zum Auslösen und Beheben strukturiert. Diese Methode wird durch mehrere Edge-Funktionen unterstützt, einschließlich IPSec-VPN, Lastausgleichsdienst, Hochverfügbarkeit, Funktionstest, Edge-Dateisystem und Ressourcenreservierung. Für diese Alarme wird ein eindeutiger Alarmcode verwendet, der nicht mit dem Ereigniscode identisch ist. Weitere Informationen finden Sie im Dokument *NSX-Protokollierung und -Systemereignisse*.

In der Regel wird ein Alarm vom System automatisch gelöscht, wenn der Fehler behoben ist. Einige Alarme werden nicht automatisch bei einer Aktualisierung der Konfiguration gelöscht. Sobald das Problem behoben wurde, müssen Sie die Alarme manuell löschen.

Hier ist ein Beispiel der API, die Sie zum Aufheben der Warnungen verwenden können.

Sie können Alarme für eine bestimmte Quelle abrufen, beispielsweise Cluster, Host, Ressourcenpool, Sicherheitsgruppe oder NSX Edge. Anzeigen von Alarmen für eine Quelle von *sourceId*:

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

Beheben aller Alarme für eine Quelle von *sourceId*:

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

Sie können NSX-Alarme anzeigen, einschließlich Nachrichtenbus-, Bereitstellungs-Plugin-, Service Composer- und Edge-Alarmen:

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

Sie können einen bestimmten NSX-Alarm durch *alarmId* anzeigen:

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

Sie können einen bestimmten NSX-Alarm durch *alarmId* beheben:

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

Weitere Informationen zur API finden Sie im Dokument *Handbuch zu NSX-API*.

Format eines Alarms

Sie können das Format eines Alarms über die API anzeigen.

Das Format eines Alarms enthält die folgenden Informationen.

```
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-Alarme

Alarme machen den vCenter Server-Administrator auf Guest Introspection-Ereignisse aufmerksam, die ein Eingreifen erfordern. Alarme werden automatisch beendet, wenn der Alarmstatus nicht länger vorliegt.

vCenter Server-Alarme können ohne ein benutzerdefiniertes vSphere-Plug-In angezeigt werden. Weitere Informationen zu Ereignissen und Alarmen finden Sie im *vCenter Server-Administratorhandbuch*.

Bei der Registrierung als vCenter Server-Erweiterung definiert NSX Manager die Regeln zum Erstellen und Entfernen von Alarmen basierend auf Ereignissen von den drei Guest Introspection-Komponenten: SVM, Guest Introspection-Modul und Thin Agent. Regeln können angepasst werden. Anweisungen zum Erstellen neuer benutzerdefinierter Regeln für Alarme finden Sie in der vCenter Server-Dokumentation. In einigen Fällen gibt es mehrere mögliche Ursachen für einen Alarm. In den folgenden Tabellen werden die möglichen Ursachen und die zugehörigen Aktionen aufgeführt, die zur Problembeseitigung ergriffen werden können.

Hostalarme

Hostalarme werden durch Ereignisse generiert, die den Integritätsstatus des Guest Introspection-Moduls betreffen.

Tabelle 1-1. Fehler (Kennzeichnung in Rot)

Mögliche Ursache	Aktion
Das Guest Introspection-Modul wurde auf dem Host installiert, meldet aber keinen Status mehr an den NSX Manager.	1 Stellen Sie sicher, dass Guest Introspection ausgeführt wird, indem Sie sich beim Host anmelden und den Befehl `/etc/init.d/vShield-Endpoint-Mux start` eingeben. 2 Stellen Sie sicher, dass das Netzwerk ordnungsgemäß konfiguriert ist, damit Guest Introspection eine Verbindung zu NSX Manager herstellen kann. 3 Starten Sie NSX Manager neu.

SVM-Alarme

SVM-Alarme werden durch Ereignisse generiert, die den Systemzustand der SVM betreffen.

Tabelle 1-2. Rote SVM-Alarme

Problem	Aktion
Die Protokollversion stimmt nicht mit der des Guest Introspection-Moduls überein	Stellen Sie sicher, dass das Guest Introspection-Modul und die SVM über ein kompatibles Protokoll verfügen.
Guest Introspection konnte keine Verbindung zur SVM herstellen	Stellen Sie sicher, dass die SVM eingeschaltet ist und dass das Netzwerk ordnungsgemäß konfiguriert ist.
Die SVM meldet ihren Status auch dann nicht, wenn Gäste verbunden sind.	Interner Fehler. Kontaktieren Sie den für Sie zuständigen Vertreter des technischen Supports von VMware.

Festlegen der Protokollierungsebene von NSX-Komponenten

Sie können die Protokollierungsebene für jede NSX-Komponente festlegen.

Je nach Komponente werden, wie unten dargestellt, verschiedene Ebenen unterstützt.

```
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
```

Aktivieren der Protokollierung für IPSec-VPN

Sie können die Protokollierung des gesamten IPSec-VPN-Datenverkehrs aktivieren.

Standardmäßig ist die Protokollierung aktiviert und dafür die Ebene WARNUNG festgelegt.

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
3. Doppelklicken Sie auf eine NSX Edge-Instanz.
4. Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
5. Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
6. Klicken Sie auf ▶ neben **Protokollierungsrichtlinie (Logging Policy)** und klicken Sie dann auf **Protokollierung aktivieren (Enable logging)**, um den Datenverkehrsfluss zwischen dem lokalen Subnetz und dem Peer-Subnetz zu protokollieren und die Protokollierungsebene auszuwählen.
7. Wählen Sie die Protokollierungsebene aus und klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

SSL VPN-Plus-Protokolle

SSL VPN-Plus-Gateway-Protokolle werden an den auf der NSX Edge-Appliance konfigurierten Syslog-Server gesendet. SSL VPN-Plus Client-Protokolle werden im folgenden Verzeichnis auf dem Computer des Remotebenutzers gespeichert: `%PROGRAMFILES%/VMWARE/SSL VPN Client/`.

Ändern der SSL VPN-Plus Client-Protokolle und der Protokollierungsebene

1. Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **Servereinstellungen (Server Settings)**.

2 Wechseln Sie zum Abschnitt „Protokollierungsrichtlinie“ und erweitern Sie den Abschnitt, um die aktuellen Einstellungen anzuzeigen.

3 Klicken Sie auf **Ändern (Change)**.

4 Aktivieren Sie das Kontrollkästchen **Protokollierung aktivieren (Enable logging)**, um die Protokollierung einzuschalten.

   ODER

   Deaktivieren Sie das Kontrollkästchen **Protokollierung aktivieren (Enable logging)**, um die Protokollierung auszuschalten.

5 Wählen Sie die erforderliche Protokollierungsebene aus.

   Hinweis SSL VPN-Plus Client-Protokolle sind standardmäßig aktiviert, und die Protokollierungsebene ist auf „NOTICE“ (HINWEIS) festgelegt.

6 Klicken Sie auf **OK**.

Überwachungsprotokolle

Die Überwachungsprotokolle dokumentieren alle Aktionen von Benutzern, die sich bei NSX Manager angemeldet haben.

Anzeigen des Überwachungsprotokolls

Auf der Registerkarte **Überwachungsprotokolle** wird eine Ansicht der von allen NSX Manager-Benutzern durchgeführten Aktionen bereitgestellt. NSX Manager behält bis zu 100.000 Überwachungsprotokolle bei.

Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an.

2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.

3 Klicken Sie in der Spalte **Name** auf einen NSX Server und anschließend auf die Registerkarte **Überwachen**.

4 Klicken Sie auf die Registerkarte **Überwachungsprotokolle**.

5 Sobald Details des Überwachungsprotokolls zur Verfügung stehen, ist der Text in der Spalte **Vorgang** anklickbar. Klicken Sie auf den Text in der Spalte **Vorgang**, um die Details des Überwachungsprotokolls anzuzeigen.

6 Wählen Sie in **Änderungsdetails – Überwachungsprotokoll** den Eintrag **Geänderte Zeilen** aus, wenn nur Eigenschaften angezeigt werden sollen, deren Werte sich für diesen Überwachungsprotokollvorgang geändert haben.

Konfigurieren eines Syslog-Servers

Sie können einen Syslog-Server als Repository für Protokolle von NSX-Komponenten und Hosts konfigurieren.

Konfigurieren eines Syslog-Servers für NSX Manager

Wenn Sie einen Syslog-Server angeben, sendet NSX Manager alle Überwachungsprotokolle und Systemereignisse an den Syslog-Server.

Syslog-Daten sind hilfreich bei der Problembehebung und bei der Überprüfung von Daten, die während der Installation und Konfiguration protokolliert worden sind.

NSX Edge unterstützt zwei Syslog-Server. NSX Manager und NSX Controller unterstützten einen Syslog-Server.

Vorgehensweise

1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

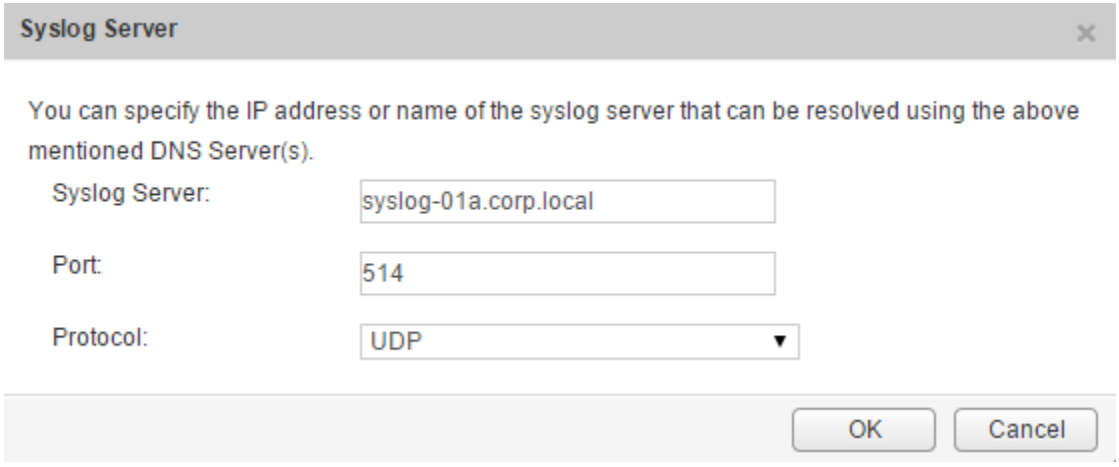
   Navigieren Sie in einem Web-Browser zur NSX Manager Appliance-GUI unter https://<nsx-manager-ip> oder https://<nsx-manager-hostname> und melden Sie sich als Administrator mit dem Kennwort an, das Sie bei der Installation von NSX Manager konfiguriert haben.

2 Klicken Sie auf der Startseite auf **Appliance-Einstellungen verwalten (Manage Appliance Settings) > Allgemein (General)**.

3 Klicken Sie neben **Syslog-Server (Syslog Server)** auf **Bearbeiten (Edit)**.

4 Geben Sie die IP-Adresse oder den Hostnamen, Port und Protokoll des Syslog-Servers ein.

   Beispiel:



5 Klicken Sie auf **OK**.

Die Remoteprotokollierung von NSX Manager ist aktiviert und die Protokolle werden auf Ihrem eigenständigen Syslog-Server gespeichert.

Konfigurieren von Syslog-Servern für NSX Edge

Sie können einen oder zwei Remote-Syslog-Server konfigurieren. NSX Edge-Ereignisse und -Protokolle im Zusammenhang mit Firewallereignissen, die von NSX Edge-Appliances ausgehen, werden an die Syslog-Server gesendet.

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
3. Doppelklicken Sie auf eine NSX Edge-Instanz.
4. Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf die Registerkarte **Einstellungen**.
5. Klicken Sie im Fenster **Details** neben den Syslog-Servern auf **Ändern**.
6. Geben Sie die IP-Adressen beider Remote-Syslog-Server ein und wählen Sie das Protokoll aus.
7. Klicken Sie auf **OK**, um die Konfiguration zu speichern.

Konfigurieren eines Syslog-Servers für NSX Controller

Wenn Sie einen Syslog-Server für NSX Controller konfigurieren, sendet NSX Manager alle Überwachungsprotokolle und Systemereignisse an den Syslog-Server. Syslog-Daten sind hilfreich bei der Problembehebung und bei der Überprüfung von Daten, die während der Installation und Konfiguration protokolliert worden sind. Die Konfiguration des Syslog-Servers auf den NSX Controllern kann nur über die NSX-API durchgeführt werden. VMware empfiehlt die Verwendung des UDP-Protokolls für Syslog.

Vorgehensweise

1. Um Syslog auf dem NSX Controller zu aktivieren, verwenden Sie die im Folgenden dargestellte NSX-API. Damit wird der Controller-Syslog-Exporter hinzugefügt und ein Syslog-Exporter auf dem angegebenen Controller-Knoten konfiguriert.

```
Request
POST https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Request Body:
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

2 Sie können den Controller-Syslog-Exporter abfragen und Details zum konfigurierten Syslog-Exporter auf dem angegebenen Controller-Knoten mithilfe der nachfolgend dargestellten NSX-API abrufen.

```
Request
GET https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Response Body:
<?xml version="1.0" encoding="UTF-8"?>
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

3 Wenn er nicht erforderlich ist, können Sie den Syslog-Exporter auf dem angegebenen Controller-Knoten mithilfe der im Folgenden dargestellten NSX-API löschen.

```
Request
DELETE https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
```

Weiter

Weitere Informationen zur API erhalten Sie unter *Handbuch zu NSX-API*.

Erfassen von Tech-Support-Protokollen

In bestimmten Situationen kann es notwendig sein, Tech-Support-Protokolle von den NSX-Komponenten und den Hosts zu erfassen, um ein Problem an VMware zu melden.

Zur Erfassung der Host-Tech-Support-Protokolle führen Sie den Befehl `export host-tech-support` aus (siehe „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*).

Herunterladen der Protokolle des technischen Supports für NSX

Sie können die Systemprotokolle von NSX Manager und die Protokolle des Web-Managers auf Ihren Desktop herunterladen.

Vorgehensweise

1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

2 Klicken Sie unter Appliance-Verwaltung auf **Appliance-Einstellungen verwalten**.

3 Klicken Sie auf  und anschließend auf **Tech-Support-Protokoll herunterladen**.

4 Klicken Sie auf **Herunterladen**.

5 Wenn das Protokoll fertig gestellt wurde, klicken Sie auf **Speichern**, um das Protokoll auf Ihren Desktop herunterzuladen.

   Das Protokoll ist komprimiert und hat die Dateierweiterung `.gz`.

Weiter

Sie können das Protokoll mit einem Dienstprogramm für die Dekomprimierung öffnen, indem Sie das Speicherverzeichnis für die Datei mit der Option **Alle Dateien** durchsuchen.

Herunterladen von Tech-Support-Protokollen für NSX Edge

Sie können Protokolle für den technischen Support für jede NSX Edge-Instanz herunterladen. Wenn High Availability für die NSX Edge-Instanz aktiviert ist, werden die Support-Protokolle von beiden virtuellen NSX Edge-Maschinen heruntergeladen.

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
3. Wählen Sie eine NSX Edge-Instanz aus.
4. Klicken Sie auf **Aktionen** ( ), und wählen Sie **Herunterladen von Tech-Support-Protokollen**.
5. Sobald die Protokolle für den technischen Support generiert wurden, klicken Sie auf **Herunterladen**.

Herunterladen von technischen Support-Protokollen für NSX Controller

Sie können Protokolle für den technischen Support für jede NSX Controller-Instanz herunterladen. Diese produktspezifischen Protokolle enthalten Diagnoseinformationen für die Analyse.

So erfassen Sie NSX Controller-Protokolle:

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
3. Wählen Sie unter **Management** den Controller aus, von dem Sie Protokolle herunterladen möchten.
4. Klicken Sie auf **Tech-Support-Protokolle herunterladen**.
5. Klicken Sie auf **Herunterladen**.

   NSX Manager startet den Download des NSX Controller-Protokolls und erhält die Sperre.

   Hinweis Laden Sie die NSX Controller einzeln herunter. Wenn der erste Download abgeschlossen ist, starten Sie mit den nächsten. Wenn Sie Protokolle von mehreren Controllern gleichzeitig herunterladen, kann ein Fehler auftreten.

6. Wenn das Protokoll fertig gestellt wurde, klicken Sie auf **Speichern**, um das Protokoll auf Ihren Desktop herunterzuladen.

   Das Protokoll ist komprimiert und hat die Dateierweiterung `.gz`.

Sie können die heruntergeladenen Protokolle nun analysieren.

Weiter

Wenn Sie Diagnosedaten für den technischen Support von VMware hochladen möchten, schlagen Sie im Knowledgebase-Artikel 2070100 nach.

NSX - und Host-Protokolle 2

Sie können mithilfe der Protokolle in den verschiedenen NSX-Komponenten und auf den Hosts Probleme ermitteln und beheben.

Dieses Kapitel behandelt die folgenden Themen:

Grundlegendes zu NSX-Protokollen

Sie können den Syslog-Server konfigurieren und Protokolle des technischen Supports für die einzelnen NSX-Komponenten anzeigen. Protokolle der Verwaltungsebene sind über NSX Manager verfügbar, Protokolle der Datenebene hingegen über vCenter Server. Daher ist es ratsam, denselben Syslog-Server für die NSX-Komponente und vCenter Server anzugeben, um beim Betrachten von Protokollen auf dem Syslog-Server ein vollständiges Bild zu erhalten.

Informationen zum Konfigurieren eines Syslog-Servers für durch einen vCenter Server verwaltete Hosts finden Sie in der entsprechenden Version der vSphere-Dokumentation unter https://docs.vmware.com.

Hinweis Syslog- oder Jump-Server, die zur Erfassung von Protokollen und zum Zugriff auf eine NSX-DLR-Kontroll-VM (Distributed Logical Router) verwendet werden, können sich nicht auf dem logischen Switch befinden, der direkt den logischen Schnittstellen (LIFs) dieses DLR angefügt wurde.

Tabelle 2-1. NSX-Protokolle

Komponente	Beschreibung
ESXi-Protokolle	Diese Protokolle werden als Teil des VM-Support-Pakets erfasst, das von vCenter Server generiert wird. Weitere Informationen zu ESXi-Protokolldateien finden Sie in der vSphere-Dokumentation.
NSX Edge-Protokolle	Verwenden Sie den Befehl `show log [follow | reverse]` in der Befehlszeilenschnittstelle von NSX Edge. Laden Sie das Protokollpaket für den technischen Support über die Benutzeroberfläche von NSX Edge herunter.

Tabelle 2-1. NSX-Protokolle (Fortsetzung)

Komponente	Beschreibung
NSX Manager-Protokolle	Verwenden Sie den Befehl `show log` in der Befehlszeilenschnittstelle von NSX Manager. Laden Sie das Protokollpaket für den technischen Support über die Benutzeroberfläche der virtuellen NSX Manager-Appliance herunter.
Routing-Protokolle	Siehe Handbuch *NSX-Protokollierung und -Systemereignisse*.
Firewallprotokolle	Siehe Firewallprotokolle.
Guest Introspection-Protokolle	Siehe Guest Introspection-Protokolle.

NSX Manager

Informationen zum Angeben eines Syslog-Servers erhalten Sie unter Konfigurieren eines Syslog-Servers für NSX Manager.

Informationen zum Herunterladen der Protokolle des technischen Supports erhalten Sie unter Herunterladen der Protokolle des technischen Supports für NSX.

NSX Edge

Informationen zum Angeben eines Syslog-Servers erhalten Sie unter Konfigurieren von Syslog-Servern für NSX Edge.

Informationen zum Herunterladen der Protokolle des technischen Supports erhalten Sie unter Herunterladen von Tech-Support-Protokollen für NSX Edge.

NSX Controller

Informationen zum Angeben eines Syslog-Servers erhalten Sie unter Konfigurieren eines Syslog-Servers für NSX Controller.

Informationen zum Herunterladen der Protokolle des technischen Supports erhalten Sie unter Herunterladen von technischen Support-Protokollen für NSX Controller.

Firewall

Weitere Informationen finden Sie unter Firewallprotokolle.

Firewallprotokolle

Die Firewall generiert und speichert Protokolldateien, wie z. B. das Audit-, Regelmeldungs- und Systemereignisprotokoll. Sie müssen einen Syslog-Server für jedes Cluster konfigurieren, für das eine Firewall aktiviert ist. Der Syslog-Server wird im Attribut `Syslog.global.logHost` angegeben.

Die Firewall generiert Protokolle, wie in der folgenden Tabelle beschrieben.

Tabelle 2-2. Firewallprotokolle

Protokolltyp	Beschreibung	Speicherort
Regelmeldungsprotokolle	Schließen alle Zugriffsentscheidungen wie etwa zugelassener oder verweigerter Datenverkehr für jede Regel ein, falls die Protokollierung aktiviert wurde. Enthält die DFW-Paketprotokolle für die Regeln, für die die Protokollierung aktiviert wurde.	/var/log/dfwpktlogs.log
Überwachungsprotokolle	Schließen Verwaltungsprotokolle und Konfigurationsänderungen für die verteilte Firewall ein.	/home/secureall/secureall/logs/vsm.log
Systemereignisprotokolle	Schließen die angewendete Konfiguration der verteilten Firewall, erstellte, gelöschte oder fehlgeschlagene Filter, zu Sicherheitsgruppen hinzugefügte virtuelle Maschinen usw. ein.	/home/secureall/secureall/logs/vsm.log
Datenebene-/VMKernel-Protokolle	Erfassen die Aktivitäten in Verbindung mit einem Firewall-Kernel-Modul (VSIP). Sie enthalten Protokolleinträge für Mails, die vom System generiert werden.	/var/log/vmkernel.log
Nachrichtenbus-Client-/VSFWD-Protokolle	Erfassen die Aktivitäten eines Firewall-Agenten.	/var/log/vsfwd.log

Hinweis Um auf die die Datei *vsm.log* zuzugreifen, führen Sie den Befehl `show log manager` in der NSX Manager-Befehlszeilenschnittstelle aus und anschließend den Befehl *grep* für das Schlüsselwort *vsm.log*. Diese Datei ist nur für den Benutzer bzw. die Benutzergruppe mit *root*-Rechten zugänglich.

Regelmeldungsprotokolle

Regelmeldungsprotokolle schließen alle Zugriffsentscheidungen wie etwa zugelassener oder verweigerter Datenverkehr für jede Regel ein, falls die Protokollierung aktiviert wurde. Diese Protokolle werden auf jedem Host unter `/var/log/dfwpktlogs.log` gespeichert.

Hier sind Beispiele für Firewallprotokollmeldungen:

```
 # 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
```

Weitere Beispiele:

```
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
```

Im nachfolgenden Beispiel:

- 1002 ist die ID der Verteilten Firewall.
- „domain-c7“ ist die Cluster-ID im von vCenter verwalteten Objektbrowser (MOB).
- 192.168.110.10/138 ist die Quell-IP-Adresse.
- 192.168.110.255/138 ist die Ziel-IP-Adresse.
- *RULE_TAG* ist ein Beispiel für den Text, den Sie im Textfeld **Tag** eingeben, wenn Sie die Firewallregel hinzufügen oder bearbeiten.

Im folgenden Beispiel wird das Ergebnis eines Ping-Befehls von 192.168.110.10 auf 172.16.10.12 angezeigt.

```
 # 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
```

Die folgenden Tabellen erläutern die Textfelder der Firewallprotokollmeldung.

Tabelle 2-3. Komponenten eines Eintrags in der Protokolldatei

Komponente	Wert im Beispiel
Zeitstempel	2017-04-11T21:09:59
Firewallspezifischer Teil	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

Tabelle 2-4. Firewallspezifischer Teil des Eintrags der Protokolldatei

Element	Mögliche Werte
Filter-Hash	Eine Zahl, mit der der Filtername und andere Informationen abgerufen werden können.
AF-Wert	INET, INET6

Tabelle 2-4. Firewallspezifischer Teil des Eintrags der Protokolldatei (Fortsetzung)

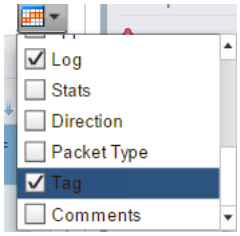
Element	Mögliche Werte
Grund	■ match: Paket stimmt mit einer Regel überein. ■ bad-offset: interner Datenpfadfehler beim Erhalt des Pakets. ■ fragment: die nicht-ersten Fragmente, nachdem sie zum ersten Fragment zusammengesetzt wurden. ■ short: Paket zu kurz (z. B. unvollständig, IP-Header oder TCP/UDP-Header fehlt). ■ normalize: falsch formatierte Pakete ohne korrekten Header oder Payload. ■ memory: Datenpfad ohne Speicher. ■ bad-timestamp: ungültiger TCP-Zeitstempel. ■ proto-cksum: falsche Protokollprüfsumme. ■ state-mismatch: TCP-Pakete, die die TCP-Status-Maschinenprüfung nicht bestehen. ■ state-insert: doppelte Verbindung gefunden. ■ state-limit: maximale Anzahl an Status erreicht, die ein Datenpfad nachverfolgen kann. ■ SpoofGuard: Paket von SpoofGuard verworfen. ■ TERM: Eine Verbindung wird beendet.
Aktion	■ PASS: Paket wird angenommen. ■ DROP: Paket wird verworfen. ■ NAT: SNAT-Regel. ■ NONAT: Stimmt mit SNAT-Regel überein, kann die Adresse aber nicht übersetzen. ■ RDR: DNAT-Regel. ■ NORDR: Stimmt mit DNAT-Regel überein, kann die Adresse aber nicht übersetzen. ■ PUNT: Sendet das Paket zu einer Dienst-VM, die auf demselben Hypervisor der aktuellen virtuellen Maschine ausgeführt wird. ■ REDIRECT: Sendet das Paket zu einem Netzwerkdienst, der auf einem anderen Hypervisor als der der aktuellen virtuellen Maschine ausgeführt wird. ■ COPY: Nimmt das Paket an und sendet eine Kopie davon zu einer Dienst-VM, die auf demselben Hypervisor der aktuellen virtuellen Maschine ausgeführt wird. ■ REJECT: Weist das Paket zurück.
Regelsatz und Regel-ID	*Regelsatz*/*Regel-ID*
Richtung	IN, OUT
Paketlänge	*length*
Protokoll	TCP, UDP, ICMP oder PROTO (Protokollnummer) Bei TCP-Verbindungen wird der tatsächliche Grund für das Beenden einer Verbindung nach dem Schlüsselwort TCP angezeigt. Wenn TERM der Grund für eine TCP-Sitzung ist, wird in der Zeile PROTO eine zusätzliche Erläuterung angezeigt. Zu möglichen Gründen für das Beenden einer TCP-Verbindung gehören: RST (TCP-RST-Paket), FIN (TCP-FIN-Paket) und TIMEOUT (zu lange inaktiv). Im o. g. Beispiel ist es *RST*. Das bedeutet, dass in der Verbindung ein *RST* -Paket vorhanden ist, das zurückgesetzt werden muss. Bei anderen Verbindungen als TCP-Verbindungen (UDP, ICMP oder andere Protokolle) gibt es als Grund für das Beenden einer Verbindung nur TIMEOUT.
Quell-IP-Adresse und -Port	*IP address*/*port*
Ziel-IP-Adresse und -Port	*IP address*/*port*
TCP-Flags	S (SYN), SA (SYN-ACK), A (ACK), P (PUSH), U (URGENT), F (FIN), R (RESET)

Tabelle 2-4. Firewallspezifischer Teil des Eintrags der Protokolldatei (Fortsetzung)

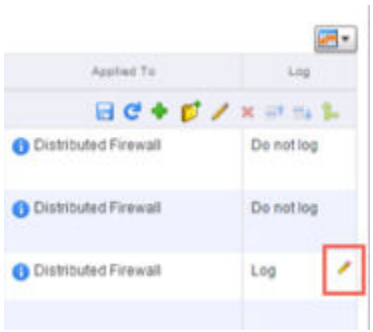
Element	Mögliche Werte
Anzahl an Paketen	Anzahl an Paketen. 22/14 – eingehende Pakete/ausgehende Pakete
Anzahl an Bytes	Anzahl an Bytes. 7684/1070 – eingehende Bytes/ausgehende Bytes

Um eine Regemeldung zu aktivieren, melden Sie sich bei vSphere Web Client an.

1 Aktivieren Sie die Spalte **Protokoll** auf der Seite **Networking & Security > Firewall**.



2 Sie aktivieren die Protokollierung für eine Regel, indem Sie den Mauszeiger über einer Zelle in der Protokolltabelle halten und auf das Bleistiftsymbol klicken.



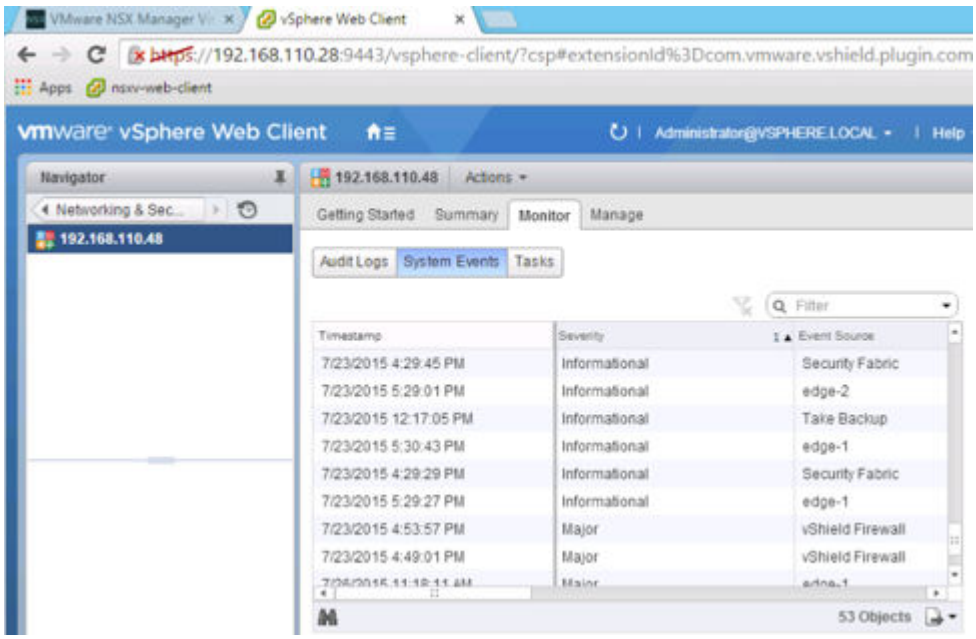
Hinweis Um benutzerdefinierten Text in der Firewallprotokollmeldung anzuzeigen, aktivieren Sie die Spalte **Tag** und klicken Sie auf das Stiftsymbol, um den gewünschten Text hinzuzufügen.

Audit- und Systemereignisprotokolle

Überwachungsprotokolle schließen Verwaltungsprotokolle und Konfigurationsänderungen für die verteilte Firewall ein. Diese werden unter `/home/secureall/secureall/logs/vsm.log` gespeichert.

Systemereignisprotokolle schließen die angewendete Konfiguration der verteilten Firewall, erstellte, gelöschte oder fehlgeschlagene Filter, zu Sicherheitsgruppen hinzugefügte virtuelle Maschinen usw. ein. Diese Protokolle werden unter `/home/secureall/secureall/logs/vsm.log` gespeichert.

Navigieren Sie zum Anzeigen von Audit- und Systemereignisprotokollen in der Benutzeroberfläche zu **Networking & Security > Installation > Verwaltung** und doppelklicken Sie auf die IP-Adresse von NSX Manager. Klicken Sie dann auf die Registerkarte **Überwachen**.



Weitere Informationen finden Sie unter *NSX-Protokollierung und -Systemereignisse*.

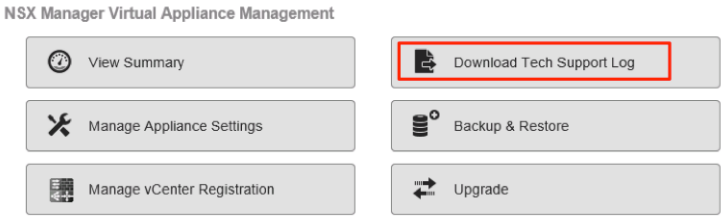
NSX-Protokolle für das Routing

Es wird empfohlen, alle NSX-Komponenten so zu konfigurieren, dass deren Protokolle an einen zentralen Collector gesendet werden, damit sie an einer Stelle ausgewertet werden können.

Bei Bedarf können Sie die Protokollierungsebene der NSX-Komponenten ändern. Weitere Informationen finden Sie im Thema „Protokollierungsebene von NSX-Komponenten festlegen“ unter *NSX-Protokollierung und -Systemereignisse*.

NSX Manager-Protokolle

- `show log` in der NSX Manager-Befehlszeilenschnittstelle (CLI)
- Tech-Support-Protokollpaket, dass über die NSX Manager-Benutzeroberfläche zusammengestellt werden kann



Das NSX Manager-Protokoll enthält Informationen zur Verwaltungskomponente, die die CRUD-Vorgänge betreffen (Create/Read/Update/Delete, Erstellen/Lesen/Aktualisieren/Löschen).

Controller-Protokolle

Controller enthalten mehrere Module, von denen viele eigene Protokolldateien generieren. Auf Controller-Protokolle kann mit dem Befehl `show log <log file> [ filtered-by <string> ]` zugegriffen werden. Die folgenden Protokolldateien betreffen das Routing:

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log`: Dieses Protokoll verwaltet die Konfiguration und den internen API-Server.
- `cloudnet/cloudnet.nsx-controller.log`: Dies ist das Protokoll für den zentralen Controller-Prozess.
- `cloudnet/cloudnet_cpp.log.nsx-controller.log`: Dieses Protokoll verwaltet das Clustering und Bootstrap.
- `cloudnet/cloudnet_cpp.log.ERROR`: Diese Datei ist vorhanden, wenn ein Fehler auftritt.

Controller-Protokolle sind umfangreich und in den meisten Fällen nur erforderlich, wenn das VMware-Technikteam zur Fehlerbehebung in schwierigeren Fällen hinzugezogen wird.

Zusätzlich zum Aufruf über die `show log`-CLI können einzelne Protokolldateien mithilfe des Befehls `watch log <logfile> [ filtered-by <string> ]` in Echtzeit, d. h. zum Zeitpunkt der Aktualisierung, eingesehen werden.

Die Protokolle sind im Controller-Support-Paket enthalten, das durch Auswahl des Controller-Knotens in der NSX-Benutzeroberfläche und durch Klicken auf das Symbol **Tech-Support-Protokolle herunterladen (Download tech support logs)** generiert und heruntergeladen werden kann.

ESXi Host-Protokolle

Durch auf ESXi-Hosts ausgeführten NSX-Komponenten werden folgende Protokolldateien erstellt:

- VMkernel-Protokolle: `/var/log/vmkernel.log`
- Protokolle des Steuerungskomponenten-Agenten: `/var/log/netcpa.log`
- Protokolle des Nachrichtenbus-Client: `/var/log/vsfwd.log`

Die Protokolle können auch als Bestandteil des VM-Support-Pakets zusammengestellt werden, das von vCenter Server generiert wird. Diese Datei ist nur für den Benutzer bzw. die Benutzergruppen mit *root*-Rechten zugänglich.

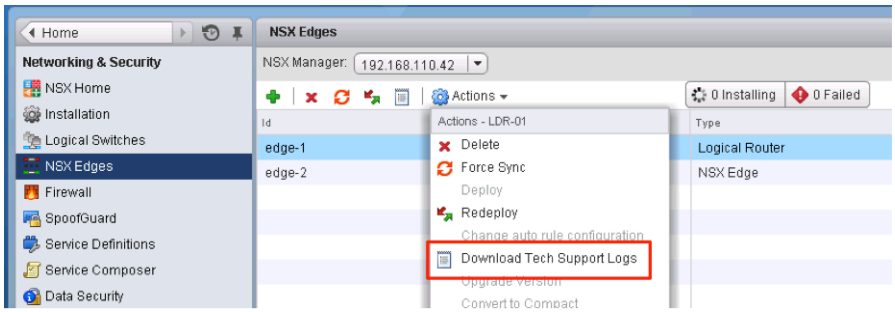
ESG-/DLR-Kontroll-VM-Protokolle

Für den Zugriff auf die Protokolldateien des ESG und der DLR-Kontroll-VM haben Sie zwei Möglichkeiten: Sie können diese mithilfe einer CLI darstellen oder das Tech-Support-Paket mithilfe der Befehlszeilenschnittstelle (CLI) oder der Benutzeroberfläche herunterladen.

Zur Darstellung der Protokolle verwenden Sie den CLI-Befehl `show log [ follow | reverse ]`.

So laden Sie das Tech-Support-Paket herunter:

- An der CLI wechseln Sie in den `enable`-Modus und führen Sie dann den Befehl `export tech-support <[ scp | ftp ]> <URI>` aus.
- Im vSphere Web Client wählen Sie die Option **Tech-Support-Protokolle herunterladen (Download Tech Support Logs)** im Menü **Aktionen (Actions)** aus.



Andere nützliche Dateien und deren Speicherorte

Auch wenn es sich dabei im engeren Sinn nicht um Protokolle handelt, gibt es eine Vielzahl von Dateien, die für das Verständnis und die Fehlerbehebung des NSX-Routings eine Unterstützung bieten.

- Die Datei `/etc/vmware/netcpa/config-by-vsm.xml` zur Konfiguration des Steuerungskomponenten-Agenten enthält Informationen über die folgenden Komponenten:
  - Controller, IP-Adressen, TCP-Ports, Zertifikat-Fingerabdrücke, Aktivierung/Deaktivierung von SSL
  - dvUplinks am DVS, mit VXLAN aktiviert (Gruppierungsrichtlinie, Namen, UUID)
  - DLR-Instanzen, die der Host erkennt (DLR-ID und -Name)
- Die Datei `/etc/vmware/netcpa/netcpa.xml` zur Konfiguration des Steuerungskomponenten-Agenten enthält verschiedene Konfigurationsoptionen für netcpa, inklusive der Protokollierungsebene (diese ist standardmäßig **info**).
- Zertifikatdateien der Steuerungskomponente: `/etc/vmware/ssl/rui-for-netcpa.*`
  - Zwei Dateien: Hostzertifikat und privater Schlüssel des Host
  - Verwendet für die Authentifizierung von Hostverbindungen mit Controllern

Alle diese Dateien werden vom Agenten der Steuerungskomponente mithilfe von Informationen des NSX Manager erstellt, die über die von vsfwd bereitgestellte Nachrichtenbusverbindung übertragen werden.

Guest Introspection-Protokolle

Es gibt verschiedene Protokolle, die Sie erfassen können, um sie bei der Fehlerbehebung für Guest Introspection zu verwenden.

Protokolle des ESX-GI-Moduls (MUX)

Wenn virtuelle Maschinen auf einem ESXi-Host nicht mit Guest Introspection funktionieren oder wenn auf einem Host hinsichtlich der Kommunikation mit der SVA Alarme ausgelöst werden, liegt möglicherweise ein Problem beim ESX-GI-Modul auf dem ESXi-Host vor.

Protokollpfad und Beispielmeldung

MUX-Protokollpfad
/var/log/syslog
var/run/syslog.log

Meldungen des ESX-GI-Moduls (MUX) weisen das Format <Zeitstempel>EPSecMUX<[ThreadID]>: <Meldung> auf.

Beispiel:

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

Im obigen Beispiel:

- [ERROR] ist die Art der Benachrichtigung. Andere mögliche Typen sind [DEBUG] oder [INFO].
- (EPSEC) gibt an, dass die Nachrichten zur Endpoint-Sicherheit gehören.

Protokolldateien aktivieren und anzeigen

Um die auf dem Host installierte Version des ESX-GI-Modul-VIBs anzuzeigen, führen Sie den Befehl `#esxcli software vib list | grep epsec–mux` aus.

Um die vollständige Protokollierung zu aktivieren, führen Sie diese Schritte in der Eingabeaufforderung des ESXi-Hosts aus.

1 Führen Sie den Befehl „ps -c |grep Mux“ aus, um die ESX-GI-Modulprozesse anzuzeigen, die gerade ausgeführt werden.

   Beispiel:

   ```
   ~ # 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 Wenn der Dienst nicht ausgeführt wird, können Sie ihn mit diesen Befehlen erneut starten:`/etc/init.d/vShield–Endpoint–Mux start` oder `/etc//init.d/vShield–Endpoint–Mux restart`.

3 Um die ESX-GI-Modulprozesse, die gerade ausgeführt werden, anzuhalten, darunter auch den watchdog.sh-Prozess, führen Sie den Befehl `~ # kill –9 192223 192233 192236` aus.

   Beachten Sie, dass zwei ESX-GI-Modulprozesse erzeugt werden.

4 Starten Sie ein ESX-GI-Modul mit einer neuen Option –d. Beachten Sie, dass die Option „-d“ für die EPSec-MUX-Builds 5.1.0-01255202 und 5.1.0-01814505 `~ # /usr/lib/vmware/vShield–End–point–Mux –d 900 –c 910` nicht vorhanden ist.

5 Zeigen Sie die Protokollnachrichten des ESX GI-Moduls in der Datei `/var/log/syslog.log` auf dem ESXi-Host an. Überprüfen Sie, ob die Einträge zu globalen Lösungen, zur Lösungs-ID und zur Portnummer korrekt sind.

Beispiel: Muxconfig.xml-Beispieldatei

```
<?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–al–
pha–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-Protokolle

Der Thin Agent ist auf dem VM-Gastbetriebssystem installiert und erkennt Anmeldedetails von Benutzern.

Protokollpfad und Beispielmeldung

Der Thin Agent besteht aus GI-Treibern – vsepflt.sys, vnetflt.sys und vnetwfp.sys (Windows 10 und höher).

Die Thin Agent-Protokolle befinden sich als Teil des vCenter-Protokollpakets auf dem ESXi-Host. Der Protokollpfad lautet `/vmfs/volumes/<datastore>/<vmname>/vmware.log` Zum Beispiel: `/vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log`

Thin Agent-Meldungen weisen folgendes Format auf: <Zeitstempel> <VM name=""><Process name=""><[PID]>: <Meldung>.</[PID]>

Im Beispielprotokoll unter `Guest: vnet or Guest:vsep` werden Protokollmeldungen für die jeweiligen GI-Treiber angegeben, gefolgt von Debugging-Meldungen.

Beispiel:

```
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
```

Beispiel: Aktivieren der vShield Guest Introspection Thin Agent-Treiber-Protokollierung

Weil die Debugging-Einstellung die Datei vmware.log so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

Für dieses Verfahren müssen Sie die Windows-Registry ändern. Bevor Sie die Registry ändern, erstellen Sie eine Sicherungskopie. Weitere Informationen zum Sichern und Wiederherstellen der Registry finden Sie im Microsoft Knowledgebase-Artikel 136393.

So aktivieren Sie die Debugging-Protokollierung für den Thin Agent-Treiber:

1 Klicken Sie auf **Start > Ausführen (Start > Run)**. Geben Sie „regedit“ ein und klicken Sie auf **OK**. Die Registry-Editor-Fenster wird geöffnet. Weitere Informationen finden Sie im Microsoft Knowledgebase-Artikel 256986.

2 Erstellen Sie mit dem Registry-Editor diesen Schlüssel: `HKEY_LOCAL_Machine\SYSTEM\CurrentControlSet\services\vsepflt\parameters`.

3 Erstellen Sie unter dem neu erstellten Parameterschlüssel diese DWORDs. Stellen Sie sicher, dass hexadezimal ausgewählt ist, wenn Sie diese Werten eingeben:

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

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

Andere Werte für den `log level`-Parameterschlüssel:

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

4 Öffnen Sie eine Eingabeaufforderung als Administrator. Führen Sie diese Befehle aus, um das Laden Minitreiber des vShield Endpoint-Dateisystems zu beenden und ihn dann erneut zu laden:

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

Sie finden die Protokolleinträge in der vmware.log-Datei, die sich auf der virtuellen Maschine befindet.

Aktivieren der vShield GI Netzwerktreiber-Protokollierung

Weil die Debugging-Einstellung die Datei vmware.log so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

Für dieses Verfahren müssen Sie die Windows-Registry ändern. Bevor Sie die Registry ändern, erstellen Sie eine Sicherungskopie. Weitere Informationen zum Sichern und Wiederherstellen der Registry finden Sie im Microsoft Knowledgebase-Artikel 136393.

1 Klicken Sie auf **Start > Ausführen (Start > Run)**. Geben Sie „regedit“ ein und klicken Sie auf **OK**. Die Registry-Editor-Fenster wird geöffnet. Weitere Informationen finden Sie im Microsoft Knowledgebase-Artikel 256986.

2 So bearbeiten Sie die Registry:

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

3 Starten Sie die virtuelle Maschine neu.

Speicherort der Protokolldateien vsepflt.sys und vnetflt.sys

Mit den log_dest-Registry-Einstellungen DWORD: 0x00000001 meldet sich der Endpoint Thin Agent-Treiber beim Debugger an. Führen Sie den Debugger (DbgView von SysInternals oder windbg) aus, um die Debugging-Ausgabe zu erfassen.

Alternativ können Sie die log_dest-Registry-Einstellung auf DWORD:0x000000002 festlegen. Dann werden die Treiberprotokolle in der Datei vmware.log ausgegeben, die sich im entsprechenden VM-Ordner auf dem ESXi-Host befindet.

Aktivieren der UMC-Protokollierung

Die Benutzermodus-Komponente (UMC) von Guest Introspection wird im VMware Tools-Dienst in der geschützten virtuelle Maschine ausgeführt.

1 Erstellen Sie unter Windows XP und Windows Server 2003 eine `Tools–Config`-Datei, wenn unter folgendem Pfad keine vorhanden ist: `C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware Tools\tools.conf`.

2 Erstellen Sie unter Windows Vista, Windows 7 und Windows Server 2008 eine `Tools–Config`-Datei, wenn unter folgendem Pfad keine vorhanden ist: `C:\ProgramData\VMWare\VMware Tools\tools.conf`

3 Fügen Sie diese Zeilen in der Datei `tools.conf` , um die UMC-Komponentenprotokollierung zu aktivieren.

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

Mit der Einstellung `vsep.handler = vmx` werden die Protokolle der UMC-Komponente in der Datei `vmware.log` ausgegeben, die sich im entsprechenden VM-Ordner auf dem ESXi-Host befindet.

Mit den folgenden Einstellungsprotokollen werden die Protokolle der UMC-Komponente in der angegebenen Protokolldatei ausgegeben.

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

GI-EPSecLib- und SVM-Protokolle

Die EPSecLib empfängt Ereignisse vom ESX-GI-Modul (MUX) des ESXi-Hosts.

Protokollpfad und Beispielmeldung

EPSecLib-Protokollpfad
/var/log/syslog
var/run/syslog

EPSecLib-Nachrichten weisen folgendes Format auf: <Zeitstempel> <VM Name><Process Name><[PID]>: <Meldung>

Im folgenden Beispiel ist [ERROR] der Nachrichtentyp und (EPSEC) steht für die Nachrichten, die sich auf Guest Introspection beziehen.

Beispiel:

```
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.
```

Erfassen von Protokollen

So aktivieren Sie die Debugging-Protokollierung für die EPSec-Bibliothek, die eine Komponente der GI-SVM ist:

1 Melden Sie sich bei der GI-SVM mit dem Konsolenkennwort von NSX Manager an.

2 Erstellen Sie die Datei `/etc/epseclib.conf` und fügen Sie Folgendes hinzu:

```
ENABLE_DEBUG=TRUE

ENABLE_SUPPORT=TRUE
```

3 Ändern Sie die Berechtigungen, indem Sie den Befehl `chmod 644 /etc/epseclib.conf` ausführen.

4 Starten Sie den GI-SVM-Prozess neu, indem Sie den Befehl `/usr/local/sbin/rcusvm restart` ausführen.

Dies aktiviert die Debugging-Protokollierung für EPSecLib auf der GI-SVM. Die Debugging-Protokolle finden Sie im Verzeichnis /var/log/messages (gilt für NSX for vSphere 6.2.x und 6.3.x). Weil die Debugging-Einstellung die Datei vmware.log so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

GI-SVM-Protokolle

Bevor Sie Protokolle erfassen, legen Sie die Host-ID oder Host-MOID fest:

- Führen Sie die Befehle `show cluster all` und `show cluster <cluster ID>` in NSX Manager aus.

  Beispiel:

```
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 Um den aktuellen Protokollierungsstatus zu ermitteln, führen Sie diesen Befehl aus:

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

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

2 Um den aktuellen Protokollierungsstatus zu ändern, führen Sie diesen Befehl aus:

  `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 Um Protokolle zu generieren, führen Sie diesen Befehl aus:

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

  Wählen Sie `Send` und `Download`.

Beachten Sie, dass dieser Befehl GI-SVM-Protokolle generiert und die Datei als `techsupport-logs.log.gz`-Datei speichert. Weil die Debugging-Einstellung die Datei vmware.log so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

Systemereignisse

3

Alle Komponenten in NSX melden Systemereignisse. Diese Ereignisse sollen Sie bei der Überwachung der Integrität und der Sicherheit der Umgebung sowie bei der Behebung von Problemen unterstützen.

Jede Ereignismeldung enthält folgende Informationen:

- Eindeutiger Ereigniscode
- Schweregrad
- Beschreibung des Ereignisses und, wenn erforderlich, empfohlene Aktionen.

Erfassen von Tech-Support-Protokollen und Kontaktieren des VMware-Supports

Bei einigen Ereignissen gehört zur empfohlenen Aktion das Erfassen von Tech-Support-Protokollen und die Kontaktaufnahme mit dem VMware-Support.

- Informationen zum Erfassen von NSX Manager-Tech-Support-Protokollen erhalten Sie unter Herunterladen der Protokolle des technischen Supports für NSX.
- Informationen zum Erfassen von NSX Edge-Tech-Support-Protokollen erhalten Sie unter Herunterladen von Tech-Support-Protokollen für NSX Edge.
- Zur Erfassung der Host-Tech-Support-Protokolle führen Sie den Befehl `export host-tech-support` aus (siehe „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*).
- Erläuterungen zur Kontaktaufnahme mit dem VMware-Support erhalten Sie unter „How to file a Support Request in My VMware“ (Wie stelle ich in „Mein VMware“ eine Support-Anfrage, http://kb.vmware.com/kb/2006985).

Erzwingen einer Synchronisierung von NSX Edge

Bei einigen Ereignissen gehört zur empfohlenen Aktion die Erzwingung einer Synchronisierung von NSX Edge. Weitere Informationen finden Sie unter „Erzwingen der Synchronisierung von NSX Edge mit NSX Manager“ im *Administratorhandbuch für NSX*. Beim Erzwingen einer Synchronisierung handelt es sich um einen unterbrechenden Vorgang, der die NSX Edge-VM neu startet.

Schweregrad des Systemereignisses

Für jedes Ereignis gilt einer der folgenden Schweregrade:

- Zur Information
- Niedrig
- Mittel
- Haupt
- Kritisch
- Hoch

In den folgenden Themen werden Systemereignismeldungen mit den Schweregraden „Haupt“, „Kritisch“ und „Hoch“ von verschiedenen Komponenten dargestellt.

Dieses Kapitel behandelt die folgenden Themen:

Sicherheitssystemereignisse

Die Tabelle erläutert Systemereignismeldungen für die Sicherheit mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
11002	Kritisch	Nein	`Herstellen der Verbindung mit vCenter Server nicht möglich. Ungültiger Benutzername bzw. ungültiges Kennwort (Unable to connect to vCenter Server Bad username/password).`	Fehler bei der vCenter Server-Konfiguration. Aktion: Stellen Sie sicher, dass die vCenter Server-Konfiguration korrekt ist und die richtigen Anmeldedaten bereitgestellt werden. Weitere Informationen finden Sie unter „Registrieren von vCenter Server bei NSX Manager“ im *Administratorhandbuch für NSX* und „Verbinden von NSX Manager mit vCenter Server“ im *Fehlerbehebungshandbuch zu NSX*.
11006	Kritisch	Nein	`Verbindung zu vCenter Server ist unterbrochen (Lost vCenter Server connectivity).`	Die Verbindung mit vCenter Server wurde getrennt. Aktion: Überprüfen Sie vCenter Server auf mögliche Konnektivitätsprobleme. Weitere Informationen finden Sie unter „Verbinden von NSX Manager mit vCenter Server“ und „Fehlerbehebung bei NSX Manager-Problemen“ im Dokument *Fehlerbehebungshandbuch zu NSX*.
230000	Kritisch	Nein	`SSO-Konfigurationsaufgabe auf NSX Manager fehlgeschlagen (SSO Configuration Task on NSX Manager failed).`	Die SSO-Konfiguration (Single Sign-On) konnte nicht durchgeführt werden. Zu möglichen Ursachen gehören ungültige Anmeldedaten, eine ungültige Konfiguration oder eine Zeitüberschreitung bei der Synchronisierung. Aktion: Überprüfen Sie die Fehlermeldung und konfigurieren Sie SSO erneut. Weitere Informationen finden Sie unter „Konfigurieren von Single Sign-On“ im Dokument *Administratorhandbuch für NSX*. Außerdem erhalten Sie entsprechende Erläuterungen unter „Konfigurieren des NSX SSO Lookup Service schlägt fehl“ im *Fehlerbehebungshandbuch zu NSX*.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
230002	Kritisch	Nein	`SSO-STS-Client ist getrennt (SSO STS Client disconnected).`	Die Registrierung von NSX Manager beim SSO-Dienst ist fehlgeschlagen oder die Verbindung mit dem SSO-Dienst wurde getrennt. Aktion: Überprüfen Sie die Konfiguration auf eventuelle Probleme wie ungültige Anmeldedaten, fehlende Synchronisierung und Probleme der Netzwerkkonnektivität. Dieses Ereignis kann auch aufgrund spezieller technischer VMware-Probleme auftreten. Weitere Informationen finden Sie im KB-Artikel „SSL certificate of the STS service cannot be verified“ (SSL-Zertifikat des STS-Dienstes kann nicht verifiziert werden, http://kb.vmware.com/kb/2121696) und „Registering NSX Manager to Lookup Service with External Platform Service Controller (PSC) fails with the error: server certificate chain not verified“ (Registrieren von NSX Manager beim Lookup Service mit dem externen Platform Service Controller (PSC) scheitert mit folgender Fehlermeldung: Serverzertifikatskette wurde nicht verifiziert http://kb.vmware.com/kb/2132645).
240000	Kritisch	Nein	`Es wurde ein Eintrag {0} zur Authentifizierungs-Blacklist hinzugefügt (Added an entry {0} to authentication black list).`	Ein Benutzer mit einer bestimmten IP-Adresse konnte sich nicht zehnmal hintereinander nicht anmelden und wurde 30 Minuten lang gesperrt. Aktion: Prüfen Sie, ob ein potenzielles Sicherheitsrisiko vorliegt.

Distributed-Firewall-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für die verteilte Firewall mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301001	Kritisch	Nein	`Fehler beim Aktualisieren der Filterkonfiguration auf dem Host (Filter config update failed on host).`	Der Host hat die Filterkonfiguration nicht erhalten/analysiert oder das Gerät */dev/dvfiltertbl* konnte nicht geöffnet werden. Aktion: Überprüfen Sie das Schlüsselwertpaar auf den Kontext und auf Fehlerursachen. Eventuell stimmt auch die VIB-Version von NSX Manager und den vorbereiteten Hosts nicht überein und es sind unerwartete Upgrade-Probleme aufgetreten. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301002	Haupt	Nein	`Filterkonfiguration wird nicht auf vNIC angewendet (Filter config not applied to vnic).`	Die Filterkonfiguration konnte nicht auf vNIC angewendet werden. Mögliche Ursachen: Fehler beim Öffnen, Analysieren oder Aktualisieren der Filterkonfiguration. Dieser Fehler sollte mit der verteilten Firewall eigentlich nicht auftreten, kann aber in NetX-Szenarien (Network Extensibility, Netzwerk-Erweiterbarkeit) vorkommen. Aktion: Erfassen Sie die Tech-Support-Pakete für ESXi und NSX Manager und wenden Sie sich an den technischen Support von VMware.
301031	Kritisch	Nein	`Fehler beim Aktualisieren der Firewallkonfiguration auf dem Host (Firewall config update failed on host).`	Firewallkonfiguration konnte nicht empfangen/analysiert/aktualisiert werden. Der Schlüsselwert verfügt über Kontextinformationen wie die Generierungsnummer und noch über weitere Debug-Informationen. Aktion: Stellen Sie sicher, dass der Hostvorbereitungsvorgang korrekt durchgeführt wurde. Melden Sie sich beim Host an und erfassen Sie die Datei `/var/log/vsfwd.log`. Erzwingen Sie anschließend die Synchronisierung der Firewallkonfiguration mit der `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>`-API (siehe „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*). Wenn die Distributed Firewall-Konfiguration auf dem Host weiterhin nicht aktualisiert werden kann, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und kontaktieren Sie den technischen Support von VMware.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301032	Haupt	Nein	`Fehler beim Anwenden der Firewallregel auf vNIC (Failed to apply firewall rule to vnic).`	Fehler beim Anwenden der Firewallregeln auf die vNIC. Aktion: Stellen Sie sicher, dass die vsip-Kernel-Heaps über ausreichend freien Arbeitsspeicher verfügen (siehe „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*.) Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware. Stellen Sie sicher, dass die Hostprotokolle (*vmkernel.log* und *vsfwd.log*) den Zeitraum enthalten, in dem die Firewallkonfiguration auf die vNIC angewendet wurde.
301041	Kritisch	Nein	`Aktualisieren der Containerkonfiguration auf Host fehlgeschlagen (Container configuration update failed on host).`	Ein Vorgang mit Zusammenhang mit der Netzwerk- und Sicherheits-Containerkonfiguration konnte nicht durchgeführt werden. Der Schlüsselwert verfügt über Kontextinformationen wie den Containernamen und die Generierungsnummer. Aktion: Stellen Sie sicher, dass die vsip-Kernel-Heaps über ausreichend freien Arbeitsspeicher verfügen (siehe „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*.) Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware. Stellen Sie sicher, dass die Hostprotokolle (*vmkernel.log* und *vsfwd.log*) den Zeitraum enthalten, in dem die Containerkonfiguration auf die vNIC angewendet wurde.
301051	Haupt	Nein	`Flow fehlt auf dem Host (Flow missed on host).`	Es wurden Flussdaten für eine oder mehrere Sitzungen zu und von geschützten virtuellen Maschinen verworfen oder sie konnten nicht gelesen oder nicht an NSX Manager gesendet werden. Aktion: Stellen Sie sicher, dass die vsip-Kernel-Heaps über ausreichend freien Arbeitsspeicher verfügen und dass sich die vsfwd-Arbeitsspeichernutzung innerhalb der Ressourcengrenzwerte bewegt (siehe „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*.) Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301061	Kritisch	Nein	`Fehler beim Aktualisieren der SpoofGuard-Konfiguration auf dem Host (Spoofguard config update failed on host).`	Eine Konfigurationsvorgang im Zusammenhang mit SpoofGuard konnte nicht durchgeführt werden. Aktion: Stellen Sie sicher, dass der Hostvorbereitungsvorgang korrekt durchgeführt wurde. Melden Sie sich beim Host an und erfassen Sie die Datei `/var/log/vsfwd.log`. Erzwingen Sie anschließend die Synchronisierung der Firewallkonfiguration mit der `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>` -API (siehe „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*). Wenn die SpoofGuard-Konfiguration weiterhin fehlschlägt, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware. Stellen Sie sicher, dass die Protokolle den Zeitraum enthalten, in dem der Host die SpoofGuard-Konfiguration erhalten hat.
301062	Haupt	Nein	`Fehler beim Anwenden von SpoofGuard auf vnic (Failed to apply spoofguard to vnic).`	SpoofGuard konnte nicht auf eine vNIC angewendet werden. Aktion: Stellen Sie sicher, dass der Hostvorbereitungsvorgang korrekt durchgeführt wurde. Melden Sie sich beim Host an und erfassen Sie die Datei `/var/log/vsfwd.log`. Erzwingen Sie anschließend die Synchronisierung der Firewallkonfiguration mit der `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>`-API (siehe „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*). Wenn die SpoofGuard-Konfiguration weiterhin fehlschlägt, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301064	Haupt	Nein	`Fehler beim Deaktivieren von SpoofGuard für vnic (Failed to disable spoofguard for vnic).`	SpoofGuard konnte nicht für eine vNIC deaktiviert werden. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301072	Kritisch	Nein	`Fehler beim Löschen der Legacy-App-Dienst-VM (Failed to delete legacy App service vm).`	Die vShield-App-Dienst-VM für „vCloud Networking and Security“ konnte nicht gelöscht werden. Aktion: Stellen Sie sicher, dass der Vorgang „Upgrade von vShield App auf die verteilte Firewall“ im *Upgrade-Handbuch für NSX* korrekt durchgeführt wurde.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301080	Kritisch	Nein	`CPU-Schwellenwert der Firewall überschritten (Firewall CPU threshold crossed).`	Der Schwellenwert für die vsfwd-CPU-Nutzung wurde überschritten. Aktion: Informationen dazu finden Sie im Abschnitt „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*. Sie müssen möglicherweise die Ressourcennutzung des Hosts verringern. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301081	Kritisch	Nein	`Speicherschwellenwert der Firewall überschritten (Firewall memory threshold crossed).`	Der Schwellenwert für die vsfwd-Arbeitsspeichernutzung wurde überschritten. Aktion: Informationen dazu finden Sie im Abschnitt „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*. Sie müssen möglicherweise die Ressourcennutzung des Hosts verringern, inklusive der Anzahl der konfigurierten Firewallregeln oder der Netzwerk- und Sicherheitscontainer. Zur Reduzierung der Anzahl der Firewallregeln verwenden Sie die `appliedTo`-Funktion. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301082	Kritisch	Nein	`ConnectionsPerSecond-Schwellenwert der Firewall überschritten (Firewall ConnectionsPerSecond threshold crossed).`	Der Schwellenwert für die Firewallverbindungen pro Sekunde wurde überschritten. Aktion: Informationen dazu finden Sie im Abschnitt „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*. Sie müssen möglicherweise die Ressourcennutzung des Hosts verringern, inklusive der Anzahl der aktiven Verbindungen zu und von VMs auf dem Host.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301501	Kritisch	Nein	Zeitüberschreitung für das Firewall-Konfigurations-Update Version {version#} auf Host {hostID} (Firewall configuration update version {version#} to host {hostID} timed out). Die Firewall-Konfiguration auf Host wird auf Version {version#} synchronisiert (Firewall configuration on host is synced upto version {version#}).	Ein Host benötigte mehr als zwei Minuten zur Verarbeitung der Aktualisierung der Firewallkonfiguration. Die Zeit für die Aktualisierung wurde überschritten. Aktion: Stellen Sie sicher, dass vsfwd korrekt funktioniert und dass Regeln für den Host veröffentlicht wurden. Weitere Informationen finden Sie unter „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301502	Kritisch	Nein	Zeitüberschreitung für das SpoofGuard-Konfigurations-Update Nummer {number#} auf Host {hostID}. (Spoofguard configuration update number {number#} to host {hostID} timed out). Die SpoofGuard-Konfiguration auf Host wird auf Version {version#} synchronisiert (Spoofguard configuration on host is synced upto version {version#}).	Ein Host benötigte mehr als zwei Minuten zur Verarbeitung der Aktualisierung der Spoofguard-Konfiguration. Die Zeit für die Aktualisierung wurde überschritten. Aktion: Stellen Sie sicher, dass vsfwd korrekt funktioniert und dass Regeln für den Host veröffentlicht wurden. Weitere Informationen finden Sie unter „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301503	Kritisch	Nein	Veröffentlichung der Firewall-Konfiguration Version {1} auf Cluster {0} fehlgeschlagen (Failed to publish firewall configuration version {version#} to cluster {clusterID}). Details finden Sie in den Protokollen (Refer logs for details).	Die Veröffentlichung der Firewallregeln konnte für einen Cluster oder für einen oder mehrere Hosts nicht durchgeführt werden. Aktion: Informationen dazu finden Sie unter „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301504	Kritisch	Nein	`Veröffentlichung der Container-Updates auf Cluster {clusterID} fehlgeschlagen (Failed to publish container updates to cluster {clusterID}). Details finden Sie in den Protokollen (Refer logs for details).`	Die Veröffentlichung der Aktualisierung von Netzwerk- und Sicherheitscontainern konnte für einen Cluster oder für einen oder mehrere Hosts nicht durchgeführt werden. Aktion: Informationen dazu finden Sie unter „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301505	Kritisch	Nein	`Veröffentlichung der SpoofGuard-Updates auf Cluster {clusterID} fehlgeschlagen (Failed to publish spoofguard updates to cluster {clusterID}). Details finden Sie in den Protokollen (Refer logs for details).`	Die Veröffentlichung der SpoofGuard-Aktualisierungen konnte für einen Cluster oder für einen oder mehrere Hosts nicht durchgeführt werden. Aktion: Informationen dazu finden Sie unter „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301506	Kritisch	Nein	`Veröffentlichung der Ausschlusslisten-Updates auf Cluster {clusterID} fehlgeschlagen (Failed to publish exclude list updates to cluster {clusterID}). Details finden Sie in den Protokollen (Refer logs for details).`	Die Veröffentlichung der Aktualisierungen von Ausschlusslisten konnte für einen Cluster oder für einen oder mehrere Hosts nicht durchgeführt werden. Aktion: Informationen dazu finden Sie unter „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301508	Kritisch	Nein	`Synchronisierung von Host {hostID} fehlgeschlagen (Failed to sync host {hostID}). Details finden Sie in den Protokollen (Refer logs for details).`	Ein Firewallvorgang zur Erzwingung der Synchronisierung über die `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>`-API ist fehlgeschlagen. Aktion: Informationen dazu finden Sie unter „Fehlerbehebung für die verteilte Firewall“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301510	Kritisch	Nein	`Der Vorgang zum Erzwingen der Synchronisierung für den Cluster ist fehlgeschlagen (Force sync operation failed for the cluster).`	Ein Firewallvorgang zur Erzwingung der Synchronisierung über die `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` -API ist fehlgeschlagen. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301512	Haupt	Nein	`Firewall ist auf dem Host {hostID}[{hostID}] installiert. (Firewall is installed on host {hostID}[{hostID}]).`	Die verteilte Firewall wurde erfolgreich auf einem Host installiert. Aktion: Wechseln Sie in vCenter Server zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte „Hostvorbereitung“ aus. Stellen Sie sicher, dass für den Firewallstatus grün angezeigt wird.
301513	Haupt	Nein	`Firewall wurde auf dem Host {hostID}[{hostID}] deinstalliert. (Firewall is uninstalled on host {hostID}[{hostID}]).`	verteilte Firewall wurde von einem Host deinstalliert. Wenn die Distributed Firewall-Komponenten nicht deinstalliert werden können, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host, und wenden Sie sich an den technischen Support von VMware.
301514	Kritisch	Nein	`Firewall ist auf Cluster {clusterID} aktiviert. (Firewall is enabled on cluster {clusterID}).`	Die verteilte Firewall wurde erfolgreich auf einem Cluster installiert. Aktion: Wechseln Sie in vCenter Server zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte „Hostvorbereitung“ aus. Stellen Sie sicher, dass für den Firewallstatus grün angezeigt wird.
301515	Kritisch	Nein	`Firewall wurde auf dem Cluster {clusterID} deinstalliert. (Firewall is uninstalled on cluster {clusterID}).`	Die verteilte Firewall wurde von einem Cluster deinstalliert. Aktion: Wenn die Distributed Firewall-Komponenten nicht deinstalliert werden können, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host, und wenden Sie sich an den technischen Support von VMware.
301516	Kritisch	Nein	`Firewall ist auf Cluster {clusterID} deaktiviert. (Firewall is disabled on cluster {clusterID}).`	verteilte Firewall wurde auf allen Hosts in einem Cluster deaktiviert. Aktion: Keine erforderlich.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301034	Haupt	Nein	`Firewallregeln konnten nicht auf Host angewendet werden (Failed to apply Firewall rules to host).`	Der Regelabschnitt einer verteilten Firewall konnte nicht angewendet werden. Aktion: Stellen Sie sicher, dass die vsip-Kernel-Heaps über ausreichend freien Arbeitsspeicher verfügen (siehe „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*.) Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301043	Kritisch	Nein	`Containerkonfiguration konnte nicht auf vNic angewendet werden. (Failed to apply container configuration to vnic).`	Eine Netzwerk- und Sicherheits-Containerkonfiguration konnte nicht angewendet werden. Aktion: Stellen Sie sicher, dass die vsip-Kernel-Heaps über ausreichend freien Arbeitsspeicher verfügen (siehe „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*.) Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301044	Kritisch	Nein	`Containerkonfiguration konnte nicht auf Host angewendet werden (Failed to apply container configuration to host).`	Eine Netzwerk- und Sicherheits-Containerkonfiguration konnte nicht angewendet werden. Aktion: Stellen Sie sicher, dass die vsip-Kernel-Heaps über ausreichend freien Arbeitsspeicher verfügen (siehe „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*.) Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.
301066	Haupt	Nein	`SpoofGuard-Konfiguration konnte nicht auf Host angewendet werden (Failed to apply Spoofguard configuration to host).`	SpoofGuard konnte insgesamt nicht auf die vNICs angewendet werden. Aktion: Stellen Sie sicher, dass die vsip-Kernel-Heaps über ausreichend freien Arbeitsspeicher verfügen (siehe „Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen“ im *Administratorhandbuch für NSX*.) Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301100	Kritisch	Nein	`Aktualisierung der Firewall-Zeitüberschreitungskonfiguration auf Host nicht erfolgreich. (Firewall timeout configuration update failed on host).`	Die Zeitüberschreitungskonfiguration für den Firewall-Sitzungs-Timer konnte nicht aktualisiert werden. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware. Erzwingen Sie nach der Erfassung der Protokolle die Synchronisierung der Firewallkonfiguration mit der REST-API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` oder wechseln Sie zu **Installation > Hostvorbereitung** und wählen Sie unter **Aktionen** die Option **ForceSync-Dienste** aus.
301101	Haupt	Nein	`Firewall-Zeitüberschreitungskonfiguration konnte nicht auf vNic angewendet werden. (Failed to apply firewall timeout configuration to vnic).`	Die Zeitüberschreitungskonfiguration für den Firewall-Sitzungs-Timer konnte nicht aktualisiert werden. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware. Erzwingen Sie nach der Erfassung der Protokolle die Synchronisierung der Firewallkonfiguration mit der REST-API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` oder wechseln Sie zu **Installation > Hostvorbereitung** und wählen Sie unter **Aktionen** die Option **ForceSync-Dienste** aus.
301103	Haupt	Nein	`Firewall-Zeitüberschreitungskonfiguration konnte nicht auf Host angewendet werden (Failed to apply firewall timeout configuration to host).`	Die Zeitüberschreitungskonfiguration für den Firewall-Sitzungs-Timer konnte nicht aktualisiert werden. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und den Host und wenden Sie sich an den technischen Support von VMware. Erzwingen Sie nach der Erfassung der Protokolle die Synchronisierung der Firewallkonfiguration mit der REST-API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` oder wechseln Sie zu **Installation > Hostvorbereitung** und wählen Sie unter **Aktionen** die Option **ForceSync-Dienste** aus.
301200	Haupt	Nein	`Flow-Analyse für Application Rule Manager gestartet (Application Rule Manager flow analysis started).`	Flow-Analyse für Application Rule Manager gestartet. Aktion: Keine erforderlich.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
301201	Haupt	Nein	Flow-Analyse für Application Rule Manager fehlgeschlagen (Application Rule Manager flow analysis failed).	Flow-Analyse für Application Rule Manager fehlgeschlagen. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und wenden Sie sich an den technischen Support von VMware. Starten Sie eine neue Überwachungssitzung für die gleichen vNICs wie in der fehlgeschlagenen Sitzung, um den Vorgang erneut auszuführen.
301202	Haupt	Nein	Flow-Analyse für Application Rule Manager abgeschlossen (Application Rule Manager flow analysis completed).	Flow-Analyse für Application Rule Manager wurde abgeschlossen. Aktion: Keine erforderlich.

NSX Edge-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für NSX Edge mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“. Systemereignisse mit Informationen zum Schweregrad werden aufgeführt, wenn der Alarm durch solche Ereignisse ausgelöst wird.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30011	Hoch	Nicht verfügbar	Keine der NSX Edge-VMs befindet sich im Bereitstellungszustand. Möglicherweise ist die Netzwerkverbindung unterbrochen (None of the NSX Edge VMs found in serving state. There is a possibility of network disruption).	Die NSX Edge-VMs müssen automatisch von diesem Status aus wiederhergestellt werden. Suchen Sie nach einem Trap mit dem Ereigniscode 30202 oder 30203. Aktion: Informationen dazu finden Sie unter „Beheben von Fehlern der Edge-Appliance“ im *Fehlerbehebungshandbuch zu NSX*.
30013	Kritisch	130013	NSX Manager hat festgestellt, dass NSX Edge-VM (vmId: {#}) einen ungültigen Status hat (NSX Manager found NSX Edge VM (vmId : {#}) in bad state). Eine erzwungene Synchronisierung ist erforderlich (Needs a force sync).	Die NSX Edge-VM meldet einen fehlerhaften Status und funktioniert eventuell nicht korrekt. Aktion: Wenn ein problematischer Staus ermittelt wurde, wird automatisch eine erzwungene Synchronisierung ausgelöst. Wenn die automatische Erzwingung der Synchronisierung scheitert, versuchen Sie, die Synchronisierung manuell zu erzwingen.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30014	Haupt	Nicht verfügbar	`Fehler beim Kommunizieren mit der NSX Edge-VM (Failed to communicate with the NSX Edge VM).`	NSX Manager kommuniziert mit NSX Edge über VIX oder den Nachrichtenbus. Der Kommunikationskanal wird von NSX Manager je nachdem ausgewählt, ob die Hostvorbereitung zum Zeitpunkt der Edge-Bereitstellung oder der erneuten Edge-Bereitstellung durchgeführt oder nicht durchgeführt wurde. Dieses Ereignis weist darauf hin, dass NSX Manager nicht mehr mit NSX Edge kommunizieren kann. Aktion: Informationen dazu finden Sie unter „Beheben von Fehlern der Edge-Appliance“ im *Fehlerbehebungshandbuch zu NSX*.
30027	Zur Information	130027	`NSX Edge-VM (vmld: {#}) ist ausgeschaltet (NSX Edge VM (vmId : {#}) is powered off).`	Die NSX Edge-VM wurde ausgeschaltet. Aktion: Rein informatives Ereignis
30032	Hoch	130032	`Die NSX Edge-Appliance mit vmId: {#} wurde nicht in der vCenter-Bestandsliste gefunden (NSX Edge appliance with vmId : {#} not found in the vCenter inventory).`	Die NSX Edge-VM wurde wahrscheinlich direkt aus vCenter Server gelöscht. Es handelt sich hier um keinen unterstützen Vorgang, da NSX-verwaltete Objekte über die vSphere Web Client-Schnittstelle für NSX hinzugefügt oder gelöscht werden müssen. Aktion: Stellen Sie das Edge erneut bereit oder stellen Sie ein neues Edge bereit.
30033	Hoch	130033	`NSX Edge-VM (vmId : {#}) nicht im vCenter-Bestand gefunden (NSX Edge VM (vmId : {#}) not found in the vCenter inventory).`	Die NSX Edge-VM kann in der vCenter-Bestandsliste nicht gefunden werden. Aktion: Prüfen Sie, ob die VM versehentlich gelöscht wurde. Nach der Bestätigung wird das Edge erneut bereitgestellt.
30034	Kritisch	130034	`Keine der NSX Edge-VMs befindet sich im Bereitstellungszustand. Möglicherweise ist die Netzwerkverbindung unterbrochen (None of the NSX Edge VMs found in serving state. There is a possibility of network disruption).`	Die Edge-VM reagiert nicht auf die von NSX Manager gesendete Systemstatusprüfung. Aktion: Stellen Sie sicher, dass die Edge-VM eingeschaltet ist. Erfassen Sie anschließend die Edge-Protokolle und wenden Sie sich an den technischen Support von VMware.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30037	Kritisch	Nicht verfügbar	Die in {#} geänderte Edge-Firewallregel ist für {#} nicht mehr verfügbar (Edge firewall rule modified as {#} is no longer available for {#}).	In der Firewallregel ist ein ungültiges GroupingObject (IPSet, Sicherheitsgruppe, etc.) vorhanden. Aktion: Führen Sie in der Firewallregel die erforderlichen Aktualisierungen durch.
30038	Kritisch	Nicht verfügbar	Die eingeschaltete NSX Edge-Appliance: {EdgeID #}, {vmName #}, verstößt gegen eine Anti-Affinitätsregel für virtuelle Maschinen (Powered-on NSX Edge appliance : {EdgeId #}, {vmName #} violates the virtual machine anti-affinity rule).	Die NSX Edge-Hochverfügbarkeit wendet automatisch Anti-Affinitätsregeln auf vSphere-Hosts an, sodass die aktiven und Standby-Edge-VMs auf unterschiedlichen Hosts bereitgestellt werden. Dieses Ereignis weist darauf hin, dass diese Anti-Affinitätsregeln aus dem Cluster entfernt wurden und dass beide Edge-VMs auf demselben Host ausgeführt werden. Aktion: Wechseln Sie zu vCenter Server und überprüfen Sie die Anti-Affinitätsregeln.
30045	Kritisch	Nicht verfügbar	Die Systemstatusprüfung der NSX Edge-VM ist mit kritischen vix-Fehlern fehlgeschlagen. Eine weitergehende Systemstatusprüfung ist für diese VM deaktiviert. Stellen Sie sie erneut bereit oder erzwingen Sie eine Synchronisierung der VM, um die Systemstatusprüfung wieder aufzunehmen (NSX Edge VM health check failing with critical vix errors. Further health check is disabled for vm. Please redeploy or forcesync vm to resume health check).	Die Netzwerkumgebung verursacht eventuell immer wieder Fehler bei der Kommunikation mit der Edge-VM über den VIX-Kanal. Aktion: Erfassen Sie die NSX Manager- und NSX Edge-Tech-Support-Protokolle, wenn NSX Edge antwortet. Erzwingen Sie dann eine Synchronisierung. Wenn das Problem weiterhin besteht, stellen Sie NSX Edge erneut bereit (siehe „Erneutes Bereitstellen von NSX Edge“ im *Administratorhandbuch für NSX*). **Hinweis** Das erneute Bereitstellen ist eine Aktion, die den Betrieb unterbricht. Es empfiehlt sich, zuerst eine erzwungene Synchronisierung durchzuführen und erst, wenn sich das Problem dadurch nicht beheben lässt, eine erneute Bereitstellung vorzunehmen.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30046	Kritisch	Nicht verfügbar	Das Veröffentlichen der Vorab-Regeln ist auf der Edge fehlgeschlagen: {EdgeID#}, vm: {#} für Erstellungsnummer {#} (Pre rules publish failed on edge: {EdgeID#}, vm: {#} for generation number {#}). Details finden Sie in den Protokollen (Refer logs for detail). Möglicherweise ist das Erzwingen der Synchronisierung notwendig (It may need forcesync).	Die NSX Edge-Firewallregeln sind eventuell nicht mehr synchron. Dieser Fehler wird generiert, wenn die Vorabregeln (konfiguriert mit der DFW-Benutzeroberfläche/API) fehlschlagen. Aktion: Wenn das Problem nicht automatisch durch den integrierten Wiederherstellungsvorgang behoben wird, erzwingen Sie die Synchronisierung manuell.
30100	Kritisch	Nicht verfügbar	Die Synchronisierung von NSX Edge wurde erzwungen (NSX Edge was force synced).	Für die NSX Edge-VM wurde die Synchronisierung erzwungen. Aktion: Wenn das Problem durch das Erzwingen der Synchronisierung nicht behoben wird, erfassen Sie die Tech-Support-Protokolle für NSX Manager und NSX Edge und wenden Sie sich an den technischen Support von VMware.
30102	Hoch	130102	Der Status von NSX Edge (vmId : {IP Address}) ist ungültig (NSX Edge (vmId : {IP Address}) is in Bad State). Eine erzwungene Synchronisierung ist erforderlich (Needs a force sync).	Bei der NSX Edge-VM ist ein interner Fehler aufgetreten. Aktion: Wenn das Problem nicht automatisch durch den integrierten Wiederherstellungsvorgang behoben wird, erzwingen Sie die Synchronisierung manuell.
30148	Kritisch	Nicht verfügbar	Die CPU-Nutzung von NSX Edge hat sich erhöht. Die {#} wichtigsten Prozesse sind: {#} (NSX Edge CPU usage has increased. {#} Top processes are: {#}).	Die CPU-Nutzung der NSX Edge-VM ist dauerhaft hoch. Aktion: Informationen dazu finden Sie unter „Beheben von Fehlern der Edge-Appliance“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und NSX Edge und wenden Sie sich an den technischen Support von VMware.
30153	Haupt	Nicht verfügbar	Die AESNI-Crypto-Engine ist verfügbar (AESNI crypto engine is up).	Die AESNI-Crypto-Engine ist verfügbar. Aktion: Keine erforderlich.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30154	Haupt	Nicht verfügbar	Die AESNI-Crypto-Engine ist nicht verfügbar (AESNI crypto engine is down).	Die AESNI-Crypto-Engine ist nicht verfügbar. Aktion: Keine erforderlich. Dies ist der vorgesehene Status.
30155	Hoch	130155	Nicht genügend CPU- und/oder Arbeitsspeicherressourcen auf Host oder im Ressourcenpool während der Ressourcenreservierung zum Zeitpunkt der Bereitstellung des NSX Edge (Insufficient CPU and/or Memory Resources available on Host or Resource Pool, during resource reservation at the time of NSX Edge deployment).	Nicht genügend CPU- und/oder Arbeitsspeicherressourcen auf Host oder im Ressourcenpool Sie können die verfügbaren und reservierten Ressourcen anzeigen, indem Sie zur Seite **Home > Hosts und Cluster > [Clustername] (Hosts and Clusters > [Cluster-name])**> **Überwachung (Monitor) > Ressourcenreservierung (Resource Reservation)** navigieren. Nach der Prüfung der verfügbaren Ressourcen geben Sie die Ressourcen im Rahmen der Appliancekonfiguration erneut an, damit das Limit für die Ressourcenreservierung erfolgreich ist.
30180	Kritisch	Nicht verfügbar	NSX Edge weist nicht genügend Arbeitsspeicher auf. Für Edge wird in 3 Sekunden ein Neustart durchgeführt. Dies sind die fünf wichtigsten Prozesse: {#} (NSX Edge is out of memory. The Edge is rebooting in 3 seconds. Top 5 processes are: {#}).	Der Arbeitsspeicher der NSX Edge-VM ist nicht mehr ausreichend. Zur Wiederherstellung wurde ein Neustart ausgelöst. Aktion: Informationen dazu finden Sie unter „Beheben von Fehlern der Edge-Appliance“ im *Fehlerbehebungshandbuch zu NSX*. Wenn das Problem weiterhin besteht, erfassen Sie die Tech-Support-Protokolle für NSX Manager und NSX Edge und wenden Sie sich an den technischen Support von VMware.
30181	Kritisch	130181	NSX Edge {EdgeID#} VM-Name {#} Dateisystem ist schreibgeschützt (NSX Edge {EdgeID#} VM name {#} file system is read only).	Bei den Speichergeräten für die Sicherung der NSX Edge-VM ist ein Konnektivitätsproblem aufgetreten. Aktion: Überprüfen Sie das Problem der Konnektivität mit dem Sicherungsdatenspeicher und korrigieren Sie es. Wenn das Konnektivitätsproblem behoben ist, ist es sinnvoll, die Synchronisierung manuell zu erzwingen.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30202	Haupt	Nicht verfügbar	NSX Edge {EdgeID#} HighAvailability wurde umgeschaltet (NSX Edge {EdgeID#} HighAvailability switch over happened). Auf der VM {#} mit dem Namen {#} wurde der Status ACTIVE aktiviert (VM {#} name {#} has moved to ACTIVE state).	Ein HA-Failover ist aufgetreten und die sekundäre NSX Edge-VM ist vom Status STANDBY auf den Status AKTIV übergegangen. Aktion: Es ist keine Aktion erforderlich.
30203	Haupt	Nicht verfügbar	NSX Edge {EdgeID} HighAvailability wurde umgeschaltet (NSX Edge {EdgeID} HighAvailability switch over happened). Auf der VM {#} mit dem Namen {#} wurde der Status STANDBY aktiviert (VM {#} name {#} has moved to STANDBY state).	Ein HA-Failover ist aufgetreten und die primäre NSX Edge-VM ist vom Status AKTIV auf den Status STANDBY übergegangen. Aktion: Es ist keine Aktion erforderlich.
30205	Kritisch	130205	Split Brain-Syndrom für NSX Edge {EdgeID} mit HighAvailability erkannt (Split Brain detected for NSX Edge {EdgeID} with HighAvailability).	Aufgrund eines Netzwerkfehlers können die für HA konfigurierten NSX Edge-VMs nicht bestimmen, ob die andere VM online ist. In diesem Fall gehen beide VMs davon aus, dass die jeweils andere online ist, und erhalten den Status AKTIV. Dies kann zu einer Unterbrechung der Netzwerkverbindung führen. Aktion: Überprüfen Sie die Netzwerkinfrastruktur (virtuell und physisch) auf Fehler, speziell bei den Schnittstellen und beim Pfad, der für HA konfiguriert ist.
30302	Kritisch	130302	Der virtualServer/Pool des LoadBalancer: {virtualServerName]} Protokoll: {#} serverIp: {IP Address} hat den Zustand in "down" geändert (LoadBalancer virtualServer/pool : {virtualServerName]} Protocol : {#} serverIp : {IP Address} changed the state to down).	Ein virtueller Server oder Pool im NSX Edge-Load-Balancer ist nicht verfügbar. Aktion: Informationen dazu finden Sie im Abschnitt „Load Balancing“ im *Fehlerbehebungshandbuch zu NSX*.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30303	Haupt	Nicht verfügbar	`Der virtualServer/Pool des LoadBalancer: {0} Protokoll: {#} serverIp: {IP Address} hat den Zustand in "wrong" geändert (LoadBalancer virtualServer/pool : {0} Protocol : {#} serverIp : {IP Address} changed to a wrong state).`	Bei einem virtuellen Server oder Pool im NSX Edge-Load-Balancer ist ein interner Fehler aufgetreten. Aktion: Informationen dazu finden Sie im Abschnitt „Load Balancing“ im *Fehlerbehebungshandbuch zu NSX*.
30304	Haupt	130304	`LoadBalancer-Pool: {0} Protokoll: {#} serverIp: {IP Address} ist in einen Warnstatus gewechselt (LoadBalancer pool : {0} Protocol : {#} serverIp : {IP address} changed to a warning state).`	Der Status eines NSX Edge-Load-Balancer-Pools wurde in **Warnung (warning)** geändert. Aktion: Informationen dazu finden Sie im Abschnitt „Load Balancing“ im *Fehlerbehebungshandbuch zu NSX*.
30402	Kritisch	130402	`IPsec-Kanal von localIp: {IP address} zu peerIp: {IP address} hat den Status in "down" geändert (IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to down).`	Ein NSX Edge-IPSec-VPN-Kanal ist nicht verfügbar. Aktion: Schlagen Sie für Informationen dazu im Abschnitt „Virtuelle Private Netzwerke (VPN)“ im *Fehlerbehebungshandbuch zu NSX* nach.
30404	Kritisch	130404	`EDGE IPSEC TUNNEL DOWN : IPsec-Tunnel von localSubnet: {subnet} zu peerSubnet: {subnet} hat den Status in "down" geändert (EDGE IPSEC TUNNEL DOWN : IPsec Tunnel from localSubnet : {subnet} to peerSubnet : {subnet} changed the status to down).`	Ein NSX Edge-IPSec-VPN-Kanal ist nicht verfügbar. Aktion: Schlagen Sie für Informationen dazu im Abschnitt „Virtuelle Private Netzwerke (VPN)“ im *Fehlerbehebungshandbuch zu NSX* nach.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30405	Haupt	Nicht verfügbar	IPsec-Kanal von localIp: {IP address} zu peerIp: {IP address} hat den Status in "unknown" geändert (IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown).	Der Status eines NSX Edge-IPSec-VPN-Kanals kann nicht ermittelt werden. Aktion: Schlagen Sie für Informationen dazu im Abschnitt „Virtuelle Private Netzwerke (VPN)“ im *Fehlerbehebungshandbuch zu NSX* nach.
30406	Haupt	Nicht verfügbar	IPsec-Kanal von localIp: {IP address} zu peerIp: {IP address} hat den Status in "unknown" geändert (IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown).	Der Status eines NSX Edge-IPSec-VPN-Kanals kann nicht ermittelt werden. Aktion: Schlagen Sie für Informationen dazu im Abschnitt „Virtuelle Private Netzwerke (VPN)“ im *Fehlerbehebungshandbuch zu NSX* nach.
30701	Kritisch	Nicht verfügbar	Der NSX Edge DHCP-Relay-Dienst auf Edge {EdgeID} ist deaktiviert, da kein externer DHCP-Server angegeben wurde (NSX Edge DHCP Relay service on edge {EdgeID} is disabled because there is no external DHCP server provided). Überprüfen Sie die Server-IP oder das referenzierte Gruppierungsobjekt (Please check server IP or referenced grouping object).	Der NSX Edge-DHCP-Relay-Dienst wurde deaktiviert. Mögliche Ursachen: (1) Der DHCP-Relay-Vorgang wird nicht ausgeführt. (2) Es ist kein externer DHCP-Server vorhanden. Dies kann daran liegen, dass das Gruppenobjekt, auf das vom Relay verwiesen wird, gelöscht wurde. Aktion: Informationen dazu finden Sie unter „Konfigurieren des DHCP-Relays“ im *Administratorhandbuch für NSX*.

Ereigniscode	Schweregrad des Ereignisses	Alarmcode	Ereignismeldung	Beschreibung
30206	Kritisch	Nicht verfügbar	Split Brain-Syndrom wurde für NSX Edge {EdgeID} mit HighAvailability behoben (Resolved Split Brain for NSX Edge {EdgeID} with HighAvailability).	Die beiden NSX Edge-HA-Appliances können miteinander kommunizieren und verfügen über einen neu verhandelten aktiven und Standby-Status. Aktion: Informationen dazu finden Sie unter „Troubleshooting NSX Edge High Availability (HA) issues“ (Fehlerbehebung für NSX Edge-Hochverfügbarkeitsprobleme): (http://kb.vmware.com/kb/2126560).
30207	Kritisch	Nicht verfügbar	Es wurde versucht, eine Split-Brain-Auflösung für NSX Edge {EdgeID} mit der Anzahl {value} durchzuführen (Attempted Split Brain resolution for NSX Edge {EdgeID} with count {value}).	Die beiden NSX Edge-HA-Appliances versuchen, neu zu verhandeln und sich von einer Split-Brain-Bedingung wiederherzustellen. **Hinweis** Der von diesem Ereignis gemeldete Wiederherstellungsmechansimus tritt nur in NSX Edge-Versionen vor 6.2.3 auf. Aktion: Informationen dazu finden Sie unter „Troubleshooting NSX Edge High Availability (HA) issues“ (Fehlerbehebung für NSX Edge-Hochverfügbarkeitsprobleme): (http://kb.vmware.com/kb/2126560).

Fabric-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für die Fabric-Systemereignisse.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250000	Zur Information	Nein	Alter Betriebsstatus der Bereitstellungseinheit war {#}, neuer Betriebsstatus ist {#} und alter Fortschrittsstatus war {#}, neuer Fortschrittsstatus ist {#} (Deployment unit old operational status was {#} , new operational status is {#} and old progress state was {#}, new progress state is {#}). Überprüfen Sie die Alarmzeichenfolge, um die Hauptursache zu ermitteln (Check alarm string for root cause).	Rein informatives Ereignis.
250001	Zur Information	Nein	Eine Bereitstellungseinheit wurde erstellt (A deployment unit has been created).	Rein informatives Ereignis.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250002	Zur Information	Nein	Eine Bereitstellungseinheit in NSX wurde aktualisiert. Fabric-Dienste werden auf dem Cluster aktualisiert (A deployment unit in NSX has been updated. Fabric services will be updated on the cluster).	Rein informatives Ereignis.
250003	Zur Information	Nein	Eine Bereitstellungseinheit wurde in NSX gelöscht (A deployment unit has been deleted from NSX).	Rein informatives Ereignis.
250004	Hoch	Ja	Der Dienst {#} konnte auf dem Host {#} nicht bereitgestellt werden, da der Datenspeicher {#} nicht mit dem Host verbunden ist. Stellen sie sicher, dass eine Verbindung besteht, oder geben Sie einen anderen Datenspeicher an (Please verify that it is connected, or provide a different datastore).	Der Datenspeicher, auf dem virtuelle Sicherheitsmaschinen für den Host gespeichert werden, konnte nicht konfiguriert werden. Aktion: Stellen Sie sicher, dass der Host den Datenspeicher erreichen kann.
250005	Hoch	Ja	Die Installation der Bereitstellungseinheit ist fehlgeschlagen. Stellen Sie sicher, dass auf alle OVF-/VIB-URLs zugegriffen werden kann und dass die erforderlichen Netzwerkports geöffnet sind (Installation of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open).	ESXi-Host konnte während einer NSX-Dienstinstallation auf dem Host nicht auf VIBs/OVFs von NSX zugreifen. In der vCenter-Systemereignistabelle wird Folgendes angezeigt: 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'. Aktion: Weitere Informationen finden Sie im Dokument *Fehlerbehebungshandbuch zu NSX*.
250006	Zur Information	Nein	Der Fabric-Agent für Fabric-Netzwerkdienste wurde erfolgreich auf einem Host installiert (The fabric agent for network fabric services installed successfully on a host).	Rein informatives Ereignis.
250007	Zur Information	Nein	Der Fabric-Agent wurde erfolgreich von einem Host entfernt (The fabric agent was removed successfully from a host).	Rein informatives Ereignis.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250008	Hoch	Ja	`Der Speicherort der OVF-/VIB-Dateien hat sich geändert. Der Dienst muss neu bereitgestellt werden (Location of OVF / VIB files has changed. Service must be redeployed).`	NSX-VIBs und -OVFs sind über eine URL verfügbar, die sich je nach NSX-Version unterscheidet. Um die korrekten VIBs zu ermitteln, müssen Sie zu *https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties* wechseln. Wenn sich die NSX Manager-IP-Adresse ändert, müssen Sie das NSX-OVF oder -VIB eventuell erneut bereitstellen. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
250009	Hoch	Ja	`Die Aktualisierung der Bereitstellungseinheit ist fehlgeschlagen. Stellen Sie sicher, dass auf alle OVF-/VIB-URLs zugegriffen werden kann und dass die erforderlichen Netzwerkports geöffnet sind (Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open).`	EAM konnte während eines Host-Upgrades nicht auf VIBs/OVFs von NSX zugreifen. In der vCenter-Systemereignistabelle wird Folgendes angezeigt: `Event Message:'Upgrade of deployment unit failed. Stellen Sie sicher, dass auf alle OVF-/VIB-URLs zugegriffen werden kann und dass die erforderlichen Netzwerkports geöffnet sind. ‚Modul: Sicherheits-Fabric‘ (Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.', Module:'Security Fabric').` Aktion: Weitere Informationen finden Sie im Dokument *Fehlerbehebungshandbuch zu NSX*.
250012	Hoch	Ja	`Die folgenden Dienste müssen erfolgreich installiert werden, damit der Dienst {#} funktionieren kann: {#} (Following service(s) need to be installed successfully for Service {#} to function: {#}).`	Der Dienst, der installiert wird, ist von einem anderen Dienst abhängig, der noch nicht installiert wurde. Aktion: Stellen Sie den erforderlichen Dienst auf dem Cluster bereit.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250014	Hoch	Ja	`Fehler beim Benachrichtigen der Sicherheitslösung vor dem Upgrade. Die Lösung ist nicht erreichbar oder antwortet nicht. Stellen Sie sicher, dass auf die Lösungs-URLs von NSX aus zugegriffen werden kann. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird erneut bereitgestellt (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).`	Es ist ein Fehler beim Benachrichtigen der Sicherheitslösung vor dem Upgrade aufgetreten. Die Lösung ist eventuell nicht erreichbar oder antwortet nicht. Aktion: Stellen Sie sicher, dass von NSX auf die Lösungs-URLs zugegriffen werden kann. Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben. Der Dienst wird erneut bereitgestellt.
250015	Hoch	Ja	`Keine Rückmeldung von der Sicherheitslösung wegen der Upgrade-Benachrichtigung selbst nach einer Zeitüberschreitung. Stellen Sie sicher, dass auf die Lösungs-URLs von NSX aus zugegriffen werden kann und dass NSX von der Lösung erreichbar ist. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird erneut bereitgestellt (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).`	Es ist auch nach einer Zeitüberschreitung kein Callback von der Sicherheitslösung für die Upgrade-Benachrichtigung erfolgt. Aktion: Stellen Sie sicher, dass von NSX auf die Lösung-URLs zugegriffen werden kann und dass NSX von der Lösung erreicht werden kann. Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250016	Hoch	Nein	Die Deinstallation des Dienstes ist nicht möglich. Stellen Sie sicher, dass auf die Lösungs-URLs von NSX aus zugegriffen werden kann und dass NSX von der Lösung erreichbar ist. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird entfernt (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).	Fehler beim Deinstallieren des Dienstes. Aktion: Stellen Sie sicher, dass von NSX auf die Lösung-URLs zugegriffen werden kann und dass NSX von der Lösung erreicht werden kann. Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
250017	Hoch	Ja	Fehler beim Benachrichtigen der Sicherheitslösung vor der Deinstallation. Führen Sie zur erneuten Benachrichtigung eine Behebung durch oder löschen Sie zur Deinstallation ohne Benachrichtigung. Stellen Sie sicher, dass auf die Lösungs-URLs von NSX aus zugegriffen werden kann und dass NSX von der Lösung erreichbar ist. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird entfernt (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).	Fehler bei der Benachrichtigung der Sicherheitslösung vor der Deinstallation. Beheben Sie das Problem durch erneute Benachrichtigung oder löschen Sie zur Deinstallation ohne Benachrichtigung. Aktion: Stellen Sie sicher, dass von NSX auf die Lösung-URLs zugegriffen werden kann und dass NSX von der Lösung erreicht werden kann. Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250018	Hoch	Ja	`Fehler beim Benachrichtigen der Sicherheitslösung vor der Deinstallation. Führen Sie zur erneuten Benachrichtigung eine Behebung durch oder löschen Sie zur Deinstallation ohne Benachrichtigung. Stellen Sie sicher, dass auf die Lösungs-URLs von NSX aus zugegriffen werden kann und dass NSX von der Lösung erreichbar ist. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird entfernt (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).`	Fehler bei der Benachrichtigung der Sicherheitslösung vor der Deinstallation. Beheben Sie das Problem durch erneute Benachrichtigung oder löschen Sie zur Deinstallation ohne Benachrichtigung. Aktion: Stellen Sie sicher, dass von NSX auf die Lösung-URLs zugegriffen werden kann und dass NSX von der Lösung erreicht werden kann. Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
250019	Hoch	Ja	`Der Server wurde neu gestartet, während die Sicherheitslösung über die Deinstallation benachrichtigt wurde. Stellen Sie sicher, dass auf die Lösungs-URLs von NSX aus zugegriffen werden kann und dass NSX von der Lösung erreichbar ist. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird deinstalliert (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).`	Der Server wurde während der Benachrichtigung der Sicherheitslösung über die Deinstallation neu gestartet. Aktion: Stellen Sie sicher, dass von NSX auf die Lösungs-URLs zugegriffen werden kann. Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben. Der Dienst wird deinstalliert.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250020	Hoch	Ja	`Der Server wurde neu gestartet, während die Sicherheitslösung über das Upgrade benachrichtigt wurde. Stellen Sie sicher, dass auf die Lösungs-URLs von NSX aus zugegriffen werden kann und dass NSX von der Lösung erreichbar ist. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird erneut bereitgestellt (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).`	Der Server wurde während der Benachrichtigung der Sicherheitslösung über das Upgrade neu gestartet. Aktion: Stellen Sie sicher, dass von NSX auf die Lösungs-URLs zugegriffen werden kann. Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben. Der Dienst wird erneut bereitgestellt.
250021	Kritisch	Nein	`Der NSX Manager basiert auf dem EAM-Dienst in vCenter zur Bereitstellung/Überwachung von NSX-Vibs auf ESX (NSX Manager relies on the EAM service in vCenter for deploying/monitoring NSX vibs on ESX). Die Verbindung zu diesem EAM-Dienst wurde getrennt (The connection to this EAM service has gone down). Eventuell wurde der EAM-Dienst neu gestartet/angehalten oder es ist ein Problem im EAM-Dienst aufgetreten (This could be due to EAM service or vCenter restart/stop or an issue in the EAM service). Überprüfen Sie, ob VC aktiviert ist und der EAM-Dienst in VC ausgeführt wird (Verify that vCenter is up, and the EAM service in vCenter is running). Außerdem können Sie im EAM-Mob prüfen, ob EAM wie erwartet funktioniert (Further, we can look at EAM mob to verify that EAM is functioning as expected).`	NSX Manager basiert auf dem EAM-Dienst in vCenter zur Bereitstellung/Überwachung von NSX-VIBs auf ESX. Die Verbindung zu diesem EAM-Dienst wurde getrennt. Eventuell wurde der EAM-Dienst oder vCenter neu gestartet/angehalten, oder es ist ein Problem im EAM-Dienst aufgetreten. Aktion: Stellen Sie sicher, dass vCenter verfügbar ist und dass der EAM-Dienst in vCenter ausgeführt wird. Stellen Sie sicher, dass der Zugriff auf die EAM-MOB-URL **`http://{vCenter_IP}/eam/mob/`** möglich ist und EAM wie erwartet funktioniert. Weitere Informationen finden Sie unter „Infrastrukturvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250022	Kritisch	Nein	`Der NSX Manager basiert auf dem EAM-Dienst in VC zur Bereitstellung/Überwachung von NSX-Vibs auf ESX. Die Verbindung zu diesem EAM-Dienst wurde getrennt. Eventuell wurde der EAM-Dienst neu gestartet/angehalten oder es ist ein Problem im EAM-Dienst aufgetreten. Überprüfen Sie, ob VC aktiviert ist und der EAM-Dienst in VC ausgeführt wird. Außerdem können Sie im EAM-Mob prüfen, ob EAM wie erwartet funktioniert. (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 basiert auf dem EAM-Dienst in vCenter zur Bereitstellung/Überwachung von NSX-VIBs auf ESX. Die Verbindung zu diesem EAM-Dienst wurde getrennt. Eventuell wurde der EAM-Dienst oder vCenter neu gestartet/angehalten, oder es ist ein Problem im EAM-Dienst aufgetreten. Aktion: Stellen Sie sicher, dass vCenter verfügbar ist und dass der EAM-Dienst in vCenter ausgeführt wird. Stellen Sie sicher, dass der Zugriff auf die EAM-MOB-URL **`http://{vCenter_IP}/eam/mob/`** möglich ist und EAM wie erwartet funktioniert. Weitere Informationen finden Sie unter „Infrastrukturvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.
250023	Hoch	Ja	`Die Bereinigung vor der Deinstallation ist fehlgeschlagen. Beheben Sie mit „API auflösen“ den Alarm. Der Dienst wird entfernt (Pre Uninstall cleanup failed. Use resolve API to resolve the Alarm. Service will be removed).`	Interne Bereinigungsaufgaben vor der Deinstallation konnten nicht abgeschlossen werden. Aktion: Verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben. Der Dienst wird entfernt.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
250024	Hoch	Ja	Die unterstützende EAM-Agency für diese Bereitstellung wurde nicht gefunden. Möglicherweise ist die Initialisierung der VC-Dienste noch nicht abgeschlossen. Versuchen Sie, den Alarm aufzulösen, um zu überprüfen, ob die Agency existiert (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). Falls Sie die Agency manuell gelöscht haben, löschen Sie den Bereitstellungseintrag aus NSX (In case you have deleted the agency manually, please delete the deployment unit entry from NSX).	EAM stellt VIBs auf ESXi-Hosts bereit. Auf jedem mit NSX vorbereiteten Cluster wird eine EAM-Agency installiert. Wenn diese Agency nicht gefunden wird, werden eventuell die vCenter Server-Dienste initialisiert oder die Agency wurde unabsichtlich manuell gelöscht.
250025	Hoch	Ja	Dieses Ereignis wird bei einem Versuch generiert, NSX-Vibs mit EAM auf einem zustandslosen Host zu aktualisieren oder zu deinstallieren. Alle zustandslosen Hosts sollten mit der Funktion zur automatischen Bereitstellung vorbereitet werden. Reparieren Sie die Konfiguration mithilfe der Funktion für die automatische Bereitstellung und beheben Sie den Alarm mit der Auflösungs-API (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).	Dieses Ereignis wird beim Versuch generiert, NSX-VIBS auf dem zustandslosen Host unter Verwendung von EAM zu aktualisieren oder zu deinstallieren. Alle zustandslosen Hosts sollten mit der Funktion zur automatischen Bereitstellung vorbereitet werden. Aktion: Korrigieren Sie die Konfiguration unter Verwendung der Funktion zur automatischen Bereitstellung und verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.

Bereitstellungs-Plug-In-Systemereignisse

Die Tabelle erläutert die Systemereignismeldungen für das Bereitstellungs-Plug-In mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
280000	Hoch	Ja	`Alarm für 'IP-Pool ausgeschöpft' des Bereitstellungs-Plugins (Deployment Plugin IP pool exhausted alarm).`	Eine IP-Adresse konnte einer NSX-Dienst-VM nicht zugewiesen werden, da der Quell-IP-Pool ausgeschöpft ist. Aktion: Fügen Sie dem Pool IP-Adressen zu.
280001	Hoch	Ja	`Generischer Alarm des Bereitstellungs-Plugins (Deployment Plugin generic alarm).`	Jeder Dienst wie Guest Introspection verfügt über einen Satz an Plug-Ins zur Konfiguration des Dienstes auf jedem Host. Jedes Problem im Plug-In-Code wird als generischer Alarm gemeldet. Der Dienst wird nur dann grün angezeigt, wenn alle Plug-Ins für den Dienst erfolgreich sind. Dieses Ereignis erfasst eine Teilmenge möglicher Ausnahmen. Aktion: Lösen Sie den Alarm mithilfe der `resolve`-API auf. Der Dienst wird bereitgestellt.
280004	Hoch	Ja	`Alarm für generische Ausnahme des Bereitstellungs-Plugins (Deployment Plugin generic exception alarm).`	Jeder Dienst wie Guest Introspection verfügt über einen Satz an Plug-Ins zur Konfiguration des Dienstes auf jedem Host. Jedes Problem im Plug-In-Code wird als generische Ausnahme des Alarms gemeldet. Der Dienst wird nur dann grün angezeigt, wenn alle Plug-Ins für den Dienst erfolgreich sind. Dieses Ereignis erfasst alle möglichen Ausnahmen. Aktion: Lösen Sie den Alarm mithilfe der `resolve`-API auf. Der Dienst wird bereitgestellt.
280005	Hoch	Ja	`VM muss neu gestartet werden, damit einige Änderungen vorgenommen werden bzw. wirksam werden (VM needs to be rebooted for some changes to be made/take effect).`	VM muss neu gestartet werden, damit einige Änderungen vorgenommen bzw. wirksam werden. Aktion: Lösen Sie den Alarm mithilfe der `resolve`-API auf. Dadurch wird die VM neu gestartet.

Messaging-Systemereignisse

Die Tabelle erläutert Messaging-Systemereignismeldungen mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereignis-niscode	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
390001	Hoch	Ja	`Host-Nachrichten-konfiguration fehl-geschlagen (Host messaging configu-ration failed).`	Der NSX-Nachrichtenbus wird nach der Hostvorbereitung eingerichtet, wenn der ESX Agent Manager (EAM) NSX darüber informiert hat, dass NSX-VIBs erfolgreich auf einem ESXi-Host installiert wurden. Dieses Ereignis weist darauf hin, dass die Einrichtung des Nachrichtenbusses auf dem Host nicht durchgeführt werden konnte. Ab der Version NSX 6.2.3 wird dies durch ein rotes Fehlersymbol neben dem betreffenden Host auf der Registerkarte **Installation > Hostvorbereitung** angezeigt. Aktion: Schritte zur Fehlerbehebung finden Sie im Dokument *Fehlerbehebungshandbuch zu NSX*.
390002	Hoch	Ja	`Neukonfiguration der Host-Nachrich-tenverbindung fehl-geschlagen (Host messaging connecti-on reconfiguration failed).`	Wenn NSX feststellt, dass sich die RMQ-Broker-Details geändert haben, versucht NSX, die neuesten RMQ-Broker-Informationen an den Server zu senden. Wenn diese Informationen nicht von NSX gesendet werden können, wird dieser Alarm ausgelöst. Aktion: Schritte zur Fehlerbehebung finden Sie im Dokument *Fehlerbehebungshandbuch zu NSX*.
390003	Hoch	Ja	`Die Konfiguration der Host-Nachrich-tenverbindung ist fehlgeschlagen und Benachrichtigungen wurden übersprungen (Host messaging configuration fai-led and notificati-ons were skipped).`	NSX wird versuchen, erneut einen Messaging-Kanal einzurichten, wenn ein vorbereiteter Host erneut mit dem vCenter Server verbunden wird. Dieses Ereignis weist darauf hin, dass die Einrichtung nicht durchgeführt werden konnte und dass andere NSX-Module, die von dem Messaging-Kanal abhängig sind, nicht benachrichtigt werden. Aktion: Schritte zur Fehlerbehebung finden Sie im Dokument *Fehlerbehebungshandbuch zu NSX*.
391002	Kritisch	Nein	`Nachrichteninfra-struktur funktio-niert nicht auf Host (Messaging infrastructure down on host).`	Es fehlen zwei oder mehr Taktsignalmeldungen zwischen NSX Manager und einem NSX-Host. Aktion: Schritte zur Fehlerbehebung finden Sie im Dokument *Fehlerbehebungshandbuch zu NSX*.
321100	Kritisch	Nein	`Das Messaging-Konto {account #} wird deaktiviert (Disab-ling messaging ac-count {account #}). Das Kennwort ist abgelaufen (Pass-word has expired).`	Für einen ESXi-Host, eine NSX Edge-VM oder eine USVM, der/die als Nachrichtenbus fungiert, wurde das RabbitMQ-Kennwort nicht innerhalb des vorgesehenen Zeitraums von zwei Stunden nach der anfänglichen Bereitstellung oder Hostvorbereitung geändert. Aktion: Prüfen Sie ein mögliches Kommunikationsproblem zwischen NSX Managerund dem Nachrichtenbusclient. Stellen Sie sicher, dass der Client ausgeführt wird. Vor der Durchführung einer erneuten Synchronisierung oder einer erneuten Bereitstellung erfassen Sie die entsprechenden Protokolle. Schritte zur Fehlerbehebung finden Sie im Dokument *Fehlerbehebungshandbuch zu NSX*.

Service Composer-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für Service Composer mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
300000	Kritisch	Ja	`Richtlinie {#} wird als Folge des ausdrücklichen Löschvorgangs ihrer abhängigen SecurityGroup gelöscht (Policy {#} is deleted as a result of explicit deletion of its dependent SecurityGroup).`	Eine Dienstrichtlinie wurde gelöscht, als eine abhängige Sicherheitsgruppe gelöscht wurde. Aktion: Erstellen Sie die Sicherheitsrichtlinie erneut.
300001	Hoch	Ja	`Richtlinie ist nicht synchronisiert (Policy is out of sync).`	Service Composer hat einen Fehler bei dem Versuch festgestellt, Regeln für diese Dienstrichtlinie zu erzwingen. Aktion: Überprüfen Sie die Fehlermeldung auf Hinweise, welche Regeln in der Richtlinie geändert werden müssen. Beheben Sie den Alarm mit Service Composer oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
300002	Hoch	Ja	`Die Firewallregeln dieser Richtlinie sind nicht synchronisiert. Es werden keine Änderungen dieser Richtlinie, die Firewalls betreffen, übertragen, bis dieser Alarm aufgelöst ist (Firewall rules on this Policy are out of sync. No Firewall related changes from this policy will be pushed, until this alarm is resolved).`	Dieser Fehler wurde durch ein Problem mit der Firewallkonfiguration ausgelöst. Aktion: Überprüfen Sie die Fehlermeldung auf Details der Richtlinie (und eventuell der Regeln), die den Fehler ausgelöst haben. Stellen Sie sicher, dass der Alarm mithilfe von Service Composer oder der `resolve`-API aufgelöst wird, um die Richtlinie zu synchronisieren. Informationen dazu finden Sie auch unter „Troubleshooting issues with Service Composer in NSX 6.x“ (Fehlerbehebung von Problemen mit Service Composer in NSX 6.x, http://kb.vmware.com/kb/2132612).

Ereignis-niscode	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
300003	Hoch	Ja	`Die Netzwerk-Introspektionsregeln dieser Richtlinie sind nicht synchronisiert. Es werden keine Änderungen dieser Richtlinie, die Netzwerk-Introspektionen betreffen, übertragen, bis dieser Alarm aufgelöst ist (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).`	Dieser Fehler wurde durch ein Problem mit der Konfiguration der Netzwerk-Introspektion ausgelöst. Aktion: Überprüfen Sie die Fehlermeldung auf Details der Richtlinie (und eventuell der Regeln), die den Fehler ausgelöst haben. Stellen Sie sicher, dass der Alarm mithilfe von Service Composer oder mit dem Parameter `action=resolve` in der API `systemalarms` behoben wird, um die Richtlinie zu synchronisieren. Informationen dazu finden Sie auch unter „Troubleshooting issues with Service Composer in NSX 6.x“ (Fehlerbehebung von Problemen mit Service Composer in NSX 6.x, http://kb.vmware.com/kb/2132612). Beheben Sie den Alarm mit Service Composer oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
300004	Hoch	Ja	`Die Gast-Introspektionsregeln dieser Richtlinie sind nicht synchronisiert. Es werden keine Änderungen dieser Richtlinie, die Gast-Introspektionen betreffen, übertragen, bis dieser Alarm aufgelöst ist (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).`	Dieser Fehler wurde durch ein Problem mit der Konfiguration der Guest Introspection ausgelöst. Aktion: Überprüfen Sie die Fehlermeldung auf Details der Richtlinie (und eventuell der Regeln), die den Fehler ausgelöst haben. Stellen Sie sicher, dass der Alarm mithilfe von Service Composer oder mit dem Parameter `action=resolve` in der API `systemalarms` behoben wird, um die Richtlinie zu synchronisieren. Informationen dazu finden Sie auch unter „Troubleshooting issues with Service Composer in NSX 6.x“ (Fehlerbehebung von Problemen mit Service Composer in NSX 6.x, http://kb.vmware.com/kb/2132612).

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
300005	Hoch	Ja	`Service Composer ist nicht synchronisiert. Es werden keine Änderungen von Service Composer zur Firewall/Netzwerk-Introspektion übertragen (Service Composer is out of sync. No changes from Service Composer will be pushed to Firewall/Network Introspection).`	Service Composer hat einen Fehler bei der Synchronisierung einer Richtlinie festgestellt. Es werden keine Änderungen an die Firewall oder an Dienste der Netzwerk-Introspektion gesendet. Aktion: Überprüfen Sie die Fehlermeldung, um festzustellen, welche Richtlinien und/oder Firewallabschnitte bearbeitet werden müssen. Lösen Sie den Alarm mit Service Composer oder der `resolve`-API auf.
300006	Hoch	Ja	`Service Composer ist aufgrund eines Synchronisierungsfehlers beim Neustarten nicht synchronisiert (Service Composer is out of sync due to failure on sync on reboot operation).`	Service Composer hat einen Fehler bei der Synchronisierung einer Richtlinie beim Neustart festgestellt. Es werden keine Änderungen an die Firewall oder an Dienste der Netzwerk-Introspektion gesendet. Aktion: Überprüfen Sie die Fehlermeldung, um festzustellen, welche Richtlinien und/oder Firewallabschnitte bearbeitet werden müssen. Beheben Sie den Alarm mit Service Composer oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
300007	Hoch	Ja	`Service Composer ist nicht synchronisiert. Es werden keine Änderungen von Service Composer zur Firewall/Netzwerk-Introspektion übertragen (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 hat einen Synchronisierungsfehler bei der Wiederherstellung von Firewallregelsätzen auf eine frühere Version festgestellt. Es werden keine Änderungen an die Firewall oder an Dienste der Netzwerk-Introspektion gesendet. Aktion: Beheben Sie den Alarm mit Service Composer oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.

Ereignis-niscode	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
300008	Hoch	Ja	`Fehler beim Löschen des Abschnitts gemäß der Richtlinie (Failure while deleting section corresponding to the Policy).`	Service Composer hat einen Fehler beim Löschen des Firewallregelabschnitts für die Richtlinie festgestellt. Diese Problem tritt auf, wenn der Manager für einen Drittanbieterdienst mit NSX Service Insertion nicht erreicht werden kann. Aktion: Prüfen Sie ein mögliches Konnektivitätsproblem mit dem Service Manager des Drittanbieters. Beheben Sie den Alarm mit Service Composer oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
300009	Hoch	Ja	`Fehler beim Neuordnen des Abschnitts aufgrund der Vorrangänderung (Failure while reordering section to reflect precedence change).`	Service Composer hat einen Fehler bei der Synchronisierung einer Richtlinie beim Neustart festgestellt. Es werden keine Änderungen an die Firewall oder an Dienste der Netzwerk-Introspektion gesendet. Aktion: Überprüfen Sie die Fehlermeldung, um festzustellen, welche Richtlinien und/oder Firewallabschnitte bearbeitet werden müssen. Beheben Sie den Alarm mit Service Composer oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.
300010	Hoch	Ja	`Fehler beim Initialisieren der Einstellung für das automatische Speichern von Entwürfen (Failure while initializing auto save drafts setting).`	Service Composer hat einen Fehler bei der Initialisierung von Einstellungen für das automatische Speichern von Entwürfen festgestellt. Aktion: Überprüfen Sie die Fehlermeldung, um festzustellen, welche Richtlinien und/oder Firewallabschnitte bearbeitet werden müssen. Beheben Sie den Alarm mit Service Composer oder verwenden Sie den Parameter `action=resolve` in der API `systemalarms`, um den Alarm zu beheben.

GI-SVM-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für universelle Guest Introspection-Dienst-VMs (GI-SVMs) mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereig-niscode	Schwere-grad des Ereignisses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
295002	Haupt			NSX Manager empfängt keine Signale von der Guest Introspection-USVM. Aktion: Rufen Sie die Protokolle zum technischen Support für NSX Manager und USVM ab und öffnen Sie eine Support-Anfrage.
295003	Zur Information			NSX Manager empfängt keine Signale von der USVM. Aktion: Wiederherstellungsereignis nach der Meldung von Ereignis 295002.
295010	Zur Information			Die Verbindung zwischen der USVM und dem Guest Introspection-Hostmodul wird hergestellt. Aktion: Rein informatives Ereignis Keine Aktion erforderlich.

SVM-Vorgangs-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für Dienst-VMs (Service VMs, SVMs) mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereigniscode	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
280002	Hoch	Ja	Einige der Ereignisse für diesen Agenten wurden von NSX verpasst. Mögliche Gründe sind ein Neustart oder vorübergehender Verlust der Verbindung mit vCenter Server. Warnung: Durch Beheben des Alarms wird die VM gelöscht und ein weiterer Alarm über eine fehlende Agenten-VM ausgegeben. Durch seine Behebung wird die VM erneut bereitgestellt (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).	Bei einer bereitgestellten Dienst-VM ist ein interner Fehler aufgetreten. Aktion: Durch Auflösung des Alarms wird die VM gelöscht und ein zweiter Alarm zum Löschvorgang gemeldet. Die Auflösung des zweiten Alarms installiert die VM erneut. Wenn die VM nicht erneut bereitgestellt werden kann, wird der ursprüngliche Alarm erneut gemeldet. Wenn der Alarm erneut ausgelöst wird, erfassen Sie die SVM-Protokolle mithilfe der Prozedur im KB-Artikel http://kb.vmware.com/kb/2144624 und kontaktieren Sie den technischen VMware-Support.
280003	Hoch	Ja	Einige der Ereignisse für diesen Agenten wurden von NSX verpasst. Mögliche Gründe sind ein Neustart oder vorübergehender Verlust der Verbindung mit vCenter Server. Warnung: Durch Beheben des Alarms wird die VM neu gestartet (Some of the events for this agent were missed by NSX. Probably reason could be re-	Eine bereitgestellte Dienst-VM wurde erneut gestartet. Aktion: Durch Auflösung des Alarms wird die VM erneut gestartet. Wenn die VM nicht erneut gestartet werden kann, tritt der Alarm erneut auf. Erfassen Sie die SVM-Protokolle mithilfe der Prozedur im KB-Artikel http://kb.vmware.com/kb/2144624 und kontaktieren Sie den technischen VMware-Support.

Ereignis-code	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
			`boot or temporary connectivity loss with vCenter Server.Warning: Resolving the alarm will restart the VM).`	
280006	Hoch	Ja	`Das Markieren des Agenten als verfügbar ist fehlgeschlagen (Failed to mark agent as available).`	Bei der Kennzeichnung der ESX-Agent-VM als verfügbar ist ein interner Fehler aufgetreten. Aktion: Lösen Sie den Alarm mit dem Parameter `action=resolve` in der `systemalarms` -API auf. Wenn der Alarm nicht aufgelöst werden kann, erfassen Sie die SVM-Protokolle mithilfe der Prozedur im KB-Artikel http://kb.vmware.com/kb/2144624 und kontaktieren Sie den technischen VMware-Support.

Replikation – Globale Synchronisierungs-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für die Replikation mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereignis-code	Schweregrad des Ereignisses	Alarm ausgelöst	Ereignismeldung	Beschreibung
310001	Kritisch	Nein	`Vollständige Synchronisierung fehlgeschlagen für Objekttyp {#} auf NSX Manager {#} (Full sync failed for object type {#} on NSX Manager {#}).`	Auf einem sekundären NSX Manager konnte keine komplette Synchronisierung globaler Objekte durchgeführt werden. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und wenden Sie sich an den technischen Support von VMware.
310003	Kritisch	Nein	`Globaler Synchronisierungsvorgang für die Entität {#} auf NSX Manager {#} fehlgeschlagen (Universal sync operation failed for the entity {#} on NSX Manager {#}).`	Die Synchronisierung eines globalen Objekts mit dem sekundären NSX Manager in einer Cross-vCenter-Umgebung konnte nicht durchgeführt werden. Aktion: Erfassen Sie die Tech-Support-Protokolle für NSX Manager und wenden Sie sich an den technischen Support von VMware.

NSX Management-Systemereignisse

Die Tabelle erläutert Systemereignismeldungen für NSX Management mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereignis-code	Schwere-grad des Ereig-nisses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
320001	Kritisch	Nein	`Die NSX Manager-IP wurde einer anderen Maschine mit der MAC-Adresse zugewie-sen (The NSX Manager IP has been assigned to another machine with the MAC Add-ress).`	Die NSX Manager Management-IP-Adresse wurde einer VM in demselben Netzwerk zugewiesen. Vor der Version 6.2.3 wurde eine doppelte NSX Manager-IP-Adresse nicht erkannt oder nicht verhindert. Diese kann zu einem Ausfall des Daten-pfads führen. In Version 6.2.3 und höher wird dieses Ereignis ausgelöst, wenn eine doppelte Adresse ermittelt wird. Aktion: Beheben Sie das Problem der doppelten Adresse.

Mit dem logischen Netzwerk in Zusammenhang stehende Systemereignisse

Die Tabelle erläutert Systemereignismeldungen, die mit dem logischen Netzwerk in Zusammenhang ste-hen.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
814	Kritisch	Nein	`Der logische Switch {#} ist nicht mehr ord-nungsgemäß konfigu-riert, da einige der stützenden verteilten virtuellen Portgruppen geändert und/oder ent-fernt wurden (Logical Switch {#} is no longer properly configured since some of the ba-cking distributed vir-tual port groups were modified and/or remo-ved).`	Eine oder mehrere DVS-Portgruppen, die einen logischen NSX-Switch stützen, wurden geändert oder gelöscht, oder die Änderung des Steuerungskomponenten-Modus für den logischen Switch konnte nicht durchgeführt werden. Aktion: Wenn das Ereignis durch das Löschen oder Ändern einer Portgruppe ausgelöst wurde, wird eine Fehlermeldung auf der Seite der logischen Switches im vSphere Web Client angezeigt. Klicken Sie auf den Fehler, um die fehlenden DVS-Portgruppen zu erstellen. Wenn das Ereignis durch das Scheitern der Änderung des Steuerungskomponenten-Modus ausgelöst wurde, führen Sie die Aktualisierung erneut durch. Informationen dazu finden Sie unter „Aktualisieren von Transportzonen und logischen Switches“ im *Upgrade-Handbuch für NSX*.
1900	Kritisch	Nein	`Die VXLAN-Initialisie-rung auf dem Host ist fehlgeschlagen (VXLAN initialization failed on the host).`	Die VXLAN-Initialisierung konnte nicht durchgeführt werden, da die VMkernel-NICs für die erforderliche Anzahl an VTEPs nicht konfiguriert werden konnten. NSX bereitet den vom Benutzer für VXLAN ausgewählten DVS vor und erstellt eine DV-Portguppe für die VTEP-VMkernel-NICs. Die Gruppierung, die Load-Balancing-Methode, die MTU und die VLAN-ID werden bei der VXLAN-Konfiguration ausgewählt. Die Gruppierungs- und Load-Balancing-Methoden müssen mit der Konfiguration des für das VXLAN ausgewählten DVS übereinstimmen. Aktion: Überprüfen Sie die Datei `vmkernel.log`. Weitere Informationen finden Sie auch im Abschnitt „Infrastrukturvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.
1901	Kritisch	Nein	`Die VXLAN-Portinitiali-sierung auf dem Host ist fehlgeschlagen (VXLAN port initializa-tion failed on the host).`	VXLAN konnte auf dem zugeordneten DV-Port nicht konfiguriert werden, und der Port wurde getrennt. NSX bereitet den vom Benutzer für VXLAN ausgewählten DVS vor und erstellt eine DV-Portguppe für jeden konfigurierten logischen Switch. Aktion: Überprüfen Sie die Datei `vmkernel.log`. Weitere Informationen finden Sie auch im Abschnitt „Infrastrukturvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.
1902	Kritisch	Nein	`Die VXLAN-Instanz ist auf dem Host nicht vor-handen (VXLAN instance does not exist on the host).`	Die VXLAN-Konfiguration wurde für einen DV-Port empfangen, obwohl der DVS auf dem ESXI-Host noch nicht für VXLAN aktiviert ist. Aktion: Überprüfen Sie die Datei `vmkernel.log`. Weitere Informationen finden Sie auch im Abschnitt „Infrastrukturvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
1903	Kritisch	Nein	`Der logische Switch {#} funktioniert nicht ordnungsgemäß, da die stützende IP-Schnittstelle nicht einer bestimmten Multicast-Gruppe beitreten konnte (Logical Switch {#} can't work properly since the backing IP interface couldn't join specific multicast group).`	Die VTEP-Schnittstelle konnte nicht der angegebenen Multicast-Gruppe beitreten. Solange dieses Problem nicht behoben ist, wird dadurch der Datenverkehr zu bestimmten Hosts beeinträchtigt. NSX verwendet einen regelmäßigen Wiederholungsmechanismus (alle fünf Sekunden) für den Beitritt zur Multicast-Gruppe. Aktion: Überprüfen Sie die Datei `vmkernel.log`. Weitere Informationen finden Sie auch im Abschnitt „Infrastrukturvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.
1905	Kritisch	Nein	`Transportzone darf nicht verwendet werden, da die stützende IP-Schnittstelle nicht die korrekte IP-Adresse abrufen kann (Transport Zone may not be used since the backing IP interface can't acquire correct IP Address).`	Der VTEP-VMkernel-NIC konnte keine gültige IP-Adresse zugewiesen werden. Der gesamte VXLAN-Datenverkehr über die VMkernel-NIC wird verworfen. Aktion: Machen Sie DHCP auf Transport-VLANs für VXLAN verfügbar, wenn Sie DHCP für die IP-Zuweisung für VMKNics verwenden. Weitere Informationen finden Sie unter „NSX host preparation fails with error: Insufficient IP addresses in IP pool“ (NSX-Hostvorbereitung schlägt fehl mit der Fehlermeldung: Unzureichende IP-Adressen im IP-Pool, http://kb.vmware.com/kb/2137025).
1906	Kritisch	Nein	`VXLAN-Overlay-Klasse fehlt auf DVS (VXLAN overlay class is missing on DVS).`	NSX-VIBs wurden nicht installiert, wenn der DVS für VXLAN konfiguriert wurde. Alle VXLAN-Schnittstellen können keine Verbindungen mit dem DVS herstellen. Aktion: Informationen dazu finden Sie unter „Network connectivity issues after upgrade in NSX/VCNS environment“ (Probleme der Netzwerkkonnektivität nach dem Upgrade in der NSX/VCNS-Umgebung, http://kb.vmware.com/kb/2107951).
1920	Kritisch	Nein	`Der VXLAN-Controller {#} wurde entfernt, da keine Verbindung hergestellt werden kann. Überprüfen Sie die IP-Konfiguration des Controllers und führen Sie eine erneute Bereitstellung durch (VXLAN Controller {#} has been removed due to the connection can't be built, please check controller IP configuration and deploy again).`	Der Controller konnte nicht bereitgestellt werden. Aktion: Prüfen Sie, ob die zugewiesene IP-Adresse erreicht werden kann. Darüber hinaus finden Sie im Abschnitt „NSX-Controller“ im *Fehlerbehebungshandbuch zu NSX* weitere Informationen.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
1930	Kritisch	Nein	`Der Controller {#} kann die Verbindung zum Kno-ten {#} (aktiv = {#}) nicht herstellen (The controller {#} cannot establish the connecti-on to the node {#}(ac-tive={#})). Aktueller Verbindungsstatus = {#} (Current connection status = {#}).`	Zwei Controller-Knoten wurden getrennt, sodass die Kom-munikation von Controller zu Controller beeinträchtigt ist. Aktion: Informationen dazu finden Sie im Abschnitt „NSX-Controller“ im *Fehlerbehebungshandbuch zu NSX*.
1935	Kritisch	Nein	`Informationen zum Host {#} konnten nicht an Controller gesendet werden, da alle Con-troller inaktiv sind (Host {#} information could not be sent to controllers as all con-trollers are inactive). Nachdem Controller ak-tiv werden, ist mögli-cherweise eine Control-ler-Synchronisierung erforderlich (Control-ler synchronization may be needed once control-lers become active).`	Die Hostzertifikatinformationen konnten nicht zum NSX Con-troller-Cluster gesendet werden. Der Kommunikationskanal zwischen dem Host und dem Controller-Cluster weist even-tuell ein unerwartetes Verhalten auf. Aktion: Stellen Sie sicher, dass sich der NSX Controller-Cluster vor der Vorbereitung eines ESXi-Hosts in einem nor-malen Status befindet. Beheben Sie dieses Problem mit der `controller sync`-API.
1937	Kritisch	Nein	`VXLAN vmknic {#} [Port-gruppe = {#}] fehlt auf dem Host {#} oder wurde dort gelöscht (VXLAN vmknic {#} [PortGroup = {#}] is missing or de-leted from host {#}).`	Die VXLAN-VMkernel-NIC fehlt oder wurde auf dem Host gelöscht. Dies beeinträchtigt den Datenverkehr zum und vom Host. Aktion: Um das Problem zu beheben, klicken Sie auf der Registerkarte **Installation > Vorbereitung des logischen Netzwerks > VXLAN-Transport** auf **Auflösen**.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
1939	Kritisch	Nein	`VXLAN vmknic {#} [Port-gruppe = {#}] wurde eventuell von Host {#} gelöscht oder bei der Host-vCenter-Verbindung sind Probleme aufgetre-ten (VXLAN vmknic {#} [PortGroup = {#}] may have been deleted from the host {#} or the host-vCenter connection may have issues).`	NSX Manager hat festgestellt, dass eine VXLAN-VMkernel-NIC auf Virtual Center fehlt. Dies kann durch Probleme bei der Kommunikation vom vCenter Server zum Host verur-sacht worden sein. Darüber hinaus kann NSX Manager bei einem Neustart von vCenter Server oder eines Hosts für ei-nen kurzen Zeitraum die VXLAN-VMkernel-NIC nicht ermit-teln. Es wird dann dieses Ereignis angezeigt. Wenn der Neustart von vCenter Server und des Hosts abgeschlossen ist, überprüft NSX Manager die VXLAN-VMkernel-NICs er-neut und löscht das Ereignis, wenn kein Problem besteht. Aktion: Wenn das Problem nicht vorübergehender Natur ist, beheben Sie es durch Klicken auf die Schaltfläche **Auflösen** auf der Registerkarte **Installation > Vorbereitung des logi-schen Netzwerks > VXLAN-Transport**.
1941	Kritisch	Nein	`Host-Verbindungsstatus geändert: Ereignis-Code: {#}, Host: {#} (ID: {#}), NSX Manager - Firewall-Agent: {#}, NSX Manager - Steuer-ebenen-Agent: {#}, Steuerebenen-Agent - Controller: {#} (Host Connection Status Chan-ged: Event Code: {#}, Host: {#} (ID: {#}), NSX Manager - Firewall Agent: {#}, NSX Manager - Control Plane Agent: {#}, Control Plane Agent - Controllers: {#}).`	NSX Manager hat für eine der folgenden Verbindungen den Status „down“ ermittelt: NSX Manager zum Hostagenten der Firewall, NSX Manager zum Hostagenten der Steuerungs-komponente oder Hostagent der Steuerungskomponente zu NSX Controller. Aktion: Wenn die Verbindung NSX Manager zum Hostagen-ten der Firewall ausgefallen ist, überprüfen Sie das NSX Manager- und Firewallagentenprotokoll (*/var/log/vsfwd.log*) oder senden Sie den REST-API-Aufruf POST `https://NSX-Manager-IP-Add-ress/api/2.0/nwfabric/configure?action=synchron-ize`, um die Verbindung neu zu synchronisieren. Wenn die Verbindung von NSX Manager zum Agenten der Steuer-ungskomponente getrennt ist, überprüfen Sie das Protokoll für NSX Manager und den Agenten der Steuerungskompo-nente (*/var/log/netcpa.log*). Wenn die Verbindung vom Agenten der Steuerungskomponente zum NSX Controller unterbrochen ist, wechseln Sie zu **Networking & Security > Installation** und überprüfen Sie den Status der Hostverbin-dung.
1942	Kritisch	Nein	`Die stützende Portgrup-pe [MOID = {#}] von Lo-gicalSwitch {#} ist als fehlend markiert (The backing portgroup [moid = {#}] of LogicalSwitch {#} is marked as mis-sing).`	NSX Manager hat festgestellt, dass für einen logischen NSX-Switch eine stützende DV-Portguppe in Virtual Center fehlt. Aktion: Klicken Sie auf die Schaltfläche **Auflösen** auf der Registerkarte **Installation > Vorbereitung des logischen Netzwerks > VXLAN-Transport** oder verwenden Sie die REST API (POST `https://<vsm-ip>/api/2.0/vdn/vir-tualwires/<vw-id>/backing?action=remediate`), um die Portgruppe neu zu erstellen.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
1945	Kritisch	Nein	`Das Gerät {#} auf Controller {#} hat die Datenträgerlatenz-Warnung aktiviert (The device {#} on controller {#} has the disk latency alert on).`	NSX Manager hat für NSX Controller eine hohe Festplattenlatenz ermittelt. Aktion: Informationen dazu finden Sie im Abschnitt „NSX Controller“ im *Fehlerbehebungshandbuch zu NSX*.
1946	Zur Information	Nein	`Alle Datenträgerlatenz-Warnungen auf Controller {0} sind deaktiviert (All disk latency alerts on controller {0} are off).`	NSX Manager erkennt hohe Festplattenlatenz auf einem Controller nicht mehr. Aktion: Rein informatives Ereignis Es ist keine Aktion erforderlich.
1947	Kritisch	Nein	`Controller-VM ist in vCenter ausgeschaltet (Controller Virtual Machine is powered off on vCenter).`	NSX Manager hat ermittelt, dass eine NSX Controller-VM in Virtual Center ausgeschaltet wurde. Der Status des Controller-Clusters lautet eventuell „Getrennt“, wodurch jeder Vorgang beeinträchtigt ist, für den ein Arbeits-Cluster erforderlich ist. Aktion: Klicken Sie auf die Schaltfläche **Auflösen** für den Controller auf der Registerkarte **Installation > Verwaltung** oder rufen Sie die API POST `https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate` auf, um die Controller-VM einzuschalten.
1948	Kritisch	Nein	`Controller-VM ist von vCenter gelöscht (Controller Virtual Machine is deleted from vCenter).`	NSX Manager hat ermittelt, dass eine NSX Controller-VM aus Virtual Center gelöscht wurde. Der Status des Controller-Clusters lautet eventuell „Getrennt“, wodurch jeder Vorgang beeinträchtigt ist, für den ein Arbeits-Cluster erforderlich ist. Aktion: Klicken Sie auf die Schaltfläche **Auflösen** für den Controller auf der Registerkarte **Installation > Verwaltung** oder rufen Sie die API POST `https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate` auf, um den Status des Controllers in der Datenbank NSX Manager zu entfernen.
1952	Kritisch	Nein	`Die VXLAN-Portgruppe [moid = dvportgroup-xx] und zugewiesene DVS verfügen über unterschiedliche Gruppierungsrichtlinien (The VXLAN portgroup [moid = dvportgroup-xx] and associated DVS have different teaming policies).`	NSX Manager hat ermittelt, dass sich die Teaming-Richtlinie einer VXLAN-Portgruppe von der Teaming-Richtlinie des zugehörigen DVS unterscheidet. Dies kann zu einem unvorhersehbaren Verhalten führen. Aktion: Konfigurieren Sie die VXLAN-Portgruppe oder den DVS neu, damit diese über gleiche Teaming-Richtlinie verfügen.

Systemereignisse der identitätsbasierten Firewall

Die Tabelle erläutert Systemereignismeldungen für die identitätsbasierte Firewall mit dem Schweregrad „Haupt“, „Kritisch“ oder „Hoch“.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
395000	Kritisch	Nein	`SecurityLog bei Domänencontrol-ler-Eventlog-Server ist voll (SecurityLog on Domain Control-ler Eventlog Server is Full).`	Das Sicherheitsprotokoll auf dem Active Directory-Ereignisproto-kollserver ist voll. Wenn die identitätsbasierte Firewall für die Ver-wendung des Protokoll-Scraping konfiguriert ist, funktioniert sie in diesem Fall nicht mehr. Aktion: Wenden Sie sich an ihren Active Directory-Serveradminist-rator, damit dieser die Größe des Sicherheitsprotokolls erhöht, oder archivieren Sie das Sicherheitsprotokoll.

Systemereignisse bei der Hostvorbereitung

Die Tabelle erläutert alle Systemereignismeldungen im Zusammenhang mit der Hostvorbereitung.

Hinweis Mehrere ESX Agent Manager-Ereignisse sind einem einzigen Ereignis auf NSX zugeordnet.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Zur Infor-mation	Ja	Ein VIB-Modul wurde auf den Host {hostID} hochgeladen. Es wird aber erst dann voll-ständig installiert, wenn der Host {hostID} in den Wartungsmodus versetzt worden ist (A VIB module has been uploaded to the host {hostID}, but will not be fully installed un-til the host {hostID} has been put in main-tenance mode).	ESX Agent Manager versetzt den Host in den Wartungs-modus. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Kritisch	Ja	Eine Agenten-VM soll auf einem Host bereit-gestellt werden, aber diese Bereitstellung ist nicht möglich, da der vSphere ESX Agent Manager nicht auf das OVF-Paket für den Agenten zugreifen kann (An agent virtual ma-chine is expected to be deployed on a host, but the agent virtual machine cannot be de-ployed because the vSphere ESX Agent Ma-nager is unable to ac-cess the OVF package for the agent). Dies geschieht in der Re-gel, weil der Webser-ver für die Bereit-stellung des OVF-Pa-kets nicht verfügbar ist (This typically happens because the Web server providing the OVF package is down). Der Webserver gehört oft zu der Lö-sung, die die Agency	ESX Agent Manager stellt den Agenten erneut bereit. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
			erstellt (The Web ser-ver is often internal to the solution that created the Agency).	
270000	Kritisch	Ja	Ein Agenten-VIB-Modul soll auf einem Host bereitgestellt werden, aber die Bereitstel-lung des VIM-Moduls ist nicht möglich, da der vSphere ESX Agent Manager nicht auf das VIB-Paket für den Agenten zugreifen kann (An agent VIB module is expected to be de-ployed 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). Dies geschieht in der Re-gel, weil der Webser-ver für die Bereit-stellung des VIB-Pa-kets nicht verfügbar ist (This typically happens because the Web server providing the VIB package is down). Der Webserver gehört oft zu der Lö-sung, die die Agency erstellt (The Web ser-ver is often internal to the solution that created the Agency).	ESX Agent Manager installiert das VIB-Modul erneut. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Eine Agenten-VM soll auf einem Host bereitgestellt werden, aber die Bereitstellung des Agenten ist nicht möglich, da er nicht kompatibel mit dem Host {hostID} ist (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 stellt den Agenten erneut bereit. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf. Allerdings bleibt das Problem wahrscheinlich bestehen, bis Sie den Host oder die Lösung aktualisieren, damit der Agent mit dem Host kompatibel ist.
270000	Hoch	Ja	`Eine Agenten-VM soll eingeschaltet werden, aber es sind keine freien IP-Adressen im VM-IP-Adressenpool des Agenten vorhanden (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).`	Aktion: Um das Problem zu beheben, machen Sie einige IP-Adressen frei oder fügen Sie weitere IP-Adressen zum IP-Pool hinzu. Lösen Sie anschließend den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Eine Agenten-VM soll auf einem Host bereitgestellt werden, aber diese Bereitstellung ist nicht möglich, da der Host {hostID} nicht über genügend freie CPU- oder Arbeitsspeicherressourcen verfügt (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 stellt die Agenten-VM erneut bereit. Allerdings bleibt das Problem wahrscheinlich bestehen, bis genügend CPU- und Speicherressourcen zur Verfügung gestellt werden. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Eine Agenten-VM soll auf einem Host bereit-gestellt werden, aber diese Bereitstellung ist nicht möglich, da der Agentendatenspei-cher des Hosts nicht über genügend freien Speicherplatz verfügt (An agent virtual ma-chine 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 stellt die Agenten-VM erneut bereit. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf. Allerdings bleibt das Problem wahrscheinlich bestehen, bis entweder: Sie Speicherplatz im Agenten-VM-Datenspeicher des Hosts freimachen oder Sie einen neuen Agenten-VM-Datenspeicher mit genügend freiem Speicherplatz konfigurieren.
270000	Hoch	Ja	`Eine Agenten-VM soll eingeschaltet werden, aber die Agenten-VM wird ausgeschaltet, weil im VM-Netzwerk des Agenten keine IP-Adressen definiert sind (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).`	Aktion: Erstellen Sie einen IP-Pool im VM-Netzwerk des Agenten virtuelle Maschine und lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systema-larms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	Eine Agenten-VM soll auf einem Host bereit-gestellt werden, aber die Bereitstellung des Agenten ist nicht mög-lich, da der Agenten-datenspeicher auf dem Host {hostID} nicht konfiguriert wurde (An agent virtual machine is expected to be de-ployed on a host, but the agent cannot be deployed because the agent datastore has not been configured on the host {hostID}).	Aktion: Sie müssen den Datenspeicher der Agenten-VM auf dem Host konfigurieren.
270000	Hoch	Ja	Eine Agenten-VM soll auf einem Host bereit-gestellt werden, aber die Bereitstellung des Agenten ist nicht mög-lich, da das Agenten-netzwerk auf dem Host nicht konfiguriert wurde (An agent virtu-al machine is expected to be deployed on a host, but the agent cannot be deployed be-cause the agent net-work has not been con-figured on the host).	Aktion: Sie müssen das Netzwerk der Agenten-VM auf dem Host konfigurieren.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	Eine Agenten-VM soll auf einem Host bereit-gestellt werden, aber die Bereitstellung des Agenten ist nicht mög-lich, da das Agenten-netzwerk auf dem Host nicht konfiguriert wurde (An agent virtu-al machine is expected to be deployed on a host, but the agent cannot be deployed be-cause the agent net-work has not been con-figured on the host). Der Host muss zu einem der in customAgentVm-Network aufgeführten Netzwerke hinzugefügt werden (The host needs to be added to one of the networks listed in customAgentVmNetwork).	Aktion: Sie müssen eines der *customAgentVmNetwork*-Netzwerke zum Host hinzufügen.

Ereignis-niscode	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Eine Agenten-VM soll auf einem Host bereit-gestellt werden, aber die Bereitstellung des Agenten ist nicht mög-lich, da der Agenten-datenspeicher auf dem Host nicht konfigu-riert wurde (An agent virtual machine is ex-pected to be deployed on a host, but the agent cannot be de-ployed because the agent datastore has not been configured on the host). Der Host muss zu einem der in customAgentVmDatastore aufgeführten Daten-speicher hinzugefügt werden (The host needs to be added to one of the datastores listed in customAgentVmDatas-tor).`	Sie müssen einen der Datenspeicher mit dem Namen *customAgentVmDatastore* zum Host hinzufügen.
270000	Hoch	Ja	`Die Lösung, die die Agency erstellt hat, ist nicht mehr bei vCenter Server regist-riert (The solution that created the agen-cy is no longer regis-tered with the vCenter server).`	ESX Agent Manager entfernt die Agency. Aktion: Klicken Sie auf der Registerkarte **Hostvorberei-tung (Host Preparation)** auf die Option **Auflösen (Re-solve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Auf einem Host ist ein dvFilter-Switch vorhanden, aber keine Agenten auf dem Host hängen vom dvFilter ab (A dvFilter switch exists on a host but no agents on the host depend on dvFilter). Dies geschieht in der Regel, wenn eine Hostverbindung bei der Änderung einer Agency-Konfiguration getrennt wird (This typically happens if a host is disconnected when an agency configuration changed).`	ESX Agent Manager entfernt den *dvFilterSwitch*. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Eine Agenten-VM soll auf einem Host bereitgestellt werden, aber diese Bereitstellung ist fehlgeschlagen, da die Bereitstellung des OVF-Pakets fehlgeschlagen ist (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). Die Bereitstellung kann wahrscheinlich erst erfolgreich ausgeführt werden, wenn die Lösung, die das OVF-Paket bereitstellt, aktualisiert oder gepatcht wurde und ein gültiges OVF-Paket für die Agenten-VM bereitstellen kann (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 versucht, die OVF-Bereitstellung erneut durchzuführen. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Eine Agenten-VM soll eingeschaltet werden, aber eine OVF-Eigenschaft fehlt oder weist einen ungültigen Wert auf (An agent virtual machine needs to be powered on, but an OVF property is either missing or has an invalid value).`	Aktion: Aktualisieren Sie die OVF-Umgebung in der Agentenkonfiguration, die für die Bereitstellung der Agenten-VM genutzt wird.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Im vCenter-Bestand wurde eine Agenten-VM gefunden, die zu keiner Agency in dieser vSphere ESX Agent Manager-Serverinstanz gehört (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 schaltet die Agenten-VM aus (sofern sie eingeschaltet ist) und löscht sie. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Ein VIB-Modul setzt voraus, dass sich der Host im Wartungsmodus befindet, aber der vSphere ESX Agent Manager kann den Host nicht in den Wartungsmodus versetzen (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). Dies kann geschehen, wenn auf dem Host, der nicht verschoben werden kann, virtuelle Maschinen vorhanden sind, die angehalten werden müssen, damit der Host in den Wartungsmodus versetzt werden kann (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 versucht, den Host in den Wartungsmodus zu versetzen. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf. Allerdings bleibt das Problem wahrscheinlich bestehen, bis Sie virtuelle Maschinen ausschalten oder verschieben, um den Host in den Wartungsmodus zu versetzen.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Kritisch	Ja	`Ein VIB-Modul soll auf einem Host installiert werden, aber diese Installation ist fehlgeschlagen, weil das VIB-Paket ein ungültiges Format aufweist (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). Die Installation kann wahrscheinlich erst erfolgreich ausgeführt werden, wenn die Lösung, die das Paket bereitstellt, aktualisiert oder gepatcht wurde und ein gültiges VIB-Paket bereitstellen kann (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 versucht, die VIB-Bereitstellung erneut durchzuführen. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Ein VIB-Modul soll auf einem Host installiert werden, aber es wurde nicht installiert (A VIB module is expected to be installed on a host, but it has not been installed). Normalerweise gibt ein spezifischeres Problem (eine Unterklasse dieses Problems) den speziellen Grund an, warum die Installation des VIB-Moduls fehlgeschlagen ist (Typically, a more specific issue (a subclass of this issue) indicates the particular reason why the VIB module installation failed).`	ESX Agent Manager versucht, die VIB-Bereitstellung erneut durchzuführen. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Zur Information	Ja	`Ein VIB-Modul wurde auf den Host hochgeladen, aber es wird erst aktiviert, wenn der Host neu gestartet wird (A VIB module has been uploaded to the host, but will not be activated until the host is rebooted).`	ESX Agent Manager versetzt den Host in den Wartungsmodus und startet ihn neu. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Ein VIB-Modul konnte nicht installiert werden, da die automatische Installation von vSphere ESX Agent Manager auf dem Host nicht zulässig ist (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).`	Aktion: Wechseln Sie zum vSphere Update Manager und installieren Sie die erforderlichen Bulletins auf dem Host oder fügen Sie die Bulletins dem Image-Profil des Hosts hinzu. Weitere Informationen finden Sie in der vSphere-Dokumentation.

Ereignis-niscode	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Ein VIB-Modul konnte nicht deinstalliert werden, da die automatische Deinstallation von vSphere ESX Agent Manager auf dem Host nicht zulässig ist (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).`	Aktion: Wechseln Sie zum vSphere Update Manager und deinstallieren Sie die erforderlichen Bulletins auf dem Host oder fügen Sie die Bulletins dem Image-Profil des Hosts hinzu. Weitere Informationen finden Sie in der vSphere-Dokumentation.
270000	Hoch	Ja	`Eine Agenten-VM ist beschädigt (An agent virtual machine is corrupt).`	ESX Agent Manager löscht die Agenten-VM und stellt sie erneut bereit. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf. So beheben Sie das Problem manuell: Beheben Sie das Problem mit der fehlenden Datei und schalten Sie die Agenten-VM ein.

Ereignis-niscode	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Eine Agenten-VM soll von einem Host entfernt werden, aber sie wurde nicht entfernt (An agent virtual machine is expected to be removed from a host, but the agent virtual machine has not been removed). Normalerweise gibt ein spezifischeres Problem (eine Unterklasse dieses Problems) den speziellen Grund an, warum vSphere ESX Agent Manager die Agenten-VM nicht entfernen konnte (z. B. weil der Host im Wartungsmodus, ausgeschaltet oder im Standby-Modus ist) (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 stellt den Agenten erneut bereit. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Eine Agenten-VM ist eine VM-Vorlage (An agent virtual machine is a virtual machine template).`	ESX Agent Manager wandelt die Agenten-VM-Vorlage in eine virtuelle Maschine um. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-niscode	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	Eine Agenten-VM soll auf einem Host bereitgestellt werden, aber sie wurde nicht bereitgestellt (An agent virtual machine is expected to be deployed on a host, but the agent virtual machine has not been deployed). Normalerweise gibt ein spezifischeres Problem (eine Unterklasse dieses Problems) den speziellen Grund an, warum vSphere ESX Agent Manager den Agenten nicht bereitstellen konnte (z. B. weil der Zugriff auf das OVF-Paket für den Agenten nicht möglich war oder eine Hostkonfiguration fehlt) (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). Dieses Problem kann auch auftreten, wenn die Agenten-VM explizit vom Host gelöscht wird (This issue can also happen if the agent virtual machine is explicitly deleted from the host).	ESX Agent Manager stellt die Agenten-VM erneut bereit. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Eine Agenten-VM soll eingeschaltet werden, aber sie wurde ausgeschaltet (An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off).`	ESX Agent Manager schaltet die Agenten-VM ein. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Eine Agenten-VM soll ausgeschaltet werden, aber sie wurde eingeschaltet (An agent virtual machine is expected to be powered off, but the agent virtual machine is powered off).`	ESX Agent Manager schaltet die Agenten-VM aus. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Eine Agenten-VM soll eingeschaltet werden, aber sie wurde angehalten (An agent virtual machine is expected to be powered on, but the agent virtual machine is suspended).`	ESX Agent Manager schaltet die Agenten-VM ein. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`Eine Agenten-VM soll in einem bestimmten Ordner der Agenten-VM gespeichert sein, befindet sich aber in einem anderen Ordner (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 verschiebt die Agenten-VM zurück in den designierten Agentenordner. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.

Ereignis-code	Schwere-grad des Ereignis-ses	Alarm aus-gelöst	Ereignismeldung	Beschreibung
270000	Hoch	Ja	`Eine Agenten-VM soll in einem bestimmten Ressourcenpool der Agenten-VM gespeichert sein, befindet sich aber in einem anderen Ressourcenpool (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 verschiebt die Agenten-VM zurück in den designierten Ressourcenpool. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.
270000	Hoch	Ja	`EAM-Alarm empfangen (EAM alarm received).`	ESX Agent Manager hat ein NSX-Installations- oder Upgrade-Problem mit den NSX-VIBs oder den Dienst-VMs erkannt. Aktion: Klicken Sie auf der Registerkarte **Hostvorbereitung (Host Preparation)** auf die Option **Auflösen (Resolve)** oder lösen Sie den Alarm mithilfe des Parameters `action=resolve` in der `systemalarms`-API auf.