VMware NSX for vSphere 6.3.7 Release Notes

VMware NSX for vSphere 6.3.7 | Released November 15, 2018 | Build 10667122

See the Revision History of this document.

What's in the Release Notes

The release notes cover the following topics:

- What's New in NSX 6.3.7
- Versions, System Requirements, and Installation
- Deprecated and Discontinued Functionality
- Upgrade Notes
- FIPS Compliance
- Revision History
- Resolved Issues
- Known Issues

What's New in NSX 6.3.7

NSX for vSphere 6.3.7 addresses a number of specific customer bugs. SeeResolved Issues for more information.

View Release Notes for previous versions:

- NSX 6.3.6
- NSX 6.3.5
- NSX 6.3.4
- NSX 6.3.3
- NSX 6.3.2
- NSX 6.3.1
- NSX 6.3.0

Versions, System Requirements, and Installation

Note:

- The table below lists recommended versions of VMware software. These

recommendations are general and should not replace or override environment-specific recommendations.

- This information is current as of the publication date of this document.
- For the **minimum supported** version of NSX and other VMware products, see the VMware Product Interoperability Matrix. VMware declares minimum supported versions based on internal testing.
    - The minimum supported version of vSphere required for NSX interoperability changes between NSX 6.3.2 and NSX 6.3.3. See the VMware Product Interoperability Matrix for details.

Product or Component	Recommended Version
NSX for vSphere	VMware recommends the latest NSX release for new deployments. When upgrading existing deployments, please review the NSX Release Notes or contact your VMware technical support representative for more information on specific issues before planning an upgrade.
vSphere	• vSphere 5.5U3 and later • vSphere 6.0U3 and later. 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. • vSphere 6.5U1 and later. vSphere 6.5U1 resolves the issue of EAM failing with OutOfMemory. See *VMware Knowledge Base Article 2135378* for more information.
Guest Introspection for Windows	All versions of VMware Tools are supported. Some Guest Introspection-based features require newer VMware Tools versions: • Use VMware Tools 10.0.9 and 10.0.12 to enable the optional Thin Agent Network Introspection Driver component packaged with VMware Tools. • Upgrade to 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). • Use VMware Tools 10.1.0 and later for Windows 10 support. • Use VMware Tools 10.1.10 and later for Windows Server 2016 support.
Guest Introspection for Linux	This NSX version supports the following Linux versions: • RHEL 7 GA (64 bit) • SLES 12 GA (64 bit) • Ubuntu 14.04 LTS (64 bit)

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*.

- **NSX for vSphere 6.1.x** reached End of Availability (EOA) and End of General Support (EOGS) on January 15, 2017. (See also *VMware knowledge base article 2144769*.)
- **NSX for vSphere 6.2.x** will reach End of General Support (EOGS) on August 20 2018.
- **NSX Data Security removed:** As of NSX 6.3.0, the NSX Data Security feature has been removed from the product.
- **NSX Activity Monitoring (SAM) deprecated:** As of NSX 6.3.0, Activity Monitoring is no longer a supported feature of NSX. As a replacement, please use Endpoint Monitoring. For more information see Endpoint Monitoring in the *NSX Administration Guide*.
- **Web Access Terminal removed**: Web Access Terminal (WAT) has been removed from NSX 6.3.0. You cannot configure Web Access SSL VPN-Plus and enable the public URL access through NSX Edge. VMware recommends using the full access client with SSL VPN deployments for improved security. If you are using WAT functionality in an earlier release, you must disable it before upgrading to 6.3.0.
- **IS-IS removed from NSX Edge**: From NSX 6.3.0, you cannot configure IS-IS Protocol from the **Routing** tab.

- **vCNS Edges no longer supported**. You must upgrade to an NSX Edge first before upgrading to NSX 6.3.x.

General Behavior Changes

If you have more than one vSphere Distributed Switch, and if VXLAN is configured on one of them, you must connect any Distributed Logical Router interfaces to port groups on that vSphere Distributed Switch. Starting in NSX 6.3.6, this configuration is enforced in the UI and API. In earlier releases, you were not prevented from creating an invalid configuration.

API Removals and Behavior Changes

Changes in API error handling

NSX 6.3.5 introduces these changes in error handling:

- If an API request results in a database exception on the NSX Manager, the response is *500 Internal server error*. In previous releases, NSX Manager responded with*200 OK*, even though the request failed.
- If you send an API request with an empty body when a request body is expected, the response is *400 Bad request*. In previous releases NSX Manager responded with*500 Internal server error.*
- If you specify an incorrect security group in this API, GET /api/2.0/services/policy/securitygroup/{ID}/securitypolicies, the response is *404 Not found*. In previous releases NSX Manager responded with *200 OK*.

Changes in backup and restore API defaults

Starting in 6.3.3, the defaults for two backup and restore parameters have changed to match the defaults in the UI. Previously **passiveMode** and **useEPSV** defaulted to *false*, now they default to *true*. This affects the following APIs:

- PUT /api/1.0/appliance-management/backuprestore/backupsettings
- PUT /api/1.0/appliance-management/backuprestore/backupsettings/ftpsettings

Deleting firewall configuration or default section

- Starting in 6.3.0, this request is rejected if the default section is specified:DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId
- A new method is introduced to get default configuration. Use the output of this method to replace entire configuration or any of the default sections:
  - Get default configuration with GET /api/4.0/firewall/globalroot-0/defaultconfig
  - Update entire configuration with PUT /api/4.0/firewall/globalroot-0/config
  - Update single section with PUT /4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}

defaultOriginate parameter:

Starting in NSX 6.3.0, the defaultOriginate parameter is removed from the following methods for

logical (distributed) router NSX Edge appliances only:

- GET/PUT /api/4.0/edges/{edge-id}/routing/config/ospf
- GET/PUT /api/4.0/edges/{edge-id}/routing/config/bgp
- GET/PUT /api/4.0/edges/{edge-id}/routing/config

Setting defaultOriginate to true on an NSX 6.3.0 or later logical (distributed) router edge appliance will fail.

All IS-IS methods removed from NSX Edge routing.

- GET/PUT/DELETE /4.0/edges/{edge-id}/routing/config/isis
- GET/PUT /4.0/edges/{edge-id}/routing/config

CLI Removals and Behavior Changes

Do not use unsupported commands on NSX Controller nodes
There are undocumented commands to configure NTP and DNS on NSX Controller nodes. These commands are not supported, and should not be used on NSX Controller nodes. You should only use commands which are documented in the NSX CLI Guide.

Upgrade Notes

- General Upgrade Notes
- Upgrade Notes for NSX Components
- Upgrade Notes for FIPS

Note: For a list of known issues affecting installation and upgrades see the section,Installation and Upgrade Known Issues.

General Upgrade Notes

- To upgrade NSX, you must perform a full NSX upgrade including host cluster upgrade (which upgrades the host VIBs). For instructions, see the *NSX Upgrade Guide* including the Upgrade Host Clusters section.

- **System Requirements**: For information on system requirements while installing and upgrading NSX, see the System Requirements for NSX section in NSX documentation.

- **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.

- **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 validate** that your upgrade to NSX 6.3.x was successful seeknowledge base article 2134525.

- There is no support for upgrades from vCloud Networking and Security to NSX 6.3.x. You must upgrade to a supported 6.2.x release first.

- **Interoperability:** Check the VMware Product Interoperability Matrix for all relevant VMware products before upgrading.
  - **Upgrading to vSphere 6.5a or later**: When upgrading from vSphere 5.5 or 6.0 to vSphere 6.5a or later, you must first upgrade to NSX 6.3.x. See Upgrading vSphere in an NSX Environment in the *NSX Upgrade Guide*.
    Note: NSX 6.2.x is not compatible with vSphere 6.5.
  - **Upgrading to NSX 6.3.3 or later:** The minimum supported version of vSphere for NSX interoperability changes between NSX 6.3.2 and NSX 6.3.3. See the VMware Product Interoperability Matrix for details.

- **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.
- **Networking and Security plug-in**: After upgrading NSX Manager, you must log out and log back in to the vSphere Web Client. If the NSX plug-in does not display correctly, clear your browser cache and history. If the Networking and Security plug-in does not appear in the vSphere Web Client, reset the vSphere Web Client server as explained in the *NSX Upgrade Guide*.
- **Stateless environments**: 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:
  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:

  1. Find the new VIB URL from `https://<NSXManager>/bin/vdn/nwfabric.properties`.
  2. Fetch VIBs of required ESX host version from corresponding URL.
  3. Add them to host image profile.

Upgrade Notes for NSX Components

NSX Manager Upgrade

- Important: If you are upgrading NSX 6.2.0, 6.2.1, or 6.2.2 to NSX 6.3.5 or later, you must complete a workaround before starting the upgrade. See VMware Knowledge Base article 000051624 for details.

- If you use SFTP for NSX backups, change to `hmac-sha2-256` after upgrading to 6.3.x because there is no support for `hmac-sha1`. See *VMware Knowledge Base article 2149282* for a list of supported security algorithms in 6.3.x.

- If you want to upgrade from NSX 6.3.3 to NSX 6.3.4 or later you must first follow the workaround instructions in *VMware Knowledge Base article 2151719*.

- When you upgrade NSX Manager to NSX 6.3.6 or later, a backup is automatically taken and saved locally as part of the upgrade process. See Upgrade NSX Manager for more information.

Controller Upgrade

- In NSX 6.3.3, the NSX Controller appliance disk size changes from 20GB to 28GB.
- The NSX Controller cluster must contain three controller nodes to upgrade to NSX 6.3.3. If it has fewer than three controllers, you must add controllers before starting the upgrade. See Deploy NSX Controller Cluster for instructions.
- In NSX 6.3.3, the underlying operating system of the NSX Controller changes. This means that when you upgrade from NSX 6.3.2 or earlier to NSX 6.3.3 or later, instead of an in-place software upgrade, the existing controllers are deleted one at a time, and new Photon OS based controllers are deployed using the same IP addresses.

  When the controllers are deleted, this also deletes any associated DRS anti-affinity rules. You must create new anti-affinity rules in vCenter to prevent the new controller VMs from residing on the same host.

  See Upgrade the NSX Controller Cluster for more information on controller upgrades.

Host Cluster Upgrade

- In NSX 6.3.3, NSX VIB names change. The esx-vxlan and esx-vsip VIBs are replaced with esx-nsxv if you have NSX 6.3.3 or later.
- **Rebootless upgrade and uninstall on hosts:** On vSphere 6.0 and later, once you have upgraded to NSX 6.3.x, any subsequent NSX VIB changes will not require a reboot. Instead hosts must enter maintenance mode to complete the VIB change.

  A host reboot **is not required** during the following tasks:

  - NSX 6.3.0 to NSX 6.3.x upgrades on ESXi 6.0 or later.
  - The NSX 6.3.x VIB install that is required after upgrading ESXi from 6.0 to 6.5.0a or later.
    Note: The ESXi upgrade still requires a host reboot.
  - NSX 6.3.x VIB uninstall on ESXi 6.0 or later.

  A host reboot **is required** during the following tasks:

  - NSX 6.2.x or earlier to NSX 6.3.x upgrades (any ESXi version).
  - NSX 6.3.0 to NSX 6.3.x upgrades on ESXi 5.5.
  - The NSX 6.3.x VIB install that is required after upgrading ESXi from 5.5 to 6.0 or later.
  - NSX 6.3.x VIB uninstall on ESXi 5.5.
- **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: Do the following:

- 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.

NSX Edge Upgrade

- In NSX 6.3.0, the NSX Edge appliance disk sizes have changed:
  - **Compact, Large, Quad Large**: 1 disk 584MB + 1 disk 512MB
  - **XLarge**: 1 disk 584MB + 1 disk 2GB + 1 disk 256MB
- **Host clusters must be prepared for NSX before upgrading NSX Edge appliances**
  Management-plane communication between NSX Manager and Edge via the VIX channel is no longer supported starting in 6.3.0. Only the message bus channel is supported. When you upgrade from NSX 6.2.x or earlier to NSX 6.3.0 or later, you must verify that host clusters where NSX Edge appliances are deployed are prepared for NSX, and that the messaging infrastructure status is GREEN. If host clusters are not prepared for NSX, upgrade of the NSX Edge appliance will fail. See Upgrade NSX Edge in the *NSX Upgrade Guide* for details.
- **Upgrading Edge Services Gateway (ESG):**
  Starting in NSX 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:

  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

  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 above for defaults).

- **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:ECDHE-ECDSA-AES256-SHA</ciphers>
    <clientAuth>ignore</clientAuth>
    <serviceCertificate>certificate-4</serviceCertificate>
  </clientSsl>
  <serverSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <serviceCertificate>certificate-4</serviceCertificate>
  </serverSsl>
  ...
</applicationProfile>
```

- **Set Correct Cipher version for Load Balanced Clients on vROPs versions older than 6.2.0:** vROPs pool members on vROPs versions older than 6.2.0 use TLS version 1.0 and therefore you must set a monitor extension value explicitly by setting "ssl-version=10" in the NSX Load Balancer configuration. See Create a Service Monitor in the *NSX Administration Guide* for instructions.

```
{
   "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"
}
```

Guest Introspection Upgrade

- Guest Introspection VM's now contain additional host identifying information in an XML file on the machine. When logging in to the Guest Introspection VM, the file "/opt/vmware/etc/vami/ovfEnv.xml" should include host identity information.

Upgrade Notes for FIPS

When you upgrade from a version of NSX earlier than NSX 6.3.0 to NSX 6.3.0 or later, you must not enable FIPS mode before the upgrade is completed. Enabling FIPS mode before the upgrade is complete will interrupt communication between upgraded and not-upgraded components. See Understanding FIPS Mode and NSX Upgrade in the *NSX Upgrade Guide* for more information.

- Ciphers supported on OS X Yosemite and OS X El Capitan: If you are using SSL VPN client on OS X 10.11 (EL Capitan), you will be able to connect using AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA38, AES256-SHA and AES128-SHA ciphers and those using OS X 10.10 (Yosemite) will be able to connect using AES256-SHA and AES128-SHA ciphers only.

- Do not enable FIPS before the upgrade to NSX 6.3.x is complete. SeeUnderstand FIPS mode and NSX Upgrade in the *NSX Upgrade Guide* for more information.

- Before you enable FIPS, verify any partner solutions are FIPS mode certified. See the VMware Compatibility Guide and the relevant partner documentation.

FIPS Compliance

- **NSS and OpenSwan**: The NSX Edge IPsec VPN uses the Mozilla NSS crypto module. Due to critical security issues, this version of NSX uses a newer version of NSS that has not been FIPS 140-2 validated. VMware affirms that the module works correctly, but it is no longer formally validated.
- **NSS and Password Entry**: The NSX Edge password hashing use the Mozilla NSS crypto module. Due to critical security issues, this version of NSX uses a newer version of NSS that has not been FIPS 140-2 validated. VMware affirms that the module works correctly, but it is no longer formally validated.
- **Controller and Clustering VPN**: The NSX Controller uses IPsec VPN to connect Controller clusters. The IPsec VPN uses the VMware Linux kernel crypto module (Photon 1 environment), which is in the process of being CMVP validated.

Document Revision History

15 Nov 2018: First edition.
3 Mar 2019: Second edition. Added resolved issue 2249307.
13 May 2019. Third edition. Updated Host Cluster Upgrade section.

Resolved Issues

The resolved issues are grouped as follows.

- Logical Networking and NSX Edge Resolved Issues
- General Resolved Issues
- NSX Controller Resolved Issues
- NSX Manager Resolved Issues
- Installation and Upgrade Resolved Issues
- Security Services Resolved Issues

Logical Networking and NSX Edge Resolved Issues

- **Fixed Issue 2207483: High latency for both E-W and N-S routed traffic**
  TxWorld of VM generating routed traffic takes 100% CPU resulting in high latency.

- **Fixed Issue 2188666: Not able to connect to gateway with 5 digit port number using SSLVPN Linux client CLI**
  Need to use SSLVPN Client GUI on Linux to connect to the gateway with 5 digit port number as this works with GUI, but SSLVPN Linux CLI works with up to 4 digit port numbers.

- **Fixed Issue 2185457: Increase in network latency for bridged workloads**
  Workloads with high traffic (pps) on bridged networks can cause latency between VLAN and VXLAN.

- **Fixed Issue 2182874: Cannot VDR ID if there are overlapping VDR IDs across sites**
  The segment range of one site had to be changed if more than one site has segment range overlap when attempting to bring this site into multi-vc.

- **Fixed Issue 2181650: Accept GARP as a valid reply when sending ARP request to refresh ARP entry**
  Some old devices send GARP as reply to ARP request.

- **Fixed Issue 2181435: In ESX 5.5, Hostd crashes during stats polling**
  In ESX 5.5, Hostd crashes during stats polling. Hostd needs to be restarted.

- **Fixed Issue 2179054: Avoid IXGBE driver restart during NSX installation & upgrades**
  There is a network outage of 5-10 seconds for the services on the host.

- **Fixed Issue 2178950: Traffic disruption or more than two VMs in vCenter for the same edge when HA is enabled**
  Traffic disruption seen or more than two VMs in vCenter for the same edge when HA is enabled. Restore done by edit appliances or change of appliance placement leads to stranded VMs causing network disruption.

- **Fixed Issue 2177514: In some case, DaD ping forwarded back, causing DaD process to detect duplicate IP addresses**
  System event reports fake duplicated IP detected.

- **Fixed Issue 2176316: Edge name is not updated in firewall rule**
  After change in Edge name from Edge UI, Firewall UI continues to show old edge name

- **Fixed Issue 2172005: The BGP neighborship flaps when the "show ip bgp" CLI command is issued**

When BGP has learns routes with AS_PATH longer than 126 characters and the "show ip bgp" command is issued, the routing stack restarts. Route churn and possible traffic outage until BGP re-converges.

- **Fixed Issue 2171616: SSL VPN Windows client process crashes when the ESG host name cannot be resolved**
  When HTTP proxy is configured and ESG host name cannot be resolved, client process crashes.

- **Fixed Issue 2167176: DLRs Edges with HA enabled tmpfs partition becomes full**
  The /var/run directory (tmpfs) fills up completely when HA was enabled. When full, this would prevent any configuration from working.

- **Fixed Issue 2164068: Edge tmpfs partition full after some time when HA is enabled**
  Rsync is used to synchronize files between Edge VMs in an HA pair. Due to the way the rsync was compiled, each periodic invocation of rsync generated an error log messages that was saved in a log file on the tmpfs partition. After some time, the partition would become full, which seriously impacts the normal operation of the Edge.

- **Fixed Issue 2156094: Unable to connect to gateway with five digit port number using SSL VPN Linux Client CLI**
  Need to use SSL VPN Client GUI on Linux to connect to the gateway with five digit port number as this works with GUI, but SSL VPN Linux CLI works with up to four digit port numbers.

- **Fixed Issue 2152060: Monitor service engine (Nagios) on edge has memory leak**
  Load Balancer won't functional well when its configuration is using monitor service for no memory.

- **Fixed Issue 2140512: After upgrading to 6.3.x or later, missing TransportZone (vdnscope) entries in MP database result in errors with VXLAN and Logical Networking**
  VXLAN and logical network errors on clusters prepped for NSX.

- **Fixed Issue 2134760: Installation of SSL VPN Mac client is successfully done, but unable to run the app**
  The client will not open even after successful installation.

- **Fixed Issue 2100704: NSX Edge can lose VMCI connections to NSX Manager in certain scenarios**
  Edges become unmanageable, which results in the inability to push configurations to the Edges.

- **Fixed Issue 2092516: Multiple monitor workers update pool member status concurrently**
  Load balancing is not functional well, with some traffic slow to dispatch to unhealthy server, or healthy server never has traffic to handle.

- **Fixed Issue 2078866: On host reboot, nsxv-vib fails in refreshHostdNetstackCache()**
  The VXLAN Rx throughput performance might be degraded.

- **Fixed Issue 2028337: Top five CPU-consuming processes not shown when Edge CPU usage above 90 percent**
  When Edge CPU usage is greater than 90 percent, a notification is sent to the Manager showing a list of the five top CPU-consuming processes since the Edge was started. This list most likely does not show the top five CPU users at this very instant, making it difficult to diagnose CPU usage problems.

- **Fixed Issue1983497: Purple screen appears when bridge failover and bridge configuration change happen at the same time**
  When a bridge failover and bridge configuration change happen at the same time, it may result into deadlock and cause purple screen. The chances of running into deadlock are low.

- **Fixed Issue 2181633: ARP suppression of sub interface IP addresses of guest VMs fails.**
  ARP resolution of these interfaces takes slightly longer than usual (1 second) for the first time.

- **Fixed Issue 2170329: DNS configuration fails to apply on SSLVPN Windows client interface**
  DNS query fails, affecting access.

General Resolved Issues

- **Fixed Issue 2183198: UI displays an error when retrieving a port from a ToR switch that has no port**
  If a physical switch on a hardware gateway has no port, the NSX UI throws an error when trying to get the port from the switch. The error, “Unable to fetch inventory information” displays in the UI while trying to retrieve the port information.

- **Fixed Issue 2176000: Encoding difference in the messages sent by Management Plane and expected by host resulted in invalid uplink port names of DVS leading to failure in MAC resolution**
  DLR fails to resolve mac addresses of VMs on the different ESXi hosts.

- **Fixed Issue 2170413: API /api/3.0/ai/directorygroup not working**
  NullPointerException is thrown from backend and API returns error. Unable to automate workflow.

- **Fixed Issue 2170395: domain_object is not in sync with ai_group table**
  When the service composer page is loaded, the SQLGrammarException is thrown due to SQL containing an empty list of group ids.

- **Fixed Issue 2131680: Multicast packets when hitting a reject firewall rule result in excessive logging in the vmkernel log**
  Excessive logging to vmkernel log causes the host to stop logging.

- **Fixed Issue 2129177: If GI-SVM is deleted or removed during the upgrade process and backward compatibility mode, identity firewall through Guest Introspection (GI) will not work unless the GI cluster is upgraded**
  Identity firewall will not work and no logs related to identity firewall would be seen. Identity

firewall protection will be suspended unless the cluster is upgraded.

- **Fixed Issue 2105632: USVMs attempt to sync time with Google (external) NTP servers**
  The timesync service has been modified to prevent this behavior.

- **Fixed Issue 2003396: DLR LIFs/Routes go missing after reboot or on a new host join if there are a large number of routes configured**
  The routes are not seen as configured.

- **Issue 1960383: Failure in network creation due to timeout when high number of inventory objects are deleted in short span of time**
  Network creation timeout happens due to delay in dvpg creation in NSX.

- **Fixed Issue 2058770: Excessive login events are raised at vCenter and vCenter SSO server experiences high load**
  vCenter SSO server experiences excessive login events and high load when vCenter SSO users make many NSX APIs requests in a short span of time. This might result in sluggish behavior.

- **Fixed Issue 2046427: Changing Vmknic or LS dvs portgroup teaming policy can result in DP outage**
  During Host preparation (VXLAN), if user is setting vmknic teaming policy, then the Uplink teaming policy on DVS are set accordingly. Any new
  Logical switch dvs pg that are created also get this teaming policy.

- **Fixed Issue 2178339: rsyslog 8.15.0-7.ph1 removed ExecReload line in systemd service file causing /var/log/syslog and /var/log/messages to not logrotate properly**
  This causes /var/log partition to take up 100% disk space so new logs cannot be written.

- **Fixed Issue 2146879: In a standalone setup, force sync doesn't sync ToR and ToR bindings**
  In a standalone setup, when HW binding or HW transport node config is out of sync between Management Plane and controller, force sync cannot sync the config. ToR configurations cannot be synced to controller in case ToR bindings are out of sync.

- **Fixed Issue 2146749: ESXi host loses locale ID configuration after reboot**
  Host receives the wrong localeId and the corresponding routes get flushed.

- **Fixed Issue 2200396: Vdr Instances get recreated on ESXi host in secondary site after failover**
  Traffic disruption and network outage of around 40 seconds after failover.

- **Fixed Issue 2100296: NSX 6.3.5 Web Client plugin is not showing any NSX Manager after disabling SSL/TLS1.0 on the vCenters/PSCs**
  Disabling SSL/TLS1.0 on the vCenters, NSX breaks the communication with vCenters, NSX or ESX. vCenter Application will not communicate with NSX Manager.

- **Fixed Issue 2077492: NSX Manager auto creates ipsecsite Id for ipsec sites already present**
  - NSX Manager auto creates ipsecsite Id for ipsec sites already present.

    - NSX for vSphere upgrade from 6.2.x to 6.3.5 or 6.4.0a may introduce duplicate siteIds for the Ipsec sites.
    - Once duplicate siteIds are introduced, the next ipsec configuration fails.
    - You see an error similar to: [13646] [Ipsec] Duplicate Ipsec site Ids ipsecsite-id found.
- **Fixed Issue 2177097: When using API call /api/2.0/vdn/config/segments to create a pool with 1 Segment ID it fails with, "Segment id is out of range, valid range is 5000-16777215"**
  When using the API /api/2.0/vdn/config/segments, if you provide the same start and end value when creating a single value segment, it fails with an error.

- **Fixed Issue 2172267: Deleting NSX Edge during host unresponsiveness causes orphaned objects in vCenter**
  Edge instance on NSX Manager is deleted, but Edge appliance is still present in vCenter and serves data path until NSX Manager marks this Edge as orphaned and deletes the Edge in clean up process. There is no way to delete the Edge appliance from NSX Manager.

- **Fixed Issue 2097255: SNMP traps are not sent when FIPS is enabled on NSX Manager appliance**
  No SNMP traps are received.

NSX Controller Resolved Issues

- **Fixed Issue 2181306: Controller runs out of memory and cannot provide service normally**
  The controller supports an ssh interface for querying cluster membership and status. If a client accesses this and does not close the sessions, the controller keeps the sessions alive indefinitely. With enough sessions left open, the controller runs out of memory.

NSX Manager Resolved Issues

- **Fixed Issue 2171653: Security scan on NSX Manager reports “HTTP Security Header Not Detected"**
  Security scan reports this issue. Clickjacking attacks can occur.

- **Fixed Issue 2161066: Connecting Usage Meter with NSX Manager fails or invalid XML character error while processing an API response**
  Connecting Usage Meter with NSX Manager fails with an error.

- **Fixed Issue 2145195: Heartbeat alert for all the USVMs and high CPU usage on NSX Manager**
  NSX Manager alerts that all the USVMs have not been responding to heartbeat. Its CPU usage is high caused by postgres session.

- **Fixed Issue 2144825: Manager root partition full due to many nsx-tcserver-wrapper.log files**
  NSX UI is inaccessible and many other services stop working due to shortage of space.

- **Fixed Issue 2141490: ToR binding on NSX Manager and controller out of sync**
  Unable to modify the HW binding on a logical switch or delete the configuration. UI shows the following error: "Failed to do operation on the Controller. {0}"

- **Fixed Issue 2066631: Error message popup displays when logging in with a Security Administrator user role and selecting a VM**
  The error message, "There is no authority to access object global and function library.tagging. Confirm the authority of the function and object access scope" displayed as a popup.

- **Fixed Issue 2189810: Guest VMs protected by PAN drop traffic when an API call is made by a third party Service Insertion solution to NSX Manager to retrieve all the SecurityGroups/IPSets configured as part of Service Insertion**
  NSX Manager returns an empty config for IPSets or SecurityGroups containing IPSets. As a result, IPSets or SecurityGroups containing IPSets are reported empty to the third party Manager. The guest VMs protected by PAN or other third party firewall devices would drop the traffic as no rules match and hit default deny rule. Running the API call https://NSXMGR_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset does not return any IPs for IPSets or SecurityGroups containing IPSets.

  All guest VMs protected by PAN or other third party firewall devices would drop the traffic as no rules match and hit default deny rule.

- **Fixed Issue 2178700: NSX Manager fails to sync VDR LIF information to controller if any one of the VDR LIFs is consuming a deleted virtualwire**
  VDR LIF operations fail, leaving the user unable to modify LIF configuration.

- **Fixed Issue 2249307: The Locale ID on ESXi host is reset to default upon ESXi host reconnection to NSX Manager**
  Missing DLR routes. DLR no longer routing traffic. Host receives the wrong Locale ID and the intended DLR routes are not retained.

Installation and Upgrade Resolved Issues

- **Fixed Issue 2133143: Stale cluster entries in NSX DB**
  Some stale cluster entries are present in NSX DB after upgrading from 6.2.2 through 6.2.9.

- **Fixed Issue 2112773: Controller upgrade failed**
  A controller failed during upgrade from 6.2.4 to 6.3.6.

Security Services Resolved Issues

- **Fixed Issue 2098645: Null pointer exception when Security group has reference to deleted AD-Group**
  If an AD-Group (ai_group) is deleted and there is a Security group that has reference to the deleted AD-Group, SG->VM translation will throw null pointer exception. Service Composer page does not load correctly.

- **Fixed Issue 2032988, 2032990, 2032991: Vulnerability due to CVE-2017-5753, CVE-2017-5715 (Specter), and CVE-2017-5754 (Meltdown)**
  Potential security issue due to CVE-2017-5753, CVE-2017-5715 (Specter), and CVE-2017-5754 (Meltdown) vulnerabilities.

Known Issues

The known issues are grouped as follows.

- Installation and Upgrade Known Issues
- General Known Issues

Installation and Upgrade Known Issues

- **Issue 2001988: During NSX host cluster upgrade, Installation status in Host Preparation tab alternates between "not ready" and "installing" for the entire cluster when each host in the cluster is upgrading**
  During NSX upgrade, clicking "upgrade available" for NSX prepared cluster triggers host upgrade. For clusters configured with DRS FULL AUTOMATIC, the installation status alternates between "installing" and "not ready", even though the hosts are upgraded in the background without issues.

  Workaround: This is a user interface issue and can be ignored. Wait for the host cluster upgrade to proceed.

General Known Issues

- **Issue 2158182: DHCP service and HA with link-local IP share the same vNic cause DHCP renew packet to be dropped**
  If the HA address is a link-local address (169.x.x.x), the DR may drop DHCP renew unicast packet to this link-local address, which may cause DHCP client to renew fail.

  Workaround: Select a vNic without DHCP service as HA interface, or use a routable IP address as HA interface IP, i.e., 192.168.x.x

- **Issue 1467382: 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:

  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 1849042/1849043: Admin account lockout when password aging is configured on the NSX Edge appliance**
  If password aging is configured for the admin user on the NSX Edge appliance, when the password ages out there is a 7 day period where the user will be asked to change the password when logging into the appliance. Failure to change the password will result in the account being locked. Additionally, if the password is changed at the time of logging in at the CLI prompt, the new password may not meet the strong password policy enforced by

the UI and REST.

Workaround: To avoid this problem, always use the UI or REST API to change the admin password before the existing password expires. If the account does become locked, also use the UI or REST API to configure a new password and the account will become unlocked again.

- **Issue 2204383: SSLVPN Linux client fails to verify server certificate for Linux versions that use sql cert9.db**
  Server validation fails with internal error.

  Workaround: None.