Copyright notice

2020 Mirantis, Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. No part of this publication may be reproduced in any written, electronic, recording, or photocopying form without written permission of Mirantis, Inc.

Mirantis, Inc. reserves the right to modify the content of this document at any time without prior notice. Functionality described in the document may not be available at the moment. The document contains the latest information at the time of publication.

Mirantis, Inc. and the Mirantis Logo are trademarks of Mirantis, Inc. and/or its affiliates in the United States an other countries. Third party trademarks, service marks, and names mentioned in this document are the properties of their respective owners.
What's new

This section provides the details about the features and enhancements introduced with the latest MCP release version.

Note

The MCP integration of the community software projects, such as OpenStack, Kubernetes, OpenContrail, and Ceph, includes the integration of the features which the MCP consumers can benefit from. Refer to the MCP Q4'18 Deployment Guide for the software features that can be deployed and managed by MCP DriveTrain.

MCP DriveTrain

- Encryption of sensitive data in the Reclass model
- Galera verification and restoration pipeline
- Jenkins version upgrade
- Partitioning table for the VCP images

Encryption of sensitive data in the Reclass model

SECURITY

Implemented the GPG encryption to protect sensitive data in the Git repositories of the Reclass model as well as the key management mechanism for secrets encryption and decryption.

Learn more

MCP Operations Guide: Manage secrets in the Reclass model

Galera verification and restoration pipeline

Implemented the automatic way to verify and restore the Galera cluster in the MCP deployment. In case of a cluster outage, the number of manual steps to start the cluster, as well as ensuring the necessary access can significantly delay the restoration of services and is prone to operator errors. Therefore, to reduce the complexity of the procedure and support greater scalability, the Verify and Restore Galera cluster pipeline has been created.
Jenkins version upgrade
Upgraded the Jenkins version in DriveTrain to the latest LTS v2.138.3.

Partitioning table for the VCP images
Implemented the dynamical strategy to prevent uploads from filling up the disk on the VCP nodes.

OpenStack

- Rate limiting for the NGINX proxy service
- TCP-only support for Memcached
- Encryption of the Keystone tokens stored within Memcached
- Octavia enhancements
- Ironic deployment
- Horizon load balancing
- Partitioning table for the VCP images
- Pike to Queens upgrade
- OpenStack packages update

Rate limiting for the NGINX proxy service

SECURITY
Implemented the possibility to limit the number of HTTP requests that a user can make in a given period of time for an OpenStack environment. The rate-limiting with NGINX can be used to protect an OpenStack environment against DDoS attacks as well as to protect the community application servers from being overwhelmed by too many user requests at the same time.

Learn more

MCP Operations Guide: Configuring rate limiting with NGINX

TCP-only support for Memcached

SECURITY

Disabled the Memcached listener on the UDP port by default. To reduce the attack surface and improve the product security, Memcached on the controller nodes listens on TCP only. For the existing OpenStack environments deployed on top of the earlier MCP versions, implemented the possibility to manually disable the Memcached listener on the UDP port.

Learn more

MCP Operations Guide: Disable the Memcached listener on the UDP port

Encryption of the Keystone tokens stored within Memcached

SECURITY

Implemented the protection of the Keystone tokens stored within Memcached.

MCP OpenStack supports the Memcached protection since the Pike release. By default, this functionality is disabled in the Pike deployments. For Queens, the Memcached protection is enabled by default with the ENCRYPT security strategy.

Learn more

MCP Deployment Guide: Secure Memcached for the OpenStack services
Octavia enhancements
Hardened the OpenStack Octavia LBaaS components and introduced the following enhancements:

- Added the OpenStack Queens support.
- Added the Transport Layer Security (TLS) support with Barbican.
- Changed location of the certificates used for connection to amphora. Now, they are created on the Salt Master node and then loaded on the gtw nodes.
- TECHNICAL PREVIEW Implemented clusterization for the Octavia Manager services.
- Added the Octavia artifacts to the MCP offline image.

Learn more

- MCP Reference Architecture: Plan load balancing with OpenStack Octavia
- MCP Deployment Guide: Configure load balancing with OpenStack Octavia

Ironic deployment

Added the list of the MCP Ironic supported features and known limitations. The new section in the MCP Reference Architecture Guide includes the Ironic drivers and features with known limitations that MCP DriveTrain supports. Since the Ironic service is available in MCP only as a Technical Preview feature, the driver or feature support status in that section stands for the ability of MCP DriveTrain to deploy and configure the features by means of the Ironic Salt formula through the cluster model.

Learn more

- MCP Reference Architecture: MCP Ironic supported features and known limitations
- MCP Deployment Guide: Deploy Ironic
Horizon load balancing

Enabled the load balancing mode for Horizon by default for the new MCP OpenStack deployments. The new approach allows for load reduction on one proxy node and spreading the load among all proxy nodes.

For the existing MCP OpenStack environments, implemented the flow to manually configure Horizon load balancing.

Learn more

MCP Operations Guide: Configure load balancing for Horizon

Partitioning table for the VCP images

Implemented the strategy to prevent uploads from filling up the disk on the Horizon proxy nodes.

Learn more

MCP Deployment Guide: Partitioning of a VCP node

Pike to Queens upgrade

TECHNICAL PREVIEW

Implemented the upgrade of OpenStack Pike deployments to Queens.

The official MCP documentation includes the reference information to consider when creating a detailed maintenance plan for the upgrade. We recommend using the descriptive analysis of the techniques and tools, as well as the high-level upgrade flow included in the documentation to create a cloud-specific detailed upgrade procedure, assess the risks, estimate possible downtimes, plan the rollback, backup, and testing activities.

Learn more

MCP Operations Guide: Upgrade an MCP OpenStack environment
OpenStack packages update

TECHNICAL PREVIEW

Implemented the flow to provide minor updates for the OpenStack packages without changing the major versions of the packages. In other words, the update between the package versions within a single major OpenStack release.

Learn more

MCP Operations Guide: Update OpenStack packages

Kubernetes

- Kubernetes 1.12.4 support
- Docker replaced by containerd
- Migration of kube-addon-manager to a Kubernetes pod
- Automatic Calico upgrade procedure
- Horizontal pod autoscaling
- OpenStack cloud provider
- Virtlet 1.4.4 support

Kubernetes 1.12.4 support

Updated to 1.13.5 in 2019.2.3

Added support for the community Kubernetes version 1.12.4. For the list of enhancements and bug fixes, see: Kubernetes release notes.

Caution!

MCP Q4`18 supports only Calico as a networking solution for the Kubernetes deployments. The OpenContrail integration is being finalized at the moment and will be available with the following MCP release.
Docker replaced by containerd

Completed development and added full support for containerd runtime to execute containers and manage container images on a node instead of Docker in an MCP Calico-based Kubernetes cluster. As compared to Docker, containerd introduces lower memory footprint, faster container start, easier upgrades and updates.

The upgrade procedure of a Docker-based Kubernetes cluster to the containerd-based one comprises a use case when third-party workloads run under Docker along with the MCP Kubernetes-based ones. Therefore, Docker is not stopped and removed during the upgrade to prevent these third-party workloads from being corrupted. However, you can disable Docker after the upgrade if required.

Learn more

- MCP Reference Architecture: Kubernetes cluster components
- MCP Operations Guide: Update or upgrade Kubernetes

Migration of kube-addon-manager to a Kubernetes pod

Migrated the kube-addon-manager service to a separate pod controlled by Kubernetes to fit the community implementation. Previously, kube-addon-manager was running as a systemd service and was using the default system authorization that could not be handled by Kubernetes.

The main changes made during the kube-addon-manager migration are as follows:

- kube-addon-manager uses its own service account for authorization controlled by Kubernetes
- kube-addon-manager is created as a manifest before all other addons
- kube-addon-manager is handled by kubelet

Learn more

MCP Reference Architecture: Kubernetes cluster components
**Automatic Calico upgrade procedure**

TECHNICAL PREVIEW

Implemented the automatic upgrade procedure for Calico from version 2.6 to 3.3 by adjusting the existing Kubernetes upgrade pipeline job.

Additionally, you can use the same pipeline job to update Calico to a minor version, for example, from 3.1 to 3.3.

The Calico upgrade process implies the Kubernetes services downtime for workloads operations, for example, workloads spawning and removing. The downtime is caused by the necessity of the etcd schema migration where the Calico endpoints data and other Calico configuration data is stored.

Learn more

MCP Operations Guide: Update or upgrade Kubernetes

**Horizontal pod autoscaling**

Introduced the capability to adjust the number of a Kubernetes pod replicas without using an external orchestrator by enabling the horizontal pod autoscaling feature. The feature is based on observed CPU and/or memory utilization and can be enabled using the metrics-server add-on. You can enable horizontal pod autoscaling either on a new or existing MCP Kubernetes cluster.

Learn more

MCP Deployment Guide: Enable horizontal pod autoscaling

**OpenStack cloud provider**

TECHNICAL PREVIEW in 2019.2.0, GA in 2019.2.2

Implemented the capability to use the OpenStack cloud provider functionality on new Kubernetes clusters that are deployed on VMs on top of OpenStack.

The OpenStack cloud provider extends the basic functionality of Kubernetes by fulfilling the provider requirement for several resources. This is achieved through communication with several OpenStack APIs.
The two main functions provided by the OpenStack cloud provider are PersistentVolume for pods and LoadBalancer for services.

Note
Full support for the OpenStack cloud provider is announced in the MCP 2019.2.2 update.

Learn more
- Known issue
- MCP Reference Architecture: OpenStack cloud provider for Kubernetes
- MCP Deployment Guide: Deploy OpenStack cloud provider for Kubernetes

Virtlet 1.4.4 support
Updated Virtlet to version 1.4.4 that contains the following improvements:
- Added support for Kubernetes 1.12.x
- Added support for containerd
- Added support for cpusets
- Switched to the Mirantis hardened version of libvirt
- Improved the Virtlet examples
- Added injecting of ConfigMaps or Secrets into rootfs
- Improved the Virtlet user documentation and made it available from https://docs.virtlet.cloud to introduce a more user-friendly format
- Fixed a number of bugs to harden the product robustness

Learn more
- Virtlet release notes
- Virtlet official documentation

OpenContrail
• OpenContrail 4.1 support for OpenStack
• Upgrade path from OpenContrail 3.2 to 4.1
• Update path from OpenContrail 4.0 to 4.1

OpenContrail 4.1 support for OpenStack
Added support for the community OpenContrail version 4.1 integrated with the following OpenStack releases: Ocata, Pike, Queens.

Note
The OpenContrail 4.x integration with Kubernetes 1.12 or later is not supported.

Learn more
• Release notes for the community version of Contrail 4.1
• MCP Reference Architecture: Plan OpenContrail Networking
• MCP Deployment Guide: Deploy OpenStack with OpenContrail using DriveTrain
• MCP Deployment Guide: Deploy OpenContrail manually

Upgrade path from OpenContrail 3.2 to 4.1
TECHNICAL PREVIEW
Implemented the automatic upgrade procedure for OpenContrail from version 3.2 to 4.x that allows upgrading the OpenContrail nodes in an Ocata- or Pike-based MCP cluster to version 4.1 using the Deploy - upgrade Opencontrail to 4.x Jenkins pipeline job.

Learn more
MCP Operations Guide: Upgrade the OpenContrail nodes from version 3.2 to 4.1
Update path from OpenContrail 4.0 to 4.1

TECHNICAL PREVIEW

Implemented the automatic update procedure for OpenContrail 4.x that covers the update of OpenContrail nodes from version 4.0 to 4.1. The update is performed using the Deploy - update OpenContrail to 4.x Jenkins pipeline job.

Learn more

MCP Operations Guide: Update the OpenContrail 4.x nodes

StackLight LMA

- StackLight components versions update
- Salesforce notifier service
- Retention policy for logs and audit indices

StackLight components versions update

Updated the versions of the following StackLight LMA components:

- Prometheus from version 2.2.1 to 2.5.0
- Alerta from version 5.6.10 to 6.5.0
- Alertmanager from version 0.14.0 to 0.15.3
- Pushgateway from version 0.4.0 to 0.6.0
- Grafana from version 5.2.4 to 5.3.4
- Telegraf from version 1.5.3 to 1.9.1
- td-agent from version 3.1.1-0 to 3.2.1
- Fluentd from version 1.0.2 to 1.2.6
- Elasticsearch from version 5.6.12 to 6.5.2
- Kibana from version 5.6.12 to 6.5.2

Learn more

Major components versions
Salesforce notifier service

Implemented the capability to configure Alertmanager to create Salesforce cases from Alertmanager notifications through the Salesforce notifier service. If you have already enabled Salesforce or email notifications through the Push Notification service, follow the procedure described in MCP Operations Guide: Switch to Alertmanager-based notifications.

Learn more

• MCP Operations Guide: Enable Salesforce notifications through Alertmanager
• MCP Operations Guide: Switch to Alertmanager-based notifications

Retention policy for logs and audit indices

Added the capability to manage the retention policy for logs and audit indices in an Elasticsearch cluster.

Learn more

MCP Operations Guide: Configure Elasticsearch Curator

Storage

• Ceph update to a minor version
• Native Prometheus support

1(1, 2) The major version of the component has been updated in 2019.2.2. See Updated packages and StackLight addressed issues for details.
2 The minor version of the component has been updated in 2019.2.4. See Updated MCP components and StackLight addressed issues for the Stacklight-related changes for details.
Ceph update to a minor version

TECHNICAL PREVIEW

Implemented the capability to update Ceph packages to the latest minor versions on the Ceph OSD, Monitor, and RADOS Gateway nodes using the Update Ceph packages pipeline job.

Learn more

MCP Operations Guide: Update Ceph

Native Prometheus support

Improved Ceph monitoring by adding support for the Ceph Prometheus plugin that is based on the native Prometheus exporter introduced in Ceph Luminous. The Ceph Prometheus plugin collects a wider set of Ceph metrics as opposed to Telegraf and provides for better monitoring capabilities for large clusters. Updated Ceph-related Grafana dashboards to display new metrics.

For new deployments, the Ceph Prometheus plugin is enabled by default. For existing deployments, you can enable the Ceph Prometheus plugin manually or during the upgrade of StackLight LMA.

Learn more

- MCP Operations Guide: Enable the Ceph Prometheus plugin
- MCP Operations Guide: Upgrade StackLight LMA using the Jenkins job
- MCP Operations Guide: Ceph dashboards
**Release artifacts**

The MCP release artifacts are tagged with the 2019.2.0 Release Version tag including APT repository snapshots, Git repository tags, and Docker image versions.

The combination of versions of MCP components that can be installed using the artifacts tagged with the 2019.2.0 Release Version tag are listed in Major components versions. These versions combinations have passed integration testing and are considered stable and working, with the known issues.

---

**Note**

To view the list of software packages used in MCP with their respective license information, where available, download MCP 2019.2.0 Encryption and Licensing.

---

### MCP release artifacts

<table>
<thead>
<tr>
<th>Type</th>
<th>Artifact</th>
<th>Path for Build ID 2019.2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirantis apt/deb packages</td>
<td>Extra packages</td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/extra/xenial">http://mirror.mirantis.com/2019.2.0/extra/xenial</a> xenial main ³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/extra/trusty">http://mirror.mirantis.com/2019.2.0/extra/trusty</a> trusty main ³</td>
</tr>
<tr>
<td>Ceph</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/ceph-luminous/xenial">http://mirror.mirantis.com/2019.2.0/ceph-luminous/xenial</a> xenial main ³</td>
</tr>
<tr>
<td>OpenContrail packages</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/opencontrail-3.2/xenial">http://mirror.mirantis.com/2019.2.0/opencontrail-3.2/xenial</a> xenial main</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/opencontrail-3.2/trusty">http://mirror.mirantis.com/2019.2.0/opencontrail-3.2/trusty</a> trusty main</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/opencontrail-4.0/xenial">http://mirror.mirantis.com/2019.2.0/opencontrail-4.0/xenial</a> xenial main</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/opencontrail-4.1/xenial">http://mirror.mirantis.com/2019.2.0/opencontrail-4.1/xenial</a> xenial main</td>
</tr>
<tr>
<td>Package Type</td>
<td>Packages</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>OpenStack packages</td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/openstack-mitaka/xenial">http://mirror.mirantis.com/2019.2.0/openstack-mitaka/xenial</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/openstack-ocata/xenial">http://mirror.mirantis.com/2019.2.0/openstack-ocata/xenial</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/openstack-pike/xenial">http://mirror.mirantis.com/2019.2.0/openstack-pike/xenial</a> 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/openstack-queens/xenial">http://mirror.mirantis.com/2019.2.0/openstack-queens/xenial</a> 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>deb <a href="https://mirror.mirantis.com/update/2019.2.0/openstack-pike/xenial">https://mirror.mirantis.com/update/2019.2.0/openstack-pike/xenial</a></td>
<td></td>
</tr>
<tr>
<td>Salt formulas packages</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/salt-formulas/xenial">http://mirror.mirantis.com/2019.2.0/salt-formulas/xenial</a></td>
<td></td>
</tr>
<tr>
<td>QCOW images</td>
<td>MCP cfg01 day01 image <a href="http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5">http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2">http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCP apt01 offline image <a href="http://images.mirantis.com/mcp-offline-image-2019.2.0.qcow2.md5">http://images.mirantis.com/mcp-offline-image-2019.2.0.qcow2.md5</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://images.mirantis.com/mcp-offline-image-2019.2.0.qcow2">http://images.mirantis.com/mcp-offline-image-2019.2.0.qcow2</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCP Ubuntu 16.04 image 3 <a href="http://images.mirantis.com/ubuntu-16-04-x64-mcp2019.2.0.qcow2.md5">http://images.mirantis.com/ubuntu-16-04-x64-mcp2019.2.0.qcow2.md5</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://images.mirantis.com/ubuntu-16-04-x64-mcp2019.2.0.qcow2">http://images.mirantis.com/ubuntu-16-04-x64-mcp2019.2.0.qcow2</a></td>
<td></td>
</tr>
<tr>
<td>Upstream mirrors</td>
<td>aptly deb <a href="http://mirror.mirantis.com/2019.2.0/aptly/xenial">http://mirror.mirantis.com/2019.2.0/aptly/xenial</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>squeeze main</td>
<td></td>
</tr>
<tr>
<td>Cassandra</td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/cassandra/trusty">http://mirror.mirantis.com/2019.2.0/cassandra/trusty</a> 21x main</td>
<td></td>
</tr>
<tr>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/cassandra/xenial">http://mirror.mirantis.com/2019.2.0/cassandra/xenial</a> 21x main</td>
<td></td>
</tr>
<tr>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/cassandra/xenial">http://mirror.mirantis.com/2019.2.0/cassandra/xenial</a> 21x main 3</td>
<td></td>
</tr>
<tr>
<td>Docker</td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/docker/xenial">http://mirror.mirantis.com/2019.2.0/docker/xenial</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>xenial stable 3</td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Type</td>
<td>URL</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Elastic</td>
<td>deb</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/elasticsearch-5.x/xenial">http://mirror.mirantis.com/2019.2.0/elasticsearch-5.x/xenial</a> stable main</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://mirror.mirantis.com/2019.2.0/elasticsearch-6.x/xenial">http://mirror.mirantis.com/2019.2.0/elasticsearch-6.x/xenial</a> stable main</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://mirror.mirantis.com/2019.2.0/elasticsearch-curator/xenial">http://mirror.mirantis.com/2019.2.0/elasticsearch-curator/xenial</a> stable main</td>
</tr>
<tr>
<td>Fluentd</td>
<td>deb</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/td-agent/xenial">http://mirror.mirantis.com/2019.2.0/td-agent/xenial</a> xenial contrib</td>
</tr>
<tr>
<td>GlusterFS</td>
<td>deb</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/glusterfs-3.8/xenial">http://mirror.mirantis.com/2019.2.0/glusterfs-3.8/xenial</a> xenial main</td>
</tr>
<tr>
<td>InfluxDB</td>
<td>deb</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/influxdb/xenial">http://mirror.mirantis.com/2019.2.0/influxdb/xenial</a> xenial stable</td>
</tr>
<tr>
<td>MAAS</td>
<td>deb</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/maas/xenial">http://mirror.mirantis.com/2019.2.0/maas/xenial</a> xenial main</td>
</tr>
<tr>
<td>Percona</td>
<td>deb</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/percona/xenial">http://mirror.mirantis.com/2019.2.0/percona/xenial</a> xenial main</td>
</tr>
<tr>
<td>SaltStack packages</td>
<td>deb</td>
<td><a href="http://mirror.mirantis.com/2019.2.0/saltstack-2017.7/trusty">http://mirror.mirantis.com/2019.2.0/saltstack-2017.7/trusty</a> trusty main</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://mirror.mirantis.com/2019.2.0/saltstack-2017.7/xenial">http://mirror.mirantis.com/2019.2.0/saltstack-2017.7/xenial</a> xenial main</td>
</tr>
<tr>
<td>Upstream Ubuntu</td>
<td>deb</td>
<td><a href="https://mirror.mirantis.com/2019.2.0/ubuntu/">https://mirror.mirantis.com/2019.2.0/ubuntu/</a> xenial main restricted universe</td>
</tr>
<tr>
<td>system packages</td>
<td></td>
<td><a href="https://mirror.mirantis.com/2019.2.0/ubuntu/xenial-updates">https://mirror.mirantis.com/2019.2.0/ubuntu/xenial-updates</a> main restricted universe</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://mirror.mirantis.com/2019.2.0/ubuntu/xenial-security">https://mirror.mirantis.com/2019.2.0/ubuntu/xenial-security</a> main restricted universe</td>
</tr>
<tr>
<td>MCP Git repositories</td>
<td>Jenkins pipeline library for MCP operations</td>
<td><a href="https://github.com/Mirantis/mk-pipelines/release/2019.2.0">https://github.com/Mirantis/mk-pipelines/release/2019.2.0</a></td>
</tr>
<tr>
<td></td>
<td>General Jenkins pipeline library</td>
<td><a href="https://github.com/Mirantis/pipeline-library/release/2019.2.0">https://github.com/Mirantis/pipeline-library/release/2019.2.0</a></td>
</tr>
<tr>
<td></td>
<td>Reclass system level</td>
<td><a href="https://github.com/Mirantis/reclass-system-salt-model/release/2019.2.0">https://github.com/Mirantis/reclass-system-salt-model/release/2019.2.0</a></td>
</tr>
<tr>
<td><strong>MCP common scripts</strong></td>
<td><a href="https://github.com/Mirantis/mcp-common-scripts">https://github.com/Mirantis/mcp-common-scripts</a> release/2019.2.0</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>MCP offline image model</strong></td>
<td><a href="https://github.com/Mirantis/mcp-offline-model">https://github.com/Mirantis/mcp-offline-model</a> release/2019.2.0</td>
<td></td>
</tr>
<tr>
<td><strong>Docker images</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>coredns</td>
<td><a href="docker-prod-local.artifactory.mirantis.com/mirantis/coredns/coredns:v1.2.6-4">docker-prod-local.artifactory.mirantis.com/mirantis/coredns/coredns:v1.2.6-4</a></td>
<td></td>
</tr>
<tr>
<td>etcd-operator</td>
<td><a href="quay.io/coreos/etcd-operator:v0.9.3">quay.io/coreos/etcd-operator:v0.9.3</a></td>
<td></td>
</tr>
<tr>
<td>flannel</td>
<td><a href="quay.io/coreos/flannel:v0.10.0-amd64">quay.io/coreos/flannel:v0.10.0-amd64</a></td>
<td></td>
</tr>
<tr>
<td>Image Name</td>
<td>Registry URL</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>k8s-netchecker-agent</td>
<td>mirantis/k8s-netchecker-agent:v1.2.2 (at hub.docker.com)</td>
<td></td>
</tr>
<tr>
<td>k8s-netchecker-server</td>
<td>mirantis/k8s-netchecker-server:v1.2.2 (at hub.docker.com)</td>
<td></td>
</tr>
<tr>
<td>kube-controllers</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/kube-controllers:v3.3.2</td>
<td></td>
</tr>
<tr>
<td>metallb-controller</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/metallb/controller:v0.7.3-2</td>
<td></td>
</tr>
<tr>
<td>metallb-speaker</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/metallb/speaker:v0.7.3-2</td>
<td></td>
</tr>
<tr>
<td>metrics-server</td>
<td>k8s.gcr.io/metrics-server-amd64:v0.3.1</td>
<td></td>
</tr>
<tr>
<td>mysql</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>node</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/node:v3.3.2</td>
<td></td>
</tr>
<tr>
<td>openldap</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/openldap:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>pause</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/pause-amd64:v1.12.4-3</td>
<td></td>
</tr>
<tr>
<td>phpldapadmin</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/phpldapadmin:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>postgres</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10</td>
<td></td>
</tr>
<tr>
<td>prometheus</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>prometheus_relay</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus_relay:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>pushgateway</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>registry</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>remote_storage_adapter</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>sf_notifier</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>telegraf</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>tiller</td>
<td>gcr.io/kubernetes-helm/tiller:v2.12.2</td>
<td></td>
</tr>
<tr>
<td>virtlet</td>
<td>mirantis/virtlet:v1.4.4 (at hub.docker.com)</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>visualizer</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.0</td>
<td></td>
</tr>
</tbody>
</table>
| calico-bird   | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/calico-bird | Other
| calico-ctl    | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/calico-ctl |
| calico-cni    | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/calico-cni |
| calico-ipam   | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/calico-ipam |
| cni-genie     | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/cni-genie |
| containernetworking-plugins | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/containernetworking-plugins |
| etcd          | https://github.com/etcd-io/etcd/releases/download/v3.3.10/etcd-v3.3.10-linux-amd64.tar.gz |
| helm          | https://storage.googleapis.com/kubernetes-helm/helm-v2.12.2-linux-amd64.tar.gz |
| hyperkube-amd64 | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/hyperkube-binaries/hyperkube_v1.12.4-3_1547129775753 |
| openstack-cloud-controller-manager | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/cloud-provider-openstack/openstack-cloud-controller-manager_v0.3.0-1_1543239267245 |
| sriov         | docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/sriov-cni/sriov_v0.3-9-g3b31f1a |

3(1, 2, 3, 4, 5) Available in the MCP offline image in the reduced size. For details, see: MCP Reference Architecture: Mirror image content.
4 Available with the MCP 2019.2.1 update. See 2019.2.1 for details.
5 Available with the MCP 2019.2.2 update. See 2019.2.2 for details.
6(1, 2, 3) Available with the MCP 2019.2.3 update. See 2019.2.3 for details.

©2020, Mirantis Inc.

Page 21
## Major components versions

The following tables list the MCP components of the Q4`18 Release Version with Build ID 2019.2.0. These components are initially installed by default depending on the cluster deployment model.

For comparison purposes, the tables also list the MCP components versions of the previous GA MCP Release Version with the Build ID 2018.11.0.

The tables divide the following types of the MCP components and their respective subcomponents:

- **Software components and Release Versions from the Mirantis repositories**
  Includes components from the Mirantis repositories that are built and managed by Mirantis. Some packages from these repositories substitute the same packages from mirrored repositories using combinations of package versions and repositories priorities of an MCP cluster.

- **Software components and Release Versions from mirrored repositories**
  Includes components from mirrored repositories that are redistributed by Mirantis but unmodified with regard to their upstream version.

### Software components and Release Versions from the Mirantis repositories

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2018.11.0</th>
<th>2019.2.0 (current release)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed storage</td>
<td>Ceph</td>
<td>12.2.8-1~u16.04+mcp0</td>
<td>12.2.11-1</td>
<td>Luminous v12.2.11 Release Notes</td>
</tr>
<tr>
<td>DriveTrain</td>
<td>Aptly</td>
<td>1.3.0</td>
<td>1.3.0</td>
<td>Resource type - Docker image</td>
</tr>
<tr>
<td></td>
<td>aptly-publisher</td>
<td>0.12.11</td>
<td>0.12.12</td>
<td>Resource type - Docker image</td>
</tr>
<tr>
<td></td>
<td>Gerrit</td>
<td>2.13.6</td>
<td>2.15.17</td>
<td>Resource type - Docker image</td>
</tr>
<tr>
<td></td>
<td>jenkins-master</td>
<td>2.121.2, 2.121.3</td>
<td>2.150.3</td>
<td>Resource type - Docker image</td>
</tr>
<tr>
<td></td>
<td>Jenkins pipeline-library</td>
<td>2018.11.0</td>
<td>2019.2.0</td>
<td>Resource type - Git repository</td>
</tr>
<tr>
<td></td>
<td>Reclass</td>
<td>1.5.1-1tcp4</td>
<td>1.5.6-1.0~u16.04+mcp0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reclass model</td>
<td>2018.11.0</td>
<td>2019.2.0</td>
<td>Resource type - Git repository</td>
</tr>
<tr>
<td></td>
<td>Salt formulas</td>
<td>2018.11.0</td>
<td>2019.2.0</td>
<td>Resource type - binary repository only</td>
</tr>
<tr>
<td>Category</td>
<td>Component</td>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------</td>
<td>--------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypervisors</td>
<td>sosreport</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>libvirt</td>
<td>4.0.0-1.7~u16.04+mcp1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>qemu</td>
<td>2.11+dfsg-1.4~u16.04+mcp1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kubernetes</td>
<td>CNI-Genie</td>
<td>1.0-191</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNI-plugins</td>
<td>0.7.2-96</td>
<td>0.7.2-173</td>
<td></td>
<td></td>
</tr>
<tr>
<td>containerd</td>
<td>n/a</td>
<td>1.25-2~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRI Proxy</td>
<td>0.12.0</td>
<td>0.14.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dashboard</td>
<td>1.10.0-4</td>
<td>1.10.1-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ExternalDNS</td>
<td>0.5.6-2</td>
<td>0.5.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kubernetes</td>
<td>1.11.3</td>
<td>1.13.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MetalLB</td>
<td>0.7.3-2</td>
<td>0.7.3-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGINX Ingress</td>
<td>0.19.0-1</td>
<td>nginx-0.24.1-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>controller</td>
<td>OpenStack cloud</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR-IOV</td>
<td>0.3-9</td>
<td>0.3-9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtlet</td>
<td>1.4.1</td>
<td>1.5.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenContrail</td>
<td>Cassandra</td>
<td>2.2.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kafka</td>
<td>2.11-0.9.0.1-0contrail1-0.9.0.1-0contrail1 1.1.1-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenContrail</td>
<td>4.0.4.0</td>
<td>4.1.4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>3.4.8</td>
<td>3.4.8, 3.4.8-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenStack Pike</td>
<td>Barbican</td>
<td>5.0.0-3~u16.04+mcp1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: OpenContrail 4.x for Kubernetes 1.12 or later is not supported. OpenContrail 3.2 is not supported for new deployments.*
<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cinder</td>
<td>11.1.1-2<del>u16.04+mcp17.2.2-3</del>u16.04+mcp138</td>
<td></td>
</tr>
<tr>
<td>Designate</td>
<td>5.0.2-2<del>u16.04+mcp16.0.3-3</del>u16.04+mcp16</td>
<td></td>
</tr>
<tr>
<td>Glance</td>
<td>15.0.1-1<del>u16.04+mcp15.2.2-2</del>u16.04+mcp16</td>
<td></td>
</tr>
<tr>
<td>Heat</td>
<td>9.0.4-1<del>u16.04+mcp14.1.7-2</del>u16.04+mcp88</td>
<td></td>
</tr>
<tr>
<td>Horizon</td>
<td>12.0.3-2<del>u16.04+mcp12.0.4-5</del>u16.04+mcp80</td>
<td></td>
</tr>
<tr>
<td>Ironic</td>
<td>9.1.4-1<del>u16.04+mcp12.9.6-2</del>u16.04+mcp56+ full support starting from 2019.2.6</td>
<td></td>
</tr>
<tr>
<td>Keystone</td>
<td>12.0.1-4<del>u16.04+mcp12.0.3-5</del>u16.04+mcp26</td>
<td></td>
</tr>
<tr>
<td>Manila</td>
<td>5.0.1-1<del>u16.04+mcp11.0.2-2</del>u16.04+ Map38 deprecation notice</td>
<td></td>
</tr>
<tr>
<td>Nova</td>
<td>16.1.4-3<del>u16.04+mcp16.128-6</del>u16.04+mcp169</td>
<td></td>
</tr>
<tr>
<td>OpenStack Networking Pike L2 Gateway</td>
<td>11.0.0-1<del>u16.04+mcp15.0.0-1</del>u16.04+mcp19</td>
<td></td>
</tr>
<tr>
<td>BGP VPN</td>
<td>11.0.0-1<del>u16.04+mcp15.0.0-1</del>u16.04+mcp19</td>
<td></td>
</tr>
<tr>
<td>ODL ML2 plugin</td>
<td>11.0.0-1<del>u16.04+mcp15.0.0-1</del>u16.04+mcp19+ neutron-plugin-ml2</td>
<td></td>
</tr>
<tr>
<td>Neutron</td>
<td>11.0.6-2<del>u16.04+mcp11.0.2-5</del>u16.04+mcp228</td>
<td></td>
</tr>
<tr>
<td>Octavia</td>
<td>1.0.2-6<del>u16.04+mcp1.0.6-8</del>u16.04+mcp21</td>
<td></td>
</tr>
<tr>
<td>OpenStack Telemetry Pike Aodh</td>
<td>5.1.0-3<del>u16.04+mcp10.0.4-4</del>u16.04+mcp16</td>
<td></td>
</tr>
<tr>
<td>Ceilometer</td>
<td>9.0.5-2<del>u16.04+mcp16.0.7-3</del>u16.04+mcp30</td>
<td></td>
</tr>
<tr>
<td>Panko</td>
<td>3.1.0-1<del>u16.04+mcp11.2-2</del>u16.04+mcp18</td>
<td></td>
</tr>
<tr>
<td>Gnocchi</td>
<td>4.0.5-2<del>u16.04+mcp25.3-3</del>u16.04+mcp2 Telemetry</td>
<td></td>
</tr>
<tr>
<td>OpenStack Queens</td>
<td>7 Barbican</td>
<td>6.0.1-4<del>u16.04+mcp12.0.1-6</del>u16.04+mcp32</td>
</tr>
<tr>
<td>Cinder</td>
<td>12.0.4-2<del>u16.04+mcp12.9.9-3</del>u16.04+mcp118</td>
<td></td>
</tr>
<tr>
<td>Designate</td>
<td>6.0.1-1.0<del>u16.04+mcp16.0.1-1.1</del>u16.04+mcp25</td>
<td></td>
</tr>
<tr>
<td>Glance</td>
<td>16.0.1-2<del>u16.04+mcp12.0.1-3</del>u16.04+mcp32</td>
<td></td>
</tr>
<tr>
<td>Heat</td>
<td>10.0.2-1.0<del>u16.04+mcp10.1.7-1.1</del>u16.04+mcp93</td>
<td></td>
</tr>
<tr>
<td>Horizon</td>
<td>13.0.1-9<del>u16.04+mcp3.0.2-10</del>u16.04+mcp87</td>
<td></td>
</tr>
<tr>
<td>Ironic</td>
<td>10.1.6-1.0<del>u16.04+mcp10.2.9-1.1</del>u16.04+mcp62</td>
<td></td>
</tr>
<tr>
<td>Keystone</td>
<td>13.0.1-3<del>u16.04+mcp13.0.4-4</del>u16.04+mcp31</td>
<td></td>
</tr>
<tr>
<td>Component/Application/service</td>
<td>2018.11.0</td>
<td>2019.2.0 (current release)</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>DriveTrain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAAS</td>
<td>2.3.5</td>
<td>2.3.5</td>
</tr>
<tr>
<td>SaltStack</td>
<td>2017.7.7</td>
<td>2017.7.8</td>
</tr>
<tr>
<td>GlusterFS</td>
<td>3.8</td>
<td>5.5</td>
</tr>
<tr>
<td>Kubernetes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calico</td>
<td>3.1.3</td>
<td>3.3.1</td>
</tr>
<tr>
<td>Calico CNI</td>
<td>3.1.3</td>
<td>3.3.1</td>
</tr>
<tr>
<td>CoreDNS</td>
<td>1.2.2-12</td>
<td>1.4.0</td>
</tr>
<tr>
<td>etcd</td>
<td>3.3.8</td>
<td>3.3.12</td>
</tr>
</tbody>
</table>

©2020, Mirantis Inc.
<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>etcd Operator</td>
<td>0.9.2</td>
</tr>
<tr>
<td>Flannel</td>
<td>0.10.0-amd64</td>
</tr>
<tr>
<td>Helm</td>
<td>n/a</td>
</tr>
<tr>
<td>Metrics Server</td>
<td>n/a</td>
</tr>
<tr>
<td>Tiller</td>
<td>n/a</td>
</tr>
<tr>
<td>OpenContrail networking</td>
<td>Redis 2:3.0</td>
</tr>
<tr>
<td>StackLight LMA</td>
<td>5.6.10</td>
</tr>
<tr>
<td>Alert</td>
<td>0.14.0</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>5.6.12</td>
</tr>
<tr>
<td>Fluentd</td>
<td>1.0.2</td>
</tr>
<tr>
<td>Grafana</td>
<td>5.2.4</td>
</tr>
<tr>
<td>Heka</td>
<td>0.10.1</td>
</tr>
<tr>
<td>InfluxDB</td>
<td>1.5.2-1</td>
</tr>
<tr>
<td>Kibana</td>
<td>5.6.12</td>
</tr>
<tr>
<td>MongoDB</td>
<td>2.6.10</td>
</tr>
<tr>
<td>Prometheus</td>
<td>2.2.1</td>
</tr>
<tr>
<td>Pushgateway</td>
<td>0.4.0</td>
</tr>
<tr>
<td>System</td>
<td>Docker</td>
</tr>
<tr>
<td></td>
<td>docker-ce 18.06.1, docker-engine 1.13.1</td>
</tr>
<tr>
<td>Git</td>
<td>2.7.4</td>
</tr>
<tr>
<td>GitLab</td>
<td>3.8.15</td>
</tr>
<tr>
<td>GlusterFS</td>
<td>5:18.09.0<del>3-0</del>ubuntu-xenial</td>
</tr>
<tr>
<td>Hekapushy</td>
<td>1.10.3</td>
</tr>
<tr>
<td>nginx</td>
<td>1.10.3</td>
</tr>
<tr>
<td>Kubernetes</td>
<td>11.10.3</td>
</tr>
<tr>
<td>MySQL</td>
<td>8.0.18</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>9.6</td>
</tr>
<tr>
<td>System</td>
<td>Docker</td>
</tr>
<tr>
<td></td>
<td>docker-ce 18.06.1, docker-engine 1.13.1</td>
</tr>
</tbody>
</table>

For the OpenStack releases support schedule, see [MCP OpenStack Releases](#). When newer versions of Ubuntu packages are available in the Mirantis repositories, MCP installs them instead of older versions available in the Ubuntu repositories.

For OpenStack Pike

For OpenStack Queens

The component has been added in 2019.2.3.

The major version of the component has been updated in 2019.2.4. See [Updated MCP components, StackLight addressed issues for 2019.2.2, and StackLight addressed issues for 2019.2.4](#) for details.

OpenContrail 4.0 is deprecated in the sake of OpenContrail 4.1 and not supported for new deployments since 2019.2.7.
Addressed issues

This section provides the list of the addressed issues in the current MCP release version.

DriveTrain

- Fixed the issue with the Linux kernel headers failing to install automatically during the upgrade of an MCP cluster.
- Fixed the issue with the Nova and Cinder tests failing when performing the sanity testing using the CVP - Sanity checks Jenkins pipeline job on the OpenStack Queens environments.
- Fixed the issue with the Deploy - upgrade MCP Drivetrain Jenkins pipeline job failing on the Update Drivetrain stage with the Failed to load ext_pillar reclass: ext_pillar.reclass error message. The issue affected the Kubernetes Calico-based deployments.
- Fixed the issue with the OpenStack endpoints being unreachable when the HAPProxy service stopped on the ctl, ntw, dbs, rgw, and prx VIP nodes.
- Fixed the issue that caused MySQL being not available in case when the HAPProxy service went down on a node. Added the Keepalived VRRP check on the dbs and other VCP nodes.
- Fixed the issue with the requests hanging when connecting to the database due to the default HAPProxy connection limit being too low for large clusters. Increased the maximum number of connections handled by the HAPProxy process to 25000 by default and added the capability to modify this value.
- Implemented the cleanup commissioning script to fix the issue with MAAS failing to reprovision hardware nodes with old software RAID. For details, see: MCP Deployment Guide: Add custom commissioning scripts.
- Fixed the issue with OpenStack Nova missing the Memcached configuration for large clusters.
- Fixed the issue with the CVP - Simplified performance tests (SPT) Jenkins pipeline job freezing in case if HW_NODES was set to an odd number of ctl and cmp nodes. In this case, the iperf processes kept running, which could cause subsequent pipeline job failures.
- Fixed the issue with MAAS importing unnecessary large images during the Salt Master node bootstrapping and causing timeout errors, for example, TimeoutError: Node 'cfg01.cookie-cid-k8s-calico.local' didn't open SSH in 1800 sec.
- Fixed the issue with the MCP cluster deployment pipeline jobs failing with the Can't contact LDAP server error message.

OpenStack

- Fixed the issue that caused the Unable to retrieve image list error message to appear on the Admin > Compute > Instance tab in OpenStack Horizon.
- Fixed the issue with inability to modify access for an existing flavor in OpenStack Horizon.
- Fixed the issue with OpenStack Horizon being unavailable if apache2 was stopped on a VIP prx node.
• Fixed the issue that caused failures of the OpenStack Pike or Queens deployment in case of Keystone connected to LDAP.

• Fixed the following RabbitMQ and Oslo issues:
  • RabbitMQ crashes
  • RabbitMQ failing to recover the cluster during the network segmentation
  • Sporadic message loss causing unreliable functioning of Neutron and some other services
• Fixed the issue with the Deploy - upgrade control VMs Jenkins pipeline job failing with the Service Unavailable (HTTP 503) error message.

• Fixed the issue with some services failing to start in case of the cinder-backup service enabled in OpenStack Queens.

• Fixed the issue with the cinder-backup service failing to start in OpenStack Queens.

• Fixed the issue with libvirt occasionally creating incorrect AppArmor rules.

• Fixed the issue with the Deploy - OpenStack Jenkins pipeline job failing in case of Redis 5.0 package installed.

• Fixed the issue with the Apache server-status module that exposed the server status metrics to an external proxy allowing an unauthenticated user to access the Server-Status web page in Horizon and gather sensitive information.

• Fixed the issue with the Tempest tests failures when Nova integration with Barbican is enabled. The Tempest tests for Nova that perform booting from an instance snapshot and unshelving of a shelved instance are now being skipped to prevent the Tempest tests failures. For details, see: MCP Deployment Guide: Deploy Barbican.

• Fixed the issue with MCP OpenStack deployments keeping only four log rotations, which could prevent from investigating the issues in detail. Now, MCP OpenStack deployments keep logs for 10 days by default.

• Fixed the issue with the Keystone catalog containing deprecated Cinder API v1 endpoints, which raised the CinderApiDown alert.

• Fixed the issue with the Designate Tempest test failing in case of a small number of Designate quota zones configured.

• Added the capability to set certain HAProxy check parameters to fix the issue with HTTP checks failing due to the lack of configuration when using SSL for the Designate, Glance, Heat, Keystone, Nova, Manila, and Neutron services.

• Fixed the issue with the Redis server not requiring authentication.

• Fixed the issue with Gnocchi containing a significant number of errors in the metricd logs in the Queens-based OpenStack deployments with Telemetry.

• Fixed the issue with the OVS network configuration occasionally failing to apply after rebooting a node on the OpenStack Pike or Queens environments with a custom interfaces configuration. This could cause the Exhausted all hosts available error for build instances.
• Fixed the issue with the ohm port moving to the DOWN state in case of the gtw01 node reboot, which affected the creation of new load balancers on the OpenStack environments with Octavia enabled.

• Fixed the issue with the Deploy - OpenStack deployment pipeline job failing when the LDAP integration for Keystone is enabled. The issue affected the OpenStack Pike and Queens releases.

Kubernetes

• Fixed the issue that caused an incorrect work of DNS clusters if a cluster or domain name contained the _ symbol on the Kubernetes clusters with ExternalDNS.

OpenContrail

• Fixed the issue with lost connections that use the Source Network Address Translation (SNAT) mechanism when Service Function Chaining (SFC) is configured with port tuples and the service chain templates v2.

The connection could be lost once you restarted the active instance of the contrail-schema service that was a part of the supervisor-config aggregate service on the ntw nodes. Only OpenContrail v3.2 was affected.

• Fixed the issue with OpenContrail v3.2 API server connection timeouts occurring due to an issue with the internal IF-MAP.

• Fixed the issue with the network connection timeouts occurring when using the Link-Local Services (LLS).

• Fixed the issue with the contrail-vrouter-agent timeouts failing to start with the Module vrouter not found in directory /lib/modules/XXX error after the upgrade of an MCP cluster.

• Fixed the issue with the OpenContrail web UI displaying erroneous critical alarms for the failed Cassandra database and missing statistics for the configuration database on all ntw nodes in the OpenContrail v4.0 deployments.

• Fixed the issue with the OpenContrail v4.0 logs from zookeeper/zookeeper.log and cassandra/system.log missing in Kibana.

• Fixed the issue with the contrail-vrouter-agent service failing to connect to the contrail-control and contrail-dns services and causing the connection down error in the output of the contrail-status command.

• Fixed the issue with configuration of the access to DNS servers on the compute nodes for OpenContrail 4.0 causing the ContrailVrouterDNSXMPPSessionsZero StackLight LMA alerts.

• Fixed the issue with ZooKeeper failing to connect to Kafka on all analytics nodes and causing some services being stuck in the initializing state during the upgrade from OpenContrail v3.2 to v4.0.

StackLight LMA
• Fixed the issue with the GlusterFS service host for Kubernetes-based clusters referring to a wrong node, which caused Telegraf fail to gather metrics from GlusterFS.

• Fixed the issue with the proxy status metrics missing in the Grafana web UI in case of Kubernetes deployments with OpenContrail.

• Fixed the issue with alerts for dropped packets on PXE interfaces by removing the Major alert for dropped packets and decreasing the default threshold for the Warning alert for dropped packets from 100 to 60.

• Fixed the issue with the CephPoolWriteOpsTooHigh alert firing on healthy Ceph clusters by adding the capability to modify the alert threshold for individual pools.

**Storage**

• Updated the default permissions for Ceph clients to avoid issues with volumes reconnecting after a client crash.

• Fixed the issue with the inability to set public network parameters for the Ceph Monitor and RADOS Gateway nodes during the creation of a deployment model.

• Added the missing Ceph parameters required to generate a deployment model with Ceph through Cookiecutter templates.

---

**Mirantis Technical Bulletins**

Mirantis constantly focuses on the product quality and stability. Therefore, aside from the fixes of the security and critical flaws for the current MCP version affecting Mirantis products and services, we provide resolution for the customer deployments on top of the previous MCP versions, which can be affected, in the form of technical bulletins. Each technical bulletin includes the detailed issue description, possible impact, steps to determine whether a deployment is affected with the issue, procedure to resolve the issue, and revert the fix if required.

Such security and critical issue advisories are also proactively e-mailed to the customers with active service contracts.

For the full list of the Mirantis Technical Bulletins, refer to the Mirantis OpenStack Technical Bulletins page at the Mirantis official website.
Known issues
This section lists the MCP known issues and workarounds.

DriveTrain

• 15644
• 21033
• 24868
• 25172
• 26113
• 26330
• 26417
• 27010
• 27135
• 27638
• 32633
• 32079
• 28046
• 34308

15644
The network driver may fail to allocate kernel memory. You may also detect the following symptoms of the issue:

• Traces in kern.log related to the BNX driver
• Ceph OSD flapping in the Ceph cluster during a rebalance

To prevent the issue, calculate the sysctl minimum reserved memory and set it using the vm.min_free_kbytes parameter for each type of node depending on your cluster model.

Caution!
For performance reasons, verify that the value set for vm.min_free_kbytes does not exceed 5% of the entire memory.

Warning
Perform the steps below before the deployment of an OpenStack environment. For existing environments, first, accomplish the procedure on a staging environment. If the staging environment does not exist, adapt the exact cluster model and launch it inside the cloud as a heat stack, which will act as a staging environment.

Workaround:
1. Open your Git project repository with the Reclass model on the cluster level.

2. In `/etc/sysctl.conf` specify the following pillar:

```plaintext
linux:
  system:
    kernel:
      sysctl:
        vm.min_free_kbytes: <calculated_value>
```

3. Choose from the following options:

   • If you are making changes before the deployment, proceed with further configuration as required.
   • If you are making changes to an existing environment, apply the changes:

     1. Log in to the Salt Master node.
     2. Apply the following state:

        ```bash
        salt '*' state.apply linux.system.kernel
        ```

21033

The Salt Master CA does not provide the Certificate Revocation List (CRL) and index files to identify the revoked or expired certificates.

Workaround:

To list all currently issued certificates, follow the step 3 of the Replace the Salt Master CA certificates procedure.

24868

During the upgrade of an MCP cluster, after the installation of the salt-master, salt-common, salt-api, and salt-minion packages, the Deploy - update cloud pipeline may hang up with the Connection refused error message and trying to connect to salt-api.

Workaround:

1. Log in to the Salt Master node.
2. Restart the salt-api service:

   ```bash
   systemctl restart salt-api.service
   ```
3. Rerun the Deploy - update cloud pipeline.
25172
When changing any network settings (routes, up_cmds commands, MTU), the linux.network formula restarts the target interface and all related interfaces. For example, when changes are related to a bridge interface, all its interfaces will be restarted what leads to VMs failures. Therefore, Mirantis recommends configuring all required bridge interfaces on KVMs before a cluster deployment.

The workaround is to apply all required settings manually without a bridge restart. If a bridge restart on a KVM node is crucial:

1. Plan a maintenance window for your MCP cluster.
2. Stop all VMs of a node that requires a bridge restart.
3. Apply the required settings changes.
4. Restart the bridge interface.
5. Start all VMs.

26113
Fixed in 2019.2.3
Occasionally, the deployment of OpenContrail v4.x with OpenStack Pike may fail due to the duplication of the salt-minion services.

Workaround:

1. Log in to the Salt Master node.
2. Apply the following state:

   ```
salt -t 10 "rgw*" cmd.run 'pkill -9 salt-minion'
   ```

   The service restarts automatically in a few minutes.

26330
The CVP - Sanity checks Jenkins pipeline may fail if the TEST_REPO parameter is not empty.

Workaround:

Leave the TEST_REPO parameter empty. This option is deprecated starting MCP Build ID 2019.2.0.
26417
When commissioning nodes with Intel X520-2 10 GB Ethernet Network Interface Cards (NICs), such cards may not be discovered.
Workaround:
Do not use Intel X520-2 10GB NICs with firmware version 0x30030001.

27010
When upgrading from the MCP Build ID 2018.11.0 to 2019.2.0, the Deploy - upgrade MCP DriveTrain Jenkins pipeline job fails due to the mirror jobs failing to trigger the newest version.
Workaround:
1. Log in to the Jenkins web UI.
2. Run the `git-mirror-downstream-mk-pipelines` and `git-mirror-downstream-pipeline-library` Jenkins pipeline jobs with BRANCHES set to release/2019.2.0.
3. Rerun the Deploy - upgrade MCP DriveTrain Jenkins pipeline job with UPDATE_PIPELINES set to false.

27135
Fixed in 2019.2.3
Creating instant backups using Backupninja, Xtrabackup, ZooKeeper, or Cassandra may fail due to an issue with permissions.
Workaround:
1. Log in to the Salt Master node.
2. Obtain the SSH RSA key specified in `/root/.ssh/id_rsa.pub`.
3. On the system level of the Reclass model, add the obtained SSH RSA key to `system/<service_name>/server.yml` for Backupninja or Xtrabackup or to `system/<service_name>/backup/server.yml` for Cassandra or ZooKeeper. For example, for Backupninja add the following pillar to `system/backupninja/server.yml`.

```
parameters:
  backupninja:
    server:
      key:
        backupninja_pub_key: enabled: true
        key: <key_from_/root/id_rsa.pub>
```
4. Apply the corresponding service state. For example, for Backupninja apply the following state on the nodes with the Backupninja pillar defined:

```
salt -C 'I@backupninja:client or I@backupninja:server' state.sls backupninja
```

**Warning**

Since the steps above presuppose manual changes to the system level of the Reclass model, the changes will be removed in case of a system upgrade and you may need to apply them again.

---

**27638**

When performing operations through Jenkins that require the Salt Minion package update and restart, for example, MCP DriveTrain upgrade, a cloud environment update, packages update, and so on, Jenkins pipeline jobs may fail due to the known community dbus-daemon issue.

**Workaround:**

1. On the Salt Master node, run:

```
systemctl daemon-reexec
systemctl restart salt-minion
```

2. Log in to the Jenkins web UI.

3. Re-run the failed Jenkins pipeline job.

---

**32633**

Occasionally, application of the Salt states across all nodes during the deployment pipelines execution fails with Pepper error: Server error. The issue affects large deployments with a big number of Salt Minions and may affect the services deployment during the later deployment steps.

To workaround the issue, select from the following options:

- Enable the Salt batching for the affected Salt states. For example, if the linux.system state fails, apply the following patch to the pipeline-library repository:

```
diff --git a/src/com/mirantis/mk/Orchestrate.groovy b/src/com/mirantis/mk/Orchestrate.groovy
index 509fe87..575d6ca 100644
--- a/src/com/mirantis/mk/Orchestrate.groovy
+++ b/src/com/mirantis/mk/Orchestrate.groovy
```

©2020, Mirantis Inc.
The patch sets the batch size to 15% of the target nodes that include the "* ${extra_tgt}" nodes. In the absence of additional conditions, the state will be applied to the 15% of the total number of these nodes.

- Manually re-run the failed state. For example, if the salt.minion state fails, perform the following steps:

1. Log in to the Salt Master node.
2. Re-apply the failed state on the affected nodes manually:
   
   ```
   salt '*' state.sls salt.minion
   ```
3. Restart the salt-minion service manually:
   
   ```
   salt '*' cmd.run 'salt-call service.restart salt-minion'
salt '*' saltutil.clear_cache
salt '*' saltutil.refresh_pillar
salt '*' saltutil.sync_all
   ```

   During the restart of the salt-minion service, verify that the Salt Master node does not catch the exception with getting the lost minion.
4. Restart the failed pipeline to proceed with update, deployment, or another required operation.

32079

The values of the net.ipv4.neigh.default.gc_thresh1, net.ipv4.neigh.default.gc_thresh2, and net.ipv4.neigh.default.gc_thresh3 kernel parameters in pillars may differ from the ones in the output of the sysctl command on the mon* and ctl* nodes because of the specific values hardcoded in Docker.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `classes/cluster/<cluster_name>/cicd/control/init.yml` and `classes/cluster/<cluster_name>/infra/config/docker.yml`, add the following pillar:

   ```
   linux:
   system:
   ```

©2020, Mirantis Inc.
```yaml
kernel:
  # hardcoded in overlay network driver https://github.com/docker/libnetwork/pull/1789/files
sysctl:
  net.ipv4.neigh.default.gc_thresh1: 8192
  net.ipv4.neigh.default.gc_thresh2: 49152
  net.ipv4.neigh.default.gc_thresh3: 65536
```

3. If you have StackLight enabled, also add the same pillar to classes/cluster/<cluster_name>/stacklight/server.yml.

4. Apply the changes:

```bash
salt '*' saltutil.sync_all
```

---

### 28046

When the Open vSwitch (OVS) network interfaces have the same MAC address, for example, when a bond interface is split into several vLANs with tags, OVS prior to version 2.10 may not add flow rules to some OVS bridges.

**Workaround:**

Choose from the following options:

- Add a unique MAC address to the ports description. For example:

  ```yaml
  bond1.${_param:a1nt_public_vlan}:
    name: bond1.${_param:a1nt_public_vlan}
    enabled: true
    proto: manual
    type: ovs_port
    bridge: br-a1nt_public
    ovs_bridge: br-a1nt_public
    hwaddress: <unique_mac>
    ovs_port_type: OVSPort
    use_interfaces:

  bond1
  ```

- Use the following configuration order:
  1. Plug the tagged interfaces into the Linux bridges.
  2. Connect the Linux bridges into the OVS bridges.

- Use external networks:
  1. Pass the entire interface to the OVS bridge and map it to a single physical network.
  2. Split the interface on vLANs by setting provider:segmentation_id for each Neutron network.
34308
The Deploy - upgrade control VMs Jenkins pipeline job may fail with the HTTP Error 504: Gateway Time-out error message. The workaround is to increase the timeout for NGINX.

Workaround:
1. Open your Git project repository with the Reclass model on the cluster level.
2. In classes/cluster/<cluster_name>/infra/config/init.yml, increase the timeout for NGINX:
   
   ```yaml
   nginx:
   server:
   site:
   nginx_proxy_salt_api:
   proxy:
   timeout: 1000
   ```

3. Apply the following state:
   
   ```
   salt -C '@salt:master' saltutil.sync_all
   salt -C '@salt:master' state.sls nginx.server
   ```

OpenStack

- 22489
- 25742
- 26149
- 26269
- 27071
- 27403
- 33365
- 33576
- 34028
- 34455

22489
Pike, Queens

In the OpenStack environments with OpenContrail and Barbican, if you use a non-default Keystone domain, the LBaaS VIP cannot be created. LBaaS cannot download a secret created by the Barbican user in any project other than the project where opencontrail_barbican_user has admin privileges.

Workaround:
1. On every OpenStack controller node where Barbican API is installed, add the following configuration to /etc/barbican/policy.json:

```json
barbican:
  server:
    policy:
      all_domains_reader: 'user:<user_ID> and project:<project_ID>'
      secret_acl_read: '"read":%(target.secret.read)s or rule:all_domains_reader"
      container_acl_read: '"read":%(target.container.read)s or rule:all_domains_reader"
```

By default, LBaaS uses the admin user to obtain secrets from Barbican. Replace `<user_ID>` and `<project_ID>` with a corresponding OpenStack ID of this user and the project where this user has an admin role.

2. Log in to the Salt Master node.

3. Apply the following state:

```
salt -C 'I@barbican:server' state.apply barbican
```

This configuration adds appropriate rights to read the secrets and containers from Barbican.

---

25742

Queens

The Reclass model for OpenStack Queens includes the deprecated Heat CloudWatch API, which may cause false positive alerts for the Heat CloudWatch service in StackLight LMA. The issue affects only the existing deployments with OpenStack Queens.

Workaround:

1. Upgrade your MCP deployment to the Build ID 2019.2.0 as described in MCP Operations Guide: Upgrade MCP to a newer release version.
2. Open your Git project repository with the Reclass model on the cluster level.
3. In openstack/init.yml, specify the following class:

```
openstack_heat_cloudwatch_api_enabled: False
```
4. Log in to the Salt Master node.
5. Apply the haproxy state on all OpenStack controller nodes:

```
salt ctl* state.apply haproxy
```
6. Apply the nginx state on all proxy nodes:

```
salt prx* state.apply nginx
```
26149
Queens

When resetting the OpenStack administrator password, the state.sls keystone state does not apply the changes. The issue affects only the OpenStack Queens release.

Workaround:

1. Log in to an OpenStack controller node.
2. Source the keystonercv3 file:

   ```bash
   source /root/keystonercv3
   ```
3. Set a new password:

   ```bash
   openstack user set admin --password <new_password>
   ```

   Once done, the services that use the administrator password will fail to authenticate.
4. From the Salt Master node, open the /srv/salt/reclass/classes/<cluster_name>/infra/secrets.yaml file and specify the new password using the keystone_admin_password parameter.
5. Re-run the Deploy - OpenStack Jenkins pipeline job.

26269
Queens. Fixed in 2019.2.3

Changing the logging level for the OpenStack services may fail.

Workaround:

1. Apply the Salt formula patch to your Oslo templates Salt formula.
2. Apply the OpenStack states depending on your deployment. For example, if on Nova compute you have Nova, Neutron, and Cinder, apply salt cmp* state.apply nova,neutron,cinder. Alternatively, re-run the Deploy - OpenStack Jenkins pipeline job.

27071
Pike, Queens
On the OpenStack Pike or Queens environments with Octavia, if during creation, updating, or deleting of a load balancer or other resources a gtw node is rebooted or the octavia-worker service is restarted, the stale load balancer stuck in the PENDING_UPDATE or PENDING_DELETE state.

Workaround:

1. Log in to any OpenStack controller node.
2. Obtain the target load balancer ID:

   ```bash
   openstack loadbalancer list | awk '/ PENDING_CREATE / {print $2}
   ```
3. Choose from the following options:
   - For the MCP version 2019.2.4 and later, run the following command:

     ```bash
     openstack loadbalancer delete --force <load_balancer_id>
     ```
   - Note
     The --force flag requires admin rights and works only if a load balancer was not updated during the last hour.
   - For the MCP versions older than 2019.2.4:
     1. Log in to any dbs node.
     2. Log in to the MySQL database:

        ```bash
        mysql -uoctavia -p
        ```
     3. Run the following command with the load balancer ID obtained in the step 2. For example:

        ```bash
        update load_balancer set provisioning_status='ERROR' \
        where id='0fc571fe-6ad1-4311-ab13-765b5526cd30';
        ```

27403
Pike, Queens

On the OpenStack Pike or Queens environments with Octavia, if a gtw node hosting the Octavia services has issues with tenant network causing the Octavia management network lb-mgmt-net to become unreachable from this gtw node, the Octavia controller services stop working properly without connection to the amphora instances.
Workaround:

- If you run the Octavia services on all gtw nodes using octavia_manager_cluster and only one gtw node has tenant network issues, manually stop the Octavia controller services (octavia-health-manager, octavia-housekeeping, octavia-worker) on the affected node until the network issue on this node is resolved. In this case, the Octavia controller services will continue working properly.

- If you run the Octavia services only on the gtw01 node, manually stop the Octavia controller services and choose from the following options:
  
  - Start the Octavia controller services on another gtw0x node:
    
    1. Open your Git project repository with the Reclass model on the cluster level.
    2. In `cluster/<cluster_name>/infra/config/nodes.yml`, change the node for the Octavia services, for example, to gtw02:

      ```yaml
      parameters:
        reclass:
          storage:
            node:
              openstack_gateway_node02:
                classes:
                  - cluster.$(_param:cluster_name).openstack.octavia_manager
                params:
                  octavia_hm_bind_ip: ${_param:octavia_health_manager_node01_address}
      
    3. Log in to the Salt Master node.
    4. Apply the following states:

      ```bash
      salt-call state.sls reclass.storage
      salt '*' saltutil.refresh_pillar
      salt -C 'I@neutron:client' state.sls neutron.client
      salt '*' mine.update
      
      5. For the gtw node where you moved the Octavia services, apply the Octavia states. For example:

      ```bash
      salt 'gtw02*' state.sls octavia
      ```

  - TECHNICAL PREVIEW Enable octavia_manager_cluster:
    
    1. Open your Git project repository with the Reclass model on the cluster level.
2. In infra/<cluster_name>/infra/config/init.yml, change the following class

- system.reclass.storage.system.openstack_gateway_single_octavia

to

- system.reclass.storage.system.openstack_gateway_cluster_octavia

3. Log in to the Salt Master node.

4. Apply the following states:

   salt-call state.sls reclass.storage
   salt '*' saltutil.refresh_pillar
   salt -C 'I@neutron:client' state.sls neutron.client
   salt '*' mine.update
   salt -C "I@octavia:manager and not *01*" state.sls octavia

33365
Pike, Queens

The Nova scheduler counts the disk space of the volume-backed instances and causes NoValidHostFound errors from Nova when booting an instance. The reason is that Nova considers the size of the root volume specified in the instance flavor to be consumed by that instance on the compute host even if the instance is booted from the Cinder volume and does not consume any disk resources on the compute host.

Workarounds:

- If your cloud uses instances booted only or mostly from Cinder volumes, increase the disk overcommit ratio:

  1. Open your Git project repository with the Reclass model on the cluster level.
  2. In cluster/<cluster_name>/openstack/control.yml, increase the disk allocation ratio as required using the disk_allocation_ratio parameter:

```yaml
nova:
  controller:
    disk_allocation_ratio: <integer>
```

3. From the Salt Master node, apply the nova state:

   salt 'ctl*' state.apply nova
• If only some instances boot from Cinder volumes, create a separate flavor of zero size for the root volume to be used by such instances. Use these flavors when creating instances booted from Cinder volumes.

1. Open your Git project repository with the Reclass model on the cluster level.

2. In cluster/<cluster_name>/openstack/control.yml, define a new flavor and set disk to 0. Set other parameters as required. For example:

```yaml
nova:
  client:
    enabled: true
  server:
    identity:
      flavor:
        flavor1:
          flavor_id: 10
          ram: 4096
          disk: 0
          vcpus: 1
```

3. From the Salt Master node, apply the novaclient state:

   ```bash
   salt 'ctl*' state.apply novaclient
   ```

33576
Pike, Queens

A Neutron port on a private network may receive traffic from other networks or VLANs during wiring. The workaround is to use iptables instead of the Open vSwitch security groups.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.

2. In cluster/<cluster_name>/openstack/compute.yaml, set the firewall_driver to iptables_hybrid:

```yaml
neutron:
  compute:
    firewall_driver: iptables_hybrid
```

3. Apply the neutron state from the Salt Master node:

   ```bash
   salt -C 'I@neutron:server' state.sls neutron
   ```
34028

Pike, Queens

The Keepalived service may fail during the upgrade from MCP versions lower than 2018.11.0 to 2019.2.0. The workaround is to disable Keepalived monitoring and enable it once you complete the upgrade.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In classes/cluster/<cluster_name>/infra/init.yml, disable Keepalived monitoring:

   ```yaml
   keepalived:
     _support:
       telegraf:
         enabled: false
   ```

3. Verify that all nodes have the Telegraf Keepalived plugin disabled:

   ```
   salt -C "**" saltutil.refresh_pillar
   ```

4. Verify that no nodes respond against test.ping:

   ```
   salt -C "I@keepalived:_support:telegraf:enabled:True" test.ping
   ```

5. Apply the change:

   ```
   salt -C 'I@telegraf:agent' state.sls telegraf
   ```

6. Once you complete the upgrade, revert the step 2.

7. Apply the change:

   ```
   salt -C 'I@telegraf:agent' state.sls telegraf
   ```

34455

Pike, Queens

After deployment of an OpenStack environment, the VCP nodes may have an incorrect DNS server if MAAS is used. The reason is that during a VCP node boot, it obtains a DNS server from MAAS, which may differ from the DNS server specified in the deployment model.

To resolve the issue for the existing VCP nodes, remove the wrong DNS server address from the /etc/resolv.conf configuration file. To resolve the issue before deploying a new environment or adding new VCP nodes to an existing environment, specify the network data in cloud-init.

To apply a workaround for existing VCP nodes:
1. Log in to the Salt Master node.
2. Obtain the MAAS DNS server address:
   
   ```
   salt-call pillar.get maas:region:bind:host
   ```
3. Remove the MAAS DNS server address from the affected nodes:
   
   ```
   salt -C '<target_compound>' cmd.run 'sed -i /<maas_server>/d /etc/resolv.conf
   ```

To apply a permanent solution for every new VCP node:

1. Log in to the Salt Master node.
2. Obtain the list of VCP nodes defined in the model:

   ```
   salt '<any_kvm_node>' --out json pillar.get salt:control:cluster:internal:node | jq -r '.[].[] | keys[]'
   ```

   Example of system response:
   
   ```
   bmk01
   cid01
   cid02
   cid03
   ... 
   prx01
   prx02
   ```
3. Determine the VCP nodes pillars that contain the cloud-init data:

   ```
   salt '<any_kvm_node>' --out yaml pillar.items | grep 'salt_control_cluster_node_cloud_init_'
   ```

   Example of system response:
   
   ```
   salt_control_cluster_node_cloud_init_openstack_control:
   salt_control_cluster_node_cloud_init_openstack_dns:
   salt_control_cluster_node_cloud_init_openstack_proxy:
   salt_control_cluster_node_cloud_init_infra_storage:
   salt_control_cluster_node_cloud_init_cicd_control:
   salt_control_cluster_node_cloud_init_stacklight_telemetry:
   ```
4. Open your Git project repository with the Recllass model on the cluster level.
5. In classes/cluster/<cluster_name>/infra/kvm.yml, specify the network data for the required nodes. For example, for the cid and prx nodes:

   ```
   parameters:
   _param:
   ```
salt_control_vcp_deploy_interface: 'ens2'
salt_control_vcp_deploy_interface_netmask: ${_param:deploy_network_netmask}
salt_control_vcp_deploy_interface_gateway: ${_param:deploy_network_gateway}
salt_control_vcp_dns_server_1: ${_param:dns_server01}
salt_control_vcp_dns_server_2: ${_param:dns_server02}
salt_control_cluster_node_cloud_init_network_data:
    network_data:
        links:
        - type: 'phy'
          id: ${_param:salt_control_vcp_deploy_interface}
          name: ${_param:salt_control_vcp_deploy_interface}
        services:
          - type: "dns"
            address: ${_param:salt_control_vcp_dns_server_1}
          - type: "dns"
            address: ${_param:salt_control_vcp_dns_server_2}
salt_control_common_network_data_networks_deploy_interface_no_dhcp_common: &common_no_dhcp_data
    link: ${_param:salt_control_vcp_deploy_interface}
    type: 'ipv4'
    netmask: ${_param:salt_control_vcp_deploy_interface_netmask}
    routes:
        - gateway: ${_param:salt_control_vcp_deploy_interface_gateway}
          network: '0.0.0.0'
          netmask: '0.0.0.0'
salt_control_cluster_node_cloud_init_cicd_control:
    network_data: ${_param:salt_control_cluster_node_cloud_init_network_data}
salt_control_cluster_node_cloud_init_openstack_proxy:
    network_data: ${_param:salt_control_cluster_node_cloud_init_network_data}
salt:
    control:
    cluster:
    node:
        cid01:
            cloud_init:
                network_data:
                    networks:
                    - <<: *common_no_dhcp_data
                      ip_address: ${_param:cicd_control_node01_deploy_address}
        cid02:
            cloud_init:
                network_data:
                    networks:
                    - <<: *common_no_dhcp_data
                      ip_address: ${_param:cicd_control_node02_deploy_address}
        cid03:
            cloud_init:
                network_data:
                    networks:
                    - <<: *common_no_dhcp_data
                      ip_address: ${_param:cicd_control_node03_deploy_address}
        prx01:
            cloud_init:
                network_data:
                    networks:
                    - <<: *common_no_dhcp_data
                      ip_address: ${_param:openstack_proxy_node01_deploy_address}
        prx02:
            cloud_init:
                network_data:
                    networks:
                    - <<: *common_no_dhcp_data
                      ip_address: ${_param:openstack_proxy_node02_deploy_address}
6. Synchronize the Salt resources:

```
salt -C 'l@salt:control' saltutil.sync_all
```

7. Proceed with OpenStack environment deployment:

- Automatically, as described in [MCP Deployment Guide: Deploy an OpenStack environment](#).
- Manually, by booting the VCP nodes:

```
salt -C 'l@salt:control' salt.control
```

**Kubernetes**

- **25969**

---

**25969**

*Note*

Fixed in the MCP 2019.2.2 update, see: [MCP 2019.2.2 addressed issues](#).

The OpenStack cloud provider redefines the internal IP of the Kubernetes nodes with an IP of every NIC and can assign a wrong IP address as a primary address of a node. This can lead to failures in the output of the kubectl exec and kubectl logs commands.

**Workaround:**

1. Log in to any Kubernetes node.
2. Choose from the following options:
   - If the Kubernetes VMs have two network interfaces:
     1. In `/etc/kubernetes/cloud-config`, set the public-network-name cfg option for OpenStack cloud provider to the name of the OpenStack environment public network:

```
[Networking]
public-network-name=public
```

2. Apply the changes:
   - On the Kubernetes Master node, run:
systemctl restart openstack-cloud-controller-manager

• On the Kubernetes Node, run:

systemctl restart kubelet

3. Repeat the steps 1-2 on the remaining Kubernetes Master nodes and Kubernetes nodes.

• If the Kubernetes VMs have more than two network interfaces:

1. In /etc/default/kubelet, set the kubelet --address parameter to 0.0.0.0 for kubelet to listen to all interfaces.

Warning
This setting may have a security impact on a Kubernetes cloud.

2. Apply the changes:

systemctl restart kubelet

3. Repeat the steps 1-2 on the remaining Kubernetes Master nodes and Kubernetes nodes.

See also
Corresponding community bug

OpenContrail

• 23177
• 24943
• 25264
• 25629
• 25857
• 26133
• 26673
• 29091

23177
Dynamic Kernel Module Support fails to build DPDK kernel modules for OpenContrail v3.2.3 on kernels newer than v4.8. The workaround is to use DPDK libraries v17.02 instead of v2.1.
24943
If the OpenContrail cluster has ports with the allowed address pair (AAP) prefix length less than /24 for IPv4 and /120 for IPv6, such AAPs may not work after the upgrade of OpenContrail v3.2 to v4.0. The workaround is to modify all AAPs on all virtual interfaces through the OpenContrail web UI. For example, change 1.2.3.4/16 to 1.2.3.4/24.

25264
Fixed in 2019.2.3
In the OpenContrail 4.x deployments, after restoring the ZooKeeper database, contrail-control may be inactive on all ntw nodes due to an issue with permissions for certificates.

Workaround:
1. Log in to the Salt Master node.
2. Change permissions:
   ```bash
   salt -C 'I@opencontrail:control' cmd.run 'chown -R contrail:contrail /etc/contrail'
   ```
3. Verify that the files are owned by the OpenContrail user:
   ```bash
   salt -C 'I@opencontrail:control' cmd.run 'ls -la /etc/contrail'
   ```

25629
Fixed in 2019.2.3
In the OpenContrail 4.x deployments, some web UI tabs fail to open. For example, opening of Setting -> Config Editor raises [SyntaxError: Failed to parse JSON body: Unexpected end of input] in logs. Opening of Monitor -> Infrastructure -> Virtual Router restarts the web UI with The worker has disconnected error in logs.

Workaround:
1. Log in to any ntw or nal node.
2. In /etc/haproxy/haproxy.cfg, remove the option nolinger parameter from the contrail-api and contrail-analytics sections of the file.
3. Repeat the step 2 on the remaining ntw and nal nodes.
The OpenContrail web UI may display the Instance data is available in config but not available in analytics false error message for some properly operating SNAT instances in Monitoring > Virtual Routers > Instances. Do not remove such instances.

26133
Tempest tests may cause contrail-api fail to start. The workaround depends on the workloads put on the cloud after performing the tempest test, contact Mirantis support to resolve the issue.

26673
Updating the name of a shared network in the Horizon web UI fails with the Failed to update network <network_name> error message. As a workaround, update the network through CLI or the OpenContrail web UI.

29253
Fixed in 2019.2.4
The Kafka service may fail to start on the MCP deployments with OpenContrail 4.1.
The Kafka service has the timeout option for connection to the ZooKeeper cluster. Sometimes, the specified timeout value is less than the time needed for ZooKeeper to perform election and start the service requests. The Kafka service stops working if connection to the ZooKeeper cluster is not established during the specified amount of time (timeout).
Workaround:
1. Log in to the Salt Master node.
2. Start the failed Kafka service on the affected node(s):

```
salt -C "<affected_node_name>" cmd.run "doctrail analyticsdb service confluent-kafka start"
```

29091
Opening or refreshing the OpenContrail 4.1 web UI in the Google Chrome browser causes the SSH handshake failure.
Workaround:
Select from the following options:

- Use a different browser, for example, Firefox or Safari
• Access the OpenContrail web UI through the prx nodes

StackLight LMA

• 28119

28119
Fixed in 2019.2.4
CADF notifications are unavailable with Elasticsearch and Kibana v6. The workaround is to deploy Elasticsearch and Kibana v5 instead during the deployment of a new MCP cluster.

Workaround:
1. Open your Git project repository with Reklass model on the cluster level.
2. In classes/cluster/<cluster_name>/stacklight/log.yml, specify the elasticsearch_version: 5 and kibana_version: 5 parameters:

```
parameters:
  _param:
    ...
  elasticsearch_version: 5
  kibana_version: 5
```
3. Log in to the Salt Master node.
4. Apply the following states:

```
salt '*' saltutil.refresh_pillar
salt '*' state.sls linux.system.repo
```
5. Proceed with further configuration as required.

Storage

• 19913
• 23318
• 24197
• 24205
• 29811

19913
Restarting the RADOS Gateway service using systemctl may fail. The workaround is to restart the service manually.

Workaround:

1. Log in to an rgw node.
2. Obtain the process ID of the RADOS Gateway service:

   ```bash
   ps uax | grep radosgw
   ```

   Example of system response:

   ```
   root     17526  0.0  0.0  13232   976 pts/0    S+   10:30 \
   0:00 grep --color=auto radosgw
   ceph     20728  0.1  1.4 1306844 58204 ?       Ssl Jan28 \
   2:51 /usr/bin/radosgw -f --cluster ceph --name client.rgw.rgw01 --setuser ceph --setgroup ceph
   ```

   Where the process ID is 20728.
3. Stop the process using the obtained process ID. For example:

   ```bash
   kill -9 $20728
   ```
4. Start the RADOS Gateway service specifying the node name, for example, client.rgw.rgw01:

   ```bash
   /usr/bin/radosgw --cluster ceph --name client.rgw.rgw01 --setuser ceph --setgroup ceph
   ```
5. Perform the steps 1 - 4 from the remaining rgw nodes one by one.

---

**23318**

Fixed in 2019.2.3

The upgrade of a Ceph cluster from Jewel to Luminous using the Ceph - upgrade Jenkins pipeline job does not include an automatic check if other components were upgraded before upgrading the rgw nodes. As a result, uploading a file to object storage may fail. The workaround is to upgrade the rgw nodes only after you have successfully upgraded the mon, mgr, and osd nodes.

---

**24197**

The `tempest.api.object_storage.test_account_quotas.AccountQuotasTest.test_admin_modify_quota` Tempest test fails because modifying the account quota is not possible even if the OpenStack user has the ResellerAdmin role. Setting a quota using the Swift CLI and API served by RADOS Gateway is also not possible. As a workaround set the quotas using the radosgw-admin utility
(requires an SSH access to an OpenStack environment) as described in **Quota management** or using the RADOS Gateway Admin Operations API as described in **Quotas**.

---

### 24205

Creating Swift containers with custom headers using the Heat stack or the `tempest.api.orchestration.stacks.test_swift_resources.SwiftResourcesTestJSON.test_acl` Tempest test fails. As a workaround, first create a container without additional parameters and then set the metadata variables as required.

---

### 29811

**Fixed in 2019.2.4**

The `mon_max_pg_per_osd` variable is set in a wrong section and does not apply on the Ceph OSDs. The workaround is to manually apply the necessary changes to the cluster model.

**Workaround:**

1. In `classes/cluster/<cluster_name>/ceph/common.yml`, define the additional parameters in the `ceph:common` pillar as follows:

   ```yaml
   parameters:
   ceph:
     common:
       config:
       global:
         mon_max_pg_per_osd: 600
   ```

2. In `/classes/service/ceph/mon/cluster.yml` and `/classes/service/ceph/mon/single.yml`, remove the configuration for `mon_max_pg_per_osd`:

   ```yaml
   common:
   #  config:
   #    mon:
   #      mon_max_pg_per_osd: 600
   ```

3. Apply the `ceph.common` state on the Ceph nodes:

   ```bash
   salt -C "I@ceph:common" state.sls ceph.common
   ```

4. Set the `noout` and `norebalance` flags:

   ```bash
   ceph osd set noout
   ceph osd set norebalance
   ```
5. Restart the Ceph Monitor services on the cmn nodes one by one. Verify that the nodes are in the HEALTH_OK status after each Ceph Monitor restart.

```
salt -C <HOST_NAME> cmd.run 'systemctl restart ceph-mon.target'
salt -C <HOST_NAME> cmd.run 'systemctl restart ceph-mgr.target'
salt -C <HOST_NAME> cmd.run 'ceph -s'
```

6. Restart the Ceph OSD services on the osd nodes one by one:

1. On each Ceph OSD node verify the OSDs running:

```
ceph001# ceph osd status 2>&1 | grep $(hostname)
```

2. For each Ceph OSD number:

```
ceph001# service ceph-osd@OSD_NR_FROM_LIST status
ceph001# service ceph-osd@OSD_NR_FROM_LIST restart
ceph001# service ceph-osd@OSD_NR_FROM_LIST status
```

3. Verify that the cluster is in the HEALTH_OK status before restarting the next Ceph OSD.

7. When the last Ceph OSD restarts, unset the noout and norebalance flags:

```
ceph osd unset noout
ceph osd unset norebalance
```
Deprecation notes

This section provides the details about deprecated and removed functionality that may have a potential impact on the existing MCP deployments.

- Global artifacts migration
- Deprecation notes for operations
- Deprecation notes for the model structure
- Manila deprecation notice

Global artifacts migration

MCP has finalized the migration to a new mirror structure at http://mirror.mirantis.com. The update details for the 2019.2.0 MCP Build ID are included in Deprecation notes for the model structure.

The structure changes apply automatically when the MCP deployment is upgraded to the new MCP Build ID.

The actual and rendered list of mirror repositories for each MCP version is always available in Release artifacts of the corresponding MCP release documentation branch.

Deprecation notes for the model structure

<table>
<thead>
<tr>
<th>Structure change details</th>
<th>Deprecated classes</th>
<th>New classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Salt formulas, OpenContrail, and updates repositories have been migrated from <a href="http://apt.mirantis.com">http://apt.mirantis.com</a> to <a href="http://mirror.mirantis.com">http://mirror.mirantis.com</a>. Therefore, the new classes have been introduced and added into the system/linux/system/repo/mcp/apt_mirantis directory. Old classes have been deprecated.</td>
<td>• system.linux.system.repo.mcp.salt</td>
<td>• system.linux.system.repo.mcp.apt_mirantis.salt-formulas</td>
</tr>
<tr>
<td></td>
<td>• system.linux.system.repo.mcp.contrail</td>
<td>• system.linux.system.repo.mcp.apt_mirantis.contrail</td>
</tr>
<tr>
<td></td>
<td>• system.linux.system.repo.mcp.updates</td>
<td>• system.linux.system.repo.mcp.apt_mirantis.update</td>
</tr>
</tbody>
</table>
Deprecation notes for operations

<table>
<thead>
<tr>
<th>Affected component</th>
<th>Operation</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack</td>
<td>Creation of Cinder multi-attach volumes and volume types</td>
<td>Disabled the capability to create multi-attach Cinder volumes and volume types in the OpenStack Ocata release since in that release the feature is experimental and not intended for production usage.</td>
</tr>
<tr>
<td>Kubernetes</td>
<td>Docker</td>
<td>Deprecated Docker in the sake of containerd for a lower memory footprint, faster container start, easier updates or upgrades of containerd compared to Docker.</td>
</tr>
<tr>
<td>StackLight LMA</td>
<td>Notifications through the Push Notification service</td>
<td>Deprecated the capability to enable email or Salesforce notifications through the Push Notification service. To enable or switch to the Alertmanager-based notifications, see MCP Operations Guide: Enable StackLight LMA notifications.</td>
</tr>
<tr>
<td></td>
<td>InfluxDB</td>
<td>Deprecated InfluxDB, InfluxDB Relay, and remote storage adapter. This functionality will be removed in the next release.</td>
</tr>
<tr>
<td>StackLight OSS</td>
<td>DevOps Portal</td>
<td>Deprecated the DevOps Portal OSS tools including the corresponding Salt formulas packages, pipeline jobs, and metadata model fragments.</td>
</tr>
</tbody>
</table>

Manila deprecation notice

In the MCP 2019.2.7 update, the Manila component is being considered for deprecation. The Manila final minor release and removal target date are currently being under review by the Mirantis product team and will be announced separately.
# Maintenance updates

Mirantis is releasing the maintenance updates for the Q4`18 MCP release.

## Q4'18 maintenance updates summary

<table>
<thead>
<tr>
<th>Maintenance update</th>
<th>Release date</th>
<th>Summary</th>
</tr>
</thead>
</table>
| 2019.2.7            | 26 December, 2019     | • Authentication for Aptly repository  
• Sosreport tool support  
• Improvements of the CVP sanity tests  
• Lock path configuration  
• StackLight and Ceph enhancements  
• Started the Manila deprecation procedure  
• Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph |
| 2019.2.6            | 05 November, 2019     | • Official support for Ironic  
• Ironic deployment automation and monitoring  
• Dogtag backup  
• Improvements of the DriveTrain configuration capabilities  
• Minor Stacklight and Ceph enhancements  
• Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph |
| 2019.2.5            | 19 August, 2019       | • Ubuntu security updates  
• Security updates for Jenkins and Gerrit configuration and usage  
• CVP enhancements  
• Automatic Galera upgrade and update  
• Enhancements for StackLight  
• Ceph cluster distributed over L3 domains and Ceph compression documentation  
• Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph |
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
</table>
| 2019.2.4| 26 June, 2019 | - Ubuntu security updates for DriveTrain and OpenStack  
- Security updates for SaltStack, Jenkins, GlusterFS  
- Security updates for OpenStack  
- Automated upgrade and update of GlusterFS and RabbitMQ  
- Improvements of the StackLight components  
- Improvements of the CVP sanity and StackLight tests  
- OpenContrail 4.0 deprecation in the sake of OpenContrail 4.1  
- Bug fixes for DriveTrain, OpenStack, OpenContrail, Ceph |
| 2019.2.3| 26 April, 2019 | - Ubuntu security updates and CVP Shaker  
- FQDN on internal endpoints in the Keystone catalog and exposition of RNG devices to Nova instances  
- Kubernetes 1.13.5 support, Helm package manager support, and automatic etcd upgrade for Kubernetes  
- Support for monitoring of Open vSwitch processes, SMART disks, and SSL certificates. Improvements in the Salesforce notifier service  
- Support for Ceph prediction alerts and Ceph pipeline jobs improvements  
- Major update of the MCP Reference Architecture documentation  
- Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph |
| 2019.2.2| 20 March, 2019 | - Full support for the OpenStack cloud provider in Kubernetes  
- Possibility to update the existing L2GW connections  
- Bug fixes for DriveTrain, OpenStack Pike and Queens, and StackLight  
- Security bug fixes for Kubernetes |
2019.2.7

The MCP 2019.2.7 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, Ceph, and StackLight MCP components.

The MCP 2019.2.7 update is available starting from December 26, 2019.

Enhancements

In the MCP 2019.2.7 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.7 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Authentication for the Aptly repository
- Sosreport tool support
- Configuring the number of instances to map
- Sanity checks improvement
- Kernel version management
- Update process improvement

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Authentication for the Aptly repository

Added the capability to enable authentication for the Aptly repository to restrict unauthenticated access to Aptly API.

Learn more

MCP Deployment Guide: Enable authentication for the Aptly repository

Sosreport tool support

Added the capability to use the sosreport tool, an extensible and portable support data collection tool, which creates diagnostic snapshots of the system, including the system log files.
and configuration details, archives the obtained data, and attaches the archive to a Salesforce case.

### Learn more

**MCP Operations Guide: Generate a sosreport**

---

**Configuring the number of instances to map**

Added the capability to configure the number of instances to map in one iteration. By default, Nova runs in batches of 50 instances and the timeout for operation is set to 60 seconds. Now you can configure the maximum number of instances and timeout using the `mapped_instances_max_count` and `mapped_instances_interval` parameters. However, take into account that increasing the `mapped_instances_max_count` value increases the amount of RAM used.

When increasing the timeout for operation, consider updating the NGINX timeout on the Salt Master node to a value larger than `mapped_instances_interval`. For details, see [34308].

---

**Sanity checks improvement**

Improved the CVP - Sanity checks Jenkins pipeline job by adding the capability to specify the `override_config` variable in `EXTRA_PARAMS` to override the global configuration.

### Learn more

**MCP Operations Guide: Perform sanity testing**

---

**Kernel version management**

Implemented the capability to manage the Ubuntu kernel version to install the required version instead of the default one during the nodes provisioning.
Update process improvement

To avoid issues with unexpected changes in mirrors, added the capability to specify the target maintenance update version using the TARGET_MCP_VERSION parameter in the Deploy - upgrade MCP DriveTrain pipeline job. For details, see step 2 in MCP Operations Guide: Update DriveTrain and step 15 in MCP Operations Guide: Upgrade DriveTrain.

OpenStack

In the MCP 2019.2.7 maintenance update, Mirantis introduces the following enhancements for OpenStack:

• SQLAlchemy performance improvement
• Lock path configuration
• Availability zones for Gnocchi instance resources

To obtain the enhancements, follow the steps described in Apply maintenance updates.

SQLAlchemy performance improvement

Added the capability to update SQLAlchemy to version 1.1.11 that includes performance enhancements and allows the OpenStack services to provide a quicker response. To update SQLAlchemy, run the Deploy - upgrade control VMs pipeline job with the OS_UPGRADE parameter set to True.

Lock path configuration

Added the capability to set the directory for lock files for the Ceilometer, Cinder, Designate, Glance, Ironic, Neutron, and Nova OpenStack services.

Learn more

MCP Operations Guide: Set the directory for lock files
Availability zones for Gnocchi instance resources
Implemented the capability to add availability zones to a Gnocchi instance resource.

Learn more
MCP Operations Guide: Add availability zone to Gnocchi instance resource

StackLight
In the MCP 2019.2.7 maintenance update, Mirantis introduces the following enhancements for StackLight:

- Authentication for Prometheus and Alertmanager
- OpenStack tenant monitoring
- Prometeus alerts enhancement

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Authentication for Prometheus and Alertmanager
Implemented authentication for Prometheus and Alertmanager web UIs through the proxy nodes that are available if external access to cloud resources is enabled in your OpenStack deployment.

Learn more
MCP Operations Guide: Configure authentication for Prometheus and Alertmanager

OpenStack tenant monitoring
Enhanced OpenStack tenant monitoring by improving the Grafana dashboards:

- Improved the Ceph pools overview dashboard to display the read and write IOPS and throughput per pool as well as sort the pools by top 5.
• Added the Nova - users and Nova - tenants dashboards and improved the Nova - instances dashboard to display comprehensive information about the usage and allocation of CPU, RAM, disk throughput, IOPS, and space by file, network, and block devices, as well as the information about the network throughput. Added the capability to sort these metrics by top users, tenants, and instances.

• Improved the Nova - utilization dashboard.

• Removed the Openstack - Tenants dashboard in favor of the informative Nova - users and Nova - tenants dashboards.

Learn more

- MCP Operations Guide: Ceph dashboards
- MCP Operations Guide: OpenStack dashboards

Prometheus alerts enhancement
Enhanced the Prometheus alerts by adding the PrometheusRuleEvaluationsFailed alert that raises in case of evaluation failures of the Prometheus recording rules.

Learn more

MCP Operations Guide: Prometheus alerts

Ceph
In the MCP 2019.2.7 maintenance update, Mirantis introduces the following enhancement for Ceph:

TECHNICAL PREVIEW

Added the capability to enable the ceph-volume tool that uses Logical Volume Management (LVM) for provisioning of block devices.

To obtain this enhancement, follow the steps described in Apply maintenance updates.

Learn more

MCP Operations Guide: Enable ceph-volume
Addressed issues

The MCP 2019.2.7 update contains fixes for several MCP components.

DriveTrain

• [33758] To avoid the issue with the wait_for_ready Salt state failure when adding new MAAS machines, added the capability to ignore the already deployed machines using the ignore_deployed_machines option, which is set to False by default. To enable the option, use the following pillar:

  parameters:
  maas:
    region:
      ignore_deployed_machines: true

• [34129] Fixed the issue with the Deploy - upgrade MCP DriveTrain Jenkins pipeline job raising the Finished: FAILURE error message even in case it finishes successfully.

• [34353] Fixed the issue with upgrade steps failing during the Deploy - upgrade control VMs Jenkins pipeline job execution when Octavia is running under WSGI.

• [22774] Fixed the issue with the administrator credentials being visible in the Jenkins console for the CVP - Functional tests and CVP - Performance tests Jenkins pipeline jobs.

• [31400] Fixed the issue with the CVP - Shaker network tests Jenkins pipeline job incorrect operation.

OpenStack

Issues resolutions applied automatically

• [34033][Pike, Queens] Fixed the issue with Nova failing to add a compute host to an aggregate if the aggregate is not mapped.

• [34022][Pike, Queens] Fixed the issue with the default security group, created by Heat, being not removed automatically along with the Heat stack.

• [33882][Pike, Queens] Fixed the issue with the removal of Heat stacks failing with the ConcurrentTransaction error message.

• [33681][Pike] Fixed the issue with the inability to create a flavor for a specified tenant from Heat.

• [33993][Pike] Fixed the issue with VM instances being scheduled outside the specified availability zone when booting multiple instances simultaneously.

• [33372][Queens] Fixed the issue with Cinder failing to leverage the image volume cache.

• [33487][Pike, Queens] Fixed the issue with the OpenStack Horizon being unavailable when the prx01 or prx02 nodes are down.
• [33777][Pike, Queens] Fixed the issue with Octavia build_rate_limit for the haproxy_amphora variable missing in Octavia Salt formula. Now, you can set the build rate limit for Octavia manager through Reclass using the build_rate_limit parameter:

```yaml
parameters:
  octavia:
    manager:
      haproxy_amphora:
        build_rate_limit: <value>
```

• [33378][Queens] Fixed the issue with the inability to configure caching of the Cinder SolidFire back end by adding the image_volume_cache_enabled parameter to the Cinder Salt formula.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [31956] Designate dashboard missing in Horizon

[31956] Designate dashboard missing in Horizon
Pike, Queens

Fixed the issue with Designate dashboard missing in the Horizon web UI in MCP clusters with Designate.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In cluster/<cluster_name>/openstack/dashboard.yml, add the following class:

```yaml
-system.horizon.server.plugin.designate
```

3. From the Salt Master node, apply the following state:

```bash
salt '*' saltutil.sync_all
salt -C '@horizon:server' state.sls horizon
```

OpenContrail
• [33137] Fixed the issue causing the contrail-vrouter-agent service to crash if vRouter was restarted on another OpenStack compute node.

• [33617] Fixed the issue with the -name argument being ignored for the neutron lbaas-healthmonitor-create and neutron lbaas-member-create states, which caused inability to create a Neutron LBaaS HealthMonitor or LBaaS PoolMember with the specified name.

StackLight

Issues resolutions applied automatically

• [33878] Fixed the issue with OpenStack notifications missing in the Kibana web UI after the update of RabbitMQ.

• [34049] Fixed the issue with the Deploy - upgrade StackLight Jenkins pipeline job failing during the upgrade of Elasticsearch because of a wrong syntax.

• [34251] Fixed the issue with false-positive raise of the OVSTooManyPortRunningOnAgent, OVSErrorOnPort, and OVSNonInternalPortDown alerts in case of instances removal. Increased the threshold interval.

• [33588] Fixed the issue with Telegraf failing to gather metrics if SolidFire is used as Cinder back end.

• [33883] Fixed the issue with bond members being listed twice in the Bond slave status panel of the Bond Grafana dashboard.

• [33864] Raised the threshold for the SystemSMARTDiskReallocatedSectorsCount alert from > 0 to > 10 and changed the severity from Major to Warning.

• [33756] Added the stats and openstack_web_proxy-backend HAProxy modules to exceptions to avoid false-positive raise of the HaproxyBackendOutage alert.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [34125] False-positive HaproxyBackendOutage alert
• [34387] CVP - StackLight tests pipeline failure

[34125] False-positive HaproxyBackendOutage alert
Fixed the issue with false-positive raise of the HaproxyBackendOutage alert for the aptly-api and aptly-public proxy for the HAProxy service in case of Aptly running on an offline node. If you experience the HaproxyBackendOutage alert raise, apply the issue resolution below.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In classes/cluster/cluster_name/cicd/control/init.yml, remove the following class:
   ```yaml
   system.haproxy.proxy.listen.cicd.aptly
   ```
3. From the Salt Master node, apply the following state:
   ```bash
   salt -C '<cid_nodes>' saltutil.sync_all
   salt -C '<cid_nodes>' state.sls haproxy
   ```

[34387] CVP - StackLight tests pipeline failure

To avoid the CVP - StackLight tests Jenkins pipeline job failure with the Update test data fixture with the missing dashboards: set([u'openstack-tenants']) error message because the Openstack - Tenants dashboard has been removed from StackLight tests but is still present in the Grafana database, apply the issue resolution below. For details, see OpenStack tenant monitoring.

To apply the issue resolution:

1. Log in to Grafana web UI.
2. Open the OpenStack Tenants dashboard.
3. Click Settings > Delete.

Ceph

- [32481] Fixed the issue with the Ceph - replace failed OSD Jenkins pipeline job failing if the NVME drives are used in the deployment. Now, the pipeline supports the management of NVME-based OSDs.
- [34054] Added the CLUSTER_FLAGS parameter to the Update Ceph packages and Ceph - add node Jenkins pipeline jobs to fix the issue with the pipeline jobs ignoring the noout flags.

Known issues

This section contains the description of the MCP 2019.2.7 known issue and its workaround. For other MCP known issues also applicable to MCP 2019.2.7, see Known issues and corresponding sections in the previous maintenance updates.

- [34434] Pike to Queens upgrade failure
Pike to Queens upgrade failure

The upgrade of OpenStack Pike to Queens fails when running the Deploy - upgrade control VMs Jenkins pipeline job for the mdb role if dist-upgrade is enabled. As a workaround, do not set the OS_UPGRADE and OS_DIST_UPGRADE parameters to True when running the Deploy - upgrade control VMs Jenkins pipeline job on mdb nodes.

Updated MCP components

The MCP 2019.2.7 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.6 update.

- Updated minor versions of the MCP components
- Updated packages from the Mirantis and mirrored repositories

Note

For the full list of the versions of the major MCP components, see Major components versions.

Updated minor versions of the MCP components

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.6</th>
<th>2019.2.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>DriveTrain</td>
<td>Gerrit</td>
<td>2.13.6</td>
<td>2.15.17</td>
</tr>
<tr>
<td>System</td>
<td>Kernel</td>
<td>4.15.0.43.64</td>
<td>4.15.0.72.92</td>
</tr>
</tbody>
</table>

Updated packages from the Mirantis and mirrored repositories

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.6</th>
<th>2019.2.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack Pike</td>
<td>alembic</td>
<td>0.8.10-1.1<del>u16.04+mcp128.10-1.2</del>u16.04+mcp2</td>
<td>0.8.10-1.2~u16.04+mcp2</td>
</tr>
<tr>
<td></td>
<td>aodh</td>
<td>5.1.0-3<del>u16.04+mcp165.1.0-4</del>u16.04+mcp16</td>
<td>5.1.0-4~u16.04+mcp16</td>
</tr>
<tr>
<td></td>
<td>barbican</td>
<td>1:5.0.1-3<del>u16.04+mcp1175.0.1-4</del>u16.04+mcp17</td>
<td>1:5.0.1-4~u16.04+mcp17</td>
</tr>
<tr>
<td></td>
<td>ceilometer</td>
<td>1:9.0.7-2<del>u16.04+mcp309.0.7-3</del>u16.04+mcp30</td>
<td>1:9.0.7-3~u16.04+mcp30</td>
</tr>
<tr>
<td></td>
<td>cinder</td>
<td>2:11.2.2-2<del>u16.04+mcp211.2.2-3</del>u16.04+mcp138</td>
<td>2:11.2.2-3~u16.04+mcp138</td>
</tr>
<tr>
<td></td>
<td>designate</td>
<td>1:5.0.3-2<del>u16.04+mcp165.0.3-3</del>u16.04+mcp16</td>
<td>1:5.0.3-3~u16.04+mcp16</td>
</tr>
<tr>
<td></td>
<td>glance</td>
<td>2:15.0.2-1<del>u16.04+mcp165.0.2-2</del>u16.04+mcp16</td>
<td>2:15.0.2-2~u16.04+mcp16</td>
</tr>
<tr>
<td></td>
<td>gnocchi</td>
<td>4.0.5-2~u16.04+mcp2</td>
<td>4.0.5-3~u16.04+mcp2</td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>heat</td>
<td>1:9.0.7-1<del>u16.04+mcp169.0.7-2</del>u16.04+mcp88</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ironic</td>
<td>1:9.1.6-1<del>u16.04+mcp19.1.6-2</del>u16.04+mcp54</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ironic-inspector</td>
<td>6.0.0-1<del>u16.04+mcp2 6.0.0-2</del>u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>keystone</td>
<td>2:12.0.3-4<del>u16.04+mcp212.0.3-5</del>u16.04+mcp26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kombu</td>
<td>4.1.0-1<del>u16.04+mcp1 4.1.0-2</del>u16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manila</td>
<td>1:5.1.0-1<del>u16.04+mcp305.1.0-2</del>u16.04+mcp38</td>
<td></td>
<td></td>
</tr>
<tr>
<td>migrate</td>
<td>0.11.0-1<del>u16.04+mcp20.11.0-2</del>u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-baremetal</td>
<td>0.1.1-2<del>u16.04+mcp7 0.1.1-2</del>u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-bgpvpn</td>
<td>7.0.0-2<del>u16.04+mcp247.0.1-2</del>u16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-sfc</td>
<td>5.0.0-1<del>u16.04+mcp2 5.0.0-2</del>u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron</td>
<td>2:11.0.8-4<del>u16.04+mcp223.0.8-5</del>u16.04+mcp228</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-dynamic-routing</td>
<td>2:11.0.0-1<del>u16.04+mcp211.0.0-2</del>u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-fwaas</td>
<td>2:11.0.2-2<del>u16.04+mcp210.0.2-3</del>u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-ldaas</td>
<td>2:11.0.4-1<del>u16.04+mcp211.0.4-2</del>u16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nova</td>
<td>2:16.1.8-5<del>u16.04+mcp216.1.8-6</del>u16.04+mcp169</td>
<td></td>
<td></td>
</tr>
<tr>
<td>octavia</td>
<td>1.0.5-7<del>u16.04+mcp211.0.5-8</del>u16.04+mcp21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>panko</td>
<td>3.1.0-1<del>u16.04+mcp183.1.0-2</del>u16.04+mcp18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-neutron-lib</td>
<td>1.9.1-1<del>u16.04+mcp111.9.1-2</del>u16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.concurrency</td>
<td>3.21.2-1<del>u16.04+mcp13.21.2-2</del>u16.04+mcp4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.db</td>
<td>4.25.2-3<del>u16.04+mcp18.25.2-4</del>u16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-pyknpip</td>
<td>0.5.0-1.1<del>u16.04+mcp20.5.0-1.2</del>u16.04+mcp22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-sqlalchemy-utils</td>
<td>0.30.12-3~u16.04+mco</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-taskflow</td>
<td>2.14.2-1.1<del>u16.04+mcp214.2-1.2</del>u16.04+mcp4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sqlalchemy</td>
<td>1.0.13+ds1-1.1<del>u16.04+mcp2+ds1-1.1</del>u16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmware-nsx</td>
<td>11.0.2-2<del>u16.04+mcp421.0.2-3</del>u16.04+mcp42</td>
<td></td>
<td></td>
</tr>
<tr>
<td>websockify</td>
<td>0.8.0+dfsg1-7<del>u16.04+dfsg1-7</del>u16.04+dfsg1-7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenStack Queens</td>
<td>aemlcbic</td>
<td>0.8.10-1.1<del>u16.04+mcp28.10-1.2</del>u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>aodh</td>
<td>6.0.1-2<del>u16.04+mcp166.0.1-3</del>u16.04+mcp15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>barbican</td>
<td>1:6.0.1-5<del>u16.04+mcp326.0.1-6</del>u16.04+mcp32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ceilometer</td>
<td>1:10.0.1-2<del>u16.04+mcp310.0.1-3</del>u16.04+mcp33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cinder</td>
<td>2:12.0.9-2<del>u16.04+mcp218.09-3</del>u16.04+mcp118</td>
<td></td>
<td></td>
</tr>
<tr>
<td>designate</td>
<td>1:6.0.1-1.0<del>u16.04+mcp250.1-1.1</del>u16.04+mcp25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>glance</td>
<td>2:16.0.1-2<del>u16.04+mcp16.0.1-3</del>u16.04+mcp32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gnocchi</td>
<td>4.2.4-4-16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>heat</td>
<td>1:10.0.3-1-16.04+mcp93</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ironic</td>
<td>1:10.1.9-1-16.04+mcp62</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ironic-inspector</td>
<td>7.2.0-1-16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>keystone</td>
<td>2:13.0.2-3-16.04+mcp31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kombu</td>
<td>4.1.0-1-16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manila</td>
<td>1:6.3.1-2-16.04+mcp52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>migrate</td>
<td>0.11.0-1-16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-bagpipe</td>
<td>8.0.1-2-16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-sfc</td>
<td>6.0.0-1-16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron</td>
<td>2:12.0.1-7-16.04+mcp168</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-dynamic-routing</td>
<td>2:12.0.1-7-16.04+mcp168</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-fwaas</td>
<td>2:12.0.1-1-16.04+mcp13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-lbaas</td>
<td>2:12.0.0-2-16.04+mcp61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-vpnaas</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nova</td>
<td>2:17.0.12-8-16.04+mcp174</td>
<td></td>
<td></td>
</tr>
<tr>
<td>octavia</td>
<td>2.1.2-8-16.04+mcp92</td>
<td></td>
<td></td>
</tr>
<tr>
<td>octavia-dashboard</td>
<td>1.0.2-1.3-16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>panko</td>
<td>4.0.2-2-16.04+mcp15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-neutron-lib</td>
<td>1.13.0-1-16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-neutronclient</td>
<td>1:6.7.0-1.0-16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-octaviaclient</td>
<td>1.4.1-3-16.04+mcp8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-openstackclient</td>
<td>3.14.3-1-16.04+mcp24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-openstacksdk</td>
<td>0.11.3-repack-1-16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.placement</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.concurrency</td>
<td>8.25.1-1-16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.db</td>
<td>4.33.4-1-16.04+mcp8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-pykmip</td>
<td>0.7.0-2.0-16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-sqlalchemy-utils</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-subunit2sql</td>
<td>1.8.0-4.0-16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-swiftclient</td>
<td>1:3.5.0-2-16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-taskflow</td>
<td>3.1.0-1-16.04+mcp13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sqlalchemy</td>
<td>1.0.13+ds1-1.1-16.04+mcp12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2020, Mirantis Inc.
websockify 0.8.0+dfsg1-7~u16.04+dfsg1-7~u16.04+mcp8

OpenContrail 4.1
ceilometer-plugin-contrail 4.1~20190927152323-0.4.1~201911127132224-0
contrail 4.1~20190927152323-0.4.1~201911127132224-0
contrail-heat 4.1~20190927152323-0.4.1~201911127132224-0
contrail-vrouter-dpdk 4.1~20190927152323-4.1~201911127132224
contrail-web-controller 4.1~20190927152323-0.4.1~201911127132224-0
contrail-web-core 4.1~20190927152323-0.4.1~201911127132224-0
neutron-plugin-contrail 4.1~20190927152323-0.4.1~201911127132224-0

Salt formulas
salt-formula-aodh 0.2+201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-apache 0.2+201909260852.99062920191181257.65ed4b7~xenial1
salt-formula-aptly 2017.2+201812071109.76b23792019111061606.6260086~xenial1
salt-formula-auditd 0.1+201907181609.76b23792019111061606.6260086~xenial1
salt-formula-backupninja 0.2+201907181609.76b23792019111061606.6260086~xenial1
salt-formula-barbican 2018.1+201910070822.201816620191131604.16494a~xenial1
salt-formula-bind 0.1+201910081540.201816620191131604.16494a~xenial1
salt-formula-cassandra 0.1+201907151245.95ff7b720191181096.75ed4b7~xenial1
salt-formula-ceilometer 2016.12.1+20191109201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-ceph 0.1+201910081540.201816620191131604.16494a~xenial1
salt-formula-cinder 2016.12.1+201910091353.8e752af201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-collectd 0.2+201811221326.32816c1201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-debmirror 2018.1+201909241520.201816620191131604.16494a~xenial1
salt-formula-designate 2016.12.1+201910091353.8e752af201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-docker 0.1+201910031453.95ff7b720191181096.75ed4b7~xenial1
salt-formula-dogtag 0.1+201910301245.8b5aeb5201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-elasticsearch 0.2+201908021521.7c08252019101061606.6260086~xenial1
salt-formula-fluentd 0.1+201905231626.32816c1201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-galera 1.0+2019080110831.350fe201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-gerrit 2017.2+201907151001.201816620191131604.16494a~xenial1
salt-formula-git 0.2+201811221326.32816c1201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-glance 2016.12.1+20191000401.201816620191131604.16494a~xenial1
salt-formula-gnokchi 2018.1+201910041907.201816620191131604.16494a~xenial1
salt-formula-grafana 0.1+201909251318.0a8aaf201910070821.8c6729201911290838.15dddb~xenial1
salt-formula-haproxy 0.2+201910141532.7f77e201910070821.8c6729201911290838.15dddb~xenial1
<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>salt-formula-heat</td>
<td>2016.12.1+201910040</td>
<td>80f16ee2018620141290843.5c80f8</td>
</tr>
<tr>
<td>salt-formula-horizon</td>
<td>2016.12.1+201907221</td>
<td>92f1f820181071624.c18aeef~xenial1</td>
</tr>
<tr>
<td>salt-formula-influxdb</td>
<td>0.1+201811221327.32</td>
<td>9864b20191071624.c18aeef~xenial1</td>
</tr>
<tr>
<td>salt-formula-ironic</td>
<td>0.1+201910071620.c6</td>
<td>10f4f2019102190859.570eb1~xenial1</td>
</tr>
<tr>
<td>salt-formula-java</td>
<td>0.2+201811121411 dd</td>
<td>0a3e201911071035.455b2b3~xenial1</td>
</tr>
<tr>
<td>salt-formula-keepalived</td>
<td>0.2+201812152230.9b</td>
<td>629b201911171107.33c0fb2~xenial1</td>
</tr>
<tr>
<td>salt-formula-keycloak</td>
<td>2018.1+20181206160</td>
<td>36751a201911170927.f6ce7a1~xenial1</td>
</tr>
<tr>
<td>salt-formula-keycloak</td>
<td>2018.1+20181206160</td>
<td>36751a201911170927.f6ce7a1~xenial1</td>
</tr>
<tr>
<td>salt-formula-libvirt</td>
<td>0.1+201811221327.21</td>
<td>0a3e201911071610608.cc7754~xenial1</td>
</tr>
<tr>
<td>salt-formula-linux</td>
<td>2017.4.1+2019010112402974d02017170905.cac8946~xenial1</td>
<td></td>
</tr>
<tr>
<td>salt-formula-lldp</td>
<td>0.1+201911221327.3c</td>
<td>9864b20191071624.c18aeef~xenial1</td>
</tr>
<tr>
<td>salt-formula-logrotate</td>
<td>0.1+201910170929.0a</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-maas</td>
<td>0.0.1+201910111546</td>
<td>4a60e20191107121129.3183ad~xenial1</td>
</tr>
<tr>
<td>salt-formula-manila</td>
<td>2017.6+201910071505.3b</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-memcached</td>
<td>0.2+201910071508.0a</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-mongodb</td>
<td>0.2+201908021518.f6</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-mysql</td>
<td>0.2+201811221327.4e</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-neutron</td>
<td>2016.12.1+201910221</td>
<td>1a6b9a201911071624.c18aeef~xenial1</td>
</tr>
<tr>
<td>salt-formula-nginx</td>
<td>0.2+201908211443.23</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-nova</td>
<td>2016.12.1+2019100412217.15</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-ntp</td>
<td>0.2+201908220911.a6</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-octavia</td>
<td>2017.6+201910251518.2b</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-openldap</td>
<td>0.2+201910101508.4a</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-openldap</td>
<td>2017.3+201811221327.4a</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-openscap</td>
<td>0.1+201812201717.e7</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-opensslh</td>
<td>0.2+201909251506.47</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-oslo-temp</td>
<td>2018.1+201908300927.4b</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-panko</td>
<td>2017.6+201908260859.2b</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-postgresql</td>
<td>2017.4+201907311420.4b</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-powerdns</td>
<td>0.1+201812150647.97</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-prometheus</td>
<td>0.1+201909251319.db</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
<tr>
<td>salt-formula-rabbitmq</td>
<td>0.2+201909241136.a2</td>
<td>93e201911071036.314279b~xenial1</td>
</tr>
</tbody>
</table>
## Release artifacts

This section lists the artifacts of the MCP 2019.2.7 maintenance update.

### MCP release artifacts

<table>
<thead>
<tr>
<th>Type</th>
<th>Artifact</th>
<th>Path</th>
</tr>
</thead>
</table>

**Note**

<table>
<thead>
<tr>
<th>OpenContrail packages</th>
<th>deb <a href="http://mirror.mirantis.com/update/2019.2.7/opencontrail-4.1/xenial">http://mirror.mirantis.com/update/2019.2.7/opencontrail-4.1/xenial</a> xenial main</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salt formulas packages</td>
<td><a href="http://mirror.mirantis.com/update/2019.2.7/salt-formulas/xenial">http://mirror.mirantis.com/update/2019.2.7/salt-formulas/xenial</a> xenial main</td>
</tr>
<tr>
<td>QCOW images</td>
<td>MCP cfg01 day01 image</td>
</tr>
<tr>
<td>Upstream mirrors</td>
<td>aptly</td>
</tr>
<tr>
<td>Docker</td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.7/docker/xenial">http://mirror.mirantis.com/update/2019.2.7/docker/xenial</a> xenial stable</td>
</tr>
<tr>
<td>Fluentd</td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/td-agent/xenial">http://mirror.mirantis.com/2019.2.0/td-agent/xenial</a> xenial contrib 17</td>
</tr>
<tr>
<td>InfluxDB</td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/influxdb/xenial">http://mirror.mirantis.com/2019.2.0/influxdb/xenial</a> xenial stable</td>
</tr>
<tr>
<td>Package</td>
<td>Type</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>MAAS</td>
<td>deb</td>
</tr>
<tr>
<td>Percona</td>
<td>deb</td>
</tr>
<tr>
<td>Upstream Ubuntu system packages</td>
<td>deb</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| Repository       | Jenkins pipeline library for MCP operations | <a href="https://github.com/Mirantis/mk-pipelines/">https://github.com/Mirantis/mk-pipelines/</a> 2019.2.7 |
|                  | alertmanager | docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.7 |
|                  | aptly | docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.7 |
|                  | compose | docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>Registry URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>gainsight</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.4</td>
</tr>
<tr>
<td>gainsight_elasticsearch</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.7</td>
</tr>
<tr>
<td>gerrit</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.5</td>
</tr>
<tr>
<td>grafana</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.7</td>
</tr>
<tr>
<td>heka</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.5</td>
</tr>
<tr>
<td>jenkins</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.5</td>
</tr>
<tr>
<td>jnlp-slave</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.7</td>
</tr>
<tr>
<td>mysql</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.7</td>
</tr>
<tr>
<td>openldap</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/external/osixia/openldap</td>
</tr>
<tr>
<td>phpldapadmin</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.5</td>
</tr>
<tr>
<td>postgres</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/external/library/postgres</td>
</tr>
<tr>
<td>prometheus</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.6</td>
</tr>
<tr>
<td>prometheus_relay</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/prometheus_relay:2019.2.5</td>
</tr>
<tr>
<td>pushgateway</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6</td>
</tr>
<tr>
<td>registry</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.7</td>
</tr>
<tr>
<td>remote_storage_adapter</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.7</td>
</tr>
<tr>
<td>sf_notifier</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.7</td>
</tr>
<tr>
<td>telegraf</td>
<td>docker-pro-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.6</td>
</tr>
<tr>
<td>visualizer</td>
<td>docker-pro-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.7</td>
</tr>
<tr>
<td>Other</td>
<td>octavia</td>
</tr>
</tbody>
</table>
Apply maintenance updates

**Caution!**

If you are updating from MCP 2019.2.6 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.6, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

### Update procedure workflow

<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DriveTrain</td>
<td>1. Update DriveTrain as described in <em><a href="#">MCP Operations Guide</a></em>: Update DriveTrain to a minor release version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enable authentication for Aptly repositories.</td>
</tr>
<tr>
<td>2</td>
<td>OpenContrail</td>
<td>Update the OpenContrail packages as described in <em><a href="#">MCP Operations Guide</a></em>: Update the OpenContrail 4.x nodes.</td>
</tr>
<tr>
<td>3</td>
<td>OpenStack</td>
<td>1. Update the OpenStack packages as described in <em><a href="#">MCP Operations Guide</a></em>: Update OpenStack packages but set OS_UPGRADE to True in the Deploy - upgrade control VMs pipeline job to update SQLALchemy to version 1.1.11.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform the steps described in <em><a href="#">Issues resolutions requiring manual application</a></em>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Optional. Set the directory for lock files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Optional. Add availability zone to Gnocchi instance resource.</td>
</tr>
<tr>
<td>3.1</td>
<td>Galera cluster</td>
<td>Update the Galera cluster as described in <em><a href="#">MCP Operations Guide</a></em>: Update Galera.</td>
</tr>
<tr>
<td>3.2</td>
<td>RabbitMQ</td>
<td>Update the RabbitMQ component as described in <em><a href="#">MCP Operations Guide</a></em>: Update RabbitMQ.</td>
</tr>
<tr>
<td>4</td>
<td>Kubernetes</td>
<td>Update the Kubernetes packages as described in <em><a href="#">MCP Operations Guide</a></em>: Update or upgrade Kubernetes.</td>
</tr>
</tbody>
</table>
1. Update StackLight LMA using the Deploy - upgrade StackLight Jenkins pipeline job as described in MCP Operations Guide: Update StackLight LMA.

2. Perform the steps described in Issues resolutions requiring manual application.

3. Configure authentication for Prometheus and Alertmanager.

Ceph updates will be applied during the DriveTrain update. Optional. Technical preview. Enable the ceph-volume tool.

Select from the following options:

- MCP Operations Guide: Apply security updates using Jenkins
- MCP Operations Guide: Apply security updates manually

See also

Known issues

2019.2.6

The MCP 2019.2.6 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, Ceph, and StackLight MCP components.

The MCP 2019.2.6 update is available starting from November 05, 2019.

Enhancements

In the MCP 2019.2.6 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.6 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Remote logging for auditd
- Redis server memory limits
- Salt Master threads and batching
- Multi-server NTP integration
- Manual mirrors update procedure
- Automatic dogtag backup

Available in the MCP offline image in the reduced size. For details, see: MCP Reference Architecture: Mirror image content.
To obtain the enhancements, follow the steps described in *Apply maintenance updates*.

Remote logging for `auditd`
Added the capability to configure a remote host for `auditd`.

Learn more
*MCP Operations Guide: Configure remote logging for auditd*

Redis server memory limits
Added the capability to configure the memory rules and limits for the Redis server.

Learn more
*MCP Operations Guide: Configure Redis server memory limits*

Salt Master threads and batching
Added the capability to configure the number of worker threads for the salt-master process on the Salt Master node based on the available CPU and set up batching for the pipeline jobs to run Salt states, targeted for a large number of nodes, on a predefined amount of nodes.

Learn more
*MCP Deployment Guide: Configure Salt Master threads and batching*

Multi-server NTP integration
Introduced support for multiple Network Time Protocol (NTP) servers on new or existing MCP clusters to provide a more flexible and wide NTP support for clustered applications such as Ceph, Galera, and others.

Learn more

MCP Operations Guide: Configure multiple NTP servers

Local mirrors update procedure
Added the procedure to update local mirrors in an MCP offline deployment manually or by recreating the existing local mirror VM with the latest version of the MCP offline image to obtain maintenance updates.

Learn more

MCP Operations Guide: Update local mirrors

Automatic Dogtag backup
Added the capability to automatically back up the Dogtag server files and database using the Backupninja backup Jenkins pipeline job. Also, enhanced and simplified the manual backup procedure.

The manual restore procedure is being finalized and will be available shortly.

Learn more

MCP Operations Guide: Back up the Dogtag server files and database starting from 2019.2.6

OpenStack
In the MCP 2019.2.6 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Ironic general availability
The networking-generic-switch ML2 plugin for Ironic multitenancy

Oslo policies configuration

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Ironic general availability

Introduced official support for Ironic that is now fully integrated into MCP with the following additional enhancements:

- Automated the initial Ironic deployment procedure that is now integrated into the OpenStack deployment Jenkins pipeline
- Added the possibility to enable SSL on Ironic internal API on existing OpenStack environments
- Implemented the Ironic upgrade procedure from OpenStack Pike to Queens

Learn more

- MCP Reference Architecture: Ironic planning
- MCP Deployment Guide: Deploy Ironic
- MCP Operations Guide: Enable SSL on Ironic internal API
- MCP Operations Guide: Upgrade the OpenStack control plane from Pike to Queens
- Monitoring of Ironic

The networking-generic-switch ML2 plugin for Ironic multitenancy

TECHNICAL PREVIEW

The networking-generic-switch ML2 mechanism driver in Neutron implements the features required for multitenancy support on the Ironic bare metal nodes. This driver requires the corresponding configuration of the Neutron server service.

Learn more

MCP Operations Guide: Enable the networking-generic-switch driver
Oslo policies configuration

Added the capability to set Oslo policies through the Reclass model. To set an Oslo policy, use the following pillar:

```yaml
<component>
  <service>
    oslo_policy:
      param1: value1
    ...
```

For example:

```yaml
glance:
  server:
    oslo_policy:
      policy_file: 'policy.json'
```

StackLight

In the MCP 2019.2.6 maintenance update, Mirantis introduces the following enhancements for StackLight:

- Monitoring of Ironic
- Prometheus version update
- Docker, OVS, RabbitMQ, and system alerts

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Monitoring of Ironic

Enhanced Stacklight LMA to monitor Ironic processes and health, including the log messages with severities, API availability, API endpoints, the number of nodes and their provision state, the number of drivers and the hosts on which the drivers are enabled. Added the Ironic dashboard in Grafana and a number of Ironic alerts.

Learn more

- MCP Operations Guide: Enable Ironic monitoring
- MCP Operations Guide: Ironic alerts
- MCP Operations Guide: OpenStack dashboards
Prometheus version update
Updated Prometheus from version 2.5.0 to 2.12.0.

Docker, OVS, RabbitMQ, and system alerts
Enhanced the Docker, OVS, RabbitMQ, and system monitoring by adding support for the following alerts:

- DockerServiceReplicaFlapping
- OVSTooManyPortRunningOnAgent, OVSErrorOnPort, OVSNonInternalPortDown, OVSOtherFailed
- RabbitmqFStatUsageWarning and RabbitmqFStatUsageCritical
- SystemCpuStealTimeWarning and SystemCpuStealTimeCritical

Learn more
- MCP Operations Guide: Docker alerts
- MCP Operations Guide: OVS alerts
- MCP Operations Guide: RabbitMQ alerts
- MCP Operations Guide: System alerts

Ceph
In the MCP 2019.2.6 maintenance update, Mirantis enhanced the Ceph Salt formula to automatically update the Ceph keyring permissions based on the configuration of the cluster model. To update the keyrings, apply the salt-call state.sls ceph state.
To obtain the enhancements, follow the steps described in Apply maintenance updates.

Addressed issues
The MCP 2019.2.6 update contains fixes for several MCP components.

DriveTrain
Issues resolutions applied automatically

- [31606] Fixed the issue with Open vSwitch being unable to configure the name servers.
- [30103] Added the capability to upgrade the Linux kernel from non-HWE to HWE using the Deploy - upgrade MCP DriveTrain Jenkins pipeline job.
- [33565] Added the capability for the Deploy - update system package(s) Jenkins pipeline job to obtain the new packages dependencies to fix the issue with the pipeline job not updating an existing package that depends on a new one.
- [33536] Added the Shibboleth Salt formula missing in MCP 2019.2.0.
• [33770] Fixed the CVE-2019-14287 to avoid potential bypassing of runas restrictions.
• [33609] Fixed the issue with the maas-dhcpd service failure after the restore of a MAAS PostgreSQL database using the Backupninja service.
• [32594] Fixed the issue with the duplicated folders creation after the restore of a MAAS PostgreSQL database using the Backupninja service.
• [32632] Fixed the issue that caused alerts after disabling the Jenkins service on the Salt Master node during the CD/CD deployment. Adjusted the raise condition for the DockerService {{ camel_case_name }} Outage alert.
• [31910] Fixed the incorrect rendering of the MAAS DHCP configuration in case DHCP relay was configured. Added the capability to configure the DHCP relay for MAAS fabrics in the Salt formula.
• [32021] Improved the output of the vm2vm tests in CVP - Sanity checks by adding the missing measurement details.
• [32907] Fixed the issue with linux.system.user failing to create a user if no group with the similar name is present.
• [30813] Improved logging for the HTTP services to avoid issues with incorrect IPs logged.
• [33213] Fixed the issue with incorrect update of the HAProxy timeout due to a missing time unit.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [32133] HAProxy status is down for aptly-public in online deployments
• [29769] Loss of access to the Salt Master node

[32133] HAProxy status is down for aptly-public in online deployments

Fixed the issue with the aptly endpoint being enabled in HAProxy on the CI/CD nodes even if the cluster has no aptly node (in online deployments) and causing HAProxy to report that the aptly-public endpoint is in the DOWN state.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. In classes/cluster/<cluster_name>/cicd/control/init.yml, remove or comment out the following class:
### classes:
```
...  
- system.haproxy.proxy.listen.cicd.aptly
...  
```

3. Refresh pillars:
```
salt -C 'I@jenkins:client and I@haproxy:proxy' saltutil.refresh_pillar
```

4. Apply the changes to HAProxy on the CI/CD nodes:
```
salt -C 'I@jenkins:client and I@haproxy:proxy' state.apply haproxy.proxy
```

[29769] Loss of access to the Salt Master node

Added a helper to update the time stamp of the last password change to avoid issues with lost access to the Salt Master node. Due to CIS 5.4.1.1, the Salt Master node password expiration is set to maximum 90 days with a subsequent access lock if the password is not updated. As a result, if the user does not update the password, even if PasswordAuthentication is disabled, access to the Salt Master node may be lost. To apply the issue resolution, perform the steps described in MCP Deployment Guide: Modify Salt Master password expiration.

OpenStack

Issues resolutions applied automatically

- [24635] [Pike, Queens] Enabled the keystonemiddleware service tokens for Nova, Glance, and Cinder services to avoid failure of long-running operations due to token expiration.
- [33456] [Pike] Fixed the issue with the inability to set an unlimited quota for Cinder volumes through Heat templates.
- [31963] [Queens] Fixed the issue with pymysql causing Nova API to respond with a 500 Internal Server Error.
- [31702] [Pike, Queens] Fixed the issue with the Heat stack creation failing with the pymysql.err.InternalError error.
- [32592] [Queens] Added the capability to configure the number of retries when removing a Ceph RBD volume during the Nova instance deletion to avoid leaving orphaned Ceph RBD volumes.
- [32913] [Queens] Fixed the issue with inability to output some log messages from Nova when using fluentd as a logging back end. The issue caused the TypeError: can't serialize Instance exception.
- [31575] [Pike, Queens] Fixed the issue causing the side panel or the Instances page in the Horizon web UI failing to load properly after logging in.
• [26806] [Pike, Queens] Fixed the issue causing an image conversion to a Solidfire-backed volume to fail with the ImageUnacceptable error due to Cinder incorrectly checking the available free space.

• [33755] [Queens] Fixed the issue with inability to set the availability zone for the Neutron server.

• [33771] [Pike, Queens] Switched Octavia API to WSGI to improve the performance under heavy loads and avoid connectivity issues.

• [32949] [Pike, Queens] Added the capability to configure the default DNS for Neutron and use it if DNS was not specified during the network creation to avoid issues with tenant name servers.

• [32852] [Pike, Queens] Fixed the issue with Ironic deployment failing with the Failed to install packages: virtualbmc error message on the bare metal nodes.

• [32200] [Pike, Queens] Fixed the issue with inability to configure the Keystone domain with the LDAP back end due to hardcoded user_description_attribute.

• [30853] [Pike, Queens] Fixed the issue with inability to redefine the Fujitsu volume back-end driver in the Cinder Salt formula. For the Fujitsu engine, use the following pillar to override the driver:

```yaml
parameters:
cinder:
  backend:
    engine: fujitsu
    volume_driver: <driver>
```

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [32645] Missing measurements in Gnocchi on environments with Barbican

[32645] Missing measurements in Gnocchi on environments with Barbican
Pike, Queens

Fixed the issue with Gnocchi failing to collect some metrics from other OpenStack services if Barbican listens to the same notification topic as Ceilometer does. The issue affected only the OpenStack environments with Barbican enabled.

To apply the issue resolution:
1. Log in to the Salt Master node.

2. Create a separate topic for Barbican to listen to Keystone messages:
   1. In classes/cluster/<cluster_name>/openstack/init.yml, add the keystone_notification_topics parameter right after openstack_notification_topics:

```
parameters:
  _param:
    ...
  openstack_notification_topics: <some_value>
  keystone_notification_topics: "${_param:openstack_notification_topics},barbican"
```

   2. In classes/cluster/<cluster_name>/openstack/barbican.yml, add the ks_notifications_topic parameter:

```
parameters:
  babican:
    server:
      ...
    ks_notifications_topic: barbican
```

3. Refresh pillars on the Keystone and Barbican nodes and apply the changes:

```
salt -C 'I@keystone:server' saltutil.refresh_pillar
salt -C 'I@barbican:server' saltutil.refresh_pillar
salt -C 'I@keystone:server:role:primary' state.apply keystone.server
salt -C 'I@keystone:server' state.apply keystone.server
salt -C 'I@barbican:server:role:primary' state.apply barbican.server
salt -C 'I@barbican:server' state.apply barbican.server
```

OpenContrail

Issues resolutions applied automatically

This section provides the list of the OpenContrail issues resolutions that are automatically applied to your MCP cluster after you perform the steps described in Apply maintenance updates.

- [32926] Fixed the issue with the contrail-topology and contrail-snmp-collector services getting stuck at the initialization stage.
- [32113] Fixed the issue that caused network creation through the Horizon web UI to take a significant amount of time.
- [32508] Fixed the issue with Neutron failing to send network-changed events to Nova. As a result, after associating a floating IP, Nova obtained the refreshed information with a delay of 5-10 minutes instead of 6-10 seconds.
- [29092] Fixed the issue with a Permission Denied error appearing in the OpenContrail web UI when accessing the Configure > Services > Service Instances tab from a different project as a non-admin user.
Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

[33721] Fixed the issue with forbidden requests to metadata from a VM due to the missing metadata secret in the Reclass model.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. In classes/cluster/<cluster_name>/opencontrail/compute.yml, replace the following pillar:

```yaml
parameters:
  _param:
    opencontrail_compute_address: ${_param:tenant_address}
{%- if cookiecutter.get('kubernetes_enabled','False') == 'False' and cookiecutter.openstack_enabled == 'True' %}
  {%- if cookiecutter.openstack_enabled == 'True' %}
    opencontrail:
      compute:
        secret: ${_param:openstack_metadata_password_generated}
  endif %}
with:

```yaml
parameters:
  _param:
    opencontrail_compute_address: ${_param:tenant_address}
{%- if cookiecutter.openstack_enabled == 'True' %}
    opencontrail:
      compute:
        secret: ${_param:openstack_metadata_password_generated}
```

3. Apply the opencontrail.compute state:

```bash
salt -C 'I@opencontrail:compute' state.apply opencontrail.compute exclude=opentonrail.client
```

StackLight

Issues resolutions applied automatically

- 33577 Fixed the issue with Prometheus Elasticsearch exporter failing to query Elasticsearch through HTTPS.
• 32966 Fixed the issue with the procstat_running metric value being always 1 even in case of a process failure.
• 33351 Fixed the incorrect view of the gauge threshold panels of the RabbitMQ Grafana dashboard.
• 32794 Disabled stacking for the Client IOPS by pool panel of the Ceph pools overview Grafana dashboard to avoid misinterpretation of the pools values appearance.
• 33727 Fixed the search patterns for the Kafka and Cassandra processes to avoid KafkaServiceDown and CassandraServiceDown false positive alerts.
• 33543 Fixed the issue with a wrong file path for the Horizon access log in the Fluentd configuration on the prx nodes.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [32116] StackLight deployment fails with stack creation failed error

[32116] StackLight deployment fails with stack creation failed error
Fixed the issue that could cause StackLight deployment to fail with the Stack creation failed, retrying in 3 seconds. services.sf_notifier.environment.SFDC_SANDBOX_ENABLED must be a string, number or null error message in the deployments with Salesforce notifier enabled due to an incorrect value for the sf_notifier_sfdc_sandbox_enabled parameter.
To apply the issue resolution:

1. Log in to the Salt Master node.
2. In classes/cluster/<cluster_name>/stacklight/server.yml, enclose the sf_notifier_sfdc_sandbox_enabled value in double quotation marks. For example:

   ```yaml
   parameters:
     _param:
       sf_notifier_sfdc_sandbox_enabled: "True"
   ```

3. Refresh pillars on the affected nodes and apply the docker.client state:

   ```bash
   salt -C 'I@prometheus:server and I@docker:client' saltutil.refresh_pillar
   salt -C 'I@prometheus:server and I@docker:client' state.apply docker.client
   ```
Issues resolutions applied automatically

• [32288] Fixed the issue with the Ceph backup scripts starting a Ceph Monitor node after the backup even if it was stopped before running the script.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [32895] Ceph cluster deployment failure
• [23428] Tempest test failure

[32895] Ceph cluster deployment failure
Fixed the issue causing failure of the Ceph cluster deployment during the deployment of Ceph OSDs due to unnecessary escape characters in the keyring caps. Added the capability to use the pre-generated admin and radosgw keyrings during the Ceph cluster deployment.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In classes/cluster/cluster_name/ceph/common.yml, remove the backslash characters \ from the caps definitions. For example:

```yaml
ceph:
    common:
        public_network: ${_param:ceph_public_network}
        cluster_network: ${_param:ceph_cluster_network}
    keyring:
        glance:
            name: ${_param:glance_storage_user}
            caps:
                mon: "allow r, allow command "osd blacklist"
                osd: "profile rbd pool=images"
        cinder:
            name: ${_param:cinder_storage_user}
            caps:
                mon: "allow r, allow command "osd blacklist"
                osd: "profile rbd pool=volumes, profile rbd-read-only pool=images, profile rbd pool=${_param:cinder_ceph_backup_pool}" 
        nova:
            name: ${_param:nova_storage_user}
            caps:
                mon: "allow r, allow command "osd blacklist"
                osd: "profile rbd pool=vms, profile rbd-read-only pool=images"
```
[23428] Tempest test failure
Fixed the issue with the test_create_object_with_expect_continue Tempest test failing on a new MCP cluster with the ssl.SSLError: certificate verify failed error message due to a misconfiguration of the RADOS Gateway Swift and S3 endpoint.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Apply the nginx state on the prx nodes:

   salt -C "I@nginx:server:site:ceph_radosgw" state.sls nginx

Known issues
This section lists the MCP 2019.2.6 known issues and workarounds. For other MCP known issues also applicable to MCP 2019.2.6, see Known issues and corresponding sections in the previous maintenance updates.

- [33878] OpenStack notifications missing in Kibana
- [33909] The post-deployment Barbican state may fail
- [34116] Load balancer amphora may get stuck

[33878] OpenStack notifications missing in Kibana
Fixed in 2019.2.7
OpenStack notifications may be missing in the Kibana web UI after the update of RabbitMQ.

Workaround:

1. Log in to the Salt Master node.
2. Apply the following state:

   salt -C "I@fluentd:agent and I@rabbitmq:server" service.restart td-agent

[33909] The post-deployment Barbican state may fail
During the post-deployment Barbican configuration changes or during the upgrade of an OpenStack environment with Barbican, the barbican.server state may fail with the "Rendering SLS 'base:barbican.server' failed: Jinja variable 'dict object' has no attribute 'key'" error. The error may occur, for example, due to the Mine data deletion after calling the mine.flush function.

Workaround:

1. Obtain the Dogtag certificate location:
salt -C 'I@dogtag:server:role:master' pillar.get dogtag:server:export_pem_file_path

Example of system response:

/etc/dogtag/kra_admin_cert.pem

2. Apply the following state:

salt -C 'I@dogtag:server:role:master' mine.send dogtag_admin_cert \
mine_function=cmd.run 'cat /etc/dogtag/kra_admin_cert.pem'

3. Rerun the failed Barbican state.

[34116] Load balancer amphora may get stuck

A load balancer amphora may get stuck with BOOTING status after the update of MCP Control Plane and the log file may contain the WARNING octavia.amphorae.drivers.haproxy.rest_api_driver [-] Could not connect to instance. Retrying. error message. Once you update the gtw node, the amphora returns to the READY status. No workaround is required.

Updated MCP components

The MCP 2019.2.6 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.5 update.

- Updated minor versions of the MCP components
- Updated packages from the Mirantis and mirrored repositories

Note

For the full list of the versions of the major MCP components, see Major components versions.
### Updated minor versions of the MCP components

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.5</th>
<th>2019.2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacklight</td>
<td>Prometheus</td>
<td>2.5.0</td>
<td>2.12.0</td>
</tr>
</tbody>
</table>

### Updated packages from the Mirantis and mirrored repositories

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.5</th>
<th>2019.2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack Pike</td>
<td>ceilometer</td>
<td>1:9.0.7-2<del>u16.04+mcp299.0.7-2</del>u16.04+mcp30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cinder</td>
<td>2:11.2.2-2<del>u16.04+mcp113.2.2-2</del>u16.04+mcp135</td>
<td></td>
</tr>
<tr>
<td></td>
<td>glance</td>
<td>2:15.0.2-1<del>u16.04+mcp145.0.2-1</del>u16.04+mcp16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>heat</td>
<td>1:9.0.7-1<del>u16.04+mcp69.0.7-1</del>u16.04+mcp76</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ironic</td>
<td>1:9.1.6-1<del>u16.04+mcp39.1.6-1</del>u16.04+mcp54</td>
<td></td>
</tr>
<tr>
<td></td>
<td>networking-bagpipe</td>
<td>7.0.0-2<del>u16.04+mcp127.0.1-2</del>u16.04+mcp7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>neutron</td>
<td>2:11.0.8-2<del>u16.04+mcp224.0.8-4</del>u16.04+mcp223</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nova</td>
<td>2:16.1.8-5<del>u16.04+mcp148.1.8-5</del>u16.04+mcp154</td>
<td></td>
</tr>
<tr>
<td></td>
<td>octavia</td>
<td>1.0.4-6<del>u16.04+mcp161.0.5-7</del>u16.04+mcp21</td>
<td></td>
</tr>
<tr>
<td></td>
<td>python-barbicanclient</td>
<td>4.5.3-1.1<del>u16.04+mcp9.5.3-1.1</del>u16.04+mcp12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>python-django-openstack</td>
<td>3.6.1-2~u16.04+mcp10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>python-glance-store</td>
<td>0.22.0-3<del>u16.04+mcp90.22.0-3</del>u16.04+mcp11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>python-oslo.policy</td>
<td>1.25.4-1<del>u16.04+mcp51.25.4-1</del>u16.04+mcp6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>python-pymysql</td>
<td>0.7.6-1.1<del>u16.04+mcp20.7.6-1.1</del>u16.04+mcp3</td>
<td></td>
</tr>
<tr>
<td>OpenStack Queens</td>
<td>ceilometer</td>
<td>1:10.0.1-2<del>u16.04+mcp300.0.1-2</del>u16.04+mcp31</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cinder</td>
<td>2:12.0.7-2<del>u16.04+mcp12.0.7-2</del>u16.04+mcp118</td>
<td></td>
</tr>
<tr>
<td></td>
<td>designate-dashboard</td>
<td>6.0.0-1.0<del>u16.04+mcp6.0.1-1.0</del>u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>glance</td>
<td>2:16.0.1-2<del>u16.04+mcp216.0.1-2</del>u16.04+mcp32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>heat</td>
<td>1:10.0.3-1.0<del>u16.04+mcp13.0-3-1.0</del>u16.04+mcp82</td>
<td></td>
</tr>
<tr>
<td></td>
<td>horizon</td>
<td>3:13.0.2-10<del>u16.04+mcp78.0.2-10</del>u16.04+mcp87</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ironic</td>
<td>1:10.1.9-1.0<del>u16.04+mcp148.1.9-1.0</del>u16.04+mcp60</td>
<td></td>
</tr>
<tr>
<td></td>
<td>manila</td>
<td>1:6.3.0-2<del>u16.04+mcp86.3.1-2</del>u16.04+mcp60</td>
<td></td>
</tr>
<tr>
<td></td>
<td>networking-bgpvpn</td>
<td>8.0.1-1.0<del>u16.04+mcp180.1-1.0</del>u16.04+mcp15</td>
<td></td>
</tr>
<tr>
<td></td>
<td>networking-ovn</td>
<td>4.0.3-1.0<del>u16.04+mcp380.3-1.0</del>u16.04+mcp78</td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------</td>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td>neutron</td>
<td>2:12.1.0-5~u16.04+mcp110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-fwaas</td>
<td>2:12.0.1-1.0~u16.04+mcp121</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-lbaas</td>
<td>2:12.0.0-2~u16.04+mcp132</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nova</td>
<td>2:17.0.11-8~u16.01+mcp117</td>
<td></td>
<td></td>
</tr>
<tr>
<td>octavia</td>
<td>2.1.7<del>u16.04+mcp72.1.2-8</del>u16.04+mcp86</td>
<td></td>
<td></td>
</tr>
<tr>
<td>octavia-dashboard</td>
<td>1.0.1-1.3<del>u16.04+mcp10.2-1.3</del>u16.04+mcp3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-barbicanclient</td>
<td>4.6.1-1.0<del>u16.04+mcp126.1-1.0</del>u16.04+mcp14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-glance-store</td>
<td>0.23.0-2<del>u16.04+mcp10.23.0-2</del>u16.04+mcp15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ironic-inspector</td>
<td>2.1.0.0-2<del>u16.04+mcp131.2-1.0</del>u16.04+mcp20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ironic-lib</td>
<td>2.12.2-1.0<del>u16.04+mcp1612.3-1.0</del>u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-keystonemiddleware</td>
<td>2.1.0-1.0<del>u16.04+mcp121.0-1.0</del>u16.04+mcp20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-openstackclient</td>
<td>3.14.3-1.0<del>u16.04+mcp184.3-1.0</del>u16.04+mcp19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-openstacksdk</td>
<td>0.11.3+repack-1.0<del>u16.04+mcp141.1</del>repack-1.0~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-os-brick</td>
<td>2.3.8-1.0<del>u16.04+mcp8.3.8-1.0</del>u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.log</td>
<td>3.36.0-1.0<del>u16.04+mcp126.0-1.0</del>u16.04+mcp15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.messaging</td>
<td>5.35.5-2<del>u16.04+mcp26.35.5-2</del>u16.04+mcp31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ovsdbapp</td>
<td>0.10.3-1.0<del>u16.04+mcp1010.4-1.0</del>u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-pymysql</td>
<td>0.8.0-1<del>u16.04+mcp1 0.8.0-1</del>u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-swiftclient</td>
<td>1:3.5.0-2<del>u16.04+mcp71:3.5.0-2</del>u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sushy</td>
<td>1.3.3-1<del>u16.04+mcp1 1.3.3-1</del>u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenContrail 4.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ceilometer-plugin-contrail</td>
<td>4.1<del>20190723091617-04.1</del>20190927152323-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>contrail</td>
<td>4.1<del>20190723091617-04.1</del>20190927152323-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>contrail-heat</td>
<td>4.1<del>20190723091617-04.1</del>20190927152323-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>contrail-vrouter-dpdk</td>
<td>4.1<del>20190723091617-4.1</del>20190927152323-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>contrail-web-controller</td>
<td>4.1<del>20190723091617-04.1</del>20190927152323-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>contrail-web-core</td>
<td>4.1<del>20190723091617-04.1</del>20190927152323-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-plugin-contrail</td>
<td>4.1<del>20190723091617-04.1</del>20190927152323-0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salt formulas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-aodh</td>
<td>0.2+201908021613.55~u16.04+mcp110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-apache</td>
<td>0.2+201908091710.76~u16.04+mcp121</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-backports</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-backports-config</td>
<td>0.1+201909271115.a35cfb9~xenial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-backupninja</td>
<td>0.2+201907311426.26~u16.04+mcp132</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-barbican</td>
<td>18.1+201908091203.2018fb288bb0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-baremetal</td>
<td>0.1+20190812270854.79~u16.04+mcp15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>©2020, Mirantis Inc.</td>
<td>Page 96</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salt Formula Name</td>
<td>Version</td>
<td>SHA1 Hash</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>salt-formula-bind</td>
<td>0.1+201812201615.c17662004910815431.e24f7f8~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-ceilometer</td>
<td>2016.12.1+201908021615.72f12229a20d41e01881617.c2595874e435f8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-ceilometer</td>
<td>0.1+201908091302.e7204e22091081540432d1c8~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-cinder</td>
<td>2016.12.1+20190731162301.60f0240190813533.e752a7e ~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-debmirror</td>
<td>2018.1+201812281232.8730773~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-designate</td>
<td>2016.12.1+201908051r2091410813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-docker</td>
<td>0.1+201905211772.b7204e22091081540432d1c8~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-dogtag</td>
<td>0.1+20190731162301.60f0240190813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-glance</td>
<td>2016.12.1+20190731162301.60f0240190813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-iptables</td>
<td>1.0+201811211247.c601d0b20191021624.20d4102~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-ironic</td>
<td>0.1+201905231618.b7204e22091081540432d1c8~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-keystone</td>
<td>2016.12.1+20190731162301.60f0240190813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-linux</td>
<td>2017.4.1+20190731162301.60f0240190813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-logrotate</td>
<td>0.1+201907311335.7c615a20b0017100929.06c56cc~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-memcached</td>
<td>0.2+201903250937.0e6204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-nginx</td>
<td>0.2+201907311335.7c615a20b0017100929.06c56cc~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-memcached</td>
<td>2016.12.1+20190731162301.60f0240190813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-neutron</td>
<td>2016.12.1+20190731162301.60f0240190813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-nginx</td>
<td>0.2+201907311335.7c615a20b0017100929.06c56cc~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-nova</td>
<td>2016.12.1+20190731162301.60f0240190813533.e752a7e~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-ntp</td>
<td>0.2+201811221327.ad6204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-octavia</td>
<td>2017.6+201908050949.25420b204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-opencontrail</td>
<td>0.2+201907191135.260124b010100815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-openssh</td>
<td>0.2+201905061452.3e87420b204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-oslo-tempest</td>
<td>0.2+201811221327.ad6204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-panko</td>
<td>2017.6+201905241116.87420b204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-prometheus</td>
<td>0.1+201907111546.2c615a20b0017100929.06c56cc~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-rabbitmq</td>
<td>0.2+201908010825.9e6204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-reclass</td>
<td>0.2+201811221327.ad6204e220910815432.874f475~xenial1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Release artifacts

This section lists the artifacts of the MCP 2019.2.6 maintenance update.

<table>
<thead>
<tr>
<th>Type</th>
<th>Artifact</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirantis apt/deb packages</td>
<td>OpenStack packages</td>
<td>deb <a href="https://mirror.mirantis.com/update/2019.2.0/openstack-pike/xenial">https://mirror.mirantis.com/update/2019.2.0/openstack-pike/xenial</a> xenial main</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deb <a href="https://mirror.mirantis.com/update/2019.2.0/openstack-queens/xenial">https://mirror.mirantis.com/update/2019.2.0/openstack-queens/xenial</a> xenial main</td>
</tr>
<tr>
<td></td>
<td>Extra packages</td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.0/extra/xenial">http://mirror.mirantis.com/update/2019.2.0/extra/xenial</a> xenial main</td>
</tr>
<tr>
<td></td>
<td>Ceph</td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.0/ceph-luminous/xenial">http://mirror.mirantis.com/update/2019.2.0/ceph-luminous/xenial</a> xenial main</td>
</tr>
<tr>
<td>OpenContrail packages</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.0/opencontrail-4.1/xenial">http://mirror.mirantis.com/update/2019.2.0/opencontrail-4.1/xenial</a> xenial main</td>
</tr>
<tr>
<td>Salt formulas packages</td>
<td></td>
<td><a href="http://mirror.mirantis.com/update/2019.2.0/salt-formulas/xenial">http://mirror.mirantis.com/update/2019.2.0/salt-formulas/xenial</a> xenial main</td>
</tr>
</tbody>
</table>

Note

All 2019.2.6 packages are available at http://mirror.mirantis.com/update/2019.2.0/.
<table>
<thead>
<tr>
<th>QCOW images</th>
<th>MCP cfg01 day01 image</th>
<th><a href="http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5">http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5</a> <a href="http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2">http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstream mirrors</td>
<td>aptly</td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/aptly/xenial">http://mirror.mirantis.com/2019.2.0/aptly/xenial</a> squeeze main</td>
</tr>
<tr>
<td>Docker</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.0/docker/xenial">http://mirror.mirantis.com/update/2019.2.0/docker/xenial</a> xenial stable</td>
</tr>
<tr>
<td>Fluentd</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/td-agent/xenial">http://mirror.mirantis.com/2019.2.0/td-agent/xenial</a> xenial contrib 18</td>
</tr>
<tr>
<td>GlusterFS</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.0/glusterfs-3.8/xenial">http://mirror.mirantis.com/update/2019.2.0/glusterfs-3.8/xenial</a> xenial main 18</td>
</tr>
<tr>
<td>InfluxDB</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2019.2.0/influxdb/xenial">http://mirror.mirantis.com/2019.2.0/influxdb/xenial</a> xenial stable</td>
</tr>
<tr>
<td>MAAS</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.0/maas/xenial">http://mirror.mirantis.com/update/2019.2.0/maas/xenial</a> xenial main 18</td>
</tr>
<tr>
<td>Percona</td>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/update/2019.2.0/percona/xenial">http://mirror.mirantis.com/update/2019.2.0/percona/xenial</a> xenial main 18</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>MCP Git repositories</td>
<td>Jenkins pipeline library for MCP operations <a href="https://github.com/Mirantis/mk-pipelines/release/2019.2.0">https://github.com/Mirantis/mk-pipelines/release/2019.2.0</a></td>
<td></td>
</tr>
<tr>
<td>General Jenkins pipeline library</td>
<td><a href="https://github.com/Mirantis/pipeline-library/release/2019.2.0">https://github.com/Mirantis/pipeline-library/release/2019.2.0</a></td>
<td></td>
</tr>
<tr>
<td>Reclass system level</td>
<td><a href="https://github.com/Mirantis/reclass-system-salt-model/release/2019.2.0">https://github.com/Mirantis/reclass-system-salt-model/release/2019.2.0</a></td>
<td></td>
</tr>
<tr>
<td>MCP common scripts</td>
<td><a href="https://github.com/Mirantis/mcp-common-scripts/release/2019.2.0">https://github.com/Mirantis/mcp-common-scripts/release/2019.2.0</a></td>
<td></td>
</tr>
<tr>
<td>MCP offline image model</td>
<td><a href="https://github.com/Mirantis/mcp-offline-model/release/2019.2.0">https://github.com/Mirantis/mcp-offline-model/release/2019.2.0</a></td>
<td></td>
</tr>
<tr>
<td>Docker images</td>
<td>alerta-web docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.0 18</td>
<td></td>
</tr>
<tr>
<td>alertmanager</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 18</td>
<td></td>
</tr>
<tr>
<td>aptly</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.0 18</td>
<td></td>
</tr>
<tr>
<td>aptly-api</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-api:2019.2.0 18</td>
<td></td>
</tr>
<tr>
<td>aptly-public</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.0 18</td>
<td></td>
</tr>
<tr>
<td>aptly-publisher</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.0 18</td>
<td></td>
</tr>
<tr>
<td>compose</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 18</td>
<td></td>
</tr>
<tr>
<td>cvp-rally</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 18</td>
<td></td>
</tr>
<tr>
<td>elasticsearch</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/elasticsearch:2019.2.0 18</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Repository</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>gainsight</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.4</td>
<td></td>
</tr>
<tr>
<td>gerrit</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.5</td>
<td></td>
</tr>
<tr>
<td>grafana</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>heka</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>jenkins</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.5</td>
<td></td>
</tr>
<tr>
<td>jnlp-slave</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>mysql</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>openldap</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/openldap:1.2.2</td>
<td></td>
</tr>
<tr>
<td>phpldapadmin</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.5</td>
<td></td>
</tr>
<tr>
<td>postgres</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10</td>
<td></td>
</tr>
<tr>
<td>prometheus</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>prometheus_relay</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus_relay:2019.2.5</td>
<td></td>
</tr>
<tr>
<td>pushgateway</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>registry</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>remote_storage_adapter</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>sf_notifier</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4</td>
<td></td>
</tr>
<tr>
<td>telegraf</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.6</td>
<td></td>
</tr>
<tr>
<td>visualizer</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.0</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>octavia</td>
<td></td>
</tr>
</tbody>
</table>

Apply maintenance updates
Caution!

If you are updating from MCP 2019.2.5 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.5, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

18(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34)

Available in the MCP offline image in the reduced size. For details, see: MCP Reference Architecture: Mirror image content.
## Update procedure workflow

<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DriveTrain</td>
<td>1. Update DriveTrain as described in MCP Operations Guide:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Update DriveTrain to a minor release version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform the steps described in Issues resolutions requiring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- manual application.</td>
</tr>
<tr>
<td>2</td>
<td>OpenContrail</td>
<td>1. Update the OpenContrail packages as described in MCP Operations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guide: Update the OpenContrail 4.x nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform the steps described in Issues resolutions requiring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- manual application.</td>
</tr>
<tr>
<td>3</td>
<td>OpenStack</td>
<td>1. Update the OpenStack packages as described in MCP Operations Guide:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update OpenStack packages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform the steps described in Issues resolutions requiring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- manual application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Optional. For environments with Ironic, Enable SSL on Ironic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>internal API.</td>
</tr>
<tr>
<td>3.1</td>
<td>Galera cluster</td>
<td>Update the Galera cluster as described in MCP Operations Guide:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update Galera.</td>
</tr>
<tr>
<td>3.2</td>
<td>RabbitMQ</td>
<td>Update the RabbitMQ component as described in MCP Operations Guide:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update RabbitMQ.</td>
</tr>
<tr>
<td>4</td>
<td>Kubernetes</td>
<td>Update the Kubernetes packages as described in MCP Operations Guide:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update or upgrade Kubernetes.</td>
</tr>
<tr>
<td></td>
<td>StackLight LMA</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1.</td>
<td>Update StackLight LMA using the Deploy - upgrade StackLight Jenkins pipeline job as described in MCP Operations Guide: Update StackLight LMA.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Perform the steps described in Issues resolutions requiring manual application.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Ceph</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Perform the steps described in Issues resolutions requiring manual application.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Optional. Update Ceph keyring permissions as described in Ceph.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Ubuntu Xenial packages</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select from the following options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MCP Operations Guide: Apply security updates using Jenkins</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MCP Operations Guide: Apply security updates manually</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See also

Known issues

2019.2.5

The MCP 2019.2.5 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, Ceph, and StackLight MCP components.

The MCP 2019.2.5 update is available starting from 19 August, 2019.

Enhancements

In the MCP 2019.2.5 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.5 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

• Security updates for Jenkins and Gerrit configuration
• AuditTrail plugin and Jenkins logging to StackLight
• Galera parameters configuration
• HAProxy global parameters configuration
• SSH connection for Jenkins slaves
• CVP enhancements
• Backupninja backup and restore pipelines

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Security updates for Jenkins and Gerrit configuration

Introduced the following enhancements in the Jenkins and Gerrit configuration:

• Switched from the HTTP to HTTPS schema for Jenkins on the cid nodes. Since Jenkins on the Salt Master node is disabled after deployment, it does not require SSL. Therefore, Jenkins on the Salt Master node has the HTTP scheme.
• Switched from the HTTP to HTTPS schema for Gerrit on the cid nodes.
• Switched OpenLDAP to the TLS connection.
• Added Jenkins and Gerrit authorization in OpenLDAP through HTTPS.

AuditTrail plugin and Jenkins logging to StackLight

Implemented audit logging in Jenkins. Now, you can keep a log of the users who performed particular Jenkins operations, such as managing and using jobs.

Learn more

MCP Operations Guide: Enable Jenkins audit logging

Galera parameters configuration

Added the capability to configure the tmp_table_size, max_heap_table_size, and table_open_cache parameters of the MySQL my.cnf configuration file.
HAProxy global parameters configuration
Added the capability to configure the parameters of the global section of the HAProxy configuration file during the deployment of HAProxy.

SSH connection for Jenkins slaves
Implemented the ability to set up the SSH connection for Jenkins slaves instead of the Java Network Launch Protocol (JNLP), which is used by default.

CVP enhancements
To align the cvp-configuration repository branch name format with the MCP product components naming convention, introduced the new release/2019.2.0 branch and deprecated the old 2019.2.0 branch. For the MCP Q4’18 release, use the release/2019.2.0 branch.
Backupninja backup and restore pipelines

Added the capability to backup and restore the MAAS PostgreSQL database and the Salt Master node using the Backupninja salt-master/MaaS backup and Backupninja restore salt-master/MaaS backup Jenkins pipeline jobs.

Learn more

- MCP Operations Guide: Back up and restore the Salt Master node starting from 2019.2.5
- MCP Operations Guide: Back up and restore a MAAS PostgreSQL database starting from 2019.2.5

OpenStack

In the MCP 2019.2.5 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Automatic Galera upgrade and update
- Secure Keystone built-in user names

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Automatic Galera upgrade and update

Implemented the Deploy - upgrade Galera pipeline job that enables the automated upgrade and update of a Galera cluster.

Learn more

MCP Operations Guide: Upgrade Galera automatically

Secure Keystone built-in user names

Implemented the autogeneration of the secure user names for the Keystone administration and users by default. This new functionality applies to the OpenStack environments deployed on top of the MCP 2019.2.5 or newer maintenance update.
StackLight
In the MCP 2019.2.5 maintenance update, Mirantis introduces the following enhancements for StackLight:

- Monitoring of the number of queues
- Alert for RabbitMQ errors in logs
- Telegraf alert
- SMART disks alerts

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Monitoring of the number of queues
Enhanced Stacklight LMA to monitor the number of queues and raise the RabbitMQUnequalQueueCritical alert if the RabbitMQ cluster nodes have an inconsistent number of queues for 10 minutes.

Learn more
MCP Operations Guide: RabbitMQ alerts

Alert for RabbitMQ errors in logs
Enhanced the RabbitMQ alerts by adding the RabbitmqErrorLogsMajor alert that raises when the RabbitMQ logs on a particular node contain errors.

Learn more
MCP Operations Guide: RabbitMQ alerts

Telegraf alert
Added the TelegrafGatherErrors alert that raises when Telegraf fails to gather metrics on a particular node.
SMART disks alerts

Enhanced the alerts for SMART disks by adding the SystemSMARTDiskOfflineUncorrectableSectors alert that raises when a disk on a particular node has offline uncorrectable sectors.

Ceph

In the MCP 2019.2.5 maintenance update, Mirantis introduces the following enhancements for Ceph:

- Ceph cluster distributed over L3 domains
- Ceph compression

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Ceph cluster distributed over L3 domains

Added the capability to deploy a Ceph cluster with nodes allocated over different L3 compartments to ensure the best level of high availability and data distribution.

Ceph compression
Enhanced Ceph documentation by adding an instruction on how to manually enable compression of uploaded objects using the Ceph compression plugins for a more rational capacity usage on the MCP cluster.

Learn more

MCP Operations Guide: Ceph compression

Addressed issues
The MCP 2019.2.5 update contains fixes for several MCP components.

DriveTrain

Issues resolutions applied automatically

• 32205 Fixed the issue with massive nova-compute down alerts raising during a MySQL backup.
• 31031 Fixed the issue with the Verify and Restore Galera cluster Jenkins pipeline job failing to restore the Galera cluster.
• 30707 Fixed the issue with highstate failing for any kvm node.
• 31587 Fixed the issue with DriveTrain VMs missing HAProxy after a redeployment.
• 31877 Fixed the issue with the :guilabel: Deploy - OpenStack Jenkins pipeline job failing with the Data failed to compile error message in case you have previously configured the Nova directory on a separate device on the OpenStack compute nodes.
• 31381 Improved the security of internal repositories in Gerrit.
• 32132 Fixed the issue with some CVP pipelines failing when a cluster had a password-secured artifactory or image pulling was impossible. Introduced the force_pull parameter to enable or disable force pulling of an image and perform Docker run only. The CVP images are now pulled to the cid node automatically during deployment.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [31360] Ubuntu security
• [31387] Cannot use encrypted pillar inside another variable
[31360] Ubuntu security

Fixed the following Ubuntu security issues:

- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479

To apply the fixes, perform the steps described in Mirantis Technical Bulletin.

[31387] Cannot use encrypted pillar inside another variable

Implemented the possibility to configure the cluster model of a new MCP deployment to
download Debian packages, Git mirrors, VM images, or any files required for cluster deployment
from a secured HTTP/HTTPS server that can be accessible through login credentials. Such
functionality may be required for offline installations when internal mirrors are secured.

The deployment engineer can define the user ID and password encrypted parameters in the
cluster Reclass model and use them in URLs to access the required sources. For example:

```yaml
parameters:
  _param:
    secured_source_username: <ENCRYPTED_USERNAME>
    secured_source_password: <ENCRYPTED_PASSWORD>
  linux:
    system:
    repo:
      repo-example:
        source: "deb http://${_param:secured_source_username}:${_param:secured_source_password}@example.com/ubuntu xenial main"
```

Previously, the source parameter was not able to decrypt values for the login credentials during
the APT mirrors configuration that led to a deployment failure. In MCP 2019.2.5, each Salt state
using sources from any HTTP/HTTPS secured server has been updated with specific parameters
that enables the deployment engineer to set the secured source properties.

Learn more

MCP Deployment Guide: Use secured sources for mirrors, repositories, and files.

OpenStack

Issues resolutions applied automatically

- [31271] [Pike, Queens] Fixed the issue when systemd did not restart the nova-novncproxy
daemon after its unexpected exit.
We recommend that you verify that the fix has been applied correctly after the packages update. Verify that the nova-novncproxy process is running and the process ID is not changing:

```
systemctl status nova-novncproxy
pgrep nova-novncproxy
```

- [30156] [Pike, Queens] Fixed the issue with the Deploy - upgrade computes pipeline enabling the OpenStack services that were manually disabled before running the pipeline.
- [31028] [Pike] Fixed the issue with Barbican interfering with other services, such as Ceilometer, Aodh, Panko, or Designate, by consuming notifications needed by these services to function properly.
- [31397] [Pike to Queens upgrade] Fixed the issue with the Deploy - upgrade control VMs pipeline job failing with the heat-keystone-setup-domain authorization error for the ctl01 node during the OpenStack environment upgrade from Pike to Queens.
- [31413] [Pike to Queens upgrade] Fixed the issue with the Deploy - upgrade control VMs pipeline job failing with the `AttributeError: 'module' object has no attribute 'is_coroutine_function'"`, exception during the upgrade of OpenStack from Pike to Queens.
- [30377] [Pike to Queens upgrade] Fixed the issue with instance migration failing during the upgrade of OpenStack from Pike to Queens.
- [30622] [Queens] Renamed iscsi_helper, deprecated since OpenStack Queens, to target_helper.
- [29463] [Pike, Queens] Fixed the issue with Open vSwitch agent on the gtw nodes failing to create new ports in case a high number of resources is observed.
- [31733] [Pike, Queens] Fixed the issue with the Neutron Open vSwitch agent hanging after a restart on the gtw nodes with more than 1000 ports.
- [30590] [Pike, Queens] Fixed the issue with Neutron PUT requests taking too much time.
- [30411] [Pike, Queens] Fixed the issue with a temporary instability of RabbitMQ causing a significant increase of the Neutron Open vSwitch agent resynchronization time.
- [30412] [Pike] Fixed the issue with the Ironic compute driver for Nova deleting hypervisors from the Nova database when Keystone was down but failing to remove the corresponding resource providers for placement, which caused inability to recreate the hypervisors when Keystone was up again.
- [31375] [Pike, Queens] Fixed the issue with inability to switch between the Chinese Simplified and Chinese Traditional languages in the Horizon dashboard.
- [30917] [Salt] Fixed the issue with the OpenStack controller nodes being not permitted to use the signing policy for qemu_vnc_ca on the Salt Master node.
- [30592] [Queens] Fixed the issue with the Nova VM migration failing in case of an unavailable Neutron API during the final stages of the migration and leaving the VMs on the target OpenStack compute nodes while the database was still pointing to the old compute nodes. To mitigate this issue, you can now configure the number of retries of the Nova calls to Neutron API.
Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

- [31204] Systemd does not restart the apache2 daemon
- [30537] Excessive disk usage while clearing ephemeral LVM volumes using shred
- [30656] The creation of large Heat stacks fails with 502 bad gateway error

[31204] Systemd does not restart the apache2 daemon
Pike, Queens

Fixed the issue when systemd did not restart the apache2 daemon after its unexpected exit. To apply the fix, Apache should be upgraded. The resolution applies automatically when you select the OS_UPGRADE or OS_DIST_UPGRADE check boxes when running the Deploy - upgrade control VMs Jenkins pipeline.

To verify that the fix has been applied correctly:

1. After the Apache2 packages update, verify that the apache2 service is running:
   
   ```
   systemctl status apache2
   ```

2. Verify that the process ID is not changing:

   ```
   pgrep apache2
   ```

[30537] Excessive disk usage while clearing ephemeral LVM volumes using shred
Pike

Implemented the ability to set the ionice level for the ephemeral LVM volume shred operation in nova-compute to prevent excessive disk consumption. Setting of the ionice level described below makes sense if:

- nova:compute:lvm:ephemeral is set to True
- nova:compute:lvm:volume_clear is set to zero or shred

To apply the issue resolution:

1. Log in to the Salt Master node.
2. In classes/cluster/<cluster_name>/openstack/compute.yml, set the level for
 volume_clear_ionice_level as required:

```
nova:
  compute:
    lvm:
      volume_clear_ionice_level: <level>
```

Possible <level> values are as follows:

- idle - to use the idle scheduling class. This option impacts system performance the
  least with a downside of increased time for a volume clearance.
- From 0 to 7 - to use the best-effort scheduling class. Set the priority level to the
  specified number.
- No value - not to set the I/O scheduling class explicitly. Mirantis does not recommend
  using no value since this is the most aggressive option in terms of system performance
  impact.

3. Apply the changes:

```
salt -C 'I@nova:compute' state.sls nova.compute
```

[30656] The creation of large Heat stacks fails with 502 bad gateway error

Fixed the issue that caused the failure during the creation of a large Heat stack. The issue was
caused by the HAProxy timeout of 60 seconds. Now, the default timeout value is 2 minutes.

To apply the issue resolution, apply the haproxy state on the OpenStack controller nodes.

If you have changed the default timeout value on your deployment before the update, it will
remain unchanged.

To tune the timeout parameter depending on the needs of an already deployed environment:

1. Log in to the Salt Master node.
2. In /srv/salt/reclass/nodes/_generated/ctl01.<cluster_name>.local.yml, set the timeout
   parameter as required. For example:

```
parameters:
  haproxy:
    proxy:
      listen:
        heat_api:
          timeout:
            client: '90s'
            server: '3m'
```

©2020, Mirantis Inc.
3. Apply the change:

```
salt -C 'l@haproxy:proxy:listen:heat_api' state.sls haproxy
```

OpenContrail

This section provides the list of the OpenContrail issues resolutions that are automatically applied to your MCP cluster after you perform the steps described in Apply maintenance updates.

- [31354] Fixed the following issues with the Cassandra - restore Jenkins pipeline job:
  - Failing because of a syntax error in the DB cleanup command.
  - Using a wrong port to connect to the Cassandra database during the restore procedure.
  - Using an invalid backup for the restore procedure.
- [25238] Fixed the issue with networks duplication in the Horizon web UI.
- [31273] Fixed the contrail-vrouter-agent crashing during the in DynamicPeer::DeleteTimeout() function.
- [31697] Fixed the issue with inability to allocate a floating IP in the Horizon web UI by setting the description field to some value. Added support for the service-type, standard-attr-timestamp, and standard-attr-description missing standard extensions of Neutron. The issue affected the OpenStack Queens environments with OpenContrail 4.1.
- [29107] Fixed the issue that caused the OpenContrail web UI to end the session and log the user out in case of an error.
- [32142] Fixed the broken MultiCast tree in OpenContrail 4.1.

StackLight

- [31805] Decreased the number of Pushgateway replicas to one to fix the issue with metrics being split into two pieces without replica control because Pushgateway does not support clustering.
- [31655] Enhanced the StackLight upgrade Jenkins pipeline job by changing the Elasticsearch timeout from five minutes to two hours to avoid the cases when Elasticsearch has not enough time to become green after an update.
- [31032] Fixed the permissions wrongly set for the Prometheus configuration directory.
- [31454] Fixed the issue with the Distribution of PGs per OSD panel of the Ceph OSD overview Grafana dashboard displaying no Ceph OSDs because of a query timeout. Also, updated the Distribution of PGs per OSD panel to display the data in bars instead of lines.
- [31241] Fixed the logs severity in the raise condition of the RabbitmqErrorLogsTooHigh alert.
- [31017] Fixed the calculation for the API availability metrics.
- [31586] Fixed the issue with the Prometheus formula failing to run with Salesforce notifications enabled.
Ceph

- [30065] Removed the redundant TARGET_SERVERS parameter from the Update Ceph packages Jenkins pipeline job.
- [28705] Fixed the issue with the Ceph - remove node Jenkins pipeline job failing to remove packages of the Ceph Monitor and RADOS Gateway nodes.

Known issues

This section lists the MCP 2019.2.5 known issues and workarounds.

- [32334] Glusterd is not started back after being killed
- [32510] Networking does not work after compute reboot

[32334] Glusterd is not started back after being killed

The Glusterd service does not restart automatically after its child processes failed or were unexpectedly killed.

Note

Re-apply the provided workaround if any of the GlusterFS packages has been re-installed or upgraded.

Workaround:

Caution!

Perform the procedure on each KVM node in your deployment.

1. In the /lib/systemd/system/glusterd.service file, set the Restart option in the [Service] section:

```ini
[Service]
...
Restart=on-abort
...
```

The recommended values include:

- **on-abort**
The service restarts only if the service process exits due to an uncaught signal not specified as a clean exit status.

• **on-failure**
  The service restarts when the process exits with a non-zero exit code, is terminated by a signal including on core dump and excluding the aforementioned four signals, when an operation such as service reload times out, and when the configured watchdog timeout is triggered.

2. Apply the changes:

```
systemctl daemon-reload
```

[32510] Networking does not work after compute reboot

After reboot of the compute node in the MCP OpenStack deployments with Neutron OVS VLAN tenant networks with network nodes and without a Distributed Virtual Router (DVR) on the compute nodes, Open vSwitch blocks the br-prv bridge system ports such as br-ctl, br-mesh, and br-storage. The affected compute node loses connectivity with all infrastructure that include services' APIs, databases, storage, and VXLAN members.

The affected configuration:

```
OpenVSwitch:
- bridge: br-prv
 ports:
  - bond0
  - br-prv: internal
  - br-ctl: internal, options: tag=43
  - br-mesh: internal, options: tag=200
  - br-storage: internal, options: tag=30
```

The workaround is to separate the br-prv ports from the system ports and use the br-sys linked OVS bridge to control these ports.

**Updated MCP components**

The MCP 2019.2.5 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.4 update.

```
Note
For the full list of the versions of the major MCP components, see [Major components versions](#).
```
## Updated packages from the Mirantis and mirrored repositories

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.4</th>
<th>2019.2.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack Pike</td>
<td>aodh</td>
<td>5.1.0-3-`u16.04+mcp120</td>
<td>5.1.0-3-`u16.04+mcp16</td>
</tr>
<tr>
<td></td>
<td>barbican</td>
<td>1:5.0.1-3-`u16.04+mcp135</td>
<td>1:5.0.1-3-`u16.04+mcp17</td>
</tr>
<tr>
<td></td>
<td>ceilometer</td>
<td>1:9.0.6-2-`u16.04+mcp229</td>
<td>1:9.0.6-2-`u16.04+mcp29</td>
</tr>
<tr>
<td></td>
<td>designate</td>
<td>1:5.0.2-2-`u16.04+mcp195</td>
<td>1:5.0.2-2-`u16.04+mcp16</td>
</tr>
<tr>
<td></td>
<td>glance</td>
<td>2:15.0.1-1-`u16.04+mcp215</td>
<td>2:15.0.2-1-`u16.04+mcp14</td>
</tr>
<tr>
<td></td>
<td>heat</td>
<td>1:9.0.7-1-`u16.04+mcp449</td>
<td>1:9.0.7-1-`u16.04+mcp65</td>
</tr>
<tr>
<td></td>
<td>horizon</td>
<td>3:12.0.4-4-`u16.04+mcp692</td>
<td>3:12.0.4-5-`u16.04+mcp80</td>
</tr>
<tr>
<td></td>
<td>ironic</td>
<td>1:9.1.6-1-`u16.04+mcp499</td>
<td>1:9.1.6-1-`u16.04+mcp53</td>
</tr>
<tr>
<td></td>
<td>keystone</td>
<td>2:12.0.2-4-`u16.04+mcp214</td>
<td>2:12.0.3-4-`u16.04+mcp21</td>
</tr>
<tr>
<td></td>
<td>libvirt</td>
<td>4.0.0-1.8.10-`u16.04+mcp10</td>
<td>4.0.0-1.8.10-`u16.04+mcp2</td>
</tr>
<tr>
<td></td>
<td>manila</td>
<td>1:5.0.3-1-`u16.04+mcp515</td>
<td>1:5.0.3-1-`u16.04+mcp38</td>
</tr>
<tr>
<td></td>
<td>manila-ui</td>
<td>2.10.2-1-`u16.04+mcp10</td>
<td>2.10.3-1-`u16.04+mcp6</td>
</tr>
<tr>
<td></td>
<td>networking-baremetal</td>
<td>0.1.1-2-`u16.04+mcp5</td>
<td>0.1.1-2-`u16.04+mcp5</td>
</tr>
<tr>
<td></td>
<td>networking-bgpvpn</td>
<td>7.0.0-2-`u16.04+mcp187</td>
<td>7.0.0-2-`u16.04+mcp24</td>
</tr>
<tr>
<td></td>
<td>networking-generic-switch</td>
<td>0.4.1-1-`u16.04+mcp10</td>
<td>0.4.1-1-`u16.04+mcp11</td>
</tr>
<tr>
<td></td>
<td>networking-l2gw</td>
<td>1:11.0.0-1-`u16.04+mcp171</td>
<td>1:11.0.0-1-`u16.04+mcp19</td>
</tr>
<tr>
<td></td>
<td>neutron</td>
<td>2:11.0.8-2-`u16.04+mcp278</td>
<td>2:11.0.8-2-`u16.04+mcp204</td>
</tr>
<tr>
<td></td>
<td>neutron-fwaas</td>
<td>2:11.0.2-2-`u16.04+mcp311</td>
<td>2:11.0.2-2-`u16.04+mcp10</td>
</tr>
<tr>
<td></td>
<td>neutron-lbaas</td>
<td>2:11.0.3-1-`u16.04+mcp1110</td>
<td>2:11.0.4-1-`u16.04+mcp11</td>
</tr>
<tr>
<td></td>
<td>nova</td>
<td>2:16.1.8-4-`u16.04+mcp2136</td>
<td>2:16.1.8-5-`u16.04+mcp142</td>
</tr>
<tr>
<td></td>
<td>octavia</td>
<td>1.0.3-7-`u16.04+mcp151</td>
<td>1.0.3-7-`u16.04+mcp15</td>
</tr>
<tr>
<td></td>
<td>openvswitch</td>
<td>2.9.0-0.1-`u16.04+mcp2</td>
<td>2.9.5-1-`u16.04+mcp</td>
</tr>
<tr>
<td></td>
<td>panko</td>
<td>3.1.0-1-`u16.04+mcp163</td>
<td>3.1.0-1-`u16.04+mcp13</td>
</tr>
<tr>
<td></td>
<td>python-brick-cinderclient</td>
<td>0.5.0-1-`u16.04+mcp5</td>
<td>0.5.1-1-`u16.04+mcp2</td>
</tr>
<tr>
<td></td>
<td>python-castellan</td>
<td>0.12.3-1-`u16.04+mcp70</td>
<td>0.12.3-1-`u16.04+mcp11</td>
</tr>
<tr>
<td></td>
<td>python-ceilometerclient</td>
<td>2.9.0-2-`u16.04+mcp2</td>
<td>2.9.0-2-`u16.04+mcp3</td>
</tr>
<tr>
<td></td>
<td>python-debtcollector</td>
<td>1.17.1-0.1-`u16.04+mcp217</td>
<td>1.17.2-0.1-`u16.04+mcp2</td>
</tr>
<tr>
<td></td>
<td>python-designateclient</td>
<td>2.7.0-1-`u16.04+mcp8</td>
<td>2.7.1-1-`u16.04+mcp4</td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------</td>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>python-futurist</td>
<td>1.3.1-1~u16.04+mcp2</td>
<td>1.3.2-1~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-glance-store</td>
<td>0.22.0-3~u16.04+mcp9</td>
<td>0.22.0-3~u16.04+mcp9</td>
<td></td>
</tr>
<tr>
<td>python-glanceclient</td>
<td>1:2.8.0-1~u16.04+mcp16</td>
<td>1:2.8.0-1~u16.04+mcp16</td>
<td></td>
</tr>
<tr>
<td>python-heatclient</td>
<td>1.11.1-1~u16.04+mcp6</td>
<td>1.11.1-1~u16.04+mcp6</td>
<td></td>
</tr>
<tr>
<td>python-ironic-lib</td>
<td>2.10.1-1~u16.04+mcp3</td>
<td>2.10.2-1~u16.04+mcp3</td>
<td></td>
</tr>
<tr>
<td>python-ironicclient</td>
<td>1.17.1-1~u16.04+mcp7</td>
<td>1.17.2-1~u16.04+mcp7</td>
<td></td>
</tr>
<tr>
<td>python-keystoneauth1</td>
<td>3.1.0-1<del>u16.04+mcp123.1.1-1</del>u16.04+mcp6</td>
<td>3.1.0-1<del>u16.04+mcp123.1.1-1</del>u16.04+mcp6</td>
<td></td>
</tr>
<tr>
<td>python-idappool</td>
<td>2.1.0-1~u16.04+mcp6</td>
<td>2.1.1-1~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-manilaclient</td>
<td>1.17.3-1<del>u16.04+mcp81.17.4-1</del>u16.04+mcp7</td>
<td>1.17.3-1<del>u16.04+mcp81.17.4-1</del>u16.04+mcp7</td>
<td></td>
</tr>
<tr>
<td>python-neutron-lib</td>
<td>1.9.1-1~u16.04+mcp9</td>
<td>1.9.1-1~u16.04+mcp11</td>
<td></td>
</tr>
<tr>
<td>python-neutronclient</td>
<td>1:6.5.0-1<del>u16.04+mcp196.5.0-1</del>u16.04+mcp23</td>
<td>1:6.5.0-1<del>u16.04+mcp196.5.0-1</del>u16.04+mcp23</td>
<td></td>
</tr>
<tr>
<td>python-octaviaclient</td>
<td>1.2.0-1~u16.04+mcp4</td>
<td>1.2.1-1~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-openstacksdk</td>
<td>0.9.18-1<del>u16.04+mcp10.9.18-1</del>u16.04+mcp4</td>
<td>0.9.18-1<del>u16.04+mcp10.9.18-1</del>u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>python-os-brick</td>
<td>1.15.8-1-1<del>u16.04+mcp115.9.1-1</del>u16.04+mcp8</td>
<td>1.15.8-1-1<del>u16.04+mcp115.9.1-1</del>u16.04+mcp8</td>
<td></td>
</tr>
<tr>
<td>python-os-client-config</td>
<td>1.28.0-1<del>u16.04+mcp71.28.1-1</del>u16.04+mcp2</td>
<td>1.28.0-1<del>u16.04+mcp71.28.1-1</del>u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-os-traitst</td>
<td>0.3.3-1~u16.04+mcp3</td>
<td>0.3.3-1~u16.04+mcp5</td>
<td></td>
</tr>
<tr>
<td>python-os-vif</td>
<td>1.7.1-1~u16.04+mcp0</td>
<td>1.7.1-1~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-osc-lib</td>
<td>1.7.0-1~u16.04+mcp5</td>
<td>1.7.1-1~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-oslo.config</td>
<td>1:4.11.1-1<del>u16.04+mcp44.11.2-1</del>u16.04+mcp4</td>
<td>1:4.11.1-1<del>u16.04+mcp44.11.2-1</del>u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>python-oslo.db</td>
<td>4.25.2-3<del>u16.04+mcp34.25.2-3</del>u16.04+mcp11</td>
<td>4.25.2-3<del>u16.04+mcp34.25.2-3</del>u16.04+mcp11</td>
<td></td>
</tr>
<tr>
<td>python-oslo.i18n</td>
<td>3.17.1-1<del>u16.04+mcp43.17.2-1</del>u16.04+mcp4</td>
<td>3.17.1-1<del>u16.04+mcp43.17.2-1</del>u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>python-oslo.middleware</td>
<td>3.30.1-1<del>u16.04+mcp43.30.2-1</del>u16.04+mcp4</td>
<td>3.30.1-1<del>u16.04+mcp43.30.2-1</del>u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>python-oslo.policy</td>
<td>1.25.3-1<del>u16.04+mcp41.25.4-1</del>u16.04+mcp5</td>
<td>1.25.3-1<del>u16.04+mcp41.25.4-1</del>u16.04+mcp5</td>
<td></td>
</tr>
<tr>
<td>python-oslo.reports</td>
<td>1.22.1-1.1<del>u16.04+mcp222.2-1.1</del>u16.04+mcp2</td>
<td>1.22.1-1.1<del>u16.04+mcp222.2-1.1</del>u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-oslo.rootwrap</td>
<td>5.9.2-1~u16.04+mcp6</td>
<td>5.9.3-1~u16.04+mcp5</td>
<td></td>
</tr>
<tr>
<td>python-oslo.serialization</td>
<td>2.20.2-1<del>u16.04+mcp52.20.3-1</del>u16.04+mcp5</td>
<td>2.20.2-1<del>u16.04+mcp52.20.3-1</del>u16.04+mcp5</td>
<td></td>
</tr>
<tr>
<td>python-oslo.utils</td>
<td>3.28.3-1<del>u16.04+mcp53.28.4-1</del>u16.04+mcp6</td>
<td>3.28.3-1<del>u16.04+mcp53.28.4-1</del>u16.04+mcp6</td>
<td></td>
</tr>
<tr>
<td>python-pankoclient</td>
<td>0.3.0-2~u16.04+mcp5</td>
<td>0.3.0-2~u16.04+mcp7</td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>python-pycadf</td>
<td>2.6.0-1~u16.04+mcp4</td>
<td>2.6.1-1~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>python-swiftclient</td>
<td>1:3.4.0-1~u16.04+mcp4</td>
<td>1:3.4.1-1~u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>python-taskflow</td>
<td>2.14.1-1.1~u16.04+mcp4</td>
<td>2.14.2-1.1~u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>python-tooz</td>
<td>1.58.0-1~u16.04+mcp4</td>
<td>1.58.1-1~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>qemu</td>
<td>1:2.11+dfsg-1.7.13-1.0~u16.04+mcp2</td>
<td>1:2.11+dfsg-1.7.13-1.0~u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>stevedore</td>
<td>1:1.25.1-1~u16.04+mcp4</td>
<td>1:1.25.2-1~u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>sushy</td>
<td>1.1.1-1~u16.04+mcp0</td>
<td>1.1.1-1~u16.04+mcp4</td>
<td></td>
</tr>
<tr>
<td>OpenStack Queens</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cinder</td>
<td>2:12.0.7-2<del>u16.04+mcp100 0.7-2</del>u16.04+mcp112</td>
<td>2:12.0.7-2<del>u16.04+mcp110 0.7-2</del>u16.04+mcp112</td>
<td></td>
</tr>
<tr>
<td>heat</td>
<td>1:10.0.3-1.0<del>u16.04+mcp110 0.3-1.0</del>u16.04+mcp63</td>
<td>1:10.0.3-1.0<del>u16.04+mcp110 0.3-1.0</del>u16.04+mcp63</td>
<td></td>
</tr>
<tr>
<td>horizon</td>
<td>3:13.0.2-10<del>u16.04+mcp173 0.2-10</del>u16.04+mcp76</td>
<td>3:13.0.2-10<del>u16.04+mcp173 0.2-10</del>u16.04+mcp76</td>
<td></td>
</tr>
<tr>
<td>ironic</td>
<td>1:10.1.8-1.0<del>u16.04+mcp140 1.9-1.0</del>u16.04+mcp43</td>
<td>1:10.1.8-1.0<del>u16.04+mcp140 1.9-1.0</del>u16.04+mcp43</td>
<td></td>
</tr>
<tr>
<td>keystone</td>
<td>2:13.0.2-3<del>u16.04+mcp130 0.2-3</del>u16.04+mcp32</td>
<td>2:13.0.2-3<del>u16.04+mcp130 0.2-3</del>u16.04+mcp32</td>
<td></td>
</tr>
<tr>
<td>libvirt</td>
<td>4.0.0-1.8.10<del>u16.04+mcp340 0.10-1.8.10</del>u16.04+mcp2</td>
<td>4.0.0-1.8.10<del>u16.04+mcp340 0.10-1.8.10</del>u16.04+mcp2</td>
<td></td>
</tr>
<tr>
<td>networking-ovn</td>
<td>4.0.3-1.0<del>u16.04+mcp340 0.3-1.0</del>u16.04+mcp39</td>
<td>4.0.3-1.0<del>u16.04+mcp340 0.3-1.0</del>u16.04+mcp39</td>
<td></td>
</tr>
<tr>
<td>neutron</td>
<td>2:12.0.6-5<del>u16.04+mcp202 1.0-5</del>u16.04+mcp136</td>
<td>2:12.0.6-5<del>u16.04+mcp202 1.0-5</del>u16.04+mcp136</td>
<td></td>
</tr>
<tr>
<td>neutron-lbaas</td>
<td>2:12.0.0-2<del>u16.04+mcp502 0.0-2</del>u16.04+mcp53</td>
<td>2:12.0.0-2<del>u16.04+mcp502 0.0-2</del>u16.04+mcp53</td>
<td></td>
</tr>
<tr>
<td>nova</td>
<td>2:17.0.10-7<del>u16.01+mcp180 0.11-8</del>u16.01+mcp139</td>
<td>2:17.0.10-7<del>u16.01+mcp180 0.11-8</del>u16.01+mcp139</td>
<td></td>
</tr>
<tr>
<td>octavia</td>
<td>2.1.0-7<del>u16.04+mcp792 2.1.1-7</del>u16.04+mcp76</td>
<td>2.1.0-7<del>u16.04+mcp792 2.1.1-7</del>u16.04+mcp76</td>
<td></td>
</tr>
<tr>
<td>python-automaton</td>
<td>1:14.0-1.0<del>u16.04+mcp614 0.1-0</del>u16.04+mcp76</td>
<td>1:14.0-1.0<del>u16.04+mcp614 0.1-0</del>u16.04+mcp76</td>
<td></td>
</tr>
<tr>
<td>python-castellan</td>
<td>0.17.0-2.0<del>u16.04+mcp117 0.2-0</del>u16.04+mcp17</td>
<td>0.17.0-2.0<del>u16.04+mcp117 0.2-0</del>u16.04+mcp17</td>
<td></td>
</tr>
<tr>
<td>python-octaviaclient</td>
<td>1.4.0-3<del>u16.04+mcp111 4.1-3</del>u16.04+mcp7</td>
<td>1.4.0-3<del>u16.04+mcp111 4.1-3</del>u16.04+mcp7</td>
<td></td>
</tr>
<tr>
<td>python-openstacksdk</td>
<td>0.11.3+repack-1.0<del>u16.04+mcp104 0.2-1.0</del>u16.04+mcp10</td>
<td>0.11.3+repack-1.0<del>u16.04+mcp104 0.2-1.0</del>u16.04+mcp10</td>
<td></td>
</tr>
<tr>
<td>python-os-brick</td>
<td>2.3.7-1.0<del>u16.04+mcp8 3.8-1.0</del>u16.04+mcp8</td>
<td>2.3.7-1.0<del>u16.04+mcp8 3.8-1.0</del>u16.04+mcp8</td>
<td></td>
</tr>
<tr>
<td>python-os-vif</td>
<td>1.9.1-1.0<del>u16.04+mcp8 9.1-1.0</del>u16.04+mcp10</td>
<td>1.9.1-1.0<del>u16.04+mcp8 9.1-1.0</del>u16.04+mcp10</td>
<td></td>
</tr>
<tr>
<td>python-oslo.db</td>
<td>4.33.2-1.0<del>u16.04+mcp103 4.1-0</del>u16.04+mcp8</td>
<td>4.33.2-1.0<del>u16.04+mcp103 4.1-0</del>u16.04+mcp8</td>
<td></td>
</tr>
<tr>
<td>python-oslo.policy</td>
<td>1.33.2-1.0<del>u16.04+mcp533 2.1-0</del>u16.04+mcp6</td>
<td>1.33.2-1.0<del>u16.04+mcp533 2.1-0</del>u16.04+mcp6</td>
<td></td>
</tr>
<tr>
<td>python-taskflow</td>
<td>3.1.0-1.0<del>u16.04+mcp111 0.1-0</del>u16.04+mcp13</td>
<td>3.1.0-1.0<del>u16.04+mcp111 0.1-0</del>u16.04+mcp13</td>
<td></td>
</tr>
<tr>
<td>python-vmware-nsxlib</td>
<td>12.0.4-1.0<del>u16.04+mcp560 4-1.0</del>u16.04+mcp59</td>
<td>12.0.4-1.0<del>u16.04+mcp560 4-1.0</del>u16.04+mcp59</td>
<td></td>
</tr>
<tr>
<td>stevedore</td>
<td>1:1.28.0-1<del>u16.04+mcp71 28.0-1</del>u16.04+mcp9</td>
<td>1:1.28.0-1<del>u16.04+mcp71 28.0-1</del>u16.04+mcp9</td>
<td></td>
</tr>
<tr>
<td>OpenContrail 4.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ceilometer-plugin-contrail</td>
<td>4.1<del>20190620130104 0.4.1</del>20190723091617</td>
<td>4.1<del>20190620130104 0.4.1</del>20190723091617</td>
<td></td>
</tr>
<tr>
<td>contrail</td>
<td>4.1<del>20190620130104 0.4.1</del>20190723091617</td>
<td>4.1<del>20190620130104 0.4.1</del>20190723091617</td>
<td></td>
</tr>
<tr>
<td>contrail-heat</td>
<td>4.1<del>20190620130104 0.4.1</del>20190723091617</td>
<td>4.1<del>20190620130104 0.4.1</del>20190723091617</td>
<td></td>
</tr>
<tr>
<td>Salt formulas</td>
<td>version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-aodh</td>
<td>201905231515.94</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-api</td>
<td>201905311132.78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-auditd</td>
<td>201811291017.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-backupninja</td>
<td>201903221820.d122</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-barbican</td>
<td>2018.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-cassandra</td>
<td>201902071300.452</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-ceilometer</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-ceilometer</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-cinder</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-designate</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-dogtag</td>
<td>201812171734.dae</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-elasticsearch</td>
<td>201906240959.c9a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-failover</td>
<td>201905111036.14b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-gerrit</td>
<td>2017.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-glance</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-gluusterfs</td>
<td>2017.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-gnocchi</td>
<td>2018.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-haproxy</td>
<td>201905210701.803</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-haproxy</td>
<td>201905222301.535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-heat</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-horizon</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-jenkins</td>
<td>2017.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-keystone</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-linux</td>
<td>2017.4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-logrotate</td>
<td>201811221327.5be</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-maas</td>
<td>201904041109.6d4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-manila</td>
<td>2017.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-mongodb</td>
<td>20190211526.147</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-neutron</td>
<td>2016.12.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-nginx</td>
<td>201905231631.300</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Extra packages

<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache2</td>
<td>2.4.18-2.3ubuntu3.10</td>
</tr>
<tr>
<td>keepalived</td>
<td>1:1.3.9-1.0.18.04.1-0+deb9-0+deb9-0.18.04.2-0+deb9.1+deb9.2</td>
</tr>
<tr>
<td>openscap</td>
<td>1.2.17-2-0+deb9.4-0+deb9.5-0+deb9.6</td>
</tr>
<tr>
<td>postgresql-9.6</td>
<td>n/a</td>
</tr>
<tr>
<td>prometheus-relay</td>
<td>0.3-1-0+deb9.4-0+deb9.5-0.3-1-0+deb9.4-0+deb9.5</td>
</tr>
<tr>
<td>telegraf</td>
<td>1:1.9.1-3-0+deb9.6-0+deb9.7-1:1.9.1-3-0+deb9.6-0+deb9.7</td>
</tr>
<tr>
<td>xccdf-benchmarks</td>
<td>1.0.2-1-0+deb9.4-0+deb9.5-1.1.1-1-0+deb9.4-0+deb9.5</td>
</tr>
</tbody>
</table>

### Note


### Apply maintenance updates

**Caution!**

If you are updating from MCP 2019.2.4 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.4, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

### Update procedure workflow
<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Workflow</th>
</tr>
</thead>
</table>
| 1  | DriveTrain    | 1. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.  
    |               | 2. Perform the steps described in Issues resolutions requiring manual application.  
    |               | 5. Optional. MCP Operations Guide: Configure Jenkins SSH slaves instead of JNLP.  
| 2  | OpenContrail  | Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes. |
| 3  | OpenStack     | 1. Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages.  
    |               | 2. Perform the steps described in Issues resolutions requiring manual application. |
| 3.1| Galera cluster| Update the Galera cluster as described in MCP Operations Guide: Update Galera.     |
| 3.2| RabbitMQ      | Update the RabbitMQ component as described in MCP Operations Guide: Update RabbitMQ.   |
| 4  | Kubernetes    | Update the Kubernetes packages as described in MCP Operations Guide: Update or upgrade Kubernetes. |
| 5  | StackLight LMA| Update StackLight LMA using the Deploy - upgrade StackLight Jenkins pipeline job as described in MCP Operations Guide: Update StackLight LMA. |
| 6  | Ceph          | Ceph updates will be applied during the DriveTrain update. Optional. MCP Operations Guide: Enable Ceph compression. |
| 7  | Ubuntu Xenial packages | Select from the following options:  
    |               | • MCP Operations Guide: Apply security updates using Jenkins  
    |               | • MCP Operations Guide: Apply security updates manually |

See also

Known issues
2019.2.4
The MCP 2019.2.4 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, Kubernetes, OpenContrail, Ceph, and StackLight MCP components.
The MCP 2019.2.4 update is available starting from June, 26.

Enhancements
In the MCP 2019.2.4 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain
In the MCP 2019.2.4 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Ubuntu security updates
- SaltStack traffic encryption with TLS 1.2
- Security updates for Jenkins configuration
- GlusterFS security improvements
- GlusterFS upgrade and update
- CVP pipelines

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Ubuntu security updates
Published the following Ubuntu 16.04 security updates:

- For Apache2 web server:
  - CVE-2019-0211
  - CVE-2018-17199
  - CVE-2019-0217
  - CVE-2019-0220
- For linux-image-generic-hwe-16.04 4.15.0.50.71:
  - USN-3981-2
  - USN-3982-1

SaltStack traffic encryption with TLS 1.2
Adjusted the DriveTrain services configuration to use the SaltSatck API encryption with the TLS 1.2 encrypted endpoints used by default in the Reclass system model.
Security updates for Jenkins configuration

Introduced the following enhancements in the Jenkins configuration:

- Enabled the Cross-Site Request Forgery (CSRF) protection by default.
- Changed the default access mode in Jenkins to allow only authenticated users to access the Jenkins UI.

Caution!
This enhancement is applicable to new MCP deployments only.

GlusterFS security improvements

Added the possibility to configure allowed and rejected IP addresses for the GlusterFS volumes. By default, MCP restricts the access to the control network for all preconfigured GlusterFS volumes.

Learn more

MCP Operations Guide: Configure allowed and rejected IP addresses for the GlusterFS volumes

GlusterFS upgrade and update

TECHNICAL PREVIEW

Implemented the automated upgrade and update procedures for GlusterFS to version 5.5. If you do not have any services that run on top of the GlusterFS volumes except the Docker Swarm services, you can use the all-in-one Update GlusterFS pipeline job. Otherwise, upgrade or update the GlusterFS components separately using three dedicated pipeline jobs:

- Update glusterfs servers
- Update glusterfs clients
- Update glusterfs cluster.op-version
Mirantis recommends using three dedicated pipeline jobs instead of the Update GlusterFS one for a more controlled and granular upgrade or update process.

New MCP deployments contain GlusterFS version 5.5 by default.

Learn more
- MCP Operations Guide: Upgrade GlusterFS
- MCP Operations Guide: Update GlusterFS

CVP pipelines
Introduced the following enhancements in the CVP Jenkins pipeline jobs:
- CPV - Sanity checks:
  - Added new tests to verify the network configurations, mounted file systems.
  - Improved the tests to avoid false positive cases.
  - Improved the tests output for a better issue debugging.
  - Improved the UI tests.
  - Added the capability to select the tests by tag/mark.
  - Added the capability to repull the cvp-sanity-checks Docker image only if needed.
  - Added the full.log file that contains requests and responses to the Salt Master API.
  - Removed the deprecated parameters and added the new ones.
- CVP - StackLight tests:
  - Added the capability for the job to work in the offline mode using the cvp-sanity-checks Docker image.
  - Removed the deprecated parameters and added the new ones.

Learn more
- MCP Operations Guide: Execute the CVP - Sanity checks pipeline
- MCP Operations Guide: Execute the CVP - StackLight tests pipeline

OpenStack
In the MCP 2019.2.4 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Ubuntu security updates
- Keystone security compliance policies
- The TLS version and allowed SSL ciphers options for nova console proxy server
- The force option for deleting the Octavia load balancers
- The TLS version 1.2 and allowed SSL ciphers for libvirt
- RabbitMQ upgrade and update
- Constrain the range of SSH ciphers to be accepted by the OpenSSH server
- Disable DHCP on gateway nodes

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Ubuntu security updates
Backported the following security updates for Pike and Queens:

- **USN-3978-1** qemu-kvm vulnerabilities
- **USN-3985-1** libvirt vulnerabilities
- **USN-3720-1** python-cryptography vulnerabilities (for Queens)

Keystone security compliance policies
Implemented the possibility to enable additional Keystone security compliance features independently of each other based on your corporate security policy. All available features apply only to the SQL back end for the Identity driver. By default, all security compliance features are disabled.

Learn more
MCP Operations Guide: Enable Keystone security compliance policies

The TLS version and allowed SSL ciphers options for nova console proxy server
Added the ability to specify a required TLS version and allowed SSL ciphers to use by the Nova console proxy server.
Learn more

MCP Deployment Guide: Enable TLS encryption between the OpenStack compute nodes and VNC clients

The TLS version 1.2 and allowed SSL ciphers for libvirt

Unhardcoded the tls_priority setting in /etc/libvirt/libvirtd.conf and added the following TLS v.1.2 Federal Information Processing Standard (FIPS) approved SSHD strong cipher suites:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384

RabbitMQ upgrade and update

Implemented the Deploy - upgrade RabbitMQ pipeline job that enables the automated upgrade and update of the RabbitMQ component.

Learn more

- MCP Operations guide: Upgrade RabbitMQ
- MCP Operations guide: Update RabbitMQ

Constrain the range of SSH ciphers to be accepted by the OpenSSH server
Enhanced the OpenSSH server to accept only strong ciphers and disabled the following weak ones:

- arcfour
- arcfour128
- arcfour256

Learn more

MCP Deployment Guide: Configure secure SSH ciphers

The force option for deleting the Octavia load balancers

Added the --force flag to the loadbalancer delete command to simplify the deletion of load balancers that hang in the PENDING state. For the usage details, see: 27071.

Disable DHCP on gateway nodes

Added the capability to disable DHCP on the gateway nodes so that DHCP can be handled on dedicated DHCP servers separately. The gateway:dhcp_agent_enabled: false option allows distributing load in terms of the number of OVS ports per node.

OpenContrail

In the MCP 2019.2.4 maintenance update, Mirantis added the possibility to set and modify the flow_cache_timeout for OpenContrail vRouter through the OpenContrail Salt formula. By default, the timeout value is 180 seconds. The value can be modified on highly loaded clusters by configuring flow_cache_timeout in your Reclass model.

To obtain the enhancement, first follow the steps described in Apply maintenance updates.

Learn more

MCP Operations Guide: Define aging time for flow records
StackLight

In the MCP 2019.2.4 maintenance update, Mirantis introduces the following enhancements for StackLight LMA:

- Elasticsearch and Kibana versions update
- Prometheus Elasticsearch exporter
- TLS encryption for StackLight
- VM state indicator
- Docker services logging
- KPI measurements
- Alerts optimization
- CADF notifications handled by Fluentd

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Elasticsearch and Kibana versions update

Updated Elasticsearch and Kibana from version 5.6.12 to 6.8.0.

Prometheus Elasticsearch exporter

Added support for Prometheus Elasticsearch exporter that periodically sends configured queries to the Elasticsearch cluster and exposes the results as Prometheus metrics that you can view in the Prometheus web UI.

Learn more

- MCP Reference Architecture: StackLight LMA components
- MPC Operations Guide: Enable Prometheus Elasticsearch exporter
TLS encryption for StackLight
Added the capability to encrypt the communication between Prometheus and Telegraf as well as Fluentd and Elasticsearch inside an MCP deployment over the Transport Layer Security (TLS) protocol.

**Warning**
The functionality does not cover encryption of the traffic between HAProxy and Elasticsearch.

**Learn more**
MCP Operations Guide: Enable TLS for StackLight

---

VM state indicator
Implemented the openstack_nova_instance_status and libvirt_domain_info_state metrics to provide an overview of a VM status from the OpenStack perspective and state from the libvirt perspective. To view the metrics, use the Prometheus web UI.

**Learn more**
MCP Operations Guide: Use the Prometheus web UI

---

Docker services logging
Added the capability for Fluentd to parse the Docker logs and send them to Elasticsearch. Now, you can view the Docker services logs in the Kibana web UI.

---

KPI measurements
Implemented the KPI Downtime and KPI Provisioning Grafana dashboards as well as the OVSInstanceArpingCheckDown and OpencontrailInstancePingCheckDownKey alerts to provide...
an overview of the infrastructure stability based on the following Key Performance Indicator (KPI) measurements:

**Provisioning KPI**

Provides the percentage of instances provisioning failures from the perspective of OpenStack notifications by tracking the compute.instance.create.start, compute.instance.create.end, and compute.instance.create.error Nova notifications and calculating the KPI on a daily basis. The measurements reset at midnight.

**Downtime KPI**

Provides the percentage of downtime check failures. Depending on the MCP cluster configuration, the downtime KPI includes the following measurements:

- The states of instances from the OpenStack perspective. In this case, a check is considered as failed if the instance state is ERROR.
- The instances network checks from the OVS or OpenContrail perspective:
  - For OVS, StackLight LMA performs Address Resolution Protocol (ARP) pings of the DHCP assigned IP address of the OpenStack instances. The check is considered as failed if all DHCP assigned IPs of the instance do not respond to ARP pings for 10 minutes.
  - For OpenContrail, StackLight LMA pings the link-local IP addresses of the OpenStack instances. The check is considered as failed if all link-local IPs of the instance do not respond to pings for 10 minutes.

**Learn more**

- MCP Operations Guide: KPI dashboards
- OVSInstanceArpingCheckDown alert
- OpencontrailInstancePingCheckDown alert

**Alerts optimization**

Enhanced the StackLight LMA alerts to provide for a more optimized infrastructure monitoring.

- Reconsidered the severities of the RabbitMQ* alerts and adjusted the Alertmanager* and SystemMemory* alerts.
- Restructured and enhanced the alerts documentation to provide alerts customization capabilities and troubleshooting recommendations, as well as list the alerts that require post-deployment tuning according to the deployment configuration.
- Added the following alerts:
  - BondInterfaceSingleSlave
  - OVSInstanceArpingCheckDown
• OpencontrailInstancePingCheckDown
• ContrailHealthCheckDisabled
• ContrailHealthCheckFailed
• ContrailGlobalVrouterConfigCheckDisabled
• ContrailGlobalVrouterConfigCheckFailed

• Removed the inefficient ContrailFLows*, NovaHypervisor*, NovaAggregate*, NovaTotalVCPUs*, NovaTotalMemory*, and NovaTotalDisk*, MemcachedServiceRespawn, MemcachedItemsNoneMinor, SystemSwap*, PrometheusTargetSamples*, and PrometheusDataIngestionWarning alerts.

Note
These alerts will be removed automatically when updating to MCP 2019.2.4. However, if you have modified any of these alerts, you must remove them manually as described in MCP Operations Guide: Manage alerts.

Learn more
• MCP Operations Guide: Available StackLight LMA alerts
• MCP Operations Guide: Alerts that require tuning

CADF notifications handled by Fluentd
Added the capability for Fluentd to handle the OpenStack Cloud Auditing Data Federation (CADF) notifications instead of Heka. Deprecated the Heka service.

If required, you can configure Fluentd running on the RabbitMQ nodes to forward the Cloud Auditing Data Federation (CADF) events to specific external security information and event management (SIEM) systems. For details, see MCP Operations Guide: Enable sending CADF events to external SIEM systems.

To enable CADF notifications handling by Fluentd and remove Heka:

1. On the cluster level of the Reclass model:
   1. In openstack/message_queue.yml, add the following class:

```
- system.fluentd.label.notifications
```

   2. In stacklight/client.yml, remove the following class:
3. In stacklight/server.yml, remove the Heka classes:

- system.heka.remote_collector.container
- system.heka.remote_collector.input.amqp
- system.heka.remote_collector.output.elasticsearch
- system.heka.remote_collector.output.telegraf

2. From the Salt Master node:

1. Update the Fluentd configuration:

```
salt -C "I@fluentd:agent" state.sls fluentd
```

2. Apply the changes:

```
salt -C "I@docker:swarm:role:master and I@prometheus:server" state.sls docker.client
```

3. Remove the Docker service with Heka:

```
salt -C "I@docker:swarm:role:master and I@prometheus:server" cmd.run 'docker service rm monitoring_remote_collector'
```

Ceph

Improved the Ceph Cluster Grafana dashboard by adding single statistics panels displaying the total, available, and used capacity of a Ceph cluster.

To obtain this enhancement, follow the steps described in Apply maintenance updates.

Learn more

MCP Operations Guide: Ceph dashboards

Documentation

Deprecated MCP Standard Configuration. The relevant information from this document is being updated and migrated to MCP Reference Architecture. Once the migration is complete, MCP Standard Configuration will be removed from the MCP documentation.

Addressed issues

The MCP 2019.2.4 update contains fixes for the DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph MCP components.

DriveTrain
Issues resolutions applied automatically

- [30840] Fixed the issue with the deployment failure of an OpenStack environment with OpenContrail 4.1 when applying the salt.minion.cert sls state.
- [30596] Fixed the issue with the Xtrabackup formula not changing permissions for /usr/local/bin/innobackupex-runner.sh on the dbs01 node.
- [30436] Fixed the issue with the Telemetry mdb nodes not using the Xenial image for deployment.
- [30288] Fixed the typo in infra/init.yml of the Cookiecutter templates to correctly render the openstack_version and jenkins_pipelines_branch parameters values during a Reclass deployment model generation.
- [30212] Fixed the issue with the DriveTrain update failing with the Docker containers for CI/CD services are having troubles with starting. error. The fix disables the Docker bridge in docker/host.yml of the Reclass model to prevent network conflicts.
- [30068] Fixed the typo in the system.haproxy.proxy.listen.openstack.novanc_large class of the HAProxy haproxy/proxy/listen/openstack/large_setup.yml file in the Reclass system model, which prevented the creation of the deployment model for large OpenStack clusters.
- [29923] Fixed the issue with the Deploy - OpenStack pipeline job being scheduled to run on the Jenkins master agent node instead of the slave agent node.
- [29941] Fixed the issue with the Deploy - virt snapshot VM pipeline job using the PATH variable to store /var/lib/libvirt/images regardless of the system environment PATH. The fix renames PATH to LIBVIRT_IMAGES_PATH to avoid collision with system variables.
- [27016] Fixed the issue with an MCP Kubernetes cluster with OpenContrail and StackLight failing to deploy due to the An un-handled exception was caught by salt's global exception handler error in cloud-init. The fix improves the wait_time condition checks in config-drive/master_config.yaml of the MCP common scripts.
- [30330] Fixed the issue with missing parameters for the IP and host name configuration for kvm nodes in the Model Designer web UI when the OpenStack Cluster Size parameter is set to Service Provider platform (50 to 150 nodes).
- [30658] Fixed the issue with the tests being unstable in case of slow responses of the Salt Master node or connection loss.
- [30401] Fixed the issue with no report being generated for the CVP - Performance tests Jenkins pipeline job.
- [30277] Fixed the naming for Docker containers with tests, which caused an unexpected error in case of CVP jobs running simultaneously.
- [30106] Added an exception that appears if a CVP job that requires the OpenStack component is run on a Kubernetes-based MCP cluster.
- [29195] Fixed the issue with the TOOLS_REPO parameter that caused the CVP - Functional tests in offline mode to fail with the can't read /home/rally/cvp-configuration/tempest/tempest_ext.conf: No such file or directory error message.
• [30449] Fixed the issue with the cleanup script not working properly for the CVP - Functional tests CVP - Performance tests, and CVP - HA tests Jenkins pipeline jobs because of a wrong path set by default.
• [30969] Fixed the issue with the HTTP/HTTPS protocols discovering in the CVP - Sanity checks UI tests.

Issues resolutions requiring manual application

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.</td>
</tr>
</tbody>
</table>

• [29128] Wrong user and password permissions in MySQL backup script
• [28628] Inability to modify client_body_buffer_size and ssl_trusted_certificate
• [30275] Jenkins losing connection to slave nodes while updating Ceph packages

[29128] Wrong user and password permissions in MySQL backup script
Modified the root user and password permissions in the innobackupex-runner.sh script used for MySQL backups to resolve the issue with user credentials available in cleartext.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Apply the following state:

```
salt 'dbs*' cmd.run 'chmod 750 /usr/local/sbin/innobackupex-runner.sh'
```

[28628] Inability to modify client_body_buffer_size and ssl_trusted_certificate
Enhanced the NGINX Salt formula by implementing the possibility to:

• Add the ssl_trusted_certificate parameter for the Online Certificate Status Protocol (OCSP) needs if the site.ssl.engine parameter is not defined in the NGINX Salt formula.
• Change the client_body_buffer_size parameter value that is based on the location.size parameter value by default.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Apply the following state:
salt -C '@nginx:server' state.apply nginx

[30275] Jenkins losing connection to slave nodes while updating Ceph packages
Fixed the issue with Jenkins losing connection to the jenkins-slave nodes during the execution of the Update Ceph packages pipeline job.
To apply the issue resolution:
1. Log in to the Salt Master node.
2. In ./reclass/classes/cluster/<cluster_name>/cicd/control/leader.yml, remove the following parameters:
   
   ```
   jenkins_slave_user: admin
   jenkins_slave_password: ${_param:jenkins_admin_password}
   ```
3. Refresh pillars:
   
   ```
   salt '*' saltutil.refresh_pillar
   ```

OpenStack

Issues resolutions applied automatically

- [30353] [Salt] Changed the default value of the Glance image protected type from string to bool to prevent the Glance state failures.
- [29437] [Salt] Added the Cinder volume image_conversion_dir configuration option to set the path to a directory used for temporary storage during image conversion. This prevents huge disk and input/output consumption on the controller nodes if no volume nodes are used.
- [30257] [Queens] Unhardcoded the RabbitMQ tuning settings in the Oslo templates Salt formula.
- [30178] [Pike, Queens] Changed the Oslo messaging configuration to treat the SSL error timeouts as socket timeouts. This prevents the Connection Forced: Too many heartbeats missed timeout errors on the compute nodes.
- [29447] [Pike, Queens] Added the possibility to handle possible TypeError in on_inbound_method in oslo_messaging to raise the Connection already closed recoverable error if another thread closes the RabbitMQ connection.
- [29308] [Pike] Fixed the retry logic in the RabbitMQ ensure method to prevent the nova-compute services from being unable to connect to RabbitMQ after restart of the RabbitMQ cluster.
- [30643] [Pike, Queens] Fixed the issue with Horizon displaying the Unable to connect to Neutron: 'frozenset' object has no attribute '_getitem_' error message in the Horizon logs
causing the instances list page to become empty. The error occurred during the network_list requests when the parameter list was too long.

• [29118] [Queens] Fixed the issue in Horizon that logged a user out with the keypair 403 (Quota Exceeded) error message from Nova. Previously, Horizon interpreted the Nova 403 error message as an unauthorized access and immediately logged the user out. Now, Horizon raises the corresponding Quota exceeded, too many key pairs. error message.

• [29415] [Queens] Fixed the Horizon test failures in the test environments with Python 3.5 and Django 2.0.

• [30447] [Salt] Unhardcoded the authentication URLs for the OpenID Connect (OIDC) protocol in the Keystone Salt formula.

• [30027] [Salt] Set the etc/hosts entries to lowercase in the Keystone Salt formula to prevent the glance image-list failed. HTTPMultipleChoices (HTTP 300) Requested version of OpenStack Images API is not available. exception after an MCP cluster redeployment with the cluster name containing capital letters.

• [29843] [Pike] Fixed the issue in the OpenStack control plane upgrade from Pike to Queens of the OpenStack deployments with Octavia. Previously, the Deploy - upgrade control VMs pipeline job could fail with the NotFound: The resource could not be found. (HTTP 404) error.

• [29844] [Pike] Fixed the issue in the Deploy - upgrade control VMs pipeline job failing during the application of the octavia.upgrade.verify._api state with Internal Server Error (HTTP 500) due to a missing ca-cert.pem on the MCP OpenStack deployments with Octavia.

• [29862] [Pike, Queens] Fixed the issue with the dist-upgrade stage errors being ignored during the execution of the OpenStack Deploy - upgrade control VMs pipeline job. The fix replaces runSaltProcessStep in the osUpgrade and osDistUpgrade functions with cmdRun, which has the ability to verify the return error codes.

• [30149] [Pike, Queens] Fixed the issue with live migration of instances between the Pike and Queens-based compute nodes after all controller nodes are upgraded to Queens. In Queens, the controller nodes send events about NICs being plugged only to the source compute nodes, while the Pike compute nodes logic expects these events on the destination nodes. The fix passes these events to both source and destination compute nodes.

• [29798] [Pike, Queens] Fixed the issue with the Barbican verification failure during the update of the OpenStack control plane by adding retries to the barbicanv1 client.

• [29451] [Reclass] Fixed the issue with IP being used instead of FQDN in OS_AUTH_URL for keystonercv3, keystonerc files, as well as in catalog and endpoint lists for admin and internal endpoints. The fix sets FQDN instead of IP for OS_AUTH_URL in keystonercv3.

• [29377] [Queens, Salt] Fixed the issue with the bootstrap procedure creating the Keystone admin user and executing on all OpenStack controller nodes. Added the cluster role node check to the Keystone Salt formula to execute the bootstrap procedure only once on the first OpenStack controller node only.

• [29357] [Salt] Updated the port configuration for RabbitMQ in the Barbican metadata to consistently use the port 5672.
• [29126] [Salt] Fixed the issue with the gnocchi.server state failing during an OpenStack cluster deployment by updating the Redis configuration for all Ceilometer-related components.

• [28990] [Salt] Fixed the potential security issue in an image corruption, compromising, or being overwritten due to the Glance show_multiple_locations and show_image_direct_url parameters being set to True by default. The fix sets these parameters to False by default.

• [28973] [Pike] Fixed the issue with inability to change the language to Chinese in Horizon dashboard.

• [28896] [Pike Queens] Added support for the | symbol to the VNC UI in Horizon. To apply the fix on existing OpenStack environments, stop the required instances using Nova or virsh and start them using Nova.

• [28726] [Queens] Fixed the issue with the Horizon Angular-based dashboards, for example, for uploading an image or creating a snapshot, not being refreshed after an item on the dashboard page changes its status from the transition state. For example, an image could remain in the endless Creating state until the page is reloaded. The fix adds a periodical check for the status of an item being in the transition state.

• [28711] [Pike Queens] Fixed the issue with the discrepancy between the availability zone name of an aggregate and a host after renaming the availability zone for an aggregate. Now, PUT /os-aggregates/{aggregate_id} and POST /os-aggregates/{aggregate_id}/action return an HTTP 400 message during an availability zone renaming if the hosts of an aggregate have any instances.

• [28688] [Pike] Fixed the following issues with image upload failures when Glance is used with the Swift back end:
  • Fixed the issue with renewing connections to Swift by adding usage of the cached auth_ref property instead of obtaining a new one each time a given token is about to expire.
  • Fixed the issue with the last chunk being left in storage when an image upload to the Swift back end fails. Previously, chunks were counted after uploading, now, they are counted before uploading.

• [28616] [Queens] Fixed the issue with glance-api failing to validate self-signed certificates when using Glance with Swift back end and SSL enabled.

• [27017] [Salt] Fixed the issue with inability to configure the Heat reauthentication methods by adding the possibility to set the reauthentication_auth_method parameter for Heat in the Reclass cluster model.

• [29603] [Salt] Fixed the issue with loss of connectivity to a guest VM after applying configuration changes to the Neutron OVS bridges. The fix adds linux:network:libvirt_vnet_repair: true to automatically reattach the libvirt vnet interfaces by getting the information about them from the current libvirt definitions to repair a guest VM connectivity with the host.

• [27276] [Salt] Fixed the issue with importing errors and loading warnings on the Salt Master node from the neutronv2 modules.

• [30150] [Pike] Fixed the issue with the MAC address is in use error when migrating a VM with a direct-physical port if the SR-IOV Physical Function (PF) passthrough (PT) ports are
used. The fix adds a reset of a MAC address when unbinding a direct-physical port from a VM.

- [29402] [Salt] Fixed the issue with the Neutron Salt formula being unable to handle the default quotas by adding a capability to configure them.

- [29110] [Pike] Fixed the issue with failures during bulk creation of IPv6 subnets using API, leading to HTTP/1.1 500 Internal Server Error.

- [29040] [Salt] Added the capability to change the hardcoded values in the Cinder, Glance, and Nova configuration files by adding the configmap pillars to related Salt formulas.

- [25928] [Pike] Fixed the issue that caused approximately 5% of instances to fail during the live migration of QEMU v2.5 to v2.11.

- [30410] [Queens] Fixed the issue with inability to create a new VM after upgrading an MCP cluster.

- [27222] Fixed the issue with the /var/log/glance/api.log permissions causing the upgrade of OpenStack to fail with the Salt state on controller nodes (``ctl*``) failed exception.

- [31278] [Pike] Fixed the issue with MySQL occasionally failing on the Galera nodes.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

- [28172] MySQL server node fails after desyncing itself from group
- [29930] Excessive disk usage while clearing ephemeral LVM volumes using shred
- [30205] The Telemetry notification queues in RabbitMQ with disabled Telemetry
- [27765] Nova live snapshot feature not using Ceph back end snapshot mechanism
- [30216] The fs.inotify.max_user_instances value reaches the maximum limit
- [31284] Neutron failing to connect to MySQL

[28172] MySQL server node fails after desyncing itself from group

Pike, Queens

Fixed the issue that caused the MySQL server node failure after it desynced itself from the Galera cluster.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Restart the MySQL service on every database server node, one by one.
   For example:
   
   ```
   salt 'dbs03*' cmd.run 'systemctl restart mysql'
   ```

3. Verify that every node loaded the updated Galera provider.
   For example:
   
   ```
   salt 'dbs*' mysql.status | grep -A1 wsrep_provider_version
   ```

   Example of system response:
   
   ```
   wsrep_provider_version:
     3.20(r7e383f7)
   --
   wsrep_provider_version:
     3.20(r7e383f7)
   --
   wsrep_provider_version:
     3.20(r7e383f7)
   ```

[29930] Excessive disk usage while clearing ephemeral LVM volumes using shred

Queens

Implemented the ability to set the ionice level for the ephemeral LVM volume shred operation in nova-compute to prevent excessive disk consumption. Setting of the ionice level described below makes sense if:

- nova:compute:lvm:ephemeral is set to True
- nova:compute:lvm:volume_clear is set to zero or shred

To apply the issue resolution:

1. Log in to the Salt Master node.
2. In `classes/cluster/<cluster_name>/openstack/compute.yml`, set the level for `volume_clear_ionice_level` as required:
   
   ```
   nova:
     compute:
       lvm:
         volume_clear_ionice_level: <level>
   ```

   Possible `<level>` values are as follows:
• idle - to use the idle scheduling class. This option impacts system performance the least with a downside of increased time for a volume clearance.

• From 0 to 7 - to use the best-effort scheduling class. Set the priority level to the specified number.

• No value - not to set the I/O scheduling class explicitly. Mirantis does not recommend using no value since this is the most aggressive option in terms of system performance impact.

3. Apply the changes:

```
salt -C '@nova:compute' state.sls nova.compute
```

[30205] The Telemetry notification queues in RabbitMQ with disabled Telemetry

Pike, Queens

Disabled the Telemetry notification queues in RabbitMQ for the OpenStack clusters with StackLight enabled and Telemetry disabled.

To apply the issue resolution:

1. Log in to the Salt Master node.

2. In `classes/cluster/<cluster_name>/openstack/init.yml`, remove the notifications variable from the `openstack_notification_topics` parameter leaving only the `$_param:stacklight_notification_topic` variable:

```
openstack_notification_topics: "$_param:stacklight_notification_topic"
```

3. Apply the changes:

```
salt "ctl*" state.sls keystone,glance,heat
salt -C "ctl* or cmp*" state.sls nova,neutron,cinder -b 20
```

[27765] Nova live snapshot feature not using Ceph back end snapshot mechanism

Pike, Queens

Added support for the Ceph back end snapshotting mechanism to the Nova VM live snapshotting feature on the OpenStack environments with Ceph back end used for Nova.

To apply the issue resolution:

1. Log in to the Salt Master node.

2. In `classes/cluster/<cluster_name>/openstack/control.yml` of your Reclass model, add the following parameter:
3. In `classes/cluster/<cluster_name>/openstack/compute/init.yml`, add the following parameter:

   ```yaml
   glance:
     server:
       show_multiple_locations: True
   ```

4. Apply the changes:

   ```bash
   salt -C 'I@glance:server' state.sls glance.server
   salt -C 'I@nova:compute' state.sls nova.compute
   ```

5. Log in to the cmn01 node.

6. Define the rbd permission for pools where images and VMs are stored:

   ```bash
   ceph-authtool /etc/ceph/ceph.client.nova.keyring -n client.nova \
   --cap osd 'profile rbd pool=vms, profile rbd pool=images' \
   --cap mon 'allow r, allow command "osd blacklist"'
   ```

   Substitute the vms and images values with the corresponding pool names for Nova and Glance.

7. Apply the changes for Ceph:

   ```bash
   ceph auth import -i /etc/ceph/ceph.client.nova.keyring
   ```

---

**[30216]** The `fs.inotify.max_user_instances` value reaches the maximum limit

Pike, Queens

Fixed the issue with reaching the maximum limit of the `fs.inotify.max_user_instances` parameter value that prevented an OpenStack compute node to be configured as a DHCP node. The fix increases the default value to 4096 with the possibility to modify it as required.

To apply the issue resolution:

1. Log in to the Salt Master node.

2. In `classes/system/neutron/compute/cluster.yml` of your Reclass model, verify that the following snippet exists:
Linux:
  System:
  Kernel:
  Sysctl:
    fs.inotify.max_user_instances: 4096

3. Apply the changes to the OpenStack compute nodes hosting DHCP:

    salt 'cmp<node_number*>' state.apply linux.system.kernel

[31284] Neutron failing to connect to MySQL

Pike

Fixed the issue with neutron-server failing to reconnect to MySQL after a crash of a MySQL server.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Apply the neutron state on the OpenStack controller nodes:

    salt -C '@neutron:server' state.sls neutron

OpenContrail

This section provides the list of the OpenContrail issues resolutions that are automatically applied to your MCP cluster after you perform the steps described in Apply maintenance updates.

- [30480] Added the missing var/crashes directory to the OpenContrail analytics container for the contrail-analytics-nodemgr service to properly handle logging of the OpenContrail monitoring, alarm, and web UI services.
- [30406] Fixed the issue in the Crossfilter JavaScript library that could cause random data loss and unexpected behavior in the OpenContrail web UI.
- [29849] Fixed the issue with the network objects such as networks, subnets, and others not being created after the update of OpenContrail 4.x in the MCP OpenStack deployments if SSL is enabled on the Keystone internal endpoints. The fix adds the usage of insecure = true for connection to Keystone through SSL.
- [29450] Fixed the issue with the OpenContrail Salt formulas using the ifmap-server package for OpenContrail 4.x instead of the internal implementation of ifmap.
- [29090] Fixed the issue with contrail-config-nodemgr spawning NodeTool.Repair for non-existing keyspaces by removing the keyspace repairing of the DISCOVERY_SERVER service, which is not used by OpenContrail starting version 4.0.
• [28202] Fixed the issue with infinite connection retries to contrail-api by setting the wait_for_connect parameter to False in the OpenContrail Salt formula.

• [29809] Fixed the issue with the OpenContrail states failing due to the dependencies of the Python packages for OpenContrail during an initial deployment of OpenStack with OpenContrail.

• [29253] Fixed the issue with the OpenContrail health check failing due to the non-working confluent-kafka service that often fails on slow environments during the OpenContrail deployment because of connection timeouts. The fix changes the restart option in the confluent-kafka service file.

• [29041] Fixed the issue with slow logging in to the OpenContrail web UI after upgrading OpenContrail to version 4.1. The fix removes contrail-charts.css from dashboard.tmpl since it is also included to contrail.thirdparty.unified.css.

• [27600] Fixed the issue with ordering of the schema-transformer objects reinit in OpenContrail 4.1 to avoid downtime during the contrail-schema failover. This fixes the issue of route targets being temporarily removed from an SNAT routing instance during the reinit procedure.

• [29812] Fixed the issue with the contrail-webui service failing to start after updating OpenContrail version 4.x due to the missing quotation mark in /etc/contrail/config.global.js.

• [28286] Fixed the issue with inability to select any availability zone in the Horizon web UI while launching an instance on the OpenStack Queens environments with OpenContrail 4.1.

• [29354] Fixed the issue with inability to list, create, update, or delete load balancers by non-admin users in OpenContrail 4.1.

• [31269] Fixed the contrail-vrouter-agent crashing during the VrfEntry::DeleteTimeout() assertion.

• [29190] Fixed the issue with connectivity between the VMs through an external network in case when the VMs were connected to networks with different forwarding modes L2 or L3 (default) and L3 only. The issue appeared when a VM tried to reach the floating IP of another VM through SNAT to an external network hosting the floating IP.

StackLight

Issues resolutions applied automatically

• [30343] To prevent the issue with Alertmanager cluster synchronization failures, changed the version of Alertmanager to 0.14.0. Now, when deploying MCP Q4`18, Alertmanager v0.14.0 installs by default instead of v0.15.3.

• [29228] Fixed the issue with the Telegraf Ceph input plugin failing to gather Ceph metrics after upgrading Ceph to Luminous.

• [28126] Fixed the issue with no data being available in the Snapshots graphs of the Glance Grafana dashboard.

• [24049] Fixed the issue with the name for the Elasticsearch cluster instance being set improperly, which could cause performance degradation.
• [28803] Fixed the issue with Telegraf failing to gather OpenStack metrics in case of an incorrect deployment of one OpenStack compute node.

• [29254] Fixed the issue that caused the queries with commas, such as abc{d="x",e="y"} to fail in Gainsight.

• [30422] Fixed the issue with the rate interval variables in the Jenkins, Apache, and System disk I/O Grafana dashboards to display a dynamic rate interval instead of a static one.

• [30558] Fixed the issue with inability to set the timeout for Prometheus Relay by adding the PrometheusRelayClientTimeout. Now, you can define the timeout for Prometheus Relay as described in MCP Operations Guide: Configure Prometheus long-term storage.

• [26897] Fixed the issue with the libvirt-exporter logs being gathered with no severities.

• [29246] Fixed the issue that could cause user lockout in case of a Salesforce authentication exception. Now, in case of wrong credentials provided, 30 seconds must pass before the next attempt.

• [27144] Fixed the discrepancy in disk usage data between the Horizon web UI and the Nova utilization dashboard in Grafana.

• [30429] Fixed the issue with the Telegraf plugin for OpenStack randomly hanging on until a manual restart.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [26249] Grafana dashboard displays no data
• [27504] Alertmanager notifications include internal URLs

[26249] Grafana dashboard displays no data
Fixed the issue with the Prometheus Stats Grafana dashboard displaying no data in the Queries duration panels.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In stacklight/client.yml, replace the following parameter:

   grafana_prometheus_port: ${_param:prometheus_relay_bind_port}

   with:
grafana_prometheus_port: \${_param:cluster_prometheus_relay_port}

3. In stacklight/init.yml, add the following parameter to the _param section:

cluster_prometheus_relay_port: 8080

4. Log in to the Salt Master node.

5. Apply the following state:

\texttt{salt -C \textquoteleft I@grafana:client\textquoteleft state.sls grafana.client}

[27504] Alertmanager notifications include internal URLs

Fixed the issue with the Alertmanager notifications including internal URLs instead of public ones.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In infra/config/proxy.yml, remove the cluster_public_host parameter.
3. In infra/init.yml, set the cluster_public_host parameter to the cluster external address of FQDN, if any. Otherwise, set the parameter to \${_param:openstack_proxy_address} or \${_param:kubernetes_proxy_address} according to your deployment type.
4. In stacklight/server.yml:
   1. Set the alertmanager_external_url parameter to \${_param:cluster_public_host}.
   2. Remove the following parameters:

   \begin{verbatim}
   cluster_public_host: \${_param:cluster_vip_address}
   # Proxy
   cluster_ssl_certificate:
     enabled: true
     pem_file: /etc/haproxy/ssl/${_param:cluster_public_host}-all.pem
   haproxy_bind_address: \${_param:cluster_vip_address}
   \end{verbatim}

5. Log in to the Salt Master node.

6. Apply the following states one by one:

\texttt{salt -C \textquoteleft I@docker:swarm and I@prometheus:server\textquoteleft state.sls prometheus -b 1}
\texttt{salt -C \textquoteleft I@salt:minion\textquoteleft state.sls salt.minion.cert}

Ceph

Issues resolutions applied automatically
• [29926] Fixed the issue with the Ceph Hosts Overview Grafana dashboard displaying incorrect data in the AVG Disk Utilization panel.
• [30204] Fixed the issue with the rate_interval drop-down menu missing in all Grafana dashboards for Ceph.
• [30131] Fixed the issue with the WaitForHealthy function in the Ceph pipeline jobs that could get stuck for 16 minutes with no reason.
• [29946] Fixed the issue with improper Ceph backup during the upgrade of a Ceph cluster from Jewel to Luminous using the Ceph - upgrade pipeline job. Added the BACKUP_DIR parameter that enables specifying of the target directory for the backup.
• [29452] Fixed the issue with IPs being used by radosgw-swift instead of FQDN in the URLs for the admin and internal RADOS Gateway endpoints.
• [27293] Added the capability to use permanent disk names during the Ceph deployment to prevent the disks names changing after each reboot or commissioning.

Issues resolutions requiring manual application

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

• [30161] Ceph Monitor nodes backups can cause cluster outage
• [29811] Inability to change the maximum number of PGs per OSD

[30161] Ceph Monitor nodes backups can cause cluster outage
Fixed the issue with scheduled backups of the Ceph Monitor nodes, which could cause cluster raise condition or outage. Now, the backups for different Ceph Monitor nodes run at a different time. An additional health check has been added to verify the Ceph Monitor nodes during backup.

To apply the issue resolution:
1. Open your Git project repository with the Reclass model on the cluster level.
2. In classes/cluster/cluster_name/ceph/mon.yml, add the following parameters:

```yaml
parameters:
  ceph:
    backup:
      client:
        backup_times:
          hour: ${_param:ceph_backup_time}
```
3. In classes/cluster/cluster_name/ceph/init.yml, add the following pillar in the parameters section:

```yaml
ceph_mon_node01_ceph_backup_hour: 2
ceph_mon_node02_ceph_backup_hour: 3
ceph_mon_node03_ceph_backup_hour: 4
```

4. In classes/cluster/cluster_name/infra/config/nodes.yml, for each Ceph Monitor node specify the ceph_backup_time parameter. For example:

```yaml
ceph_mon_node01:
  params:
    {%- if cookiecutter.get('static_ips_on_deploy_network_enabled', 'False') == 'True' %}
    deploy_address: ${_param:ceph_mon_node01_deploy_address}
    {%- endif %}
    ceph_public_address: ${_param:ceph_mon_node01_ceph_public_address}
    ceph_backup_time: ${_param:ceph_mon_node01_ceph_backup_hour}
```

5. Log in to the Salt Master node.

6. Apply the following state:

```
salt -C "I@ceph:monitor" state.sls ceph.backup
```

7. In crontab on each Ceph Monitor, verify that the scripts running time changed.

[29811] Inability to change the maximum number of PGs per OSD

Fixed the issue with inability to change the maximum number of PGs per OSD using the mon_max_pg_per_osd parameter.

To apply the issue resolution:

1. Log in to the Salt Master node.

2. Apply the ceph.common state on all Ceph nodes:

```
salt -C "$@ceph:common" state.sls ceph.common
```

3. Restart the Ceph Monitor, Manager, OSD, and RADOS Gateway services on the Ceph nodes in the following strict order:

```
Warning
After the restart of every service, wait for the system to become healthy. Use the ceph health command to verify the Ceph cluster status.
```
1. Restart the Ceph Monitor and Manager services on all cmn nodes one by one:

```bash
salt -C NODE_NAME cmd.run 'systemctl restart ceph-mon.target'
salt -C NODE_NAME cmd.run 'systemctl restart ceph-mgr.target'
salt -C NODE_NAME cmd.run 'ceph -s'
```

2. Restart the Ceph OSD services on all osd nodes one by one:

```bash
salt -C NODE_NAME cmd.run 'systemctl restart ceph-osd@<osd_num>'
```

3. Restart the RADOS Gateway service on all rgw nodes one by one:

```bash
salt -C NODE_NAME cmd.run 'systemctl restart ceph-radosgw.target'
```

### Known issues

This section lists the MCP 2019.2.4 known issues and workarounds.

- [31028] Barbican may interfere with other services
- [31397] Upgrade of controller VMs fails on the ctl01 node
- [31462] Kubernetes deployment failure

**[31028] Barbican may interfere with other services**

PIKE, fixed in 2019.2.5

Barbican may interfere with other services, such as Ceilometer, Aodh, Panko, or Designate, by consuming notifications needed by these services to function properly. The symptoms of the issue include:

- The event alarms are sometimes not triggered
- The Designate records are sometimes not automatically created
- Some events are missing in Panko

**Workaround:**

1. Log in to the Salt Master node.
2. Open your project Git repository with the Reclass model on the cluster level.
3. In the `/classes/cluster/<cluster_name>/openstack/control.yml` file, set an additional topic for Keystone to send notifications to:

```yaml
keystone:
  server:
    notification:
      topics: "notifications, stacklight_notifications, barbican_notifications"
```
4. In the /classes/cluster/<cluster_name>/openstack/barbican.yml file, configure Barbican to listen on its own topic:

```
barbican:
  server:
    ks_notifications_topic: barbican_notifications
```

5. Apply the changes:

```
salt 'ctl*' state.apply keystone -b 1
salt 'kmn*' state.apply barbican -b 1
```

[31397] Upgrade of controller VMs fails on the ctl01 node

PIKE TO QUEENS UPGRADE, fixed in 2019.2.5

The Deploy - upgrade control VMs pipeline job fails for the ctl01 node during the OpenStack environment upgrade from Pike to Queens with heat-keystone-setup-domain authorization error.

Workaround:

1. Log in to the Salt Master node.
2. Open your project Git repository with the Reclass model on the cluster level.
3. In /classes/cluster/<cluster_name>/infra/init.yml, add the system.linux.network.hosts.openstack class.
4. Refresh pillars:

```
salt '*' saltutil.pillar_refresh
```
5. Apply the changes:

```
salt '*' state.apply linux.network.host
salt 'ctl*' state.apply keystone.server
```
6. Verify the Keystone endpoint list:

```
salt 'ctl*' cmd.run "./root/keystonercv3; openstack user list"
```

The system response must contain the Keystone user list.

Example of system response extract:

```
ctl03.8827.local:
+-------------------------------+----------------------+
| ID                           | Name                 |
+-------------------------------+----------------------+
```
7. Rerun the Deploy - upgrade control VMs pipeline job.

[31462] Kubernetes deployment failure

The Kubernetes with Calico deployment using the Deploy - OpenStack pipeline job fails during the CA file generation stage.

Workaround:

1. Log in to the Salt Master node.
2. Update mine:

   ```bash
code
   state.sls salt.minion.ca
   ```
3. Create the CA file:

   ```bash
code
   state.sls salt.minion.cert
   ```
4. Re-run the Deploy - OpenStack pipeline job to finalize the Kubernetes deployment.

Updated MCP components

The MCP 2019.2.4 update includes the following changes in the minor and versions of the MCP components compared to the MCP 2019.2.3 update.

- Updated major versions of the MCP components
- Updated packages from the Mirantis and mirrored repositories
- Updated Kubernetes components

Note

For the full list of the versions of the major MCP components, see [Major components versions](#).
Updated major versions of the MCP components

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.3</th>
<th>2019.2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacklight</td>
<td>Alertmanager</td>
<td>0.15.3</td>
<td>0.14.0</td>
</tr>
<tr>
<td></td>
<td>Elasticsearch</td>
<td>5.6.12</td>
<td>6.8.0</td>
</tr>
<tr>
<td>Kibana</td>
<td></td>
<td>5.6.12</td>
<td>6.8.0</td>
</tr>
<tr>
<td>DriveTrain</td>
<td>GlusterFS</td>
<td>3.8</td>
<td>5.5</td>
</tr>
</tbody>
</table>

Updated packages from the Mirantis and mirrored repositories

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.3</th>
<th>2019.2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack Pike</td>
<td>barbican</td>
<td>1:5.0.1-3~u16.04+mcp9</td>
<td>1:5.0.1-3~u16.04+mcp13</td>
</tr>
<tr>
<td></td>
<td>ceilometer</td>
<td>1:9.0.6-2~u16.04+mcp7</td>
<td>1:9.0.6-2~u16.04+mcp22</td>
</tr>
<tr>
<td></td>
<td>cinder</td>
<td>2:11.2.0-2~u16.04+mcp102</td>
<td>2:11.2.2-2~u16.04+mcp104</td>
</tr>
<tr>
<td></td>
<td>dpdk</td>
<td>17.05.2-1~u16.04+mcp17</td>
<td>17.11.3-4~u16.04+mcp1</td>
</tr>
<tr>
<td></td>
<td>galera-3</td>
<td>n/a</td>
<td>25.3.20-1~u16.04+mcp</td>
</tr>
<tr>
<td></td>
<td>heat</td>
<td>1:9.0.5-1~u16.04+mcp2</td>
<td>1:9.0.7-1~u16.04+mcp4</td>
</tr>
<tr>
<td></td>
<td>horizon</td>
<td>3:12.0.3-4~u16.04+mcp6</td>
<td>3:12.0.4-4~u16.04+mcp69</td>
</tr>
<tr>
<td></td>
<td>ironic</td>
<td>1:9.1.6-1~u16.04+mcp36</td>
<td>1:9.16-1~u16.04+mcp49</td>
</tr>
<tr>
<td></td>
<td>libvirt</td>
<td>4.0.0-1.8.5~u16.04+mcp10</td>
<td>4.0.0-1.8.10~u16.04+mcp1</td>
</tr>
<tr>
<td></td>
<td>manila</td>
<td>1:5.0.3-1~u16.04+mcp1</td>
<td>1:5.0.3-1~u16.04+mcp5</td>
</tr>
<tr>
<td></td>
<td>networking-bagpipe</td>
<td>7.0.0-2~u16.04+mcp12</td>
<td>7.0.0-2~u16.04+mcp12</td>
</tr>
<tr>
<td></td>
<td>networking-l2gw</td>
<td>1:11.0.0-1~u16.04+mcp11</td>
<td>1:11.0.0-1~u16.04+mcp17</td>
</tr>
<tr>
<td></td>
<td>networking-odl</td>
<td>1:11.0.0-1~u16.04+mcp1</td>
<td>1:11.0.0-1~u16.04+mcp15</td>
</tr>
<tr>
<td></td>
<td>neutron</td>
<td>2:11.0.6-2~u16.04+mcp2</td>
<td>2:11.0.8-2~u16.04+mcp17</td>
</tr>
<tr>
<td></td>
<td>neutron-fwaas</td>
<td>2:11.0.1-2~u16.04+mcp1</td>
<td>2:11.0.2-2~u16.04+mcp8</td>
</tr>
<tr>
<td></td>
<td>neutron-lbaas</td>
<td>2:11.0.3-1~u16.04+mcp1</td>
<td>2:11.0.3-1~u16.04+mcp15</td>
</tr>
<tr>
<td></td>
<td>nova</td>
<td>2:16.1.7-4~u16.04+mcp16</td>
<td>2:16.1.8-4~u16.04+mcp18</td>
</tr>
<tr>
<td></td>
<td>octavia</td>
<td>1.0.3-6~u16.04+mcp151</td>
<td>1.0.3-7~u16.04+mcp15</td>
</tr>
<tr>
<td></td>
<td>openvswitch</td>
<td>2.8.4-0.0.17.10.1~u16.04+mcp124</td>
<td>2.8.4-0.0.17.10.1~u16.04+mcp15</td>
</tr>
<tr>
<td></td>
<td>panko</td>
<td>3.1.0-1~u16.04+mcp143</td>
<td>3.1.0-1~u16.04+mcp15</td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>python-amqp</td>
<td>2.2.1-1<del>exp1</del>u16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-aodhclient</td>
<td>0.9.0-1~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-barbicanclient</td>
<td>4.5.3-1.1~u16.04+mcp4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-castellan</td>
<td>0.12.2-1~u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-cinderclient</td>
<td>1:3.1.0-1~u16.04+mcp3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-cliff</td>
<td>2.8.2-1~u16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-glance-store</td>
<td>0.22.0-3~u16.04+mcp4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-monascaclient</td>
<td>1.7.1-1~u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-openstackclient</td>
<td>3.12.1-1~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-os-brick</td>
<td>1.15.7-1~u16.04+mcp17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.cache</td>
<td>1.25.1-1~u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.context</td>
<td>1:2.17.1-1~u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.db</td>
<td>4.25.1-3~u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.log</td>
<td>3.30.2-1~u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.messaging</td>
<td>5.30.7-1~u16.04+mcp18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.privsep</td>
<td>1.22.1-1~u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.service</td>
<td>1.25.1-1~u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ovsdbapp</td>
<td>0.4.3-1~u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-vmware-nsxlib</td>
<td>11.0.3-1.0~u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>qemu</td>
<td>1:2.11+dfsg-1.7.3~u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rabbitmq-server</td>
<td>3.6.15-3~u16.04+mcp13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmware-nsx</td>
<td>11.0.2-2~u16.04+mcp42</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenStack Queens</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aodh</td>
<td>6.0.1-2~u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>barbican</td>
<td>1:6.0.1-4~u16.04+mcp32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ceilometer</td>
<td>1:10.0.1-2~u16.04+mcp30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cinder</td>
<td>2:12.0.5-2~u16.04+mcp100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>designate</td>
<td>1:6.0.1-1.0~u16.04+mcp22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>galera-3</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>glance</td>
<td>2:16.0.1-2~u16.04+mcp27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gnocchi</td>
<td>4.2.4-4~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>heat</td>
<td>1:10.0.2-1.0~u16.04+mcp59</td>
<td></td>
<td></td>
</tr>
<tr>
<td>heat-dashboard</td>
<td>1.0.2-4~u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>horizon</td>
<td>3:13.0.1-10~u16.04+mcp74</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>horizon-contrail-panels</td>
<td>2:0.1.2-1<del>u16.04+mcp2:0.1.2-1</del>u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ironic</td>
<td>1:10.1.8-1.0<del>u16.04+mcp10.1.8-1.0</del>u16.04+mcp57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>keystone</td>
<td>2:13.0.2-3<del>u16.04+mcp3:13.0.2-3</del>u16.04+mcp30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>libvirt</td>
<td>4.0.0-1.8.5<del>u16.04+mcp4.0.0-1.8.10</del>u16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manila</td>
<td>1:6.1.0-2<del>u16.04+mcp2:6.3.0-2</del>u16.04+mcp47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>manila-ui</td>
<td>2:13.0-1.0<del>u16.04+mcp2:13.1-1.0</del>u16.04+mcp4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-bagpipe</td>
<td>8.0.1-2<del>u16.04+mcp8.0.1-2</del>u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-baremetal</td>
<td>1.0.0-1<del>u16.04+mcp1.0.0-1</del>u16.04+mcp13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-bgpvpn</td>
<td>8.0.1-1.0<del>u16.04+mcp8.0.1-1.0</del>u16.04+mcp13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-generic-switch</td>
<td>1.0.0-1<del>u16.04+mcp1.0.0-1</del>u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-l2gw</td>
<td>1:12.0.1-1.0<del>u16.04+mcp1:12.0.1-1.0</del>u16.04+mcp17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-odl</td>
<td>1:12.0.0-1.0<del>u16.04+mcp1:12.0.0-1.0</del>u16.04+mcp45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>networking-ovn</td>
<td>4.0.3-1.0<del>u16.04+mcp2:0.3-1.0</del>u16.04+mcp3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron</td>
<td>2:12.0.5-5<del>u16.04+mcp2:13.0-5-5</del>u16.04+mcp201</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-fwaas</td>
<td>2:12.0.1-1.0<del>u16.04+mcp2:12.0.1-1.0</del>u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>neutron-lbaas</td>
<td>2:12.0.0-2<del>u16.04+mcp2:12.0.0-2</del>u16.04+mcp50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nova</td>
<td>2:17.0.9-6<del>u16.01+mcp2:18.0.9-6</del>u16.01+mcp188</td>
<td></td>
<td></td>
</tr>
<tr>
<td>octavia</td>
<td>2.0.4-6<del>u16.04+mcp5:2.1.0.7</del>u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>octavia-dashboard</td>
<td>1.0.1-1.3<del>u16.04+mcp1:1.3-1.3</del>u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>openswitch</td>
<td>2.9.0-0.1<del>u16.04+mcp2:9.5-1</del>u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>panko</td>
<td>4.0.2-2<del>u16.04+mcp4:0.2-2</del>u16.04+mcp15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-amqp</td>
<td>2.2.1-1<del>exp1</del>u16.04+mcp2:2.1-1<del>exp1</del>u16.04+mcp3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-aodhclient</td>
<td>1.0.0-1<del>u16.04+mcp1.0.0-1</del>u16.04+mcp8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-automaton</td>
<td>1.14.0-1.0<del>u16.04+mcp4:14.0-1.0</del>u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-barbicanclient</td>
<td>4.6.1-1.0<del>u16.04+mcp4:6.1-1.0</del>u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-brick-cinderclient</td>
<td>0.8.0-1<del>u16.04+mcp0.8.0-1</del>u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-castellan</td>
<td>0.17.0-1.0<del>u16.04+mcp0.17.0-1.0</del>u16.04+mcp15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-cinderclient</td>
<td>1:3.5.0-1.0<del>u16.04+mcp1:5.0-1.0</del>u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-cryptography</td>
<td>2.1.4-1.0<del>u16.04+mcp2:1.4-1.1.2</del>u16.04+mcp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-debtcollector</td>
<td>1.19.0-0.1<del>u16.04+mcp1.19.0-0.1</del>u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-designateclient</td>
<td>2.9.0-1.0<del>u16.04+mcp2:9.0-1.0</del>u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-futurist</td>
<td>1.6.0-1.0<del>u16.04+mcp1.6.0-1.0</del>u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package Name</td>
<td>Version</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------</td>
<td></td>
</tr>
<tr>
<td>python-glance-store</td>
<td>0.23.0-2~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-glanceclient</td>
<td>1:2.10.1-1.0~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-heatclient</td>
<td>1.14.0-1.0~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ironic-lib</td>
<td>2.12.2-1.0~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ironicclient</td>
<td>2.2.1-1.0~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-keystonemiddleware</td>
<td>1:2.15.0-1.0~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-keystoneclient</td>
<td>1:3.15.0-1.0~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-keystonemiddleware</td>
<td>2.21.0-1.0~u16.04+mcp17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ladappool</td>
<td>2.2.0-1~u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-manilaclient</td>
<td>1.21.1-1-1.0~u16.04+mcp21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-monascaclient</td>
<td>1.10.0-1.0~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-neutron-lib</td>
<td>1.13.0-1.0~u16.04+mcp9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-neutronclient</td>
<td>1:6.7.0-1.0~u16.04+mcp37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-novaclient</td>
<td>2:9.1.1-1~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-octaviaclient</td>
<td>1.4.0-3~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-openstackclient</td>
<td>3:14.3-1.0~u16.04+mcp14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-openstacksdk</td>
<td>0.11.3+repack-1.0~u16.04+mcp14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-os-brick</td>
<td>2.3.5-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-os-client-config</td>
<td>1.29.0-1.0~u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-os-traits</td>
<td>0.5.0-1.0~u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-os-vif</td>
<td>1.9.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-osc-lib</td>
<td>1.9.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.cache</td>
<td>1.28.0-1.0~u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.concurrency</td>
<td>8.25.1-1.0~u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.config</td>
<td>1:5.2.0-1.0~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.context</td>
<td>1:2.20.0-1.0~u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.db</td>
<td>4.33.1-1.0~u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.i18n</td>
<td>3.19.0-1.0~u16.04+mcp8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.log</td>
<td>3.36.0-1.0~u16.04+mcp8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.messaging</td>
<td>5.35.4-2~u16.04+mcp25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.middleware</td>
<td>3.34.0-1.0~u16.04+mcp8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.policy</td>
<td>1.33.2-1.0~u16.04+mcp5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.privsep</td>
<td>1.27.0-1.0~u16.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.reports</td>
<td>1.26.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.rootwrap</td>
<td>5.13.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.serialization</td>
<td>2.24.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.service</td>
<td>1.29.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo-utils</td>
<td>3.35.1-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-oslo.versionedobjects</td>
<td>1.31.3-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-ovsdbapp</td>
<td>0.10.3-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-pankoclient</td>
<td>0.4.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-pycadf</td>
<td>2.7.0-1~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-swiftclient</td>
<td>1:3.5.0-2~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-taskflow</td>
<td>3.1.0-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-tooz</td>
<td>1.60.1-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>python-vmware-nsxlib</td>
<td>12.0.4-1.0~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>qemu</td>
<td>1:2.11+dfsg-1.4~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rabbitmq-server</td>
<td>3.6.15-3~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ryu</td>
<td>4.15-1~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stevedore</td>
<td>1:1.28.0-1~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sushy</td>
<td>1.3.3-1~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tempest</td>
<td>1:18.0.0-1~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmware-nsx</td>
<td>12.0.2-2~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>websockify</td>
<td>0.8.0+dfsg1-7~u16.04+mcp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OpenContrail 4.1

<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ceilometer-plugin-contrail</td>
<td>1.1<del>20190412052601-04.1</del>20190620130104-0</td>
</tr>
<tr>
<td>contrail</td>
<td>4.1<del>20190412052601-04.1</del>20190620130104-0</td>
</tr>
<tr>
<td>contrail-heat</td>
<td>4.1<del>20190412052601-04.1</del>20190620130104-0</td>
</tr>
<tr>
<td>contrail-vrouter-dpk</td>
<td>4.1<del>20190412052601-04.1</del>20190620130104-0</td>
</tr>
<tr>
<td>contrail-web-controller</td>
<td>4.1<del>20190412052601-04.1</del>20190620130104-0</td>
</tr>
<tr>
<td>contrail-web-core</td>
<td>4.1<del>20190412052601-04.1</del>20190620130104-0</td>
</tr>
<tr>
<td>neutron-plugin-contrail</td>
<td>4.1<del>20190412052601-04.1</del>20190620130104-0</td>
</tr>
</tbody>
</table>

Salt formulas

<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>salt-formula-aodh</td>
<td>0.2+201903281534.81704254-201903281534.81704254-201903281534.81704254</td>
</tr>
<tr>
<td>salt-formula-apache</td>
<td>0.2+201903280900.00000000-201903280900.00000000-201903280900.00000000</td>
</tr>
<tr>
<td>salt-formula-barbican</td>
<td>2018.1+201903281534.81704254-201903281534.81704254-201903281534.81704254</td>
</tr>
<tr>
<td>salt-formula-ceilometer</td>
<td>2016.12.1+2018122111452255-201903281534.81704254-201903281534.81704254</td>
</tr>
<tr>
<td>salt-formula-ceph</td>
<td>0.1+201903271759.65904599-201903271759.65904599-201903271759.65904599</td>
</tr>
</tbody>
</table>

©2020, Mirantis Inc.
<table>
<thead>
<tr>
<th>Package Name</th>
<th>Version</th>
<th>Last Updated</th>
<th>Hash ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>salt-formula-cinder</td>
<td>2016.12.1+2019032911</td>
<td>2019041017 20190522 058.690c239</td>
<td>b760fa3f77ebc0b2d8a2e7530405554</td>
</tr>
<tr>
<td>salt-formula-designate</td>
<td>2016.12.1+2018122115</td>
<td>2019040617</td>
<td>2014f8868db61e6c3f4f62d</td>
</tr>
<tr>
<td>salt-formula-docker</td>
<td>0.1+201903271546.64</td>
<td>20190217 11725 b72da1c        xeni</td>
<td></td>
</tr>
<tr>
<td>salt-formula-elasticsearch</td>
<td>0.2+201812131536.69</td>
<td>20190624 0959.94             xeni</td>
<td></td>
</tr>
<tr>
<td>salt-formula-fluentd</td>
<td>0.1+201811261322.27</td>
<td>20190513 31626 b5531708      xeni</td>
<td></td>
</tr>
<tr>
<td>salt-formula-gerrit</td>
<td>2017.2+20181220172</td>
<td>20190521 208025 0525c11      xeni</td>
<td></td>
</tr>
<tr>
<td>salt-formula-glance</td>
<td>2016.12.1+2019042514</td>
<td>201905111246 ed99e33         xeni</td>
<td></td>
</tr>
<tr>
<td>salt-formula-glusterfs</td>
<td>2017.3+201812211714</td>
<td>201905111341 b8054b0        xeni</td>
<td></td>
</tr>
<tr>
<td>salt-formula-gnocchi</td>
<td>2018.1+201812171745</td>
<td>20190521 2040806 d51fa27     xeni</td>
<td></td>
</tr>
<tr>
<td>salt-formula-grafana</td>
<td>0.1+201903291208 ea37f1    201906281140 b39c951       xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-haproxy</td>
<td>0.2+201903291617 e156c8b 2019063210701.8033bf0 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-heat</td>
<td>2016.12.1+20190328152           201905222032.5358e48    xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-horizon</td>
<td>2016.12.1+20190326112085582 ee201905280832.59bfec xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-ironic</td>
<td>0.1+201901091031.08665f201808231618b711aa xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-jenkins</td>
<td>2017.8+201812261202 20190617 201905111005 e7925af xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-keystone</td>
<td>2016.12.1+2019042514             20190521148 ef7061b1 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-kibana</td>
<td>0.2+201812010352.9162102086210700.65869f xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-kubernetes</td>
<td>2016.12.1+201904150981649762201905161140 a08fe43 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-linux</td>
<td>2017.4.1+2019040413 o80017431 20190281653 c37c8a4xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-manila</td>
<td>2017.6+201903281526 d3ef254201906141153 7df23f4 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-neutron</td>
<td>2016.12.1+2019042514 0008920 20190516136130 000e27 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-nginx</td>
<td>0.2+201903221825.0008920 20190516136130 000e27 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-nova</td>
<td>2016.12.1+2019042514             20190515081512 acb347xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-octavia</td>
<td>2017.6+201904231159 2017062109081281144 09c4ac6 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-opencontrail</td>
<td>0.2+201904171048 2019081261026.26 cf840 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-openssh</td>
<td>0.2+201904150940.36 2019081261452.3cf4cc7 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-oslo-tempest</td>
<td>2018.1+201903281325 20180313020490512000 3db8426 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-panko</td>
<td>2017.6+201812141859 201905241116 68551a1 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-prometheus</td>
<td>0.1+201903271541.65b20190321548.8 b291d2b xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-rabbitmq</td>
<td>0.2+201903281326.4b 201909222031.efe0645 xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-runtest</td>
<td>0.1+201904171302.55f9ba7 201904701047 74ba68b xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-telegraf</td>
<td>0.1+201903221357.5fd1e7 2019036131005.8ae18ef xeni</td>
<td></td>
<td></td>
</tr>
<tr>
<td>salt-formula-xtrabackup</td>
<td>0.2+201904051040.e940d72090640954.38 bd119 xeni</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Extra packages

<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>atop</td>
<td>n/a</td>
</tr>
<tr>
<td>jmx-exporter</td>
<td>1:0.9-2~u16.04+mcp2</td>
</tr>
<tr>
<td>jmx-exporter</td>
<td>12:0.3.2.2~u16.04+mcp3</td>
</tr>
<tr>
<td>libvirt-exporter</td>
<td>0.1-1~u16.04+mcp0</td>
</tr>
<tr>
<td>libvirt-exporter</td>
<td>0.1-1~u16.04+mcp1</td>
</tr>
<tr>
<td>td-agent-additional-plug</td>
<td>1.3-1~u16.04+mcp2</td>
</tr>
<tr>
<td>td-agent-additional-plug</td>
<td>3.1.5-1~u16.04+mcp1</td>
</tr>
<tr>
<td>telegraf</td>
<td>1:1.9.1.1-~u16.04+mcp3</td>
</tr>
<tr>
<td>telegraf</td>
<td>3:1.9.1.3-~u16.04+mcp44</td>
</tr>
<tr>
<td>telegraf-builddeeps</td>
<td>0.0+git20181221-1</td>
</tr>
<tr>
<td>telegraf-builddeeps</td>
<td>0.0+git20190613-1</td>
</tr>
<tr>
<td>xccdf-benchmarks</td>
<td>0.5.5-1~u16.04+mcp1</td>
</tr>
<tr>
<td>xccdf-benchmarks</td>
<td>1.0.2-1~u16.04+mcp1</td>
</tr>
</tbody>
</table>

**Note**


### Updated Kubernetes components

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.3</th>
<th>2019.2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kubernetes</td>
<td>containernetworking-plugins</td>
<td>0.8.0-7-g70fb96e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>external-dns</td>
<td>0.5.11-4</td>
<td>0.5.14-5</td>
</tr>
<tr>
<td></td>
<td>hyperkube</td>
<td>1.13.5-3-15537340307</td>
<td>1.13.6-4</td>
</tr>
<tr>
<td></td>
<td>hyperkube-amd64</td>
<td>1.13.5-3</td>
<td>1.13.6-4</td>
</tr>
<tr>
<td></td>
<td>nginx-ingress-controller-amd64</td>
<td>0.23.0-4</td>
<td>nginx-0.24.1-5</td>
</tr>
<tr>
<td></td>
<td>pause-amd64</td>
<td>1.13.5-3</td>
<td>1.13.6-4</td>
</tr>
</tbody>
</table>

### Apply maintenance updates

**Caution!**

If you are updating from MCP 2019.2.3 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.3, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

**Update procedure workflow**
<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DriveTrain</td>
<td>1. Update DriveTrain to a minor release version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform the steps described in Issues resolutions requiring manual application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Optional. Recommended. Remove anonymous access for Jenkins on the Salt Master node.</td>
</tr>
<tr>
<td>2</td>
<td>OpenContrail</td>
<td>1. Update the OpenContrail packages as described in Update the OpenContrail 4.x nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Optional. Define aging time for flow records.</td>
</tr>
<tr>
<td>3</td>
<td>OpenStack</td>
<td>1. Update the OpenStack packages as described in Update OpenStack packages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform the steps described in Issues resolutions requiring manual application.</td>
</tr>
<tr>
<td>3.1</td>
<td>Galera cluster</td>
<td>Update the Galera cluster as described in Update Galera.</td>
</tr>
<tr>
<td>3.2</td>
<td>RabbitMQ</td>
<td>Update the RabbitMQ component as described in Update RabbitMQ.</td>
</tr>
<tr>
<td>4</td>
<td>Kubernetes</td>
<td>Update the Kubernetes packages as described in Update or upgrade Kubernetes.</td>
</tr>
<tr>
<td>5</td>
<td>StackLight LMA</td>
<td>1. Update StackLight LMA using the Deploy - upgrade StackLight Jenkins pipeline job as described in Update StackLight LMA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enable CADF notifications handled by Fluentd.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Perform the steps described in Issues resolutions requiring manual application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enable Prometheus Elasticsearch exporter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Optional. Enable TLS for StackLight LMA.</td>
</tr>
<tr>
<td>6</td>
<td>Ceph</td>
<td>1. Update the Ceph packages as described in Update Ceph packages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Perform the steps described in Issues resolutions requiring manual application.</td>
</tr>
</tbody>
</table>
2019.2.3

The MCP 2019.2.3 update introduces enhancements and bug fixes for DriveTrain, OpenStack, Kubernetes, OpenContrail, Ceph, and StackLight MCP components. The MCP 2019.2.3 update is available starting from April, 26.

Enhancements

In the MCP 2019.2.3 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version:

DriveTrain

In the MCP 2019.2.3 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Ubuntu security updates
- CVP Shaker

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Ubuntu security updates

Published the following Ubuntu 16.04 LTS security updates:

- USN-3855-1 systemd vulnerabilities
- USN-3858-1 HAProxy vulnerabilities
- USN-3871-4 Linux kernel (HWE) vulnerabilities
- USN-3875-1 OpenJDK vulnerability

CVP Shaker

Implemented the CVP Shaker test suite allowing for automatic verification and performance measurement of the data plane networking of an MCP OpenStack deployment. CVP Shaker is based on Shaker that is a wrapper around popular system network testing tools such as iperf, iperf3, and netperf.
OpenStack

In the MCP 2019.2.3 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- **FQDN on internal endpoints in the Keystone catalog**
- **Exposition of RNG devices to Nova instances**

To obtain the enhancements, follow the steps described in *Apply maintenance updates*.

---

**FQDN on internal endpoints in the Keystone catalog**

Enforced the FQDN usage and prevented IP address usage in the Keystone service catalog.

In security-sensitive environments, a cluster internal IP address exposure is considered a security vulnerability. Therefore, rather than using service IP addresses within service catalog, we recommend that all existing MCP OpenStack deployments migrate from the IPv4-based Keystone service catalog to fully FQDN-based service catalog.

In the new MCP 2019.2.3 deployments, the OpenStack environments use FQDN on the internal endpoints in the Keystone catalog by default.

---

**Exposition of RNG devices to Nova instances**

Implemented the possibility to expose hardware Random Number Generator (HRNG) source to the OpenStack compute nodes enabling the OpenStack instances to consume HRNG from a physical machine.
Kubernetes

In the MCP 2019.2.3 maintenance update, Mirantis introduces the following enhancements for Kubernetes:

- Kubernetes 1.13.5 support
- Virtlet 1.5.0 support
- Helm package manager support
- Upgrade of etcd with no workload downtime

Kubernetes 1.13.5 support
Added support for the community Kubernetes version 1.13.5 that includes latest enhancements and bug fixes.

Virtlet 1.5.0 support
Updated Virtlet to version 1.5.0 that contains the following improvements:

- Added the possibility to specify stable System Management BIOS (SMBIOS) UUIDs
- Implemented the usage of minimal libguestfs bindings to prevent potential licensing issues
- Updated the Kubernetes-in-Kubernetes example
- Fixed the issue with file injection with multiple partitions
- Fixed the tap MTU setting
- Introduced the virtletctl validate command
- Fixed handling of a container startup failure
- Fixed the issue with the 9pfs hostPath mounts
- Updated the apparmor libvirt profile
- Fixed the network namespace handling in case of a VM failure
- Fixed the issue with active VMs being killed by a container during a Virtlet pod restart
- Added support for Kubernetes 1.13.5
- Implemented the `VirtletForceDHCPNetworkConfig` parameter to use, for example, for a Debian OpenStack image

**Learn more**
- Virtlet release notes
- Virtlet official documentation

---

**Helm package manager support**

Integrated Helm package manager into Kubernetes. Helm allows you to configure, package, and deploy applications on a Kubernetes cluster using charts packages.

**Learn more**

MCP Deployment Guide: Enable Helm support

---

**Upgrade of etcd with no workload downtime**

Implemented automatic upgrade of the etcd cluster to both major and minor versions that does not affect workloads. The etcd upgrade options are included to the Deploy - update Kubernetes cluster Jenkins pipeline job.

**Learn more**

MCP Operations Guide: Update or upgrade Kubernetes

---

StackLight
In the MCP 2019.2.3 maintenance update, Mirantis introduces the following enhancements for StackLight LMA:

- Open vSwitch monitoring
- SSL certificates monitoring
- Salesforce notifier improvement
- SMART disks monitoring

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Open vSwitch monitoring
Enhanced StackLight LMA to monitor the Neutron Open vSwitch (OVS) memory usage across nodes and raise an alert if the memory consumption of an OVS process exceeds the predefined thresholds, by default set to 20% and 30%.

Learn more
- MCP Operations Guide: Available StackLight LMA alerts

SSL certificates monitoring
Enhanced StackLight LMA to monitor SSL certificates and raise an alert when a certificate is due to expire to allow for generating a new certificate or replacing the existing one on time. By default, the alerts raise if a certificate expires less than in 60 and 30 days.

Learn more
- MCP Operations Guide: Available StackLight LMA alerts

Salesforce notifier improvement
Improved the Salesforce notifier service to properly handle the Salesforce requests timeouts.
Learn more

- MCP Reference Architecture: StackLight LMA components
- MCP Operations Guide: Enable Salesforce notifications through Alertmanager

SMART disks monitoring
Enhanced StackLight LMA to monitor physical disks that support Self-Monitoring, Analysis and Reporting Technology (SMART) and raise alerts if disk errors occur. By default, all disks on the bare metal servers are scanned.

Learn more

- MCP Operations Guide: Available StackLight LMA alerts

Ceph
In the MCP 2019.2.3 maintenance update, Mirantis introduces the following enhancements for Ceph:

- Ceph packages update
- Ceph performance alerts
- Pipeline jobs improvements

To obtain the enhancements, follow the steps described in Apply maintenance updates.

Ceph packages update
Updated the Ceph Luminous packages to 12.2.11.

Ceph performance alerts
TECHNICAL PREVIEW
Improved Ceph performance monitoring by implementing new Ceph prediction alerts. The new alerts include prediction of the IOPS consumption per OSD and pool, available RAM on the Ceph nodes, OSD disks responsiveness based on the write and read latency in a defined time range, as well as prediction whether a pool can consume all available capacity in a defined time range.
You can enable Ceph prediction only if you have previously enabled the Ceph Prometheus plugin as described in MCP Operations Guide: Enable the Ceph Prometheus plugin.

Learn more

- MCP Operations Guide: Available StackLight LMA alerts

Pipeline jobs improvements

Improved the Add a Ceph OSD node and Ceph - replace failed OSD Jenkins pipeline jobs by integrating the upmap mechanism to fine control the placement group (PG) mapping, as well as by integrating the balancer plugin to provide for better control while adding new Ceph OSD nodes or replacing a failed Ceph OSD node.

To obtain the pipeline jobs improvements:

1. On the cluster level of the Reclass model, add the following class in classes/cluster/CLUSTER_NAME/cicd/control/leader.yml to add the upmap-based pipeline job:

   ```yaml
   classes:
   - system.jenkins.client.job.ceph.add-osd-upmap
   ```

2. (Optional) If you have used the Add a Ceph OSD node Jenkins pipeline job:
   1. Remove the system.jenkins.client.job.ceph.add-osd class from the same file.
   2. Remove the old Jenkins pipeline job from the Jenkins web UI.
   3. Apply the jenkins.client state on the cid01 node:

   ```
   salt cid01\* state.sls jenkins.client
   ```

4. Verify that the Ceph - Add OSD pipeline job is available in the Jenkins web UI.

Learn more

- MCP Operations Guide: Replace a failed Ceph OSD
- MCP Operations Guide: Add a Ceph OSD node

MCP documentation
In the MCP 2019.2.3 maintenance update, Mirantis introduces the following enhancements for MCP documentation on top of continuous improvements delivered to the existing MCP guides:

- MCP Reference Architecture
- Manage RabbitMQ nodes

MCP Reference Architecture
Updated the MCP Reference Architecture by describing capabilities provided by the Cloud Provider infrastructure (CPI) as well as its structure and the most important configurations of services, physical infrastructure, and limitations of the architecture.

Learn more
MCP Reference Architecture

Manage RabbitMQ nodes
Extended MCP Operations Guide with the Manage RabbitMQ nodes section that describes how to safely manage a RabbitMQ cluster, which is sensitive to external factors like network throughput and traffic spikes. The section contains three subsections:

- Restart a single RabbitMQ node
- Restart the whole RabbitMQ cluster
- Restart a RabbitMQ cluster with clearing the Mnesia database

Learn more
MCP Operations Guide: Manage RabbitMQ nodes

Addressed issues
The MCP 2019.2.3 update contains fixes for several MCP components.

DriveTrain

- [28868] Fixed the issue with the CVP - Sanity checks Jenkins pipeline job failing during the test_drivetrain check if drivetrain_version was defined for tests.
• [26431] Fixed the issue with the false negative results of the test_check_services check for the kvm nodes.
• [27384] Fixed the issue with the host-based LDAP authentication not working.
• [28587] Fixed the issue with improper operation of git submodule update during the upgrade of an MCP cluster using the Deploy - upgrade MCP DriveTrain pipeline job.
• [26381] Fixed the issue with the Deploy - upgrade MCP DriveTrain pipeline job failing with the Uncaught Pepper error (increase verbosity for the full traceback) error message.
• [27237] Updated jenkins-master to version 2.150.3 to obtain the latest security fixes.
• [27135] Fixed the permissions issue that caused failure to create instant backups using Backupninja, Xtrabackup, Zookeeper, or Cassandra.
• [26609] Fixed the time synchronization issue in the Verify and Restore Galera cluster pipeline.
• [26997] Fixed the issue with the Deploy - OpenStack pipeline job failing in case if the ASK_ON_ERROR parameter was selected.
• [26113] Fixed the issue with the deployment of OpenContrail v4.x with OpenStack Pike occasionally failing due to the duplication of the salt-minion services.
• [26626] Fixed the issue with reload of the Docker service configuration through docker:host:options.

OpenStack

Issues resolutions applied automatically

• [26315] [Pike] Fixed the community issue that prevented the migration of any old instance after renaming the availability zones through the Horizon web UI. Now, it is not possible to rename a non-empty availability zone.
• [26552] [Queens] Fixed the issue with inability to edit an image through the Horizon web UI.
• [24809] [Pike, Queens] Added support for the CSRF_COOKIE_HTTPONLY option to fix the issues in the Launch instance menu and the Warning: Policy check failed. errors in the Compute -> Images menu of the Horizon web UI.
• [27459] [Pike, Queens] Added support for the PASSWORD_VALIDATOR setting in the Horizon web UI to prevent creation of weak passwords.
• [28185] [Pike, Queens] Fixed the issue with python-glanceclient failing to use the OS_CACERT environment variable.
• [28255] [Queens] Fixed the issue with inability to modify the Nova disk_allocation_ratio parameter.
• [28184] [Pike] Fixed the issue with self-signed certificates validation failure when using Glance with the Swift back end and SSL enabled.
• [26945] [Pike] Fixed the issue in cinder.conf breaking the scheduling logic for the OpenStack volumes.
• [25985] [Queens] Added support for the Cinder and Nova [service_user] options to avoid the token expiration for long-running operations.

• [23600] [Pike, Queens] Fixed the configuration issue in CIS 5.4.1.4. Four scored items of CIS 5.4.1 are now fully available.

• [25643] [Pike, Queens] Fixed the Salt formula configuration issue affecting the MCP OpenStack environments with Ironic and StackLight. On the OpenStack environments with Ironic, VMware and some other services that do not require libvirt are running on the local compute node. Therefore, the Prometheus libvirt metrics collection was disabled for the OpenStack compute nodes with Ironic.

• [28345] [Pike, Queens] Fixed the issue causing Open vSwitch flows loss after the restart of neutron-ovs-agent.

• [29543] [Pike, Queens] Updated Open vSwitch to version 2.8.4 for OpenStack Pike and 2.9.0 for OpenStack Queens to fix the OVS memory leak issue.

• [28349] [Queens] Fixed the community issue that caused inability to obtain the DHCP address after resizing or cold-migrating the guest VM with a specific port type.

• [28029] [Pike, Queens] Fixed the issue with the openstack usage list command showing an incomplete list of projects in the output.

• [27129] [Pike, Queens] Fixed the issue with failure to update the resources for a node and displaying the DiskNotFound error message.

• [27269] [Queens] Fixed the community issue that caused inability to obtain the DHCP address after resizing or cold-migrating the guest VM with a specific port type.

• [27890] [Pike, Queens] Fixed the issue in Keystone that caused the Deploy - cloud update pipeline job to fail during the upgrade of the ctl nodes.

• [27270] [Pike, Queens] Fixed the issue with the nova-status upgrade check command using a public endpoint regardless of the interface type defined in the placement section of nova.conf.

• [25486] [Pike, Queens] Fixed the issue in the Heat formula that caused inability to update Reclass with a custom name for the Heat user and a domain name to use as a trusted domain.

• [28006] [Queens] Fixed the issue with the flavor details pop-up menu in the Project -> Compute -> Instances menu of the Horizon web UI. Now, the pop-up menu appears once you move the cursor over the flavor value.

• [26269] [Queens] Fixed the issue with failure to change the logging level for the OpenStack services.

• [CVE-2018-1000807] [CVE-2018-1000808] [Pike] Updated the pyopenssl and dependent packages to fix security vulnerabilities. For the details, see the corresponding GitHub pyopenssl issue.

• [27985] [Pike] Fixed the issue with the volume availability zones not matching the back-end availability zones after migration or retype.

• [25448] [Pike, Queens] Fixed the issue with inability to modify the Cinder iscsi_helper value. Now, you can define the iscsi_helper and scheduler_default_filters parameters.
• [27663] [Pike, Queens] Fixed the issue with inability to set password_regex and password_regex_description in the security_compliance section of keystone.conf.

• [27457] [Pike, Queens] Added support for the SSH host key checking to prevent insecure SSH configurations.

• [27864] [Pike] Fixed the issue with the Nova user tokens configuration causing failure of the Tempest tests.

• [26861] [Pike, Queens] Fixed the issue with the nova.controller state executing cells-related actions even with the test=true setting.

• [26960] [Pike, Queens] Fixed the issue with Memcached objects being created with infinite TTL to prevent excessive memory evictions of the Memcached service.

• [26891] [Pike, Queens] Implemented rate limiting for HAProxy to prevent excessive requests.

• [26294] [Pike, Queens] Decreased the database connection idle_timeout/connection_recycle_time that caused Cinder to randomly print INFO messages containing the Error word in the log file.

• [29692] [Queens] Fixed the idempotency issue with keystone manage-bootstrap in the Keystone Salt formula that could cause errors when applying the keystone state after upgrade to OpenStack Queens.

Issues resolutions requiring manual application

---

Note
Before proceeding with the manual steps below, verify that you have performed the steps described in Apply maintenance updates.

---

• [29219] Display metric graphs for Cinder in the Grafana web UI
• [26565] Resolve the gnocchi.client.resources.v1 state failure
• [28559] Insufficient OVS timeouts causing instance traffic losses

---

[29219] Display metric graphs for Cinder in the Grafana web UI

Pike, Queens

Fixed the issue with the Cinder Grafana dashboard displaying no data for the OpenStack Pike or Queens environments. The issue affected the OpenStack environments deployed with TLS on the internal endpoints.

To display metric graphs for Cinder in the Grafana web UI:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `classes/cluster/<cluster_name>/openstack/control.yml`, remove the `osapi` and `host` parameters in the `cinder:controller` block.

   For example:

   ```yaml
   cinder:
     controller:
       enabled: true
       osapi:
         host: 127.0.0.1
   ```

   Eventually, the `cinder:controller` block should look like this:

   ```yaml
   cinder:
     controller:
       enabled: true
   ```

3. Log in to the Salt Master node.

4. Refresh the pillars:

   ```bash
   salt "*" saltutil.refresh_pillar
   salt "*" state.sls salt.minion.grains
   salt "*" mine.update
   ```

5. Apply the `telegraf` and `cinder` states on all OpenStack controller nodes:

   ```bash
   salt -C "I@cinder:controller" state.sls telegraf,cinder
   ```

6. In `classes/cluster/<cluster_name>/openstack/control.yml`, add the following configuration after the line `apache_nova_placement_api_address: ${_param:cluster_local_address}`:

   ```yaml
   apache_cinder_api_address: ${_param:cluster_local_address}
   ```

7. Refresh the pillars and apply the `apache` state:

   ```bash
   salt -C "I@cinder:controller" saltutil.pillar_refresh
   salt -C "I@cinder:controller" state.sls apache
   ```

[26565] Resolve the `gnocchi.client.resources.v1` state failure

Queens

Fixed the issue that caused the `gnocchi.client.resources.v1` state failure on the OpenStack Queens environments with SSL and Barbican. The resolution includes fixes of the alternative names for Barbican and certificate alternative names for FQDN endpoints.
To resolve the `gnocchi.client.resources.v1` state failure:

1. Log in to the Salt Master node.
2. Apply the Salt formula **patch 36685** to your Reclass model.
3. Refresh the pillars:
   ```
salt '*' saltutil.refresh_pillar
salt '*' state.sls salt.minion.grains
salt '*' mine.update
   ```
4. Apply `salt.minion.cert` and restart `apache2`:
   ```
salt -C 'I@barbican:server' state.apply salt:minion:cert
salt -C 'I@barbican:server' cmd.run 'systemctl restart apache2' -b 1
   ```
5. Apply the Salt formula **patch 36686** to your Cookiecutter templates.
6. Refresh the pillars:
   ```
salt '*' saltutil.refresh_pillar
salt '*' state.sls salt.minion.grains
salt '*' mine.update
   ```
7. Apply `salt.minion.cert` and restart `apache2`:
   ```
salt -C 'I@gnocchi:server' state.apply salt:minion:cert
salt -C 'I@gnocchi:server' cmd.run 'systemctl restart apache2' -b 1
   ```

---

### [28559] Insufficient OVS timeouts causing instance traffic losses

**Pike, Queens**

Fixed the issue with insufficient OVS timeouts causing instance traffic losses. Now, if you receive the OVS timeout errors in the neutron-openvswitch-agent logs, such as `ofctl request <...> timed out: Timeout: 10 seconds` or `Commands [<ovsdbap...>] exceeded timeout 10 seconds`, you can configure the OVS timeout parameters as required depending on the number of the OVS ports on the gtw in your cloud. For example, if you have more than 1000 ports per a gtw node, Mirantis recommends changing the OVS timeouts as described below. The same procedure can be applied to the compute nodes if required.

To increase OVS timeouts on the gateway nodes:

1. Log in to the Salt Master node.
2. Open `/srv/salt/reclass/classes/cluster/<cluster_name>/openstack/gateway.yml` for editing.
3. Add the following snippet to the parameters section of the file with the required values.
neutron:
gateway:
  of_connect_timeout: 60
  of_request_timeout: 30
  ovs_vsctl_timeout: 30  # Pike
  ovsdb_timeout: 30  # Queens and beyond

4. Apply the following state:

```
salt -C 'I@neutron:gateway' state.sls neutron
```

5. Verify whether the Open vSwitch logs contain the Datapath Invalid and no response to inactivity probe errors:

- In the neutron-openvswitch-agent logs, for example:

```
ERROR ... ofctl request <...> error Datapath Invalid 64183592930369: 
InvalidDatapath: Datapath Invalid 64183592930369
```

- In openvswitch/ovs-vswitchd.log, for example:

```
ERR|br-tun<->tcp:127.0.0.1:6633: no response to inactivity probe 
after 5 seconds, disconnecting
```

If the logs contain such errors, increase inactivity probes for the OVS bridge controllers:

1. Log in to any gtw node.
2. Run the following commands:

   ```
   ovs-vsctl set controller br-int inactivity_probe=60000
   ovs-vsctl set controller br-tun inactivity_probe=60000
   ovs-vsctl set controller br-floating inactivity_probe=60000
   ```

To increase OVS timeouts on the compute nodes:

1. Log in to the Salt Master node.
2. Open `/srv/salt/reclass/classes/cluster/<cluster_name>/openstack/compute.yml` for editing.
3. Add the following snippet to the parameters section of the file with the required values.

```
neutron:
  compute:
    of_connect_timeout: 60
    of_request_timeout: 30
    ovs_vsctl_timeout: 30  # Pike
    ovsdb_timeout: 30  # Queens and beyond
```
4. Apply the following state:

```
salt -C 'I@neutron:compute' state.sls neutron
```

5. Verify whether the Open vSwitch logs contain the Datapath Invalid and no response to inactivity probe errors:

- In the neutron-openvswitch-agent logs, for example:

```
ERROR ... ofctl request <...> error Datapath Invalid 64183592930369: 
InvalidDatapath: Datapath Invalid 64183592930369
```

- In openvswitch/ovs-vswitchd.log, for example:

```
ERR|br-tun<->tcp:127.0.0.1:6633: no response to inactivity probe 
after 5 seconds, disconnecting
```

If the logs contain such errors, increase inactivity probes for the OVS bridge controllers:

1. Log in to the target cmp node.
2. Run the following commands:

```
ovs-vsctl set controller br-int inactivity_probe=60000
ovs-vsctl set controller br-tun inactivity_probe=60000
ovs-vsctl set controller br-floating inactivity_probe=60000
```

Kubernetes

- [27634] Fixed the issue with active VMs being killed by a container during a Virtlet pod restart.
- [28450] Fixed the issue with runc using more memory during a container startup. For details, see the corresponding GitHub issue.
- [28979] Added separate stages for runConformance in the Deploy - update Kubernetes cluster pipeline job to prevent the runConformance failures during the pipeline job execution.
- [28976] Fixed the issue with a Kubernetes Node being uncordoned during a reboot.
- [26881] Renamed the targetHosts parameter for etcd to targetHostsEtcd to prevent the Deploy - update Kubernetes cluster pipeline job from failing with the The current scope already contains a variable of the name targetHosts error.
- [27425] Changed the CRI Proxy logging storage from /tmp to journald to prevent CRI and kubelet failures once /tmp is out of space.
- [27534] Adjusted the logic for the Kubernetes namespaces to fix the namespaces creation and removal errors.
• [27977] Implemented the installKubernetesClient function that is designed to install the Kubernetes resources to fix the issue with an MCP Kubernetes cluster deployment failure due to labels assigned to compute nodes.

• [28730] Fixed the issue with containerd installation failure caused by the absent configuration directory for the containerd config.toml.

• [28767] Fixed the issue with the etcd upgrade failure due to the tmp etcd directory not being cleared after the etcd installation. Added the default overwrite: true parameter to the extract_etcd section of etcd/server/service.sls in the etcd Salt formula.

• [28771] Added the missing etcd v3 configenv to /var/lib/etcd/. Previously, configenv could be used only for v2 and variables for v3 must have been created manually.

• [28953] Fixed the issue with the CNI plugins not being upgraded during the execution of the Deploy - update Kubernetes cluster pipeline job. The issue occurred because Salt formula verified only the presence of the CNI plugins installation files and not their versions. The fix adds overwrite: true to the /opt/cni/bin:archive.extracted: section of kubernetes/_common.sls in the Kubernetes Salt formula.

• [28975] Fixed the incorrect logic of the Deploy - update Kubernetes cluster pipeline job that used grep with nodeShortName for verifying the nodes statuses. This logic caused an incorrect of the nodes for clusters containing more than 10 compute nodes. For example, not only cmp1 was selected but any other cmp1X nodes such as cmp10, cmp11 are selected as well.

OpenContrail

Issues resolutions applied automatically

• [24522] Fixed the issue with multiple contrail-api workers causing newly created OpenStack projects to be invisible in the OpenContrail web UI. Changed the default number of the contrail-api workers to be used in OpenContrail from one to six.

• [25264] Fixed the issue with contrail-control being inactive on all ntw nodes after restoring the Zookeeper database for OpenContrail 4.x due to an issue with permissions for certificates.

• [27062] Fixed the issue with the inability to downgrade the python-contrail package on the OpenContrail controller nodes during the upgrade rollback of OpenContrail from version 4.1 to 3.2.

• [27225] Fixed the issue with Neutron displaying next_hop incorrectly through the Neutron client if a route table is created using the OpenContrail web UI.

• [27413] Fixed the issue with the Zookeeper - restore pipeline job not supporting the containerized versions of OpenContrail.

• [27603] Fixed the incorrect default configuration of the ZooKeeper crontab backup schedule set to run every two minutes from 2 to 3 a.m. Changed the default ZooKeeper backup cron configuration from True to False in the ZooKeeper Salt formula since this option must be configured and controlled by a cloud operator using the Relcass cluster model.
• [28174] Fixed the logic for the OpenContrail services in the backup state to prevent the contrail-schema, contrail-svc-monitor, and contrail-device-manager services from being stuck in the initializing state after the OpenContrail 4.x deployment on the Queens-based OpenStack clusters.

• [28203] Fixed the issue with Tempest failing to establish the SSH connection to a VM through the floating IP due to the Nova metadata service being unreachable on the Queens-based OpenStack clusters with OpenContrail 4.x.

• [25629] Removed option noligner from the HAProxy Salt formula for OpenContrail to fix the issue with the Setting -> Config Editor OpenContrail web UI tab that previously raised [SyntaxError: Failed to parse JSON body: Unexpected end of input] in logs.

Issues resolutions requiring manual application

[27450] Fixed the issue with the Boost UDP resolver overriding the default DNS server list for vRouter using the etc/resolve.conf file on a dedicated OpenStack compute node. Now, using the new resolv_conf_file option, you can specify a file that contains a list of DNS nameserver that contrail-vrouter-agent will use as a non-default source of custom nameservers. For details, see: MCP Operations Guide: Override the default DNS server list for vRouter.

StackLight

• [28352] Improved the Messages panel of the RabbitMQ Grafana dashboard to display absolute values instead of rates.

• [28066] Fixed the issue with the Host API Status graph being unavailable in the Cinder Grafana dashboard.

• [26450] Fixed the Apache meta for Telegraf to use the parameters from server.mods.status instead of apache:server:bind.

• [28123] Fixed the issue with the absent() function causing malfunction of the Ceph Grafana dashboards in case if one of the Prometheus servers had no data for a particular period of time.

• [27250] Added support for the containerd log format to fix the issue with the inability to parse the Kubernetes container logs.

• [27142] Fixed the discrepancy in RAM usage data between the Horizon web UI and the Nova - utilization dashboard in Grafana.

• [26918] Fixed the issue with the false negative http_response_status metric for the Aodh URL by adding support for the HTTP response code 200 for the Aodh checks in OpenStack version Pike and newer.

• [27982] Fixed the issue with the Apache Grafana dashboard incorrectly displaying a high percentage (thousands of percents) in the CPU Load panel for the ctl nodes.

• [27474] Removed the non-valuable ContrailFlow* alerts to prevent the false positive raising of such alerts.

• [27342] Adjusted the NginxServiceDown alert by adding the for: 1m variable to prevent raise of false positive alerts for the NGINX service being down.
• [27298] Fixed the issue with the inability to resolve the PacketsDroppedByCpuMajor alert in a time frame of less than 24 hours.

• [26842] Updated the monitoring interval in Telegraf to 40 seconds for Ceph Jewel to prevent timeouts in Telegraf while gathering the data.

• [24810] Improved regexp for the HDD metrics to prevent generation of false positive for HDD errors.

• [26116] Added the Fluentd label for Telegraf to fix the issues with processing severity of the Telegraf logs.

Ceph

Issues resolutions applied automatically

• [23318] Fixed the issue with failure to upload a file to the object storage, which occurred after upgrading the Ceph cluster from Jewel to Luminous using the Ceph - upgrade Jenkins pipeline job.

• [27589] Fixed the issue with the existing Ceph Monitor and Ceph OSD occasionally not functioning while adding a new Ceph OSD node.

• [25480] Fixed the issue with the duplication of parameters that define the Ceph OSD nodes count in the Cookiecutter context. Now, only ceph_osd_node_count is used.

Issues resolutions requiring manual application

[26452] Fixed the issue with multitenancy support for the Swift containers in Ceph, which affected the containers availability. For the existing MCP deployments, perform the steps below to obtain the fix. The fix will be available only for the newly created tenants.

To fix the containers availability:

1. Log in to the Salt Master node.

2. Apply the ceph.common state on the Ceph nodes:

```bash
salt -C "@ceph:common" state.sls ceph.common
```

3. Restart the Ceph Monitor services on the cmn nodes one by one. Wait for the HEALTH_OK status after each Ceph Monitor restart.

```bash
salt -C NODE_NAME cmd.run 'systemctl restart ceph-mon.target'
salt -C NODE_NAME cmd.run 'systemctl restart ceph-mgr.target'
salt -C NODE_NAME cmd.run 'ceph -s'
```
4. Restart the RADOS Gateway services on the rgw nodes one by one:

   salt -C NODE_NAME cmd.run 'systemctl restart ceph-radosgw.target'

5. Apply the keystone.client state and update the Swift endpoint:

   salt -C "I@keystone:client and *01*" state.sls keystone.client

**Known issues**

This section lists the MCP 2019.2.3 known issues and workarounds.

- [29798] Services verification fails during the OpenStack control plane update
- [29849] OpenContrail fails to create network objects
- [29809] OpenContrail states fail on the OpenStack compute nodes
- [29843] Pike to Queens upgrade fails for the OpenStack deployments with Octavia
- [29844] OpenStack with Octavia update fails due to a missing CA certificate
- [29812] The OpenContrail web UI service fails to start after update

**[29798] Services verification fails during the OpenStack control plane update**

*Fixed in 2019.2.4, OPENSTACK VCP UPDATE, QUEENS, PIKE*

During the update of the OpenStack control plane of an MCP OpenStack deployment, the verification of some services may fail due to the race condition. The list of the affected services include Aodh, Barbican, Designate, Glance, Gnocchi, Heat, Ironic, Manila, Nova, Octavia, and Panko.

The workaround is to retry the last stage of the Deploy - upgrade control VMs Jenkins pipeline job.

**[29849] OpenContrail fails to create network objects**

*Fixed in 2019.2.4, OPENSTACK WITH OPENCONTRAIL, UPDATE*

After the update of OpenContrail 4.x in the MCP OpenStack deployments, if SSL is enabled on the Keystone internal endpoints, the network objects such as networks, subnets, and others, may not be created.

To verify whether your OpenStack deployment is affected:

1. Open /etc/contrail/vnc_api_lib.ini.
2. Verify that the insecure parameter in the auth section is set to true:

   ```
   insecure = true
   ```
If the insecure parameter is not set, proceed with the workaround.
Workaround:

1. Log in to the Salt Master node.
2. Set the insecure parameter to true in the /etc/contrail/vnc_api_lib.ini file:

   ```bash
   salt -C 'I@opencontrail:control' cmd.run "sed -i '/^AUTHN_URL.*/a insecure = true' /etc/contrail/vnc_api_lib.ini"
   ```
3. Restart all contrail-api workers:

   ```bash
   salt -C 'I@opencontrail:control' cmd.run "doctrail controller service contrail-api* restart"
   ```

[29809] OpenContrail states fail on the OpenStack compute nodes
Fixed in 2019.2.4, INITIAL DEPLOYMENT

During an initial deployment of MCP OpenStack with OpenContrail, the OpenContrail states fail due to the dependencies of the Python packages for OpenContrail. The workaround is to restart salt-minions on the target compute hosts.

[29843] Pike to Queens upgrade fails for the OpenStack deployments with Octavia
Fixed in 2019.2.4, OPENSTACK PIKE TO QUEENS UPGRADE, OCTAVIA

During the upgrade of the OpenStack control plane from Pike to Queens of the MCP OpenStack deployments with Octavia, the Deploy - upgrade control VMs pipeline job may fail with the NotFound: The resource could not be found. (HTTP 404) error.

Workaround:

1. Log in to the Salt Master node.
2. Apply the following state:

   ```bash
   salt 'ctl01*' state.sls salt.minion
   ```
3. Rerun the Deploy - upgrade control VMs pipeline job from the Jenkins web UI.

[29844] OpenStack with Octavia update fails due to a missing CA certificate
Fixed in 2019.2.4, OPENSTACK VCP UPDATE, OCTAVIA

During the update of the OpenStack control plane of MCP OpenStack deployments with Octavia, the Deploy - upgrade control VMs pipeline job may fail during the application of the octavia.upgrade.verify._api state with the Internal Server Error (HTTP 500) error due to a missing ca-cert.pem.
Workaround:

1. Log in to the Salt Master node.

2. Apply the following state:

   ```bash
   salt -C "I@salt:minion:ca" state.sls salt.minion
   ```

3. Rerun the Deploy - upgrade control VMs pipeline job from the Jenkins web UI.

[29812] The OpenContrail web UI service fails to start after update
Fixed in 2019.2.4, OPENSTACK WITH OPENCONTRAIL, UPDATE

After updating OpenContrail 4.x version, the contrail-webui service may fail to start due to the missing quotation mark in /etc/contrail/config.global.js.

Workaround:

1. Log in to the Salt Master node.

2. Add the missing quotation mark in /etc/contrail/config.global.js:

   ```bash
   salt -C 'I@opencontrail:control' cmd.run template=jinja
   
   "sed -i "s/config.imageManager.authProtocol.*/config.imageManager.authProtocol = '{{pillar.opencontrail.web.identity.protocol}}';/g" /etc/contrail/config.global.js"
   ```

   After execution of the command above, the contrail-webui and contrail-webui-middleware services should restart automatically.

3. Verify that the contrail-web and contrail-webui-middleware services are in the active state:

   ```bash
   salt -C 'I@opencontrail:control' cmd.run "doctrail controller contrail-status"
   ```

Updated packages

The MCP 2019.2.3 update includes the following changes in the minor versions of the MCP packages. All other versions of the major MCP components remain the same as the MCP Q4’18 GA release including the MCP 2019.2.1 and 2019.2.2 updates and can be found in Major components versions, MCP 2019.2.1 updated packages, and MCP 2019.2.2 updated packages.

All 2019.2.3 packages are available at http://mirror.mirantis.com/update/2019.2.0/.

Updated major software components from the Mirantis and mirrored repositories

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.2</th>
<th>2019.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>DriveTrain</td>
<td>jenkins-master</td>
<td>2.138.3</td>
<td>2.150.3</td>
</tr>
<tr>
<td>OpenStack Pike</td>
<td>Cinder</td>
<td>2:11.1.1-2<del>u16.04+mcp122.0-2</del>u16.04+mcp152</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Heat</td>
<td>1:9.0.5-1<del>u16.04+mcp50.0.5-1</del>u16.04+mcp54</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Horizon</td>
<td>3:12.0.3-4<del>u16.04+mcp61.0.3-4</del>u16.04+mcp67</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Keystone</strong></td>
<td>2:12.0.1-4~u16.04+mcp16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2:12.0.2-4~u16.04+mcp14</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manila</strong></td>
<td>1:5.0.2-1~u16.04+mcp405</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.3-1~u16.04+mcp49</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Nova</strong></td>
<td>2:16.1.7-4~u16.04+mcp148</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2:16.1.7-4~u16.04+mcp165</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OpenStack Networking Pike</strong></td>
<td>Neutron 2:11.0.6-2~u16.04+mcp185</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2:11.0.6-2~u16.04+mcp201</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OpenStack Queens</strong></td>
<td>Cinder 2:12.0.5-2~u16.04+mcp17</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2:12.0.5-2~u16.04+mcp89</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Heat</strong></td>
<td>1:10.0.2-1.0~u16.04+mcp166</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.2-1.0~u16.04+mcp64</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Horizon</strong></td>
<td>3:13.0.1-10~u16.04+mcp133</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.1-10~u16.04+mcp89</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ironic</strong></td>
<td>TechPreview 1:10.1.7-1.0~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.8-1.0~u16.04+mcp32</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Keystone</strong></td>
<td>2:13.0.2-3~u16.04+mcp143</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2:13.0.2-3~u16.04+mcp19</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manila</strong></td>
<td>1:6.0.2-2~u16.04+mcp606</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.0-2~u16.04+mcp52</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Nova</strong></td>
<td>2:17.0.9-6~u16.01+mcp157</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2:17.0.9-6~u16.01+mcp189</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OpenStack Networking Queens</strong></td>
<td>Neutron 2:12.0.5-5~u16.04+mcp139</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2:12.0.5-5~u16.04+mcp155</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Kubernetes</strong></td>
<td>CNI-plugins 0.7.2-151</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.7.2-173</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>containerd</strong></td>
<td>1.2.1+1-1<del>u16.04+mcp1.2.5-2</del>u16.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CoreDNS</strong></td>
<td>1.2.6-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>etcd</strong></td>
<td>3.3.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ExternalDNS</strong></td>
<td>0.5.9-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.5.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Helm</strong></td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.12.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Kubernetes</strong></td>
<td>1.12.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.13.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NGINX Ingress controller</strong></td>
<td>0.21.0-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.23.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tiller</strong></td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.12.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Virtlet</strong></td>
<td>1.4.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.5.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Distributed storage</strong></td>
<td>Ceph 12.2.8-1~u16.04+mcp142</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2.11-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>Open vSwitch 2.8.0-4~u16.04+mcp101</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.8.4-0.0.17.10.1~u16.04</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.9.0-0.1~u16.04</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apply maintenance updates
Caution!

If you are updating from MCP 2019.2.2 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.2, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DriveTrain</td>
<td>Update DriveTrain to a minor release version.</td>
</tr>
</tbody>
</table>
| 2 | OpenContrail         | 1. Update the OpenContrail packages as described in Update the OpenContrail 4.x nodes.  
|   |                      | 2. Optional. Override the default DNS server list for vRouter.            |
| 3 | OpenStack            | 1. Update the OpenStack packages as described in MCP Operations guide: Update OpenStack packages.  
|   |                      | 2. Enable FQDN on internal endpoints in the Keystone catalog.             |
|   |                      | 3. Optional. Enable exposition of a hardware RNG device to Nova instances.|
|   |                      | 4. Optional. Perform the steps described in Issues resolutions requiring manual application. |
| 4 | Kubernetes           | 1. Update the Kubernetes packages as described in Update or upgrade Kubernetes.  
|   |                      | 2. Optional. Enable Helm support.                                         |
|   |                      | 2. Update StackLight LMA using the Deploy - upgrade StackLight Jenkins pipeline job as described in MCP Operations Guide: Update StackLight LMA but deselect the STAGE_UPGRADE_ES_KIBANA parameter. |
5 Ceph

1. Update the Ceph packages as described in Update Ceph packages.
2. Optional. Enable Ceph prediction alerts using the step 10 in Enable the Ceph Prometheus plugin.
3. Optional. Obtain the Ceph pipeline jobs improvements as described in Pipeline jobs improvements.
4. Optional. Perform the steps described in Issues resolutions requiring manual application.

6 Ubuntu Xenial packages

Select from the following options:

- Apply security updates using Jenkins
- Apply security updates manually

See also

Known issues

2019.2.2

The MCP 2019.2.2 update introduces full support for the OpenStack cloud provider in Kubernetes and the possibility to update the existing L2 Gateway connections. Also, this maintenance update contains bug fixes for several MCP components including DriveTrain, OpenStack, Kubernetes, and StackLight.

The MCP 2019.2.2 update is available starting from March, 20 and is applied automatically during the initial deployment of the MCP Q4'18 release.

Enhancements

In the MCP 2019.2.2 update, Mirantis introduces the following enhancements to the existing features of the MCP 2019.2.0 release version:

- Added full support for the OpenStack cloud provider that you can enable on new Kubernetes clusters that are deployed on VMs on top of OpenStack.

  The OpenStack cloud provider extends the basic functionality of Kubernetes by fulfilling the provider requirement for several resources. This is achieved through communication with several OpenStack APIs.

  The two main functions provided by the OpenStack cloud provider are PersistentVolume for pods and LoadBalancer for services.

Learn more

- MCP Reference Architecture: OpenStack cloud provider for Kubernetes
• MCP Deployment Guide: Deploy OpenStack cloud provider for Kubernetes

• Enabled the possibility to update the existing L2GW connections. Now, you can add or remove network interfaces, and these changes will be reflected in the existing L2GW connections.

Addressed issues

The MCP 2019.2.2 update contains fixes for several MCP components.

DriveTrain

• Fixed the issue with the false positive failures of the CVP - Sanity checks Jenkins pipeline job during the Jenkins check and the check of the Docker images on the cid nodes.

• Fixed the repository replacement issues in the Deploy - upgrade MCP DriveTrain Jenkins pipeline job.

• Fixed the issue with unencrypted OpenLDAP admin password that caused the phpldapadmin Docker service to fail with write error: Broken pipe.

• Fixed the issue with the Verify and Restore Galera cluster Jenkins pipeline job failing for a Galera cluster in the healthy state.

• Fixed the issue with the CVP - Functional tests, CVP - HA tests, and CVP - Performance tests Jenkins pipeline jobs failing if the TARGET_NODE parameter was not set. Now, if this parameter is empty, the node with the gerrit:client pillar will be used, cid01 by default.

OpenStack

• Updated the Keepalived package to version 1.3.9 to fix the Tempest smoke tests failures.

• [Queens] Updated the ExaBGP package to version 4.0.2-2~u16.04+mcp to fix the package installation failure during the OpenStack environment upgrade.

• [Pike] Updated the OpenStack Nova package to version 16.1.7-4~u16.04+mcp149 and the OpenStack Neutron package to version 11.0.6-2~u16.04+mcp185 to allow a MAC address change for the direct-physical port type during cold migration and resizing of instances and to fix the DHCP addressing operations.
• [Queens] Fixed the Nova Populate_pci_mac_address function to prevent erroneous logging of a module instead of pci_request_id. Also, implemented proper handling of IndexError in Populate_neutron_binding_profile.

• [Queens] Fixed the issue with the nova-compute service failing to start if an instance from the compute node has been evacuated and destroyed after that.

• [Queens] Fixed the issue with the disk usage report for instances booted from volumes. Previously, when booting an instance from a volume, the used_disk value in the hypervisor stats was getting increased by the size of the requested volume while the instance itself was not using any hypervisor disk resources.

• Fixed the issue with the os-vif plugin recreating the existing OVS port after the nova-compute service restart.

• Fixed the issue with the OVS bridge br-bond1 not being attached to the physical bond1 interface during a compute node deployment.

• Fixed the issue with DNS not working after deployment of an OpenStack-based MCP cluster.

• Fixed the issue with the BGP VPN update failure that occurred because the signature of the update_bgpv4n_precommit method did not match the one for networking-bgpv4n in driver_api.py. The fix updates the signature for the ODL v2 driver for BGP VPN.

• [Queens] Fixed the issue with the Horizon dashboard not displaying a confirmation alert when closing the Create image window.

Kubernetes

• [CVE-2019-5736] Updated the containerd version to 1.2.1+1-1-u16.04+1-mcp to fix the malicious container escape security vulnerability in runc. However, the fix affects memory usage: runc uses more memory during a container startup. For details, see the corresponding GitHub issue. The memory usage issue is addressed in 2019.2.3. For details, see: Kubernetes.

• [CVE-2019-100210] Updated the Kubernetes hyperkube-amd64 image to version 1.12.6 to address the json-patch requests exhausting the API server resources vulnerability.

• Fixed the issue with the OpenStack cloud provider redefining the internal IP of the Kubernetes nodes with an IP of every NIC and assigning a wrong IP address as a primary address of a node.

StackLight

• Removed the SfNotifierErrorsWarning StackLight LMA alert that was based on an unreliable metric.

• To prevent the issue with CADF notifications being unavailable, changed the version of Elasticsearch and Kibana to v5. Now, when deploying MCP Q4’18, Elasticsearch and Kibana v5 install by default instead of v6.
Note
In the 2019.2.4 maintenance update, Elasticsearch and Kibana have been updated to v6.5.2. For details, see StackLight.

Updated packages
The MCP 2019.2.2 update includes the following changes in the minor versions of the MCP packages. All other versions of the major MCP components remain the same as the MCP Q4'18 GA release including the MCP 2019.2.1 update and can be found in Major components versions and MCP 2019.2.1 updated packages.

All 2019.2.2 packages are available at http://mirror.mirantis.com/update/2019.2.0/.

Updated major software components from the Mirantis and mirrored repositories

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.1</th>
<th>2019.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kubernetes</td>
<td>containerd</td>
<td>1.2.1-1~u16.04+mcp</td>
<td>1.2.1+1-1~u16.04+mcp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.12.4</td>
<td>1.12.6</td>
</tr>
<tr>
<td></td>
<td>Cinder</td>
<td>2:12.0.4-2~u16.04+mcp76</td>
<td>2:12.0.4-2~u16.04+mcp76</td>
</tr>
<tr>
<td></td>
<td>Heat</td>
<td>1:10.0.2-1.0~u16.04+mcp56</td>
<td>1:10.0.2-1.0~u16.04+mcp56</td>
</tr>
<tr>
<td></td>
<td>Horizon</td>
<td>3:13.0.1-10~u16.04+mcp19</td>
<td>3:13.0.1-10~u16.04+mcp19</td>
</tr>
<tr>
<td></td>
<td>Neutron</td>
<td>2:12.0.5-5~u16.04+mcp139</td>
<td>2:12.0.5-5~u16.04+mcp139</td>
</tr>
<tr>
<td></td>
<td>Nova</td>
<td>2:17.0.9-6~u16.01+mcp93</td>
<td>2:17.0.9-6~u16.01+mcp157</td>
</tr>
<tr>
<td></td>
<td>Octavia</td>
<td>2.0.2-6<del>u16.04+mcp692.0.4-6</del>u16.04+mcp51</td>
<td>2.0.2-6<del>u16.04+mcp692.0.4-6</del>u16.04+mcp51</td>
</tr>
<tr>
<td>OpenStack Pike</td>
<td>L2 Gateway</td>
<td>1:11.0.0-1<del>u16.04+mcp611.0.0-1</del>u16.04+mcp12</td>
<td>1:11.0.0-1<del>u16.04+mcp611.0.0-1</del>u16.04+mcp12</td>
</tr>
<tr>
<td></td>
<td>ODL ML2 plugin</td>
<td>1:11.0.0-1<del>u16.04+mcp411.0.0-1</del>u16.04+mcp60</td>
<td>1:11.0.0-1<del>u16.04+mcp411.0.0-1</del>u16.04+mcp60</td>
</tr>
<tr>
<td></td>
<td>Neutron</td>
<td>2:11.0.6-2~u16.04+mcp185</td>
<td>2:11.0.6-2~u16.04+mcp185</td>
</tr>
<tr>
<td></td>
<td>Nova</td>
<td>2:16.1.7-4<del>u16.04+mcp616.1.7-4</del>u16.04+mcp149</td>
<td>2:16.1.7-4<del>u16.04+mcp616.1.7-4</del>u16.04+mcp149</td>
</tr>
<tr>
<td>System</td>
<td>MySQL</td>
<td>5.6.35-0.1<del>u16.04+mcp26.41-1</del>u16.04+mcp1</td>
<td>5.6.35-0.1<del>u16.04+mcp26.41-1</del>u16.04+mcp1</td>
</tr>
<tr>
<td>StackLight LMA</td>
<td>Elasticsearch</td>
<td>6.5.2</td>
<td>5.6.12 22</td>
</tr>
<tr>
<td></td>
<td>Kibana</td>
<td>6.5.2</td>
<td>5.6.12 22</td>
</tr>
</tbody>
</table>

2019.2.1
The MCP 2019.2.1 update contains bug fixes for the OpenStack Pike release and is available starting from February, 27.

22(1, 2) For details, see StackLight addressed issues.
The MCP 2019.2.1 is applied automatically during the initial deployment of the MCP Q4’18 release.

Addressed issues

MCP 2019.2.1 update contains fixes for the following issues in the OpenStack Pike release:

- Fixed the issue with the invalid values for tcp.bind written to the /etc/exabgp/exabgp.env file that caused the Neutron deployment failure during the upgrade of OpenStack from Pike to Queens.
- Added support for the Neutron network MTU configuration. The new --mtu argument enables the CLI users to set MTU for the Neutron networks.
- Fixed the issue with the checksums left unfilled by Virtio as a hypervisor internal optimization. Some DHCP clients failed to acquire an address if the checksums were left unfilled during the attempts to verify these checksums. The resolution includes adding of the ip6tables rule to fix the checksum of DHCPv6 response packets.
- Fixed the issue with a failure of the Cinder volume creation using the ScaleIO driver.
- Fixed the issue with the nova-compute service failing to start if an instance from the compute node has been evacuated and destroyed after that.
- Fixed the issue with the disk usage report for instances booted from volumes. Previously, when booting an instance from a volume, the used_disk value in the hypervisor stats was getting increased by the size of the requested volume while the instance itself was not using any hypervisor disk resources.

Updated packages

MCP 2019.2.1 update includes the following changes in the minor versions of the OpenStack packages. All other versions of the major MCP components remain the same as the MCP Q4’18 GA release and can be found in Major components versions. All 2019.2.1 packages are available at http://mirror.mirantis.com/update/2019.2.0/.

<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2019.2.0</th>
<th>2019.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack Pike</td>
<td>Cinder</td>
<td>2:11.1.1-2~u16.04+mcp140</td>
<td>2:11.0.6-2~u16.04+mcp181</td>
</tr>
<tr>
<td></td>
<td>Heat</td>
<td>1:9.0.5-1~u16.04+mcp49</td>
<td>1:9.0.5-1~u16.04+mcp50</td>
</tr>
<tr>
<td></td>
<td>Horizon</td>
<td>3:12.0.3-3~u16.04+mcp63</td>
<td>3:12.0.3-3~u16.04+mcp65</td>
</tr>
<tr>
<td></td>
<td>Ironic</td>
<td>1:9.1.6-1~u16.04+mcp31</td>
<td>1:9.1.6-1~u16.04+mcp36</td>
</tr>
<tr>
<td>OpenStack Networking Pike</td>
<td>Neutron</td>
<td>2:11.0.6-2~u16.04+mcp181</td>
<td>2:11.0.6-2~u16.04+mcp181</td>
</tr>
</tbody>
</table>