VMware NSX-T Data Center 2.3.1 and NSX Container Plug-in 2.3.1 Release Notes

VMware NSX-T Data Center 2.3.1 | 20 December 2018

VMware NSX Container Plug-in 2.3.1 | 8 November 2018

Check regularly for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- What's New
- Compatibility Requirements
- Resolved Issues
- Known Issues

What's New

What's New in NSX-T Data Center 2.3.1
NSX-T Data Center 2.3.1 is a maintenance release that resolves a number of issues found in previous releases. For new features in NSX-T Data Center 2.3, as well as known and resolved issues applicable to NSX-T Data Center 2.3.1, see NSX-T Data Center 2.3 Release Notes.

What's New in NSX Container Plug-in 2.3.1
NSX Container Plug-in (NCP) 2.3.1 is a maintenance release that resolves a number of issues found in previous releases and has the following new feature:

- Automatic scaling of NSX-T load balancers for Kubernetes LoadBalancer services. If a Kubernetes LoadBalancer service requires additional virtual servers, a new NSX-T load balancer will be created if required.

Recommended ESXi Versions for NSX-T Data Center 2.3.1

- ESXi 6.5 P03 Build 10884925
- ESXi 6.7 U1 Build 10302608

Compatibility Requirements for NCP 2.3.1

Product	Version
NCP / NSX-T Tile for PAS	2.3.1
NSX-T	2.2, 2.3, 2.3.1
Kubernetes	1.11, 1.12
OpenShift	3.10, 3.11
Kubernetes Host VM OS	Ubuntu 16.04, RHEL 7.4, 7.5
OpenShift Host VM OS	RHEL 7.4, 7.5
PAS (PCF)	OpsManager 2.2.0 + PAS 2.2.0 OpsManager 2.3.x + PAS 2.3.x

Resolved Issues

The resolved issues are grouped as follows.

- Resolved Issues in NSX-T Data Center 2.3.1
- Resolved Issues in NCP 2.3.1

Resolved Issues in NSX-T Data Center 2.3.1

- **Issue 2238957: Stale hyperbus ports are not cleaned up after an ESXi host reboot**
  If you reboot an ESXi host without powering off the container VMs running on the host, hyperbus ports are not cleaned up as expected.

- **Issue 2226523: CLI command "get debug bgp" does not work**
  Running the "get debug bgp" CLI command produces no output.

- **Issue 2241365: During an upgrade from NSX-T Data Center 2.2 to 2.3, firewall-protected VMs with ALG (application-level gateway) traffic lose network connectivity**
  During an upgrade from NSX-T Data Center 2.2 to 2.3, VMs will be migrated from hosts running NSX-T Data Center 2.2 to hosts running NSX-T Data Center 2.3. A VM that is protected by a firewall and has ALG traffic will lose network connectivity after the migration.

- **Issue 2241378: VPN tunnels show flapping behavior and traffic being dropped**
  VPN tunnels that have a firewall drop rule configured and fragmented traffic will show flapping behavior and traffic being dropped.

- **Issue 2232034: ESXi host crashes while creating support bundle if the host has a DLR bridge with more than 1024 MAC addresses**
  Running vm-support or the command "net-bridge --mac-address-table $bridgeName" leads

to buffer overflow if there is a large number of bridge forwarding entries.

- **Issue 2216746: A VM's NIC is disconnected and the VM has no network connectivity upon vMotion or power-up**
  If a large number of VMs are powered on or vmotioned concurrently, some VMs might have their NICs disconnected and have no network connectivity.

- **Issue 2216747: vMotion of VM causes its ports to be disconnected**
  When a VM has its storage on NFS and is vMotioned, which might be triggered by HA, the VM loses network connectivity.

- **Issue 2229210: Repeated operations of creating and deleting logical switch ports cause memory leak in NSX Controller**
  This issue is caused by spoof guard domain objects not being deleted when logical switch ports are deleted.

- **Issue 2220560: Excessive event logs in metricRegistry can result in memory leak in NSX Controller**
  After a large number of transactions is processed by the NSX Controller, the large amount of logging can cause a memory leak.

- **Issue 2221286: ARP entries expire shortly after VM connection goes down**
  This issue can cause VMs to be unreachable for a certain amount of time.

- **Issue 2227882: Policy-based VPN goes down with Error “No active IPsec SA, deleting childless IKE SA"**
  The error results in renegotiation and traffic drop.

- **Issues 2227885 and 2227879: Memory leak observed in IPSec VPN on Edge node with certain traffic patterns**
  When UDP-encapsulated ESP traffic (packets with destination port 4500) with destination IP owned by Edge arrives during the following windows:

  - PBR redirect rules (used by HCX) are programmed after the FIB programming of the redirected IP to loopback port
  - Missing Source Address for VPN tunnel (such as when iked misbehave or coredumped)
- **Issue 2227890: VLAN ID does not get modified after modifying tunnel ID in the logical port configuration**
  When making an API call to change the tunnel ID of a logical port, the VLAN ID does not get modified.

- **Issue 2230277: Do not flush runtime data of ports during vMotion**
  With ESXi 6.5, an issue during storage vMotion causes the runtime data on a port to be flushed, before the vMotion framework can save the data.

- **Issue 2236206: ESXi Transport Nodes may lose network access due to memory leak**
  This issue can cause an ESXi transport node in a PKS environment to lose network connectivity.

Resolved Issues in NCP 2.3.1

- **Issue 2216781: The maximum length of a tag value is limited to 65 characters in NCP 2.2.x and 256 characters in NCP 2.3.0**
  NCP 2.3.1 supports names that exceed the tag value limit for the following load balancer related Kubernetes resources:
    - LoadBalancer service
    - Ingress
    - Secret specified in an Ingress spec
    - Service specified in an Ingress spec
- **Issue: 2217051: Virtual server IP does not get updated after a LoadBalancer service's loadBalancerIP is changed**
  After creating a LoadBalancer service, if you change the service's loadBalncerIP value, the change is not reflected in the NSX-T load balancer's virtual server IP.
- **Issue 2216085: After deleting a namespace, NSX-T load balancer rules and pools are not deleted**
  When you configure Ingress resources and NSX-T load balancing, NSX-T virtual servers, pools and rules are created. If you delete the namespace the Ingress resources are in, some rules and pools are not deleted from NSX-T.

Known Issues

The known issues are grouped as follows.

- Known Issues in NSX-T Data Center 2.3.1
- Known Issues in NCP 2.3.1

Known Issues in NSX-T Data Center 2.3.1

- **Issue 2235834: RDP and HTTPS traffic problem with flow-cache enabled**
  With flow-cache enabled, issues with RDP and HTTPS traffic can occur.

  Workaround: On the Edge node, run the following commands to disable flow-cache:
    - set dataplane flow-cache disabled
    - restart service dataplane
- **Issue 2227975: Intermittent TCP traffic loss traversing an Edge node**
  TCP traffic traversing an Edge node is dropped intermittently. ICMP traffic is not impacted.

  Workaround: On the Edge node, disable flow-cache with the following commands:
    - set dataplane flow-cache disabled
    - restart service dataplane

Known Issues in NCP 2.3.1

- **Issue 2118515: In a large-scale setup, NCP takes a long time to create firewalls on NSX-T**
  In a large-scale setup (for example, 250 Kubernetes nodes, 5000 pods, 2500 network policies), it can take NCP a few minutes to create the firewall sections and rules in NSX-T.

Workaround: None. After the firewall sections and rules are created, performance should be back to normal.

- **Issue 2125755: A StatefullSet could lose network connectivity when performing canary updates and phased rolling updates**
  If a StatefulSet was created before NCP was upgraded to the current release, the StatefullSet could lose network connectivity when performing canary updates and phased rolling updates.

  Workaround: Create the StatefulSet after NCP is upgraded to the current release.

- **Issue 2131494: NGINX Kubernetes Ingress still works after changing the Ingress class from nginx to nsx**
  When you create an NGINX Kubernetes Ingress, NGINX create traffic forwarding rules. If you change the Ingress class to any other value, NGINX does not delete the rules and continues to apply them, even if you delete the Kubernetes Ingress after changing the class. This is a limitation of NGINX.

  Workaround: To delete the rules created by NGINX, delete the Kubernetes Ingress when the class value is nginx. Than re-create the Kubernetes Ingress.

- **For a Kubernetes service of type ClusterIP, Client-IP based session affinity is not supported**
  NCP does not support Client-IP based session affinity for a Kubernetes service of type ClusterIP.

  Workaround: None

- **For a Kubernetes service of type ClusterIP, the hairpin-mode flag is not supported**
  NCP does not support the hairpin-mode flag for a Kubernetes service of type ClusterIP.

  Workaround: None

- **Issue 2194845: The PAS Cloud Foundry V3 API feature "multiple processes per app" is not supported**
  When using the PAS Cloud Foundry V3 API v3-push to push an app with multiple processes, NCP does not create logical switch ports for the processes except the default one. This issue exists in NCP 2.3.0 and earlier releases.

  Workaround: None

- **Issue 2193901: Multiple PodSelectors or multiple NsSelectors for a single Kubernetes network policy rule is not supported**
  Applying multiple selectors allows only incoming traffic from specific pods.

  Workaround: Use matchLabels with matchExpressions in a single PodSelector or NsSelector instead.

- **Issue 2194646: Updating network policies when NCP is down is not supported**
  If you update a network policy when NCP is down, the destination IPset for the network policy will be incorrect when NCP comes back up.

Workaround: Recreate the network policy when NCP is up.

- **Issue 2192489: After disabling 'BOSH DNS server' in PAS director config, the Bosh DNS server (169.254.0.2) still appears in the container's resolve.conf file.**
  In a PAS environment running PAS 2.2, after you disable 'BOSH DNS server' in PAS director config, the Bosh DNS server (169.254.0.2) still appears in the container's resove.conf file. This causes a ping command with a fully qualified domain name to take a long time. This issue does not exist with PAS 2.1.

  Workaround: None. This is a PAS issue.

- **Issue 2194367: NSX-T Tile does not support PAS Isolation Segments which deploy their own Routers at this time**
  NSX-T Tile does not work with Pivotal Application Service (PAS) Isolation Segments which deploy their own GoRouters and TCP Routers. This is because NCP cannot get the IP addresses of the Router VMs and create NSX firewall rules to allow traffic from the Routers to the PAS App containers.

  Workaround: None.

- **Issue 2199504: The display name of NSX-T resources created by NCP is limited to 80 characters**
  When NCP creats an NSX-T resouce for a resource in the container environment, it generates the display name of the NSX-T resource by combining the cluster name, namespace or project name, and the name of the resource in the container environment. If the display name is longer than 80 characters, it is truncated to 80 characters.

  Workaround: None

- **Issue 2199778: With NSX-T 2.2, Ingress, Service and Secrets with names longer than 65 characters are not supported**
  With NSX-T 2.2, when `use_native_loadbalancer` is set to `True`, the names of Ingresses, Secrets and Services referenced by the Ingress, and Services of type LoadBalancer, must be 65 characters or less. Otherwise, the Ingress or Service will not work properly.

  Workaround: When configuring an Ingress, Secret, or Service, specify a name that is 65 characters or less.

- **Issue 2065750: Installing the NSX-T CNI package fails with a file conflict**
  In a RHEL environment with kubernetes installed, if you install the NSX-T CNI Package using `yum localinstall` or `rpm -i`, you get an error indicating a conflict with a file from the kubernetes-cni package.

  Workaround: Install the NSX-T CNI package with the command`rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm`.

- **Issue 2224218: After a service or app is deleted, it takes 2 minutes to release the SNAT IP back to the IP pool**
  If you delete a service or app and recreate it within 2 minutes, it will get a new SNAT IP from the IP pool.

Workaround: After deleting a service or app, wait 2 minutes before recreating it if you want to reuse the same IP.

- **Issue 2218008: Configuring different Kubernetes clusters to use the same IP block causes connectivity problems**
  If you configure different Kubernetes clusters to use the same IP block, some pods will not be able to communicate with other pods or external networks.

  Workaround: Do not configure different Kubernetes clusters to use the same IP block.

Copyright © 2022 VMware, Inc. All rights reserved.