

VMware NSX for vSphere 6.2.7 Release Notes

Document updated 21 August 2017

VMware NSX for vSphere 6.2.7 | Released 20 April 2017 | Build 5343628

What's in the Release Notes

The release notes cover the following topics:

- [What's New](#)
- [Minimum Recommended Versions, System Requirements, and Installation](#)
- [Deprecated and Discontinued Functionality](#)
- [Upgrade Notes](#)
- [Known Issues](#)
- [Resolved Issues](#)
- [Document Revision History](#)

What's New

See what's new and changed in NSX [6.2.7](#), [6.2.6](#), [6.2.5](#), [6.2.4](#), [6.2.3](#), [6.2.2](#), [6.2.1](#) and [6.2.0](#).

See [Important information about NSX 6.2.3](#).

New in 6.2.7

Updated Hardware VTEP solution: The Hardware VTEP solution that was shipped as part of NSX 6.2.3 had a restriction that prevented the use of Hardware Switch Controller (HSC) as a front end for multiple hardware VTEP switches (more than one). With NSX 6.2.7, this is no longer a restriction. You can now enable an HSC-like device to front-end multiple switches that integrate with NSX.

Critical bug fixes: This release includes a number of critical bug fixes and security updates. For details, see the [Resolved Issues](#) section.

New in 6.2.6

The 6.2.6 release primarily contains bug fixes for the multi-cipher issue and the OpenSSL upgrade. In 6.2.6, NSX Edge OpenSSL package is updated to 1.0.2j. For details, see the [Resolved Issues](#) section.

New in 6.2.5

The 6.2.5 release is a bugfix release that addresses a loss of network connectivity after performing certain vMotion operations in installations where some hosts ran a newer version of NSX, and other hosts ran an older version of NSX. See the [Resolved Issues](#) section.

New in 6.2.4

The 6.2.4 release includes the following new features. It also delivers a number of bug fixes that have been documented in the [Resolved Issues](#) section.

- **Changes in firewall status API (GET /api/4.0/firewall/globalroot-0/status)**
 - **Firewall Status API has been enhanced to include status of object updates used in firewall rules:** The firewall status API displays a generation number (generationNumber) for each rule set, which can be used to verify whether a change in rule sets has propagated to a host. In 6.2.4, a generation number for objects (generationNumberObjects) has been added to the status API. This allows you to verify whether a change in objects consumed in firewall rules has propagated to a host. Note that the object generation number may change frequently and will always be equal to or greater than the ruleset generation number.

- **Hosts and clusters not participating in firewall are excluded from output:** Clusters (and hosts inside the clusters) are no longer included in the status output if distributed firewall is disabled at the cluster level, or if the cluster is not prepared (NSX VIBs are not installed). In earlier versions of NSX these clusters and hosts are included in the output. However, because they are not configured for firewall, after a firewall rule publish their status is *InProgress*.
- **Critical bug fixes identified in NSX 6.2.3:** NSX 6.2.4 delivers a security patch for CVE-2016-2079 which is a critical input validation vulnerability for sites that uses NSX SSL VPN. For customers who use SSL VPN, VMware strongly recommends a review of CVE-2016-2079 and an upgrade to NSX 6.2.4 or later.

New in 6.2.3

Important Information about NSX for vSphere 6.2.3: For customers who have installed NSX 6.2.3 or 6.2.3a, VMware recommends installing NSX 6.2.4 or later to address critical bug fixes.

The 6.2.3 release delivers a security patch to address CVE-2016-2079. CVE-2016-2079 is a critical input validation vulnerability affecting sites that use NSX SSL-VPN. The release also includes a number of bug fixes documented in the [Resolved Issues](#) section.

Changes introduced in NSX vSphere 6.2.3:

- **Logical Switching and Routing**
 - **NSX Hardware Layer 2 Gateway Integration:** expands physical connectivity options by integrating 3rd-party hardware gateway switches into the NSX logical network
 - **New VXLAN Port 4789 in NSX 6.2.3 and later:** Before version 6.2.3, the default VXLAN UDP port number was 8472. See the NSX Upgrade Guide for details.
- **Networking and Edge Services**
 - **New Edge DHCP Options:** DHCP Option 121 supports static route option, which is used for DHCP server to publish static routes to DHCP client; DHCP Options 66, 67, 150 supports DHCP options for PXE Boot; and DHCP Option 26 supports configuration of DHCP client network interface MTU by DHCP server.
 - **Increase in DHCP Pool, static binding limits:** The following are the new limit numbers for various form factors: Compact: 2048; Large: 4096; Quad large: 4096; and X-large: 8192.
 - **Edge Firewall adds SYN flood protection:** Avoid service disruptions by enabling SYN flood protection for transit traffic. Feature is disabled by default, use the NSX REST API to enable it.
 - **NSX Edge — On Demand Failover:** Enables users to initiate on-demand failover when needed.
 - **NSX Edge — Default memory for Quad Large NSX Edge:** Has increased from 1GB to 2GB.
 - **NSX Edge — Resource Reservation:** Reserves CPU/Memory for NSX Edge during creation. The CPU/Memory reserved is based on the Edge appliance form factor. You can change the default CPU and memory resource reservation percentages using this API. The CPU/Memory percentage can be set to 0 percent each to disable resource reservation.

PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>

```
<tuningConfiguration>
  <lockUpdatesOnEdge>false</lockUpdatesOnEdge>
  <aggregatePublishing>true</aggregatePublishing>
  <edgeVMHealthCheckIntervalInMin>0</edgeVMHealthCheckIntervalInMin>
  <healthCheckCommandTimeoutInMs>120000</healthCheckCommandTimeoutInMs>
  <maxParallelVixCallsForHealthCheck>25</maxParallelVixCallsForHealthCheck>
  <publishingTimeoutInMs>1200000</publishingTimeoutInMs>
  <edgeVCpuReservationPercentage>0</edgeVCpuReservationPercentage>
  <edgeMemoryReservationPercentage>0</edgeMemoryReservationPercentage>
  <megaHertzPerVCpu>1000</megaHertzPerVCpu>
</tuningConfiguration>
```

- **Change in NSX Edge Upgrade Behavior:** Replacement NSX Edge VMs are deployed before upgrade or redeploy. The host must have sufficient resources for four NSX Edge VMs during the upgrade or redeploy of an

Edge HA pair. Default value for TCP connection timeout is changed to 21600 seconds from the previous value of 3600 seconds.

- **Cross VC NSX — Universal Distributed Logical Router (DLR) Upgrade:** Auto upgrade of Universal DLR on secondary NSX Manager, once upgraded on primary NSX Manager.
- **Flexible SNAT / DNAT rule creation:** *vnicId* no longer needed as an input parameter; removed requirement that the DNAT address must be the address of an NSX Edge vNIC.
- **NSX Edge VM (ESG, DLR) now shows both Live Location and Desired Location.** NSX Manager and NSX APIs including GET `api/4.0/edges//appliances` now return `configuredResourcePool` and `configuredDataStore` in addition to current location.
- **Edge Firewall adds SYN flood protection:** Avoid service disruptions by enabling SYN flood protection for transit traffic. Feature is disabled by default, use the NSX REST API to enable it.
- **NSX Manager exposes the ESXi hostname** on which the 3rd-party VM Series firewall SVM is running to improve operational manageability in large-scale environments.
- **NAT rule** now can be applied to a vNIC interface and not only an IP address.
- **New configuration option to set the load balancer session aging time:** This release delivers a new application rule command to set the session aging timeout value for both the server and client. If the pool is shared among multiple virtual servers, the maximum value will be set for it.
- **NSX API now returns XML output by default when "Accept" header is not provided:** Beginning in NSX 6.2.3, if the "Accept:" header is not provided in a REST API call, then the default formatting of NSX API return values is XML. Previously the NSX API returned JSON-formatted output by default. To receive JSON-formatted output, the API user must explicitly set "application/json" in the "Accept:" header when calling the function.
- **New NSX API to change the autodraft setting for NSX distributed firewall:** Starting with NSX 6.2.3, the following PUT API can be used to change the autodraft setting for the NSX distributed firewall:
 - Get the existing GlobalConfiguration:
GET `https://NSX-Manager-IP-Address/api/4.0/firewall/config/globalconfiguration`
Note: GET will not show the `autoDraftDisabled` field.
 - Add `autoDraftDisabled` config property to the global configuration and execute a PUT API call:
PUT `https://NSX-Manager-IP-Address/api/4.0/firewall/config/globalconfiguration`
Request body:

```
<globalConfiguration>
  <layer3RuleOptimize>...</layer3RuleOptimize>
  <layer2RuleOptimize>...</layer2RuleOptimize>
  <tcpStrictOption>...</tcpStrictOption>
  <autoDraftDisabled>true</autoDraftDisabled>
</globalConfiguration>
```

- **Security Services**

- **Distributed Firewall — TFTP ALG:** Enables use cases such as network boot for VMs.
- **Firewall — Granular Rule Filtering:** Simplifies troubleshooting by providing granular rule filters in UI, based on Source, Destination, Action, Enabled/Disabled, Logging, Name, Comments, Rule ID, Tag, Service, Protocol.
- **Guest Introspection — Windows 10 support**
- **SSL VPN Client — Mac OS El Capitan support**
- **Service Composer — Performance Improvements:** Enables faster startup/reboot of NSX Manager by optimizing synchronization between security policy and firewall service, and disabling auto-save of firewall drafts by default.
- **Service Composer — Status Alarms:** Raises system alarm if security policy is out-of-sync, and takes specific actions based on alarm code to resolve issue.
- **Reduction in firewall heap memory usage:** Firewall usage of IP address sets has been optimized to reduce heap memory usage.

- **Operations and Troubleshooting**

- **NSX Dashboard:** Simplifies troubleshooting by providing visibility into the overall health of NSX components in one central view.
- **Traceflow Enhancement — Network Introspection Services:** Enhances ability to trace a packet from source to destination, by identifying whether packets were forwarded to 3rd-party network introspection services, and whether the packet comes back from the 3rd-party service VM or not.
- **SNMP Support:** Configure SNMP traps for events from NSX Manager, NSX Controller, and Edge.
- **Logging is now enabled by default** for SSL VPN and L2 VPN. The default log level is notice.
- **Logging for IPsec VPN is now enabled by default** Default log level is set to warning. If you wish to disable logging or change the log level, see the section, [Enable Logging for IPsec VPN](#) in the *NSX Administration Guide*.
- **Firewall rules UI** now displays configured IP protocols and TCP/UDP port numbers associated with services.
- **NSX Edge technical support logs** have been enhanced to report memory consumption per process.
- **Enhanced communication channel health status monitoring** with new event log messages reported when the channel health status changes for a server or a cluster.
- **Central CLI Enhancements**
 - **Central CLI for Host Health:** Shows host health status, with 30+ checks in one command (including network config, VXLAN config, resource utilization, etc.)
 - **Central CLI for Packet Capture:** Provides ability to capture packet on the host and transfer the capture file to user's remote server. This eliminates the need to open up hypervisor access to network administrators, when troubleshooting logical network issues.
- **Technical support bundle per host:** Gathers per-host logs and creates a bundle that can be saved and submitted to VMware technical support for assistance.

- **Licensing Enhancements**

- **Change in default license & evaluation key distribution:** default license upon install is "NSX for vShield Endpoint", which enables use of NSX for deploying and managing vShield Endpoint for anti-virus offload capability only. Evaluation license keys can be requested through VMware sales.
- **License usage reporting:** NSX license usage counts are displayed on NSX Manager's Summary UI and also retrievable via API. NSX license usage counts will no longer be reported through vCenter licensing service.

- **Load Balancer (LB) Enhancements**

- **Configurable session timeout for VIP configured without acceleration:** Ability to configure Load Balancing L7 engine (no acceleration) VIP timeout above 5 minutes using the Application Rule "timeout client 3600s".
- **Statistics enhancement on CLI:** Global statistics are now available through CLI. Specific VIP and pool statistics are also available.
- **LB with acceleration enhancement:** Load Balancing L4 engine (acceleration enabled) will now always honor the health checks UDP, TCP source IP hash, and invalidate persistent entry.
- **Log refinements:** Load Balancer log improvements.
- **Configurable SSL authentication:** Ability to configure SSL server authentication in case of VIP with end-to-end SSL.
- **Source IP Persistent table enhancement:** Even after a configuration change, the Source IP Persistence table remains available.
- **NSX Edge load balancer system control (sysctl) sysctl.net.ipv4.vs.expire_nodest_conn parameter added to NSX Manager whitelist:** The sysctl.net.ipv4.vs.expire_nodest_conn to change the persistent connection status.

- **Solution Interoperability**

- **Customer Experience Improvement Program:** NSX supports reporting system statistics via the VMware Customer Experience Improvement Program (CEIP). Participation is optional and is configured in the vSphere Web Client.
- **VMware vRealize Log Insight 3.3.2 for NSX** provides intelligent log analytics for NSX, with monitoring and troubleshooting capabilities and customizable dashboards for network virtualization, flow analysis and alerts. This version accepts NSX Standard/Advanced/Enterprise edition license keys issued for NSX 6.2.2+.
- **vShield Endpoint Management Support:** NSX supports management of vShield Endpoint anti-virus offload capabilities. Customers who purchased vSphere with vShield Endpoint (Essentials Plus and above) can download NSX from the vSphere download site. For more information, refer to [VMware knowledge base article 2110078](#) and [VMware knowledge base article 2105558](#).

New in 6.2.2

The 6.2.2 release delivers a security patch to address the glibc vulnerability and includes a number of bug fixes documented in the [Resolved Issues](#) section. This release includes the same critical bug fixes that were provided in all the 6.1.4-based and 6.1.5-based patches. For NSX 6.1.x users, this same set of patch fixes is available in the NSX 6.1.6 release.

The main features of this release are:

- **CVE-2015-7547 (glibc) security patch:** This patch addresses [CVE-2015-7547](#), also known as the glibc vulnerability.
- **Issue 1600484: Removal of constraint validations on DHCP domain name configurations** NSX 6.2.2 re-enables support for DHCP pools with ".local" domains. See [VMware knowledge base article 2144097](#).
- **Issue 1586149: DFW UI Enhancements for better user experience.** In the previous implementation, the table used to scroll the grid to the very first item of grid when a user made a change. In the fixed implementation, whenever a rule is added, the grid scrolls to the newly added rule. Now, when refreshing the grid data for any reason (e.g. after publishing or reverting changes), the vertical scroll position of the grid is maintained.
- **Issue 1592562: Behavior change when a new Edge Service is configured.** Prior to 6.2.2, when a new Edge Service is configured, it is **enabled** by default. In 6.2.2, this behavior has changed. Now, if the current license supports the feature, then by default the feature is **enabled**. Otherwise, the feature is **disabled**.

New in 6.2.1

The 6.2.1 release delivers a number of bug fixes that have been documented in the [Resolved Issues](#) section.

- **6.1.5 fixes:** Release includes the same critical fixes as NSX-vSphere 6.1.5 content.
- **Introduced new 'show control-cluster network ipsec status' command** that allows users to inspect the Internet Protocol Security (IPsec) state.
- **Connectivity status:** NSX Manager user interface now shows the connectivity status of the NSX Controller cluster.
- **Support for vRealize Orchestrator Plug-in for NSX 1.0.3:** With NSX 6.2.1 release, NSX-vRO plugin version 1.0.3 is introduced for use with vRealize Automation 7.0.0. This plugin includes fixes that improve performance when vRealize Automation 7.0 uses NSX for vSphere 6.2.1 as a networking and security end point.
- **Starting in 6.2.1, NSX Manager queries each Controller node in the cluster to get the connection information between that controller and the other controllers in the cluster.**
This is provided in the output of the NSX REST API ("GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller" command), which now shows the peer connection status among the controller nodes. If NSX Manager finds the connection between any two controller nodes is broken, a system event is generated to alert the user.
- **Service Composer now exposes an API that enables users to configure auto creation of Firewall drafts for Service Composer workflows.**
This setting can be turned on/off using REST API and the changes can be saved across reboot. When disabled, no draft is created in the Distributed Firewall (DFW) for policy workflows. This limits the number of drafts that are auto-created in the system and provides better performance.

New in 6.2.0

NSX vSphere 6.2.0 included the following new and changed features:

- **Cross vCenter Networking and Security**

- **NSX 6.2 with vSphere 6.0 supports Cross vCenter NSX** where logical switches (LS), distributed logical routers (DLR) and distributed firewalls (DFW) can be deployed across multiple vCenters, thereby enabling logical networking and security for applications with workloads (VMs) that span multiple vCenters or multiple physical locations.
- **Consistent firewall policy across multiple vCenters:** Firewall Rule Sections in NSX can now be marked as "Universal" whereby the rules defined in these sections get replicated across multiple NSX managers. This simplifies the workflows involving defining consistent firewall policy spanning multiple NSX installations
- **Cross vCenter vMotion with DFW:** Virtual Machines that have policies defined in the "Universal" sections can be moved across hosts that belong to different vCenters with consistent security policy enforcement.
- **Universal Security Groups:** Security Groups in NSX 6.2 that are based on IP Address, IP Set, MAC Address and MAC Set can now be used in Universal rules, whereby the groups and group memberships are synced up across multiple NSX managers. This improves the consistency in object group definitions across multiple NSX managers, and enables consistent policy enforcement.
- **Universal Logical Switch (ULS):** This new functionality introduced in NSX 6.2 as a part of Cross vCenter NSX allows creation of logical switches that can span multiple vCenters, allowing the network administrator to create a contiguous L2 domain for an application or tenant.
- **Universal Distributed Logical Router (UDLR):** This new functionality introduced in NSX 6.2 as a part of Cross vCenter NSX allows creation of distributed logical routers that can span multiple vCenters. The universal distributed logical routers enable routing across the universal logical switches described earlier. In addition, NSX UDLR is capable of localized north-south routing based on the physical location of the workloads.

- **Operations and Troubleshooting Enhancements**

- **New traceflow troubleshooting tool:** Traceflow is a troubleshooting tool that helps identify if the problem is in the virtual or physical network. It provides the ability to trace a packet from source to destination and helps observe how that packet passes through the various network functions in the virtual network.
- **Flow monitoring and IPFIX separation:** In NSX 6.1.x, NSX supported IPFIX reporting, but IPFIX reporting could be enabled only if flow reporting to NSX Manager was also enabled. Starting in NSX 6.2.0, these features are decoupled. In NSX 6.2.0 and later, you can enable IPFIX independent of flow monitoring on NSX Manager.
- **New CLI monitoring and troubleshooting commands in 6.2:** See [knowledge base article 2129062](#) for more information.
- **Central CLI:** Central CLI reduces troubleshooting time for distributed network functions. Commands are run from the command line on NSX Manager and retrieve information from controllers, hosts, and the NSX Manager. This allows you to quickly access and compare information from multiple sources. The central CLI provides information about logical switches, logical routers, distributed firewall and edges.
- **CLI ping command adds configurable packet size and do-not-fragment flag:** Starting in NSX 6.2.0, the NSX CLI 'ping' command offers options to specify the data packet size (not including the ICMP header) and to set the do-not-fragment flag. See the [NSX CLI Reference](#) for details.
- **Show health of the communication channels:** NSX 6.2.0 adds the ability to monitor communication channel health. The channel health status between NSX Manager and the firewall agent, between NSX Manager and the control plane agent, and between host and the NSX Controller can be seen from the NSX Manager UI. In addition, the host command channel offers greater fault tolerance.
- **Standalone Edge L2 VPN client CLI:** Prior to NSX 6.2, a standalone NSX Edge L2 VPN client could be configured only by 'deploy OVF' settings provided to the virtual center. Commands specific to standalone NSX Edge have been added to allow configuration using the command line interface.

- **Logical Networking and Routing**

- **L2 Bridging Interoperability with Distributed Logical Router:** With VMware NSX for vSphere 6.2, L2 bridging can now participate in distributed logical routing. The VXLAN network to which the bridge instance is connected, will be used to connect the routing instance and the bridge instance together.
- **Support of /31 prefixes on ESG and DLR interfaces per RFC 3021.**
- **Enhanced support of relayed DHCP request on the ESG DHCP server.**

- **Ability to preserve VLAN IDs/headers inside NSX virtual networks.**
 - **Exact Match for redistribution filters:** The redistribution filter has same matching algorithm as ACL, so exact prefix match by default (except if le or ge options are used).
 - **Support of administrative distance for static route.**
 - **Ability to enable, relax, or disable check per interface on Edge.**
 - **Display AS path in CLI command `show ip bgp`**
 - **HA interface exclusion** from redistribution into routing protocols on the DLR NSX Edge Appliance (Control VM).
 - **Distributed logical router (DLR) force-sync avoids data loss for east-west routing traffic across the DLR.** North-south routing and bridging may continue experience an interruption.
 - **View active Edge in HA pair:** In the NSX 6.2 web client, you can find out if an NSX Edge appliance is the active or backup in an HA pair.
 - **REST API supports reverse path filter (rp_filter) on Edge:** Using the system control REST API, rp_filter sysctl can be configured through UI, and is also exposed through REST API for vNIC interfaces and sub-interfaces. See the [NSX API documentation](#) for more information.
 - **Behavior of the IP prefix GE and IP prefix LE BGP route filters:** In NSX 6.2, the following enhancements have been made to BGP route filters:
 - LE / GE keywords not allowed: For the null route network address (defined as ANY or in CIDR format 0.0.0.0/0), less-than-or-equal-to (LE) and greater-than-or-equal-to (GE) keywords are no longer allowed. In previous releases, these keywords were allowed.
 - LE and GE values in the range 0-7 are now treated as valid. In previous releases, this range was not valid.
 - For a given route prefix, you can no longer specify a GE value that is greater than the specified LE value.
- **Networking and Edge Services**
 - **The management interface of the DLR has been renamed to HA interface.** This has been done to highlight the fact that the HA keepalives travel through this interface and that interruptions in traffic on this interface can result in a split-brain condition.
 - **Load balancer health monitoring improvements:** Delivers granular health monitoring that reports information on failures, keeps track of last health check and status change, and reports failure reasons.
 - **Support VIP and pool port range:** Enables load balancer support for applications that require a range of ports.
 - **Increased maximum number of virtual IP addresses (VIPs):** VIP support rises to 1024.
 - **Security Service Enhancements**
 - **New IP address discovery mechanisms for VMs:** Authoritative enforcement of security policies based on VM names or other vCenter-based attributes requires that NSX know the IP address of the VM. In NSX 6.1 and earlier, IP address discovery for each VM relied on the presence of VMware Tools (vmtools) on that VM or the manual authorization of the IP address for that VM. NSX 6.2 introduces the option to discover the VM's IP address by doing discovery from the hypervisor. These new discovery mechanisms enable NSX to enforce object based distributed firewall rules on VMs that do not have VMware Tools installed.
 - **Solution Interoperability**
 - **Support for vSphere 6.0 Platform Services Controller topologies:** NSX now supports external Platform Services Controllers (PSC), in addition to the already supported embedded PSC configurations.
 - **Support for vRealize Orchestrator Plug-in for NSX:** NSX 6.2 supports the [NSX-vRO plug-in](#) for integration of NSX with vRealize Orchestrator.

Minimum Recommended Versions, System Requirements and Installation

The table below lists minimum recommended versions of VMware software. This information is current as of the publication date of this document. For the latest recommendations, please refer to [VMware knowledge base article 2144295](#).

Product or Component	Minimum Recommended Version
NSX for vSphere	<p>VMware recommends NSX 6.2.6 for new deployments and at minimum running NSX 6.2.2 based on critical bug fixes identified as having a general impact in an NSX environment.</p> <p>For existing deployments running a release earlier than 6.2.6, please review the NSX Release Notes and/or contact your VMware technical support representative for more information on specific issues before planning an upgrade.</p> <p>VMware recommends a minimum of 5.5U3 and 6.0U3 in NSX environments. See also the VMware Product Interoperability Matrix for interoperability information.</p> <p>Notes:</p> <ul style="list-style-type: none"> • NSX 6.2.x is not compatible with vSphere 6.5. • vSphere 6.0U3 resolves the issue of duplicate VTEPs in ESXi hosts after rebooting vCenter server. See VMware Knowledge Base article 2144605 for more information. • For Distributed Service Insertion, ESXi versions 5.5 Patch 10 and ESXi 6.0U3 or later are recommended. See VMware Knowledge Base article 2149704 for more information.
Guest Introspection	<p>Guest Introspection-based features in NSX are compatible with specific VMware Tools (VMTools) versions. To enable the optional Thin Agent Network Introspection Driver component packaged with VMware Tools, you must upgrade to one of:</p> <ul style="list-style-type: none"> • VMware Tools 10.0.8 and later to resolve Slow VMs after upgrading VMware Tools in NSX / vCloud Networking and Security. See VMware knowledge base article 2144236 • VMware Tools 10.0.9 and later for Windows 10 support
vRealize Orchestrator	NSX-vRO plugin 1.0.3 or later
VMware Integrated Openstack (VIO)	VIO 2.5.1
vCloud Director (vCD)	<ul style="list-style-type: none"> • vCD 8.0 if migrating from vCNS to NSX • vCD 8.10.1 if already on NSX

System Requirements and Installation

For the complete list of NSX installation prerequisites, see the [System Requirements for NSX](#) section in the *NSX Installation Guide*.

For installation instructions, see the [NSX Installation Guide](#) or the [NSX Cross-vCenter Installation Guide](#).

Deprecated and Discontinued Functionality

End of Life and End of Support Warnings

For information about NSX and other VMware products that must be upgraded soon, please consult the [VMware Lifecycle Product Matrix](#). Upcoming end-of-support dates include:

- vCloud Networking and Security has reached End of Availability (EOA) and End of General Support (EOGS) on September 19, 2016. (See also [VMware knowledge base article 2144733](#).) (See also [VMware knowledge base article](#)

[2144620](#).)

- NSX for vSphere 6.1.x has reached End of Availability (EOA) and End of General Support (EOGS) on January 15, 2017. (See also [VMware knowledge base article 2144769](#).)
- As of NSX 6.2.3, the NSX Data Security feature has been deprecated. In NSX 6.2.3, you can continue to use this feature at your discretion, but be aware that this feature will be removed from NSX in a future release.
- Web Access Terminal (WAT) is being deprecated and will not be included in a future maintenance release. VMware recommends using the full access client with SSL VPN deployments for improved security.

Unsupported controller commands are no longer shown

Please review the CLI guide for the complete list of supported commands. You should only use commands which are documented in this guide. The join control-cluster command is not a supported command on NSX for vSphere. See also [VMware knowledge base article 2135280](#).

TLS 1.0 support has been deprecated as of NSX 6.2.3

In the NSX VPN, IPsec, and Load Balancer cipher suites, TLS 1.0 support has been deprecated as of NSX 6.2.3. For information on changes in cipher support, see [VMware knowledge base article 2147293](#).

Upgrade Notes

- **Downgrades are not supported:**

- Always capture a backup of NSX Manager before proceeding with an upgrade.
- Once NSX has been upgraded successfully, NSX cannot be downgraded.

- **To upgrade to NSX 6.2.4 or later,** you must perform a full NSX upgrade including host cluster upgrade (which upgrades the host VIBs to 6.2.4). For instructions, see the [NSX Upgrade Guide](#) including the [Upgrade Host Clusters to NSX 6.2](#) section.
- **Minimum of 8GB memory requirement:** Upgrade to NSX 6.2.3 or later may fail on hosts with less than 8 GB of memory.
- **Upgrading Edge Services Gateway (ESG):**
Starting in 6.2.5, resource reservation is carried out at the time of NSX Edge upgrade. When vSphere HA is enabled on a cluster having insufficient resources, the upgrade operation may fail due to vSphere HA constraints being violated.

To avoid such upgrade failures, perform the following steps before you upgrade an ESG:

1. Always ensure that your installation follows the best practices laid out for vSphere HA. Refer to document [Knowledge Base article 1002080](#).
2. Use the NSX tuning configuration API:
PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>
ensuring that values for edgeVCpuReservationPercentage and edgeMemoryReservationPercentage fit within available resources for the form factor (see table below for defaults).

The following resource reservations are used by the NSX Manager if you have not explicitly set values at the time of install or upgrade.

NSX Edge Form Factor	CPU Reservation	Memory Reservation
COMPACT	1000MHz	512 MB
LARGE	2000MHz	1024 MB
QUADLARGE	4000MHz	2048 MB
X-LARGE	6000MHz	8192 MB

- **Disable vSphere's Virtual Machine Startup option where vSphere HA is enabled and Edges are deployed.** After you upgrade your 6.2.4 or earlier NSX Edges to 6.2.5 or later, you must turn off the vSphere Virtual Machine Startup option for each NSX Edge in a cluster where vSphere HA is enabled and Edges are deployed. To do this, open the vSphere Web Client, find the ESXi host where NSX Edge virtual machine resides, click Manage: Settings, and, under Virtual Machines, select VM Startup/Shutdown, click Edit, and make sure that the virtual machine is in Manual mode (that is, make sure it is not added to the Automatic Startup/Shutdown list).
- **Before upgrading to NSX 6.2.5 or later, make sure all load balancer cipher lists are colon separated.** If your cipher list uses another separator such as a comma, make a PUT call to `https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles` and replace each `<ciphers>` list in `<clientSsl>` and `<serverSsl>` with a colon-separated list. For example, the relevant segment of the request body might look like the following. Repeat this procedure for all application profiles:

```
<applicationProfile>
  <name>https-profile</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>false</sslPassthrough>
  <template>HTTPS</template>
  <serverSslEnabled>true</serverSslEnabled>
  <clientSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDSA-AES256-SHA</ciphers>
    <clientAuth>ignore</clientAuth>
    <serviceCertificate>certificate-4</serviceCertificate>
  </clientSsl>
  <serverSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDSA-AES256-SHA</ciphers>
    <serviceCertificate>certificate-4</serviceCertificate>
  </serverSsl>
  ...
</applicationProfile>
```

- **Controller disk layout:** New installations of NSX 6.2.3 or later will deploy NSX Controller appliances with updated disk partitions to provide extra cluster resiliency. In previous releases, log overflow on the controller disk might impact controller stability. In addition to adding log management enhancements to prevent overflows, the NSX Controller appliance has separate disk partitions for data and logs to safeguard against these events. If you upgrade to NSX 6.2.3 or later, the NSX Controller appliances will retain their original disk layout.
- **Upgrade paths:**
 - Upgrade path from NSX 6.x: The [VMware Product Interoperability Matrix](#) provides details about the upgrade paths from VMware NSX. Cross-vCenter NSX upgrade is covered in the [NSX Upgrade Guide](#).
 - Upgrade path from vCNS 5.5.x:
 - Using the NSX upgrade bundle you may upgrade directly from VMware vCloud Networking and Security (vCNS) 5.5.x to NSX 6.2.x. For instructions, see the *NSX Upgrade Guide*, in the section, [vCloud Networking and Security to NSX Upgrade](#). This section also includes instructions for upgrading vCNS 5.5.x to NSX in a vCloud Director environment. A separate guide, the [NSX Upgrade Guide for vShield Endpoint](#), includes instructions for upgrading vCNS 5.5.x to NSX 6.2.x if you are using vShield Endpoint for anti-virus protection only.
 - If you have virtual wires in your environment, you must update your host clusters. Once this is done, the virtual wires are renamed to logical switches. See [Update Host Clusters](#) for instructions.
- **To validate** that your upgrade to NSX 6.2.x was successful see [knowledge base article 2134525](#).
- **Partner services compatibility:** If your site uses VMware partner services for guest introspection or network introspection, you must review the [VMware Compatibility Guide](#) before you upgrade, to verify that your vendor's service is compatible with this release of NSX.
- **Known issues affecting upgrades:** See the section, [Installation and Upgrade Known Issues](#), later in this document, for a list of known upgrade-related issues.
- **New system requirements:** For the memory and CPU requirements while installing and upgrading NSX Manager, see the [System Requirements for NSX](#) section in the NSX 6.2 documentation.
- **Set Correct Cipher version for Load Balanced Clients that use TLS 1.0:** This affects vROPs pool members that use TLS version 1.0. If the servers, whose traffic is being load-balanced, use this version, you must set a monitor extension value explicitly with the "ssl-version=10" setting in the NSX Load Balancer. See the [NSX Administration Guide](#).

```
{
  "expected" : null,
  "extension" : "ssl-version=10",
  "send" : null,
  "maxRetries" : 2,
  "name" : "sm_vrops",
  "url" : "/suite-api/api/deployment/node/status",
  "timeout" : 5,
  "type" : "https",
  "receive" : null,
  "interval" : 60,
  "method" : "GET"
}
```

- **Maximum number of NAT rules:** For NSX Edge versions prior to 6.2, a user could configure 2048 SNAT and 2048 DNAT rules separately, giving a total limit of 4096 rules. Since NSX Edge version 6.2 onwards, a limit is enforced for the maximum allowed NAT rules, based on the NSX Edge appliance size:

1024 SNAT and 1024 DNAT rules for a total limit of 2048 rules for COMPACT edge.

2048 SNAT and 2048 DNAT for a total limit of 4096 rules for LARGE edge and QUADLARGE edge.

4096 SNAT and 4096 DNAT rules for a total limit of 8192 rules for XLARGE edge.

During an NSX Edge upgrade to version 6.2, any existing COMPACT edge whose total NAT rules (sum of SNAT and DNAT) exceeds the limit 2048 will fail validation, resulting in an upgrade failure. In this scenario, the user will need to change the appliance size to LARGE, QUADLARGE and retry the upgrade.

- **Behavior change in redistribution filters** on distributed logical router and Edge Services Gateway: Starting in the 6.2 release, redistribution rules in the DLR and ESG work as ACLs only. That is, if a rule is an exact match, the respective action is taken.
- **VXLAN tunnel ID:** Before upgrading to NSX 6.2.x, you must make sure your installation is not using a VXLAN tunnel ID of 4094 on any tunnels. VXLAN tunnel ID 4094 is no longer available for use. To assess and address this follow these steps:
 1. In vCenter, navigate to **Home > Networking and Security > Installation** and select the **Host Preparation** tab.
 2. Click **Configure** in the VXLAN column.
 3. In the Configure VXLAN Networking window, set the VLAN ID to a value between 1 and 4093.
- **Reset vSphere web client:** After upgrading NSX Manager, you must reset the vSphere web client server as explained in the [NSX Upgrade documentation](#). Until you do this, the **Networking and Security** tab may fail to appear in the vSphere web client. You also may need to clear your browser cache or history.
- **Stateless environments:** NSX upgrades in a stateless host environment use new VIB URLs: In NSX upgrades in a stateless host environment, the new VIBs are pre-added to the Host Image profile during the NSX upgrade process. As a result, NSX on stateless hosts upgrade process follows this sequence:

1. Manually download the latest NSX VIBs from NSX Manager from a fixed URL.

2. Add the VIBs to the host image profile.

Prior to NSX 6.2.0, there was a single URL on NSX Manager from which VIBs for a certain version of the ESX Host could be found. (Meaning the administrator only needed to know a single URL, regardless of NSX version.) In NSX 6.2.0 and later, the new NSX VIBs are available at different URLs. To find the correct VIBs, you must perform the following steps:

- Find the new VIB URL from `https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties`.
- Fetch VIBs of required ESX host version from corresponding URL.
- Add them to host image profile.

- **Autosaved drafts and Service Composer:** In NSX 6.2.3 and later, you can disable the auto draft feature by setting *autoDraftDisabled* to true. Manually configured settings are maintained during the upgrade. Disabling the auto drafts feature before making large numbers of changes to the firewall rules might improve performance, and will prevent previously saved drafts from being overwritten. You can use the following API call to set the property *autoDraftDisabled* to true in the global configuration:

1. Get the existing global firewall configuration (GlobalConfiguration):
GET <https://NSX-Manager-IP-Address/api/4.0/firewall/config/globalconfiguration>
Note that a GET will not show the autoDraftDisabled field.
2. Use a PUT call to set the property autoDraftDisabled to true in the global configuration:
PUT <https://NSX-Manager-IP-Address/api/4.0/firewall/config/globalconfiguration>
with a request body that includes:

```
<globalConfiguration>
  <layer3RuleOptimize>...</layer3RuleOptimize>
  <layer2RuleOptimize>...</layer2RuleOptimize>
  <tcpStrictOption>...</tcpStrictOption>
  <autoDraftDisabled>true</autoDraftDisabled>
</globalConfiguration>
```

- **Host may become stuck in the installing state:** During large NSX upgrades, a host may become stuck in the installing state for a long time. This can occur due to issues uninstalling old NSX VIBs. In this case the EAM thread associated with this host will be reported in the VI Client Tasks list as stuck.

Workaround: Log into vCenter using the VI Client. Right click on the stuck EAM task and cancel it. From the vSphere Web Client, issue a Resolve on the cluster. The stuck host may now show as InProgress. Log into the host and issue a reboot to force completion of the upgrade on that host.

Known Issues

Known issues are grouped as follows:

- [General Known Issues](#)
- [Installation and Upgrade Known Issues](#)
- [NSX Manager Known Issues](#)
- [Logical Networking Known Issues and NSX Edge Known Issues](#)
- [Security Services Known Issues](#)
- [Monitoring Services Known Issues](#)
- [Solution Interoperability Known Issues](#)
- [NSX Controller Known Issues](#)

General Known Issues

Issue 1708769: Increased latency on SVM (Service VM) after snapshot in NSX

This issue occurs because running a snapshot of a Service VM (SVM) can cause added network latency. Snapshot is sometimes invoked by backup applications running in the environment.

Workaround: Refer to [VMware knowledge base article 2146769](#).

Issue 1700980: For security patch CVE-2016-2775, a query name which is too long can cause a segmentation fault in lwresd

NSX 6.2.4 has BIND 9.10.4 installed with the product, but it does not use lwres option in *named.conf*, hence the product is not vulnerable.

Workaround: As the product is not vulnerable, no workaround is required.

Issue 1716328: Removing host that is in maintenance mode can result in later cluster preparation failure

If an administrator places an NSX-enabled ESXi host in maintenance mode and removes it from an NSX-prepared cluster, NSX fails to delete its record of the ID number of the removed host. After the installation is in this state, if there is another host with same ID in another cluster or if this host is being added to another cluster, the cluster preparation process will fail for that cluster.

Workaround: Restart NSX Manager or run the following API to get rid of the extra entry. Perform a PUT of the API method, <https://nsx-manager-address/api/internal/firewall/updatestatus>

Issue 1659043: Service Status for Guest Introspection reported as "Not Ready" when NSX Manager to USVM communication times out

An error message similar to "PLAIN login refused: user 'usvm-admin-host-14' - invalid credentials" may be reported for the Guest Introspection Universal SVM when the expected password change process with NSX Manager on the internal message bus (rabbit MQ) does not succeed.

Workaround: To re-establish connectivity between the USVM and NSX Manager, restart the USVM or manually delete it and then select the Resolve button on the Service Composer UI to prompt a redeploy of the USVM for the affected host only.

Issue 1662842: Guest Introspection: Connectivity lost between MUX and USVM when trying to resolve unresolvable Windows SIDs

Guest Introspection service will go into a warning state, with each Guest Introspection going in and out of a warning state. Until the Guest Introspection VM reconnects, network events will not be delivered to the NSX Manager. This will affect both Activity Monitoring and ID Firewall in the case that logon events are detected through the Guest Introspection path.

Workaround: To return Guest Introspection to a stable state, Guest Introspection VMs must be configured to ignore lookups for these well-known SIDs. This is achieved by updating a configuration file on each Guest Introspection VM and then restarting the service. In addition, Active Directory log scraping can be used as a workaround for detecting logon events for ID Firewall.

Steps to ignore SID lookups for unresolvable SIDs:

1. Login to Guest Introspection VM.
2. Edit the file at /usr/local/usvmmgmt/config/ignore-sids.lst.
3. Append the following 2 lines:
S-1-18-1
S-1-18-2
4. Save and close the file.
5. Restart the Guest Introspection service with command:
rcusvm restart.

Issue 1558285: Deleting cluster with Guest Introspection from Virtual Center results in null pointer exception

Services such as Guest Introspection must be removed first before a cluster is removed from VC

Workaround: Delete the EAM Agency for the service deployment with no associated cluster.

Issue 1629030: The packet capture central CLI (debug packet capture and show packet capture) requires vSphere 5.5U3 or higher

These commands are not supported on earlier vSphere 5.5 releases.

Workaround: VMware advises all NSX customers to run vSphere 5.5U3 or higher.

Issue 1568180: Feature list incorrect for NSX when using vCenter Server Appliance (vCSA) 5.5

You can view the features of a license in the vSphere Web Client by selecting the license and clicking **Actions > View Features**. If you upgrade to NSX 6.2.3, your license is upgraded to an Enterprise license, which enables all features. However, if NSX Manager is registered with vCenter Server Appliance (vCSA) 5.5, selecting **View Features** will display the list of features for the license used before the upgrade, not the new Enterprise license.

Workaround: All Enterprise licenses have the same features, even if they are not displayed correctly in the vSphere Web Client. See the [NSX Licensing Page](#) for more information.

Issue 1477280: Cannot create hardware gateway instances when no controller is deployed

Controllers must be deployed before any hardware gateway instances are configured. If controllers are not deployed first, the error message "Failed to do the Operation on the Controller" is shown.

Workaround: None.

Issue 1491275: NSX API returns JSON instead of XML in certain circumstances

On occasion, an API request will result in JSON, not XML, being returned to the user.

Workaround: Add Accept: application/xml to the request header.

Installation and Upgrade Known Issues

New Issue 1838229: HTTP/HTTPS Transaction fails on NSX Load Balancer after upgrading to NSX 6.1.5 or later.

Starting in NSX 6.1.5, when enabling x-forwarded-for, the HTTP connection mode has been changed from passive close (option httpclose) to the default HTTP server-close (option http-server-close) mode, keeping the client-facing connection open while the server-facing connection is closed after receiving a response from the server. This causes problems in some applications because in NSX versions earlier than 6.1.5, the Load Balancer did not close the connection proactively, but inserted the "Connection:close" header in both directions to indicate to the client or server to close the connection.

Workaround: Add an application rule with the script option httpclose and associate it with the virtual server.

New Issue 1820723: Unable to see filters on ESXi after upgrade from 6.2.x to 6.2.7 because of failure to connect to host
After you upgrade from NSX 6.2.x to 6.2.7 and cluster VIBs to 6.2.7 bits, even though the installation status shows successful and firewall enabled, the communication channel health will show the NSX Manager to Firewall Agent connectivity and NSX Manager to ControlPlane Agent connectivity as down. This will lead to the failure of Firewall rules publish and Security Policy publish, and VXLAN configuration not being sent down to hosts.

Workaround: Run the message bus sync API call for the cluster using the API POST <https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize>.

API Body:

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{Cluster-MOID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

New Issue 1435504: HTTP/HTTPS Health Check appears DOWN after upgrading from 6.0.x or 6.1.x to 6.2.x with failure reason "Return code of 127 is out of bounds - plugin may be missing"

In NSX 6.0.x and 6.1.x releases, URLs configured without double quotes (") caused Health Check to fail with this error: "Return code of 127 is out of bounds - plugin may be missing". The workaround for this was to add the double quotes (") to the input URL (this was not required for send/receive/expect fields). However, this issue was fixed in 6.2.0 and as a result, if you are upgrading from 6.0.x or 6.1.x to 6.2.x, the additional double quotes result in the pool members shown as DOWN in Health Check.

Workaround: Remove the double quotes (") in the URL field from all the relevant Health Check configurations after upgrading.

Issue 1768144: Old NSX Edge appliance resource reservations that exceed new limits may cause failure during upgrade or redeployment

In NSX 6.2.4 and earlier, you could specify an arbitrarily large resource reservation for an NSX Edge appliance. NSX did not enforce a maximum value. After NSX Manager is upgraded to 6.2.5 or later, if an existing Edge has resources reserved (especially memory) that exceed the newly enforced maximum value imposed for the chosen form factor, it would fail during Edge upgrade or redeploy (which would trigger an upgrade). For example, if the user has specified a memory reservation of 1000MB on a pre-6.2.5 LARGE Edge and, after upgrade to 6.2.5 or later, changes the appliance size to COMPACT, the user-specified memory reservation will exceed the newly enforced maximum value, in this case 512 for a COMPACT Edge, and the operation will fail.

See [Upgrading Edge Service Gateway \(ESG\)](#) for information on recommended resource allocation starting in NSX 6.2.5.

Workaround: Use the appliance REST API: PUT <https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/> to reconfigure the memory reservation to be within values specified for the form factor, without any other appliance changes. You can change the appliance size after this operation completes.

Issue 1730017: Upgrades from 6.2.3 to 6.2.7 do not show a version change for Guest Introspection

As the 6.2.3 Guest Introspection module is the latest version available, the version after a 6.2.7 upgrade remains unchanged. Note that upgrades from earlier NSX releases may show a version change to 6.2.7

Workaround: This does not affect any functionality.

Issue 1683879: Upgrade to NSX 6.2.3 or later may fail on hosts with less than 8 GB of memory

NSX 6.2.3 and later requires a minimum of 8 GB of memory on prepared hosts running networking and security services. The minimum ESXi 6.0 memory requirement of 4 GB is not sufficient to run NSX.

Workaround: None.

Issue 1673626: Modifying tcpLoose via /api/3.0/edges is not allowed after upgrading from vCloud Networking and Security to NSX

After upgrading from vCloud Networking and Security to NSX, you will see an error if you try to modify the tcpLoose setting in this API request: [/api/3.0/edges](#)

Workaround: Use tcpPickOngoingConnections setting in the globalConfig section in the API request [/api/4.0/firewall/config](#) instead.

Issue 1658720: Enabling DFW for a given cluster would fail for a vCNS to NSX upgrade scenario where the cluster has VXLAN installed and vShield App not installed (or removed before upgrade) in vCNS deployment

This issue occurs because the cluster sync status is not invoked when the hosts are upgraded.

Workaround: Restart NSX Manager.

Issue 1600281: USVM Installation Status for Guest Introspection shows as Failed in the Service Deployments tab

If the backing datastore for the Guest Introspection Universal SVM goes offline or becomes inaccessible, the USVM may need to be rebooted or re-deployed to recover.

Workaround: Reboot or re-deploy USVM to recover.

Issue 1660373: vCenter enforces expired NSX license

As of vSphere 5.5 update 3 or vSphere 6.0.x vSphere Distributed Switch is included in the NSX license. However, vCenter does not allow ESX hosts to be added to a vSphere Distributed Switch if the NSX license is expired.

Workaround: Your NSX license must be active in order to add a host to a vSphere Distributed Switch.

Issue 1569010/1645525: When upgrading from 6.1.x to NSX for vSphere 6.2.3 on a system connected to Virtual Center 5.5, the Product field in the "Assign License Key" window displays the NSX license as a generic value of "NSX for vSphere" and not a more specific version such as "NSX for vSphere - Enterprise."

Workaround: None.

Issue 1465249: Installation status for Guest Introspection shows Succeeded even though the host is offline

After installing Guest Introspection on the cluster that has one host offline, the host that is offline shows Installation Status as Succeeded and Status Unknown.

Workaround: None.

Issue 1636916: In a vCloud Air environment, when the NSX Edge version is upgraded from vCNS 5.5.x to NSX 6.x, Edge firewall rules with a source protocol value of "any" are changed to "tcp:any, udp:any"

As a result, ICMP traffic is blocked, and packet drops may be seen.

Workaround: Before upgrading your NSX Edge version, create more specific Edge firewall rules and replace "any" with specific source port values.

Issue 1660355: VMs which are migrated from 6.1.5 to 6.2.3 will not have support for TFTP ALG

Even though the host is enabled, VMs which are migrated from 6.1.5 to 6.2.3 will not have support for TFTP ALG.

Workaround: Add and remove the VM from the exclusion list or restart the VM, so that new 6.2.3 filter gets created which will have support for TFTP ALG.

Issue 1394287: Adding or removing VMs from a virtual wire does not update IP address set in vShieldApp rules

If an existing vCNS vShield App firewall installation is not upgraded to the NSX distributed firewall in enhanced mode, new VMs with firewall rules based on virtual wires will not have an updated IP address. As a result, these VMs are not protected by the NSX firewall. This issue is only seen in the following scenarios:

- After upgrading the Manager from vCNS to NSX and not switching to DFW Enhanced mode.
- If you add new VMs to a virtualWire with vshield App rules consuming those virtualwires, these rules will not have the new IP Address set for the new VMs.
This will cause the new VMs not protected by vShieldApp.

Workaround: Publish the rule again which will set the new address.

Issue 1386874: After vCenter upgrade, vCenter might lose connectivity with NSX

If you are using vCenter embedded SSO and you are upgrading vCenter 5.5 to vCenter 6.0, vCenter might lose connectivity with NSX. This happens if vCenter 5.5 was registered with NSX using the root user name. In NSX 6.2, vCenter registration with root is deprecated.

Note: If you are using external SSO, no change is necessary. You can retain the same user name, for example admin@mybusiness.mydomain, and vCenter connectivity will not be lost.

Workaround: Reregister vCenter with NSX using the administrator@vsphere.local user name instead of root.

Issue 1332563: Shutdown Guest OS for agent VMs (SVA) before powering OFF

When a host is put into maintenance mode, all service appliances are powered-off, instead of shutting down gracefully. This may lead to errors within third-party appliances.

Workaround: None.

Issue 1473537: Unable to power on the Service appliance that was deployed using the Service Deployments view

Workaround: Before you proceed, verify the following:

- The deployment of the virtual machine is complete.
- No tasks such as cloning, reconfiguring, and so on are in progress for the virtual machine displayed in VC task pane.
- In the VC events pane of the virtual machine, the following events are displayed after the deployment is initiated:

Agent VM <vm name> has been provisioned.
Mark agent as available to proceed agent workflow.

In such a case, delete the service virtual machine. In service deployment UI, the deployment is seen as Failed. Upon clicking the Red icon, an alarm for an unavailable Agent VM is displayed for the host. When you resolve the alarm, the virtual machine is redeployed and powered on.

If not all clusters in your environment are prepared, the Upgrade message for Distributed Firewall does not appear on the Host Preparation tab of Installation page

When you prepare clusters for network virtualization, distributed firewall is enabled on those clusters. If not all clusters in your environment are prepared, the upgrade message for Distributed Firewall does not appear on the Host Preparation tab.

Workaround: Use the following REST call to upgrade Distributed Firewall:

```
PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state
```

Issue 1215460: If a service group is modified after the upgrade to add or remove services, these changes are not reflected in the firewall table

User created service groups are expanded in the Edge Firewall table during upgrade - i.e., the Service column in the firewall table displays all services within the service group. If the service group is modified after the upgrade to add or remove services, these changes are not reflected in the firewall table.

Workaround: Create a new service group with a different name and then consume this service group in the firewall rule.

Issue 1088913: vSphere Distributed Switch MTU does not get updated

If you specify an MTU value lower than the MTU of the vSphere distributed switch when preparing a cluster, the vSphere Distributed Switch does not get updated to this value. This is to ensure that existing traffic with the higher frame size isn't unintentionally dropped.

Workaround: Ensure that the MTU you specify when preparing the cluster is higher than or matches the current MTU of the vSphere distributed switch. The minimum required MTU for VXLAN is 1550.

Issue 1413125: SSO cannot be reconfigured after upgrade

When the SSO server configured on NSX Manager is the one native on vCenter server, you cannot reconfigure SSO settings on NSX Manager after vCenter Server is upgraded to version 6.0 and NSX Manager is upgraded to version 6.x.

Workaround: None.

Issue 1288506: After upgrading from vCloud Networking and Security 5.5.3 to NSX vSphere 6.0.5 or later, NSX Manager does not start up if you are using an SSL certificate with DSA-1024 keysize

SSL certificates with DSA-1024 keysize are not supported in NSX vSphere 6.0.5 onwards, so the upgrade is not successful.

Workaround: Import a new SSL certificate with a supported keysize before starting the upgrade.

Issue 1266433: SSL VPN does not send upgrade notification to remote client

SSL VPN gateway does not send an upgrade notification to users. The administrator has to manually communicate that the SSL VPN gateway (server) is updated to remote users and they must update their clients.

Workaround: Users need to uninstall the older version of client and install the latest version manually.

Issue 1402307: If vCenter is rebooted during NSX vSphere upgrade process, incorrect Cluster Status is displayed

When you do host prep in an environment with multiple NSX prepared clusters during an upgrade and the vCenter Server gets rebooted after at least one cluster has been prepared, the other clusters may show Cluster Status as Not Ready instead of showing an Update link. The hosts in vCenter may also show Reboot Required.

Workaround: Do not reboot vCenter during host preparation.

Issue 1487752: Momentary loss of third-party anti-virus protection during upgrade

When upgrading from NSX 6.0.x to NSX 6.1.x or 6.2.x, you might experience momentary loss of third-party anti-virus protection for VMs. This issue does not affect upgrades from NSX 6.1.x to NSX 6.2.

Workaround: None.

Issue 1498376: Host error message appears while configuring distributed firewall

While configuring distributed firewall, if you encounter an error message related to the host, check the status of fabric feature "com.vmware.vshield.nsxmgr.messagingInfra". If the status is red, perform the following workaround.

Workaround: Use the following REST API call to reset communication between NSX Manager and a single host or all hosts in a cluster.

POST https://<NSX Manager IP>/api/2.0/nwfabric/configure?action=synchronize

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{HOST/CLUSTER MOID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

Issue 1491820: NSX Manager log collects WARN messagingTaskExecutor-7 messages after upgrade to NSX 6.2

After upgrading from NSX 6.1.x to NSX 6.2, the NSX Manager log becomes flooded with messages similar to: WARN messagingTaskExecutor-7 ControllerInfoHandler:48 - host is unknown: host-15 return empty list. There is no operational impact.

Workaround: None.

Issue 1284735: After upgrade from vCNS, cannot place new grouping objects into some upgraded grouping objects
vCNS 5.x supported creation of grouping objects at scopes below GlobalRoot (below the NSX-wide scope). For example, in vCNS 5.x you could create a grouping object as the DC or PG level. By contrast, the NSX 6.x user interface creates such objects under the GlobalRoot, and these newly created grouping objects cannot be added to existing grouping objects that were created at a lower scope (DC or PG) in your pre-upgrade vCNS installation.

Workaround: See [VMware knowledge base article 2117821](#).

Issue 1495969: After upgrading from vCNS 5.5.4 to NSX 6.2.x, the firewall on the Host Preparation tab remains disabled

After upgrading from vCNS 5.5.x to NSX 6.2.x and upgrading all the clusters, the firewall on the Host Preparation tab remains disabled. In addition, the option to upgrade the firewall does not appear in the UI. This happens only when there are hosts that are not part of any prepared clusters in the datacenter, because the VIBs will not be installed on those hosts.

Workaround: To resolve the issue, move the hosts into an NSX 6.2 prepared cluster.

Issue 1495307: During an upgrade, L2 and L3 firewall rules do not get published to hosts

After publishing a change to the distributed firewall configuration, the status remains InProgress both in the UI and the API indefinitely, and no log for L2 or L3 rules is written to the file vsfwd.log.

Workaround: During an NSX upgrade, do not publish changes to the distributed firewall configuration. To exit from the InProgress state and resolve the issue, reboot the NSX Manager virtual appliance.

Issue 1474066: The NSX REST API call to enable or disable IP detection seems to have no effect

If host cluster preparation is not yet complete, the NSX REST API call to enable or disable IP detection (https://<nsxmgr-ip>/api/2.0/xvs/networks/universalwire-5/features) has no effect.

Workaround: Before issuing this API call, make sure the host cluster preparation is complete.

Issue 1479314: NSX 6.0.7 SSL VPN clients cannot connect to NSX 6.2 SSL VPN gateways

In NSX 6.2 SSL VPN gateways, the SSLv2 and SSLv3 protocols are disabled. This means the SSL VPN gateway only accepts the TLS protocol. The SSL VPN 6.2 clients have been upgraded to use the TLS protocol by default during connection establishment. In NSX 6.0.7, the SSL VPN client uses an older version of OpenSSL library and the SSLv3 protocol to establish a connection. When an NSX 6.0.x client tries to connect to an NSX 6.2 gateway, the connection establishment fails at the SSL handshake level.

Workaround: Upgrade your SSL VPN client to NSX 6.2 after you have upgraded to NSX 6.2. For upgrade instructions, see the [NSX Upgrade documentation](#).

Issue 1434909: Must create a segment ID pool for new or upgraded logical routers

In NSX 6.2, a segment ID pool with available segment IDs must be present before you can upgrade a logical router to 6.2 or create a new 6.2 logical router. This is true even if you have no plans to use NSX logical switches in your deployment.

Workaround: If your NSX deployment does not have a local segment ID pool, create one as a prerequisite to NSX logical router upgrade or installation.

Issue 1459032: Error configuring VXLAN gateway

When configuring VXLAN using a static IP pool (at **Networking & Security > Installation > Host Preparation > Configure VXLAN**) and the configuration fails to set an IP pool gateway IP on the VTEP (because the gateway is not properly configured or is not reachable), the VXLAN configuration status enters the Error (RED) state at for the host cluster.

The error message is VXLAN Gateway cannot be set on host and the error status is VXLAN_GATEWAY_SETUP_FAILURE. In the REST API call, GET <https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>>, the status of VXLAN is as follows:

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

Workaround: To fix the error, there are two options.

- Option 1: Remove VXLAN configuration for the host cluster, fix the underlying gateway setup in the IP pool by making sure the gateway is properly configured and reachable, and then reconfigure VXLAN for the host cluster.
- Option 2: Perform the following steps.
 1. Fix the underlying gateway setup in the IP pool by making sure the gateway is properly configured and reachable.
 2. Put the host (or hosts) into maintenance mode to ensure no VM traffic is active on the host.
 3. Delete the VXLAN VTEPs from the host.
 4. Take the host out of maintenance mode. Taking hosts out of maintenance mode triggers the VXLAN VTEP creation process on NSX Manager. NSX Manager will try to re-create the required VTEPs on the host.

Issue 1463767: In a cross vCenter deployment, a universal firewall configuration section might be under (subordinate to) a local configuration section

If you move a secondary NSX Manager to the standalone (transit) state and then change it back to the secondary state, any local configuration changes that you made while it was temporarily in the standalone state might be listed above the replicated universal configuration sections inherited from the primary NSX Manager. This produces the error condition universal section has to be on top of all other sections on secondary NSX Managers.

Workaround: Use the UI option to move sections up or down so that the local section is below the universal section.

Issue 1289348: After an upgrade, firewall rules and network introspection services might be out of sync with NSX Manager

After upgrading from NSX 6.0 to NSX 6.1 or 6.2, the NSX firewall configuration displays the error message: synchronization failed / out of sync. Using the **Force Sync Services: Firewall** action does not resolve the issue.

Workaround: In NSX 6.1 and NSX 6.2, either security groups or dvPortgroups can be bound to a service profile, but not both. To resolve the issue, modify your service profiles.

Issue 1462319: The esx-dvfilter-switch-security VIB is no longer present in the output of the "esxcli software vib list | grep esx" command.

Starting in NSX 6.2, the esx-dvfilter-switch-security modules are included within the esx-vxlan VIB. The only NSX VIBs installed for 6.2 are esx-vsip and esx-vxlan. During an NSX upgrade to 6.2, the old esx-dvfilter-switch-security VIB gets removed from the ESXi hosts.

Starting in NSX 6.2.3, a third VIB, esx-vdpi, is provided along with the esx-vsip and esx-vxlan NSX VIBs. A successful installation will show all 3 VIBs.

Workaround: None.

Issue 1481083: After the upgrade, logical routers with explicit failover teaming configured might fail to forward packets properly

When the hosts are running ESXi 5.5, the explicit failover NSX 6.2 teaming policy does not support multiple active uplinks on distributed logical routers.

Workaround: Alter the explicit failover teaming policy so that there is only one active uplink and the other uplinks are in standby mode.

Issue 1485862: Uninstalling NSX from a host cluster sometimes results in an error condition

When using the Uninstall action on the **Installation: Host Preparation** tab, an error might occur with the `eam.issue.OrphanedAgency` message appearing in the EAM logs for the hosts. After using the Resolve action and rebooting the hosts, the error state continues even though the NSX VIBs are successfully uninstalled.

Workaround: Delete the orphaned agency from the vSphere ESX Agent Manager (**Administration: vCenter Server Extensions: vSphere ESX Agent Manager**).

Issue 1411275: vSphere Web Client does not display Networking and Security tab after backup and restore in NSX vSphere 6.2

When you perform a backup and restore operation after upgrading to NSX vSphere 6.2, the vSphere Web Client does not display the **Networking and Security** tab.

Workaround: When an NSX Manager backup is restored, you are logged out of the Appliance Manager. Wait a few minutes before logging in to the vSphere Web Client.

Issue 1493777: After upgrade to NSX 6.2, NSX Manager has more than 100 percentage of physical memory allocated
Starting in NSX 6.2, NSX Manager requires 16 GB of reserved memory. The former requirement was 12 GB.

Workaround: Increase the NSX Manager virtual appliance's reserved memory to 16 GB.

Issue 1393889: Data Security service status is shown as UP even when IP connectivity is not established

Data Security appliance may have not received the IP address from DHCP or is connected to an incorrect port group.

Workaround: Ensure that the Data Security appliance gets the IP from DHCP/IP Pool and is reachable from the management network. Check if the ping to the Data Security appliance is successful from NSX/ESX.

Service virtual machine deployed using the Service Deployments tab on the Installation page does not get powered on

Workaround: Follow the steps below.

1. Manually remove the service virtual machine from the ESX Agents resource pool in the cluster.
2. Click **Networking and Security** and then click **Installation**.
3. Click the **Service Deployments** tab.
4. Select the appropriate service and click the **Resolve** icon.
The service virtual machine is redeployed.

Issue 1764460: After completing Host Preparation, all cluster members appear in ready state, but cluster level erroneously appears as "Invalid"

After you complete Host Preparation, all cluster members correctly appear in "Ready" state, but cluster level appears as "Invalid" and the reason displayed is that you need a host reboot, even though the host has already been rebooted.

Workaround: Click on the red warning icon and select Resolve.

NSX Manager Known Issues

New Issue 1806368: In case of a cross-VC Failover, the DLR config is not pushed to all hosts if old controllers are reused for a previously failed primary NSX Manager that is made primary again after a failover.

In a cross-VC setup, when the primary NSX Manager fails, a secondary NSX Manager is promoted to primary and a new controller cluster is deployed to be used with the newly promoted secondary (now primary) NSX Manager. When the primary NSX Manager is back on, the secondary NSX Manager is demoted and the primary NSX Manager is restored. In this case, if you reuse the existing controllers that were deployed on this primary NSX Manager before the failover, the DLR config is not pushed to all hosts. This issue does not arise if you create a new controller cluster instead.

Workaround: Deploy a new controller cluster for the restored primary NSX Manager.

New Issue 1831131: Connection from NSX Manager to SSO fails when authenticated using the LocalOS user

Connection from NSX Manager to SSO fails when authenticated using the LocalOS user with the error: "Could not establish communication with NSX Manager. Please contact administrator."

Workaround: Add the Enterprise Admin role for nsxmanager@localos in addition to nsxmanager@domain.

Issue 1772911: NSX Manager disk space consumption increasing rapidly, task and job tables size increasing with high CPU usage

NSX Manager CPU consistently is at 100% or is regularly spiking to 100%. Running the show process monitor command in NSX Manager Command Line Interface (CLI) displays the Java process that is consuming the highest CPU cycles. Disk space consumption growing rapidly with increase in DB size, resulting in slow performance of NSX Manager.

Workaround: Contact VMware technical support.

Issue 1441874: Upgrading a single NSX Manager in a vCenter Linked Mode Environment displays an error message

In an environment with multiple VMware vCenter Servers with multiple NSX managers, when selecting one or more NSX Managers from the vSphere Web Client > Networking and Security > Installation > Host Preparation, you see this error: "Could not establish communication with NSX Manager. Please contact administrator."

Workaround: See [VMware Knowledge Base article 2127061](#) for more information.

Issue 1696750: Assigning an IPv6 address to NSX Manager via PUT API requires a reboot to take effect

Changing the configured network settings for NSX Manager via `https://{NSX Manager IP address}/api/1.0/appliance-management/system/network` requires a system reboot to take effect. Until the reboot, pre-existing settings will be shown.

Workaround: None.

Issue 1671067: NSX Plugin does not appear in vCenter Web Client while ESXTOP plugin is also installed

After deployment of NSX and successful registration with vCenter, NSX plugin does not appear in the vCenter Web Client. This issue is caused by conflict between NSX plugin and ESXTOP plugin.

Workaround: Remove ESXTOP plugin with the following procedure:

1. Make sure there is a recent backup of vCenter Snapshot vCenter VM (without quiesce)
2. Delete /usr/lib/vmware-vmware-vmware-client/plugin-packages/esxtop-plugin
`rm -R /usr/lib/vmware-vmware-vmware-client/plugin-packages/esxtop-plugin`
3. Delete /usr/lib/vmware-vmware-vmware-client/server/work
`rm -R /usr/lib/vmware-vmware-vmware-client/server/work`
4. Restart the web client
`service vmware-vmware-client restart`
5. (Optional) Ensure that there is no output from the following command: `"tail -f /var/log/vmware/vsphere-client/logs/eventlog.log | grep esx"`
6. Make sure to consolidate vCenter snapshot if that is the preferred method of roll back option

Issue 1486403: NSX Manager does not accept DNS search strings with a space delimiter

NSX Manager does not accept DNS search strings with a space delimiter. You may only use a comma as a delimiter. For example, if the DHCP server advertises eng.sample.com and sample.com for the DNS search list, NSX Manager is configured with eng.sample.com sample.com.

Workaround: Use comma separators. NSX Manager only accepts comma separator as DNS search strings.

Issue 1529178: Uploading a server certificate which does not include a common name returns an "internal server error" message

If you upload a server certificate that does not have any common name, an "internal server error" message appears.

Workaround: Use a server certificate which has both a SubAltName and a common name, or at least a common name.

Issue 1655388: NSX Manager 6.2.3 UI displays English language instead of local language when using IE11/Edge browser on Windows 10 OS for JA, CN, and DE languages

When you launch NSX Manager 6.2.3 with IE11/Edge browser on Windows 10 OS for JA, CN, and DE languages, English language is displayed.

Workaround:

Perform the following steps:

1. Launch the Microsoft Registry Editor (regedit.exe), and go to **Computer > HKEY_CURRENT_USER > SOFTWARE > Microsoft > Internet Explorer > International**.
2. Modify the value of *AcceptLanguage* file to native language. For example, If you want to change language to **DE**, change value and make the **DE** show the first position.
3. Restart the browser, and log in to the NSX Manager again. Appropriate language is displayed.

Issue 1435996: Log files exported as CSV from NSX Manager are timestamped with epoch not datetime

Log files exported as CSV from NSX Manager using the vSphere Web Client are timestamped with the epoch time in milliseconds, instead of with the appropriate time based on the time zone.

Workaround: None.

Issue 1644297: Add/delete operation for any DFW section on the primary NSX creates two DFW saved configurations on the secondary NSX

In a cross-vCenter setup, when an additional universal or local DFW section is added to the primary NSX Manager, two DFW configurations are saved on the secondary NSX Manager. While it does not affect any functionality, this issue will cause the saved configurations limit to be reached more quickly, possibly overwriting critical configurations.

Workaround: None.

Issue 1534877: NSX management service doesn't come up when the hostname's length is more than 64 characters

Certificate creation via OpenSSL library requires a hostname less than or equal to 64 characters.

Issue 1537258: NSX Manager list slow to display in Web Client

In vSphere 6.0 environments with multiple NSX Managers, the vSphere web client may take up to two minutes to display the list of NSX Managers when the logged-in user is being validated with a large AD Group set. You may see a data service timeout error when attempting to display the NSX Manager list. There is no workaround. You must wait for the list to load/relogin to see the NSX Manager list.

Issue 1534622: NSX controller shows as disconnected

NSX Manager logs report disconnection to controllers via a message similar to "ERROR http-nio-127.0.0.1-7441-exec-16908 BaseRestController:339 - Exception : 'I/O error: Read timed out; nested exception is java.net.SocketTimeoutException: Read timed out'". This condition occurs when an intermediate firewall on the network blocks the TCP/IP FIN message after the idle timeout value is reached. When this condition is occurring, the number of connections to the NSX Manager will increase.

Issue 1534606: Host Preparation Page fails to load

When running Virtual Center in linked mode, each VC must be connected to an NSX Manager on the same NSX version. If the NSX versions differ, the vSphere Web Client will only be able to communicate with the NSX Manager running the higher version of NSX. An error similar to "Could not establish communication with NSX Manager. Please contact administrator," will be displayed on the Host Preparation tab.

Workaround: All NSX managers should be upgraded to the same NSX software version.

Issue 1386874: Networking and Security Tab not displayed in vSphere Web Client

After vSphere is upgraded to 6.0, you cannot see the Networking and Security Tab when you log in to the vSphere Web Client with the root user name.

Workaround: Log in as administrator@vsphere.local or as any other vCenter user which existed on vCenter Server before the upgrade and whose role was defined in NSX Manager.

Issue 1415480: After NSX Manager backup is restored, REST call shows status of fabric feature

com.vmware.vshield.nsxmgr.messagingInfra as Red

When you restore the backup of an NSX Manager and check the status of fabric feature com.vmware.vshield.nsxmgr.messagingInfra using a REST API call, it is displayed as Red instead of Green.

Workaround: Use the following REST API call to reset communication between NSX Manager and a single host or all hosts in a cluster.

POST https://<nsxmgr-ip>/api/2.0/nwfabric/configure?action=synchronize

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.nsxmgr.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>HOST/CLUSTER MOID</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

Issue 1027066: vMotion of NSX Manager may display the error message, "Virtual ethernet card Network adapter 1 is not supported"

You can ignore this error. Networking will work correctly after vMotion.

Issue 1406471: Syslog shows host name of backed up NSX Manager on the restored NSX Manager

If a second NSX Manager is installed with the same IP address and a unique hostname as the first NSX Manager, restoring the configuration will show the first NSX Manager's hostname after a restore and the second NSX Manager's hostname after reboot.

Workaround: Host name of second NSX Manager should be configured to be same as the backed up NSX Manager.

Issue 1477041: NSX Manager virtual appliance summary page shows no DNS name

When you log in to the NSX Manager virtual appliance, the Summary page has a field for the DNS name. This field remains blank even though a DNS name has been defined for the NSX Manager appliance.

Workaround: You can view the NSX Manager's hostname and the search domains on the Manage: Network page.

Issue 1492880: NSX Manager UI do not automatically log out after changing password using NSX Command Line Interface

If you are logged in to NSX Manager and recently changed your password using CLI, you might continue to stay logged in to the NSX Manager UI using your old password. Typically, NSX Manager client should automatically log you out if the session times out for being inactive.

Workaround: Log out from the NSX Manager UI and log back in with your new password.

Issue 1468613: Unable to edit a network host name

After you login to NSX Manager virtual appliance and navigate to the Appliance Management, click Manage Appliance Settings, and click Network under Settings to edit the network host name, you might receive an invalid domain name list error. This happens when the domain names specified in the Search Domains field are separated with whitespace characters, instead of commas. NSX Manager only accepts domain names that are comma separated.

Workaround: Perform the following steps:

1. Log in to the NSX Manager virtual appliance.
2. Under **Appliance Management**, click **Manage Appliance Settings**.
3. From the Settings panel, click **Network**.
4. Click **Edit** next to DNS Servers.
5. In the Search Domains field, replace all whitespace characters with commas.
6. Click **OK** to save the changes.

Issue 1436953: False system event is generated even after successfully restoring NSX Manager from a backup

After successfully restoring NSX Manager from a backup, the following system events appear in the vSphere Web Client when you navigate to **Networking & Security: NSX Managers: Monitor: System Events**.

- Restore of NSX Manager from backup failed (with Severity=Critical).
- Restore of NSX Manager successfully completed (with Severity=Informational).

Workaround: If the final system event message shows as successful, you can ignore the system generated event messages.

Issue 1489768: Change in behavior of NSX REST API call to add a namespace in a datacenter

In NSX 6.2, the POST `https://<nsxmgr-ip>/api/2.0/namespace/datacenter/` REST API call returns a URL with an absolute path, for example `http://198.51.100.3/api/2.0/namespace/api/2.0/namespace/datacenter/datacenter-1628/2`. In previous releases of NSX, this API call returned a URL with a relative path, for example: `/api/2.0/namespace/datacenter/datacenter-1628/2`.

Workaround: None.

Logical Networking Known Issues and NSX Edge Known Issues

New Issue 1798847: In a Cross VC NSX setup, update of VXLAN UDP port can get stuck forever.

If primary NSX manager does not have any secondary NSX managers configured, then updating VXLAN UDP port hangs forever.

Workaround: Use NSX Manager API to resume port update workflow on primary NSX manager.

New Issue 1698286: Hardware VTEP in a cross-vCenter NSX environment only supported on the primary NSX Manager

In a cross-vCenter NSX environment, hardware gateway switch configurations and operations are supported only on the primary NSX Manager. Hardware gateway switches must be bound to non-universal logical switches. Hardware gateway configurations are not supported on secondary NSX Managers.

Workaround: In a cross-vCenter NSX environment it is recommended to use L2 bridging to connect logical switches to physical networks.

New Issue 1844966: NSX Edge file system becomes Read-only

If there are any storage connectivity issues where an edge is located, edge file system may enter read-only state to protect the OS file system. This is expected behaviour in a Linux server. See [VMware Knowledge Base article 2146870](#) for more information.

Workaround: Do the following:

1. Re-deploy the edge.
2. Reboot the edge(Both edges in HA pair).
3. Force sync the edge.

Issue 1799261: NSX Edge may run into split-brain condition after upgrade or redeploy

On the standby NSX Edge, the *show service highavailability* CLI command show high availability status as "Standby" but the config engine status as "Active".

Workaround: Reboot the standby NSX Edge.

Issue 1777792: Peer Endpoint set as 'ANY' causes IPSec connection to fail

When IPSec configuration on NSX Edge sets remote peer endpoint as 'ANY', the Edge acts as an IPSec "server" and waits for remote peers to initiate connections. However, when the initiator sends a request for authentication using PSK and XAUTH, the Edge displays this error message: "initial Main Mode message received on XXX.XXX.XX.XX:500 but no connection has been authorized with policy=PSK+XAUTH" and IPsec can't be established.

Workaround: Use specific peer endpoint IP or FQDN in IPSec VPN configuration instead of ANY.

Issue 1741158: Creating a new, unconfigured NSX Edge and applying configuration can result in premature Edge service activation.

If you use the NSX API to create a new, unconfigured NSX Edge, then make an API call to disable one of the Edge services on that Edge (for example, set dhcp-enabled to "false"), and finally apply configuration changes to the disabled Edge service, that service will be made active immediately.

Workaround: After you make a configuration change to an Edge service that you wish to keep in disabled state, immediately issue a PUT call to set the enabled flag to "false" for that service.

Issue 1758500: Static route with multiple next-hops does not get installed in NSX Edge routing and forwarding tables if at least one of the next-hop configured is the Edge's vNIC IP address

With ECMP and multiple next-hop addresses, NSX allows the Edge's vNIC's IP address to be configured as next-hop if at least one of the next-hop IP addresses is valid. This is accepted without any errors or warnings but route for the network is removed from the Edge's routing/forwarding table.

Workaround: Do not configure the Edge's own vNIC IP address as a next-hop in static route when using ECMP.

Issue 1733165: IPsec may cause removal of dynamic routes from NSX Edge forwarding table

If a subnet reachable via dynamic route is used as a remote subnet for IPsec configuration, NSX Edge removes this subnet from the forwarding table and does not reinstall it even after this subnet is deleted from the IPsec configuration.

Workaround: Enable/Disable routing protocol or clear routing neighborship.

Issue 1675659: Floating Static Routes are preferred to OSPF Dynamic Routes

A backup Floating Static Route is incorrectly entered into an Edge's routing table when Route Redistribution is enabled even though an OSPF Route is available.

Workaround: To work around this issue, disable the route redistribution of static into OSPF.

Note: This issue does not impact the data path. See [VMware knowledge base article 2147998](#).

Issue 1716464: NSX Load Balancer will not route to VMs newly tagged with a Security tag.

If we deploy two VMs with a given tag, and then configure an LB to route to that tag, the LB will successfully route to those two VMs. But if we then deploy a third VM with that tag, the LB only routes to the first two VMs. *Workaround:* Click "Save" on the LB Pool. This rescans the VMs and will start routing to newly tagged VMs.

Issue 1776073: When Edge with private local AS sends routes to EBGP peers, all the private AS paths are stripped off from the BGP routing updates sent.

NSX currently has a limitation that prevents it from sharing the full AS path with eBGP neighbors when the AS path contains only private AS paths. While this is the desired behavior in most cases, there are cases in which the administrator may want to share private AS paths with an eBGP neighbor.

Workaround: No workaround available to make the Edge announce all the AS paths in the BGP update.

Issue 1716545: Changing appliance size of Edge does not affect standby Edge's CPU and Memory reservation

Only the first Edge VM created as part of an HA pair is assigned the reservation settings.

To configure the same CPU/Memory reservation on both Edge VMs:

- Use the PUT API [https:// <NSXManager>/api/4.0/edgePublish/tuningConfiguration](https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration) to set explicit values for both Edge VMs.
- or
- Disable and re-enable Edge HA, which will delete the second Edge VM and redeploy a new one with the default reservations.

Workaround: None.

Issue 1510724: Default routes do not populate on the hosts after creating a new Universal Distributed Logical Router (UDLR)

After changing NSX Manager from Standalone to primary mode for the purpose of configuring Cross-vCenter in NSX for vSphere 6.2.x, you may experience these symptoms:

- When you create a new UDLR, the default routes are not populated on the host instance.
- Routes are populated on the UDLR Control VM but not on the host instance.
- Running the *show logical-router host host-ID dlr Edge-ID route* command fails to show default routes.

Workaround: To recover from this issue, refer to [VMware knowledge base article 2145959](#).

Issue 1492547: Extended convergence time seen when NSX-based OSPF area border router with highest IP address is shut down or rebooted

If an NSSA area border router which does not have the highest IP address is shut down or rebooted, traffic converges rapidly to another path. If an NSSA area border router with the highest IP address is shut down or rebooted, a multi-minute re-convergence time is seen. The OSPF process can be cleared manually to reduce the convergence time.

Workaround: See [VMware knowledge base article 2127369](#).

Issue 1542416: Data path not working for 5 min after edge re-deploy and HA failover with sub-interfaces

Redeploy or HA failover operation will see a five minute outage if sub-interfaces are used. Issue is not observed on interfaces.

Workaround: No workaround.

Issue 1706429: Communication issues when enabling high availability (HA) after initial logical (distributed) router deployment might cause both logical router appliances to be active.

If you deploy a logical router without HA and then later enable HA (deploying a new logical router appliance), or if you disable and then re-enable HA, sometimes one of the logical router appliances is missing a connected route to the HA interface. This causes both appliances to be in the active state.

Workaround: On the logical router appliance that is missing the connected route for the HA interface, either disconnect and then reconnect the vNIC of the logical router appliance, or reboot the logical router appliance.

Issue 1461421: "show ip bgp neighbor" command output for NSX Edge retains the historical count of previously established connections

The "show ip bgp neighbor" command displays the number of times that the BGP state machine transitioned into the Established state for a given peer. Changing the password used with MD5 authentication causes the peer connection to be destroyed and re-created, which in turn will clear the counters. This issue does not occur with an Edge DLR.

Workaround: To clear the counters, execute the "clear ip bgp neighbor" command.

Issue 1676085: Enabling Edge HA will fail if resource reservation fails

Starting with NSX for vSphere 6.2.3, enabling high availability on an existing Edge will fail when sufficient resources cannot be reserved for the second Edge VM appliance. The configuration will roll back to the last known good configuration. In previous releases, if HA is enabled after Edge deployment and resource reservation fails, the Edge VM still is created.

Workaround: This is an expected change in behavior.

Issue 1656713: IPsec Security Policies (SPs) missing on the NSX Edge after HA failover, traffic cannot flow over tunnel

The **Standby > Active** switchover will not work for traffic flowing on IPsec tunnels.

Workaround: Disable/Enable IPsec after the NSX Edge switchover.

Issue 1624663: After clicking "Configure Advanced Debugging" refreshes the VC UI and the change does not persist

After clicking the specific edge ID > Configuration > Action > Configure Advanced Debugging causes the VC UI to refresh and the change does not persist

Workaround: Go directly to the Edge list menu, highlight the edge, and click Action > Configure Advanced Debugging to continue with the changes.

Issue 1354824: When an Edge VM becomes corrupted or becomes otherwise unreachable due to such reasons as a power failure, system events are raised when the health check from NSX Manager fails

The system events tab will report "Edge Unreachability" events. The NSX Edges list may continue to report a Status of Deployed.

Workaround: Use the `https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status` API with `detailedStatus=true`.

Issue 1556924: L3 connectivity loss with VXLAN would block error

When DLR LIF's are configured on the host but underlying VXLAN layer is not fully prepared, connectivity through some of DLR LIF's may be affected. Some of the VMs belonging to DLR are not reachable. There might be *"Failed to Create VXLAN trunk status: Would block"* logs in `/var/log/vmkernel.log` file.

Workaround: You may delete the LIF's and recreate them. Another option is rebooting the affected ESX hosts.

Issue 1647657: Show commands on an ESXi host with VDR display no more than 2000 routes per VDR instance

Show commands on an ESXi host with VDR enabled will not show more than 2000 routes per VDR instance, although more than this maximum may be running. This issue is a display issue, and the data path will work as expected for all routes.

Workaround: No workaround.

Issue 1634215: OSPF CLI commands output does not indicate whether routing is disabled

When OSPF is disabled, routing CLI commands output does not show any message saying *"OSPF is disabled"*. The output is empty.

Workaround: The `show ip ospf` command will display the correct status.

Issue 1663902: Renaming an NSX Edge VM disrupts traffic flowing through the Edge

Issue 1647739: Redeploying an Edge VM after a vMotion operation will cause the Edge or DLR VM to be placed back on the original cluster.

Workaround: To place the Edge VM in a different resource pool or cluster, use the NSX Manager UI to configure the desired location.

Issue 1463856: When NSX Edge Firewall is enabled, existing TCP connections are blocked

TCP connections are blocked through the Edge stateful firewall as the initial three-way handshake cannot be seen.

Workaround: To handle such existing flows, do the following. Use the NSX REST API to enable the flag `"tcpPickOngoingConnections"` in the firewall global configuration. This switches the firewall from strict mode to lenient mode. Next, enable the firewall. Once existing connections have been picked up (this may take a few minutes after you enable the firewall), set the flag `"tcpPickOngoingConnections"` back to false to return the firewall to strict mode. (This setting is persistent.)

```
PUT /api/4.0/edges/{edgeId}/firewall/config/global
```

```
<globalConfig>  
  <tcpPickOngoingConnections>true</tcpPickOngoingConnections>  
</globalConfig>
```

Issue 1374523: Reboot ESXi, or run `/services.sh restart` after installation of VXLAN VIB to make the VXLAN commands available using esxcli

After installation of VXLAN VIB, you must reboot ESXi or run the `/services.sh restart` command, so that the VXLAN commands becomes available using esxcli.

Workaround: Instead of using esxcli, use localcli.

Issue 1604514: Editing/Configuring default gateway on an unmanaged DLR fails after clicking Publish

When a default gateway is added to an unmanaged DLR, the publish will fail with error "Routing Distance is support only on NSX Edge version 6.2.0 and later with NSX Edge VMs deployed". This is due to the default admin distance "1" populated on the UI.

Workaround: Remove the admin distance "1" which is populated by default.

Issue 1642087: After modifying the `securelocaltrafficbyip` parameter value in the IPsec VPN Extension, forwarding to destination networks fails

When using an NSX Edge Services Gateway, you experience this symptom:

- After changing the `securelocaltrafficbyip` value to 0 in the NSX UI (Edit IPsec VPN screen), forwarding to a remote subnet of the IPsec VPN tunnel no longer works
- After changing this parameter, you no longer see the correct information for a remote subnet in the IP routing table

Workaround: Disable and re-enable the IPsec VPN service. Then validate that the expected routing information is shown in the CLI and the UI.

Issue 1525003: Restoring an NSX Manager backup with an incorrect passphrase will silently fail as critical root folders cannot be accessed

Workaround: None.

Issue 1637639: When using the Windows 8 SSL VPN PHAT client, the virtual IP is not assigned from the IP pool

On Windows 8, the virtual IP address is not assigned as expected from the IP pool when a new IP address is assigned by the Edge Services Gateway or when the IP pool changes to use a different IP range.

Workaround: This issue occurs only on Windows 8. Use a different Windows OS to avoid experiencing this issue.

Issue 1534603: IPsec and L2 VPN service status shows as down even when the service is not enabled

Under the Settings tab in the UI, the L2 service status is displayed as down, however the API shows the L2 status as up. L2 VPN and IPsec service always shows as down in the Settings tab unless the UI page is refreshed.

Workaround: Refresh the page.

Issue 1562767: Delays in connecting to NSX load balancer do not provide consistent connections over multiple VIPs

When the load balancer is configured to use Source IP Hash load balancing, a connected client session receives a consistent connection to a backend server. The load balancer should also be able to provide, for a given connected client, consistent connections over multiple VIPs if those VIPs are backed by the same server pool. That is, when one backend server serves multiple VIPs, a given client's connection to one of that backend server's VIPs should guarantee that that client will use the same backend server when connecting to other VIPs served by that backend server. A known issue prevents the NSX load balancer from providing such consistent connections over multiple VIPs.

Issue 1553600: Delays in connecting to RIB and FIB after assigning IP address to interface

When you attempt to assign an IP address to an interface, typically, the interface information is updated immediately. However, when waiting for a polling event, you may observe a delay in seeing the assigned IP address. (The NSX logical router polls periodically to get changes in the interfaces.)

Issue 1534799: Slow convergence when OSPF area border router with highest IP address is shut down

Convergence takes a long time when the NSX-based, OSPF area border router (ABR) with highest IP address is shut down or rebooted. If an ABR that does not have the numerically highest IP address is shut down or rebooted, traffic converges quickly

to another path. However, if the ABR with the highest IP address is shut down or rebooted, a multi-minute re-convergence time is seen. The OSPF process can be cleared manually to reduce the convergence time.

Issue 1446327: Some TCP-based applications may time out when connecting through NSX Edge

The default TCP established connection inactivity timeout is 3600 seconds. The NSX Edge deletes any connections idle for more than the inactivity timeout and drops those connections.

Workaround:

1. If the application has a relatively long inactivity time, enable TCP keepalives on the hosts with `keep_alive_interval` set to less than 3600 seconds.
2. Increase the Edge TCP inactivity timeout to greater than 2 hours using the following NSX REST API. For example, to increase the inactivity timeout to 9000 seconds. NSX API URL:
`/api/4.0/edges/{edgeId}/systemcontrol/config PUT Method <systemControl>
<property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</property> </systemControl>`

Issue 1534602: UI does not display Edge management plane mode (VIX/MSGBUS), and does not provide the option to change from VIX to MSGBUS

When an Edge appliance is in VIX mode, it is not eligible to be selected for inclusion in DFW, and centralized CLI commands take much longer to run compared to MSGBUS mode

Workaround: Make sure that the cluster where the Edge is deployed is prepared for NSX and its "NSX Manager to Firewall Agent" is in "Up" state, and redeploy the Edge.

Issue 1498243: Distributed logical router advertises incorrect next hop for default route when BGP neighbor filter is set to "DENY, ANY, OUT"

With 'default originate' enabled on an NSX distributed logical router (DLR), setting a BGP neighbor filter of "DENY, ANY, OUT" on the DLR causes the DLR to advertise an incorrect next hop address for the default route. This error occurs only when a BGP neighbor filter is added with the following attributes:

- Action: DENY
- Network: ANY
- Direction: OUT

Workaround: None.

Issue 1471561: BGP/OSPF neighbor relationship is not established with directly connected routers

Dynamic routing does not work as expected with directly connected routers when ECMP routes exist for that directly connected network.

Workaround: Reboot Edge OR delete and re-create the associated vNIC interface.

Issue 1089745: Logical router LIF routes are advertised by upstream Edge Services Gateway even if logical router OSPF is disabled

Upstream Edge Services Gateway will continue to advertise OSPF external LSAs learned from logical router connected interfaces even when logical router OSPF is disabled.

Workaround: Disable redistribution of connected routes into OSPF manually and publish before disabling OSPF protocol. This ensures that routes are properly withdrawn.

Issue 1498965: Edge syslog messages do not reach remote syslog server

Immediately after deployment, the Edge syslog server cannot resolve the hostnames for any configured remote syslog servers.

Workaround: Configure remote syslog servers using their IP address, or use the UI to Force Sync the Edge.

Issue 1494025: Logical router DNS Client configuration settings are not fully applied after updating REST Edge API

Workaround: When you use REST API to configure DNS forwarder (resolver), perform the following steps:

1. Specify the DNS Client XML server's settings so that they match the DNS forwarder setting.
2. Enable DNS forwarder, and make sure that the forwarder settings are same as the DNS Client server's settings specified in the XML configuration.

Issue 1243112: Validation and error message not present for invalid next hop in static route, ECMP enabled

When trying to add a static route, with ECMP enabled, if the routing table does not contain a default route and there is an unreachable next hop in the static route configuration, no error message is displayed and the static route is not installed.

Workaround: None.

Issue 1288487: If an NSX Edge virtual machine with one sub interface backed by a logical switch is deleted through the vCenter Web Client user interface, data path may not work for a new virtual machine that connects to the same port

When the Edge virtual machine is deleted through the vCenter Web Client user interface (and not from NSX Manager), the VXLAN trunk configured on dvPort over opaque channel does not get reset. This is because trunk configuration is managed by NSX Manager.

Workaround: Manually delete the VXLAN trunk configuration by following the steps below:

1. Navigate to the vCenter Managed Object Browser by typing the following in a browser window:
`https://<vc-ip>/mob?vmodl=1`
2. Click **Content**.
3. Retrieve the dvsUuid value by following the steps below.
 - a. Click the rootFolder link (for example, group-d1(Datacenters)).
 - b. Click the data center name link (for example, datacenter-1).
 - c. Click the networkFolder link (for example, group-n6).
 - d. Click the DVS name link (for example, dvs-1)
 - e. Copy the value of uuid.
4. Click **DVSManager** and then click **updateOpaqueDataEx**.
5. In *selectionSet*, add the following XML.

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>value</dvsUuid>
  <portKey>value</portKey> <!--port number of the DVPG where trunk vnic got connected-->
</selectionSet>
```

6. In *opaqueDataSpec*, add the following XML

```
<opaqueDataSpec>
  <operation>remove</operation>
  <opaqueData>
    <key>com.vmware.net.vxlan.trunkcfg</key>
    <opaqueData></opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

7. Set **isRuntime** to false.
8. Click **Invoke Method**.
9. Repeat steps 5 through 8 for each trunk port configured on the deleted Edge virtual machine.

Issue 1637939: MD5 certificates are not supported while deploying hardware gateways

While deploying hardware gateway switches as VTEPs for logical L2 VLAN to VXLAN bridging, the physical switches support at minimum SHA1 SSL certificates for OVSDDB connection between the NSX controller and OVSDDB switch.

Workaround: None.

Issue 1637943: No support for hybrid or multicast replication modes for VNIs that have a hardware gateway binding
Hardware gateway switches when used as VTEPs for L2 VXLAN-to-VLAN bridging support Unicast replication mode only.

Workaround: Use Unicast replication mode only.

Issue 1493611: No connectivity on VLAN ID 0 in L2 VPN

NSX L2 VPN configuration incorrectly allows the user to configure an L2 VPN with VLAN ID 0. Once configured, no traffic can flow on this VPN.

Workaround: Workaround: Use a valid VLAN ID in the range from 1 to 4094.

Security Services Known Issues

New Issue 1853107: Error received on UI when the certification is unchecked or some changes on IPsec configuration are modified for IPsec VPN under PSK mode

You see the error "Failed to read certs & secrets. : 002 forgetting secrets" on the Global Configuration tab when PSK mode certification is unchecked or modified for IPsec VPN with certificate-based authentication.

See [VMware Knowledge Base article 2149868](#) for more information and the workaround.

Issue 1474650: For NetX users, ESXi 5.5.x and 6.x hosts experience a purple diagnostic screen mentioning ALERT: NMI: 709: NMI IPI received

When a large number of packets are transmitted or received by a service VM, DVFilter continues to dominate the CPU

resulting in heartbeat loss and a purple diagnostic screen. See [VMware Knowledge Base article 2149704](#) for more information.

Workaround: Upgrade the ESXi host to any of the following ESXi versions that are the minimum required to use NetX:

- 5.5 Patch 10
- ESXi 6.0U3

Issue 1741844: Using ARP snooping to detect address of vNIC with multiple IP addresses results in 100% CPU consumption

This issue occurs when a virtual machine's vNIC is configured with multiple IP addresses and ARP snooping is enabled for IP detection. The IP discovery module keeps sending vNIC-IP updates to the NSX Manager continuously to change the vNIC-IP mapping for all VMs configured with multiple IP addresses.

Workaround: There is no workaround. Currently the ARP snooping feature supports only one IP address per vNIC. For more information, see the section [IP Discovery for Virtual Machines](#) in the *NSX Administration Guide*.

Issue 1689159: The Add Rule feature in Flow Monitoring does not work correctly for ICMP flows.

When adding a rule from Flow Monitoring, the Services field will remain blank if you do not explicitly set it to ICMP and as a result, you may end up adding a rule with the service type "ANY".

Workaround: Update the Services field to reflect ICMP traffic.

Issue 1620460: NSX fails to prevent users from creating rules in Service Composer rules section

In the vSphere Web Client, the Networking and Security: Firewall interface fails to prevent users from adding rules to the Service Composer rules section. Users should be permitted to add rules above/below the Service Composer section, but not inside it.

Workaround: Do not use the "+" button at the global rule level to add rules to the Service Composer rules section.

Issue 1682552: Threshold events for CPU/Memory/CPS for Distributed Firewall (DFW) are not reported

Even when the DFW thresholds for CPU/Memory/CPS are set for reporting, the threshold events are not reported when the thresholds are crossed.

Workaround:

- Login to each ESXi host and restart the DFW controlplane process by running the following command:
`/etc/init.d/vShield_Stateful_Firewall restart`
- Verify the status using the following command:
`/etc/init.d/vShield_Stateful_Firewall status`
- The result similar to following is displayed:
`"vShield-Stateful-Firewall is running"`

Note: You should be cautious while performing this operation as this will push all DFW rules to all the filters again. If there are lot of rules, it might take some time to enforce them on all the filters.

Issue 1717635: Firewall configuration operation fails if more than one cluster is present in environment and changes are done in parallel

In an environment with multiple clusters, if two or more users modify the firewall configuration continuously in a tight loop. (for example, Add/Delete sections or rules), some operations fail, and the user will see an API response similar to:

```
<?xml version="1.0" encoding="UTF-8"? >
neutron-server.log.1:70282:2016-08-23 17:58:23.429 30787 ERROR vmware_nsx.plugins.nsx_v.plugin
<error>
<details> org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update; nested exception is
javax.persistence.PersistenceException: org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch
update </details>
<errorCode>258
</errorCode>
</error>
```

Workaround: Avoid concurrent modification of the firewall configuration.

Issue 1717994: Distributed Firewall (DFW) Status API query reports 500 internal server error intermittently

If the DFW status API query is issued while adding a new host into a host prepared cluster, the API query fails with 500 internal server error for few attempts, and then returns correct response once the host starts to get VIBs installed.

Workaround: Do not use the DFW status API query until the new host is prepared successfully.

Issue 1686036: Firewall rules cannot be added, edited, or removed when default section is deleted

If the default Layer2 or Layer3 section is deleted, publishing a firewall rule may fail.

Workaround: Do not delete the default rule. If the configuration with default rule was saved in draft, perform the following steps:

1. Delete the complete firewall configuration using following DELETE API call.
https://<NSX Manager IP>/api/4.0/firewall/globalroot-0/config
This will restore the default section on the firewall.
2. Load the saved draft of firewall rules with default section to the firewall.

Issue 1628220: DFW or NetX observations are not seen on receiver side

Traceflow may not show DFW and NetX observations on receiver side if switch port associated with the destination vNIC changed. It will not be fixed for vSphere 5.5 releases. For vSphere 6.0 and up, there is no such issue.

Workaround: Do not disable vNIC. Reboot VM.

Issue 1626233: When NetX service virtual machine (SVM) drops packets, traceflow does not generate dropped observation

The traceflow session exits after packet is sent to the NetX service virtual machine (SVM). When the SVM drops packets, traceflow does not generate dropped observation.

Workaround: There is no workaround. If the traceflow packet is not injected back, it can be assumed that the SVM dropped the packet.

Issue 1632235: During Guest Introspection installation, network drop down list displays "Specified on Host" only

When installing Guest Introspection with the NSX anti-virus-only license and vSphere Essential or Standard license, the network drop down list will display only the existing list of DV port groups. This license does not support DVS creation.

Workaround: Before installing Guest Introspection on a vSphere host with one of these licenses, first specify the network in the "Agent VM Settings" window.

Issue 1652155: Creating or migrating firewall rules using REST APIs may fail under certain conditions and report HTTP 404 error

Adding or migrating firewall rules using REST APIs is not supported under these conditions:

- Creating firewall rules as a bulk operation when the autosavedraft=true is set.
- Adding firewall rules in sections concurrently.

Workaround: Set the autoSaveDraft parameter to false in the API call when performing bulk firewall rule creation or migration.

Issue 1509687: URL length supports up to 16000 characters when assigning a single security tag to many VMs at a time in one API call

A single security tag cannot be assigned to a large number of VMs simultaneously with a single API if the URL length is more than 16,000 characters.

Workaround: To optimize performance, tag up to 500 VMs in a single call.

Issue 1662020: Publish operation may fail resulting in an error message "Last publish failed on host *host number*" on DFW UI in General and Partner Security Services sections

After changing any rule, the UI displays "Last publish failed on host *host number*". The hosts listed on the UI may not have correct version of firewall rules, resulting in lack of security and/or network disruption.

The problem is usually seen in the following scenarios:

- After upgrade from older to latest NSXv version.
- Move a host out of cluster and move it back in.
- Move a host from one cluster to another.

Workaround: To recover, you must force sync the affected clusters (firewall only).

Issue 1481522: Migrating firewall rule drafts from 6.1.x to 6.2.3 is not supported as the drafts are not compatible between the releases

Workaround: None.

Issue 1491046: IPv4 IP address does not get auto approved when SpoofGuard policy is set to Trust On First Use (TOFU) in VMware NSX for vSphere 6.2.x

Workaround: See [VMware knowledge base article 2144649](#).

Issue 1628679: With identity-based firewall, the VM for removed users continues to be part of the security group

When a user is removed from a group on the AD server, the VM where the user is logged-in continues to be a part of the security-group. This retains firewall policies at the VM vnic on the hypervisor, thereby granting the user full access to services.

Workaround: None. This behavior is expected by design.

Issue 1462027: In cross vCenter NSX deployments, multiple versions of saved firewall configurations get replicated to secondary NSX Managers

Universal Sync saves multiple copies of universal configurations on secondary NSX Managers. The list of saved configurations contains multiple drafts created by the synchronizing across NSX Managers with the same name and at the same time or with a time difference of 1 second.

Workaround: Run the API call to delete duplicate drafts.

DELETE : <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts/>

Find the drafts to be deleted by viewing all drafts:

GET: <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts>

In the following sample output, drafts 143 and 144 have the same name and were created at the same time and are therefore duplicates. Likewise, drafts 127 and 128 have the same name are off by 1 second and are also duplicates.

```
<firewallDrafts>
  <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT" timestamp="1438816120917">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT" timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT" timestamp="1438808882608">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT" timestamp="1438808881750">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
</firewallDrafts>
```

Issue 1449611: When a firewall policy in the Service Composer is out of sync due to a deleted security group, the firewall rule cannot be fixed in the UI

Workaround: In the UI, you can delete the invalid firewall rule and then add it again. Or, in the API, you can fix the firewall rule by deleting the invalid security group. Then synchronize the firewall configuration: Select **Service Composer: Security Policies**, and for each security policy that has associated firewall rules, click **Actions** and select **Synchronize Firewall Config**. To prevent this issue, modify firewall rules so that they do not refer to security groups before deleting the security groups.

Issue 1557880: Layer 2 (L2) rules may be missing if the MAC address of a VM used in the rules is modified

Because L2 rule optimization is ON by default, L2 rules with both source and destination fields specified (other than "any") will be applied to vNICs(or filters) only if the vNIC MAC address matches the source or destination MAC address list. Hosts with VMs not matching the source or destination MAC addresses will not have those L2 rules applied.

Workaround: To have L2 rules applied to all vNICs(or filters), set one of the source or destination fields to "any".

Issue 1505316: NSX NetX rule not published to host when selected service is a Service Group

When creating an L3 Redirection rule in the Partner Services tab in DFW, selecting a Service Group doesn't create the rule correctly.

Workaround: Use individual services when creating the rule instead of using a Service Group.

Issue 1496273: UI allows creation of in/out NSX firewall rules that cannot be applied to Edges

The web client incorrectly allows creation of an NSX firewall rule applied to one or more NSX Edges when the rule has traffic traveling in the 'in' or 'out' direction and when PacketType is IPV4 or IPV6. The UI should not allow creation of such rules, as NSX cannot apply them to NSX Edges.

Workaround: None.

Issue 1534574: There is no support for Cipher 3C (SHA-256) encryption algorithms for SSLVPN-Plus

Issue 1557924: Universal logical switch is allowed to be consumed in the appliedTo field of a local DFW rule

When a universal logical switch is used as a security group member, the DFW rule can use that security group in AppliedTo field. This indirectly applies the rule on the universal logical switch, which should not be allowed because it may cause unknown behavior of those rules.

Workaround: None.

Issue 1559971: Cross-vCenter NSX firewall exclude list not published if firewall is disabled on one cluster

In cross-vCenter NSX, firewall exclude list is not published to any cluster when the firewall is disabled on one of the clusters.

Workaround: Force sync the affected NSX Edges.

Issue 1407920: Firewall rule republish fails after DELETE API is used

If you delete the entire firewall configuration through the DELETE API method and then try to republish all the rules from a previously saved firewall rules draft, then the rule publish will fail.

Issue 1534585: Publishing Distributed Firewall (DFW) rules fails after referenced object is deleted in VMware NSX for vSphere 6.1.x and 6.2.x

Workaround: If this occurs, see [knowledge base article 2126275](#).

Issue 1494718: New universal rules cannot be created, and existing universal rules cannot be edited from the flow monitoring UI

Workaround: Universal rules cannot be added or edited from the flow monitoring UI. EditRule will be automatically disabled.

Issue 1442379: Service composer firewall configuration out of sync

In the NSX service composer, if any firewall policy is invalid (for example of you deleted a security group that was currently in use in a firewall rule), deleting or modifying another firewall policy causes the service composer to become out of sync with the error message Firewall configuration is not in sync.

Workaround: Delete any invalid firewall rules and then synchronize the firewall configuration. Select **Service Composer: Security Policies**, and for each security policy that has associated firewall rules, click **Actions** and select **Synchronize Firewall Config**. To prevent this issue, always fix or delete invalid firewall configurations before making further firewall configuration changes.

Issue 1066277: Security policy name does not allow more than 229 characters

The security policy name field in the Security Policy tab of Service Composer can accept up to 229 characters. This is because policy names are prepended internally with a prefix.

Workaround: None.

Issue 1443344: Some versions of 3rd-party Networks VM-Series do not work with NSX Manager default settings

Some NSX 6.1.4 or later components disable SSLv3 by default. Before you upgrade, please check that all third-party solutions integrated with your NSX deployment do *not* rely on SSLv3 communication. For example, some versions of the Palo Alto Networks VM-series solution require support for SSLv3, so please check with your vendors for their version requirements.

Issue 1660718: Service Composer policy status is shown as "In Progress" at the UI and "Pending" in the API output

Workaround: None.

Issue 1620491: Policy-level Sync status in Service Composer does not show publishing status of the rules within a policy

When a policy is created or modified, Service Composer will display a success status which indicates only the persistence state. It does not reflect whether the rules were published to the host successfully.

Workaround: Use the firewall UI to view publish status.

Issue 1317814: Service Composer goes out of sync when policy changes are made while one of the Service Managers is down

When a policy changes is made when one of multiple Service Managers is down, the changes will fail, and Service Composer will fall out of sync.

Workaround: Ensure the Service Manager is responding and then issue a force sync from Service Composer.

Issue 1070905: Cannot remove and re-add a host to a cluster protected by Guest Introspection and third-party security solutions

If you remove a host from a cluster protected by Guest Introspection and third-party security solutions by disconnecting it and then removing it from vCenter Server, you may experience problems if you try to re-add the same host to the same cluster.

Workaround: To remove a host from a protected cluster, first put the host in maintenance mode. Next, move the host into an unprotected cluster or outside all clusters and then disconnect and remove the host.

Issue 1648578: NSX forces the addition of cluster/network/storage when creating a new NetX host-based service instance

When you create a new service instance from the vSphere Web Client for NetX host-based services such as Firewall, IDS, and IPS , you are forced to add cluster/network/storage even though these are not required.

Workaround: When creating a new service instance, you may add any information for cluster/network/storage to fill out the fields. This will allow the creation of the service instance and you will be able to proceed as required.

Issue 1772504: Service Composer does not support Security Groups with MAC Set

Service Composer allows use of Security Groups in Policy configurations. In case there is a Security Group which contains MAC Set, Service Composer accepts that Security Group without complaining, but fails to enforce rules for that specific MAC Set. This is because Service Composer works on Layer3 and does not support Layer2 constructs. Note that if a Security Group has IP Set and MAC Set both, the IP set will still be effective, but the MAC Set will be ignored. There is no harm in referencing a Security Group containing MAC Set - user must be aware that the MAC Set will be ignored.

Workaround: If the user's intent is to create Firewall rules using a MAC Set, then the user should use DFW Layer2/Ethernet configuration instead of Service Composer.

Issue 1718726: Cannot force-sync Service Composer after a user has manually deleted the Service Composer's policy section using DFW REST API

In a cross-vCenter NSX environment, a user's attempt to force sync NSX Service Composer configuration will fail if there was only one policy section and that policy section (the Service Composer-managed policy section) was deleted earlier via a REST API call.

Workaround: Do not delete the Service Composer-managed policy section via a REST API call. (Note that the UI already prevents deletion of this section.)

Monitoring Services Known Issues

Issue 1655593: Missing status on NSX Dashboard when logging in as Auditor or Security Admin roles

When viewing NSX Dashboard as Auditor or Security Admin, an error message "User is not authorized to access object ... and feature ... Please check object access scope and feature permissions for the user" appears. For example, Auditor may not be able to see "Logical Switch Status" from the Dashboard.

Workaround: None.

Issue 1466790: Unable to choose VMs on bridged network using the NSX traceflow tool

Using the NSX traceflow tool, you cannot select VMs that are not attached to a logical switch. This means that VMs on an L2 bridged network cannot be chosen by VM name as the source or destination address for traceflow inspection.

Workaround: For VMs attached to L2 bridged networks, use the IP address or MAC address of the interface you wish to specify as destination in a traceflow inspection. You cannot choose VMs attached to L2 bridged networks as source.

Solution Interoperability Known Issues

New Issue 1840744: VMware ESXi 6.0.0 host experiences a purple diagnostic screen after a virtual machine is stuck in a reboot loop

This issue occurs due to race condition in dvfilter create/destroy events created by the virtual machine stuck in a reboot loop.

- For more information, see [VMware Knowledge Base article 2149782](#).

Workaround: This issue is resolved in VMware ESXi 6.0 Patch 03 and later releases, available at VMware Downloads. To work around this issue if you do not want to upgrade, power off the affected virtual machine.

Issue 1568861: The NSX Edge deployment fails during any edge deployment from a vCD cell that does not own the VC listener

The NSX Edge deployment fails during any Edge deployment from a vCD cell that does not own the VC listener. Also, NSX Edge actions, including a redeploy, fail from vCD.

Workaround: Deploy an NSX Edge from the vCD cell which owns the VC listener.

Issue 1530360: After an NSX Manager VM has failed over, Site Recovery Manager (SRM) incorrectly reports a timeout error

When a NSX Manager VM is failed over, SRM incorrectly reports a timeout error waiting for VMware Tools. In this case, VMware Tools actually is up and running within the 300 second timeout.

Workaround: None.

NSX Controller Known Issues

New Issue 1845087: NSX Controller API will be adversely affected if disk latency is very high

The NSX controller API may not respond within NSX manager's time limit if I/O latency is too high for the storage used by NSX controller. This may in turn affect upgrade and other functionalities of the NSX controller. The Network and Security plugin of the vSphere Web Client will show "High controller disk latency" as an error if the severity exceeds a certain limit.

Workaround: To resolve this issue, VMware recommends using a dedicated local hard drive and SSD.

Issue 1765354: <deployType> is a required property but it is not used

<deployType> is a required property but it is not used and does not mean anything.

Issue 1760102: Virtual machines may fail to communicate after an NSX controller is deleted and redeployed to recover from a storage outage

An NSX Controller for the vSphere 6.2.x environment may get into read-only mode in case of a storage outage. If you delete and redeploy the controller to recover from that state, some VMs may fail to communicate. Expected behavior in case of a storage outage on a controller is that rebooting of the controller should recover it from read-only mode, but currently that does not happen in NSX.

Workaround: Restart the NSX Management Service.

Issue 1516207: Controller(s) may become isolated after IPsec communication is re-enabled on an NSX controller cluster

If an NSX controller cluster is set to allow controller-to-controller communications in the clear (IPsec is disabled), and IPsec-based communication is later re-enabled, one or more controllers may become isolated from the cluster majority due to a mismatched pre-shared key ("PSK"). When this occurs, the NSX API may become unable to change the IPsec settings of the controllers.

Workaround:

Follow these steps to address this issue:

1. Disable IPSec using the NSX API.

```
PUT /2.0/vdn/controller/node
```

```
<controllerNodeConfig>  
  <ipSecEnabled>false</ipSecEnabled>  
</controllerNodeConfig>
```

2. Re-enable IPsec using the NSX API.

```
PUT /2.0/vdn/controller/node
```

```
<controllerNodeConfig>  
  <ipSecEnabled>true</ipSecEnabled>  
</controllerNodeConfig>
```

Follow these best practices to avoid this issue:

- Always use the NSX API to disable IPsec. Using the NSX Controller CLI to disable IPsec is not supported.
- Always verify that all controllers are active before you use the API to change the IPsec setting.

Issue 1306408: NSX Controller logs must be downloaded sequentially

NSX Controller logs cannot be downloaded simultaneously. Even when downloading from multiple controllers, you must wait for the download from the current controller to finish before you start the download from the next controller. Note also that you cannot cancel a log download once it has started.

Workaround: Wait for the current controller log download to finish before starting another log download.

Resolved Issues

See what's resolved in [6.2.7](#), or in [6.2.6 and earlier](#).

New Issues Resolved in NSX 6.2.7

6.2.7 resolved issues are grouped as follows:

- [General Resolved Issues in NSX 6.2.7](#)
- [Installation and Upgrade Resolved Issues in NSX 6.2.7](#)
- [NSX Manager Resolved Issues in NSX 6.2.7](#)
- [Networking and Edge Services Resolved Issues in NSX 6.2.7](#)
- [Security Services Resolved Issues in NSX 6.2.7](#)

General Resolved Issues in NSX 6.2.7

Fixed Issue 1812971: Host process crashes with "out of memory" error

The mux process hoards system memory because of a memory leak causing host processes to crash with "out of memory" error. *Fixed in 6.2.7.*

Fixed Issue 1810407: host_mux_missing_report alarm raised on the vCenter server

A memory resource contention caused the mux process to be out of memory and unable to create a mux_health_report to send to the NSX Manager. This caused a host_mux_missing_report alarm on the vCenter server. *Fixed in 6.2.7.*

Installation and Upgrade Resolved Issues in NSX 6.2.7

Fixed Issue 1716619: An issue is seen when editing interfaces on Edges deployed through vCD versions earlier than 8.20.

Fixed in 6.2.7.

Fixed Issue 1815264: vsfwd service fails to start if vmvisor memory cannot be allocated after upgrading from NSX 6.2.x to NSX 6.2.7. Fixed in 6.2.7.

Networking and Edge Services Resolved Issues in NSX 6.2.7

Fixed Issue 1811884: Logical switch is not removed in Universal Synchronization Service (Replicator) host

It is not possible to remove a logical switch in Universal Synchronization Service (Replicator) host. *Fixed in 6.2.7.*

Fixed Issue 1799194: All NSX traffic egresses out of one NIC when IP Hash teaming is selected

When NSX portgroups are configured with an IP Hash teaming policy (Static EtherChannel or LACP), all traffic from those portgroups will egress out of a single NIC. This does not cause traffic loss, but network load is not distributed across all available links. On failure of the NIC in use, all NSX portgroups will fail over to another active NIC in the team. Ingress traffic is not affected, and can be received on all available links. *Fixed in 6.2.7.*

Fixed Issue 1814096: ESXi host crashes and routing problems observed when LIF uplink IP assigned to a VM or when LIF uplink IP edited with pencil icon

The purple diagnostic screen is encountered on hosts where the LIF IP is configured. DLR routing problems are faced when LIF IP is modified. *Fixed in 6.2.7.*

Fixed Issue 1843981: DLR ARP resolution for ECMP ESG fails.

ARP resolution at the DLR for the ECMP fails and impacts North-South traffic. *Fixed in 6.2.7.*

Fixed Issue 1798469: Some NSX Edges can get into split brain scenarios even if their Highavailability status is shown correctly

Due to a race condition in the HA mechanism, some NSX edges upgraded to NSX 6.2.5 and up could get into a split brain scenario even if their "Highavailability Status" is shown correctly. This could also happen after edge redeployment. *Fixed in 6.2.7.*

Fixed Issue 1806934: Openswan's CVE-2015-3240 causes Denial of Service (DoS)

IKE daemon in libreswan before 3.15 and Openswan before 2.6.45, when built with NSS, allow remote attackers to cause a denial of service (assertion failure and daemon restart) via a zero DH g^x value in a KE payload in an IKE packet. *Fixed in 6.2.7.*

Fixed Issue 1833934: All vCNS Edges (version 5.5.4) and NSX Edges (6.1.x and 6.2.x) running on VIX communication mode get unmanageable after storage vMotion

NSX Edges running with MessageBus as communication mode are not impacted. *Fixed in 6.2.7.*

Fixed Issue 1805819: VXLAN network ping test in the vSphere Web Client fails

When performing a ping test in the vSphere Web Client, the ping passes at times and fails at times. The received encaps debug packet gets dropped because of VLAN tag mismatch. *Fixed in 6.2.7.*

Fixed Issue 1829051: DLR-generated Directed ARP packets are getting dropped

In a multi-VTEP environment, DLR initiated directed ARP packet will be dropped if the DLR port and destination VM are mapped to different vmNIC. *Fixed in 6.2.7.*

Fixed Issue 1736112: When an NSX Edge ECMP interface is disabled then enabled through UI, the connected route is not added back

In ECMP path, The connected routes are not added back, if any one of the ECMP interfaces are disabled and then enabled via UI. *Fixed in 6.2.7.*

Fixed Issue 1674229: NSX Edge can experience connectivity issue under high traffic during force sync operation.

Fixed in 6.2.7.

Fixed Issue 1802313: Edge HA Failover from node 0 to node 1 takes longer than expected

Failover from node 0 to node 1 takes longer than expected in Edge HA configured environment whereas failover of traffic from node 1 to node 0 is normal. *Fixed in 6.2.7.*

Fixed Issue 1817952: Unable to modify tcp_max_orphans and tcp_mem settings in the systemcontrol/config Load Balancer API

Fixed in 6.2.7.

After the fix, you can modify two parameters simultaneously, for example:

```
<systemControl>
  <property>sysctl.net.ipv4.tcp_max_orphans=65536</property>
  <property>sysctl.net.ipv4.tcp_mem=65536 63355 62333</property>
</systemControl>
```

Note: The system control parameter sysctl.net.ipv4.tcp_mem must be 3 numbers, and use one or more blank space as separator.

Fixed Issue 1733146: Under certain conditions, creating or modifying LIFs for a Universal DLR fails when no NSX Edge Appliance (Control VM) exists. *Fixed in 6.2.7.*

Fixed Issue 1726379: If IP multicast range has an upper bound value exceeding 99 in the last three octets, VXLAN trunk portgroup configuration fails

While configuring segment ID, if you create a multicast IP range with an upper bound value exceeding 99 in the last three octets, for example, 1.100.100.100, and a multicast or hybrid logical switch with the same multicast IP range, VXLAN trunk portgroup configuration will fail. *Fixed in 6.2.7.*

NSX Manager Resolved Issues in NSX 6.2.7

Fixed Issue 1801286: Purge and Job data tables consuming a large amount of NSX manager disk space

Auto-vacuum settings are not optimized for large DB tables, resulting in NSX Manager disk space being consumed too rapidly. *Fixed in 6.2.7.*

Fixed Issue 1702592: VMs not communicating after controllers redeployed due to a mismatch in vmID between NSX Manager and vCenter Server

Fixed in 6.2.7.

Fixed Issue 1801338: NSX Manager database consumed 100% of /common partition causing NSX Manager services to fail

Fixed in 6.2.7.

Security Services Resolved Issues in NSX 6.2.7

Fixed Issue 1807067: UI Exported/saved DFW configuration does not store negated objects in NSX

The UI does not pass "excludeSource"/"excludeDestination" true while saving the configuration for negated objects such as Security Groups or individual objects such as virtual machines. *Fixed in 6.2.7.*

Fixed Issue 1807152: When a VM is moved from one cluster to another newly prepared cluster, rules having Virtual Wire as appliedTo are not applied to the VM.

When a new cluster is added to NSX, the cluster list for rules having Applied To as Virtual Wire is not updated. So, when a VM is migrated from old cluster to the newly prepared cluster, the rules are not applied. *Fixed in 6.2.7.*

Fixed Issue 1776981: DFW dropping packets related to split TCP handshake

Distributed Firewall does not handle the split TCP handshake properly. It ignores the Window Scale Option leading to future packet drops as the window calculation is incorrect. This was being caused by the first SYN ACK packet getting lost and the re transmission of the SYN was causing a Challenge ACK being generated which caused the split TCP Handshake. *Fixed in 6.2.7.*

Fixed Issue 1808132: NSX Threshold Monitoring is disabled by default to avoid a potential crash

When the Firewall module runs, NSX disables the threshold monitoring for memory to avoid a potential crash. When the host is running ESX 6.5P01 or ESX 6.0U3 or above, the memory threshold monitoring will be automatically enabled. *Fixed in 6.2.7.*

Fixed Issue 1727303: Publishing DFW Rules fails with timeout 301501 error if multiple IP addresses are set in single vNic with ARP or DHCP snooping enabled

When IP discovery through ARP or DHCP is enabled, NSX Manager will learn IP address from ESXi hosts and publish changes in address sets to hosts. Since learning cache per vNic can hold only one IP address, vNic with multiple IP address can send so many address set updates that ESXi cannot process rule set in time as well as address set. You will see publishing failure in vsm.log with error message: "Firewall provisioning failed on Host <host-id> for reason 301501." *Fixed in 6.2.7.*

Fixed Issues 1707931, 1733235: Order of distributed firewall rules changes when service policies defined in Service Composer are present, and a firewall rule is modified or published with a filter applied in the Firewall UI

Changing the order, adding or deleting service policies created in Service Composer after one or more publish operations are made from the Networking & Security > Firewall UI will cause the order of firewall rules to change and may result in unintended consequences. *Fixed in 6.2.7.*

The following issues were resolved in earlier 6.2.x releases:

General Resolved Issues in 6.2.6 and earlier

- **Issue 1715204: Windows 2008 event log server is added as "TYPE" of "WIN2K3", if serverType is not specified in REST API request body**
If you create EventLog server API request, the server will be added as "TYPE" of "WIN2K3". If you use EventLog server only for IDFW, IDFW may not work correctly. *Fixed in 6.2.4.*
- **Fixed Issue 1685375: Remote MAC is missing from VXLAN gateway**
Remote MAC addresses are not sent after a switch reload. In rare circumstances, the NSX controller may not populate the ovsdb MAC address tables again, when a HW VTEP gateway reboots. *Fixed in 6.2.5*
- **Fixed Issue 1696192: NTP sync issues on NSX Manager**
A newer version of fcron was introduced in NSX 6.2.3. There are no environment variables defined in the fcrontab which means that the environment is not initialized for fcron run jobs. The script is unable to locate the ntpdate command because the \$PATH is empty. *Fixed in 6.2.4.*
- **Fixed Issue 1644529: Security patch to address the security vulnerability, CVE-2016-2079**
The 6.2.3 release delivers a security patch to address [CVE-2016-2079](#).
- **Fixed Issue 1571156: vCenter 6.0 restart/reboot may result in duplicate VTEPs on VXLAN prepared ESX hosts**
See [VMware knowledge base article 2144605](#). *Fixed in NSX 6.2.3.*

- **Fixed Issue 1529665: The DaaS service is not working as the service using 2 different VIPs (one VIP for HTTP and another for PCoIP) that must have exactly the same persistency**
This issue has been fixed in 6.2.1.
- **Fixed Issue 1631261: IDFW is configured to work with Log Scraper and GI is also installed, after un-installing the GI, IDFW stops working**
Fixed in NSX 6.2.2.
- **Fixed Issue 1551773: Edge Security Gateway (ESG) HA vNIC dropdown selection is always empty in VMware NSX for vSphere 6.2.0**
Fixed in NSX 6.2.2. See [VMware knowledge base article 2138158](#).
- **Fixed Issue 1608608: Security patch to address the glibc vulnerability, CVE-2015-7547**
The 6.2.2 release delivers a security patch to address [CVE-2015-7547](#).
- **Fixed Issue 1480581: netcpa sockets are CLOSED and VM fails to communicate across VNIs, subnets**
This issue was fixed by fixing thread unsafe use of boost::asio in vmacore. Fixed in NSX 6.2.2. See [VMware knowledge base article 2137011](#).
- **Fixed Issue 1583566: Rules not pushed to host**
DFW rule/ip list updates failed to be scheduled due to task framework resource limitations in NSX Manager. Error message showed a failure to queue tasks for Change Notification threads. This has been fixed in NSX 6.2.2.
- **Fixed Issue 1573818: Traffic interrupted for 50 seconds after HA failover on ESG**
This issue was caused when NSX failed to synchronize the static routes among the HA NSX Edge nodes. Fixed in NSX 6.2.2.
- **Fixed Issue 1570808: NSX load balancer IP_HASH health check issue**
In IPVS, when using the source-ip hash algorithm, if the selected backend server's weight equals 0, a "service unavailable" reply is sent even if there are healthy backend servers. This has been fixed in NSX 6.2.2.
- **Fixed Issue 1564005: In NSX NetX, cannot add rules to redirect traffic to partner devices**
Customers were unable to add traffic redirection rules to their NetX rule sets. As a result, customers were unable to redirect traffic to partner devices. This affected rules that used IP address sets. This issue was caused by incorrect handling of IP ranges in the NetX rules. Fixed in NSX 6.2.2.
- **Fixed Issue 1587660: NSX NetX error in DVFilterProcessSlowPathPackets**
Using NSX NetX without DFW resulted in an error in DVFilter. The full error message indicated NetX error PF (err=11,cr2=0x10) in DVFilterProcessSlowPathPackets: VSIPDVFPProcessSlowPathPackets: PFilterPacket. Fixed in NSX 6.2.2. See [VMware knowledge base article 2144018](#).
- **Fixed Issue 1591673: Adding ESXi host to vSphere Distributed Switch fails with license error**
In NSX 6.2.1 only, adding an ESXi host to a vSphere Distributed Switch failed with license error: "Host IP address is not licensed for the VDS feature. Cannot add this host to dvSwitch." For details, see [VMware knowledge base article 2143397](#). Fixed in NSX 6.2.2.
- **Fixed Issue 1590563: Enterprise license error after upgrade**
The NSX 6.2.1 upgrade routine allowed you to upgrade to 6.2.1 without a VMware Enterprise License, but after upgrade, the Enterprise License was required in order to use NSX. Fixed in NSX 6.2.2. See [VMware knowledge base article 2135310](#).
- **Fixed Issue 1589046: Packet sent to LIF without DHCP relay results in PSOD**
The ESXi host suffers a PSOD if a DHCP unicast packet is addressed to the IP of a LIF that is expected to have DHCP relay enabled but the actual receiving LIF does not have DHCP relay enabled. This has been fixed in NSX 6.2.2. See [VMware knowledge base article 2144314](#).
- **Fixed Issue 1593436: In VXLAN hybrid mode, controller disconnection incorrectly triggers fallback to multicast mode**
Fixed in NSX 6.2.2. See [VMware knowledge base article 2144457](#).
- **Fixed Issue 1574995: DFW Publishing error**
Modifying and saving DFW rules in filtered mode may result in rules not being saved and published. Fixed in NSX 6.2.2. See [VMware knowledge base article 2141155](#).
- **Fixed Issue 1422110: One of the NSX Controllers does not hand over master role to other controllers when it is shut down**
Fixed in NSX 6.1.5 and NSX 6.2.1.

- **Fixed Issue 1483728: Control plane connectivity fails for NSX Controller**
Control plane connectivity was seen to fail for a Controller, showing an error in netcpa related to txInProgress. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- **Fixed Issue 1487910: Upgrading Edge Services Gateway fails with "Timed out waiting for Edge vm" message**
Applying an IPv6 address to the NSX management interface causes NSX Manager to use the host name. The vsfwd proxy which connects the Edge VM to NSX Manager does not correctly handle a FQDN, resulting in an error similar to "ERROR TaskFrameworkExecutor-6 AbstractEdgeApplianceManager:185 - Timed out waiting for Edge vm {}. Vm took too long to boot and respond com.vmware.vshield.edge.exception.VshieldEdgeException". *This has been fixed in NSX 6.2.0.*
- **Fixed Issue 1571548: In NSX for vSphere release 6.2.0 and later, if a VTEP IP address is changed directly on a host or in VC, the old IP address of the VTEP is released automatically.**
Fixed in NSX 6.2.0.
- **Fixed Issue 1551164: NSX User Interface (UI) is grayed out for several seconds and exhibits slow performance on NSX for vSphere 6.2.0**
See [VMware knowledge base article 2141919](#). *Fixed in NSX 6.2.1.*
- **Fixed Issue 1545840: Cannot disable the NSX distributed firewall (DFW) on a host in VMware NSX for vSphere 6.x**
See also [VMware knowledge base article 2141915](#). *Fixed in NSX 6.2.1.*
- **Fixed Issue 1528680: VMware ESXi 5.x and 6.x experiences a purple diagnostic screen when using IP discovery in VMware NSX for vSphere 6.2.0 (KB 2134329)**
When using IP discovery on logical switches in VMware NSX for vSphere 6.2.0, the ESXi 5.x and 6.x host fails with a purple diagnostic screen as explained in [knowledge base article 2134329](#). *Fixed in NSX 6.2.1.*
- **Fixed Issue 1545885: Manage option on Security Tag portlet is grayed out by default**
On a Virtual Machine's summary page, the "Manage" hyperlink on the security tag portlet remains grayed out till the user creates a new security tag. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1476087: Some Controller logs not available for syslog export.**
Controller logs, including Zookeeper clustering logs, are not part of syslog export. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1545830: ESXi 6.0 PSOD on vdl2 when pinging with data size higher than available data size for the MTU**
Starting ping from NSX host switch attached vmknix will lead to host PSOD if data size is greater than MTU. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1545873: Users needed to configure same IP address and port number for both TCP and UDP protocol**
This release resolves the following issues as well:
 - UDP virtual server without pool configuration leads to configuration failure.
 - Statistics shows incorrect data when UDP virtual server is not associated with any pool.

Fixed in NSX 6.2.1. With 6.2.1 release, users can use the same IP address and port number for both TCP and UDP with/without a pool associated.

Install and Upgrade Resolved Issues in 6.2.6 and earlier

- **Fixed Issues 1767149/1782802: If there is a cipher chain listed that is separated by commas (","), then upgrade from NSX for vSphere 6.1.x, 6.2.0, and 6.2.1 to NSX for vSphere 6.2.5 fails**
Starting 6.2.6, you can separate the ciphers with colons (":") instead of commas (",") before upgrade. *Fixed in 6.2.6.*
- **Fixed Issue 1710454: HA Dead Time inconsistency between newly deployed and upgraded DLRs**
This issue occurred because the newly upgraded DLRs HA Dead Time are explicitly being changed from 15 seconds to 6 seconds during upgrade. Refer to the [VMware knowledge base article 2146714](#). *Fixed in 6.2.4.*
- **Fixed Issue 1578509: After EAM restart, Guest Introspection(GI) Service status is in warning state**
Fixed in NSX 6.2.3.
- **Fixed Issue 1539203: After NSX upgrade, NSX plugin gets disconnected from primary VC during a Cross-vCenter Upgrade**
Fixed in NSX 6.2.3.

- **Fixed Issue 1558017: After upgrading the NSX Edge from 6.1.x to 6.2.x, the NSX Manager vsm.log shows "INVALID DHCP CONFIG"**
If you have an interface with an IPv6 subnet, DHCP generates an empty shared subnet and treats it as an invalid operation.
- **Fixed Issue 1490496: After NSX upgrade, Guest Introspection fails to communicate with NSX Manager**
After upgrading from NSX 6.0.x to NSX 6.1.x or from NSX 6.0.x to NSX 6.2 and before the Guest Introspection service is upgraded, the NSX Manager cannot communicate with the Guest Introspection Universal Service Virtual Machine (USVM). *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- **Fixed Issue 1536179: SSL VPN-Plus client cannot be installed on Mac OS X Yosemite and higher**
Earlier versions of Mac OS X are supported. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1393503: After upgrading NSX vSphere from 6.0.7 to 6.1.3, vSphere Web Client crashes on login screen**
After upgrading NSX Manager from 6.0.7 to 6.1.3, you will see exceptions displayed on the vSphere Web Client UI login screen. You will not be able to login and perform operations on either vCenter or NSX Manager. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1088497: Guest Introspection installation fails with error**
When installing Guest Introspection on a cluster, the install fails with the following error:
Invalid format for VIB Module. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1328589: DVPort fails to enable with "Would block" due to host prep issue**
On an NSX-enabled ESXi host, the DVPort fails to enable with "Would block" due to a host preparation issue. When this occurs, the error message first noticed varies (for example, this may be seen as a VTEP creation failure in VC/hostd.log, a DVPort connect failure in vmkernel.log, or a 'SIOCSIFFLAGS' error in the guest). This happens when VIBs are loaded after the vSphere Distributed Switch (vDS) properties are pushed by vCenter. This may happen during upgrade. See [knowledge base article 2107951](#). *Fixed in NSX 6.2.0.*
- **Fixed Issue 1446544: Attempts to delete existing NSX Edge Gateway fail in an environment upgraded to NSX 6.1.4**
In NSX installations upgraded from 6.1.3 to 6.1.4, the existing NSX Edge Gateways cannot be deleted after the upgrade to 6.1.4. This issue does not affect new Edge Gateways created after the upgrade. Installations that upgraded directly from 6.1.2 or earlier are not affected by this issue. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1418836: The AES encryption unavailable when performing an NSX backup using third-party secured FTP backup.** *Fixed in NSX 6.2.0.*
- **Fixed Issue 1410153: NSX Manager UI does not display user-friendly error messages during host reboot**
In this 6.2 release, NSX Manager UI is updated to display detail error messages that describe the problems you might encounter during host reboot and provide possible solution. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1412133: Unable to install NSX VIB installation**
The installation of NSX VIB might not complete, as expected if the ixgbe driver fails to load from third-party module because it has been locked and prevents it from being used for installation. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1467438: Unable to start NSX Manager service after upgrading from vCloud Networking and Security (vCNS) 5.5.3**
After upgrading vCloud Networking and Security (vCNS) 5.5.3 to NSX 6.1.3, the NSX Manager service hangs and is unable to start successfully. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1440867: The message bus randomly does not start after NSX Edge reboot**
After restarting an Edge VM, the message bus often does not start after powering on, and an additional reboot is required. *Fixed in NSX 6.2.0.*

NSX Manager Resolved Issues in 6.2.6 and earlier

- **Fixed Issue 1668519: High CPU utilization on NSX Manager**
NSX Manager may experience sustained high CPU, especially after a reboot, when the purgetask process must process or clean up a very large volume of job entries on the NSX Manager database.
Workaround: Contact VMware technical support. See [VMware knowledge base article 2145934](#). *Fixed in 6.2.4.*
- **Fixed Issue 1603954: NSX Manager displays memory utilization at almost 100% constantly**
Reboot of NSX Manager drops the memory utilization to significantly lower than 100%, however over time the utilization value raises back up to 100% and the display remains at that level. *Fixed in 6.2.4.*

- Fixed Issue 1540187: Users cannot login through vSphere Web Client and use NSX plugin, giving out error that user/group does not have permissions**
 This issue had dependency on the timeout that happens when saml token is being generated. At times when the request operation does not complete when communicating with SSO service, NSX is not able to refresh solution registration provider internally. This causes null pointer exception for every other request once this happens.
Fixed in NSX 6.2.3 by avoiding null pointer exception and reconnecting to the SSO service if required.
- Fixed Issue 1640388: While uninstalling Guest Introspection from a cluster that does not contain any VM, an error message "Pre-Uninstall cleanup failed" appears, and the status is displayed as unresolved**
 This was a known issue in the uninstall logic of Guest Introspection.
Fixed in NSX 6.2.3.
- Fixed Issue 1534588: Previous backups are not displayed in the NSX Manager UI**
 Running a backup operation never shows a successful completion at the NSX Manager UI. Either one of these issues may manifest if a large number of backup files are stored in the destination folder. Each backup file has to be checked for compatibility before displaying the list on the same page. The current file list process can cause the page to timeout.
Fixed in NSX 6.2.3.
- Fixed Issue 1593910: Duplicate NSX Manager IP address is not detected or prevented**
 If the NSX Manager IP address is assigned to another device on the network, an explicit error or event log is not generated. As a result, NSX controllers and hosts may respond to NSX Manager using an incorrect MAC address, causing a data path outage. *Workaround:* Attempt to determine and then remove the other network device from the network or assign it a different IP address. Due to presence of duplicate NSX manager IP in the network, hosts and Controllers are responding to NSX Manager/VM using the wrong MAC address. This affects communications between NSX Manager and ESX and between NSX Manager and NSX Controllers. This can result in a datapath outage. In this case applications are impacted until the duplicate IP is removed from the network and communication channels are restored.
Fixed in NSX 6.2.3 by adding a system event when a duplicate IP address is detected.
- Fixed Issue 1489648: NSX is unavailable from the vSphere Web Client Plug-in after taking a backup of NSX Manager with quiesced snapshot**
 See [VMware knowledge base article 2142263](#). *Fixed in NSX 6.2.3.*
- Fixed Issue 1440451: NSX Manager certificate replacement requires restart of NSX Manager and may require restart of vSphere Web Client**
 After you replace the NSX Manager appliance certificate, you must always restart the NSX Manager appliance. In certain cases after a certificate replacement, the vSphere Web Client will not display the "Networking and Security" tab.
- Fixed Issue 1568861: Unable to add secondary NSX Manager if GUI is Japanese language on Firefox browser**
 When adding a secondary NSX Manager with German, Japanese, Korean, or French locale and a Firefox browser, the thumbprint dialog is not shown, blocking the configuration.
- Fixed Issue 1482989 / 1522092: NSX Networking and Security shows all hosts as GREEN but Cluster status incorrectly shown as RED**
 In NSX 6.1.4 and earlier, under rare conditions the NSX Networking and Security tab showed all hosts as GREEN but incorrectly showed the Cluster status as RED (incorrectly indicating an error condition). *Fixed in NSX 6.1.5.*
- Fixed Issue 1515656: NSX Manager CPU utilization is high after adding it to Active Directory domain**
 NSX Manager CPU utilization is high after adding it to Active Directory domain. In the system logs of the NSX Manager, multiple Postgres threads are seen as running. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- Fixed Issue 1484939: Unable to register NSX Manager 6.1.4 with vCenter, gives error: NSX Management Service operation failed**
Fixed in NSX 6.1.5 and NSX 6.2.1.
- Fixed Issue 1521710: NSX Manager web client displays error: Code 301002**
 Description: When you navigate to NSX manager > Monitor > System Events, the web client displays the following message: Filter config not applied to vnic. Code 301002. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- Fixed Issue 1479665: Starting in 6.2.1, NSX Manager queries each controller node in the cluster to get the connection information between that controller and the other controllers in the cluster**
 This is provided in the output of the NSX REST API ("GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller" command), which now shows the peer connection status between among the controller nodes. If NSX Manager finds the connection between any two controller nodes is broken, a system event is generated to alert the user. *Fixed in NSX 6.2.1.*

- **Fixed Issue 1525516: Force-sync of controller is broken if backup-restore of manager is done on another appliance**
If an NSX Manager appliance is cloned and/or restored from a backup, a force-sync operation to an NSX controller cluster will fail. This issue does not occur for an NSX Manager deployed from scratch. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1509454: NSX logging heartbeat failures for hosts that are not part of the NSX installation**
When an NSX-prepared host is directly removed from the vCenter inventory (without first unpreparing it in NSX), NSX receives an unexpected 'Host Connected' DCN which causes partial removal of messaging infrastructure components from the host. As a result, the messaging link between NSX and the host may remain active when it should have been removed, and NSX may raise false 'Alert' SystemEvents for the host. Fixed in NSX 6.2.1. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1418655: NSX Manager is non-functional after running the write erase command**
When you restart the NSX Manager after running the write erase command, you might notice that the NSX Manager is not working as expected, such as the password to access the Linux shell has been reset, the setup command is missing, and so on. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1366669: Add Domain shows error at LDAP option with Use Domain Credentials**
In NSX 6.1.x, the user when trying to add an LDAP domain, the web client gave a User Name was not specified error, even when Username was provided in UI. Fixed in NSX 6.2.0. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1352169: CA signed certificate import needs an NSX Manager reboot before becoming effective**
When you import an NSX Manager certificate signed by CA, the newly imported certificate does not become effective until NSX Manager is rebooted. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1497113: Unable to import NSX Manager to LDAPS domain**
When you attempt to add NSX manager to LDAPS domain, the following error message appears.
Cannot connect to host <Server FQDN>
error message: simple bind failed: <Server FQDN:Number>. *Fixed in NSX 6.2.0.*

Logical Networking and NSX Edge Routing Resolved Issues in 6.2.6 and earlier

- **Fixed Issues 1663902, 1717370: Performing any UPDATE/PUT operations on an ESG/DLR during production can impact traffic for a short period of time**
You will see traffic disruptions for a short period of time if you perform any UPDATE/PUT operations on an ESG/DLR during production. *Fixed in 6.2.5.*
- **Fixed Issue 1737807, 1703913: VMs lose network connectivity in NSX with DLR HA**
In an NSX environment using dynamic routing with High Availability (HA) configured on a DLR Control VM, virtual machines lose network connectivity when the DLR control VMs recover from a split-brain condition (both the primary and secondary DLR HA nodes remain in *Active* state concurrently). *Fixed in 6.2.5*
- **Fixed Issue 1717369: When configured in HA mode, both active and standby Edge VMs may be deployed on the same host**
This issue results from anti-affinity rules not being created and applied on the vSphere hosts automatically during redeploy and upgrade operations. This issue will not be seen when HA is being enabled on existing Edge. *Fixed in 6.2.5.*
- **Fixed Issue 1717371: NSX Edge virtual machines do not failover during a vSphere HA event**
When NSX Edges are installed or redeployed on a vSphere cluster which has vSphere HA enabled, during NSX Edge deployment NSX Manager enables the autostart manager for the ESX host on which the Edge is getting deployed. This is not compatible with vSphere HA and as a result vSphere does not provide HA for the Edge VM. *Fixed in 6.2.5.* See [Upgrade note regarding Automatic Startup Manager](#).
- **Fixed Issue 1606785, 1736095: NSX Edge Load Balancer may fill the /var/log/ partition with the nagios.log file messages**
/var/log partition becomes full on NSX Edge Load Balancer. *Fixed in 6.2.5.*
- **Fixed Issue 1696887: VMs lose network connectivity north of logical distributed router**
If a VM learns the pMac of the logical router as the MAC address for default gateway instead of the generic logical router MAC address, it loses connectivity north of the logical router.
Workaround: See [VMware knowledge base article 2146293](#). *Fixed in 6.2.4*
- **Fixed Issue: Data path issues for VNIs with disconnected NSX Controller**
This issue occurs because IPsec re-keying is disabled in NSX-V 6.1.5, 6.1.6, 6.2, 6.2.1 and 6.2.2 releases to avoid hitting a another known IPsec issue.

See [VMware knowledge base article 2146973](#). Fixed in NSX 6.2.3.

- **Fixed Issue 1591582: In some corner conditions ARP requests sent by VDR instance might get dropped**
VDR ARP requests for remote VMs located on other hosts may get dropped at VDR uplink output processing, causing slow connection establishment.
- **Fixed Issue 1501900: Edge OSPF router remains stuck in ExchangeStart state after changing OSPF interface IP address**
Due to a race condition, changing the IP address on an OSPF interface was causing the OSPF neighbors to remain stuck in ExchangeStart state on both sides. Under normal conditions, it is a supported operation to change the OSPF interface IP address.
Fixed in NSX 6.2.3.
- **Fixed Issue 1498251: IS-IS is not a supported routing protocol for the Edge Services Gateway router**
The references to IS-IS are removed from the UI and APIs in NSX 6.2.3.
- **Fixed Issue 1492738: Unable to add more than eight uplink interfaces during Distributed Logical Router (DLR) deployment using vSphere Web Client**
Fixed in NSX 6.2.3.
- **Fixed Issue 1552038: Intermittent loss of connectivity from NSX Edge to DLR uplink interface**
This issue was caused by the NSX Edge having the DLR NSX Edge Appliance (Control VM)'s MAC address in its ARP table rather than the local instance MAC address of the DLR. This release adds an outbound ARP filter to prevent the DLR control VM from generating ARPs related to the DLR IP address.
- **Fixed Issue 1454161: Static routes with a next hop as a /31 IP address cannot be configured**
Fixed in NSX 6.2.3.
- **Fixed Issue 1528443: VXLAN ARP cache on the hosts not being updated when an Edge VM sends a GARP during failover**
In certain deployments where the VM's and Edge are on the same VXLAN segment, VXLAN ARP cache on the host won't get updated after the Edge failover. *Fixed in NSX 6.2.3.*
- **Fixed Issue 1600874: Stranded VMs are not removed when new Edge VM is being deployed**
When upgrading an Edge, if the publish operation and roll back operations both fail, the original Edge VM remains in the NSX Manager database, while VC retains the new Edge VM's ID number. Due to this mismatch, redeploying an Edge VM will fail. A force sync also will fail with a "VM not found" error.
- **Fixed Issue 1467774: Incorrect value shown for admin distance field in "show ip bgp neighbor" command**
A route learned from a EBGP peer and advertised to an IBGP peer in the same AS incorrectly retains the previous admin distance. This issue has been fixed in 6.2.3.
- **Fixed Issue 1613383: For an NSX Edge Load Balancer running in L4 mode, the current connections value incorrectly used the total connections number**
This release fixes the issue by calculating the current connections using a sum of the active connections. This issue has been fixed in 6.2.3.
- **Fixed Issue 1584664 : If load balancer pool VM members are removed manually from the vCenter inventory without first being unconfigured in NSX, orphan database entries are left behind in the NSX Manager database. An ObjectNotFoundException will be reported in the NSX Manager logs.**
This issue has been fixed in 6.2.3.
- **Fixed Issue 1446809: NSX Edge can no longer be managed by vCloud Director if no health check recovery event is sent after an Edge reboot**
NSX Manager saves Edge connectivity status in memory. When an Edge VM fails to respond to a health check, a miss event is raised, and on recovery, a recovered event is raised. If NSX Manager is restarted, the recovery event may not be sent if no health checks were missed after the reboot. As vCloud Director depends on these events, a missed recovery event can lead to an unmanageable Edge VM from vCD.
- **Fixed Issue 1462506: Cannot redeploy NSX Edge with L2VPN Service configured with CA-signed certificate**
Cannot redeploy or change size of NSX Edge with L2VPN Service configured with CA-signed or self-signed certificate. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- **Fixed Issue 1441319: Connectivity loss after removing a logical interface (LIF) in installations with dynamic routing**
A problem was identified in the NSX Logical Router (Edge/DLR) when using dynamic routing (OSPF & BGP) that

will cause network connectivity loss after removing a LIF. This affects NSX versions 6.0.x through 6.1.4. *Fixed in NSX 6.1.5 and NSX 6.2.1.*

- **Fixed Issue 1399863: When the direct aggregate network in local and remote subnet of an IPsec VPN channel is removed, the aggregate route to the indirect subnets of the peer Edge also disappears**
When there is no default gateway on Edge and you remove all of the direct connect subnets in local subnets and part of the remote subnets at the same time when configuring IPsec, the remaining peer subnets become unreachable by IPsec VPN. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1445291: RADIUS authentication server configuration fails on NSX Edge**
In NSX 6.1.5 and earlier, the RADIUS server secret key string had a 32-character limit; if the string exceeded this character limit, the RADIUS server failed to connect with the NSX Edge. The limit is now 64 characters. *This was fixed in NSX 6.2.0.*
- **Fixed Issue 1534811: VIO Heat stack deployment fails intermittently for the VMware NSX for vSphere 6.x Edge with the error: Cannot allocate memory**
Health monitoring memory usage increases over time, eventually causing edge failure. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1500624: BGP filters are taking approximately 40 seconds to be effectively applied**
During this period all the redistribution policies are applied without filters. This delay applies only to NSX Distributed Logical Router (DLR) for OUT directions. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1484758: On NSX Edge subinterfaces, ICMP redirects are sent out, even when the Send ICMP redirect option is disabled**
By default, NSX Edge subinterfaces have Send ICMP redirect disabled. Although this option is disabled, ICMP redirects are sent out on edge subinterfaces. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1265605: Cannot add non-ASCII characters in bridge or tenant name for logical router**
NSX controller APIs do not support non-ASCII characters. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1341784: When a BGP neighbor filter rule is modified, the existing filters may not be applied for up to 40 seconds**
When BGP filters are applied to an NSX Edge running IBGP, it may take up to 40 seconds for the filters to be applied on the IBGP session. During this time, NSX Edge may advertise routes which are denied in the BGP filter for the IBGP peer. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1422110: One of the NSX Controllers does not hand over master role to other controllers when it is shut down**
Typically, when a controller assumes operations master role and is preparing to shut down, it automatically hands over the master role to other controllers. In this case, the controller fails to hand over the role to other controllers and the status becomes interrupted and then goes into disconnected mode. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1440790: Unable to pass VXLAN traffic between hosts with unicast or multicast**
When VMs are on the same host they can communicate across VXLAN with unicast or multicast, but cannot communicate when VMs are on different hosts. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1432420: Removing multiple BGP rules on NSX Edge/DLR at the same time causes web client to crash.** *Fixed in NSX 6.2.0. You can now delete multiple BGP rules at a time.*
- **Fixed Issue 1431716: Protocol address is briefly displayed after adding Border Gateway Protocol (BGP) deny rule**
You might notice that the protocol address is briefly displayed after adding Border Gateway Protocol (BGP) deny rule in NSX Edge services gateway. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1441773: VMs disconnect during vMotion**
You might notice that VMs disconnect during vMotion or you might receive alerts for VMs with disconnected NICs. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1463579: Unable to download controller snapshot**
When downloading controller snapshots, you might notice that you are unable to download snapshot for the last controller. For example, if you have three controllers, one can successfully download snapshots of the first two but you might fail to download snapshot of the third controller. *Fixed in NSX 6.2.0.*

Edge Services Resolved Issues in 6.2.6 and earlier

- **Fixed Issue 1722988: NSX Edge OpenSSL package is not updated to 1.0.2j**
In 6.2.6, NSX Edge OpenSSL package is updated to 1.0.2j. *Fixed in 6.2.6.*

- **Fixed Issue 1777121: High volume of MAC learning table updates with NSX L2 bridge and LACP may lead to out of memory condition**
When an NSX L2 bridge sees a MAC address on a different uplink, it reports a MAC learning table change to controllers via the netcpa process. Networking environments with LACP will learn the same MAC address on multiple interfaces, resulting in a very high volume of table updates and potentially exhausting the memory needed by the netcpa process to do the reporting. See [VMware Knowledge Base article 2147181](#). *Fixed in 6.2.5.*
- **Fixed Issue 1771285: Multicast IP is not set on host for bridged VXLAN network during controller sync operation, causing control plane connection to fail**
Control Plane is marked 'inactive' resulting in traffic disruption whenever controller sync is triggered in any of the following ways:
 - VDR is redeployed, upgraded, or made to force sync
 - VSM level controller state sync
 - Controller is rebooted or disconnected and connected back*Fixed in 6.2.5.*
- **Fixed Issue 1766624: Random packet drops when traffic goes through a bridge DLR on NSX**
Random packet drops when traffic goes through a bridge DLR on NSX with the ping command displaying numerous Request Timed Out messages. *Fixed in 6.2.5.*
For more information, see [VMware Knowledge Base article 2148175](#).
- **Fixed Issue 1779313: Connectivity outage after reboot of NSX Manager**
A connectivity outage was seen after reboot of NSX Manager. This happened because distributed logical router (DLR) instances were purged from ESX host due to incorrect partial sync of VDR. When this bug occurred, the NSX environment could be recovered by Force Syncing the VXLAN/routing service. *Fixed in 6.2.5.*
- **Fixed Issue 1730633: Incorrect monitor status when using grouping object**
The CLI is not showing the monitor status correctly when using grouping object. *Fixed in 6.2.5.*
- **Fixed Issue 1745928: NTLM authentication fails with no option http-server-close application rule configured**
If you configure the application rule no option http-server-close, NTLM authentication fails. *Fixed in 6.2.5*
- **Fixed Issue 1736941: NSX Edge Firewall Web Client very slow**
NSX Edge Firewall Web Client sluggish when scrolling through the Edge Firewall rules grid. *Fixed in 6.2.5.*
- **Fixed Issue 1729066: Edge SCSI disk timeout not applied.**
Edge SCSI disk timeout was not applied due to incorrect boot script file permissions. *Fixed in 6.2.5.*
- **Fixed Issue 1649098: DHCP Relay Agents do not function in NSX**
If the DHCP server is more than 10 hops away, the TTL expires in transit and DHCP packets do not arrive at the configured relay server. *Fixed in 6.2.5.*

Security Services Resolved Issues in 6.2.6 and earlier

- **Fixed Issue 1767402: DFW rules with "Applied To" set to a "Security Group" are not published to hosts**
DFW rules with the "Applied To" field set to Security Group are not pushed to ESXi hosts in a new cluster. *Fixed in 6.2.5.*
- **Fixed Issue 1760081: The Netx/Service profile rules do not show up on the hosts after publishing**
In scaled environments, the processing of the Netx/Service profile rules-set takes hours to take effect on the hosts after publishing new or modified rules. *Fixed in 6.2.5.*
- **Fixed Issue 1738421: DFW controller exits unexpectedly in response to an invalid address for a VM's NIC**
Under rare conditions, a vCenter administrator can set an invalid address for a VM's NIC and cause the DFW controller process to exit unexpectedly. *Fixed in 6.2.5.*
- **Fixed Issue 1723946: Deleted rules getting converted into ANY ANY rules momentarily.**
In a highly concurrent rule provisioning system where rules are getting modified or deleted, a rule which is being added and deleted subsequently in the next call might get published momentarily as an ANY ANY rule until the delete operation is carried out. *Fixed in 6.2.5.*
- **Fixed Issue: 1738588: Some VMs not added to a security group**
Sometimes VMs are not added to a security group with dynamic criteria until some activity refreshes the group

membership. *Fixed in 6.2.5.*

- **Fixed Issue 1733763: NSX Distributed Firewall applies incorrect TFTP ALG**
The NSX Distributed Firewall applies incorrect TFTP ALG while processing a TCP session on port 69. *Fixed in 6.2.5.*
- **Fixed Issue 1738419: Invalid address for VM's NIC causes the DFW controller process to exit**
In rare cases, a vCenter administrator can set an invalid address for a VM's NIC and cause the DFW controller process to exit unexpectedly. *Fixed in 6.2.5.*
- **Fixed Issue 1704661, 1739613: VMs lose network connectivity with the error: "Failed to restore PF state: Limit exceeded"**
VMs lose network connectivity with the error: "Failed to restore PF state: Limit exceeded." *Fixed in 6.2.5.*
- **Fixed Issue 1732337, 1724222: NSX Manager fails to push firewall rules to ESXi 6.0 P03 host**
NSX Manager fails to push firewall rules to ESXi 6.0 P03 host, and NSX Edge health check fails. *Fixed in 6.2.5.*
- **Fixed Issue 1460363: Standalone NSX Manager incorrectly allows import of universal firewall configuration**
On an NSX Manager running in stand-alone mode, universal firewall rules can be imported even though they do not apply. Once imported, these rules cannot be deleted via API or the Web Client. Instead, they are retained and treated as a local section. *Fixed in 6.2.5.*
- **Fixed Issue 1674721: NSX Edge is unmanageable after upgrading to NSX 6.2.3**
This issue occurs when serverSsl or clientSsl is configured in load balancer, but cipher's value is set as NULL in the previous version.
Workaround: Refer to the [VMware knowledge base article 2145887](#). *Fixed in 6.2.4.*
- **Fixed Issue 1698389: After changing certain routing configurations via the vSphere Web Client, routing configuration is incorrect**
Sorting then editing causes an incorrect configuration when editing BGP neighbors, OSPF Area to Interface mapping, Route Redistribution – IP Prefixes, or BGP Filters. When a large number of BGP neighbors are configured, scrolling through the list, then editing can cause an incorrect configuration.
Workaround: Refer to the [VMware knowledge base article 2146363](#). *Fixed in 6.2.4.*
- **Fixed Issue 1633694: Storage failure may induce loss of VXLAN configuration in the NSX Manager database**
After a storage failure, Virtual Center may report that the DVS is deleted, and NSX Manager responds by removing the VXLAN configuration associated with the DVS. When this condition occurs, a message similar to "INFO DCNPool-9 VcDriver:1077 - Deleting vmknix info from host tables [host-21843 : 319]" will be printed in the NSX Manager logs. *Fixed in NSX 6.2.3.*
- **Fixed Issue 1456172: NAT does not translate IP addresses when NSX Edge firewall is disabled**
When the Edge gateway firewall is disabled, all stateful services also are disabled if the Edge device is a 6.0 Extra Large or 6.1 and 6.2 Edge device. *NSX 6.2.3 release adds a warning at the UI that other stateful services also are disabled.*
- **Fixed Issue 1499601: Extended HA failover times for Edge Services Gateway (ESG) or DLR with Edge VM when using only static routes**
Fixed in NSX 6.2.3.
- **Fixed Issue 1618289: Unexpected TCP interruption on TCP sessions during Edge High Availability (HA) failover in VMware NSX for vSphere 6.2.x**
This issue occurred due to outdated internal libraries that are used in VMware NSX for vSphere 6.2.x. *Fixed in NSX 6.2.3.*
- **Fixed Issue 1653484: NSX Edge core dumps did not display function names**
NSX 6.2.3 enhances debugability by displaying memory address information in the core file. However, you must enable core dumps only when requested by VMware technical support. *Fixed in NSX 6.2.3.*
- **Fixed Issue 1604506: Cannot deploy DLR without NSX Edge VM if using default gateway for static routing use case**

When deploying a new Distributed Logical Router (DLR) through the Web Client, by selecting the "Configure Default Gateway" option during configuration, the DLR fails to create and the following error appears as a pop-up window: "[Routing] Admin Distance is supported only on NSX Edge version 6.2.0 and later with NSX Edge VMs deployed".

See the [VMware knowledge base article 2144551](#) for more information. *Fixed in NSX 6.2.3.*

- **Fixed Issue 1445057: OSPF routes configured on NSX Edge Services Gateway (ESG) not honored in the logical router (DLR), and affected packets are dropped**

The problem occurs in cases when OSPF uses IP_HDRINCL option. On certain Linux kernels, when this option is present, it prevents the IP stack from fragmenting the packets. Hence, any packets greater than the interface MTU are dropped. *Fixed in NSX 6.1.5 and NSX 6.2.1.*

Fixed Issue 1406471: Syslog shows host name of backed up NSX Manager on the restored NSX Manager

Suppose the host name of the first NSX Manager is A and a backup is created for that NSX Manager. Now a second NSX Manager is installed and configured to the same IP address as the old Manager according to backup-restore docs, but host name is B. Restore is run on this NSX Manager. The restored NSX Manager shows host name A just after restore and host name B again after reboot. *Fixed in NSX 6.1.5 and NSX 6.2.1.*

- **Fixed Issue 1444581: ESXi host might lose network connectivity**

An ESXi host might lose network connectivity and experience stability issues when multiple error messages similar to the following are logged in:

WARNING: Heartbeat: 785: PCPU 63 didn't have a heartbeat for 7 seconds; *may* be locked up. *Fixed in NSX 6.1.5 and NSX 6.2.1.*

- **Fixed Issue 1444784: VMs disconnect during vMotion**

VMs disconnect during vMotion on 6.0.8 with message, VISIP heap depleted. *Fixed in NSX 6.1.5 and NSX 6.2.1.*

- **Fixed Issue 1440867: The message bus randomly does not start after NSX Edge reboot**

After restarting an Edge VM, the message bus often does not start after powering on, and an additional reboot is required. *Fixed in NSX 6.1.5 and NSX 6.2.1.*

- **Fixed Issue 1548939: When configuring a virtual server, the previously selected IP address is applied**

When creating a new virtual server, you might notice that the IP address is automatically applied from the list of previously selected IP pool. This happens when you have previously selected an IP pool to derive the Virtual Server IP. When you attempt to edit the virtual server IP Pool information, the information is not automatically sent to the backend from the UI and previous IP address derived from the IP Pool is automatically applied. *Fixed in NSX 6.2.1.*

- **Fixed Issue 1599706: SYN/ACK packet lost in communication over LDR between two VNIs**

Fixed in NSX 6.2.2.

- **Fixed Issue 1082549: When HA is enabled on Edge Services Gateway, OSPF hello and dead interval configured to values other than 30 seconds and 120 seconds respectively can cause some traffic loss during failover**

When the primary NSX Edge fails with OSPF running and HA enabled, the time required for standby to take over exceeds the graceful restart timeout and results in OSPF neighbors removing learned routes from their Forwarding Information Base (FIB) table. This results in dataplane outage until OSPF re-initiates converges. *Fixed in NSX 6.2.0.*

- **Fixed Issue 1403594: VMs are unable to receive ping from Edge DHCP server**

VM's can ping the Edge gateway but unable to receive DHCP ping from an Edge gateway trunk over an overlay network. The Edge DHCP server is setup as a trunk port and fails to pass or receive any traffic. However, when the Edge Gateway and the DHCP Edge are on the same host they are able to ping each other. When the DHCP Edge is moved to another host, the DHCP Edge is unable to receive ping from the Edge Gateway. *Fixed in NSX 6.2.0.*

- **Fixed Issue 1477176: Edge Load Balancer stats not correctly displayed in the vSphere Web Client**

The Load Balancer does not display the number of concurrent connection statistics in the chart in vSphere Web Client UI. *Fixed in NSX 6.2.0.*

- **Fixed Issue 1484743: Unable to pass traffic through load balancer after upgrading to NSX 6.1.2 or later**

When using option Insert X-Forwarded-For on NSX Edge Load Balancer, traffic may not pass through the load balancer. *Fixed in NSX 6.2.0.*

- **Fixed Issue 1449461: Running the clear ip ospf neighbor command returns a segmentation fault error**

Fixed in NSX 6.2.0.

- **Fixed Issue 1418264: Unable to process Kerberos requests**

Certain Kerberos requests are failing when being balanced with an NSX Edge. *Fixed in NSX 6.2.0.*

- **Fixed Issues 1558051, 1769174: For clusters with a DFW in disabled state, Exclude list updates are not enforced and filters get created on the Exclude lists**

Exclude list updates are not enforced if one of the clusters has a DFW in disabled state. This was happening as the isFirewallEnabled API had a strict check and would return 'true' only if all the hosts had DFW enabled. If any cluster in the environment had Firewall disabled, it returned 'false'.

After the fix, the API now checks if firewall is Enabled for any cluster and returns 'true' if any one of the clusters in the environment has Firewall Enabled.

Also, filters were getting created on Exclude list updates on hosts with the DFW disabled. After the fix, for each of the excluded VMs, the API gets the cluster and if the cluster has firewall enabled, adds the system vNIC IDs of that cluster and the vNIC IDs of the VM, and publishes the exclude list for each cluster. Migration of VM from one cluster to another cluster is handled by publishing Exclude list for the VM cluster. *Fixed in 6.2.4.*

- **Fixed Issue 1694483: After installing or upgrading to NSX for vSphere 6.2.3 with Distributed Firewall (DFW) and Security Groups (SG) configured, you may encounter traffic disruption upon a vMotion operation on compute virtual machines**
See [VMware knowledge base article 2146227](#). *Fixed in 6.2.4.*
- **Fixed Issue 1689356: Editing a security group via search removes all objects from the security group**
Editing a security group by searching for a statically included member, for example, a VM, and then removing that member causes all statically included members to be removed from the security group. *Fixed in 6.2.4.*
- **Fixed Issue 1675694: Distributed firewall drops packets when reusing the same IP and port after a disrupted connection**
Connections in the half-closed state do not disconnect, causing new connections to that IP and port to fail. *Fixed in 6.2.4.*
- **Fixed Issue 1698863: Retransmission of the initial TFTP packet on an established TFTP session while distributed firewall is enabled might cause a purple diagnostic screen**
Fixed in 6.2.4.
- **Fixed Issue 1701195: Distributed firewall experiences heap exhaustion**
In larger deployments with high consolidation ratios (number of provisioned VMs per host), distributed firewall would experience exhaustion of heap memory as DFW in VMkernel has a limited amount available (up to 1.5GB on large memory hosts). *Fixed in 6.2.4. The maximum heap size has been increased to 3GB for ESXi 6.0 hosts that have memory of 96GB or more, enabling a higher consolidation ratio.*
- **Fixed Issue 1712698: Service Composer Security Policy rules are deleted after attempting to modify Security Policy firewall rules**
Fixed in 6.2.4.
- **Fixed Issue 1620109: Deployment of third-party service VMs may not complete as expected, and Installation Status will be reported as "Failed"**
For example, the SVM may not receive the expected IP address. An error message of "Value provided for parameter property.info.key was not correct" is seen in the NSX Manager logs.
See [VMware knowledge base article 2145376](#). *Fixed in NSX 6.2.3.*
- **Fixed Issue 1619570: In a large-scale DFW configuration with millions of rules and Service Composer, rule publishing may require several seconds to complete after a reboot. During this time, new rules cannot be published**
NSX 6.2.3 reduces the time to sync the firewall rules on reboot by re-syncing only those firewall policies for which the latest revision has not been processed due to reboot.
- **Fixed Issue 1526781: Querying the getFirewallConfigLayer3SectionByName API does not return the responseHeaders field on NSX 6.2.x**
This issue has been fixed in 6.2.3 and the ETag header information reinstated in the API output.
- **Fixed Issue 1599576: An edited rule in a universal firewall section may fail to be published because a null value was being set for the Global Section ID field.**
No error message is reported. *Fixed in NSX 6.2.3.*
- **Fixed Issue 1558501: Guest Introspection installation may fail when the Universal SVM to NSX Manager connection fails**
When NSX Manager is configured with a FQDN only, the messaging channel between NSX Manager and the Guest Introspection Service VM may fail. When this issue occurs, the Guest Introspection Service Status remains in "Warning" status. An "UnknownHostException" message is displayed in the eventmanager.log file on the USVM. *Fixed in NSX 6.2.3 by adding automatic DNS support.*
- **Fixed Issue 1673068: Editing firewall rules within Service Composer Policy section causes out-of-sync configuration**
Service Composer goes out-of-sync when firewall rules are added or edited from within the Service Composer policy section of the firewall configuration screen. Fixed by changing the Service Composer section of the firewall configuration to read-only. Rules created through Service Composer must be managed through Service Composer. *Fixed in NSX 6.2.3.*

- **Fixed Issue 1639612: MSRPC connectivity issues with Windows 2008 and later in NSX for vSphere 6.2.x**
In later versions of Windows which support 64-bit addressing, the DCE/EPM protocol negotiates NDR64 as the transfer encoding format, leading the firewall to not parse the EPM response packet, hence failing to detect the dynamic port to open. See [VMware knowledge base article 2145135](#). *Fixed in NSX 6.2.3.*
- **Fixed Issue 1567693: Using IPset as source/destination in NetX rule displays the error Invalid container type: IPSet**
Fixed in NSX 6.2.3.
- **Fixed Issue 1407920: If you delete the firewall configuration using a REST API call, you cannot load and publish saved configurations**
When you delete the firewall configuration, a new default section is created with a new section ID. When you load a saved draft (that has the same section name but an older section ID), section names conflict and display the following error:
Duplicate key value violates unique constraint *firewall_section_name_key*.
Fixed in NSX 6.2.3.
- **Fixed Issue 1498504: VM loses firewall protection when removed from one of two overlapping service groups**
NetX filters (created by firewall workflow) on the host are removed when another service created by Service Composer workflow is applied to the same VM. This could happen, for example, when one service profile was applied to two overlapping service groups. In this case if a VM is in both service groups and then is removed from one of the service groups, it loses protection. *Fixed in 6.2.3* by introducing the **priority** field in the service profile. If there are overlapping service groups for a vNIC on a host, the service profile with the highest priority is applied.
- **Fixed Issue 1550370: Linux virtual machines with NFSv3 mounts experience an operating system hang after more than 15 minutes outage on the upstream datapath**
See [VMware knowledge base article 2133815](#). *Fixed in NSX 6.2.3.*
- **Fixed Issue 1494366: Copy and paste of a firewall rule with negate source/destination enabled will list a new rule with Negate option disabled**
When copying a firewall rule with the negate source/destination option enabled, a new firewall is created with this option disabled. *Fixed in NSX 6.2.3.*
- **Fixed Issue 1473767: Flow Monitoring drops flows that exceed a 2 million flows / 5 minutes limit**
NSX Flow Monitoring retains up to 2 million flow records. If hosts generate more than 2 million records in 5 minutes, new flows are dropped. *Fixed in NSX 6.2.3.*
See [VMware knowledge base article 2091376](#).
- **Fixed Issue 1611238: In 6.2.x Edge Firewall only the Security Groups created at Edge Scope (SGs at Edge Scope can be created only through REST) used to appear**
In 6.2.3, SGs created at Global Scope (these can be created in UI) and SGs created at Edge scope for the corresponding Edge (these can be created only through REST) appear in the Edge Firewall in the Security Group listing under the Source/Destination columns.
Fixed in NSX 6.2.3.
- **Fixed Issue 1516460: Firewall rules continued to be marked as valid even after the applied-to logical switch in the rule was deleted**
Fixed in 6.2.3.
- **Fixed Issue 1542157: Loss of distributed firewall functionality after vMotion of protected VMs to destination host**
Removing an NSX-prepared host from the VC inventory removes the host entry in the internal firewall tables. Later adding that host back to the VC inventory was not re-creating the firewall table entries. *Fixed in 6.2.3.*
- **Fixed Issue 1592439: Service Composer fails to translate virtual machines into security-groups**
This issue occurred due to a deadlock in EpSecLib on the Universal Service Virtual Machine (USVM). *Fixed in 6.2.3.*
- **Fixed Issue 1534597: NSX for vSphere 6.x Controllers disconnect intermittently**
Due to an IPSEC bug in the StrongSWAN package that was shipping in 6.1.4 and earlier releases, the tunnels between controllers weren't established after IPSEC rekeying. This caused partial connectivity failures between controllers resulting in multiple different issues. For more information see [knowledge base article 2127655](#). *Fixed in NSX 6.1.5 and 6.2.1*
- **Fixed Issue 1491042: LDAP Domain Objects take too long to return or fail to return in Security Group Object Selection screen.** *Fixed in NSX 6.1.5 and NSX 6.2.1.*

- Fixed Issue 1468169: Delayed mouse movement when viewing FW rules**
 In NSX Networking and Security section of vSphere Web Client, moving the mouse over rows in the Firewall Rules display results in a 3 second delay each time the mouse is moved. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- Fixed Issue 1476642: Some IP SpoofGuard rules in NSX-v are not applied correctly**
 Some IP SpoofGuard rules in NSX-v are not applied correctly. Instance is not present in the Security Group in NSX-v and needs to be manually added to the security group. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- Fixed Issue 1510350: Bulk deletion in Service Composer user interface generates "between 0 to 0" message**
 Bulk deletion of policies (~100) from the NSX Service Composer user interface generates a message, "It should be between 0 to 0". You may safely ignore this message. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- Fixed Issue 1515656: Background operation for Policy deletion may take long time with high CPU utilization**
 Deletion of a policy reevaluates all the remaining policies in background. This may take more than an hour on setups having large number of policies, large number of security groups, and/or large number of rules per policy. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- Fixed Issue 1515630: All queued publishable tasks are marked as failed after the default timeout of 20 minutes**
 Queues are maintained per NSX Edge and can publish in parallel for different Edges. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- Fixed Issue 1545879: If you rename an existing firewall draft, the operation will fail with the UI displaying "Internal Server Error"**
Fixed in NSX 6.2.1.
- Fixed Issue 1545893: Some DFW central CLIs show "ERROR output 100" output**
 In some situations, where a Virtual Network Adapter (vNIC) is disconnected, a discrepancy can arise between the vNIC state information in NSX Manager and the Host leading to an "ERROR output 100" in the centralized CLI. *Fixed in NSX 6.2.1.*
- Fixed Issue 1545853: Application Profile list is not sorted.**
 The list of Application Profile names in NSX Edge when Service Insertion is enabled, is presented in an unordered fashion. This release incorporates the fix to present the Application Profile list in a sorted manner. *Fixed in NSX 6.2.1.*
- Fixed Issue 1545895: Central CLI commands that are run for a specific ESXi host time out on some setups**
Fixed in NSX 6.2.1.
- Fixed Issue 1491365: The vsfwd.log gets overwritten quickly with a large number of container updates**
 After the SpoofGuard policy is changed the NSX Manager promptly sends the change to host but host takes longer to process the change and update the state of the virtual machine's SpoofGuard state. *Fixed in NSX 6.2.0.*
- Fixed Issue 1113755: Cannot configure NSX firewall using security groups or other grouping objects defined at global scope**
 Administrator users defined at the NSX Edge scope cannot access objects defined at the global scope. For example, if user *abc* is defined at Edge scope and security group *sg-1* is defined at global scope, then *abc* will not be able to use *sg-1* in firewall configuration on the NSX Edge. *Fixed in NSX 6.2.0.*
- Fixed Issue 1425691: Delayed mouse movement when viewing FW rules**
 In the NSX Networking and Security section of vSphere Web Client, moving the mouse over rows in the Firewall Rules display results in a 3 second delay. *Fixed in NSX 6.2.0.*
- Fixed Issue 1352926: UI shows error Firewall Publish Failed despite successful publish**
 If Distributed Firewall is enabled on a subset of clusters in your environment and you update an application group that is used in one or more active firewall rules, any publish action on the UI will display an error message containing IDs of the hosts belonging to the clusters where NSX firewall is not enabled. *Fixed in NSX 6.2.0.*
- Fixed Issue 1295384: Deleting security rules via REST displays error**
 If a REST API call is used to delete security rules created by Service Composer, the corresponding rule set is not actually deleted in the service profile cache resulting in an ObjectNotFoundException error. *Fixed in NSX 6.2.0.*
- Fixed Issue 1412713: Firewall rules do not reflect newly added virtual machine**
 When new VMs were added to the logical switch, firewall rules are not updated correctly to include the newly added VMs. If you make a change to the firewall and publish changes the new objects are added to the policy. *Fixed in NSX 6.2.0.*
- Fixed Issue 1448022: Cannot select Active Directory objects when configuring security groups**
 In NSX 6.1.x, AD/LDAP Domain Objects took a long time to return in the Security Group Object selection screen.

Fixed in NSX 6.2.0.

- **Fixed Issue 1473585: Cannot add firewall rule with source/destination as multiple comma-separated IP addresses.** *Fixed in NSX 6.2.0.*
- **Fixed Issue 1460351: Unable to move NSX Distributed Firewall (DFW) section at the top of the list**
When using Service Composer to create a security group policy, the section created in the DFW table cannot be added to the top of the list. There is no way to move DFW section up or down. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1501451: Security policy configured as a port range causes firewall to go out of sync**
Configuring security policies as a port range (for example, "5900-5964") will cause the firewall to go out of sync with a NumberFormatException error. *Fixed in NSX 6.2.0.*

Monitoring Services Resolved Issues in 6.2.6 and earlier

- **Fixed Issue 1697118: All IPFIX flows are tagged as new flows rather than updated flows, resulting in frequent updates to the IPFIX collector**
Also, the frequency for sending active flows does not honor the active flow timeout configured value. *Fixed in 6.2.4.*
- **Fixed Issue 1617561: vmkernel log files floods with "ALERT: vdrb: VdrArpInput:1015: CP:Malformed pkt"**
This happens when networking device such as server is sending ARP request in IEEE 802 Networks ARP format. *Fixed in 6.2.3.*
- **Fixed Issue 1525620: The icmpCode value in a distributed firewall rule was not being sent to the host. The protocolName and subProtocolName values work as expected**
Fixed in 6.2.3.
- **Fixed Issue 1563830: Applying firewall rule on a DLR appliance with the source or destination as 'mgmtInterface' fails**
A message similar to "vShield Edge:10014:Configuration failed on NSX Edge vm" is reported in the NSX Manager logs. *Fixed in 6.2.3.*
- **Fixed Issue 1474498: Importing draft firewall rules fails after existing firewall configuration is removed by a REST API request**
This issue occurs when drafts are created in VMware NSX for vSphere 6.1.x and 6.2.x containing *section id = null*. *Fixed in 6.2.3.*
- **Fixed Issue 1545888: When reporting flow statistics, index 0 (bytes-in) and index 1 (bytes out) counts are sometimes reversed.**
Index 0 holds the counts for traffic for the origination direction and, and index 1 holds the counts for traffic in the reverse direction. *Fixed in NSX 6.2.1.*
- **Fixed Issue 1460085: The #show interface command does not display the bandwidth/speed of vNic_0 interface**
After running the "#show interface" command, a full duplex, "0 M/s" speed is displayed but not the bandwidth/speed of NSX Edge vNic_0 interface. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1288395: When IPFIX configuration is enabled for Distributed Firewall, firewall ports in the ESXi management interface for NetFlow for vDS or SNMP may be removed**
When a collector IP and port is defined for IPFIX, the firewall for ESXi management interface is opened up in the outbound direction for the specified UDP collector ports. This operation may remove the dynamic ruleset configuration on ESXi management interface firewall for the following services if they were previously configured on the ESXi host:
 - Netflow collector port configuration on vDS
 - SNMP target port configuration*Fixed in NSX 6.2.0.*
- **Fixed Issue 1354728: Unable to process Denied/Block events through IPFIX protocol**
Typically, vsfwd user process handles the collection of flows, including dropped/denied ones and processes them for IPFIX. This happens when the IPFIX Collector fails to see the Denied/Block events because the vSIP drop packet queue is either too narrow or is wrapped around by inactive flow events. In this release, the ability to send Denied/Block events using the IPFIX protocol is implemented. *Fixed in NSX 6.2.0.*

Solution Interoperability Resolved Issues in 6.2.6 and earlier

- **Fixed Issue 1571170: Some Log Insight reports are not supported in NSX 6.2 with some vRealize Content Pack versions**

Fixed in the latest version of the Log Insight Content Pack. Download and install the content pack from [VMware Solution Exchange](#). Fixed in NSX 6.2.3.

- **Fixed Issue 1484506: Purple diagnostic screen during ESXi upgrade**
When you are upgrading an NSX-enabled vSphere 5.5U2 host to vSphere 6.0, some of the ESXi host upgrades might halt with a purple diagnostic screen. See [VMware knowledge base article 2137826](#). *Fixed in 6.2.3.*
- **Fixed Issue 1453802: Copy of VM via vCloud Connector fails when route traverses NSX Load Balancer.** *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- **Fixed Issue 1462006: In VIO Deployment, some newly deployed VMs appear to have valid port and IPs assigned but do not have access to the network.** *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- **Fixed Issue 1482665: Slow login to NSX tab of vSphere web client with AD-backed SSO**
In NSX for vSphere installations that use SSO for AD authentication, the user's initial login to the NSX Networking and Security section of the vSphere Web Client takes a long time. *Fixed in NSX 6.1.5 and NSX 6.2.1.*
- **Fixed Issue 1326669: Unable to set up organizational network**
When attempting to set up an organization-wide network, vCloud Director fails with an error message. *Fixed in NSX 6.2.0.*
- **Fixed Issue 1497044: Unable to launch multiple VMs using VIO setup**
Users using VMware Integrated OpenStack were unable to launch large numbers of VMs or publish large numbers of firewall rules in a short period of time. This resulted in Error publishing ip for vnic messages in the log. *Fixed in NSX 6.2.0.*

Document Revision History

20 August 2015: First edition for NSX 6.2.0.
17 December 2015: First edition for NSX 6.2.1.
04 March 2016: First edition for NSX 6.2.2. Security patch to address glibc vulnerability.
09 June 2016: First edition for NSX 6.2.3.
25 August 2016: First edition for NSX 6.2.4.
02 September 2016: Second edition for NSX 6.2.4. Added known issue.
09 September 2016: Third edition for NSX 6.2.4. Added known issue.
23 September 2016: Fourth edition for NSX 6.2.4. Moved 2 known issues to resolved.
06 October 2016: Fifth edition for NSX 6.2.4. Added known issues.
16 November 2016: Sixth edition for NSX 6.2.4. Added KB.
28 November 2016: Sixth edition for NSX 6.2.4. Changes to bug 1685894.
05 January 2017: First edition for NSX 6.2.5.
10 January 2017: Second edition for NSX 6.2.5. Added resolved issues.
02 February 2017: First edition for NSX 6.2.6.
21 February 2017: Second edition for NSX 6.2.6. Changes to bug 1772911.
20 April 2017: First edition for NSX 6.2.7.
27 April 2017: Second edition for NSX 6.2.7. Added known issue 1698286.
05 May 2017: Third edition for NSX 6.2.7. Added known issues 1435504, 1798847, and resolved issue 1843981.
02 June 2017: Fourth edition for NSX 6.2.7. Added resolved issues 1814096, 1799194, 1811884.
29 June 2017: Fifth edition for NSX 6.2.7. Added resolved issue 1807067.
21 August 2017: Sixth edition for NSX 6.2.7. Deleted issue.