MCP Q3`18 Release Notes

version q3-18
What’s new

The Q3`18 MCP release focuses on the product quality and stability being released without blocking and critical issues. Also, this MCP release includes support for OpenStack Pike, OpenStack Queens with OVS and StackLight LMA, Kubernetes 1.11, OpenContrail 4.0, and Ceph Luminous.

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 Q3’18 Deployment Guide for the software features that can be deployed and managed by MCP DriveTrain.

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

MCP DriveTrain

- Reclass upgrade
- Security updates implementation
- Jenkins operational capabilities improvements

Reclass upgrade

Included the Reclass v1.5.x within the release-tagged repository. The integration of the new Reclass version does not require any specific manual upgrade procedures for new deployments, and is automatically enforced during the automatic upgrade from the previous Build IDs.

Learn more

MCP Operations Guide: Reclass upgrade notes

Security updates implementation

Implemented the capability to obtain security updates for the host operating system packages of your OpenStack-based MCP cluster starting from the Build ID 2018.8.0 using the update
repositories. The update repositories provide for update of the specific Ubuntu packages for the CI/CD, OpenStack, and StackLight LMA nodes.

Learn more
MCP Operations Guide: Obtain Ubuntu security updates

Jenkins operational capabilities improvements

• Added support for the Job Configuration History Jenkins plugin that allows for inspecting the history of jobs configuration changes.

Learn more
MCP Operations Guide: Job configuration history

• Enabled the Matrix-based security authorization by default. This authorization scheme enables the operator to grant specific permissions to users and groups. As an identity provider and authentication server, Jenkins uses the DriveTrain OpenLDAP server.

Learn more
MCP Operations Guide: Jenkins Matrix-based security authorization

OpenStack

• OpenStack Queens support
• X.509 certificates for authentication
• TLS encryption between the OpenStack compute nodes and VNC clients
• OpenStack Octavia integration
• OpenStack services configuration through Model Designer
• MySQL back end for PowerDNS
• OpenStack Ocata to Pike upgrade
OpenStack Queens support
Added support for the OpenStack Queens release for the new MCP OpenStack with OVS and StackLight LMA deployments. The OpenStack Queens with OpenContrail configuration is available as technical preview only.
MCP provides integration of a number of the OpenStack community features introduced with Queens which the MCP consumers can benefit from. Refer to the MCP Q3’18 Deployment Guide for the OpenStack software features that can be deployed and managed by MCP DriveTrain.
For the users who prefer older releases of OpenStack, MCP can also accommodate the OpenStack Pike deployments.

Learn more

- MCP Q3’18 Deployment Guide
- MCP Release Compatibility Matrix

X.509 certificates for authentication
SECURITY
Enhanced the OpenStack security by adding an ability to configure OpenStack APIs to use X.509 certificates for communicating with the MySQL database and RabbitMQ server. The added functionality provides for greater identity assurance of OpenStack clients making the connection and ensures that the communications are encrypted.

Learn more

- MCP Deployment Guide: Configure OpenStack APIs to use X.509 certificates for MySQL
- MCP Deployment Guide: Configure OpenStack APIs to use X.509 certificates for RabbitMQ

TLS encryption between the OpenStack compute nodes and VNC clients
SECURITY

Implemented an ability to encrypt the communications between the OpenStack compute nodes and VNC clients over TLS for the Queens-based OpenStack deployments.

Learn more

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

OpenStack Octavia integration

Integrated OpenStack Octavia with the Neutron LBaaS driver v2 for OpenStack Pike and Queens. OpenStack Octavia provides advanced load balancing by acting as a back-end driver for Neutron LBaaS and handling all networking requests by the Octavia API.

Caution!

Octavia works with Neutron OVS as a network solution only. OpenContrail is not supported.

The main advantage of Octavia comparing to just using the Neutron LBaaS driver is that Octavia provides easy on-demand scaling of load-balancing services, what makes it an enterprise-class solution.

Learn more

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

OpenStack services configuration through Model Designer

Added a capability to enable and configure the following services during the deployment metadata model creation using the Model designer web UI:

• Tenant Telemetry
• Designate
• Manila
• Barbican
• TLS for internal endpoints, MySQL, and RabbitMQ

Learn more

• MCP Deployment Guide: General deployment parameters
• MCP Deployment Guide: Product related parameters

MySQL back end for PowerDNS

Added a possibility to use the PowerDNS underlying Domain Name system (DNS) server with the MySQL back end instead of the default SQLite one.

Learn more

MCP Deployment Guide: Enable the MySQL back end for PowerDNS

OpenStack Ocata to Pike upgrade

TECHNICAL PREVIEW

Implemented the upgrade of OpenStack Ocata deployments to Pike.

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.

The upgrade procedure has been tested on the component level. Therefore, the OpenStack upgrade ability is marked as a technical preview feature.
Kubernetes

MCP introduces the following Kubernetes-related updates:

- Kubernetes 1.11.3
- NGINX Ingress controller
- Virtlet 1.4.1 and security improvements
- Kubernetes with existing Ceph RBD storage
- Calico 3.1
  - Manual Calico upgrade from version 2.6 to 3.1
  - The containerd runtime instead of Docker

Kubernetes 1.11.3

Added support for the upstream Kubernetes version 1.11.3. For the list of enhancements and bug fixes, see Kubernetes release notes.

NGINX Ingress controller

Implemented the possibility to enable the NGINX Ingress controller if you use MetalLB in your MCP Kubernetes-based cluster to provide an external access to Kubernetes services. The NGINX Ingress controller provides load balancing, SSL termination, and name-based virtual hosting.

Virtlet 1.4.1 and security improvements

Updated Virtlet to version 1.4.1 and added support for the following items:
• Persistent root file system
• Block persistent volumes
• Resizing of root volumes
• Mounting of arbitrary Kubernetes volumes by 9pfs

Also, improved Virtlet security:
• Added support for verification of image checksum
• Implemented the AppArmor profiles

Learn more

• MCP Reference Architecture: Virtlet limitations
• Virtlet release notes
• Virtlet official documentation

Kubernetes with existing Ceph RBD storage

Added the possibility to connect your Kubernetes cluster to an existing external Ceph RADOS Block Device (RBD) storage.

Learn more

MCP Deployment Guide: Enable an external Ceph RBD storage

Calico 3.1

Added support for Calico version 3.1 that has significant enhancements as compared to the previous version 2.6, including support for Kubernetes 1.11. For a detailed list of features and improvements, see Calico release notes 3.1.0 and 3.0.1. Calico version 3.1 is installed by default on new MCP Kubernetes-based clusters.

Manual Calico upgrade from version 2.6 to 3.1
Implemented the manual upgrade procedure for Calico from version 2.6 to 3.1 on the MCP Kubernetes-based clusters.

**Caution!**

This upgrade procedure is applicable when MCP is upgraded from Build ID 2018.8.0 to a newer MCP release version.

MCP does not support the Calico upgrade path for the MCP Build IDs earlier than 2018.8.0.

Learn more

[MCP Operations Guide: Upgrade Calico from version 2.6 to 3.1](#)

---

**The containerd runtime instead of Docker**

**TECHNICAL PREVIEW**

Added support for the containerd runtime to execute containers and manage container images on a node instead of Docker. You can enable this option while generating your MCP deployment metadata model. Disabled by default. Also, added this option to the default configuration of EDGE Cloud MVP.

The containerd runtime is available as technical preview. Use such configuration for testing and evaluation purposes only.

Learn more

- MCP Deployment Guide: Kubernetes product parameters
- MCP Deployment Guide: Deploy Edge Cloud MVP

---

**OpenContrail**

MCP introduces the following OpenContrail-related updates:
Caution!

Starting with MCP Build ID 2018.11.0, OpenContrail 3.2 is not supported for new deployments.

• Added support for OpenContrail 4.0 with Kubernetes 1.11 including the corresponding changes in Cookiecutter and the MCP Jenkins deployment pipelines.
• Hardened support for OpenContrail 4.0 with OpenStack Ocata.
• TECHNICAL PREVIEW Added support for OpenContrail 4.0 with OpenStack Queens including the corresponding changes in Cookiecutter and the MCP Jenkins deployment pipelines. This feature is available as technical preview only.
• Added QEMU 2.11 support for the OpenContrail vRouter packages.

See also

• MCP Deployment Guide: Deploy OpenStack with OpenContrail
• MCP Deployment Guide: Deploy Kubernetes with OpenContrail

StackLight LMA

• Grafana improvements
• Docker garbage collection
• StackLight LMA upgrade

Grafana improvements

• Updated Grafana version from 5.1.3 to 5.2.4.

Learn more

Major components versions
• Extended the libvirt exporter functionality to collect tenant metrics from Nova and implemented the OpenStack Tenants Grafana dashboard that provides a detailed view of Nova instances usage per tenants and users.

   Learn more
   MCP Operations Guide: OpenStack tenants dashboard

• Added the capability for Grafana to display the OpenStack tenant data stored in the Gnocchi time series database.
   If your OpenStack version is Pike or newer and you have deployed Tenant Telemetry based on Ceilometer, Aodh, Panko, and Gnocchi, you can also add Gnocchi as the data source for Grafana.

   Learn more
   MCP Operations Guide: Add the Gnocchi data source to Grafana

• Added the Keepalived Telegraf input plugin that allows for gathering metrics about the state of a Virtual Router Redundancy Protocol (VRRP) instance. Improved the Keepalived Grafana dashboard to display the process responsiveness.

   Learn more
   MCP Operations Guide: Keepalived dashboard

Docker garbage collection
Implemented the Docker garbage collector cron job for old StackLight LMA containers and volumes. The cron job is disabled by default.

   Learn more
   MCP Operations Guide: Enable Docker garbage collection
StackLight LMA upgrade

TECHNICAL PREVIEW

Simplified the upgrade of StackLight LMA by introducing the following improvements:

- Implemented the Deploy - upgrade Stacklight Jenkins pipeline that provides for a seamless automatic upgrade starting from Build ID 2018.8.0.

- Improved the StackLight LMA upgrade procedure for a better view on how to upgrade StackLight LMA of a particular MCP version to the latest supported one.

Learn more

MCP Operations Guide: StackLight LMA upgrade
Release artifacts

The MCP release artifacts are tagged with the 2018.11.0 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 2018.11.0 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 and their respective license information, download MCP 2018.11.0 Encryption and Licensing.

---

<table>
<thead>
<tr>
<th>Type</th>
<th>Artifact</th>
<th>Path for Build ID 2018.11.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirantis apt/deb</td>
<td>Extra packages</td>
<td>deb [<a href="http://mirror.mirantis.com/2018.11.0/extra/xenial/xenial">http://mirror.mirantis.com/2018.11.0/extra/xenial/xenial</a>]</td>
</tr>
<tr>
<td>Mirantis QCOW images</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ceph</td>
<td>deb [<a href="http://mirror.mirantis.com/2018.11.0/ceph-luminous/xenial">http://mirror.mirantis.com/2018.11.0/ceph-luminous/xenial</a>]</td>
<td></td>
</tr>
<tr>
<td>Salt formulas packages</td>
<td>deb [<a href="http://apt.mirantis.com/xenial/">http://apt.mirantis.com/xenial/</a> 2018.11.0 salt]</td>
<td></td>
</tr>
<tr>
<td>MCP cfg01 day01 image</td>
<td>[<a href="http://images.mirantis.com/cfg01-day01-2018.11.0.qcow2.md5">http://images.mirantis.com/cfg01-day01-2018.11.0.qcow2.md5</a>]</td>
<td>[<a href="http://images.mirantis.com/cfg01-day01-2018.11.0.qcow2">http://images.mirantis.com/cfg01-day01-2018.11.0.qcow2</a>]</td>
</tr>
</tbody>
</table>
| MCP apt01 offline image | http://images.mirantis.com/mcp-offline-image-2018.11.0.qcow2.md5  
http://images.mirantis.com/mcp-offline-image-2018.11.0.qcow2 |
|------------------------|----------------------------------------------------------------|
| VCP Ubuntu 16.04 image | http://images.mirantis.com/ubuntu-16-04-x64-mcp2018.1.0.qcow2.md5  
http://images.mirantis.com/ubuntu-16-04-x64-mcp2018.1.0.qcow2 |
| Upstream mirrors       | aptly
|                        | deb http://mirror.mirantis.com/2018.11.0/aptly/xenial squeeze main |
| Cassandra              | deb http://mirror.mirantis.com/2018.11.0/cassandra/trusty 21x main  
deb http://mirror.mirantis.com/2018.11.0/cassandra/xenial 21x main |
| Docker                 | deb http://mirror.mirantis.com/2018.11.0/docker/xenial stable  
deb http://mirror.mirantis.com/2018.11.0/docker-1.x/xenial
|                        | ubuntu-xenial main |
| Elastic                | deb http://mirror.mirantis.com/2018.11.0/elasticsearch-2.x/xenial stable main  
deb http://mirror.mirantis.com/2018.11.0/elasticsearch-5.x/xenial stable main  
deb http://mirror.mirantis.com/2018.11.0/elasticsearch-5/xenial stable main  
deb http://mirror.mirantis.com/2018.11.0/elasticsearch-curator/xenial stable main  
deb http://mirror.mirantis.com/2018.11.0/elasticsearch-curator-5/xenial stable main |
<p>| Fluentd                | deb <a href="http://mirror.mirantis.com/2018.11.0/td-agent/xenial">http://mirror.mirantis.com/2018.11.0/td-agent/xenial</a> xenial contrib |
| GlusterFS              | deb <a href="http://mirror.mirantis.com/2018.11.0/glusterfs-3.8/xenial">http://mirror.mirantis.com/2018.11.0/glusterfs-3.8/xenial</a> xenial main |
| InfluxDB               | deb <a href="http://mirror.mirantis.com/2018.11.0/influxdb/xenial">http://mirror.mirantis.com/2018.11.0/influxdb/xenial</a> xenial stable |
| Kibana                 | deb <a href="http://mirror.mirantis.com/2018.11.0/kibana-4.6/xenial">http://mirror.mirantis.com/2018.11.0/kibana-4.6/xenial</a> stable main |
| MAAS                   | deb <a href="http://mirror.mirantis.com/2018.11.0/maas/xenial">http://mirror.mirantis.com/2018.11.0/maas/xenial</a> xenial main |</p>
<table>
<thead>
<tr>
<th>Percona</th>
<th>deb <a href="http://mirror.mirantis.com/2018.11.0/percona/xenial">http://mirror.mirantis.com/2018.11.0/percona/xenial</a> xenial main</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaltStack packages</td>
<td>deb <a href="http://mirror.mirantis.com/2018.11.0/saltstack-2017.7/trusty">http://mirror.mirantis.com/2018.11.0/saltstack-2017.7/trusty</a> trusty main</td>
</tr>
<tr>
<td></td>
<td>deb <a href="http://mirror.mirantis.com/2018.11.0/saltstack-2017.7/xenial">http://mirror.mirantis.com/2018.11.0/saltstack-2017.7/xenial</a> xenial main</td>
</tr>
<tr>
<td>Upstream Ubuntu system packages</td>
<td>deb <a href="https://mirror.mirantis.com/2018.11.0/ubuntu/xenial">https://mirror.mirantis.com/2018.11.0/ubuntu/xenial</a> xenial main restricted universe</td>
</tr>
<tr>
<td></td>
<td>deb <a href="https://mirror.mirantis.com/2018.11.0/ubuntu/xenial-updates">https://mirror.mirantis.com/2018.11.0/ubuntu/xenial-updates</a> main restricted universe</td>
</tr>
<tr>
<td></td>
<td>deb <a href="https://mirror.mirantis.com/2018.11.0/ubuntu/xenial-security">https://mirror.mirantis.com/2018.11.0/ubuntu/xenial-security</a> main restricted universe</td>
</tr>
<tr>
<td>MCP Git repositories</td>
<td>Jenkins pipeline library for MCP operations</td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/Mirantis/mk-pipelines/">https://github.com/Mirantis/mk-pipelines/</a> tag 2018.11.0</td>
</tr>
<tr>
<td>General Jenkins pipeline library</td>
<td><a href="https://github.com/Mirantis/pipeline-library/">https://github.com/Mirantis/pipeline-library/</a> tag 2018.11.0</td>
</tr>
<tr>
<td>Reclass system level</td>
<td><a href="https://github.com/Mirantis/reclass-system-salt-model/">https://github.com/Mirantis/reclass-system-salt-model/</a> tag 2018.11.0</td>
</tr>
<tr>
<td>MCP common scripts</td>
<td><a href="https://github.com/Mirantis/mcp-common-scripts/">https://github.com/Mirantis/mcp-common-scripts/</a> tag 2018.11.0</td>
</tr>
<tr>
<td>MCP offline image model</td>
<td><a href="https://github.com/Mirantis/mcp-offline-model">https://github.com/Mirantis/mcp-offline-model</a> tag 2018.11.0</td>
</tr>
<tr>
<td>Docker images</td>
<td>alerta-web</td>
</tr>
<tr>
<td></td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2018.11.0</td>
</tr>
<tr>
<td></td>
<td>alertmanager</td>
</tr>
<tr>
<td></td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2018.11.0</td>
</tr>
<tr>
<td>aptly</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2018.11.0</td>
</tr>
<tr>
<td>aptly-api</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-api:2018.11.0</td>
</tr>
<tr>
<td>aptly-public</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2018.11.0</td>
</tr>
<tr>
<td>aptly-publisher</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2018.11.0</td>
</tr>
<tr>
<td>cluster-proportional-autoscaler-amd64</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/cluster-proportional-autoscaler-amd64:2018.11.0</td>
</tr>
<tr>
<td>compose</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/compose:2018.11.0</td>
</tr>
<tr>
<td>Image</td>
<td>Docker Registry</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>contrail-cni</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/contrail-integration/contrail-cni:v1.2.0</td>
</tr>
<tr>
<td>ctl</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/ctl:v3.1.3</td>
</tr>
<tr>
<td>cni</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/cni:v3.1.3</td>
</tr>
<tr>
<td>coredns</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/coredns/coredns:v1.2.2-12</td>
</tr>
<tr>
<td>cvp-rally</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cvp-rally:2018.11.0</td>
</tr>
<tr>
<td>elasticsearch</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/elasticsearch:2018.11.0</td>
</tr>
<tr>
<td>etcd</td>
<td>quay.io/coreos/etcd:v3.3.8</td>
</tr>
<tr>
<td>etcd-operator</td>
<td>quay.io/coreos/etcd-operator:v0.9.2</td>
</tr>
<tr>
<td>flannel</td>
<td>quay.io/coreos/flannel:v0.10.0-amd64</td>
</tr>
<tr>
<td>gainsight</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2018.11.0</td>
</tr>
<tr>
<td>gerrit</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2018.11.0</td>
</tr>
<tr>
<td>grafana</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/grafana:2018.11.0</td>
</tr>
<tr>
<td>heka</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2018.11.0</td>
</tr>
<tr>
<td>hyperkube-amd64</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/hyperkube-amd64:v1.11.3-2</td>
</tr>
<tr>
<td>janitor-monkey</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/oss/janitor-monkey:2018.11.0</td>
</tr>
<tr>
<td>jenkins</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2018.11.0</td>
</tr>
<tr>
<td>jnlp-slave</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2018.11.0</td>
</tr>
<tr>
<td>k8s-dns-kube-dns-amd64</td>
<td>gcr.io/google_containers/k8s-dns-kube-dns-amd64:1.14.5</td>
</tr>
<tr>
<td>Container Name</td>
<td>Registry Path</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>k8s-dns-dnsmasq-amd64</td>
<td>gcr.io/google_containers/k8s-dns-dnsmasq-amd64:1.14.5</td>
</tr>
<tr>
<td>k8s-dns-sidecar-amd64</td>
<td>gcr.io/google_containers/k8s-dns-sidecar-amd64:1.14.5</td>
</tr>
<tr>
<td>k8s-netchecker-agent</td>
<td>mirantis/k8s-netchecker-agent:v1.2.2 (at hub.docker.com)</td>
</tr>
<tr>
<td>k8s-netchecker-server</td>
<td>mirantis/k8s-netchecker-server:v1.2.2 (at hub.docker.com)</td>
</tr>
<tr>
<td>kube-controllers</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/kube-controllers:v3.1.3</td>
</tr>
<tr>
<td>kubernetes-dashboard-amd64</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/kubernetes-dashboard-amd64:v1.10.0-4</td>
</tr>
<tr>
<td>metallb-controller</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/metallb/controller:v0.7.3-2</td>
</tr>
<tr>
<td>metallb-speaker</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/metallb/speaker:v0.7.3-2</td>
</tr>
<tr>
<td>mongo</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/mongo:2018.11.0</td>
</tr>
<tr>
<td>mysql</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2018.11.0</td>
</tr>
<tr>
<td>nginx-ingress-controller-amd64</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/nginx/nginx-ingress-controller-amd64:nginx-0.19.0-1</td>
</tr>
<tr>
<td>node</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/node:v3.1.3</td>
</tr>
<tr>
<td>openldap</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/openldap:2018.11.0</td>
</tr>
<tr>
<td>pause</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/pause:2018.11.0</td>
</tr>
<tr>
<td>phpldapadmin</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2018.11.0</td>
</tr>
<tr>
<td>postgres</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/postgres:2018.11.0</td>
</tr>
<tr>
<td>prometheus</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2018.11.0</td>
</tr>
<tr>
<td>prometheus_relay</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus_relay:2018.11.0</td>
</tr>
<tr>
<td>pushgateway</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2018.11.0</td>
</tr>
<tr>
<td></td>
<td>Image URL</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>pushkin</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/oss/pushkin:2018.11.0</td>
</tr>
<tr>
<td>qa-tools</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/oss/qa-tools:2018.11.0</td>
</tr>
<tr>
<td>registry</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2018.11.0</td>
</tr>
<tr>
<td>remote_storage_adapter</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2018.11.0</td>
</tr>
<tr>
<td>rundeck</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/oss/rundeck:2018.11.0</td>
</tr>
<tr>
<td>security-monkey-api</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/oss/security-monkey-api:2018.11.0</td>
</tr>
<tr>
<td>security-monkey-scheduler</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/oss/security-monkey-scheduler:2018.11.0</td>
</tr>
<tr>
<td>telegraf</td>
<td>docker-prod-local.artifactory.mirantis.com/openstack-telegraf:2018.11.0</td>
</tr>
<tr>
<td>tiller</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/tiller:2018.11.0</td>
</tr>
<tr>
<td>virtlet</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/virtlet:v1.4.1</td>
</tr>
<tr>
<td>visualizer</td>
<td>docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2018.11.0</td>
</tr>
</tbody>
</table>

1(1, 2, 3, 4, 5), Available in the MCP offline image. For details, see: MCP Reference 6, 7, 8, 9, 10, Architecture: Mirror image content. 11, 12, 13, 14, 15)
## Major components versions

The following tables list the MCP components of the Q3`18 Release Version with Build ID 2018.11.0. 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 versions, which are 2018.8.0 and 2018.8.0-milestone1.

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>2018.8.0</th>
<th>2018.8.0-milestone1</th>
<th>2018.11.0 (current release)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed storage</td>
<td>Ceph</td>
<td>12.2.4-1xenial+mir3</td>
<td>12.2.4-1xenial+mir3</td>
<td>12.2.8-1~u1 6.04+mcp142</td>
<td>Luminous v12.2.4 Release Notes</td>
</tr>
<tr>
<td>DriveTrain</td>
<td>Aptly</td>
<td>1.3.0</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>0.12.11</td>
<td>0.12.11</td>
<td>Resource type - Docker image</td>
</tr>
<tr>
<td>Gerrit</td>
<td></td>
<td>2.13.6</td>
<td>2.13.6</td>
<td>2.13.6</td>
<td>Resource type - Docker image</td>
</tr>
<tr>
<td>jenkins-master</td>
<td></td>
<td>2.121.2, 2.100</td>
<td>2.121.2, 2.100</td>
<td>2.121.2, 2.121.3</td>
<td>Resource type - Docker image. Version 2.121.2 for cfg01, 2.121.3 for CI/CD.</td>
</tr>
<tr>
<td>Component</td>
<td>Version 1</td>
<td>Version 2</td>
<td>Version 3</td>
<td>Resource Type</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
<td>--------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Jenkins pipeline-library</td>
<td>2018.8.0</td>
<td>2018.8.0-mil estone1</td>
<td>2018.11.0</td>
<td>Resource type - Git repository</td>
<td></td>
</tr>
<tr>
<td>Reclass model</td>
<td>1.4.1-1tcp4</td>
<td>1.4.1-1tcp4</td>
<td>1.5.1-1tcp4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salt formulas</td>
<td>2018.8.0</td>
<td>2018.8.0-mil estone1</td>
<td>2018.11.0</td>
<td>Resource type - Git repository</td>
<td></td>
</tr>
<tr>
<td>Hypervisors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>libvirt</td>
<td>4.0.0-1.7~u1 6.04+mcp2</td>
<td>4.0.0-1.7~u1 6.04+mcp2</td>
<td>4.0.0-1.7~u1 6.04+mcp3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>qemu</td>
<td>2.11+dfsg-1.4~u16.04+mcp2</td>
<td>2.11+dfsg-1.4~u16.04+mcp2</td>
<td>2.11+dfsg-1.4~u16.04+mcp2</td>
<td>qemu-kvm</td>
<td></td>
</tr>
<tr>
<td>Kubernetes</td>
<td>1.10.4-4</td>
<td>1.10.4-4</td>
<td>1.11.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viritet</td>
<td>1.1.2</td>
<td>1.1.2</td>
<td>1.4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenContrail</td>
<td>2.2.12, 2.1.20</td>
<td>2.2.12, 2.1.20</td>
<td>2.2.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cassandra</td>
<td>2.11-0.9.0.1-0contrail1, 2.9.2-0.0contrail0</td>
<td>2.11-0.9.0.1-0contrail1, 2.9.2-0.0contrail0</td>
<td>2.11-0.9.0.1-0contrail1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kafka</td>
<td>4.0.4.0, 3.2.11.0</td>
<td>4.0.4.0, 3.2.11.0</td>
<td>4.0.4.0</td>
<td>OpenContrail 3.2 is not supported for new deployments starting Build ID 2018.11.0. OpenContrail 4.0 with OpenStack Queens is available as technical preview.</td>
<td></td>
</tr>
<tr>
<td>OpenStack Pike 2</td>
<td>5.0.0-3~u16.04+mcp0</td>
<td>5.0.0-3~u16.04+mcp0</td>
<td>5.0.0-3~u16.04+mcp0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barbican</td>
<td>11.1.1-2~u1 6.04+mcp77</td>
<td>11.1.1-2~u1 6.04+mcp77</td>
<td>11.1.1-2~u1 6.04+mcp77</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Pike</td>
<td>Queens 2</td>
<td>Pike</td>
<td>Queens 2</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>Designate</td>
<td>5.0.2-2~u16.04+mcp6</td>
<td>5.0.2-2~u16.04+mcp6</td>
<td>5.0.2-2~u16.04+mcp6</td>
<td>For Telemetry</td>
<td></td>
</tr>
<tr>
<td>Glance</td>
<td>15.0.1-1~u16.04+mcp11</td>
<td>15.0.1-1~u16.04+mcp11</td>
<td>15.0.1-1~u16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heat</td>
<td>9.0.4-1~u16.04+mcp31</td>
<td>9.0.4-1~u16.04+mcp31</td>
<td>9.0.4-1~u16.04+mcp31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Horizon</td>
<td>12.0.3-2~u16.04+mcp48</td>
<td>12.0.3-2~u16.04+mcp48</td>
<td>12.0.3-2~u16.04+mcp48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ironic</td>
<td>9.1.4-1~u16.04+mcp29</td>
<td>9.1.4-1~u16.04+mcp29</td>
<td>9.1.4-1~u16.04+mcp29</td>
<td>Technical preview</td>
<td></td>
</tr>
<tr>
<td>Manila</td>
<td>5.0.1-1~u16.04+mcp61</td>
<td>5.0.1-1~u16.04+mcp61</td>
<td>5.0.1-1~u16.04+mcp61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nova</td>
<td>16.1.4-3~u16.04+mcp132</td>
<td>16.1.4-3~u16.04+mcp132</td>
<td>16.1.4-3~u16.04+mcp132</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP VPN</td>
<td>7.0.0-2~u16.04+mcp2</td>
<td>7.0.0-2~u16.04+mcp2</td>
<td>7.0.0-2~u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2 Gateway</td>
<td>11.0.0-1~u16.04+mcp6</td>
<td>11.0.0-1~u16.04+mcp6</td>
<td>11.0.0-1~u16.04+mcp6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networking ODML2 plugin</td>
<td>11.0.5-1~u16.04+mcp133</td>
<td>11.0.5-1~u16.04+mcp133</td>
<td>11.0.5-1~u16.04+mcp133</td>
<td>neutron-plugin-ml2</td>
<td></td>
</tr>
<tr>
<td>Neutron</td>
<td>11.0.5-1~u16.04+mcp133</td>
<td>11.0.5-1~u16.04+mcp133</td>
<td>11.0.5-1~u16.04+mcp133</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Octavia</td>
<td>N/A</td>
<td>N/A</td>
<td>1.0.2-6~u16.04+mcp40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aodh</td>
<td>5.1.0-3~u16.04+mcp10</td>
<td>5.1.0-3~u16.04+mcp10</td>
<td>5.1.0-3~u16.04+mcp10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ceilometer</td>
<td>9.0.5-2~u16.04+mcp16</td>
<td>9.0.5-2~u16.04+mcp16</td>
<td>9.0.5-2~u16.04+mcp16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panko</td>
<td>3.1.0-1~u16.04+mcp11</td>
<td>3.1.0-1~u16.04+mcp11</td>
<td>3.1.0-1~u16.04+mcp11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gnocchi</td>
<td>4.0.5-2~u16.04+mcp2</td>
<td>4.0.5-2~u16.04+mcp2</td>
<td>4.0.5-2~u16.04+mcp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barbican</td>
<td>n/a</td>
<td>n/a</td>
<td>6.0.1-4~u16.04+mcp12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Version</td>
<td>Dependent</td>
<td>MCP</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------</td>
<td>-----------</td>
<td>-----</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>Cinder</td>
<td>n/a</td>
<td>n/a</td>
<td>12.0.4-2~u1 6.04+mcp69</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designate</td>
<td>n/a</td>
<td>n/a</td>
<td>6.0.1-1.0~u1 6.04+mcp16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Glance</td>
<td>n/a</td>
<td>n/a</td>
<td>16.0.1-2~u1 6.04+mcp21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heat</td>
<td>n/a</td>
<td>n/a</td>
<td>10.0.2-1.0~u1 16.04+mcp37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Horizon</td>
<td>n/a</td>
<td>n/a</td>
<td>13.0.1-9~u1 6.04+mcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ironic</td>
<td>n/a</td>
<td>n/a</td>
<td>10.1.6-1.0~u1 16.04+mcp25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keystone</td>
<td>n/a</td>
<td>n/a</td>
<td>13.0.1-3~u1 6.04+mcp18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manila</td>
<td>n/a</td>
<td>n/a</td>
<td>6.0.2-2~u16.04+mcp44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nova</td>
<td>n/a</td>
<td>n/a</td>
<td>17.0.7-6~u1 6.01+mcp90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenStack Networking</td>
<td>BGP VPN</td>
<td>n/a</td>
<td>8.0.1-1.0~u1 6.04+mcp7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queens</td>
<td>L2 Gateway</td>
<td>n/a</td>
<td>12.0.1-1.0~u1 16.04+mcp10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Networking               | Networking | n/a | 12.0.0-1.0~u1 16.04+mcp39 | neutron-plug
<p>| ODL ML2 plugin           | Neutron  | n/a       | 12.0.5-5<del>u1 6.04+mcp62 |
| Octavia                  | n/a     | n/a       | 2.0.2-6</del>u16.04+mcp62 |
| OpenStack Telemetry      | Aodh     | n/a       | 6.0.1-2<del>u16.04+mcp9 |
| Queens                   | Ceilometer | n/a | 10.0.1-2</del>u1 6.04 |
|                          | Panko    | n/a       | 4.0.2-2~u16.04+mcp7 |</p>
<table>
<thead>
<tr>
<th>Component</th>
<th>Application/service</th>
<th>2018.8.0</th>
<th>2018.8.0-milestone1</th>
<th>2018.11.0 (current release)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DriveTrain</td>
<td>MAAS</td>
<td>2.3.3</td>
<td>2.3.3</td>
<td>2.3.5</td>
<td></td>
</tr>
<tr>
<td>SaltStack</td>
<td>2017.7</td>
<td>2017.7</td>
<td>2017.7</td>
<td>2017.7.8</td>
<td></td>
</tr>
<tr>
<td>Kubernetes</td>
<td>Calico</td>
<td>2.6.10</td>
<td>2.6.10</td>
<td>3.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Calico CNI</td>
<td>1.11.6</td>
<td>1.11.6</td>
<td>3.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>etcd</td>
<td>3.3.8</td>
<td>3.3.8</td>
<td>3.3.8</td>
<td></td>
</tr>
<tr>
<td>OpenContrail networking</td>
<td>Redis</td>
<td>2:3.0, 2:2.8</td>
<td>2:3.0, 2:2.8</td>
<td>2:3.0</td>
<td></td>
</tr>
<tr>
<td>StackLight LMA</td>
<td>Alerta</td>
<td>5.2.0</td>
<td>5.2.0</td>
<td>5.6.10</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------</td>
<td>-------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Alertmanager</td>
<td>0.14.0</td>
<td>0.14.0</td>
<td>0.14.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>5.6.9</td>
<td>5.6.9</td>
<td>5.6.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fluentd</td>
<td>1.0.2</td>
<td>1.0.2</td>
<td>1.0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fluentd is included to the td-agent 3.1.1-0 package.</td>
<td></td>
</tr>
<tr>
<td>Grafana</td>
<td>5.1.3</td>
<td>5.1.3</td>
<td>5.2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heka</td>
<td>0.10.1</td>
<td>0.10.1</td>
<td>0.10.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>InfluxDB</td>
<td>1.5.2-1</td>
<td>1.5.2-1</td>
<td>1.5.2-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kibana</td>
<td>5.6.9</td>
<td>5.6.9</td>
<td>5.6.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MongoDB</td>
<td>2.6.10</td>
<td>2.6.10</td>
<td>2.6.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For Alerta</td>
<td></td>
</tr>
<tr>
<td>Prometheus</td>
<td>2.2.1</td>
<td>2.2.1</td>
<td>2.2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pushgateway</td>
<td>0.4.0</td>
<td>0.4.0</td>
<td>0.4.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System</th>
<th>Docker</th>
<th>docker-ce 18.03.1, docker-engine 1.13.1</th>
<th>docker-ce 18.03.1, docker-engine 1.13.1</th>
<th>docker-ce 18.06.1, docker-engine 1.13.1</th>
<th>Version 18.06.1 on StackLight, OpenContrail, and CI/CD nodes, 1.13.1 on Kubernetes nodes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Git</td>
<td>2.7.4</td>
<td>2.7.4</td>
<td>2.7.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GlusterFS</td>
<td>3.8.15</td>
<td>3.8.15</td>
<td>3.8.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAProxy</td>
<td>1.6.3</td>
<td>1.6.3</td>
<td>1.6.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGINX</td>
<td>1.10.3</td>
<td>1.10.3</td>
<td>1.10.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>2.4.40</td>
<td>2.4.40</td>
<td>2.4.40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Galera</td>
<td>25.3.14</td>
<td>25.3.14</td>
<td>25.3.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MySQL</td>
<td>5.6.35</td>
<td>5.6.35</td>
<td>5.6.35</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Base OS</th>
<th>Ubuntu Xenial</th>
<th>Ubuntu Xenial</th>
<th>Ubuntu Xenial</th>
<th>Ubuntu Xenial</th>
</tr>
</thead>
<tbody>
<tr>
<td>2(1, 2)</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4(1, 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5(1, 2, 3, 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6(1, 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For the OpenStack releases support schedule, see MCP OpenStack Releases.
Linux image versions when newer versions of Ubuntu packages are available in the Mirantis repositories, MCP installs them instead of the versions available in the Ubuntu repositories:
- linux-image-virtual-lts-xenial
- linux-image-generic-lts-xenial
- version 4.4.0.116
- linux-image-generic-hwe-16.04 version 4.15.0.36.59
Addressed issues
This section provides the list of the addressed issues in the current MCP release version.

DriveTrain

- Fixed the issue with the definition missing for Gerrit SSH on port 29418, which caused only Gerrit being exposed through prx0[1-2].
- Fixed the restoring of the MySQL database using Xtrabackup failing in the offline mode with the following error message: tar: qpress-11-linux-x64.tar: Cannot open: No such file or directory.
- Fixed the issue with network interface controllers (NICs) with some specific configurations failing to automatically apply the changes. Now, changes to the NIC configuration apply without the need to reboot the cmp nodes.
- Fixes the issue with the Deploy - OpenStack job failing on the linux.system.file state with the 404 error when trying to fetch the qcow2 images from http://images.mirantis.com/.
- Fixed a typo in cloud-update.groovy that caused the Deploy - update cloud pipeline fail with the groovy.lang.MissingPropertyException: No such property: True for class: WorkflowScript error message.
- Fixed the following CVP pipelines issues:
  - The issue with the CVP performance, functional, and HA tests pipelines using Keystone API v2 only. Now, the pipelines can use either Keystone API v2 or v3.
  - The issue with the CVP HA tests pipeline failing to stop if a Tempest test run fails.
- Fixed the issue with the Deploy - OpenStack occasionally failing with the SaltInvocationError: ca_server did not respond salt master must permit peers to call the sign_remote_certificate function error message.

OpenStack

- Fixed the issue with Ceilometer having no permissions to publish events to Panko.
- Fixed the issue with the Neutron port containing an outdated host information in case of evacuation failure.
- Fixed a number of security issues by updating Django, QEMU, and the python-cryptography package.
- Removed the deprecated Ceilometer API to avoid unnecessary log messages about database connectivity failures for the OpenStack Pike and newer versions deployments.
- Fixed the issue that caused an OVS port remain in br-int if spawning an instance on a new host during the host evacuation fails.
- Fixed the incorrect version of the Keystone endpoint located in Horizon in the OpenRC v2 and v3 file for OpenStack Pike.
• Fixed the issue with the RabbitMQ three-node cluster stopping to receive connection after approximately five minutes of processing messages from services and a huge number of agents. The issue affected MCP clusters containing one thousand or more compute nodes.

• Fixed the issue with Xtrabackup cron job for MySQL that caused the database being not available for other MCP cluster activities.

• Fixed the issue in the ceph-backup-runner.sh backup rotation script that was trying to remove backup directories instead of files.

• Fixed the issue with the ceilometer-agent-notification service hanging up after some period of time after deployment, with no logs written to /var/log/ceilometer/ceilometer-agent-notification.log, no new samples being collected and sent to Gnocchi, and no Aodh alarms targeting such samples.

Kubernetes

• Fixed the issue with the Kubernetes Nodes (cmp) autogeneration supporting up to 155 nodes only.

• Fixed the Artifactory availability issue that might appear when deploying a Kubernetes cluster without access to Mirantis internal network using the Deploy - OpenStack Jenkins pipeline job.

• Fixed the issue with the Kubernetes dashboard being not accessible due to the role-based access control being not supported by default in the Kubernetes dashboard.

OpenContrail

• Fixed the issue with the deployment of Kubernetes 1.10 with OpenContrail 4.0 that caused the Kubernetes Nodes to have the apt_mk_version=stable MCP version instead of the Build ID.

• Fixed the issue with updating a subnet in Horizon failing with the Bad subnet request error message.

• Fixed the issue with OpenContrail v3.2 that caused the inability to create a load balancer and assign an IP address to it.

• Fixed the issue with the Deploy - upgrade Opencontrail to 4.x Jenkins pipeline job failing to start the vRouter on cmp nodes.

• Fixed the issue with failure to assign a floating IP to a VIP if the floating IP was created after the VIP allocation. The issue affected OpenContrail v3.x.

• Fixed the issue with the conformance tests from the StatefulSetBasic set failing if the concurrency was more than the number of compute nodes. The issue caused the logs inside pods to contain network outage messages. The issue affected the MCP clusters with OpenContrail 4.0 and Kubernetes 1.1x.

• Fixed the issue with the old package versions remaining on the ntw and nal nodes after upgrade of OpenContrail from v3.2 to v4.0. This caused both versions of the services trying to open the same network ports after the node reboot.
• Fixed the issue with inability to create networks with custom network policies in Horizon when using OpenContrail v4.0 and OpenStack Ocata.

• Fixed the issue with some OpenContrail services being inactive after on one of the analytic nodes after deploying OpenContrail v4.0.

• Fixed the issue with unnecessary packages being installed during the deployment of Kubernetes with OpenContrail v4.0, which caused Kubernetes cluster outage.

• Fixed the issue with reaching the Kubernetes master API with a port exposed through a load balancer with an associated floating IP.

Networking

• Fixed the issue with VMs failing to obtain an IP address due to missing Open vSwitch VXLAN flows.

• Fixed the issue with the Open vSwitch flows missing after the restart of the Open vSwitch agents.

• Fixed the issues with the RabbitMQ cluster causing a number of report and queue-related issues after the restart of the msg node.

StackLight LMA

• Fixed the issue with the status panels in the Heat Grafana dashboard displaying no data.

• Fixed the issue with Fluentd failing to start if Barbican is installed.

• Fixed a typo in medium.yml causing the creation of two log02 nodes, one on kvm02 and the correct one on kvm11.

• Implemented the possibility to modify header_timeout and client_timeout to fix the issue with default timeouts for the input.rabbitmq plugin blocking the system from receiving the RabbitMQ status in StackLight LMA.

• Fixed the issue with Telegraf failing to gather metrics from an OpenStack region in case of multiple regions configured. Now, you can specify the required region using the region = “RegionOne” parameter.

• Increased the scrape interval and timeout for Prometheus long-term storage to fix the issue with metrics not being collected in case of large clouds. Now, the scrape interval and timeout are set to 30 seconds by default.

• Fixed the data collection point for requests per seconds for the OpenContrail API and discovery services.

• Fixed the issue with redundant HaproxyBackednOutage alert firing for the contrail_collector_stats, contrail_config_stats, and contrail_openstack_stats nodes in case of HaProxy being used for load balancing.

• Fixed the calculation of instances and tenants in Gainsight.

• Fixed the issue with the Push Notifications service incorrectly handling the converted cases.

• Fixed the issue with Fluentd failing to parse the contrail-vrouter-nodemgr-stderr.log log file.
• Fixed the issue with the MySQL wsrep logs sent to syslog being represented with the ERROR severity.

• Fixed the issue with the inability to override the remote_agent parameters.

• Fixed the issue with the Telegraf remote agent failing to gather some of the OpenStack metrics and responding with the Unable to extract hypervisors: unexpected end of JSON input error message.

• Fixed the issue with the Telegraf input plugin using a significant amount of time to collect the OpenStack metrics.

• Fixed the issue with the Keepalived Grafana dashboard displaying incorrect data.

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

- 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.

- If the Gerrit container is recreated, the Jenkins update service config build fails with the WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! warning during the git fetch step for obtaining the upstream libraries. The issue occurs because of the old entries in the /var/jenkins_home/.ssh/known_hosts file.
  Workaround:
  1. Log in to the Jenkins Master container.
  2. Delete the old entry of ssh-keygen in /var/jenkins_home/.ssh/known_hosts.

- During the upgrade of an MCP cluster, the Linux kernel headers may not be installed by default.
  Workaround:
  Verify that you have the latest linux-headers installed on the kvm, cmp, and other hardware nodes. Use the example below where cmp10. is a set of nodes.
  Example:

  # Check that the command will be applied to only needed nodes
  salt -E "cmp10." test.ping
  # Perform the upgrade
  salt -E "cmp10." cmd.run "export DEBIAN_FRONTEND=noninteractive && apt-get \
  update & & apt-get -y -o \n  Dpkg::Options::="--force-confdef" -o Dpkg::Options::="--force-confnew" \n  install linux-headers-generic linux-headers-$\(uname -r\) linux-headers-generic-hwe-16.04"

- 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:

    systemctl restart salt-api.service

3. Rerun the Deploy - update cloud pipeline.

• While upgrading the MCP Build ID from 2018.8-milestone1 to 2018.11, the salt-formula-octavia cannot be updated with the No such file or directory error.

   Workaround:
   1. Log in to the Salt Master node.
   2. Run the following commands:

       apt-get update
       apt-get remove --purge salt-formula-octavia && apt-get install salt-formula-octavia

3. Rerun the Deploy - upgrade MCP DriveTrain pipeline.

• 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.

**OpenStack**

• The OpenStack services perform log rotation on a daily basis. By default, an MCP OpenStack deployment keeps four log rotations, meaning that the OpenStack logs are being kept for four days only, which may prevent from investigating the issues in details.

   Workaround:
   1. Open your Git project repository with the Reclass model on the cluster level.
   2. In /classes/cluster/<cluster_name>/infra/init.yml, add the following pillar specifying the number of rotations to keep using the keep_rotate parameter:
The Keystone catalog contains deprecated Cinder API v1 endpoints, which raises the CinderApiDown alert.

**Workaround:**

1. Upgrade your MCP cluster to the latest supported Build ID as described in [MCP Deployment Guide: Upgrade an MCP cluster](#).
2. Log in to any OpenStack controller node.
3. Remove the Cinder API v1 endpoints from the catalog:

   ```
source /root/keystonercv3
openstack endpoint list --service cinder -f value -c ID | xargs -I {} \ 
openstack endpoint delete {}  
```

The Designate Tempest test may fail when a small number of Designate quota zones is configured.

**Workaround:**

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `openstack/control.yml`, increase the Designate quota using the `designate_quota_zones` parameter:

   ```
parameters:
  _param:
    designate_quota_zones: <NUMBER>
  designate:
    server:
      quota:
        zones: ${_param:designate_quota_zones}
```

Replace `<NUMBER>` with the desired Designate zones quota. For example, 100 is enough for the Designate Tempest tests to pass. If not set, the default value is 10.

3. From an OpenStack controller node, run the following state:
When using SSL for the Designate, Glance, Heat, Keystone, Nova, Manila, and Neutron services, the HTTP checks may fail since this feature requires a specific HAProxy configuration. As a result, without additional HAProxy configuration, only TCP health checks are being performed while the service itself may be in the error state. The workaround is to manually enable the HTTPS checks.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. Specify the check parameters below in the configuration files of your OpenStack environment services as required. The files location depends on the location of the certain HAProxy services. For example:
   - `/openstack/control.yml` for the core services
   - `/openstack/share.yml` for the Manila services
   - `/openstack/barbican.yml` for the Barbican services
   - `/openstack/telemetry.yml` for the Tenant Telemetry services

   For example, for the designate and Keystone public API HAProxy back ends, specify:

   ```
   haproxy_designate_check_params: check inter 10s fastinter 2s downinter 3s \n   rise 3 fall 3 check-ssl verify none
   haproxy_keystone_public_api_check_params: check inter 10s fastinter 2s \n   downinter 3s rise 3 fall 3 check-ssl verify none
   ```

3. In the same files, set the HAProxy options:

   ```
   haproxy_http_check_options:
   - httpchk GET /
   - httpclose
   - tcplog
   ```

   As a result, the HAProxy listen section should look as follows:

   ```
   haproxy:
   proxy:
   listen:
   designate_api:
   type: ~
   options: ${_param:haproxy_http_check_options}
   keystone_public_api:
   type: ~
   options: ${_param:haproxy_http_check_options}
   ```
Note
The Nova placement API service in OpenStack Pike returns 401 instead of 200. This is an expected behavior. Verify that the pillar includes the corresponding settings.

4. Log in to the Salt Master node.

5. Update the HAProxy configuration and restart the HAProxy service:

   ```bash
salt -C 'I@haproxy:proxy' state.apply haproxy
   ```

   Once done, HAProxy will use layer 7 health checks to determine if a service is up and running.

   • The Redis server for Gnocchi does not require authentication. The workaround is to manually configure authentication for Redis.

   Workaround:

   1. Open your Git project repository with the Reclass model on the cluster level.
   2. In `/classes/cluster/<cluster_name>/openstack/telemetry.yml`, specify the following parameters:

   ```yaml
   parameters:
   openstack_telemetry_redis_password: 'my_secret_password'
   openstack_telemetry_redis_url: ...nel_fallback=${_param:redis_sentinel_node02_address}:26379&sentinel_fallback=${_param:redis_sentinel_node03_address}:26379
   redis:
   cluster:
   password: ${_param:openstack_telemetry_redis_password}
   ```

   Note
   Generate a strong password. For details, see Auth password.

3. Log in to the Salt Master node.

4. Refresh pillars:

   ```bash
   salt -C 'I@redis:server' saltutil.pillar_refresh
   ```

   Note
   While switching to auth in Redis, a glitch in metrics gathering occurs. Some new samples can be lost.

5. Apply the redis states:
6. Apply the following states:

```
salt -C 'I@redis:cluster:role:master' state.sls redis
salt -C 'I@redis:cluster:role:slave' state.sls redis
```

7. Verify the authentication by connecting to a Redis node. For example:

```
redis-cli -h [redis_node_ip] -p 6379
```

Execute:

```
10.11.0.98:6379> KEYS *
```

The output should include the (error) NOAUTH Authentication required. error message.

- 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. Apply the Salt formula patch to your Barbican Salt formula.
2. On every OpenStack controller node where Barbican API is installed, add the following configuration to /etc/barbican/policy.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.

3. Log in to the Salt Master node.
4. 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.
In the Queens-based OpenStack deployments with Telemetry, Gnocchi may contain many errors in the metricd logs. For example:

```
ERROR gnocchi.cli.metricd: Error while listening for new measures notification, retrying
Traceback (most recent call last):
  File "/usr/lib/python2.7/dist-packages/gnocchi/cli/metricd.py", line 185,
in _fill_sacks_to_process
  for sack in self.incoming.iter_on_sacks_to_process():
    File "/usr/lib/python2.7/dist-packages/gnocchi/incoming/redis.py", line 122,
in iter_on_sacks_to_process
    db = self._client.connection_pool.connection_kwargs['db']
  KeyError: 'db'
```

But these errors do not affect the Gnocchi service functionality and its testing does not detect any failures.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `openstack/telemetry.yml`, modify the `openstack_telemetry_redis_url` parameter as follows:

   ```yaml
   openstack_telemetry_redis_url: ...
el_fallback=${_param:redis_sentinel_node02_address}:26379&sentinel_fallback=${_param:redis_sentinel_node03_address}:26379
   ```
3. Log in to the Salt Master node.
4. Reapply the following states:

   ```
salt 'mdb*' saltutil.pillar_refresh
salt 'mdb*' state.sls aodh
salt 'mdb*' state.sls ceilometer
salt 'mdb*' state.sls gnocchi
   ```

The maximum size of a Glance image is limited to 30 GB on the system level of the Reclass model in `nginx/server/proxy/openstack/glance.yml`.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `openstack/proxy.yml`, add the following parameters under `nginx:server:site`:

   ```yaml
   ... 
   nginx_proxy_openstack_api_glance:
     proxy:
       request_buffer: false
       size: 100000m
   ```
On the OpenStack Pike or Queens-based environments with a custom interfaces configuration, the OVS network configuration is not always applied after rebooting a node. It may result in the Exhausted all hosts available error for build instances.

As a workaround, after rebooting a node, apply the linux.network state to restore network configuration.

If the gtw01 node is rebooted, the ohm port moves to the DOWN state. It affects creation of new load balancers.

Workaround:
1. Log in to the Salt Master node.
2. Apply the following state for the gtw01 node where the Octavia manager is located:

   ```
salt -C 'I@octavia:manager' state.sls octavia.manager
   ```

On the OpenStack Pike 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 load balancer stucks in the PENDING_UPDATE or PENDING_DELETE state.

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

   ```
   openstack loadbalancer list | awk '/ PENDING_CREATE / {print $2}
   ```
3. Log in to any dbs node.
4. Log in to the MySQL database:

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

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

On the OpenStack Pike 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:

1. Manually stop the Octavia controller services (octavia-health-manager, octavia-housekeeping, octavia-worker) on the affected node.
2. Open your Git project repository with the Reclass model on the cluster level.
3. 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}
   ```

4. Log in to the Salt Master node.
5. 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
   ```

6. For the `gtw` node where you moved the Octavia services, apply the Octavia states. For example:

   ```bash
   salt 'gtw02*' state.sls octavia
   salt 'gtw02*' state.sls salt.minion.ca
   salt 'gtw02*' state.sls salt.minion.cert
   ```

The Deploy - OpenStack deployment pipeline fails when the LDAP integration for Keystone is enabled. The issue affects the OpenStack Pike and Queens releases.

Workaround:

1. Log in to the Salt Master node.
2. Proceed with one of the following:
   - For OpenStack Pike:
     1. Verify that the LDAP integration for Keystone is disabled. For details, see MCP Deployment Guide: Configure LDAP with Keystone server.
     2. Run the Deploy - OpenStack deployment pipeline.
3. Once successfully deployed, enable the LDAP integration for Keystone as described in MCP Deployment Guide: Configure LDAP with Keystone server.

4. Apply the following state for the OpenStack controller nodes:

```bash
salt -C 'I@keystone:server' state.apply keystone.server -b 1
```

- For OpenStack Queens:
  1. Apply the patch 32250 and patch 32251 to your Keystone Salt formula.
  2. Run the Deploy - OpenStack deployment pipeline.
  3. Once successfully deployed, manually create a domain as described in Create a domain.

**Kubernetes**

- On the Kubernetes clusters with ExternalDNS, if a cluster or domain name contains the `_` symbol, the DNS cluster may not work correctly. As a workaround, replace `_` with `-` in your cluster and domain names.

**OpenContrail**

- Dynamic Kernel Module Support fails to build DPDK kernel modules for OpenContrail v3.2 on kernels newer than v4.8. The workaround is to use DPDK libraries v17.02 instead of v2.1.

- OpenContrail v3.2 API server connection timeouts may occur due to an issue with the internal IF-MAP. The workaround is to use the Java-based irond IF-MAP.

- During the upgrade of OpenContrail from v3.2 to v4.0, the Deploy - upgrade Opencontrail to 4.x pipeline fails due to ZooKeeper failing to connect to Kafka on all analytics nodes. This causes some services stuck in the initializing state, for example:

```text
contrail-collector: initializing
contrail-analytics-api: initializing (UvePartitions:UVE-Aggregation[None], Collector connection down)
contrail-alarm-gen: initializing (Collector, Zookeeper:AlarmGenerator[Connection time-out] connection down)
```

Workaround:

1. Restart ZooKeeper on all analyticsdb containers.
2. Once ZooKeeper is up and running, restart the services that are stuck.
3. Rerun the Deploy - upgrade Opencontrail to 4.x pipeline.

- After upgrading an MCP cluster, network connection timeouts may occur when using the Link-Local Services (LLS). The issue appears due to the recreation of the global-vrouter-config OpenContrail pillar model with a different name. This leads to the presence of two opposite global-vrouter-config objects created for a single system configuration. The Link-local services are configured for default-global-vrouter-config and
an opposite configuration of a vRouter removes the Link-local service entries from the OpenContrail agents.

Workaround:

1. From an OpenContrail controller node, obtain a list of running global vRouter configurations:

   ```
salt-call contrail.global_vrouter_config_list
   ```

2. If more than one configuration is listed, remove all vRouter configurations except for default-global-vrouter-config:

   ```
salt-call contrail.global_vrouter_config_delete <global-vrouter-config-name>
   ```

3. Restart the contrail-control services on every node one by one:

   ```
service contrail-control restart
   ```

   • After upgrading an MCP cluster, the contrail-vrouter-agent may not start with the Module vrouter not found in directory /lib/modules/XXX error. The issue occurs due to the missing Linux kernel headers required by the contrail-vrouter-dkms module.

     Since the Linux kernel headers are necessary for MCP upgrade, this issue relates to any MCP upgrade procedure that contains the apt-get dist-upgrade step.

     Workaround:

     Verify that you have the latest linux-headers installed on the kvm, cmp, and other hardware nodes. Use the example below where cmp10. is a set of nodes.

     Example:

     ```
     # Check that the command will be applied to only needed nodes
     salt -E "cmp10." test.ping
     # Perform the upgrade
     salt -E "cmp10." cmd.run "export DEBIAN_FRONTEND=noninteractive && apt-get \
     update && apt-get -y -o \n     Dpkg::Options::="--force-confdef" -o Dpkg::Options::="--force-confnew" \n     install linux-headers-generic linux-headers-$\{uname -r\} linux-headers-generic-hwe-16.04"
     ```

     • 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.
In the OpenContrail 4.0 deployments, the OpenContrail web UI displays erroneous critical alarms for the failed Cassandra database on all ntw nodes. The issue occurs due to the contrail-database-nodemgr service that is absent in the opencontrail_controller container. The issue affects the OpenContrail controller node UVE status that is not propagated to the OpenContrail collector.

Workaround:

1. Log in to the opencontrail_controller container on any ntw node.
2. Verify the actual status of the Cassandra database:

   ```
   nodetool status
   ```
3. Choose from the following options:
   - If the database is up and running, disregard the critical alarms in the OpenContrail web UI.
   - If the database is down on either of the ntw nodes, contact Mirantis support to resolve the issue.
   - The OpenContrail v4.0 logs from zookeeper/zookeeper.log and cassandra/system.log logs are missing in Kibana.

Workaround:

1. Log in to the Salt Master node.
2. Create `/var/log/analyticsdb/cassandra` and `/var/log/analyticsdb/zookeeper` for every nal node:

   ```
   salt 'nal*' file.mkdir /var/log/analyticsdb/cassandra
   salt 'nal*' file.mkdir /var/log/analyticsdb/zookeeper
   ```
3. Create `/var/log/configdb/cassandra` and `/var/log/configdb/zookeeper` for every ntw node:

   ```
   salt 'ntw*' file.mkdir /var/log/configdb/cassandra
   salt 'ntw*' file.mkdir /var/log/configdb/zookeeper
   ```
4. Change the Cassandra logging directory owner to the Cassandra user on the nal and ntw nodes:

   ```
   salt 'nal*' cmd.run "chown \$(echo \$(doctrail analyticsdb 'id -u cassandra'))\n:\$(doctrail analyticsdb 'id -G cassandra')) /var/log/analyticsdb/cassandra"
   salt 'ntw*' cmd.run "chown \$(echo \$(doctrail controller 'id -u cassandra'))\n:\$(doctrail controller 'id -G cassandra')) /var/log/configdb/cassandra"
   ```
5. In your project Git repository with Reclass model, add the following snippets to classes/cluster/<cluster_name>/opencontrail/analytics.yml and classes/cluster/<cluster_name>/opencontrail/control.yml:

```yaml
parameters:
  _param:
fluentd:
  agent:
    config:
      label:
        cassandra_zookeeper:
          input:
            tail_cassandra_v4_log_files:
              type: tail
              path:
                - /var/log/configdb/cassandra/*.log
                - /var/log/analyticsdb/cassandra/*.log
              tag: temp.cassandra
              pos_file: "$(fluentd:agent:dir:positiondb)/cassandra_v4.pos"
              path_key: log_location
              parser:
                type: multiline
                format: '/(?<Timestamp>[0-9]{4}-[0-9]{2}-[0-9]{2}\s[0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3})\s+-\s+(?<java_severity_label>[A-Z]*)\s+-\s+(?<Payload>.*)/'
                format_firstline: '/^[0-9]{4}-[0-9]{2}-[0-9]{2}\s[0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3}/'
                time_key: Timestamp
                keep_time_key: false
                time_format: '%Y-%m-%d %H:%M:%S,%N'
          tail_zookeeper_v4_log_files:
            type: tail
            path:
              - /var/log/configdb/zookeeper
              - /var/log/analyticsdb/zookeeper
            tag: opencontrail.zookeeper
            pos_file: "$(fluentd:agent:dir:positiondb)/zookeeper_v4.pos"
            parser:
              type: multiline
              format: '/(?<Timestamp>[0-9]{4}-[0-9]{2}-[0-9]{2}\s[0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3})\s+-\s+(?<java_severity_label>[A-Z]*)\s+(?<Payload>.*)/'
              format_firstline: '/^[0-9]{4}-[0-9]{2}-[0-9]{2}\s[0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3}/'
              time_key: Timestamp
              keep_time_key: false
              time_format: '%Y-%m-%d %H:%M:%S,%N'

opencontrail:
  ...
  database:
    logdirs:
      - /var/log/analyticsdb/cassandra
      - /var/log/analyticsdb/zookeeper
  ...
  control:
    role: $(._param:opencontrail_node_role)
    logdirs:
      - /var/log/configdb/cassandra
      - /var/log/configdb/zookeeper
  ...
  docker:
    client:
      compose:
        opencontrail:
          status: up
          pull: true
          service:
            controller:
              image: $(._param:opencontrail_controller_image)
              container_name: $(._param:opencontrail_controller_container_name)
              volumes:
                - /var/log/configdb/cassandra/var/log/cassandra
                - /var/log/configdb/zookeeper/var/log/zookeeper
            analyticsdb:
              image: $(._param:opencontrail_analyticsdb_image)
              container_name: $(._param:opencontrail_analyticsdb_container_name)
              volumes:
                - /var/log/analyticsdb/cassandra/var/log/cassandra
                - /var/log/analyticsdb/zookeeper/var/log/zookeeper

6. Reapply the following states for every ntw and nal node:

```
salt -C 'ntw*' or nal* state.sls docker.client.compose
salt -C 'ntw*' or nal* state.sls fluentd
```
• In the OpenContrail 4.0 deployments, after restoring a Zookeeper database, contrail-control may be inactive on all ntw nodes due to an issue with permissions for certificates.

Workaround:

1. Log in to any OpenContrail controller node.
2. Change permissions:

   ```
   chown -R contrail:contrail /etc/contrail
   ```

• The access to DNS servers is not configured on compute nodes for OpenContrail 4.0 causing the ContrailVrouterDNSXMPPSessionsZero StackLight LMA alerts.

Workaround:

1. Log in to the Salt Master node.
2. Apply the fix patch to your OpenContrail Salt formula in
   ```
   salt-formulas/opencontrail/etc/contrail/contrail-vrouter-agent.conf.
   ```
3. Apply the following states:

   ```
   salt-call saltutil.sync_all
   salt 'cmp*' state.sls opencontrail.compute
   ```

   Warning
   Next time you update the OpenContrail Salt formula, verify whether it already contains the above fix patch. If not, reapply the above changes after the Salt formula update.

• In OpenContrail 3.2, the contrail-vrouter-agent service cannot connect to the contrail-control and contrail-dns services because it uses the vhost0 IP as a source IP for connection. The following error occurs in the output of the contrail-status command:

   ```
   == Contrail vRouter ==
   ...
   contrail-vrouter-agent initializing (XMPP:control-node:10.11.0.224, XMPP:control-node:10.11.0.226, XMPP:dns-server:10.11.0.225, XMPP:dns-server:10.11.0.226 connection down, No Configuration for self)
   ...
   ```

Workaround:
1. Log in to any vRouter node (usually cmp*).
2. In contrail-vrouter-agent.conf, find the VIRTUAL-HOST-INTERFACE section.
3. In this section, uncomment the compute_node_address line and specify the correct source IP address for connection to contrail-control and contrail-dns services. For example:

```
# List of IP addresses assigned for the compute node other than vhost. Specify this only if vhost interface is un-numbered in host-os. Agent will use one of the compute_node_address to run services that need IP Address in host-os (like metadata...)
compute_node_address = 10.204.216.28
```

4. Repeat the above steps on the remaining vRouter nodes.

**StackLight LMA**

- The GlusterFS service host for Kubernetes-based clusters refers to a wrong node. As a result, Telegraf fails to gather metrics from GlusterFS.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `/classes/cluster/<cluster_name>/kubernetes/init.yml`, replace the following parameter:

```
  glusterfs_service_host: ${_param:kubernetes_control_node03_address}
```

with:

```
  glusterfs_service_host: ${_param:infra_kvm_address}
```

3. Log in to the Salt Master node.
4. Apply the following state:

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

- The Gainsight integration service may not operate properly due to an issue with the Gainsight Docker image. The workaround is to use the newer available image.

Workaround:

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

```
parameters:
  _param:
```

3. Log in to the Salt Master node.

4. Refresh Salt pillars:

   ```
   salt -C '*' saltutil.refresh_pillar -t 2
   ```

5. Apply the new Docker image for Gainsight:

   ```
   salt -C 'I@docker:swarm:role:master' state.sls docker.client
Deprecation notes

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

- Global artifact migration
- Deprecation notes for the model structure
- Deprecation notes for Salt formulas
- Deprecation notes for Jenkins pipeline jobs
- Deprecation notes for operations

Global artifact migration

Starting from the MCP Build ID 2018.4.0, MCP is being migrated to a new mirror structure at http://mirror.mirantis.com. Each release version partially updates the system mirror references as described in Deprecation notes for the model structure. The 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>Affected structure</th>
<th>Details</th>
</tr>
</thead>
</table>
The repo_local directory has been migrated and collapsed into the repo directory under linux/system/.

The list of the classes migrated and deprecated since the MCP 2018.7.0 release include:

- linux/system/repo_local/mcp/apt_mirantis/influxdb.yml
- linux/system/repo_local/mcp/apt_mirantis/docker_legacy.yml
- linux/system/repo_local/mcp/apt_mirantis/maas.yml
- linux/system/repo_local/mcp/apt_mirantis/cassandra.yml
- linux/system/repo_local/mcp/apt_mirantis/glusterfs.yml
- linux/system/repo_local/mcp/apt_mirantis/docker.yml
- linux/system/repo_local/mcp/apt_mirantis/saltstack.yml
- linux/system/repo_local/mcp/apt_mirantis/ubuntu.yml
- linux/system/repo_local/mcp/apt_mirantis/saltstack_2016_3.yml

The list of the classes migrated to linux/system/repo/mcp/apt_mirantis/elastic/init.yml and deprecated include:

- linux/system/repo/mcp/apt_mirantis/elastic/2x.yml (deprecated since the MCP 2018.7 release)
- linux/system/repo/mcp/apt_mirantis/elastic/5x.yml (deprecated since the MCP 2018.7 release)
- linux/system/repo/mcp/apt_mirantis/grafana.yml (deprecated since the MCP 2018.8.0 release)

The linux/system/repo/mcp/apt_mirantis/saltstack_2016_3.yml class has been migrated to the linux/system/repo/mcp/apt_mirantis/saltstack.yml class and deprecated since the MCP 2018.7 release

---

**Deprecation notes for Salt formulas**

<table>
<thead>
<tr>
<th>Affected Salt formula</th>
<th>Details</th>
</tr>
</thead>
</table>

©2020, Mirantis Inc.
<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cinder</td>
<td>The cinderng module is deprecated in favor of the cinderv3 module</td>
</tr>
<tr>
<td>glance</td>
<td>The glanceng module is deprecated in favor of the glancev2 module</td>
</tr>
<tr>
<td>heat</td>
<td>The heat module is deprecated in favor of the heatv1 module</td>
</tr>
<tr>
<td>ironic</td>
<td>The ironicng module is deprecated in favor of the ironicv1 module</td>
</tr>
<tr>
<td>keystone</td>
<td>The keystoneng module is deprecated in favor of the keystonev3 module</td>
</tr>
<tr>
<td>neutron</td>
<td>The neutronng module is deprecated in favor of the neutronv2 module</td>
</tr>
<tr>
<td>nova</td>
<td>The novang module is deprecated in favor of the novav21 module</td>
</tr>
</tbody>
</table>

## Deprecation notes for Jenkins pipeline jobs

<table>
<thead>
<tr>
<th>Affected pipeline job</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy - Rollout change</td>
<td>Removed from the mk-pipelines repository and the system Reclass model as deprecated. The related Reclass class is system.jenkins.client.job.deploy.rollout.</td>
</tr>
<tr>
<td>Git - Merge branches Deploy - Test services in environment</td>
<td>Removed from the mk-pipelines repository and the system Reclass model as deprecated. The related Reclass class is system.jenkins.client.job.deploy.test.</td>
</tr>
<tr>
<td>Deploy - update Salt environment</td>
<td>Removed from the system Reclass model only. The related Reclass class is system.jenkins.client.job.deploy.update.update_salt_environment. The corresponding Groovy files are still present in the mk-pipelines repository and will be removed completely in next releases.</td>
</tr>
<tr>
<td>Kafka demo</td>
<td>Removed from the system Reclass model only. The related Reclass class is system.jenkins.client.job.deploy.lab.demo. The corresponding Groovy files are still present in the mk-pipelines repository and will be removed completely in next releases.</td>
</tr>
</tbody>
</table>

## Deprecation notes for operations
## Deprecation notes for operations

<table>
<thead>
<tr>
<th>Affected component</th>
<th>Operation</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ceph</td>
<td>Decapod operations</td>
<td>Removed as deprecated from the system Reclass model. The Decapod operations related Reclass classes start with the <code>system.jenkins.client.job.decapod</code> prefix.</td>
</tr>
<tr>
<td>OpenStack</td>
<td>Barbican Certificate Orders and Certificate Authorities API</td>
<td>Since OpenStack Ocata, the Barbican certificate provisioning API is deprecated. The system Reclass model is not affected. However, Mirantis recommends provisioning TLS certificates using the Certification Authority specific tools rather than the Barbican API. Externally provisioned certificates can still be stored and managed using Barbican.</td>
</tr>
<tr>
<td>GlusterFS</td>
<td>Fernet keys storage in OpenStack</td>
<td>Due to a big number of observed issues, MCP removed the possibility of storing fernet keys in GlusterFS. Now, the fernet keys should be stored in separate directories on each server and are automatically synchronized using the rsync utility from the first OpenStack controller node.</td>
</tr>
</tbody>
</table>