

MCP Q4`18 Release Notes

version q4-18

Copyright notice

2025 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 and 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.

Learn more

[MCP Operations Guide: Restore a Galera cluster automatically](#)

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.

Learn more

[MCP Deployment Guide: Partitioning of a VCP node](#)

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

DOCUMENTATION TECHNICAL PREVIEW

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, and 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 ²

- 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 ¹
- Kibana from version 5.6.12 to 6.5.2 ¹

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](#)

- 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.

Storage

- Ceph update to a minor version
 - Native Prometheus support
-

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

Type	Artifact	Path for Build ID 2019.2.0
Mirantis apt/deb packages	Extra packages	deb http://mirror.mirantis.com/2019.2.0/extra/xenial xenial main ³ deb http://mirror.mirantis.com/2019.2.0/extra/trusty trusty main
	Ceph	deb http://mirror.mirantis.com/2019.2.0/ceph-luminous/xenial xenial main ³
	OpenContrail packages	deb http://mirror.mirantis.com/2019.2.0/opencontrail-3.2/ xenial xenial main deb http://mirror.mirantis.com/2019.2.0/opencontrail-3.2/ trusty trusty main deb http://mirror.mirantis.com/2019.2.0/opencontrail-4.0/ xenial xenial main deb http://mirror.mirantis.com/2019.2.0/opencontrail-4.1/ xenial xenial main

	OpenStack packages	<p>deb http://mirror.mirantis.com/2019.2.0/openstack-mitaka/xenial xenial main</p> <p>deb http://mirror.mirantis.com/2019.2.0/openstack-ocata/xenial xenial main</p> <p>deb http://mirror.mirantis.com/2019.2.0/openstack-pike/xenial xenial main³</p> <p>deb http://mirror.mirantis.com/2019.2.0/openstack-queens/xenial xenial main³</p> <p>deb https://mirror.mirantis.com/update/2019.2.0/openstack-pike/xenial xenial main⁴</p>
	Salt formulas packages ³	http://mirror.mirantis.com/2019.2.0/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	<p>http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5</p> <p>http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2</p>
	MCP apt01 offline image	<p>http://images.mirantis.com/mcp-offline-image-2019.2.0.qcow2.md5</p> <p>http://images.mirantis.com/mcp-offline-image-2019.2.0.qcow2</p>
	VCP Ubuntu 16.04 image ³	<p>http://images.mirantis.com/ubuntu-16-04-x64-mcp2019.2.0.qcow2.md5</p> <p>http://images.mirantis.com/ubuntu-16-04-x64-mcp2019.2.0.qcow2</p>
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	<p>deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main</p> <p>deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main³</p>
	Docker	deb http://mirror.mirantis.com/2019.2.0/docker/xenial xenial stable ³
	Elastic	<p>deb http://mirror.mirantis.com/2019.2.0/elasticsearch-5.x/xenial stable main³</p> <p>deb http://mirror.mirantis.com/2019.2.0/elasticsearch-6.x/xenial stable main³</p> <p>deb http://mirror.mirantis.com/2019.2.0/elasticsearch-curator/xenial stable main</p> <p>deb http://mirror.mirantis.com/2019.2.0/elasticsearch-curator-5/xenial stable main³</p>

	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³
	GlusterFS	deb http://mirror.mirantis.com/2019.2.0/glusterfs-3.8/xenial xenial main ³
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/2019.2.0/maas/xenial xenial main ³
	Percona	deb http://mirror.mirantis.com/2019.2.0/percona/xenial xenial main ³
	SaltStack packages	deb http://mirror.mirantis.com/2019.2.0/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/2019.2.0/saltstack-2017.7/xenial xenial main ³
	Upstream Ubuntu system packages ³	deb https://mirror.mirantis.com/2019.2.0/ubuntu/ xenial main restricted universe deb https://mirror.mirantis.com/2019.2.0/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/2019.2.0/ubuntu/xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/release/2019.2.0
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/release/2019.2.0
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model/release/2019.2.0
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts/release/2019.2.0
	MCP offline image model	https://github.com/Mirantis/mcp-offline-model/release/2019.2.0
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.0 ³
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.0 ³
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.0 ³
	aptly-api	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-api:2019.2.0

	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.0 ³
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.0 ³
	cluster-proportional-autoscaler-amd64	docker-prod-local.artifactory.mirantis.com/mirantis/external/cluster-proportional-autoscaler-amd64:2019.2.0
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/compose:2019.2.0 ³
	contrail-cni	docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/contrail-integration/contrail-cni:v1.2.0
	coredns	docker-prod-local.artifactory.mirantis.com/mirantis/coredns/coredns:v1.2.6-4
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.0 ³
	elasticsearch	docker-prod-local.artifactory.mirantis.com/mirantis/external/elasticsearch:2019.2.0 ³
	etcd-operator	quay.io/coreos/etcd-operator:v0.9.3
	flannel	quay.io/coreos/flannel:v0.10.0-amd64
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.0 ³
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.0 ³
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.0 ³
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.0 ³
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.0 ³
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.0 ³
	k8s-netchecker-agent	mirantis/k8s-netchecker-agent:v1.2.2 (at hub.docker.com)
	k8s-netchecker-server	mirantis/k8s-netchecker-server:v1.2.2 (at hub.docker.com)
	kube-controllers	docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/kube-controllers:v3.3.2
	kubernetes-dashboard-amd64	docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/kubernetes-dashboard-amd64:v1.10.1-2

metallb-controller	docker-prod-local.artifactory.mirantis.com/mirantis/metallb/controller:v0.7.3-2
metallb-speaker	docker-prod-local.artifactory.mirantis.com/mirantis/metallb/speaker:v0.7.3-2
metrics-server	k8s.gcr.io/metrics-server-amd64:v0.3.1
mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.0 ³
nginx-ingress-controller-amd64	docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes-ingress-nginx/nginx-ingress-controller-amd64:nginx-0.21.0-3
node	docker-prod-local.artifactory.mirantis.com/mirantis/projectcalico/calico/node:v3.3.2
openldap	docker-prod-local.artifactory.mirantis.com/mirantis/external/openldap:2019.2.0 ³
pause	docker-prod-local.artifactory.mirantis.com/mirantis/kubernetes/pause-amd64:v1.12.4-3
phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/openldap:1.2.2 ³
postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³
prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.0 ³
prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus_relay:2019.2.0 ³
pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.0 ³
qa-tools	docker-prod-local.artifactory.mirantis.com/mirantis/oss/qa-tools:2019.2.0 ³
registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.0 ³
remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.0 ³
sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.0 ³
telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.0 ³
tiller	gcr.io/kubernetes-helm/tiller:v2.12.2 ⁶
virtlet	mirantis/virtlet:v1.4.4 (at hub.docker.com)

	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.0 ³
Other	calico-bird	docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/projectcalico/bird/birdcl-v0.3.3
	calico-ctl	docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/projectcalico/calicoctl/calicoctl-v3.3.2
	calico-cni	docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/projectcalico/cni-plugin/calico-v3.3.2
	calico-ipam	docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/projectcalico/cni-plugin/calico-ipam-v3.3.2
	cni-genie	docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/cni-genie/genie_v2.0-1-g209d3c4
	containernetworking-plugins	docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/containernetworking-plugins/containernetworking-plugins_v0.7.2-151-g1d23302.tar.gz
	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 ⁶
	hyperkube-amd64	docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/hyperkube-binaries/hyperkube_v1.12.4-3_1547129775753 docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/hyperkube-binaries/hyperkube_v1.12.6-5_1551704156632 ⁵ docker-prod-local.artifactory.mirantis.com/binary-prod-local/mirantis/kubernetes/hyperkube-binaries/hyperkube_v1.13.5-3_1553734030770 ⁶
	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.0 ³
	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 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)

11, 12, 13, 14,
15, 16, 17, 18,
19, 20, 21, 22,
23, 24, 25, 26,
27, 28, 29, 30,
31, 32, 33, 34,
35, 36, 37, 38,
39, 40, 41, 42,
43, 44, 45)

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.

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

Component	Application/service	2018.11.0	2019.2.0 (current maintenance update)	Comments
Distributed storage	Ceph Nautilus	n/a	14.2.22	Nautilus v14.2.19 Release Notes
	Ceph Luminous	12.2.8-1~u16.04+mcp142	12.2.13	Luminous v12.2.13 Release Notes
DriveTrain	Aptly	1.3.0	1.3.0	Resource type - Docker image
	aptly-publisher	0.12.11	0.12.12	Resource type - Docker image
	Gerrit	2.13.6	2.15.17	Resource type - Docker image
	jenkins-master	2.121.2, 2.121.3	2.263.4	Resource type - Docker image
	Jenkins pipeline-library	2018.11.0	2019.2.0	Resource type - Git repository

	Reclass	1.5.1-1tcp4	1.5.6-1.0~u16.0 4+mcp8	
	Reclass model	2018.11.0	2019.2.0	Resource type - Git repository
	Salt formulas	2018.11.0	2019.2.0	Resource type - binary repository only
	sosreport	n/a	3.8.0-1~u16.04 +mcp4 ¹⁶	
Hypervisors	libvirt	4.0.0-1.7~u16.0 4+mcp3	4.0.0-1.8.10~u1 6.04+mcp2	
	qemu	2.11+dfsg-1.4~ u16.04+mcp2	1:2.11+dfsg-1.7. 39~u16.04+mc p1 ¹² , 1:2.11+df sg-1.7.39~u16.0 4+mcp1 ¹¹	qemu-kvm
Kubernetes support terminated since 2019.2.5	CNI-Genie	1.0-191	2.0-1	Kubernetes support termination notice
	CNI-plugins	0.7.2-96	0.7.2-173	
	containerd	n/a	1.2.5-2~u16.04 +mcp	
	CRI Proxy	0.12.0	0.14.0	
	Dashboard	1.10.0-4	1.10.1-2	
	ExternalDNS	0.5.6-2	0.5.11	
	Kubernetes	1.11.3	1.13.6	
	MetalLB	0.7.3-2	0.7.3-2	
	NGINX Ingress controller	0.19.0-1	nginx-0.24.1-5	
	OpenStack cloud provider	n/a	0.3.0-1	
	SR-IOV	0.3-9	0.3-9	
	Virtlet	1.4.1	1.5.0	
OpenContrail networking	Cassandra	2.2.12	2.2.12, 3.10	

	Kafka	2.11-0.9.0.1-0contrail1	2.11-0.9.0.1-0contrail1, 1.1.1-1	Version 1.1.1-1 for the confluent-kafka-2.11 package in OpenContrail 4.1.3.0.
	OpenContrail	4.0.4.0	4.1.4.0 ¹⁵	OpenContrail 4.x for Kubernetes 1.12 or later is not supported. OpenContrail 3.2 is not supported for new deployments.
	ZooKeeper	3.4.8	3.4.8, 3.4.8-1	
OpenStack Pike 7	Barbican	5.0.0-3~u16.04+mcp0	1:5.0.1-4~u16.04+mcp17	
	Cinder	11.1.1-2~u16.04+mcp77	2:11.2.2-3~u16.04+mcp156	
	Designate	5.0.2-2~u16.04+mcp6	1:5.0.3-3~u16.04+mcp19	
	Glance	15.0.1-1~u16.04+mcp11	2:15.0.2-2~u16.04+mcp20	
	Heat	9.0.4-1~u16.04+mcp31	1:9.0.7-2~u16.04+mcp112	
	Horizon	12.0.3-2~u16.04+mcp48	3:12.0.4-5~u16.04+mcp96	
	Ironic	9.1.4-1~u16.04+mcp29	1:9.1.6-2~u16.04+mcp56	Full support starting from 2019.2.6
	Keystone	12.0.1-4~u16.04+mcp9	2:12.0.3-5~u16.04+mcp40	
	Manila	5.0.1-1~u16.04+mcp61	1:5.1.0-2~u16.04+mcp43	Manila deprecation notice
	Nova	16.1.4-3~u16.04+mcp132	2:16.1.8-7~u16.04+mcp313	
OpenStack Networking Pike	BGP VPN	7.0.0-2~u16.04+mcp18	7.0.1-2~u16.04+mcp11	
	L2 Gateway	11.0.0-1~u16.04+mcp6	1:11.0.0-1~u16.04+mcp23	

	ODL ML2 plugin	11.0.0-1~u16.04+mcp55	1:11.0.0-1~u16.04+mcp66	For neutron-plugin-ml2
	Neutron	11.0.6-2~u16.04+mcp122	2:11.0.8-6~u16.04+mcp280	
	Octavia	1.0.2-6~u16.04+mcp40	1.0.5-8~u16.04+mcp21	
OpenStack Telemetry Pike	Aodh	5.1.0-3~u16.04+mcp10	5.1.0-4~u16.04+mcp16	
	Ceilometer	9.0.5-2~u16.04+mcp16	1:9.0.7-3~u16.04+mcp33	
	Panko	3.1.0-1~u16.04+mcp11	3.1.1-2~u16.04+mcp12	
	Gnocchi	4.0.5-2~u16.04+mcp2	4.0.5-3~u16.04+mcp5	For Telemetry
OpenStack Queens ⁷	Barbican	6.0.1-4~u16.04+mcp12	1:6.0.1-6~u16.04+mcp32	
	Cinder	12.0.4-2~u16.04+mcp69	2:12.0.10-3~u16.04+mcp168	
	Designate	6.0.1-1.0~u16.04+mcp16	1:6.0.1-1.1~u16.04+mcp33	
	Glance	16.0.1-2~u16.04+mcp21	2:16.0.1-3~u16.04+mcp36	
	Heat	10.0.2-1.0~u16.04+mcp37	1:10.0.3-1.1~u16.04+mcp123	
	Horizon	13.0.1-9~u16.04+mcp	3:13.0.3-10~u16.04+mcp108	
	Ironic	10.1.6-1.0~u16.04+mcp25	1:10.1.10-1.1~u16.04+mcp79	
	Keystone	13.0.1-3~u16.04+mcp18	2:13.0.4-4~u16.04+mcp51	
	Manila	6.0.2-2~u16.04+mcp44	1:6.3.2-3~u16.04+mcp138	Manila deprecation notice
	Nova	17.0.7-6~u16.01+mcp90	2:17.0.13-10~u16.04+mcp388	
OpenStack Networking Queens	BGP VPN	8.0.1-1.0~u16.04+mcp7	8.0.1-1.0~u16.04+mcp15	

	L2 Gateway	12.0.1-1.0~u16.04+mcp10	1:12.0.1-1.0~u16.04+mcp21	
	Networking ODL ML2 plugin	12.0.0-1.0~u16.04+mcp39	1:12.0.0-1.0~u16.04+mcp45	neutron-plugin-ml2
	Neutron	12.0.5-5~u16.04+mcp62	2:12.1.1-9~u16.04+mcp538	
	Octavia	2.0.2-6~u16.04+mcp62	2.1.2-10~u16.04+mcp129	
OpenStack Telemetry Queens	Aodh	6.0.1-2~u16.04+mcp9	6.0.1-3~u16.04+mcp15	
	Ceilometer	10.0.1-2~u16.04	1:10.0.1-3~u16.04+mcp43	
	Panko	4.0.2-2~u16.04+mcp7	4.0.2-3~u16.04+mcp16	
	Gnocchi	4.2.4-4~u16.04+mcp8	4.2.4-5~u16.04+mcp12	For Telemetry
StackLight LMA	jmx-exporter	1:0.9-2~u16.04+mcp21	2:0.3.2-2~u16.04+mcp4	
	libvirt-exporter	0.1-1~u16.04+mcp0	0.1-1~u16.04+mcp9	
	Telegraf	1.5.3~mcp20180726123134~bdfbf30-0	1:1.9.1-3~u16.04+mcp116	
System	Open vSwitch	2.8.0-4~u16.04+mcp1	2.9.5-2~u16.04+mcp	openvswitch-common, openvswitch-switch, python-openvswitch
	RabbitMQ	3.6.15-3~u16.04+mcp1	3.8.17-1~u16.04+mcp1	

Software components and Release Versions from mirrored repositories

Component	Application/service	2018.11.0	2019.2.0 (current maintenance update)	Comments
DriveTrain	MAAS	2.3.5	2.3.5	
	SaltStack	2017.7.7	2017.7.8	
	GlusterFS	3.8	5.5	

Kubernetes support terminated since 2019.2.5	Calico	3.1.3	3.3.1	Kubernetes support termination notice
	Calico CNI	3.1.3	3.3.1	
	CoreDNS	1.2.2-12	1.4.0	
	etcd	3.3.8	3.3.12	
	etcd Operator	0.9.2	0.9.3	
	Flannel	0.10.0-amd64	0.10.0-amd64	
	Helm	n/a	2.12.2 ¹³	
	Metrics Server	n/a	0.3.1	
	Tiller	n/a	2.12.2 ¹³	
OpenContrail networking	Redis	2:3.0	2:3.0, 2:3.0.6-1ubuntu0.3	redis-server
StackLight LMA	Alerta	5.6.10	6.5.0	
	Alertmanager	0.14.0	0.14.0 ¹⁴	
	Elasticsearch	5.6.12	6.8.0 ¹⁴	
	Fluentd	1.0.2	1.2.6	Fluentd is included to the td-agent 3.2.1 package.
	Grafana	5.2.4	5.3.4	
	Heka	0.10.1	0.10.1	
	InfluxDB	1.5.2-1	1.5.2-1	
	Kibana	5.6.12	6.8.0 ¹⁴	
	MongoDB	2.6.10	2.6.10	For Alerta
	Prometheus	2.2.1	2.12.0	
	Pushgateway	0.4.0	0.6.0	
System	Docker	docker-ce 18.06.1, docker-engine 1.13.1	docker-ce 5:18.09.0~3-0~ubuntu-xenial	
	Git	2.7.4	2.7.4	
	GlusterFS	3.8.15	3.8.15	
	HAProxy	1.6.3	1.6.3	
	NGINX	1.10.3	1.10.3	

	OpenLDAP	2.4.40	2.4.44	
	Galera	25.3.14	25.3.37.binary-1~u16.04+mcp	
	MySQL	5.6.35	5.7.43-1~u16.04+mcp1	
		n/a	5.7.36-1~u16.04+mcp2 ^{Optional}	
	PostgreSQL	9.6	9.6.10	
	Base OS ⁸	Ubuntu Xenial ⁹	Ubuntu Xenial ¹⁰	
	OS for HW nodes ⁸	Ubuntu Xenial ⁹	Ubuntu Xenial ¹⁰	

7(1, 2) For the OpenStack releases support schedule, see [MCP OpenStack Releases](#).

8(1, 2) When newer versions of Ubuntu packages are available in the Mirantis repositories, MCP installs them instead of the versions available in the Ubuntu repositories.

9(1, 2) linux-image-generic-hwe-16.04 version 4.15.0.36.59

10(1, 2) linux-image-generic-hwe-16.04 version 4.15.0.43.64

11 For OpenStack Pike

12 For OpenStack Queens

13(1, 2) The component has been added in 2019.2.3.

14(1, 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.

15 OpenContrail 4.0 is deprecated in the sake of OpenContrail 4.1 and not supported for new deployments since 2019.2.4.

16 The component has been added in 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 HAProxy 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 HAProxy 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 HAProxy connection limit being too low for large clusters. Increased the maximum number of connections handled by the HAProxy 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.cookiec-cicd-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 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
- 35060
- 34708

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:

```
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:

```
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:

```
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 '@backupninja:client or !@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/Orchestrator.groovy b/src/com/mirantis/mk/Orchestrator.groovy
index 509fe87..575d6ca 100644
--- a/src/com/mirantis/mk/Orchestrator.groovy
+++ b/src/com/mirantis/mk/Orchestrator.groovy
@@ -44,7 +44,7 @@ def installFoundationInfra(master, staticMgmtNet=false, extra_tgt = "") {
    } catch (Throwable e) {
        common.warningMsg('Salt state salt.minion.base is not present in the Salt-formula yet.')
    }
- salt.enforceState([saltId: master, target: "* ${extra_tgt}", state: ['linux.system'], retries: 2])
+ salt.enforceState([saltId: master, target: "* ${extra_tgt}", state: ['linux.system'], batch: '15', retries: 2])
+ if (staticMgmtNet) {
+     salt.runSaltProcessStep(master, "* ${extra_tgt}", 'cmd.shell', ["salt-call state.sls linux.network; salt-call service.restart salt-minion"], null, true, 60)
+ }
```

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:
    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:

```
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:

```
bond1.${_param:aint_public_vlan}:
  name: bond1.${_param:aint_public_vlan}
  enabled: true
  proto: manual
  type: ovs_port
  bridge: br-aint_public
  ovs_bridge: br-aint_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:

```
nginx:
server:
site:
  nginx_proxy_salt_api:
    proxy:
      timeout: 1000
```

3. Apply the following state:

```
salt -C 'l@salt:master' saltutil.sync_all
salt -C 'l@salt:master' state.sls nginx.server
```

35060

The service.enable Salt module does not enable the nova-novncproxy service if it was disabled using systemd.

Workaround:

- Enable the service using systemd
 - Disable the service using Salt and then enable it also using Salt
-

34708

Due to the specifics of SaltStack version 2017.7, when using the x509.py module, Salt ignores the test=True option and applies the changes.

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`:

```
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:

```
source /root/keystonercv3
```

3. Set a new password:

```
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 sticks 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. Choose from the following options:

- For the MCP version 2019.2.4 and later, run the following command:

```
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:

```
mysql -uoctavia -p
```

3. 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';
```

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:

```

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:

```

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:

```

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:

```
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:

```
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:


```
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`:

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

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

```
salt -C 'l@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:

```
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

```

- 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:

```

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

```

```

id: 'private-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:
      internal:
        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 `kubect exec` and `kubect 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.

Seealso

[Corresponding community bug](#)

OpenContrail

- 23177
- 24943
- 25264
- 25629
- 25857
- 26133
- 26673
- 29091
- 34807
- 35484

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:

```
salt -C 'I@opencontrail:control' cmd.run 'chown -R contrail:contrail /etc/contrail'
```

3. Verify that the files are owned by the OpenContrail user:

```
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.

25857

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

Fixed in 2019.2.8 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
-

34807

The OpenContrail 4.1 vRouter may crash when applying the `contrail-vrouter-agent` configuration. No workaround is required, the vRouter automatically restarts after the crash and correctly applies the new configuration.

35484

After upgrading an MCP cluster, some VMs on the OpenStack compute nodes can be unreachable through a floating IP due to an incorrect checksum. In such case, the `InterfaceConfiguration: Virtual-network UUID mismatch for interface` error entry appears in the router-agent log for the interface of the affected VM.

The workaround is to manually disable tx-checksumming for the bond interface. For details, see [Juniper documentation: Troubleshooting: SSH/TCP traffic fails in Contrail due to checksum errors](#).

Workaround:

1. Log in to the OpenStack compute node that runs the affected VM.
2. Disable tx-checksumming for the bond interface:

```
ethtool -K bond0 tx off
```

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 Reclass 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:

```
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:

```
kill -9 $20728
```

4. Start the RADOS Gateway service specifying the node name, for example, client.rgw.rgw01:

```
/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:

```
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`:

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

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

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

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

```
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
- Kubernetes support termination notice
- Manila deprecation notice
- Gainsight 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

Deprecation notes for the model structure

Structure change details	Deprecated classes	New classes
The Salt formulas, OpenContrail, and updates repositories have been migrated from http://apt.mirantis.com to http://mirror.mirantis.com . Therefore, the new classes have been introduced and added into the system/linux/system/repo/mcp/apt_mirantis directory. Old classes have been deprecated.	<ul style="list-style-type: none"> • system.linux.system.repo.mcp.salt • system.linux.system.repo.mcp.contrail • system.linux.system.repo.mcp.updates 	<ul style="list-style-type: none"> • system.linux.system.repo.mcp.salt • system.linux.system.repo.mcp.contrail • system.linux.system.repo.mcp.updates

Deprecation notes for operations

Deprecation notes for operations

Affected component	Operation	Details
OpenStack	Creation of Cinder multi-attach volumes and volume types	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.
Kubernetes	Docker	Deprecated Docker in the sake of containerd for a lower memory footprint, faster container start, easier updates or upgrades of containerd compared to Docker.
StackLight LMA	Notifications through the Push Notification service	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 .
	InfluxDB	Deprecated InfluxDB, InfluxDB Relay, and remote storage adapter. This functionality will be removed in the next release.
StackLight OSS	DevOps Portal	Deprecated the DevOps Portal OSS tools including the corresponding Salt formulas packages, pipeline jobs, and metadata model fragments.

Kubernetes support termination notice

Starting with the MCP 2019.2.5 update, the Kubernetes component is no longer supported as a part of the MCP product. This implies that Kubernetes is not tested and not shipped as an MCP component. Although the Kubernetes Salt formula is available in the community driven [SaltStack formulas](#) ecosystem, Mirantis takes no responsibility for its maintenance.

Customers looking for a Kubernetes distribution and Kubernetes lifecycle management tools are encouraged to evaluate the Mirantis Kubernetes-as-a-Service (KaaS) and Docker Enterprise products.

Manila deprecation notice

In the MCP 2019.2.7 update, the OpenStack Manila component is being considered for deprecation. The corresponding capabilities are still available, although not further enhanced.

Starting with the 2019.2.11 maintenance update, the OpenStack Manila component will no longer be supported by Mirantis. For those existing customers who have the Manila functionality explicitly included in the scope of their contracts, Mirantis will continue to fulfill the corresponding support obligations.

Gainsight deprecation notice

Starting with the MCP 2019.2.9 update, the Gainsight integration service is considered as deprecated.

Maintenance updates

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

Q4`18 maintenance updates summary

Maintenance update	Release date	Summary
2019.2.26	December 22, 2023	<ul style="list-style-type: none"> • Bug fix for DriveTrain • Security bug fixes for DriveTrain and OpenStack
2019.2.25	September 15, 2023	<ul style="list-style-type: none"> • Bug fixes for OpenStack and StackLight • Security bug fixes for DriveTrain, OpenStack, and StackLight
2019.2.24	June 16, 2023	<ul style="list-style-type: none"> • Bug fixes for DriveTrain and OpenStack • Security bug fixes for OpenStack
2019.2.23	March 17, 2023	<ul style="list-style-type: none"> • Bug fixes for DriveTrain, OpenStack, and StackLight • Security bug fixes for OpenStack
2019.2.22	December 16, 2022	<ul style="list-style-type: none"> • Bug fixes for DriveTrain and OpenStack • Security bug fixes for OpenStack
2019.2.21	September 16, 2022	<ul style="list-style-type: none"> • Bug fixes for DriveTrain, OpenStack, StackLight, and Ceph • Security bug fixes for DriveTrain and OpenStack
2019.2.20	July 15, 2022	<ul style="list-style-type: none"> • Request limiting for custom locations • Documentation on Barbican certificates renewal • Bug fixes for DriveTrain and OpenStack
2019.2.19	May 16, 2022	<ul style="list-style-type: none"> • Bug fixes for DriveTrain, OpenStack, and Ceph • Security bug fixes for DriveTrain and OpenStack
2019.2.18	March 14, 2022	<ul style="list-style-type: none"> • Support for MySQL 5.7 • Bug fixes for DriveTrain, OpenStack, and Ceph

2019.2.17	December 22, 2021	<ul style="list-style-type: none"> • Security updates for Docker containers • Pre-update DriveTrain verification • Glance database cleanup • HTTP output for Fluentd
2019.2.16	October 15, 2021	<ul style="list-style-type: none"> • Kernel Crash Dump configuration • Time stamps in Jenkins pipeline jobs • Host passthrough for VCP • Cinder coordination • Disabling of Nova cell mapping • Bug fixes for DriveTrain, OpenStack, and Ceph
2019.2.15	July 30, 2021	<ul style="list-style-type: none"> • RabbitMQ queue mirroring and troubleshooting • Randomized RabbitMQ reconnection intervals • User ID support in the Nova policy • Bug fixes for DriveTrain, OpenStack, StackLight, and Ceph
2019.2.14	May 28, 2021	<ul style="list-style-type: none"> • Granular distribution of Ceph keys • Disk and CPU wait alerts • Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph
2019.2.13	March 16, 2021	<ul style="list-style-type: none"> • Nonclustered RabbitMQ • Arbitrary Galera parameters • Ceph pipeline jobs improvements • Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph
2019.2.12	December 11, 2020	<ul style="list-style-type: none"> • Security updates for QEMU • Keystone credential keys backup and restore • OpenStack database cleanup • OpenContrail statistics • Disabling of HTTP probes for OpenStack public endpoints

2019.2.11	September 30, 2020	<ul style="list-style-type: none"> • Security improvements for Docker containers • Ubuntu security updates • Gnocchi and Panko policies configuration • OpenContrail IPv6 capabilities documentation • Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph
2019.2.10	July 23, 2020	<ul style="list-style-type: none"> • RabbitMQ 3.8.2 support • Ceph Nautilus support • RBD monitoring • CpuFlagsFilter filter for live migrations • Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph
2019.2.9	April 30, 2020	<ul style="list-style-type: none"> • Cross-AZ high availability for Neutron agents • Alertmanager integrations support • Alerts and metrics enhancements • Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph
2019.2.8	March 5, 2020	<ul style="list-style-type: none"> • OpenStack availability zones monitoring • Capability to apply maintenance updates of a particular version • Update process improvements • Octavia amphora HA mode support • Numerous documentation improvements • Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph
2019.2.7	December 26, 2019	<ul style="list-style-type: none"> • 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	November 5, 2019	<ul style="list-style-type: none"> • 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	August 19, 2019	<ul style="list-style-type: none"> • 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 • Announcement of Kubernetes support termination • Bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph
2019.2.4	June 26, 2019	<ul style="list-style-type: none"> • 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	April 26, 2019	<ul style="list-style-type: none"> • 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	March 20, 2019	<ul style="list-style-type: none"> • 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
2019.2.1	February 27, 2019	Bug fixes for the OpenStack Pike release

2019.2.26

The MCP 2019.2.26 update introduces a bug fix for the DriveTrain component, security updates for DriveTrain and OpenStack. The update is available since December 22, 2023.

Addressed issues

The MCP 2019.2.26 update contains fixes for the following MCP components:

- DriveTrain
 - [37188] Fixed the issue with the libvirt-exporter blockages caused by liveMigration memory stats collection taking more time than the prometheus scrape timeout.
 - [37233, 37234 - 37241, 37243, 37248] Updated various docker containers to fix vulnerabilities:

- alerta
 - alertmanager
 - prometheus
 - prometheus-es-exporter
 - sf-notifier
 - sf-reporter
 - docker-aptly
 - docker-gerrit
 - docker-jenkins
 - docker-jnlp-slave
 - docker-mysql
 - docker-openldap
 - docker-phpldapadmin
 - docker-registry
 - docker-ssh-slave
- OpenStack
 - [37242][Pike, Queens] Updated MySQL-wsrep to version 5.7.42 to include the upstream security fixes.
 - [37251] Updated python-urllib3 to fix the following vulnerabilities:
 - [CVE-2023-45803](#)
 - [CVE-2023-43804](#)
 - [CVE-2018-25091](#)

Known issues

The MCP 2019.2.26 maintenance update does not contain newly detected known issues. Though, be sure to review the previously detected issues that may still be affecting your MCP deployment and address them as outlined in Known issues and corresponding sections of the previous maintenance updates.

Updated MCP components

The MCP 2019.2.26 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.25 update.

All 2019.2.26 packages are available at <http://mirror.mirantis.com/update/2019.2.26/>.

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.25	2019.2.26
Extra	telegraf	1:1.9.1-3~u16.04+m cp116	1:1.9.1-3~u16.04+m cp128

	libvirt-exporter	0.1-1~u16.04+mcp8	0.1-1~u16.04+mcp9
OpenStack Pike	mysql-wsrep-5.7	5.7.42-1~u16.04+mc p1	5.7.43-1~u16.04+mc p1
	python-urllib3	1.21.1-1~u16.04+mc p4	1.21.1-1~u16.04+mc p5
OpenStack Queens	mysql-wsrep-5.7	5.7.42-1~u16.04+mc p1	5.7.43-1~u16.04+mc p1
	python-urllib3	1.21.1-1~u16.04+mc p4	1.21.1-1~u16.04+mc p5
Salt formulas	salt-formula-jenkins	2017.8+2022042610 34.22b4455~xenial1	2017.8+2023102310 20.11e18b2~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.26 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.26/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.26/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.26/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.26/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.26/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.26/opencontrail-4.1/xenial xenial main
	Salt formulas packages ¹⁷	http://mirror.mirantis.com/update/2019.2.26/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2

	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.26.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.26.qcow2
	VCP Ubuntu 16.04 image ¹⁷	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.26/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.26/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.26/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.26/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.26/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ¹⁷
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.26/glusterfs-5/xenial xenial main ¹⁷
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.26/maas/xenial xenial main ¹⁷
	Percona	deb http://mirror.mirantis.com/update/2019.2.26/percona/xenial xenial main ¹⁷

	SaltStack packages	<p>deb http://mirror.mirantis.com/update/2019.2.26/saltstack-2017.7/trusty trusty main</p> <p>deb http://mirror.mirantis.com/update/2019.2.26/saltstack-2017.7/xenial xenial main ¹⁷</p> <p>deb http://mirror.mirantis.com/update/2019.2.26/salt-2017.7.8/ xenial xenial main ¹⁷</p>
	Upstream Ubuntu system packages ¹⁷	<p>deb https://mirror.mirantis.com/update/2019.2.26/ubuntu/xenial main restricted universe</p> <p>deb https://mirror.mirantis.com/update/2019.2.26/ubuntu/xenial-updates main restricted universe</p> <p>deb https://mirror.mirantis.com/update/2019.2.26/ubuntu/xenial-security main restricted universe</p>
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.26
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.26
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.26
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.26
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.26 ¹⁷
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.26 ¹⁷
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.26 ¹⁷
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.26 ¹⁷
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.26 ¹⁷
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:2019.2.25 ¹⁷
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ¹⁷
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-reporter:2019.2.26 ¹⁷

	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ¹⁷
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.26 ¹⁷
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.23 ¹⁷
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ¹⁷
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.26 ¹⁷
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.26 ¹⁷
	ssh-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/ssh-slave:2019.2.26 ¹⁷
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.26 ¹⁷
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.26 ¹⁷
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.26 ¹⁷
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/postgresql:2019.2.25 ¹⁷
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.26 ¹⁷
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ¹⁷
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ¹⁷
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.26 ¹⁷
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ¹⁷
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.26 ¹⁷
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ¹⁷
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.25

Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ¹⁷
-------	---------	---

17(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35, 36)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.25 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.25, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .
3 1	Galera cluster	<ol style="list-style-type: none"> Update the Galera cluster as described in MCP Operations Guide: Update Galera. Optional. Upgrade Galera to v5.7 as described in Upgrade Galera.

3	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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none">• MCP Operations Guide: Apply security updates using Jenkins• MCP Operations Guide: Apply security updates manually

2019.2.25

The MCP 2019.2.25 update introduces bug fixes for the OpenStack and StackLight components, security updates for DriveTrain, OpenStack, and StackLight. The update is available since September 15, 2023.

Addressed issues

The MCP 2019.2.25 update contains fixes for the following MCP components:

- OpenStack
 - [37199][Pike, Queens] Fixed the SSO logout issue in OpenStack Horizon.
 - [37196][Pike] Updated dnsmasq to address the [USN-6034-1](#) and [CVE-2023-28450](#) vulnerabilities.
 - [37195][Pike, Queens] Updated sqlparse to eliminate [CVE-2023-30608](#).
 - [37193][Pike, Queens] Updated the MySQL MySQL-wsrep package to version 5.7.42 to include the upstream security fixes.
- StackLight
 - [37192] Added the HTTP proxy configuration for the Slack notifications receiver to solve the issue with Alertmanager notification failures.
- DriveTrain
 - [37209, 37203, 37202, 37186, 37185] Updated the following docker images to fix vulnerabilities:

- docker-aptly
- docker-compose
- docker-gerrit
- docker-mysql
- docker-phpldapadmin
- docker-ssh-slave
- alerta
- cvp-sanity-checks
- postgresql
- prometheus-es-exporter
- registry
- sf-notifier
- sf-reporter
- visualizer

Known issues

The MCP 2019.2.25 maintenance update does not contain newly detected known issues. Though, be sure to review the previously detected issues that may still be affecting your MCP deployment and address them as outlined in Known issues and corresponding sections of the previous maintenance updates.

Updated MCP components

The MCP 2019.2.25 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.24 update.

All 2019.2.25 packages are available at <http://mirror.mirantis.com/update/2019.2.25/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.24	2019.2.25
Extra	telegraf	1:1.9.1-3~u16.04+mcp103	1:1.9.1-3~u16.04+mcp116
OpenStack Pike	dnsmasq	2.79-1~u16.04+mcp4	2.79-1~u16.04+mcp5
	horizon	3:12.0.4-5~u16.04+mcp95	3:12.0.4-5~u16.04+mcp96
	mysql-wsrep-5.7	5.7.41-1~u16.04+mcp1	5.7.42-1~u16.04+mcp1
OpenStack Queens	dnsmasq	2.79-1~u16.04+mcp4	2.79-1~u16.04+mcp5

	horizon	3:13.0.3-10~u16.04+mcp107	3:13.0.3-10~u16.04+mcp108
	mssql-wsrep-5.7	5.7.41-1~u16.04+mcp1	5.7.42-1~u16.04+mcp1
Salt formulas	salt-formula-prometheus	0.1+202301111450.1a61355~xenial1	0.1+202306290959.5a38e6d~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.25 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.25/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.25/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.25/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.25/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.25/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.25/opencontrail-4.1/xenial xenial main
	Salt formulas packages ¹⁸	http://mirror.mirantis.com/update/2019.2.25/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.25.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.25.qcow2
	VCP Ubuntu 16.04 image ¹⁸	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

Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.25/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.25/elastics earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.25/elastics earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.25/elastics earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.25/elastics earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ¹⁸
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.25/glusterfs-5/xenial xenial main ¹⁸
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.25/maas/xenial xenial main ¹⁸
	Percona	deb http://mirror.mirantis.com/update/2019.2.25/percona/xenial xenial main ¹⁸
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.25/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.25/saltstack-2017.7/xenial xenial main ¹⁸ deb http://mirror.mirantis.com/update/2019.2.25/salt-2017.7.8/ xenial xenial main ¹⁸

	Upstream Ubuntu system packages ¹⁸	deb https://mirror.mirantis.com/update/2019.2.25/ubuntu/xenial/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.25/ubuntu/xenial-updates/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.25/ubuntu/xenial-security/main/restricted/universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.25
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.25
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.25
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.25
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.25 ¹⁸
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.21 ¹⁸
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.25 ¹⁸
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.25 ¹⁸
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.25 ¹⁸
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:2019.2.25 ¹⁸
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ¹⁸
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-reporter:2019.2.25 ¹⁸
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ¹⁸
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.25 ¹⁸
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.23 ¹⁸

	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ¹⁸
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.24 ¹⁸
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.25 ¹⁸
	ssh-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/ssh-slave:2019.2.25 ¹⁸
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.25 ¹⁸
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.24 ¹⁸
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.25 ¹⁸
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/postgresql:2019.2.25 ¹⁸
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.23 ¹⁸
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ¹⁸
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ¹⁸
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.25 ¹⁸
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ¹⁸
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.24 ¹⁸
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ¹⁸
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.25
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ¹⁸

18(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35, 36)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.24 maintenance update, proceed with the steps below right away.

If you are updating from MCP maintenance update prior to 2019.2.24, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages.
3 . 1	Galera cluster	<ol style="list-style-type: none"> Update the Galera cluster as described in MCP Operations Guide: Update Galera. Optional. Upgrade Galera to v5.7 as described in Upgrade 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none">• MCP Operations Guide: Apply security updates using Jenkins• MCP Operations Guide: Apply security updates manually

2019.2.24

The MCP 2019.2.24 update introduces bug fixes for DriveTrain and OpenStack components and is available since June 16, 2023.

Addressed issues

The MCP 2019.2.24 update contains fixes for the following MCP components:

- DriveTrain
 - [37181] Defined the virtualenv version in the Jenkins slave docker images to eliminate job failures in Jenkins.
 - [37151] Updated docker images to fix vulnerabilities.
 - [37144] Fixed the logging issue caused by parsing .gz and .zip log files.
 - [37131] Fixed the Designate API failures during the upgrade procedure.
 - [37125] Added the pagination limit and filtering images by visibility to increase the speed of listing big amounts of Glance images by the OpenStack Telegraf plug-in.
- OpenStack
 - [37136][Pike, Queens] Updated MySQL to 5.7.41 and WSREP to v25.33 to eliminate vulnerabilities.
 - [37135][Pike, Queens] Updated the python-django packages to eliminate [CVE-2023-23969](#).
 - [37127][Queens] Fixed the Nova package versioning issue to eliminate the incorrect updates.
 - [37107][Pike, Queens] Fixed the malfunction of the --wait flag for the openstack server rebuild command by adding the current instance status check.
 - [37105][Pike] Fixed the page loading issue in Horizon by changing the query type.

Known issues

The MCP 2019.2.24 maintenance update does not contain newly detected known issues. Though, be sure to review the previously detected issues that may still be affecting your MCP deployment and address them as outlined in Known issues and corresponding sections of the previous maintenance updates.

Updated MCP components

The MCP 2019.2.24 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.23 update.

All 2019.2.24 packages are available at <http://mirror.mirantis.com/update/2019.2.24/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.23	2019.2.24
Extra	telegraf	1:1.9.1-3~u16.04+mcp88	1:1.9.1-3~u16.04+mcp103
OpenStack Pike	manila	1:5.1.0-2~u16.04+mcp42	1:5.1.0-2~u16.04+mcp43
	python-django	1:1.11.29-1~u16.04+mcp7	1:1.11.29-1~u16.04+mcp8
	python-openstackclient	3.12.2-1~u16.04+mcp20	3.12.2-1~u16.04+mcp21
OpenStack Queens	mysql-wsrep-5.7	5.7.39-1~u16.04+mcp1	5.7.41-1~u16.04+mcp1
	nova	2:17.0.13-10~u16.04+mcp387	2:17.0.13-10~u16.04+mcp388
	python-django	1:1.11.29-1~u16.04+mcp6	1:1.11.29-1~u16.04+mcp7
	python-ldappool	2.2.0-1~u16.04+mcp9	2.2.0-1~u16.04+mcp10
	python-openstackclient	3.14.3-1.0~u16.04+mcp40	3.14.3-1.0~u16.04+mcp42
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20230115204809-0	4.1~20230322204808-0

	contrail	4.1~20230115204809-0	4.1~20230322204808-0
	contrail-heat	4.1~20230115204809-0	4.1~20230322204808-0
	contrail-vrouter-dpdk	4.1~20230115204809	4.1~20230322204808
	contrail-web-controller	4.1~20230115204809-0	4.1~20230322204808-0
	contrail-web-core	4.1~20230115204809-0	4.1~20230322204808-0
	neutron-plugin-contrail	4.1~20230115204809-0	4.1~20230322204808-0
Salt formulas	salt-formula-ceph	0.1+202204042203.ded30f9~xenial1	0.1+202304141305.f2d2a22~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.24 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.24/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.24/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.24/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.24/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.24/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.24/opencontrail-4.1/xenial xenial main
	Salt formulas packages ¹⁹	http://mirror.mirantis.com/update/2019.2.24/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2

	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.24.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.24.qcow2
	VCP Ubuntu 16.04 image ¹⁹	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.24/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.24/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.24/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.24/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.24/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ¹⁹
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.24/glusterfs-5/xenial xenial main ¹⁹
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.24/maas/xenial xenial main ¹⁹
	Percona	deb http://mirror.mirantis.com/update/2019.2.24/percona/xenial xenial main ¹⁹

	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.24/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.24/saltstack-2017.7/xenial xenial main ¹⁹ deb http://mirror.mirantis.com/update/2019.2.24/salt-2017.7.8/ xenial xenial main ¹⁹
	Upstream Ubuntu system packages ¹⁹	deb https://mirror.mirantis.com/update/2019.2.24/ubuntu/xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.24/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.24/ubuntu/xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.24
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.24
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.24
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.24
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.24 ¹⁹
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.21 ¹⁹
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.24 ¹⁹
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.24 ¹⁹
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.24 ¹⁹
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ¹⁹
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ¹⁹
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-reporter:2019.2.24 ¹⁹

	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ¹⁹
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.24 ¹⁹
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.23 ¹⁹
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ¹⁹
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.24 ¹⁹
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.24 ¹⁹
	ssh-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/ssh-slave:2019.2.24 ¹⁹
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.24 ¹⁹
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.24 ¹⁹
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.24 ¹⁹
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/postgresql:2019.2.24 ¹⁹
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.24 ¹⁹
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ¹⁹
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ¹⁹
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ¹⁹
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ¹⁹
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.24 ¹⁹
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ¹⁹
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6

Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ¹⁹
-------	---------	---

19(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35, 36)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.23 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.23, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .
3 1	Galera cluster	<ol style="list-style-type: none"> Update the Galera cluster as described in MCP Operations Guide: Update Galera. Optional. Upgrade Galera to v5.7 as described in Upgrade Galera.

3	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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none">• MCP Operations Guide: Apply security updates using Jenkins• MCP Operations Guide: Apply security updates manually

2019.2.23

The MCP 2019.2.23 update introduces bug fixes for DriveTrain, OpenStack, and StackLight components and is available since March 17, 2023.

Addressed issues

The MCP 2019.2.23 update contains fixes for the following MCP components:

- DriveTrain
 - [37108] Fixed the issue with the pre-upgrade check failures when Ceph is not enabled.
 - [37068] Fixed the Dogtag certificate monitoring issue caused by a missing pillar.
 - [37064] Fixed the issue causing overload of the log files for the Elasticsearch engine.
 - [33592] Fixed the issue causing the designate-central service failures due to database absence.
- OpenStack
 - [37088, 37087, 37086][Queens, Pike] Fixed security issues to eliminate [OSSA-2023-002: Arbitrary file access through custom VMDK flat descriptor](#).
 - [37073][Queens] Fixed the issue with inability to use the forward slash sign in Cinder snapshot metadata.
 - [37069][Queens, Pike] Fixed the floating IP (FIP) configuration issue caused by inability to remove the existing FIP on DVR routers.
- StackLight
 - [37070] Upgraded the Prometheus Docker image to the 2019.2.23 version to improve the write-ahead logging management and eliminate the OOM container termination issue.

Known issues

The MCP 2019.2.23 maintenance update does not contain newly detected known problems. Though, be sure to review the previously detected issues that may still be affecting your MCP deployment and address them as outlined in Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.23 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.22 update.

All 2019.2.23 packages are available at <http://mirror.mirantis.com/update/2019.2.23/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.22	2019.2.23
Extra	telegraf	1:1.9.1-3~u16.04+mcp82	1:1.9.1-3~u16.04+mcp88
OpenStack Pike	cinder	2:11.2.2-3~u16.04+mcp154	2:11.2.2-3~u16.04+mcp156
	glance	2:15.0.2-2~u16.04+mcp18	2:15.0.2-2~u16.04+mcp20
	neutron	2:11.0.8-6~u16.04+mcp279	2:11.0.8-6~u16.04+mcp280
	nova	2:16.1.8-7~u16.04+mcp312	2:16.1.8-7~u16.04+mcp313
OpenStack Queens	cinder	2:12.0.10-3~u16.04+mcp165	2:12.0.10-3~u16.04+mcp168
	glance	2:16.0.1-3~u16.04+mcp34	2:16.0.1-3~u16.04+mcp36
	neutron	2:12.1.1-9~u16.04+mcp537	2:12.1.1-9~u16.04+mcp538
	nova	2:17.0.13-9~u16.04+mcp387	2:17.0.13-10~u16.04+mcp387
	tempest	1:18.0.0-1~u16.04+mcp50	1:18.0.0-1~u16.04+mcp57

OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20221110150249-0	4.1~20230115204809-0
	contrail	4.1~20221110150249-0	4.1~20230115204809-0
	contrail-heat	4.1~20221110150249-0	4.1~20230115204809-0
	contrail-vrouter-dpdk	4.1~20221110150249	4.1~20230115204809
	contrail-web-controller	4.1~20221110150249-0	4.1~20230115204809-0
	contrail-web-core	4.1~20221110150249-0	4.1~20230115204809-0
	neutron-plugin-contrail	4.1~20221110150249-0	4.1~20230115204809-0
Salt formulas	salt-formula-dogtag	0.1+202206240847.16d8a3a~xenial1	0.1+202301131252.de3ccbf~xenial1
	salt-formula-fluentd	0.1+202202150823.31e6c81~xenial1	0.1+202302091045.5e5d5f0~xenial1
	salt-formula-git	0.2+201911071622.e9fda84~xenial1	0.2+202301161936.3ff2b32~xenial1
	salt-formula-glusterfs	2017.3+202008180918.cf065bb~xenial1	2017.3+202302021225.39f28bc~xenial1
	salt-formula-prometheus	0.1+202111031532.f681e07~xenial1	0.1+202301111450.1a61355~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.23 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.23/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.23/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.23/extra/xenial xenial main

	Ceph	deb http://mirror.mirantis.com/update/2019.2.23/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.23/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.23/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²⁰	http://mirror.mirantis.com/update/2019.2.23/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.23.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.23.qcow2
	VCP Ubuntu 16.04 image ²⁰	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.23/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.23/elasticsearch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.23/elasticsearch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.23/elasticsearch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.23/elasticsearch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²⁰
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.23/glusterfs-5/xenial xenial main ²⁰

	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.23/maas/xenial xenial main ²⁰
	Percona	deb http://mirror.mirantis.com/update/2019.2.23/percona/xenial xenial main ²⁰
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.23/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.23/saltstack-2017.7/xenial xenial main ²⁰ deb http://mirror.mirantis.com/update/2019.2.23/salt-2017.7.8/ xenial xenial main ²⁰
	Upstream Ubuntu system packages ²⁰	deb https://mirror.mirantis.com/update/2019.2.23/ubuntu/ xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.23/ubuntu/ xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.23/ubuntu/ xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.23
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.23
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.23
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.23
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.23 ²⁰
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.21 ²⁰
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.23 ²⁰
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.23 ²⁰
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.23 ²⁰

compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²⁰
cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²⁰
gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-reporter:2019.2.23 ²⁰
gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²⁰
gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²⁰
grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.23 ²⁰
heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²⁰
jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.23 ²⁰
jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.23 ²⁰
ssh-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/ssh-slave:2019.2.23 ²⁰
mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.23 ²⁰
openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.23 ²⁰
phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.23 ²⁰
postgres	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/postgresql:2019.2.22 ²⁰
prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.23 ²⁰
prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²⁰
pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²⁰
registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²⁰
remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²⁰

	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.23 ²⁰
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ²⁰
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²⁰

20(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.22 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.22, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .

3 · 1	Galera cluster	<ol style="list-style-type: none">1. Update the Galera cluster as described in MCP Operations Guide: Update Galera.2. Optional. Upgrade Galera to v5.7 as described in Upgrade 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none">• MCP Operations Guide: Apply security updates using Jenkins• MCP Operations Guide: Apply security updates manually

2019.2.22

The MCP 2019.2.22 update introduces bug fixes for DriveTrain and OpenStack components and is available starting from December 16, 2022.

Addressed issues

The MCP 2019.2.22 update contains fixes for the following MCP components:

- DriveTrain
 - [37043] Fixed the issue with the incorrect order of Galera and MySQL packages installation during the Galera cluster update and during the Upgrade OS stage.
 - [37013] Fixed the issue causing the NGINX failure due to the configuration file containing the dot symbols in the location section.
 - [36930] Fixed the high CPU loads issue in environments with NFS storage enabled by making the `image_cache_manager_interval` parameter configurable.

Note

Within Mirantis Cloud Platform, the parameter defaults to 0, but we recommend following the upstream default value of 2400. For details about the

image_cache_manager_interval parameter, see [OpenStack documentation: Configuration options](#).

- [35604] Fixed the issue with QEMU overconsuming system resources by adding the following options:
 - qemu_max_processes
Sets the maximum number of processes that a QEMU user can run. This option overrides the default value set by the host OS.
 - qemu_max_files
Sets the maximum number of files that a QEMU user can open.
- OpenStack:
 - [37023][Pike, Queens] Updated dnsmasq to the most recent Ubuntu Bionic release to eliminate [USN-4976-2: Dnsmasq vulnerability](#).
 - [37019][Pike, Queens] Fixed the Neutron traffic overloading issue by fetching a new upstream version of the Galera library.
 - [37017][Pike] Fixed the instance_fault table overloading issue by adding InstanceInvalidState to the table exceptions.
 - [37014][Pike, Queens] Fixed the issue causing ldappool to retry an incorrect password until reaching the retry limit.
 - [37012][Pike, Queens] Updated the MySQL wsrep package to version 5.7.39 to include the upstream security fixes.

Known issues

For MCP known issues applicable to MCP 2019.2.22, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.22 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.21 update.

All 2019.2.22 packages are available at <http://mirror.mirantis.com/update/2019.2.22/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.21	2019.2.22
OpenStack Pike	dnsmasq	2.79-1~u16.04+mcp3	2.79-1~u16.04+mcp4
	galera-3	25.3.20-1~u16.04+mcp	25.3.37.binary-1~u16.04+mcp
	keystone	2:12.0.3-5~u16.04+mcp39	2:12.0.3-5~u16.04+mcp40
	mysql-wsrep-5.7	5.7.36-1~u16.04+mcp2	5.7.39-1~u16.04+mcp1
	nova	2:16.1.8-6~u16.04+mcp312	2:16.1.8-7~u16.04+mcp312
	python-ldappool	2.1.1-1~u16.04+mcp2	2.1.1-1~u16.04+mcp3
OpenStack Queens	dnsmasq	2.79-1~u16.04+mcp3	2.79-1~u16.04+mcp4
	galera-3	25.3.20-1~u16.04+mcp	25.3.37.binary-1~u16.04+mcp
	mysql-wsrep-5.7	5.7.36-1~u16.04+mcp2	5.7.39-1~u16.04+mcp1
	neutron	2:12.1.1-9~u16.04+mcp533	2:12.1.1-9~u16.04+mcp537
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20220608204809-0	4.1~20221110150249-0
	contrail	4.1~20220608204809-0	4.1~20221110150249-0
	contrail-heat	4.1~20220608204809-0	4.1~20221110150249-0
	contrail-vrouter-dpdk	4.1~20220608204809	4.1~20221110150249
	contrail-web-controller	4.1~20220608204809-0	4.1~20221110150249-0
	contrail-web-core	4.1~20220608204809-0	4.1~20221110150249-0
	neutron-plugin-contrail	4.1~20220608204809-0	4.1~20221110150249-0
Salt formulas	salt-galera	1.0+202203132239.bf9af16~xenial1	1.0+202211301744.41253db~xenial1
	salt-formula-nginx	0.2+202206031408.0f605c4~xenial1	0.2+202210030853.e79f06b~xenial1

	salt-formula-nova	2016.12.1+202208251059.4311a8a~xenial1	2016.12.1+202211021201.c62d321~xenial1
--	-------------------	--	--

Release artifacts

This section lists the artifacts of the MCP 2019.2.22 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.22/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.22/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.22/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.22/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.22/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.22/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²¹	http://mirror.mirantis.com/update/2019.2.22/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.22.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.22.qcow2
	VCP Ubuntu 16.04 image ²¹	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main

	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.22/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.22/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.22/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.22/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.22/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²¹
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.22/glusterfs-5/xenial xenial main ²¹
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.22/maas/xenial xenial main ²¹
	Percona	deb http://mirror.mirantis.com/update/2019.2.22/percona/xenial xenial main ²¹
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.22/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.22/saltstack-2017.7/xenial xenial main ²¹ deb http://mirror.mirantis.com/update/2019.2.22/salt-2017.7.8/ xenial xenial main ²¹
	Upstream Ubuntu system packages ²¹	deb https://mirror.mirantis.com/update/2019.2.22/ubuntu/xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.22/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.22/ubuntu/xenial-security main restricted universe

MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.22
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.22
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.22
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.22
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.22 ²¹
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.21 ²¹
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.19 ²¹
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.19 ²¹
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.22 ²¹
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²¹
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²¹
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-reporter:2019.2.22 ²¹
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²¹
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²¹
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.19 ²¹
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²¹
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.19 ²¹
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.22 ²¹
	ssh-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/ssh-slave:2019.2.22 ²¹

	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.22 ²¹
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.22 ²¹
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.22 ²¹
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/postgresql:2019.2.22 ²¹
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²¹
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²¹
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²¹
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²¹
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²¹
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.22 ²¹
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ²¹
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²¹

21(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)

11, 12, 13, 14,
15, 16, 17, 18,
19, 20, 21, 22,
23, 24, 25, 26,
27, 28, 29, 30,
31, 32, 33, 34,
35, 36)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.21 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.21, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .
3 · 1	Galera cluster	<ol style="list-style-type: none"> Update the Galera cluster as described in MCP Operations Guide: Update Galera. Optional. Upgrade Galera to v5.7 as described in Upgrade 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> MCP Operations Guide: Apply security updates using Jenkins MCP Operations Guide: Apply security updates manually

2019.2.21

The MCP 2019.2.21 update introduces bug fixes for DriveTrain, OpenStack, StackLight, and Ceph components and is available starting from September 16, 2022.

Addressed issues

The MCP 2019.2.21 update contains fixes for the following MCP components:

- DriveTrain:
 - [36976] Updated the mysql, sf-reporter, phpldapadmin, postgresql, and gainsight Docker images to fix security vulnerabilities.
- OpenStack:
 - [36956][Queens] Fixed the issue causing a timeout during the Panko database execution and affecting the MySQL database.
 - [36953][Queens] Fixed the issue wherein Keystone failed to parse multi-valued claims from OpenID Connect (OIDC) tokens. Enhanced the Keystone Salt formula by implementing the capability to configure oidc_claim_delimiter.
 - [36948][Pike, Queens] Fixed the issue wherein the upgrade of a Galera cluster to version 5.7 was failing if AppArmor was present on the database nodes.
 - [36935][Pike, Queens] Updated the pyroute2 package to version 0.5.4 to prevent the privsep_helper process from leaking memory. The issue could cause slow router processing times.
 - **[36897][Pike, Queens] Fixed the issue with the nova-serialproxy package failing to create the systemd unit.**
 - [36888][Pike] Fixed the issue wherein upgrading OpenStack Pike to Queens failed with the an exception when applying the designate.upgrade Salt state.
 - [36780][Pike, Queens] Upgraded Redis to version 5.0.14 on OpenStack Pike and OpenStack Queens to eliminate the [CVE-2021-32628](#) security vulnerability.
 - [35136][Queens] Fixed the issue wherein scheduling a VM failed with a number of Unexpected API errors.
- StackLight:
 - [36816] Replaced token-based authentication with basic HTTP authentication for the Alerta receiver for Alertmanager notifications.
- Ceph:
 - [36942] Fixed the issue wherein upgrading Ceph Luminous (v12.2.11 or v12.2.13) to Nautilus (v14.2.22) was causing PGs outage and failure of the cinder-volume and glance-api services.

Known issues

This section contains the MCP 2019.2.21 known issues and workarounds. For other MCP known issues also applicable to MCP 2019.2.21, see Known issues and corresponding sections in the previous maintenance updates.

- [36960] Redis 5.0 causes update failures in OpenStack Pike deployments
 - [33592] The 'designate-central' service fails due to database absence
-

[36960] Redis 5.0 causes update failures in OpenStack Pike deployments

Applying the MCP 2019.2.21 maintenance update to environments with OpenStack Pike and telemetry enabled may fail during Redis upgrade to version 5.0.

Workaround:

1. Open the cluster level of your deployment model.
2. In `openstack/telemetry.yml`, set the Redis server version to 5.0:

```
redis:  
  server:  
    version: 5.0
```

[33592] The 'designate-central' service fails due to database absence

The designate-central service may fail due to a long database absence, which may be caused, for example, by the Galera upgrade procedure running long.

Workaround:

1. Log in to an OpenStack controller node.
2. Restart the designate-central service on all OpenStack controller nodes:

```
root@ctl01:~# systemctl restart designate-central
```

Updated MCP components

The MCP 2019.2.21 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.20 update.

All 2019.2.21 packages are available at <http://mirror.mirantis.com/update/2019.2.21/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.20	2019.2.21
OpenStack Pike	designate	1:5.0.3-3~u16.04+mcp18	1:5.0.3-3~u16.04+mcp19
	hiredis	n/a	0.14.0-2.1~u16.04+mcp1
	mysql-wsrep-5.7	5.7.36-1~u16.04+mcp1	5.7.36-1~u16.04+mcp2
	nova	2:16.1.8-6~u16.04+mcp311	2:16.1.8-6~u16.04+mcp312
	pyroute2	0.4.21-0.1~u16.04+mcp1	0.5.4-1~u16.04+mcp1
	redis	n/a	5:5.0.14-1~u16.04+mcp1
OpenStack Queens	mysql-wsrep-5.7	5.7.36-1~u16.04+mcp1	5.7.36-1~u16.04+mcp2
	neutron	2:12.1.1-9~u16.04+mcp531	2:12.1.1-9~u16.04+mcp533
	nova	2:17.0.13-9~u16.04+mcp386	2:17.0.13-9~u16.04+mcp387
	panko	4.0.2-3~u16.04+mcp15	4.0.2-3~u16.04+mcp16
	pyroute2	0.4.21-0.1~u16.04+mcp1	0.5.4-1~u16.04+mcp1
	python-openstacksdk	0.11.4-1.0~u16.04+mcp9	0.11.4-1.0~u16.04+mcp10
	python-pymysql	0.8.0-3~u16.04+mcp4	0.8.0-3~u16.04+mcp5
	redis	5:5.0.0-4~u16.04+mcp	5:5.0.14-1~u16.04+mcp1
	OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20220608204809-0

	contrail	4.1~20220608204809-0	4.1~20220822204809-0
	contrail-heat	4.1~20220608204809-0	4.1~20220822204809-0
	contrail-vrouter-dpdk	4.1~20220608204809	4.1~20220822204809
	contrail-web-controller	4.1~20220608204809-0	4.1~20220822204809-0
	contrail-web-core	4.1~20220608204809-0	4.1~20220822204809-0
	neutron-plugin-contrail	4.1~20220608204809-0	4.1~20220822204809-0
Salt formulas	salt-formula-designate	2016.12.1+202109011205.c25ae21~xenial1	2016.12.1+202207272215.a7f0869~xenial1
	salt-formula-keystone	2016.12.1+202202090848.7b768d0~xenial1	2016.12.1+202208111930.655af6d~xenial1
	salt-formula-nova	2016.12.1+202204200839.1a55e09~xenial1	2016.12.1+202208251059.4311a8a~xenial1
	salt-formula-shibboleth	0.0.2+201909240833.f539306~xenial1	0.0.2+202208111729.befc1df~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.21 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.21/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.21/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.21/extra/xenial xenial main

	Ceph	deb http://mirror.mirantis.com/update/2019.2.21/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.21/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.21/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²²	http://mirror.mirantis.com/update/2019.2.21/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.21.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.21.qcow2
	VCP Ubuntu 16.04 image ²²	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.21/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.21/elasticsearch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.21/elasticsearch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.21/elasticsearch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.21/elasticsearch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²²
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.21/glusterfs-5/xenial xenial main ²²

	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.21/maas/xenial xenial main ²²
	Percona	deb http://mirror.mirantis.com/update/2019.2.21/percona/xenial xenial main ²²
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.21/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.21/saltstack-2017.7/xenial xenial main ²² deb http://mirror.mirantis.com/update/2019.2.21/salt-2017.7.8/ xenial xenial main ²²
	Upstream Ubuntu system packages ²²	deb https://mirror.mirantis.com/update/2019.2.21/ubuntu/xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.21/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.21/ubuntu/xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.21
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.21
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.21
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.21
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.19 ²²
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.21 ²²
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.19 ²²
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.19 ²²
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.19 ²²

compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²²
cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²²
gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-reporter:2019.2.21 ²²
gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²²
gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²²
grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.19 ²²
heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²²
jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.19 ²²
jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.19 ²²
ssh-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/ssh-slave:2019.2.20 ²²
mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.21 ²²
openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.19 ²²
phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.21 ²²
postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.24-alpine ²²
prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²²
prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²²
pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²²
registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²²
remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²²

	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.19 ²²
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ²²
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²²

22(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.19 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.20, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. For environments with OpenStack Pike and telemetry enabled, Switch Redis server to version 5. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .

3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .
3 · 1	Galera cluster	<ol style="list-style-type: none"> 1. Update the Galera cluster as described in MCP Operations Guide: Update Galera. 2. Optional. Upgrade Galera to v5.7 as described in Upgrade 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	<p>Select from the following options:</p> <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.20

The MCP 2019.2.20 update introduces enhancements and bug fixes for DriveTrain and OpenStack MCP components and is available starting from July 15, 2022.

Enhancements

In the MCP 2019.2.20 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

- Request limiting for custom locations
- Barbican certificates renewal documentation

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Request limiting for custom locations

Implemented the capability to configure request limiting for custom locations by IP or HTTP.

Learn more

[MCP Operations Guide: Configure request limiting for custom locations](#)

Barbican certificates renewal documentation

Enhanced the MCP Operations Guide by adding instructions on how to renew the administrator or system Barbican certificates stored in Dogtag, as well as on how to add a new LDAP user certificate.

Learn more

[MCP Operations Guide: Barbican certificates](#)

Addressed issues

The MCP 2019.2.20 update contains fixes for several MCP components.

DriveTrain

- [36912] Updated the following Docker images to fix a number of security vulnerabilities: mysql, phpldapadmin, sf-reporter, sh-slave, postgres, alerta.
- [36911] Disabled kernel.unprivileged_usersns_clone to prevent the possibility of exploiting [CVE-2022-1966](#).
- [36892] Fixed defining of resolv.sls with an opportunity to modify the head part of the resolv.conf file.
- [36884] Updated the python-django package to fix the [USN-5269-2](#) and [USN-5373-2](#) security vulnerabilities.
- [36883] Updated the dnsmasq package to fix the [USN-5408-1](#) security vulnerability.
- [36870] Implemented monitoring of internal Barbican certificates to prevent certificate expiry issues.
- [36854] Improved the NGINX Salt formula by implementing the capability to restrict access to custom URLs.

OpenStack

- [36914][Queens] Added the missing interface parameter for Aodh configuration.
- [36889][Queens] Fixed the issue that caused the OpenStack server rebuild API call to fail on the NUMA topology filter. For details, see community issue [1804502](#).
- [36844][Pike, Queens] Fixed the issue wherein the OpenStack CLI showed wrong information about the aggregates with names beginning with a digit.
- [36482][Queens] Fixed the issue wherein an RPC query of an Open vSwitch agent took an excessive amount of time.
- [36773][Pike] Improved server response for some incorrect user data in Heat to prevent server outage.

Known issues

For MCP known issues applicable to MCP 2019.2.20, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.20 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.19 update.

All 2019.2.20 packages are available at <http://mirror.mirantis.com/update/2019.2.20/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.19	2019.2.20
OpenStack Pike	dnsmasq	2.79-1~u16.04+mcp2	2.79-1~u16.04+mcp3
	python-django	1:1.11.29-1~u16.04+mcp6	1:1.11.29-1~u16.04+mcp7
OpenStack Queens	dnsmasq	2.79-1~u16.04+mcp2	2.79-1~u16.04+mcp3
	neutron	2:12.1.1-9~u16.04+mcp530	2:12.1.1-9~u16.04+mcp531
	neutron-fwaas	2:12.0.1-1.1~u16.04+mcp13	2:12.0.2-1.1~u16.04+mcp11
	nova	2:17.0.13-9~u16.04+mcp383	2:17.0.13-9~u16.04+mcp386

	paramiko	2.8.0-1~u16.04+mcp1	2.8.0-1~u16.04+mcp2
	python-django	1:1.11.29-1~u16.04+mcp5	1:1.11.29-1~u16.04+mcp6
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20220415204912-0	4.1~20220608204809-0
	contrail	4.1~20220415204912-0	4.1~20220608204809-0
	contrail-heat	4.1~20220415204912-0	4.1~20220608204809-0
	contrail-vrouter-dpdk	4.1~20220415204912	4.1~20220608204809
	contrail-web-controller	4.1~20220415204912-0	4.1~20220608204809-0
	contrail-web-core	4.1~20220415204912-0	4.1~20220608204809-0
	neutron-plugin-contrail	4.1~20220415204912-0	4.1~20220608204809-0
Salt formulas	salt-formula-dogtag	0.1+202101221336.9cdc1ea~xenial1	0.1+202206240847.16d8a3a~xenial1
	salt-formula-linux	2017.4.1+202109071201.e238712~xenial1	2017.4.1+202206240848.d5f1437~xenial1
	salt-formula-nginx	0.2+202107151609.b43965f~xenial1	0.2+202206031408.0f605c4~xenial1
	salt-formula-oslo-templates	2018.1+202108101148.8e4faa8~xenial1	2018.1+202206171641.cd18262~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.20 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.20/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.20/openstack-queens/xenial xenial main

	Extra packages	deb http://mirror.mirantis.com/update/2019.2.20/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.20/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.20/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.20/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²³	http://mirror.mirantis.com/update/2019.2.20/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.20.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.20.qcow2
	VCP Ubuntu 16.04 image ²³	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.20/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.20/elasticsearch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.20/elasticsearch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.20/elasticsearch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.20/elasticsearch-curator-5/xenial stable main

	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²³
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.20/glusterfs-5/xenial xenial main ²³
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.20/maas/xenial xenial main ²³
	Percona	deb http://mirror.mirantis.com/update/2019.2.20/percona/xenial xenial main ²³
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.20/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.20/saltstack-2017.7/xenial xenial main ²³ deb http://mirror.mirantis.com/update/2019.2.20/salt-2017.7.8/ xenial xenial main ²³
	Upstream Ubuntu system packages ²³	deb https://mirror.mirantis.com/update/2019.2.20/ubuntu/ xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.20/ubuntu/ xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.20/ubuntu/ xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.20
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.20
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.20
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.20
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.19 ²³
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.14 ²³
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.19 ²³

aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.19 ²³
aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.19 ²³
compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²³
cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²³
gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-reporter:2019.2.20 ²³
gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²³
gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²³
grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.19 ²³
heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²³
jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.19 ²³
jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.19 ²³
ssh-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/ssh-slave:2019.2.20 ²³
mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.20 ²³
openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.19 ²³
phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.20 ²³
postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.22-alpine ²³
prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²³
prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²³
pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²³

	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²³
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²³
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.19 ²³
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ²³
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²³

23(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.19 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.19, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.

2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages.
3 · 1	Galera cluster	<ol style="list-style-type: none"> 1. Update the Galera cluster as described in MCP Operations Guide: Update Galera. 2. Optional. Upgrade Galera to v5.7 as described in Upgrade 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 as described in MCP Operations Guide: Update StackLight LMA.
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.19

The MCP 2019.2.19 update introduces bug fixes for DriveTrain, OpenStack, and Ceph MCP components and is available starting from May 16, 2022.

Addressed issues

The MCP 2019.2.19 update contains fixes for several MCP components.

DriveTrain

- [36733] Fixed the issue wherein Jenkins pipeline jobs were broken due to non-updated plugins after performing an offline update of DriveTrain during MCP maintenance update.
- [36817] Fixed the issue that caused MySQL upgrade failure.

- [36876] Increased `wait_timeout` for Jenkins master to fix the issue wherein a timeout error occurred during installation of Jenkins plugins.
- [36787] Enhanced the Nova Salt Formula by implementing the capability to manage the `enable_new_services` parameter (set to `False` by default). This helps to avoid issues with newly deployed OpenStack compute nodes being added to Nova enabled by default.
- [36688] Fixed the issue that caused failure to restore the Cassandra database.
- [36857] Fixed the issue that caused a pipeline-library error to occur after applying MCP maintenance updates.
- [36809] Updated the `qemu` package to fix a number of security vulnerabilities.
- [36851] Updated the `python-oslo.utils` package to fix the [CVE-2022-0718](#) security vulnerability.
- [36852] Updated the `python-paramiko` package to fix the [CVE-2022-24302](#) security vulnerability.

OpenStack

- [36777][Pike] Fixed handling of an invalid input for obtaining all metrics in Gnocchi.
- [36776][Pike] Fixed the issue that caused invalid input validation for Neutron.
- [36775][Pike] Fixed the issue that caused a non-handled error in case of a malformed login request to the Horizon web UI.
- [36774][Pike] Fixed the issue wherein the arguments for namespaces requests failed to be validated, leading to non-handled errors.
- [36772][Pike] Fixed the issue wherein the Heat API response was handled incorrectly.
- [36769][Pike] Fixed the issue wherein invalid requests to API could allow disclosing an internal SQL query.
- [36742][Queens] Fixed the issue that caused inability to create a full volume backup if one backup was already present. The driver now honors whether `--incremental` is specified or not.
- [36693][Pike] Fixed the issue that caused VM `cpuset` overlap during the VM resize after migration.
- [36301][Pike] Fixed the issue wherein VM instances failed to obtain IPv6 addresses through DHCP.
- [36758][Queens] Fixed the issue wherein the L3 agent failed to configure SNAT namespace, which caused an external connectivity issue for instances on attached networks.
- [36689][Queens] Fixed the issue that caused PCI devices within a VM to change order upon an OpenStack compute node reboot.
- [36804][Queens] Fixed the issue that caused MySQL DBDeadlock errors appearing upon the `nova.instance_info_caches` update.

Ceph

- [36797] Fixed the issue wherein addition of a single Ceph OSD node caused all objects in the cloud to be misplaced and caused the cluster to virtually backfill every single placement group.
- [36790] Fixed the issue wherein the Ceph - upgrade and Update Ceph packages Jenkins pipeline jobs were updating packages without checking the consistency between components.

Known issues

For MCP known issues applicable to MCP 2019.2.19, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.19 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.18 update.

All 2019.2.19 packages are available at <http://mirror.mirantis.com/update/2019.2.19/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.18	2019.2.19
OpenStack Pike	gnocchi	4.0.5-3~u16.04+mcp4	4.0.5-3~u16.04+mcp5
	heat	1:9.0.7-2~u16.04+mcp108	1:9.0.7-2~u16.04+mcp112
	horizon	3:12.0.4-5~u16.04+mcp92	3:12.0.4-5~u16.04+mcp95
	mod-wsgi	4.4.15-0.1.1~u16.04+mcp2	4.4.15-0.1.1~u16.04+mcp3
	mysql-wsrep-5.7	5.7.35-1~u16.04+mcp1	5.7.36-1~u16.04+mcp1
	neutron	2:11.0.8-6~u16.04+mcp278	2:11.0.8-6~u16.04+mcp279
	nova	2:16.1.8-6~u16.04+mcp306	2:16.1.8-6~u16.04+mcp311

	paramiko	2.8.0-1~u16.04+mcp1	2.8.0-1~u16.04+mcp2
	python-django-opensack-auth	3.6.1-2~u16.04+mcp10	3.6.1-2~u16.04+mcp11
	python-oslo.db	4.25.2-4~u16.04+mcp12	4.25.2-4~u16.04+mcp13
	python-oslo.utils	3.28.4-1~u16.04+mcp6	3.28.4-1~u16.04+mcp7
	qemu	1:2.11+dfsg-1.7.31~u16.04+mcp1	1:2.11+dfsg-1.7.39~u16.04+mcp1
OpenStack Queens	ironic	1:10.1.10-1.1~u16.04+mcp77	1:10.1.10-1.1~u16.04+mcp79
	mysql-wsrep-5.7	5.7.35-1~u16.04+mcp1	5.7.36-1~u16.04+mcp1
	neutron	2:12.1.1-9~u16.04+mcp519	2:12.1.1-9~u16.04+mcp530
	nova	2:17.0.13-9~u16.04+mcp375	2:17.0.13-9~u16.04+mcp383
	python-openstacksdk	0.11.4-1.0~u16.04+mcp8	0.11.4-1.0~u16.04+mcp9
	python-oslo.db	4.33.4-1.1~u16.04+mcp9	4.33.4-1.1~u16.04+mcp10
	python-oslo.rootwrap	5.13.0-1.0~u16.04+mcp10	5.13.0-1.0~u16.04+mcp11
	python-oslo.utils	3.35.1-1.0~u16.04+mcp8	3.35.1-1.0~u16.04+mcp9
	qemu	1:2.11+dfsg-1.7.31~u16.04+mcp1	1:2.11+dfsg-1.7.39~u16.04+mcp1
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20220208204811-0	4.1~20220415204912-0
	contrail	4.1~20220208204811-0	4.1~20220415204912-0
	contrail-heat	4.1~20220208204811-0	4.1~20220415204912-0
	contrail-vrouter-dpdk	4.1~20220208204811	4.1~20220415204912
	contrail-web-controller	4.1~20220208204811-0	4.1~20220415204912-0

	contrail-web-core	4.1~20220208204811-0	4.1~20220415204912-0
	neutron-plugin-contrail	4.1~20220208204811-0	4.1~20220415204912-0
Salt formulas	salt-formula-ceph	0.1+202108051019.6bac757~xenial1	0.1+202204042203.ded30f9~xenial1
	salt-formula-jenkins	2017.8+202111181744.68c98d4~xenial1	2017.8+202204261034.22b4455~xenial1
	salt-formula-nova	2016.12.1+202109291213.0d675b9~xenial1	2016.12.1+202204200839.1a55e09~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.19 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.19/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.19/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.19/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.19/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.19/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.19/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²⁴	http://mirror.mirantis.com/update/2019.2.19/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2

	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.19.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.19.qcow2
	VCP Ubuntu 16.04 image ²⁴	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.19/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.19/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.19/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.19/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.19/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²⁴
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.19/glusterfs-5/xenial xenial main ²⁴
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.19/maas/xenial xenial main ²⁴
	Percona	deb http://mirror.mirantis.com/update/2019.2.19/percona/xenial xenial main ²⁴

	SaltStack packages	<p>deb http://mirror.mirantis.com/update/2019.2.19/saltstack-2017.7/trusty trusty main</p> <p>deb http://mirror.mirantis.com/update/2019.2.19/saltstack-2017.7/xenial xenial main ²⁴</p> <p>deb http://mirror.mirantis.com/update/2019.2.19/salt-2017.7.8/ xenial xenial main ²⁴</p>
	Upstream Ubuntu system packages ²⁴	<p>deb https://mirror.mirantis.com/update/2019.2.19/ubuntu/xenial main restricted universe</p> <p>deb https://mirror.mirantis.com/update/2019.2.19/ubuntu/xenial-updates main restricted universe</p> <p>deb https://mirror.mirantis.com/update/2019.2.19/ubuntu/xenial-security main restricted universe</p>
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.19
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.19
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.19
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.19
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.19 ²⁴
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.14 ²⁴
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.19 ²⁴
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.19 ²⁴
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.19 ²⁴
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²⁴
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²⁴
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.19 ²⁴

	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²⁴
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²⁴
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.19 ²⁴
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²⁴
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.19 ²⁴
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.19 ²⁴
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.19 ²⁴
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.19 ²⁴
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.19 ²⁴
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.22-alpine ²⁴
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²⁴
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²⁴
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²⁴
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²⁴
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²⁴
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.19 ²⁴
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ²⁴
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²⁴

24(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.18 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.18, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	1. Optional. Verify DriveTrain . 2. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version .
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .
3 . 1	Galera cluster	1. Update the Galera cluster as described in MCP Operations Guide: Update Galera . 2. Optional. Upgrade Galera to v5.7 as described in Upgrade 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.18

The MCP 2019.2.18 update introduces enhancements and bug fixes for DriveTrain, OpenStack, and Ceph MCP components.

The MCP 2019.2.18 update is available starting from March 14, 2022.

Enhancements

In the MCP 2019.2.18 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

- Support for MySQL version 5.7

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Support for MySQL version 5.7

Added support for the MySQL Galera version 5.7. Now, both the 5.6 and 5.7 versions are supported. If required, upgrade your Galera cluster to version 5.7 automatically using the Deploy - upgrade Galera cluster Jenkins pipeline job as described in [MCP Operations Guide: Upgrade Galera to v5.7 automatically](#) or manually as described in [MCP Operations Guide: Upgrade Galera to v5.7 manually](#).

Addressed issues

The MCP 2019.2.18 update contains fixes for the following MCP components:

- DriveTrain:

- [36767] Fixed a number of security vulnerabilities in Docker containers.
- [36761] Fixed the issue that caused the inoperability of periodical backups for Salt Master nodes.
- [36754] Set the default Neutron dhcp_lease_duration parameter to 86400 to avoid the overloading of DHCP agents.
- [36736] Removed a deprecated HAProxy user from MySQL.
- [36734] Fixed the issue that caused the inability to prepare the Jenkins worker node for executing any Salt-based Jenkins pipeline job after upgrading DriveTrain in an offline MCP deployment.
- [36710] Fixed the issues wherein Fluentd failed to keep up with the volume of logs it was expected to process. Enhanced the Fluentd Salt formula to support the multi-worker configuration.
- OpenStack:
 - [36763][Queens] Fixed the issue wherein Cinder ignored the availability zone when retying a volume in a multi-availability zone environment. Added the scheduler_retype_use_az availability zone filter that you can use for retying.
 - [36716][Queens] Fixed the issue wherein the heat_cloudwatch_api backends were down after upgrading OpenStack Pike to Queens.
 - [36719][Pike, Queens] Fixed the wrong time stamp format in the td-agent configuration, which caused failure to ship logs from Panko, Aodh, and Barbican to Elasticsearch.
- Ceph:
 - [36764] Fixed the issue with upmap in Jenkins pipeline jobs that caused an error and proceeded to a standard rebalancing when adding Ceph OSDs into undersized placement groups.

Known issues

This section contains the MCP 2019.2.18 known issues and workarounds. For other MCP known issues also applicable to MCP 2019.2.18, see Known issues and corresponding sections in the previous maintenance updates.

- [36857] A 'pipeline-library' error after applying maintenance update
- [36817] MySQL upgrade failure
- [36733] Broken plugin dependencies after offline update

[36857] A 'pipeline-library' error after applying maintenance update

Fixed in 2019.2.19

Due to a community issue causing incompatibility of several plugins with the current Jenkins version, a pipeline-library error occurs after applying MCP maintenance updates.

Workaround:

1. Log in to the Salt Master node.
2. Update the salt-formula-jenkins package to the version from the MCP maintenance update 2019.2.19 (or newer, if any):

```
wget http://mirror.mirantis.com/update/2019.2.19/salt-formulas/xenial/pool/main/s/salt-formula-jenkins/salt-formula-jenkins_2017.8%2B202204261034.22b4455~xenial1_all.deb  
dpkg -i salt-formula-jenkins*.deb
```

3. Refresh pillars and synchronize Salt modules:

```
salt '*' saltutil.refresh_pillar  
salt '*' saltutil.sync_all
```

4. Apply the jenkins.client.plugin state:

```
salt -C "@jenkins:client and not !@salt:master" state.sls jenkins.client.plugin
```

5. Execute the following script to manually trigger Jenkins restart:

```
JENKINS_USERNAME=$(salt --out newline_values_only -C "@jenkins:client and not !@salt:master" config.get jenkins:client:master:username)  
JENKINS_PASSWORD=$(salt --out newline_values_only -C "@jenkins:client and not !@salt:master" config.get jenkins:client:master:password)  
JENKINS_HOST=$(salt --out newline_values_only -C "@jenkins:client and not !@salt:master" config.get jenkins:client:master:host)  
JENKINS_PORT=$(salt --out newline_values_only -C "@jenkins:client and not !@salt:master" config.get jenkins:client:master:port)  
JENKINS_PROTO=$(salt --out newline_values_only -C "@jenkins:client and not !@salt:master" config.get jenkins:client:master:proto)  
  
cd $(mktemp -d)  
wget "${JENKINS_PROTO}://${JENKINS_HOST}:${JENKINS_PORT}/jnlpjars/jenkins-cli.jar"  
java -jar jenkins-cli.jar -s "${JENKINS_PROTO}://${JENKINS_HOST}:${JENKINS_PORT}" -auth "${JENKINS_USERNAME}:${JENKINS_PASSWORD}" safe-restart
```

6. Verify that Jenkins has successfully rebooted. The following command should return a list of plugins instead of a 50* error:

```
java -jar jenkins-cli.jar -s "${JENKINS_PROTO}://${JENKINS_HOST}:${JENKINS_PORT}" -auth "${JENKINS_USERNAME}:${JENKINS_PASSWORD}" list-plugins
```

7. Apply the changes:

```
salt -C "@jenkins:client and not !@salt:master" state.sls jenkins.client
```

[36817] MySQL upgrade failure

Fixed in 2019.2.19

During the Galera upgrade to v5.7, the mysql-common package should be upgraded to version 5.7.35. If mysql-common 5.7.36 was already installed, the Deploy - upgrade Galera cluster Jenkins pipeline job may fail.

As a workaround, set the OS_DIST_UPGRADE flag in the parameters of the Deploy - upgrade Galera cluster Jenkins pipeline job.

[36733] Broken plugin dependencies after offline update

Fixed in 2019.2.19

Performing an offline update of DriveTrain to MCP maintenance update 2019.2.18 using local mirrors leads to broken plugin dependencies. In this case, Jenkins jobs fail to load Git-based repositories that include pipeline-library, the entry point to all Jenkins pipeline jobs.

Workaround:

1. Download all required plugins from a host with Internet access:

Commands and list of required plugins

```
mkdir -p temp_plugins
cd temp_plugins
rm -rf *.hpi
cat > urls.txt << EOF
http://archives.jenkins-ci.org/plugins/workflow-step-api/622.vb\_8e7c15b\_c95a\_/workflow-step-api.hpi
http://archives.jenkins-ci.org/plugins/workflow-cps/2659.v52d3de6044d0/workflow-cps.hpi
http://archives.jenkins-ci.org/plugins/github-branch-source/2.9.9/github-branch-source.hpi
http://archives.jenkins-ci.org/plugins/apache-httpcomponents-client-4-api/4.5.13-1.0/apache-httpcomponents-client-4-api.hpi
http://archives.jenkins-ci.org/plugins/command-launcher/1.2/command-launcher.hpi
http://archives.jenkins-ci.org/plugins/build-monitor-plugin/1.12+build.201809061734/build-monitor-plugin.hpi
http://archives.jenkins-ci.org/plugins/config-file-provider/3.8.0/config-file-provider.hpi
http://archives.jenkins-ci.org/plugins/bootstrap5-api/5.1.1-1/bootstrap5-api.hpi
http://archives.jenkins-ci.org/plugins/discard-old-build/1.05/discard-old-build.hpi
http://archives.jenkins-ci.org/plugins/blueocean-personalization/1.24.8/blueocean-personalization.hpi
http://archives.jenkins-ci.org/plugins/external-monitor-job/1.4/external-monitor-job.hpi
http://archives.jenkins-ci.org/plugins/token-macro/2.13/token-macro.hpi
http://archives.jenkins-ci.org/plugins/workflow-cps-global-lib/2.19/workflow-cps-global-lib.hpi
http://archives.jenkins-ci.org/plugins/favorite/2.3.2/favorite.hpi
http://archives.jenkins-ci.org/plugins/trilead-api/1.0.13/trilead-api.hpi
http://archives.jenkins-ci.org/plugins/popper-api/1.16.1-2/popper-api.hpi
http://archives.jenkins-ci.org/plugins/jsch/0.1.55.2/jsch.hpi
http://archives.jenkins-ci.org/plugins/credentials-binding/1.27.1/credentials-binding.hpi
http://archives.jenkins-ci.org/plugins/pam-auth/1.5.1/pam-auth.hpi
http://archives.jenkins-ci.org/plugins/okhttp-api/4.9.3-105.vb96869f8ac3a/okhttp-api.hpi
http://archives.jenkins-ci.org/plugins/pipeline-stage-tags-metadata/1.9.3/pipeline-stage-tags-metadata.hpi
http://archives.jenkins-ci.org/plugins/ldap/1.20/ldap.hpi
http://archives.jenkins-ci.org/plugins/performance/3.12/performance.hpi
http://archives.jenkins-ci.org/plugins/copyartifact/1.46.2/copyartifact.hpi
http://archives.jenkins-ci.org/plugins/pipeline-utility-steps/2.1.0/pipeline-utility-steps.hpi
http://archives.jenkins-ci.org/plugins/blueocean-pipeline-api-impl/1.24.8/blueocean-pipeline-api-impl.hpi
http://archives.jenkins-ci.org/plugins/workflow-remote-loader/1.5/workflow-remote-loader.hpi
http://archives.jenkins-ci.org/plugins/blueocean-display-url/2.4.1/blueocean-display-url.hpi
http://archives.jenkins-ci.org/plugins/mercurial/2.14/mercurial.hpi
http://archives.jenkins-ci.org/plugins/echarts-api/5.2.1-2/echarts-api.hpi
http://archives.jenkins-ci.org/plugins/simple-theme-plugin/0.5.1/simple-theme-plugin.hpi
http://archives.jenkins-ci.org/plugins/github-api/1.301-378.v9807bd746da5/github-api.hpi
http://archives.jenkins-ci.org/plugins/matrix-auth/2.6.6/matrix-auth.hpi
EOF
```

<http://archives.jenkins-ci.org/plugins/pubsub-light/1.13/pubsub-light.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-aggregator/2.5/workflow-aggregator.hpi>
<http://archives.jenkins-ci.org/plugins/bootstrap4-api/4.6.0-3/bootstrap4-api.hpi>
<http://archives.jenkins-ci.org/plugins/test-stability/2.3/test-stability.hpi>
<http://archives.jenkins-ci.org/plugins/multiple-scms/0.6/multiple-scms.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-durable-task-step/2.40/workflow-durable-task-step.hpi>
<http://archives.jenkins-ci.org/plugins/jdk-tool/1.1/jdk-tool.hpi>
<http://archives.jenkins-ci.org/plugins/extensible-choice-parameter/1.6.0/extensible-choice-parameter.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-graph-analysis/1.11/pipeline-graph-analysis.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-rest-impl/1.24.8/blueocean-rest-impl.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-jwt/1.24.8/blueocean-jwt.hpi>
<http://archives.jenkins-ci.org/plugins/windows-slaves/1.0/windows-slaves.hpi>
<http://archives.jenkins-ci.org/plugins/envinject/2.3.0/envinject.hpi>
<http://archives.jenkins-ci.org/plugins/email-ext/2.84/email-ext.hpi>
<http://archives.jenkins-ci.org/plugins/caffeine-api/2.9.2-29.v717aac953ff3/caffeine-api.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-autofavorite/1.2.5/blueocean-autofavorite.hpi>
<http://archives.jenkins-ci.org/plugins/handy-uri-templates-2-api/2.1.8-1.0/handy-uri-templates-2-api.hpi>
<http://archives.jenkins-ci.org/plugins/prometheus/2.0.0/prometheus.hpi>
http://archives.jenkins-ci.org/plugins/cloudbees-folder/6.688.vfc7a_a_69059e0/cloudbees-folder.hpi
<http://archives.jenkins-ci.org/plugins/structs/308.v852b473a2b8c/structs.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-support/3.8/workflow-support.hpi>
<http://archives.jenkins-ci.org/plugins/envinject-api/1.8/envinject-api.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-rest/1.24.8/blueocean-rest.hpi>
<http://archives.jenkins-ci.org/plugins/extended-choice-parameter/0.76/extended-choice-parameter.hpi>
<http://archives.jenkins-ci.org/plugins/javadoc/1.6/javadoc.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-scm-step/2.13/workflow-scm-step.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-events/1.24.8/blueocean-events.hpi>
<http://archives.jenkins-ci.org/plugins/sse-gateway/1.24/sse-gateway.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean/1.24.8/blueocean.hpi>
<http://archives.jenkins-ci.org/plugins/monitoring/1.87.0/monitoring.hpi>
<http://archives.jenkins-ci.org/plugins/ant/1.8/ant.hpi>
<http://archives.jenkins-ci.org/plugins/jquery3-api/3.6.0-2/jquery3-api.hpi>
<http://archives.jenkins-ci.org/plugins/artifactory/3.15.4/artifactory.hpi>
<http://archives.jenkins-ci.org/plugins/ace-editor/1.1/ace-editor.hpi>
<http://archives.jenkins-ci.org/plugins/ssh-agent/1.17/ssh-agent.hpi>
<http://archives.jenkins-ci.org/plugins/handlebars/1.1.1/handlebars.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-dashboard/1.24.8/blueocean-dashboard.hpi>
<http://archives.jenkins-ci.org/plugins/popper2-api/2.10.2-1/popper2-api.hpi>
<http://archives.jenkins-ci.org/plugins/display-url-api/2.3.5/display-url-api.hpi>
<http://archives.jenkins-ci.org/plugins/branch-api/2.6.2/branch-api.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-model-extensions/1.9.3/pipeline-model-extensions.hpi>
<http://archives.jenkins-ci.org/plugins/jenkins-design-language/1.24.8/jenkins-design-language.hpi>
<http://archives.jenkins-ci.org/plugins/font-awesome-api/5.15.4-1/font-awesome-api.hpi>
<http://archives.jenkins-ci.org/plugins/junit/1.53/junit.hpi>
<http://archives.jenkins-ci.org/plugins/mailer/1.34.2/mailer.hpi>
<http://archives.jenkins-ci.org/plugins/antisamy-markup-formatter/1.5/antisamy-markup-formatter.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-multibranch/2.24/workflow-multibranch.hpi>

<http://archives.jenkins-ci.org/plugins/credentials/2.6.1/credentials.hpi>
<http://archives.jenkins-ci.org/plugins/git-client/3.9.0/git-client.hpi>
<http://archives.jenkins-ci.org/plugins/github/1.34.2/github.hpi>
<http://archives.jenkins-ci.org/plugins/run-condition/1.5/run-condition.hpi>
<http://archives.jenkins-ci.org/plugins/lockable-resources/2.14/lockable-resources.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-build-step/2.16/pipeline-build-step.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-jira/1.24.8/blueocean-jira.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-i18n/1.24.8/blueocean-i18n.hpi>
<http://archives.jenkins-ci.org/plugins/jira/3.3/jira.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-core-js/1.24.8/blueocean-core-js.hpi>
<http://archives.jenkins-ci.org/plugins/rebuild/1.33/rebuild.hpi>
<http://archives.jenkins-ci.org/plugins/heavy-job/1.1/heavy-job.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-web/1.24.8/blueocean-web.hpi>
<http://archives.jenkins-ci.org/plugins/metrics/4.0.2.2/metrics.hpi>
<http://archives.jenkins-ci.org/plugins/jobConfigHistory/2.18.2/jobConfigHistory.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-milestone-step/1.3.1/pipeline-milestone-step.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-rest-api/2.10/pipeline-rest-api.hpi>
<http://archives.jenkins-ci.org/plugins/authentication-tokens/1.3/authentication-tokens.hpi>
<http://archives.jenkins-ci.org/plugins/snakeyaml-api/1.29.1/snakeyaml-api.hpi>
<http://archives.jenkins-ci.org/plugins/ivy/2.1/ivy.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-stage-step/291.vf0a8a7aeeb50/pipeline-stage-step.hpi>
<http://archives.jenkins-ci.org/plugins/htmlpublisher/1.25/htmlpublisher.hpi>
<http://archives.jenkins-ci.org/plugins/docker-workflow/1.17/docker-workflow.hpi>
<http://archives.jenkins-ci.org/plugins/momentjs/1.1.1/momentjs.hpi>
<http://archives.jenkins-ci.org/plugins/maven-plugin/3.8.1/maven-plugin.hpi>
<http://archives.jenkins-ci.org/plugins/build-timeout/1.19/build-timeout.hpi>
<http://archives.jenkins-ci.org/plugins/categorized-view/1.10/categorized-view.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-input-step/427.va6441fa17010/pipeline-input-step.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-config/1.24.8/blueocean-config.hpi>
<http://archives.jenkins-ci.org/plugins/bouncycastle-api/2.17/bouncycastle-api.hpi>
<http://archives.jenkins-ci.org/plugins/slack/2.49/slack.hpi>
<http://archives.jenkins-ci.org/plugins/durable-task/1.37/durable-task.hpi>
<http://archives.jenkins-ci.org/plugins/plugin-util-api/2.5.0/plugin-util-api.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-basic-steps/2.24/workflow-basic-steps.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-bitbucket-pipeline/1.24.8/blueocean-bitbucket-pipeline.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-model-definition/1.9.3/pipeline-model-definition.hpi>
<http://archives.jenkins-ci.org/plugins/gradle/1.29/gradle.hpi>
<http://archives.jenkins-ci.org/plugins/plain-credentials/1.8/plain-credentials.hpi>
<http://archives.jenkins-ci.org/plugins/checks-api/1.7.2/checks-api.hpi>
<http://archives.jenkins-ci.org/plugins/variant/1.4/variant.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-pipeline-editor/1.24.8/blueocean-pipeline-editor.hpi>
http://archives.jenkins-ci.org/plugins/script-security/1138.v8e727069a_025/script-security.hpi
<http://archives.jenkins-ci.org/plugins/audit-trail/3.8/audit-trail.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-commons/1.24.8/blueocean-commons.hpi>
<http://archives.jenkins-ci.org/plugins/build-blocker-plugin/1.7.3/build-blocker-plugin.hpi>
<http://archives.jenkins-ci.org/plugins/ssh-credentials/1.18.1/ssh-credentials.hpi>
<http://archives.jenkins-ci.org/plugins/timestamper/1.16/timestamper.hpi>

```
http://archives.jenkins-ci.org/plugins/git-server/1.9/git-server.hpi
http://archives.jenkins-ci.org/plugins/pipeline-stage-view/2.10/pipeline-stage-view.hpi
http://archives.jenkins-ci.org/plugins/throttle-concurrents/2.0.1/throttle-concurrents.hpi
http://archives.jenkins-ci.org/plugins/description-setter/1.10/description-setter.hpi
http://archives.jenkins-ci.org/plugins/gerrit-trigger/2.35.2/gerrit-trigger.hpi
http://archives.jenkins-ci.org/plugins/matrix-project/1.18.1/matrix-project.hpi
http://archives.jenkins-ci.org/plugins/blueocean-git-pipeline/1.24.8/blueocean-git-pipeline.hpi
http://archives.jenkins-ci.org/plugins/pipeline-model-api/1.9.3/pipeline-model-api.hpi
http://archives.jenkins-ci.org/plugins/git/4.8.3/git.hpi
http://archives.jenkins-ci.org/plugins/jquery/1.12.4-0/jquery.hpi
http://archives.jenkins-ci.org/plugins/build-user-vars-plugin/1.5/build-user-vars-plugin.hpi
http://archives.jenkins-ci.org/plugins/workflow-job/1145.v7f2433caa07f/workflow-job.hpi
http://archives.jenkins-ci.org/plugins/permissive-script-security/0.3/permissive-script-security.hpi
http://archives.jenkins-ci.org/plugins/jquery-detached/1.2.1/jquery-detached.hpi
http://archives.jenkins-ci.org/plugins/scm-api/2.6.5/scm-api.hpi
http://archives.jenkins-ci.org/plugins/blueocean-pipeline-scm-api/1.24.8/blueocean-pipeline-scm-api.hpi
http://archives.jenkins-ci.org/plugins/blueocean-github-pipeline/1.24.8/blueocean-github-pipeline.hpi
http://archives.jenkins-ci.org/plugins/workflow-api/1138.v619fd5201b_2f/workflow-api.hpi
http://archives.jenkins-ci.org/plugins/docker-commons/1.13/docker-commons.hpi
http://archives.jenkins-ci.org/plugins/ssh-slaves/1.29.4/ssh-slaves.hpi
http://archives.jenkins-ci.org/plugins/pipeline-model-declarative-agent/1.1.1/pipeline-model-declarative-agent.hpi
http://archives.jenkins-ci.org/plugins/jackson2-api/2.13.1-246.va8a9f3eaf46a/jackson2-api.hpi
http://archives.jenkins-ci.org/plugins/plot/2.1.0/plot.hpi
http://archives.jenkins-ci.org/plugins/cloudbees-bitbucket-branch-source/726.vb0c1ea6c9336/cloudbees-bitbucket-branch-source.hpi
http://archives.jenkins-ci.org/plugins/jjwt-api/0.11.2-9.c8b45b8bb173/jjwt-api.hpi
EOF
wget -i urls.txt
```

- Using any available tools and data channels, move all .hpi files to /root/temp_plugins/ of the DriveTrain LCM engine node (cid01).
- Log in to the cid01 node as root.
- Obtain the DriveTrain Jenkins endpoint and credentials:

```
salt-call pillar.get jenkins:client:master
```

Copy these elements to use in the commands that follow: Jenkins IP, port, login, password.

- Download the jenkins-cli client from the DriveTrain Jenkins to the /root folder:

```
wget https://%JENKINS_IP%:%JENKINS_PORT%/jnlpjars/jenkins-cli.jar
```

- Verify that the jenkins-cli client is operating properly:

```
java -jar jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% list-plugins
```

The command output should include a list of all installed plugins and versions.

Note

In the steps that follow, assume that the .hpi files are located in the /root/temp_plugins directory.

7. Copy the .hpi plugin files to the Docker volume.

Note

The CLI tool requires an accessible URI to install the plugin, file:// in the example below.

```
rm -rf /srv/volumes/jenkins/fresh_plugins
mkdir /srv/volumes/jenkins/fresh_plugins
chmod 755 /srv/volumes/jenkins/fresh_plugins
cd /root/temp_plugins
cp *.hpi /srv/volumes/jenkins/fresh_plugins/
chmod 644 /srv/volumes/jenkins/fresh_plugins/*.hpi
```

8. Install the plugins:

```
ls *.hpi | xargs -t {} java -jar ../jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% install-plugin file:///var/jenkins_home/fresh_plugins/{}
```

9. Remove the temporary folder from the Docker volume:

```
rm -rf /srv/volumes/jenkins/fresh_plugins
```

10 Reboot Jenkins:

```
cd /root/
java -jar jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% safe-restart
```

Rebooting requires some time. During this time, Jenkins responds with 503 errors.

11 Verify the successful rebooting of Jenkins:

```
java -jar jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% list-plugins
```

If Jenkins is up and running, the output will include plugins in the place of Java tracebacks.

Updated MCP components

The MCP 2019.2.18 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.17 update.

All 2019.2.18 packages are available at <http://mirror.mirantis.com/update/2019.2.18/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.17	2019.2.18
OpenStack Pike	mysql-wsrep-5.7	n/a	5.7.35-1~u16.04+mcp1
OpenStack Queens	cinder	2:12.0.10-3~u16.04+mcp163	2:12.0.10-3~u16.04+mcp165
	mysql-wsrep-5.7	n/a	5.7.35-1~u16.04+mcp1
	neutron	2:12.1.1-9~u16.04+mcp501	2:12.1.1-9~u16.04+mcp519
	nova	2:17.0.13-9~u16.04+mcp372	2:17.0.13-9~u16.04+mcp375
	python-openstacksdk	0.11.4-1.0~u16.04+mcp7	0.11.4-1.0~u16.04+mcp8
	tempest	1:18.0.0-1~u16.04+mcp49	1:18.0.0-1~u16.04+mcp50
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20211115204810-0	4.1~20220208204811-0
	contrail	4.1~20211115204810-0	4.1~20220208204811-0
	contrail-heat	4.1~20211115204810-0	4.1~20220208204811-0
	contrail-vrouter-dpdk	4.1~20211115204810	4.1~20220208204811
	contrail-web-controller	4.1~20211115204810-0	4.1~20220208204811-0
	contrail-web-core	4.1~20211115204810-0	4.1~20220208204811-0
	neutron-plugin-contrail	4.1~20211115204810-0	4.1~20220208204811-0
Salt formulas	salt-formula-aodh	0.2+202108311502.edbfbe8~xenial1	0.2+202202012215.4295f02~xenial1
	salt-formula-barbican	2018.1+202109010910.022c812~xenial1	2018.1+202202011235.bd9afa2~xenial1
	salt-formula-fluentd	0.1+202111011102.502878a~xenial1	0.1+202202150823.31e6c81~xenial1
	salt-formula-galera	1.0+202104021252.1bc3f26~xenial1	1.0+202202111716.4007a0e~xenial1

	salt-formula-keystone	2016.12.1+202108301124.89d65be~xenial1	2016.12.1+202202090848.7b768d0~xenial1
	salt-formula-mysql	0.2+201911111532.7acd6b9~xenial1	0.2+202202030947.0c40fac~xenial1
	salt-formula-panko	2017.6+202109011200.4a9181a~xenial1	2017.6+202202011633.30da83d~xenial1
	salt-formula-xtrabackup	0.2+202104280838.551ef05~xenial1	0.2+202202090921.8566c57~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.18 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.18/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.18/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.18/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.18/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.18/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.18/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²⁵	http://mirror.mirantis.com/update/2019.2.18/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.18.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.18.qcow2

	VCP Ubuntu 16.04 image ²⁵	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.18/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.18/elastics earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.18/elastics earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.18/elastics earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.18/elastics earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²⁵
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.18/glusterfs-5/xenial xenial main ²⁵
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.18/maas/xenial xenial main ²⁵
	Percona	deb http://mirror.mirantis.com/update/2019.2.18/percona/xenial xenial main ²⁵
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.18/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.18/saltstack-2017.7/xenial xenial main ²⁵ deb http://mirror.mirantis.com/update/2019.2.18/salt-2017.7.8/ xenial xenial main ²⁵

	Upstream Ubuntu system packages ²⁵	deb https://mirror.mirantis.com/update/2019.2.18/ubuntu/xenial/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.18/ubuntu/xenial-updates/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.18/ubuntu/xenial-security/main/restricted/universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.18
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.18
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.18
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.18
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.18 ²⁵
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.14 ²⁵
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.16 ²⁵
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.16 ²⁵
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.16 ²⁵
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²⁵
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²⁵
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.18 ²⁵
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²⁵
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²⁵
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.16 ²⁵

	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²⁵
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.18 ²⁵
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.18 ²⁵
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.17 ²⁵
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.18 ²⁵
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.18 ²⁵
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.22-alpine ²⁵
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²⁵
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²⁵
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²⁵
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²⁵
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²⁵
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.18 ²⁵
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ²⁵
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²⁵

25(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.17 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.17, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> Optional. Verify DriveTrain. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .
3 . 1	Galera cluster	<ol style="list-style-type: none"> Update the Galera cluster as described in MCP Operations Guide: Update Galera. Optional. Upgrade Galera to v5.7 as described in Upgrade 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.17

The MCP 2019.2.17 update introduces enhancements and bug fixes for DriveTrain, OpenStack, StackLight, and Ceph MCP components.

The MCP 2019.2.17 update is available starting from December 22, 2021.

Enhancements

In the MCP 2019.2.17 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.17 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Security updates for Docker containers
- Pre-update DriveTrain verification

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Security updates for Docker containers

Updated the MySQL, phpLDAPadmin, and Salesforce reporter Docker containers, as well as a number of packages, to fix security vulnerabilities.

Pre-update DriveTrain verification

Implemented the Deploy - pre upgrade verify MCP Drivetrain Jenkins pipeline job that you can use before applying a maintenance update to verify that your deployment model has the needed pillars.

Use Deploy - pre upgrade verify MCP Drivetrain before applying the next maintenance update.

Learn more

[MCP Operations Guide: Verify DriveTrain](#)

OpenStack

In the MCP 2019.2.17 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Glance database cleanup

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

Glance database cleanup

Implemented the capability to automatically clean up the Glance database using the Deploy - Openstack Database Cleanup Jenkins pipeline job.

Learn more

[MCP Operations Guide: Clean up an OpenStack database](#)

StackLight

In the MCP 2019.2.17 maintenance update, Mirantis introduces the following enhancements for StackLight:

- HTTP output for Fluentd

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

HTTP output for Fluentd

Implemented the following improvements for StackLight:

- Updated td-agent to version 3.8.
- Added support of the HTTP output for the Fluentd plugin.

Addressed issues

The MCP 2019.2.17 update contains fixes for several MCP components.

DriveTrain

- [36686] Fixed the issue with redundant newline for inline GPG-encoded pillars.
- [36684] Fixed the issue with some CVP Jenkins pipelines failing due to missing python-dev package.
- [36665] Updated the python-paramiko package for a proper support of ecdsa-sha2-nistp.
- [36624] Fixed the issue causing inability to set flush_thread_count for the Fluentd HTTP output.
- [36641] Fixed the issue with the Deploy - upgrade MCP DriveTrain Jenkins pipeline job failing with a timeout while executing the reclass -i 2>/dev/null | gzip -9 -c | base64 command on the Salt Master node.
- [36623] Fixed the issue causing inability to install Fluentd Gem plugins when running behind an HTTP proxy.

OpenStack

- [36666][Pike, Queens] Fixed the issue with the Nova and Neutron services leaving zombie processes on the OpenStack compute nodes.
- [36662][Pike] Added a workaround flag waiting for the vif-plugged event during the libvirt reboot to avoid issues with the domain starting to run and requesting the IP through DHCP before the networking backend finishes plugging the VIFs (virtual interfaces).
- [36664][Queens] Fixed the issue with VMs failing to start with the device not found error message after a reboot.
- [36617][Pike, Queens] Fixed the issue with the Neutron Salt formula not providing a trace if wrong network ranges were passed.
- [36587][Queens] Fixed the issue causing inability to remove deprecated Designate V1 resources through Heat.
- [36590][Queens] Added the capability to sort PCI device pools so that devices are picked in a more predictable order.
- [36629][Queens] Fixed the issue with Neutron failing to update the DVR router due to an integrity error for the DVR port bindings.
- [36595][Pike, Queens] Added the capability to purge all deleted rows of a Glance database simultaneously.

StackLight

- [36454] Added the missing `openstack_neutron_lbaas_loadbalancer_provisioning_status` and `openstack_neutron_lbaas_loadbalancer_status` load balancer metrics dividing the load balancer state to operating and provisioning, which allows identifying:
 - How many load balancers are in a specific state
 - The ID of the load balancer in a specific state
- [36654] Updated `prometheus-es-exporter` to version 0.14.0 to fix gaps in metrics.
- [36715] Fixed the issue in the Apache configuration causing `Fluentd` not to collect logs from several OpenStack services.

Ceph

- [36461] Fixed the issue with the Ceph - add osd Jenkins pipeline job failing on health checks with warnings not related to data safety.

Known issues

This section contains the MCP 2019.2.17 known issues and workarounds. For other MCP known issues also applicable to MCP 2019.2.17, see Known issues and corresponding sections in the previous maintenance updates.

- [36857] A 'pipeline-library' error after applying maintenance update
 - [36736] Deprecated `HAProxy` user in MySQL database
 - [36733] Broken plugin dependencies after offline update
-

[36857] A 'pipeline-library' error after applying maintenance update

Due to a community issue causing incompatibility of several plugins with the current Jenkins version, a pipeline-library error occurs after applying MCP maintenance updates.

Workaround:

1. Log in to the Salt Master node.
2. Update the `salt-formula-jenkins` package to the version from the MCP maintenance update 2019.2.19 (or newer, if any):

```
wget http://mirror.mirantis.com/update/2019.2.19/salt-formulas/xenial/pool/main/s/salt-formula-jenkins/salt-formula-jenkins_2017.8%2B202204261034.22b4455~xenial1_all.deb  
dpkg -i salt-formula-jenkins*.deb
```

3. Refresh pillars and synchronize Salt modules:

```
salt '*' saltutil.refresh_pillar  
salt '*' saltutil.sync_all
```

4. Apply the `jenkins.client.plugin` state:

```
salt -C "!@jenkins:client and not !@salt:master" state.sls jenkins.client.plugin
```

5. Execute the following script to manually trigger Jenkins restart:

```
JENKINS_USERNAME=$(salt --out newline_values_only -C '!@jenkins:client and not !@salt:master' config.get jenkins:client:master:username)
JENKINS_PASSWORD=$(salt --out newline_values_only -C '!@jenkins:client and not !@salt:master' config.get jenkins:client:master:password)
JENKINS_HOST=$(salt --out newline_values_only -C '!@jenkins:client and not !@salt:master' config.get jenkins:client:master:host)
JENKINS_PORT=$(salt --out newline_values_only -C '!@jenkins:client and not !@salt:master' config.get jenkins:client:master:port)
JENKINS_PROTO=$(salt --out newline_values_only -C '!@jenkins:client and not !@salt:master' config.get jenkins:client:master:proto)

cd $(mktemp -d)
wget "${JENKINS_PROTO}://${JENKINS_HOST}:${JENKINS_PORT}/jnlpjars/jenkins-cli.jar"
java -jar jenkins-cli.jar -s "${JENKINS_PROTO}://${JENKINS_HOST}:${JENKINS_PORT}" -auth "${JENKINS_USERNAME}:${JENKINS_PASSWORD}" safe-restart
```

6. Verify that Jenkins has successfully rebooted. The following command should return a list of plugins instead of a 50* error:

```
java -jar jenkins-cli.jar -s "${JENKINS_PROTO}://${JENKINS_HOST}:${JENKINS_PORT}" -auth "${JENKINS_USERNAME}:${JENKINS_PASSWORD}" list-plugins
```

7. Apply the changes:

```
salt -C "!@jenkins:client and not !@salt:master" state.sls jenkins.client
```

[36736] Deprecated HAProxy user in MySQL database

Fixed in 2019.2.18

The MySQL database contains a deprecated HAProxy user without a password. Remove the user as described below.

Workaround:

1. Log in to the Salt Master node.
2. Remove the deprecated HAProxy user:

```
salt -C "!@galera:master" cmd.run "mysql --defaults-file=/etc/mysql/debian.cnf -D mysql -e \"delete from user where user = 'haproxy'\""
```

[36733] Broken plugin dependencies after offline update

Fixed in 2019.2.19

Performing an offline update of DriveTrain to MCP maintenance update 2019.2.17 using local mirrors leads to broken plugin dependencies. In this case, Jenkins jobs fail to load Git-based repositories that include pipeline-library, the entry point to all Jenkins pipeline jobs.

Workaround:

1. Download the following plugins from a host with Internet access:

Commands and list of required plugins

```
mkdir -p temp_plugins
cd temp_plugins
rm -rf *.hpi
cat > urls.txt << EOF
http://archives.jenkins-ci.org/plugins/workflow-step-api/622.vb_8e7c15b_c95a_workflow-step-api.hpi
http://archives.jenkins-ci.org/plugins/workflow-cps/2659.v52d3de6044d0/workflow-cps.hpi
http://archives.jenkins-ci.org/plugins/github-branch-source/2.9.9/github-branch-source.hpi
http://archives.jenkins-ci.org/plugins/apache-httpcomponents-client-4-api/4.5.13-1.0/apache-httpcomponents-client-4-api.hpi
http://archives.jenkins-ci.org/plugins/command-launcher/1.2/command-launcher.hpi
http://archives.jenkins-ci.org/plugins/build-monitor-plugin/1.12+build.201809061734/build-monitor-plugin.hpi
http://archives.jenkins-ci.org/plugins/config-file-provider/3.8.0/config-file-provider.hpi
http://archives.jenkins-ci.org/plugins/bootstrap5-api/5.1.1-1/bootstrap5-api.hpi
http://archives.jenkins-ci.org/plugins/discard-old-build/1.05/discard-old-build.hpi
http://archives.jenkins-ci.org/plugins/blueocean-personalization/1.24.8/blueocean-personalization.hpi
http://archives.jenkins-ci.org/plugins/external-monitor-job/1.4/external-monitor-job.hpi
http://archives.jenkins-ci.org/plugins/token-macro/2.13/token-macro.hpi
http://archives.jenkins-ci.org/plugins/workflow-cps-global-lib/2.19/workflow-cps-global-lib.hpi
http://archives.jenkins-ci.org/plugins/favorite/2.3.2/favorite.hpi
http://archives.jenkins-ci.org/plugins/trilead-api/1.0.13/trilead-api.hpi
http://archives.jenkins-ci.org/plugins/popper-api/1.16.1-2/popper-api.hpi
http://archives.jenkins-ci.org/plugins/jsch/0.1.55.2/jsch.hpi
http://archives.jenkins-ci.org/plugins/credentials-binding/1.27.1/credentials-binding.hpi
http://archives.jenkins-ci.org/plugins/pam-auth/1.5.1/pam-auth.hpi
http://archives.jenkins-ci.org/plugins/okhttp-api/4.9.3-105.vb96869f8ac3a/okhttp-api.hpi
http://archives.jenkins-ci.org/plugins/pipeline-stage-tags-metadata/1.9.3/pipeline-stage-tags-metadata.hpi
http://archives.jenkins-ci.org/plugins/ldap/1.20/ldap.hpi
http://archives.jenkins-ci.org/plugins/performance/3.12/performance.hpi
http://archives.jenkins-ci.org/plugins/copyartifact/1.46.2/copyartifact.hpi
http://archives.jenkins-ci.org/plugins/pipeline-utility-steps/2.1.0/pipeline-utility-steps.hpi
http://archives.jenkins-ci.org/plugins/blueocean-pipeline-api-impl/1.24.8/blueocean-pipeline-api-impl.hpi
http://archives.jenkins-ci.org/plugins/workflow-remote-loader/1.5/workflow-remote-loader.hpi
http://archives.jenkins-ci.org/plugins/blueocean-display-url/2.4.1/blueocean-display-url.hpi
http://archives.jenkins-ci.org/plugins/mercurial/2.14/mercurial.hpi
http://archives.jenkins-ci.org/plugins/echarts-api/5.2.1-2/echarts-api.hpi
http://archives.jenkins-ci.org/plugins/simple-theme-plugin/0.5.1/simple-theme-plugin.hpi
http://archives.jenkins-ci.org/plugins/github-api/1.301-378.v9807bd746da5/github-api.hpi
http://archives.jenkins-ci.org/plugins/matrix-auth/2.6.6/matrix-auth.hpi
http://archives.jenkins-ci.org/plugins/pubsub-light/1.13/pubsub-light.hpi
http://archives.jenkins-ci.org/plugins/workflow-aggregator/2.5/workflow-aggregator.hpi
http://archives.jenkins-ci.org/plugins/bootstrap4-api/4.6.0-3/bootstrap4-api.hpi
http://archives.jenkins-ci.org/plugins/test-stability/2.3/test-stability.hpi
http://archives.jenkins-ci.org/plugins/multiple-scms/0.6/multiple-scms.hpi
http://archives.jenkins-ci.org/plugins/workflow-durable-task-step/2.40/workflow-durable-task-step.hpi
http://archives.jenkins-ci.org/plugins/jdk-tool/1.1/jdk-tool.hpi
http://archives.jenkins-ci.org/plugins/extensible-choice-parameter/1.6.0/extensible-choice-parameter.hpi
http://archives.jenkins-ci.org/plugins/pipeline-graph-analysis/1.11/pipeline-graph-analysis.hpi
http://archives.jenkins-ci.org/plugins/blueocean-rest-impl/1.24.8/blueocean-rest-impl.hpi
```

<http://archives.jenkins-ci.org/plugins/blueocean-jwt/1.24.8/blueocean-jwt.hpi>
<http://archives.jenkins-ci.org/plugins/windows-slaves/1.0/windows-slaves.hpi>
<http://archives.jenkins-ci.org/plugins/envinject/2.3.0/envinject.hpi>
<http://archives.jenkins-ci.org/plugins/email-ext/2.84/email-ext.hpi>
<http://archives.jenkins-ci.org/plugins/caffeine-api/2.9.2-29.v717aac953ff3/caffeine-api.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-autofavorite/1.2.5/blueocean-autofavorite.hpi>
<http://archives.jenkins-ci.org/plugins/handy-uri-templates-2-api/2.1.8-1.0/handy-uri-templates-2-api.hpi>
<http://archives.jenkins-ci.org/plugins/prometheus/2.0.0/prometheus.hpi>
http://archives.jenkins-ci.org/plugins/cloudbees-folder/6.688.vfc7a_a_69059e0/cloudbees-folder.hpi
<http://archives.jenkins-ci.org/plugins/structs/308.v852b473a2b8c/structs.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-support/3.8/workflow-support.hpi>
<http://archives.jenkins-ci.org/plugins/envinject-api/1.8/envinject-api.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-rest/1.24.8/blueocean-rest.hpi>
<http://archives.jenkins-ci.org/plugins/extended-choice-parameter/0.76/extended-choice-parameter.hpi>
<http://archives.jenkins-ci.org/plugins/javadoc/1.6/javadoc.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-scm-step/2.13/workflow-scm-step.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-events/1.24.8/blueocean-events.hpi>
<http://archives.jenkins-ci.org/plugins/sse-gateway/1.24/sse-gateway.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean/1.24.8/blueocean.hpi>
<http://archives.jenkins-ci.org/plugins/monitoring/1.87.0/monitoring.hpi>
<http://archives.jenkins-ci.org/plugins/ant/1.8/ant.hpi>
<http://archives.jenkins-ci.org/plugins/jquery3-api/3.6.0-2/jquery3-api.hpi>
<http://archives.jenkins-ci.org/plugins/artifactory/3.15.4/artifactory.hpi>
<http://archives.jenkins-ci.org/plugins/ace-editor/1.1/ace-editor.hpi>
<http://archives.jenkins-ci.org/plugins/ssh-agent/1.17/ssh-agent.hpi>
<http://archives.jenkins-ci.org/plugins/handlebars/1.1.1/handlebars.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-dashboard/1.24.8/blueocean-dashboard.hpi>
<http://archives.jenkins-ci.org/plugins/popper2-api/2.10.2-1/popper2-api.hpi>
<http://archives.jenkins-ci.org/plugins/display-url-api/2.3.5/display-url-api.hpi>
<http://archives.jenkins-ci.org/plugins/branch-api/2.6.2/branch-api.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-model-extensions/1.9.3/pipeline-model-extensions.hpi>
<http://archives.jenkins-ci.org/plugins/jenkins-design-language/1.24.8/jenkins-design-language.hpi>
<http://archives.jenkins-ci.org/plugins/font-awesome-api/5.15.4-1/font-awesome-api.hpi>
<http://archives.jenkins-ci.org/plugins/junit/1.53/junit.hpi>
<http://archives.jenkins-ci.org/plugins/mailer/1.34.2/mailer.hpi>
<http://archives.jenkins-ci.org/plugins/antisamy-markup-formatter/1.5/antisamy-markup-formatter.hpi>
<http://archives.jenkins-ci.org/plugins/workflow-multibranch/2.24/workflow-multibranch.hpi>
<http://archives.jenkins-ci.org/plugins/credentials/2.6.1/credentials.hpi>
<http://archives.jenkins-ci.org/plugins/git-client/3.9.0/git-client.hpi>
<http://archives.jenkins-ci.org/plugins/github/1.34.2/github.hpi>
<http://archives.jenkins-ci.org/plugins/run-condition/1.5/run-condition.hpi>
<http://archives.jenkins-ci.org/plugins/lockable-resources/2.14/lockable-resources.hpi>
<http://archives.jenkins-ci.org/plugins/pipeline-build-step/2.16/pipeline-build-step.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-jira/1.24.8/blueocean-jira.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-i18n/1.24.8/blueocean-i18n.hpi>
<http://archives.jenkins-ci.org/plugins/jira/3.3/jira.hpi>
<http://archives.jenkins-ci.org/plugins/blueocean-core-js/1.24.8/blueocean-core-js.hpi>

```
http://archives.jenkins-ci.org/plugins/rebuild/1.33/rebuild.hpi
http://archives.jenkins-ci.org/plugins/heavy-job/1.1/heavy-job.hpi
http://archives.jenkins-ci.org/plugins/blueocean-web/1.24.8/blueocean-web.hpi
http://archives.jenkins-ci.org/plugins/metrics/4.0.2.2/metrics.hpi
http://archives.jenkins-ci.org/plugins/jobConfigHistory/2.18.2/jobConfigHistory.hpi
http://archives.jenkins-ci.org/plugins/pipeline-milestone-step/1.3.1/pipeline-milestone-step.hpi
http://archives.jenkins-ci.org/plugins/pipeline-rest-api/2.10/pipeline-rest-api.hpi
http://archives.jenkins-ci.org/plugins/authentication-tokens/1.3/authentication-tokens.hpi
http://archives.jenkins-ci.org/plugins/snakeyaml-api/1.29.1/snakeyaml-api.hpi
http://archives.jenkins-ci.org/plugins/ivy/2.1/ivy.hpi
http://archives.jenkins-ci.org/plugins/pipeline-stage-step/291.vf0a8a7aeeb50/pipeline-stage-step.hpi
http://archives.jenkins-ci.org/plugins/htmlpublisher/1.25/htmlpublisher.hpi
http://archives.jenkins-ci.org/plugins/docker-workflow/1.17/docker-workflow.hpi
http://archives.jenkins-ci.org/plugins/momentjs/1.1.1/momentjs.hpi
http://archives.jenkins-ci.org/plugins/maven-plugin/3.8.1/maven-plugin.hpi
http://archives.jenkins-ci.org/plugins/build-timeout/1.19/build-timeout.hpi
http://archives.jenkins-ci.org/plugins/categorized-view/1.10/categorized-view.hpi
http://archives.jenkins-ci.org/plugins/pipeline-input-step/427.va6441fa17010/pipeline-input-step.hpi
http://archives.jenkins-ci.org/plugins/blueocean-config/1.24.8/blueocean-config.hpi
http://archives.jenkins-ci.org/plugins/bouncycastle-api/2.17/bouncycastle-api.hpi
http://archives.jenkins-ci.org/plugins/slack/2.49/slack.hpi
http://archives.jenkins-ci.org/plugins/durable-task/1.37/durable-task.hpi
http://archives.jenkins-ci.org/plugins/plugin-util-api/2.5.0/plugin-util-api.hpi
http://archives.jenkins-ci.org/plugins/workflow-basic-steps/2.24/workflow-basic-steps.hpi
http://archives.jenkins-ci.org/plugins/blueocean-bitbucket-pipeline/1.24.8/blueocean-bitbucket-pipeline.hpi
http://archives.jenkins-ci.org/plugins/pipeline-model-definition/1.9.3/pipeline-model-definition.hpi
http://archives.jenkins-ci.org/plugins/gradle/1.29/gradle.hpi
http://archives.jenkins-ci.org/plugins/plain-credentials/1.8/plain-credentials.hpi
http://archives.jenkins-ci.org/plugins/checks-api/1.7.2/checks-api.hpi
http://archives.jenkins-ci.org/plugins/variant/1.4/variant.hpi
http://archives.jenkins-ci.org/plugins/blueocean-pipeline-editor/1.24.8/blueocean-pipeline-editor.hpi
http://archives.jenkins-ci.org/plugins/script-security/1138.v8e727069a_025/script-security.hpi
http://archives.jenkins-ci.org/plugins/audit-trail/3.8/audit-trail.hpi
http://archives.jenkins-ci.org/plugins/blueocean-commons/1.24.8/blueocean-commons.hpi
http://archives.jenkins-ci.org/plugins/build-blocker-plugin/1.7.3/build-blocker-plugin.hpi
http://archives.jenkins-ci.org/plugins/ssh-credentials/1.18.1/ssh-credentials.hpi
http://archives.jenkins-ci.org/plugins/timestamper/1.16/timestamper.hpi
http://archives.jenkins-ci.org/plugins/git-server/1.9/git-server.hpi
http://archives.jenkins-ci.org/plugins/pipeline-stage-view/2.10/pipeline-stage-view.hpi
http://archives.jenkins-ci.org/plugins/throttle-concurrents/2.0.1/throttle-concurrents.hpi
http://archives.jenkins-ci.org/plugins/description-setter/1.10/description-setter.hpi
http://archives.jenkins-ci.org/plugins/gerrit-trigger/2.35.2/gerrit-trigger.hpi
http://archives.jenkins-ci.org/plugins/matrix-project/1.18.1/matrix-project.hpi
http://archives.jenkins-ci.org/plugins/blueocean-git-pipeline/1.24.8/blueocean-git-pipeline.hpi
http://archives.jenkins-ci.org/plugins/pipeline-model-api/1.9.3/pipeline-model-api.hpi
http://archives.jenkins-ci.org/plugins/git/4.8.3/git.hpi
http://archives.jenkins-ci.org/plugins/jquery/1.12.4-0/jquery.hpi
http://archives.jenkins-ci.org/plugins/build-user-vars-plugin/1.5/build-user-vars-plugin.hpi
http://archives.jenkins-ci.org/plugins/workflow-job/1145.v7f2433caa07f/workflow-job.hpi
http://archives.jenkins-ci.org/plugins/permissive-script-security/0.3/permissive-script-security.hpi
http://archives.jenkins-ci.org/plugins/jquery-detached/1.2.1/jquery-detached.hpi
http://archives.jenkins-ci.org/plugins/scm-api/2.6.5/scm-api.hpi
http://archives.jenkins-ci.org/plugins/blueocean-pipeline-scm-api/1.24.8/blueocean-pipeline-scm-api.hpi
http://archives.jenkins-ci.org/plugins/blueocean-github-pipeline/1.24.8/blueocean-github-pipeline.hpi
http://archives.jenkins-ci.org/plugins/workflow-api/1138.v619fd5201b_2f/workflow-api.hpi
http://archives.jenkins-ci.org/plugins/docker-commons/1.13/docker-commons.hpi
http://archives.jenkins-ci.org/plugins/ssh-slaves/1.29.4/ssh-slaves.hpi
http://archives.jenkins-ci.org/plugins/pipeline-model-declarative-agent/1.1.1/pipeline-model-declarative-agent.hpi
http://archives.jenkins-ci.org/plugins/jackson2-api/2.13.1-246.va8a9f3eaf46a/jackson2-api.hpi
http://archives.jenkins-ci.org/plugins/plot/2.1.0/plot.hpi
http://archives.jenkins-ci.org/plugins/cloudbees-bitbucket-branch-source/726.vb0c1ea6c9336/cloudbees-bitbucket-branch-source.hpi
http://archives.jenkins-ci.org/plugins/jjwt-api/0.11.2-9.c8b45b8bb173/jjwt-api.hpi
EOF
wget -i urls.txt
```

2. Using any available tools and data channels, move all .hpi files to /root/temp_plugins/ of the DriveTrain LCM engine node (cid01).
3. Log in to the cid01 node as root.

4. Obtain the DriveTrain Jenkins endpoint and credentials:

```
salt-call pillar.get jenkins:client:master
```

Copy these elements to use in the commands that follow: Jenkins IP, port, login, password.

5. Download the jenkins-cli client from the DriveTrain Jenkins to the /root folder:

```
wget https://%JENKINS_IP%:%JENKINS_PORT%/jnlpJars/jenkins-cli.jar
```

6. Verify that the jenkins-cli client is operating properly:

```
java -jar jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% list-plugins
```

The command output should include a list of all installed plugins and versions.

Note

In the steps that follow, assume that the .hpi files are located in the /root/temp_plugins directory.

7. Copy the .hpi plugin files to the Docker volume.

Note

The CLI tool requires an accessible URI to install the plugin, file:// in the example below.

```
rm -rf /srv/volumes/jenkins/fresh_plugins
mkdir /srv/volumes/jenkins/fresh_plugins
chmod 755 /srv/volumes/jenkins/fresh_plugins
cd /root/temp_plugins
cp *.hpi /srv/volumes/jenkins/fresh_plugins/
chmod 644 /srv/volumes/jenkins/fresh_plugins/*.hpi
```

8. Install the plugins:

```
ls *.hpi | xargs -t {} java -jar ../jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% install-plugin file:///var/jenkins_home/fresh_plugins/{}
```

9. Remove the temporary folder from the Docker volume:

```
rm -rf /srv/volumes/jenkins/fresh_plugins
```


10 Reboot Jenkins:

```
cd /root/
java -jar jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% safe-restart
```

Rebooting requires some time. During this time, Jenkins responds with 503 errors.

11 Verify the successful rebooting of Jenkins:

```
java -jar jenkins-cli.jar -s https://%JENKINS_IP%:%JENKINS_PORT%/ -auth %JENKINS_LOGIN%:%JENKINS_PASSWORD% list-plugins
```

If Jenkins is up and running, the output will include plugins in the place of Java tracebacks.

Updated MCP components

The MCP 2019.2.17 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.16 update.

All 2019.2.17 packages are available at <http://mirror.mirantis.com/update/2019.2.17/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.16	2019.2.17
OpenStack Pike	glance	2:15.0.2-2~u16.04+mcp17	2:15.0.2-2~u16.04+mcp18
	nova	2:16.1.8-6~u16.04+mcp304	2:16.1.8-6~u16.04+mcp306
	paramiko	2.0.0-1.1~u16.04+mcp2	2.8.0-1~u16.04+mcp1
	python-keystoneauth1	3.1.1-1~u16.04+mcp8	3.1.1-1~u16.04+mcp9
	python-oslo.rootwrap	5.9.3-1~u16.04+mcp5	5.9.3-1~u16.04+mcp6
OpenStack Queens	cinder	2:12.0.10-3~u16.04+mcp161	2:12.0.10-3~u16.04+mcp163
	glance	2:16.0.1-3~u16.04+mcp33	2:16.0.1-3~u16.04+mcp34

	heat	1:10.0.3-1.1~u16.04+mcp122	1:10.0.3-1.1~u16.04+mcp123
	keystone	2:13.0.4-4~u16.04+mcp48	2:13.0.4-4~u16.04+mcp51
	neutron	2:12.1.1-9~u16.04+mcp494	2:12.1.1-9~u16.04+mcp501
	nova	2:17.0.13-9~u16.04+mcp371	2:17.0.13-9~u16.04+mcp372
	paramiko	2.0.0-1.1~u16.04+mcp2	2.8.0-1~u16.04+mcp1
	python-keystoneauth1	3.4.1-1.0~u16.04+mcp7	3.4.1-1.0~u16.04+mcp9
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20210915204810-0	4.1~20211115204810-0
	contrail	4.1~20210915204810-0	4.1~20211115204810-0
	contrail-heat	4.1~20210915204810-0	4.1~20211115204810-0
	contrail-vrouter-dpdk	4.1~20210915204810	4.1~20211115204810
	contrail-web-controller	4.1~20210915204810-0	4.1~20211115204810-0
	contrail-web-core	4.1~20210915204810-0	4.1~20211115204810-0
	neutron-plugin-contrail	4.1~20210915204810-0	4.1~20211115204810-0
Salt formulas	salt-formula-elasticsearch	0.2+202005271243.5aab3fc~xenial1	0.2+202112141036.d3ab2ba~xenial1
	salt-formula-fluentd	0.1+202107091357.1402939~xenial1	0.1+202111011102.502878a~xenial1
	salt-formula-glance	2016.12.1+202108311506.c3ae832~xenial1	2016.12.1+202111291638.6b80406~xenial1
	salt-formula-jenkins	2017.8+202109061542.b3d3f64~xenial1	2017.8+202111181744.68c98d4~xenial1
	salt-formula-neutron	2016.12.1+202109161746.25e41f4~xenial1	2016.12.1+202111161208.4668171~xenial1

	salt-formula-prometheus	0.1+202107121529.9987b24~xenial1	0.1+202111031532.f681e07~xenial1
--	-------------------------	----------------------------------	----------------------------------

Release artifacts

This section lists the artifacts of the MCP 2019.2.17 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.17/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.17/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.17/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.17/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.17/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.17/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²⁶	http://mirror.mirantis.com/update/2019.2.17/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.17.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.17.qcow2
	VCP Ubuntu 16.04 image ²⁶	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main

	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.17/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.17/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.17/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.17/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.17/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²⁶
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.17/glusterfs-5/xenial xenial main ²⁶
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.17/maas/xenial xenial main ²⁶
	Percona	deb http://mirror.mirantis.com/update/2019.2.17/percona/xenial xenial main ²⁶
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.17/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.17/saltstack-2017.7/xenial xenial main ²⁶ deb http://mirror.mirantis.com/update/2019.2.17/salt-2017.7.8/ xenial xenial main ²⁶
	Upstream Ubuntu system packages ²⁶	deb https://mirror.mirantis.com/update/2019.2.17/ubuntu/xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.17/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.17/ubuntu/xenial-security main restricted universe

MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.17
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.17
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.17
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.17
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.16 ²⁶
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.14 ²⁶
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.16 ²⁶
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.16 ²⁶
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.16 ²⁶
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²⁶
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²⁶
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.17 ²⁶
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²⁶
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²⁶
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.16 ²⁶
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²⁶
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.16 ²⁶
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.17 ²⁶
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.17 ²⁶

	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.15 ²⁶
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.17 ²⁶
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.22-alpine ²⁶
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²⁶
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²⁶
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²⁶
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²⁶
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²⁶
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.15 ²⁶
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.17 ²⁶
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²⁶

26(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.16 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.16,

first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages.
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 as described in MCP Operations Guide: Update StackLight LMA.
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso
Known issues

2019.2.16

The MCP 2019.2.16 update introduces enhancements and bug fixes for DriveTrain, OpenStack, and Ceph MCP components.

The MCP 2019.2.16 update is available starting from October 15, 2021.

Enhancements

In the MCP 2019.2.16 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.16 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Kernel Crash Dump
- Time stamps in Jenkins pipeline jobs output

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

Kernel Crash Dump

Implemented the capability to configure kernel crash dumping for one or multiple nodes to save the system memory events for later analysis.

Learn more

- [Kernel Crash Dump](#)
 - [MCP Operations Guide: Configure kernel crash dumping](#)
-

Time stamps in Jenkins pipeline jobs output

Implemented the [Timestamper](#) Jenkins plugin that now adds time stamps to the console output of Jenkins pipeline jobs. The plugin eases logs cross-checking and helps to diagnose issues faster.

OpenStack

In the MCP 2019.2.16 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Host passthrough for VCP

- Cinder coordination
- Disabling of Nova cell mapping

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

Host passthrough for VCP

Added the capability to enable the host-passthrough CPU mode to enhance the performance of the MCP Virtualized Control Plane (VCP).

Learn more

- [libvirt documentation: CPU model and topology](#)
 - [MCP Operations Guide: Enable host passthrough for VCP](#)
-

Cinder coordination

Implemented the capability to enable Cinder coordination with MySQL as a back end to avoid Cinder race conditions in case of an active/active configuration.

Learn more

[MCP Operations Guide: Enable Cinder coordination](#)

Disabling of Nova cell mapping

Implemented the capability to disable Nova cell mapping and database migrations, for example, to faster redeploy the nova state. However, Nova cell mapping must be enabled prior to performing an upgrade.

Learn more

[MCP Operations Guide: Disable Nova cell mapping](#)

Addressed issues

The MCP 2019.2.16 update contains fixes for several MCP components.

DriveTrain

- [36501] Fixed the issue with HAProxy timeout being set in milliseconds instead of seconds, causing HAProxy to abruptly close connections.
- [36566] Fixed the issue with the CVP - Sanity checks Jenkins pipeline job failing with the AssertionError: RabbitMQ cluster is probably broken - the cluster size for each node should be (3) but the following nodes have other values error.
- [36531] Fixed the issue with an inconsistency rule defined in test_packet_checker.py with hardcoded node names, which caused the CVP - Sanity checks Jenkins pipeline job to fail if the node names were different.
- [36596] Fixed the issue causing broken Neutron with Designate integrations in case if TLS was enabled.
- [36620] Fixed the issue with cmdmod._log_cmd improperly handling tuples.
- [36469] Updated the python-django package to add support for the SameSite cookie flag.
- [36471] Updated the python-urllib3 package to fix the [CVE-2020-26137](#) security vulnerability.

OpenStack

- [36503][Pike, Queens] Corrected file and directory permissions according to the OpenStack community standards. For details, see [Security checklist](#).
- [36395][Pike] Fixed the issue with the gnocchi-statsd process failing to start when Redis was unavailable.
- [36490][Pike, Queens] Fixed the issue causing inability to create Swift containers through the Horizon web UI due to cookies settings.
- [36593][Pike, Queens] Updated the openvswitch package to fix the [CVE-2020-27827](#) and [CVE-2020-35498](#) security vulnerabilities.
- [36511][Salt] Improved the Neutron Salt formula to support configuring network port_security_enabled.
- [36591][Pike, Queens] Updated the python-nova, python-neutron, and python-keystone packages to fix the following security vulnerabilities:
 - [OSSA-2021-001](#)
 - [OSSA-2021-002](#)
 - [OSSA-2021-003](#)
 - [OSSA-2021-005](#)
 - [OSSA-2021-006](#)

- [36569][Queens] Fixed the issue with the Ironic driver in Nova where duplicate calls to Ironic were causing instance deletion failure.
- [36321][Queens] Fixed the issue with Nova failing to resume hosts after a reboot when booting a VM with an encrypted Ceph volume as a boot device.
- [36550][Queens] Fixed the issue causing a router processing to fail if CIDR was used as allowed address pair.
- [36464][Pike] Fixed the issue causing failure to delete a subport from trunk using openstack stack update.
- [36462][Queens] Fixed the issue with tokens generated without a catalog being unusable in some OpenStack services.
- [36479][Pike] Fixed the issue with a parallel volume creation, using a volume-backed image, causing the volumes to hang with the creating or error state.
- [36502][Pike] Updated the rabbitmq-server package to fix the following security vulnerabilities:
 - [CVE-2019-11287](#)
 - [CVE-2021-22116](#)
- [36486][Queens] Added the possibility to set a unique instance serial number in Nova.

Ceph

Issues resolutions applied automatically

- [36470] Fixed the issue causing failure to upgrade Ceph packages when applying MCP maintenance updates.
- [36477] Fixed the issue with the Ceph - upgrade Jenkins pipeline job failing during the Ceph Luminous to Nautilus upgrade with the problem getting command descriptions from mon error message.

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.

- [CVE-2021-20288] Unauthorized global_id reuse in cephx
-

[CVE-2021-20288] Unauthorized global_id reuse in cephx

Updated the Ceph Nautilus package to version 14.2.22 to fix the [CVE-2021-20288](#) security vulnerability. To apply the issue resolution, perform the steps below.

Warning

To avoid issues with cluster connection, perform the following procedure only after applying the MCP maintenance update 2019.2.16 as described in [Apply maintenance updates](#).

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `ceph/common.yml`, add the following pillar:

```
ceph:
  common:
    config:
      mon:
        auth_allow_insecure_global_id_reclaim: false
```

3. Log in to the Salt Master node.
4. Refresh pillars:

```
salt '*' saltutil.refresh_pillar
```

5. Apply the following state:

```
salt -l ceph:common state.apply ceph.common
```

Warning

Once you perform this step, some services can lose connection to the Ceph cluster. Known services that can be affected include:

- On `ctl*` nodes: glance-api, cinder-backup, cinder-scheduler, cinder-volume, apache2
- On `cmp*` nodes: nova-compute
- On `mdb*` nodes: gnocchi-metricd, apache2

6. Restart all ceph-mon one by one:

```
salt -C "@ceph:mon" -b 1 service.restart,test.sleep ceph-mon.target , 10
```

7. Restart the following services one by one. Wait for at least one minute between each command run:

```
salt -C "@apache:server:enabled" -b 1 service.restart,test.sleep apache2 , 5
salt -C "@glance:server" -b 1 service.restart,test.sleep glance-api , 5
salt -C "@cinder:server" -b 1 service.restart,test.sleep cinder-backup , 5
salt -C "@cinder:server" -b 1 service.restart,test.sleep cinder-scheduler , 5
salt -C "@cinder:volume" -b 1 service.restart,test.sleep cinder-volume , 5
salt -C "@nova:compute" -b 1 service.restart,test.sleep nova-compute , 5
salt -C "@gnocchi:server" -b 1 service.restart,test.sleep gnocchi-metricd , 5
```

Known issues

For MCP known issues applicable to MCP 2019.2.16, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.16 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.15 update.

All 2019.2.16 packages are available at <http://mirror.mirantis.com/update/2019.2.16/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.15	2019.2.16
Distributed storage	Ceph Nautilus	14.2.19	14.2.22
OpenStack Pike	cinder	2:11.2.2-3~u16.04+mcp153	2:11.2.2-3~u16.04+mcp154
	elixir-lang	1.7.4-0.1~u16.04+mcp	1.10.4-1+mcp1
	erlang	1:22.1.8+dfsg-1.1~u16.04+mcp1	1:23.3.4.4-1+mcp1
	gnocchi	4.0.5-3~u16.04+mcp2	4.0.5-3~u16.04+mcp4

	heat	1:9.0.7-2~u16.04+mcp107	1:9.0.7-2~u16.04+mcp108
	horizon	3:12.0.4-5~u16.04+mcp91	3:12.0.4-5~u16.04+mcp92
	keystone	2:12.0.3-5~u16.04+mcp38	2:12.0.3-5~u16.04+mcp39
	nettle	3.3-2~u16.04+mcp3	3.3-2~u16.04+mcp4
	networking-odl	1:11.0.0-1~u16.04+mcp66	1:11.0.1-1~u16.04+mcp16
	neutron	2:11.0.8-6~u16.04+mcp275	2:11.0.8-6~u16.04+mcp278
	nova	2:16.1.8-6~u16.04+mcp302	2:16.1.8-6~u16.04+mcp304
	openvswitch	2.9.5-2~u16.04+mcp	2.9.5-3~u16.04+mcp
	python-django	1:1.11.29-1~u16.04+mcp5	1:1.11.29-1~u16.04+mcp6
	python-urllib3	1.21.1-1~u16.04+mcp3	1.21.1-1~u16.04+mcp4
	rabbitmq-server	3.8.2-1~u16.04+mcp2	3.8.17-1~u16.04+mcp1
OpenStack Queens	cinder	2:12.0.10-3~u16.04+mcp158	2:12.0.10-3~u16.04+mcp161
	heat	1:10.0.3-1.1~u16.04+mcp121	1:10.0.3-1.1~u16.04+mcp122
	horizon	3:13.0.3-10~u16.04+mcp106	3:13.0.3-10~u16.04+mcp107
	keystone	2:13.0.4-4~u16.04+mcp44	2:13.0.4-4~u16.04+mcp48
	nettle	3.3-2~u16.04+mcp2	3.3-2~u16.04+mcp3
	networking-odl	1:12.0.0-1.0~u16.04+mcp45	1:12.0.1-1.0~u16.04+mcp16
	neutron	2:12.1.1-9~u16.04+mcp476	2:12.1.1-9~u16.04+mcp494
	nova	2:17.0.13-9~u16.04+mcp355	2:17.0.13-9~u16.04+mcp371
	openvswitch	2.9.5-2~u16.04+mcp	2.9.5-3~u16.04+mcp
	python-django	1:1.11.29-1~u16.04+mcp2	1:1.11.29-1~u16.04+mcp5

	python-tooz	1.60.2-1.0~u16.04+mcp3	1.60.2-1.0~u16.04+mcp4
	python-urllib3	1.21.1-1~u16.04+mcp3	1.21.1-1~u16.04+mcp4
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20210708204810-0	4.1~20210915204810-0
	contrail	4.1~20210708204810-0	4.1~20210915204810-0
	contrail-heat	4.1~20210708204810-0	4.1~20210915204810-0
	contrail-vrouter-dpdk	4.1~20210708204810	4.1~20210915204810
	contrail-web-controller	4.1~20210708204810-0	4.1~20210915204810-0
	contrail-web-core	4.1~20210708204810-0	4.1~20210915204810-0
	neutron-plugin-contrail	4.1~20210708204810-0	4.1~20210915204810-0
Salt formulas	salt-formula-aodh	0.2+202008201111.23a40f7~xenial1	0.2+202108311502.edbfbe8~xenial1
	salt-formula-aptly	2017.2+202001141131.4f6a992~xenial1	2017.2+202108311012.65c4908~xenial1
	salt-formula-backports	0.1+201909271115.a35cfb9~xenial1	0.1+202108161119.267fdd0~xenial1
	salt-formula-barbican	2018.1+202107120843.63a5ef0~xenial1	2018.1+202109010910.022c812~xenial1
	salt-formula-cassandra	0.1+202102181147.1b589bf~xenial1	0.1+202108261536.fbce8b7~xenial1
	salt-formula-ceph	0.1+202107231455.96b285e~xenial1	0.1+202108051019.6bac757~xenial1
	salt-formula-cinder	2016.12.1+202106291106.879b1e4~xenial1	2016.12.1+202108301139.f95a909~xenial1
	salt-formula-designate	2016.12.1+202010210932.14dac2e~xenial1	2016.12.1+202109011205.c25ae21~xenial1
	salt-formula-glance	2016.12.1+202008201233.48392d2~xenial1	2016.12.1+202108311506.c3ae832~xenial1

	salt-formula-gnocchi	2018.1+202003311438.e3d7c09~xenial1	2018.1+202108311055.fb143b6~xenial1
	salt-formula-haproxy	0.2+202103290839.cccd994~xenial1	0.2+202108121101.894f7ef~xenial1
	salt-formula-heat	2016.12.1+202104020759.a9e22df~xenial1	2016.12.1+202108311057.9745e2e~xenial1
	salt-formula-jenkins	2017.8+202003311035.1a3adc4~xenial1	2017.8+202109061542.b3d3f64~xenial1
	salt-formula-keystone	2016.12.1+202106241357.dbdac22~xenial1	2016.12.1+202108301124.89d65be~xenial1
	salt-formula-linux	2017.4.1+202107130920.6b848b5~xenial1	2017.4.1+202109071201.e238712~xenial1
	salt-formula-neutron	2016.12.1+202107091438.260a51c~xenial1	2016.12.1+202109161746.25e41f4~xenial1
	salt-formula-nova	2016.12.1+202106251202.2af6abf~xenial1	2016.12.1+202109291213.0d675b9~xenial1
	salt-formula-octavia	2017.6+202011111037.c3458cb~xenial1	2017.6+202109010905.5f4ff55~xenial1
	salt-formula-oslo-templates	2018.1+202107081429.3f1c8c4~xenial1	2018.1+202108101148.8e4faa8~xenial1
	salt-formula-panko	2017.6+202008180941.ab341b7~xenial1	2017.6+202109011200.4a9181a~xenial1
	salt-formula-salt	0.4+202105050946.5537917~xenial1	0.4+202109131438.691231c~xenial1
Extra packages	telegraf	1:1.9.1-3~u16.04+mc81	1:1.9.1-3~u16.04+mc82

Release artifacts

This section lists the artifacts of the MCP 2019.2.16 maintenance update.

MCP release artifacts

Type	Artifact	Path
------	----------	------

Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.16/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.16/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.16/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.16/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.16/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.16/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²⁷	http://mirror.mirantis.com/update/2019.2.16/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.16.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.16.qcow2
	VCP Ubuntu 16.04 image ²⁷	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.16/docker/xenial xenial stable

	Elastic	deb http://mirror.mirantis.com/update/2019.2.16/elastics-earch-5.x/xenial-stable-main deb http://mirror.mirantis.com/update/2019.2.16/elastics-earch-6.x/xenial-stable-main deb http://mirror.mirantis.com/update/2019.2.16/elastics-earch-curator/xenial-stable-main deb http://mirror.mirantis.com/update/2019.2.16/elastics-earch-curator-5/xenial-stable-main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial-xenial-contrib ²⁷
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.16/glusterfs-5/xenial-xenial-main ²⁷
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial-xenial-stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.16/maas/xenial-xenial-main ²⁷
	Percona	deb http://mirror.mirantis.com/update/2019.2.16/percona/xenial-xenial-main ²⁷
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.16/saltstack-2017.7/trusty-trusty-main deb http://mirror.mirantis.com/update/2019.2.16/saltstack-2017.7/xenial-xenial-main ²⁷ deb http://mirror.mirantis.com/update/2019.2.16/salt-2017.7.8/xenial-xenial-main ²⁷
	Upstream Ubuntu system packages ²⁷	deb https://mirror.mirantis.com/update/2019.2.16/ubuntu/xenial-main-restricted-universe deb https://mirror.mirantis.com/update/2019.2.16/ubuntu/xenial-updates-main-restricted-universe deb https://mirror.mirantis.com/update/2019.2.16/ubuntu/xenial-security-main-restricted-universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.16
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.16
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.16

	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.16
Docker images	alerta	docker-prod-local.artifactory.mirantis.com/openstack-docker/alerta:2019.2.16 ²⁷
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.14 ²⁷
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.16 ²⁷
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.16 ²⁷
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.16 ²⁷
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²⁷
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²⁷
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.16 ²⁷
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²⁷
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²⁷
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.16 ²⁷
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²⁷
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.16 ²⁷
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.16 ²⁷
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.15 ²⁷
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.15 ²⁷
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.15 ²⁷
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.22-alpine ²⁷

	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²⁷
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²⁷
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²⁷
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²⁷
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²⁷
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.15 ²⁷
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.14 ²⁷
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²⁷

27(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.15 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.15, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages.
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 as described in MCP Operations Guide: Update StackLight LMA.
6	Ceph	<ol style="list-style-type: none"> 1. Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages. 2. Perform the steps described in Issues resolutions requiring manual application.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.15

The MCP 2019.2.15 update introduces enhancements and bug fixes for DriveTrain, OpenStack, StackLight, and Ceph MCP components.

The MCP 2019.2.15 update is available starting from July 30, 2021.

Enhancements

In the MCP 2019.2.15 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.15 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Jenkins security update

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

Jenkins security update

Updated jenkins-master from version 2.204.3 to 2.263.4 to fix a number of security updates.

OpenStack

In the MCP 2019.2.15 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- RabbitMQ queue mirroring
- Randomized RabbitMQ reconnection intervals
- RabbitMQ queues troubleshooting
- User ID support in the Nova policy

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

RabbitMQ queue mirroring

Implemented the capability to enable RabbitMQ mirroring policy for clustered RabbitMQ configurations to reduce failures during the RabbitMQ cluster recovery. For new deployments, mirroring is enabled by default.

Learn more

[MCP Operations Guide: Enable queue mirroring](#)

Randomized RabbitMQ reconnection intervals

Implemented the capability to enable random reconnection intervals for RabbitMQ on the required OpenStack services. The feature enhances the RabbitMQ cluster operation in large OpenStack environments.

Learn more

[MCP Operations Guide: Randomize RabbitMQ reconnection intervals](#)

RabbitMQ queues troubleshooting

Added a detailed procedure on how to identify and fix non-functional queue bindings of a clustered RabbitMQ instance.

Learn more

[MCP Operations Guide: Troubleshoot RabbitMQ non-functional queue bindings](#)

User ID support in the Nova policy

Implemented the capability to use the `user_id` attribute in the Nova API `os_compute_api:os-remote-consoles` policy. For example, to allow console access only to the instance creator or administrative user, set this policy to `"os_compute_api:os-remote-consoles": {"is_admin:True" or "project_id:%(project_id)s and user_id:%(user_id)s"}`.

StackLight

In the MCP 2019.2.15 maintenance update, Mirantis introduces the following enhancements for StackLight:

- RX/TX monitoring

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

RX/TX monitoring

Implemented the `SystemRxPacketsErrorTooHigh` and `SystemTxPacketsErrorTooHigh` alerts that raise in case of errors in the RX/TX packets.

Learn more

[MCP Operations Guide: System alerts](#)

Addressed issues

The MCP 2019.2.15 update contains fixes for several MCP components.

DriveTrain

Issues resolutions applied automatically

- [36319] Fixed the issue with MAAS failing to manage IP addresses if one of the nodes was not in the READY state.
- [36334] Optimized the method of selecting the backup node during Galera backup to avoid using the most loaded node from the list of available primary nodes.
- [36313] Updated the `python-django` package to fix the [CVE-2021-28658](#) and [CVE-2021-31542](#), [CVE-2021-33203](#), and [CVE-2021-33571](#) security vulnerabilities.
- [36314] Updated the `libnettle6` package to fix the [CVE-2021-20305](#) security vulnerability.
- [36367] Updated the `python-eventlet` package to fix the [CVE-2021-21419](#) security vulnerability.
- [36364] Updated the `python-babel` and `python-babel-localedata` packages to fix the [CVE-2021-20095](#) security vulnerability.
- [36337] Updated a number of Docker images to fix security vulnerabilities.
- [36448] Enhanced the NGINX Salt formula by implementing the capability to modify the `large_client_header_buffers`.
- [36432] Added the missing `openjdk` package to the MCP offline image.

Issues resolutions requiring manual application

- [36461] Failure to upgrade Ceph to Nautilus on RADOS Gateway nodes
-

[36461] Failure to upgrade Ceph to Nautilus on RADOS Gateway nodes

Fixed the issue occurring during the Ceph upgrade from Luminous to Nautilus and causing the `ceph_version` change not to apply to standalone RADOS Gateway nodes. As a result, the Ceph upgrade to Nautilus did not apply to such nodes.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `ceph/rgw.yaml`, move all Ceph classes to the bottom of the classes list. Consider the following example:

```
- cluster.your_cluster_name.ceph
- cluster.your_cluster_name.ceph.common
- cluster.your_cluster_name.infra
```

In this case, move the Ceph classes as shown below:

```
- cluster.your_cluster_name.infra
- cluster.your_cluster_name.ceph
- cluster.your_cluster_name.ceph.common
```

Once done, proceed with the steps described in Apply maintenance updates.

OpenStack

- [36328][Queens] Fixed the issue causing VMs with encrypted ephemeral storage to get stuck in the DOWN state after an OpenStack compute node reboot.
- [36392][Pike] Fixed the issue with the Nova resource tracker operating incorrectly.
- [36224][Pike, Queens] Set the `nova_ram_allocation_ratio` in Nova to 1.0 by default to disable RAM overcommitment for Nova on new deployments.

StackLight

- [36270] Added the capability to configure the response size limit for Prometheus Relay using the `PrometheusResponseLimitBytes` environment variable to avoid issues with Prometheus Relay failing to handle requests over 1 MB.
- [36383] Fixed the issue with some Kibana logs timestamps being rounded to seconds although the original component log time stamps contained milliseconds.
- [36420] Fixed the issue with Keystone logs parsing.

Ceph

- [35727] Fixed the issue with the Update Ceph packages Jenkins pipeline job restarting Ceph OSDs even if no Ceph packages were being updated.

Known issues

For MCP known issues applicable to MCP 2019.2.15, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.15 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.14 update.

All 2019.2.15 packages are available at <http://mirror.mirantis.com/update/2019.2.15/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.14	2019.2.15
DriveTrain	jenkins-master	2.204.3	2.263.4
OpenStack Pike	horizon	3:12.0.4-5~u16.04+mcp90	3:12.0.4-5~u16.04+mcp91
	nettle	3.3-2~u16.04+mcp2	3.3-2~u16.04+mcp3
	neutron	2:11.0.8-6~u16.04+mcp274	2:11.0.8-6~u16.04+mcp275
	nova	2:16.1.8-6~u16.04+mcp301	2:16.1.8-6~u16.04+mcp302
	python-babel	2.3.4+dfsg.1-2.1~u16.04+mcp2	2.3.4+dfsg.1-2.1~u16.04+mcp3
	python-django	1:1.11.29-1~u16.04+mcp2	1:1.11.29-1~u16.04+mcp5
	python-eventlet	0.20.0-4~u16.04+mcp2	0.20.0-4~u16.04+mcp3
	python-tooz	1.58.1-1~u16.04+mcp2	1.58.1-1~u16.04+mcp3
	OpenStack Queens	cinder	2:12.0.10-3~u16.04+mcp156
elixir-lang		1.7.4-0.1~u16.04+mcp	1.10.4-1+mcp1
erlang		1:22.1.8+dfsg-1.1~u16.04+mcp1	1:23.3.4.4-1+mcp1

	glance	2:16.0.1-3~u16.04+mcp32'	2:16.0.1-3~u16.04+mcp33
	neutron	2:12.1.1-9~u16.04+mcp450	2:12.1.1-9~u16.04+mcp476
	nova	2:17.0.13-9~u16.04+mcp346	2:17.0.13-9~u16.04+mcp355
	python-babel	2.3.4+dfsg.1-2.1~u16.04+mcp2	2.3.4+dfsg.1-2.1~u16.04+mcp3
	python-eventlet	0.20.0-4~u16.04+mcp2	0.20.0-4~u16.04+mcp3
	python-glance-store	0.23.0-2~u16.04+mcp17	0.23.0-2~u16.04+mcp19
	python-manilaclient	1.21.2-1.0~u16.04+mcp19	1.21.2-1.0~u16.04+mcp21
	python-tooz	1.60.2-1.0~u16.04+mcp2	1.60.2-1.0~u16.04+mcp3
	rabbitmq-server	3.8.2-1~u16.04+mcp2	3.8.17-1~u16.04+mcp1
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20210508204813-0	4.1~20210708204810-0
	contrail	4.1~20210508204813-0	4.1~20210708204810-0
	contrail-heat	4.1~20210508204813-0	4.1~20210708204810-0
	contrail-vrouter-dpdk	4.1~20210508204813	4.1~20210708204810
	contrail-web-controller	4.1~20210508204813-0	4.1~20210708204810-0
	contrail-web-core	4.1~20210508204813-0	4.1~20210708204810-0
	neutron-plugin-contrail	4.1~20210508204813-0	4.1~20210708204810-0
Salt formulas	salt-formula-apache	0.2+202104161428.1429fd3~xenial1	0.2+202106170859.3e4eb31~xenial1
	salt-formula-barbican	2018.1+202008201011.34ba975~xenial1	2018.1+202107120843.63a5ef0~xenial1
	salt-formula-ceph	0.1+202105131553.0e79145~xenial1	0.1+202107231455.96b285e~xenial1

	salt-formula-cinder	2016.12.1+202104141728.4e7cfc6~xenial1	2016.12.1+202106291106.879b1e4~xenial1
	salt-formula-fluentd	0.1+202009021401.98eb487~xenial1	0.1+202107091357.1402939~xenial1
	salt-formula-keystone	2016.12.1+202011172142.c7d1c5f~xenial1	2016.12.1+202106241357.dbdac22~xenial1
	salt-formula-linux	2017.4.1+202104300958.2bc6bbb~xenial1	2017.4.1+202107130920.6b848b5~xenial1
	salt-formula-maas	0.0.1+202103180947.89a59c2~xenial1	0.0.1+202107081157.053aa46~xenial1
	salt-formula-neutron	2016.12.1+202103180938.0814ce9~xenial1	2016.12.1+202107091438.260a51c~xenial1
	salt-formula-nginx	0.2+202012211735.a30a545~xenial1	0.2+202107151609.b43965f~xenial1
	salt-formula-nova	2016.12.1+202104020803.31e892f~xenial1	2016.12.1+202106251202.2af6abf~xenial1
	salt-formula-oslo-templates	2018.1+202104191007.b5f8375~xenial1	2018.1+202107081429.3f1c8c4~xenial1
	salt-formula-prometheus	0.1+202101291207.8736b2f~xenial1	0.1+202107121529.9987b24~xenial1
	salt-formula-zookeeper	0.1+201903250936.79f4fbf~xenial1	0.1+202106221716.e01edf2~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.15 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.15/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.15/openstack-queens/xenial xenial main

	Extra packages	deb http://mirror.mirantis.com/update/2019.2.15/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.15/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.15/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.15/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²⁸	http://mirror.mirantis.com/update/2019.2.15/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.15.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.15.qcow2
	VCP Ubuntu 16.04 image ²⁸	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.15/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.15/elasticsearch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.15/elasticsearch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.15/elasticsearch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.15/elasticsearch-curator-5/xenial stable main

	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²⁸
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.15/glusterfs-5/xenial xenial main ²⁸
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.15/maas/xenial xenial main ²⁸
	Percona	deb http://mirror.mirantis.com/update/2019.2.15/percona/xenial xenial main ²⁸
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.15/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.15/saltstack-2017.7/xenial xenial main ²⁸ deb http://mirror.mirantis.com/update/2019.2.15/salt-2017.7.8/ xenial xenial main ²⁸
	Upstream Ubuntu system packages ²⁸	deb https://mirror.mirantis.com/update/2019.2.15/ubuntu/ xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.15/ubuntu/ xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.15/ubuntu/ xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.15
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.15
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.15
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.15
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.14 ²⁸
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.14 ²⁸
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.14 ²⁸

aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.14 ²⁸
aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.14 ²⁸
compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²⁸
cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²⁸
gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.15 ²⁸
gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²⁸
gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²⁸
grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.14 ²⁸
heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²⁸
jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.15 ²⁸
jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.15 ²⁸
mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.15 ²⁸
openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.15 ²⁸
phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.15 ²⁸
postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.22-alpine ²⁸
prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²⁸
prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²⁸
pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²⁸
registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²⁸

	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²⁸
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf-notifier:2019.2.15 ²⁸
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.14 ²⁸
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²⁸

28(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35\)](#))

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.14 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.14, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> 1. Perform the steps described in Issues resolutions requiring manual application. 2. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.

3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages .
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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Ceph updates will be applied during the DriveTrain update.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.14

The MCP 2019.2.14 update introduces enhancements and bug fixes for DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph MCP components.

The MCP 2019.2.14 update is available starting from May 28, 2021.

Enhancements

In the MCP 2019.2.14 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

StackLight

In the MCP 2019.2.14 maintenance update, Mirantis introduces the following enhancements for StackLight:

- Disk and CPU wait alerts

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Disk and CPU wait alerts

Implemented the following disk and CPU wait alerts that raise in case of high CPU I/O wait, disk backlog, and disk request queues:

- SystemCpuloWaitWarning
- SystemCpuloWaitCritical
- SystemDiskBacklogWarning
- SystemDiskBacklogCritical
- SystemDiskRequestQueuedWarning
- SystemDiskRequestQueuedCritical

Learn more

[MCP Operations Guide: System alerts](#)

Ceph

In the MCP 2019.2.14 maintenance update, Mirantis introduces the following enhancements for Ceph:

- Granular distribution of Ceph keys

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Granular distribution of Ceph keys

Implemented granular distribution of Ceph keys. Now Ceph keyring access is distributed only between the required nodes. For existing deployments, you can enable the feature as described in [MCP Operations Guide: Enable granular distribution of Ceph keys](#).

Addressed issues

The MCP 2019.2.14 update contains fixes for several MCP components.

DriveTrain

- [36332] Fixed the issue with the Docker registry service missing after deploying the APT node in the offline mode.
- [36329] Fixed the issue with failure to start the Docker Swarm service due to an expired certificate, occurring during the offline deployment of an APT node. Added a certificate expiration check to the offline image. Now, an expired Docker Swarm certificate will be automatically regenerated during the APT node deployment.

- [36140] Improved the Linux Salt formula by adding the capability to set an SSD scheduler on physical nodes through udev.
- [36097] Improved the Salt formula by adding the capability to set driver interface attributes for NICs.
- [35933] Fixed the issue with OpenContrail diagrams missing when generating a diagnostic snapshot of the system using the sosreport tool.
- [36201] Fixed the issue causing inability to manage the lvm_filters if the storage.lvm pillar was not defined.
- [36171] Updated MySQL to version 5.6.51 to fix a number of vulnerabilities.
- [36176] Improved the Apache Salt formula to add the capability to set environment variables for the virtual host.
- [35646] Fixed the issue with the Telegraf Salt formula failing to upgrade the telegraf package.
- [35632] Fixed the issue with a backup directory being hardcoded in the ceph-backup-server-runner.sh script.
- [36049] Improved the Xtrabackup Salt formula to fix several issues with recovery scripts. Added the capability to pass the force-non-empty-directories option.
- [36220] Increased the Galera default wait_timeout timeout from 1800 to 28800 seconds.
- [36221] Increased the server and client HAProxy default timeouts from 300 to 28810 seconds.
- [36222] Enabled rbd_exclusive_cinder_pool by default for new deployments with Ceph.
- [36240] Increased the RabbitMQ open file limits to 49152 and file-max limits to 248320.
- [36283] Fixed the issue with publishing of some updates to the extra repository.

OpenStack

Issues resolutions applied automatically

- [35557][Pike] Fixed the issue causing the trunk ports to remain in the DOWN state after rebooting the OpenStack compute node until the restart of the OVS agent.
- [36263][Pike, Queens] Updated the python-django package to fix the following vulnerabilities:
 - [CVE-2020-13254](#)
 - [CVE-2020-13596](#)
 - [CVE-2021-23336](#)
 - [CVE-2021-3281](#)
- [36106][Pike, Queens] Fixed the issue with image creation through the Horizon web UI failing with the 400 Bad Request: The Store URI was malformed error message.
- [36252][Pike, Queens] Fixed the issue causing Heat stack creation failures.

- [36253][Queens] Fixed the issue with Glance failing to send logs to Fluentd when the root logger was set to WARNING.
- [35611][Pike] Fixed the issue causing VM vCPUs to overlap after an evacuation or cold migration.

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.

- [36121] SSL missing for Apache

[36121] SSL missing for Apache

Pike, Queens

Fixed the issue with SSL being not configured for Apache.

To apply the issue resolution:

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

```
- system.apache.server.ssl
```

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

```
salt '*' state.apply reclass
```

OpenContrail

- [36262] Fixed the issue with an unreliable connection to ports created with allowed address pairs.
- [36072] Fixed the issue with the OpenContrail load balancer not working due to a misconfiguration in authentication.

StackLight

- [36227] Fixed the BondInterfaceSlaveDownMajor alert expression.

- [36193] Fixed the issue with the salt.minion Salt state incorrectly processing changes to the meta/grafana.yml file due to some parameters being automatically set to null.

Ceph

- [36327] Changed the misleading Ceph - add osd (upmap) Jenkins pipeline name to Ceph - add osd.
- [35627] Fixed the issue with the logrotate utility improperly functioning due to the psmisc package missing on the rgw nodes.

Known issues

For MCP known issues applicable to MCP 2019.2.14, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.14 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.13 update.

All 2019.2.14 packages are available at <http://mirror.mirantis.com/update/2019.2.14/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.13	2019.2.14
Distributed storage	Ceph Nautilus	14.2.6	14.2.19
OpenStack Pike	designate	1:5.0.3-3~u16.04+mcp17	1:5.0.3-3~u16.04+mcp18
	dnsmasq	2.79-1~u16.04+mcp1	2.79-1~u16.04+mcp2
	heat	1:9.0.7-2~u16.04+mcp105	1:9.0.7-2~u16.04+mcp107
	mysql-wsrep-5.6	5.6.48-1~u16.04+mcp1	5.6.51-1~u16.04+mcp1
	neutron	2:11.0.8-6~u16.04+mcp271	2:11.0.8-6~u16.04+mcp274
	nova	2:16.1.8-6~u16.04+mcp280	2:16.1.8-6~u16.04+mcp301

	python-django	1:1.11.29-1~u16.04+mcp1	1:1.11.29-1~u16.04+mcp2
	python-glance-store	0.22.0-3~u16.04+mcp11	0.22.0-3~u16.04+mcp13
	python-oslo.messaging	5.30.8-1~u16.04+mcp20	5.30.8-1~u16.04+mcp22
	python-oslo.service	1.25.2-1~u16.04+mcp7	1.25.2-1~u16.04+mcp9
	python-urllib3	1.21.1-1~u16.04+mcp2	1.21.1-1~u16.04+mcp3
OpenStack Queens	designate	1:6.0.1-1.1~u16.04+mcp32	1:6.0.1-1.1~u16.04+mcp33
	dnsmasq	2.79-1~u16.04+mcp1	2.79-1~u16.04+mcp2
	heat	1:10.0.3-1.1~u16.04+mcp120	1:10.0.3-1.1~u16.04+mcp121
	horizon	3:13.0.3-10~u16.04+mcp104	3:13.0.3-10~u16.04+mcp106
	horizon-contrail-panels	2:0.1.2-1~u16.04+mcp14	2:0.1.2-2~u16.04+mcp15
	mysql-wsrep-5.6	5.6.48-1~u16.04+mcp1	5.6.51-1~u16.04+mcp1
	neutron	2:12.1.1-9~u16.04+mcp423	2:12.1.1-9~u16.04+mcp450
	nova	2:17.0.13-9~u16.04+mcp341	2:17.0.13-9~u16.04+mcp346
	python-django	1:1.11.29-1~u16.04+mcp1	1:1.11.29-1~u16.04+mcp2
	python-glance-store	0.23.0-2~u16.04+mcp16	0.23.0-2~u16.04+mcp17
	python-oslo.log	3.36.0-1.0~u16.04+mcp15	3.36.0-1.0~u16.04+mcp17
	python-oslo.middleware	3.34.0-1.0~u16.04+mcp8	3.34.0-1.0~u16.04+mcp10
	python-oslo.privsep	1.27.0-1.0~u16.04+mcp7	1.27.0-1.0~u16.04+mcp9
	python-oslo.reports	1.26.0-1.0~u16.04+mcp8	1.26.0-1.0~u16.04+mcp10

	python-oslo.rootwrap	5.13.0-1.0~u16.04+mcp8	5.13.0-1.0~u16.04+mcp10
	python-oslo.service	1.29.0-1.0~u16.04+mcp9	1.29.1-1.0~u16.04+mcp5
	python-urllib3	1.21.1-1~u16.04+mcp2	1.21.1-1~u16.04+mcp3
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20210218110907-0	4.1~20210508204813-0
	contrail	4.1~20210218110907-0	4.1~20210508204813-0
	contrail-heat	4.1~20210218110907-0	4.1~20210508204813-0
	contrail-vrouter-dpdk	4.1~20210218110907	4.1~20210508204813
	contrail-web-controller	4.1~20210218110907-0	4.1~20210508204813-0
	contrail-web-core	4.1~20210218110907-0	4.1~20210508204813-0
	neutron-plugin-contrail	4.1~20210218110907-0	4.1~20210508204813-0
Salt formulas	salt-formula-apache	0.2+202102091417.b7ab9bc~xenial1	0.2+202104161428.1429fd3~xenial1
	salt-formula-ceph	0.1+202101250928.290179e~xenial1	0.1+202105131553.0e79145~xenial1
	salt-formula-cinder	2016.12.1+202101251425.ca4467b~xenial1	2016.12.1+202104141728.4e7cfc6~xenial1
	salt-formula-debmirror	2018.1+202001141154.c6d0304~xenial1	2018.1+202104211512.de9556a~xenial1
	salt-formula-galera	1.0+202101280822.57453da~xenial1	1.0+202104021252.1bc3f26~xenial1
	salt-formula-haproxy	0.2+202011121320.a2cb999~xenial1	0.2+202103290839.cccd994~xenial1
	salt-formula-heat	2016.12.1+202010211317.ec9707f~xenial1	2016.12.1+202104020759.a9e22df~xenial1
	salt-formula-linux	2017.4.1+202102181217.344de40~xenial1	2017.4.1+202104300958.2bc6bbb~xenial1

	salt-formula-logrotate	0.1+201911071036.314279b~xenial1	0.1+202103232338.dd9d315~xenial1
	salt-formula-maas	0.0.1+202008180846.14ccca3~xenial1	0.0.1+202103180947.89a59c2~xenial1
	salt-formula-neutron	2016.12.1+202011100915.4ae3012~xenial1	2016.12.1+202103180938.0814ce9~xenial1
	salt-formula-nova	2016.12.1+202102121352.d9bab1b~xenial1	2016.12.1+202104020803.31e892f~xenial1
	salt-formula-opencontrail	0.2+202102051450.a1bdd10~xenial1	0.2+202103180959.1eb29a8~xenial1
	salt-formula-oslo-templates	2018.1+202102011510.e24fd64~xenial1	2018.1+202104191007.b5f8375~xenial1
	salt-formula-salt	0.4+202102022009.9637af2~xenial1	0.4+202105050946.5537917~xenial1
	salt-formula-telegraf	0.1+202010291041.d9d7c86~xenial1	0.1+202104061211.249d419~xenial1
	salt-formula-xtrabackup	0.2+202102050620.b077d2f~xenial1	0.2+202104280838.551ef05~xenial1
Extra packages	baremetal-support-files	n/a	0.1-1
	debhelper	n/a	11.1.4.0-1~u16.04+mcp1
	dh-autoreconf	n/a	16-1~u16.04+mcp1
	kafka	n/a	2.11-0.9.0.1-1~u16.04+mcp1
	libarchive-cpio-perl	n/a	0.10-1.0~u16.04+mcp1
	libipfix	n/a	0.8.2-2~u16.04+mcp1
	prometheus-relay	0.3-1~u16.04+mcp9	0.3-1~u16.04+mcp12
	python-cassandra-driver	n/a	3.7.1-3~u16.04+mcp1
	python-sseclient	n/a	0.0.12-1~u16.04+mcp1
	reclass	1.5.6-1.0~u16.04+mcp0	1.5.6-1.0~u16.04+mcp8

	sosreport	3.8.0-1~u16.04+mcp1	3.8.0-1~u16.04+mcp4
	strip-nondeterminism	n/a	0.040-1.0~u16.04+mcp2
	telegraf	1:1.9.1-3~u16.04+mcp79	1:1.9.1-3~u16.04+mcp81
	telegraf-builddeps	0.0+git20190830-1	0.0+git20201111-1

Release artifacts

This section lists the artifacts of the MCP 2019.2.14 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.14/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.14/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.14/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.14/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.14/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.14/opencontrail-4.1/xenial xenial main
	Salt formulas packages ²⁹	http://mirror.mirantis.com/update/2019.2.14/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.14.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.14.qcow2

	VCP Ubuntu 16.04 image ²⁹	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.14/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.14/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.14/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.14/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.14/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ²⁹
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.14/glusterfs-5/xenial xenial main ²⁹
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.14/maas/xenial xenial main ²⁹
	Percona	deb http://mirror.mirantis.com/update/2019.2.14/percona/xenial xenial main ²⁹
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.14/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.14/saltstack-2017.7/xenial xenial main ²⁹ deb http://mirror.mirantis.com/update/2019.2.14/salt-2017.7.8/ xenial xenial main ²⁹

	Upstream Ubuntu system packages ²⁹	deb https://mirror.mirantis.com/update/2019.2.14/ubuntu/xenial/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.14/ubuntu/xenial-updates/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.14/ubuntu/xenial-security/main/restricted/universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.14
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.14
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.14
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.14
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.14 ²⁹
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.14 ²⁹
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.14 ²⁹
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.14 ²⁹
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.14 ²⁹
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ²⁹
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ²⁹
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.14 ²⁹
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ²⁹
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ²⁹
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.14 ²⁹

	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ²⁹
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.14 ²⁹
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.14 ²⁹
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.13 ²⁹
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.14 ²⁹
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.14 ²⁹
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.21-alpine ²⁹
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.14 ²⁹
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ²⁹
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.14 ²⁹
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ²⁹
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ²⁹
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.14 ²⁹
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.14 ²⁹
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ²⁹

29(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.13 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.13, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	<ol style="list-style-type: none"> 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Update the Ceph Nautilus packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.13

The MCP 2019.2.13 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, StackLight, and Ceph MCP components.

The MCP 2019.2.13 update is available starting from March 16, 2021.

Enhancements

In the MCP 2019.2.13 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

OpenStack

In the MCP 2019.2.13 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- RabbitMQ nonclustered configuration
- Arbitrary Galera parameters

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

RabbitMQ nonclustered configuration

Implemented the capability to set up a nonclustered active/backup RabbitMQ configuration instead of using the HA strategy. Mirantis recommends using such approach only to improve the stability and performance on large deployments if the clustered configuration causes issues. The feature is available for OpenStack Queens and starting from the RabbitMQ version 3.8.2.

Learn more

[MCP Operations Guide: Switch to nonclustered RabbitMQ](#)

Arbitrary Galera parameters

Implemented the capability to configure arbitrary Galera parameters using the `wsrep_provider_options` variable.

Learn more

[MCP Operations Guide: Configure arbitrary Galera parameters](#)

Ceph

In the MCP 2019.2.13 maintenance update, Mirantis introduces the following enhancements for Ceph:

- Pipeline jobs improvements

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

Pipeline jobs improvements

- Reorganized and improved the Ceph - add node, Ceph - add osd (upmap), Ceph - remove node, and Ceph - upgrade Jenkins pipeline jobs to provide better maintainability.
- Added a wrapper for the Ceph - add node and Ceph - remove node Jenkins pipeline jobs to simplify the process of adding new or existing Ceph OSD daemons to Ceph OSD nodes or removing Ceph OSD daemons. Enhanced Ceph documentation by adding instructions on how to add or remove Ceph OSD daemons.

Learn more

[MCP Operations Guide: Manage Ceph nodes](#)

Addressed issues

The MCP 2019.2.13 update contains fixes for several MCP components.

DriveTrain

- [35590] Fixed the issue with logrotate configuration missing for ironic-conductor. Now, you can configure log rotation for Ironic. For details, see [MCP Operations Guide: Configure log rotation using logrotate](#).
- [36161] Updated the SaltStack packages to fix the following security vulnerabilities:
 - [CVE-2020-16846](#)
 - [CVE-2020-17490](#)
 - [CVE-2020-25592](#)
- [35976] Fixed the issue with wrong permissions for the systemd unit override.conf files in the Linux, Apache, and NGINX Salt Formulas.
- [36122] Improved the Linux Salt formula by adding the capability to set direct access to some APT repositories when using proxy for the remaining ones.
- [36124] Fixed the issue with the linux-tools-common package missing in the offline mirror image.
- [36057] Fixed the issue with some Salt resources ignoring the no_proxy setting.
- [35930] Fixed the issue with autorotation missing for Dogtag backups, which could cause nodes to run out of space.
- [36110] Parameterized the logrotate:rotate count for the Apache logs.
- [35625] Fixed the issue with the innobackupex-runner.sh script failing to run if an empty directory was present from a previous run.
- [35357] Fixed the Salt states ID conflicts on the prx nodes.

OpenStack

Issues resolutions applied automatically

- [36071][Queens] Fixed the issue causing Cross-Origin Resource Sharing (CORS) outage in Cinder.
- [35971][Salt] Fixed the issue with the nova Salt state failing to control the /etc/nova/nova-compute.conf file.
- [35977][Pike, Queens] Updated the python-cryptography package to fix the issue causing a memory leak in the nova-compute process.
- [36115][Pike] Fixed the issue with Nova trying to delete VM ports even if they were explicitly passed to it at server creation.
- [36002][Pike, Queens] Fixed the issue occurring after reboot of an OpenStack compute node and causing the SR-IOV instances to fail to start on that node.

- [35866][Pike] Fixed the issue with volume creation from an image of a large size taking a significant amount of time.
- [36075][Pike] Fixed the issue with Gnocchi not generating instance resources from private flavors.
- [36060][Pike, Queens] Fixed the issue with Heat stack deletion failing due to a race condition. For details, see the [community issue](#).
- [35954][Pike] Fixed the issue with inability to reconnect to the rabbitmq-server after powering-off one of the RabbitMQ nodes when RabbitMQ is running in a clustered configuration. For details, see the [community issue](#).
- [35947][Queens] Fixed the issue causing the IPv6 fixed address of a port to be assigned and listed as belonging to an IPv4 subnet.
- [35923][Queens] Fixed the issue with the Octavia load balancers sporadically switching to the ERROR state.
- [36074][Pike] Fixed the issue causing rebuilding of one or multiple VMs to fail with the VirtualInterfaceCreateException: Virtual Interface creation failed exception after performing a cold migration.
- [36004][Pike] Fixed the issue causing Nova and Neutron to incorrectly assign interfaces.
- [35953][Pike, Queens] Fixed the issue with OpenStack flavor details being not visible in the OpenStack CLI commands.
- [35807][Pike, Queens] Added automatic startup for OVS bridges to fix the issue with the SystemRxDroppedTooHigh StackLight alerts raising false-positively.
- [35955][Pike, Queens] Improved the Ceilometer Salt formula to fix the issue with inability to modify the pipeline_processing_queues parameter in ceilometer.conf.

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.

- [36098] Nova host_subset_size set to a wrong default value

[36098] Nova host_subset_size set to a wrong default value

Pike, Queens

Fixed the issue with the host_subset_size parameter in the configuration of nova-controller being set to 30, which could cause scheduling issues. Now, host_subset_size is set to 1 by default. If

you previously did not change the `host_subset_size` value, the issue resolution will apply automatically. Otherwise, manually set `host_subset_size` to 1 as described below.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `openstack/control.yml`, set the `host_subset_size` parameter to 1:

```
nova:  
  controller:  
    host_subset_size: 1
```

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

```
salt 'ctl*' state.apply nova
```

OpenContrail

- [35981] Fixed the issue with improper handling of errors in the OpenContrail backup scripts.

StackLight

- [36052] Fixed the issue with the CVP - Sanity checks Jenkins pipeline job failing with the `AssertionError: Internal AlertManager page is not reachable` error. The issue occurred due to Salt using the GPG ciphertext instead of the decrypted plaintext to populate the intended value and affected the deployments with `secrets_encryption_enabled` set to `True`.

Ceph

- [36080] Fixed the issue with the Ceph Salt formula incorrectly updating Ceph keyrings.
- [35840] Fixed the issue with the Ceph Salt formula incorrectly setting Ceph OSD weight.

Known issues

For MCP known issues applicable to MCP 2019.2.13, see [Known issues](#) and corresponding sections in the previous maintenance updates.

- [36332] Docker registry service missing in offline deployment

[36332] Docker registry service missing in offline deployment

Fixed in 2019.2.14

The Docker registry service is missing after deploying the APT node in the offline mode.

Workaround:

1. Log in to the apt01 node.
2. In `/etc/docker/compose/docker/docker-compose.yml`, replace `image: docker-prod-local.docker.mirantis.net/mirantis/external/registry:2019.2.0` with `image: docker-prod-local.docker.mirantis.net/mirantis/external/registry:2019.2.6`.
3. Start the docker-registry service:

```
docker stack deploy --compose-file /etc/docker/compose/docker/docker-compose.yml docker
```

Updated MCP components

The MCP 2019.2.13 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.12 update.

All 2019.2.13 packages are available at <http://mirror.mirantis.com/update/2019.2.13/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.12	2019.2.13
OpenStack Pike	ceilometer	1:9.0.7-3~u16.04+mcp31	1:9.0.7-3~u16.04+mcp33
	cinder	2:11.2.2-3~u16.04+mcp150	2:11.2.2-3~u16.04+mcp153
	horizon	3:12.0.4-5~u16.04+mcp85	3:12.0.4-5~u16.04+mcp90
	neutron	2:11.0.8-5~u16.04+mcp269	2:11.0.8-6~u16.04+mcp271
	nova	2:16.1.8-6~u16.04+mcp271	2:16.1.8-6~u16.04+mcp280
	python-cryptography	2.1.4-2~u16.04+mcp	2.8-1~u16.04+mcp
	python-cryptography-vectors	2.1.4-1~u16.04+mcp	2.8-1~u16.04+mcp
	python-openstackclient	3.12.2-1~u16.04+mcp19	3.12.2-1~u16.04+mcp20
	python-os-brick	1.15.9-1~u16.04+mcp11	1.15.9-1~u16.04+mcp14

	python-oslo.messaging	5.30.8-1~u16.04+mcp19	5.30.8-1~u16.04+mcp20
	seabios	1.10.2-1.1~u16.04+mcp2	1.14.0-1.1~u16.04+mcp1
OpenStack Queens	cinder	2:12.0.10-3~u16.04+mcp152	2:12.0.10-3~u16.04+mcp156
	horizon	3:13.0.3-10~u16.04+mcp99	3:13.0.3-10~u16.04+mcp104
	horizon-mirantis-theme	0.2.0-1~u16.04+mcp3	0.2.0-1~u16.04+mcp4
	manila	1:6.3.2-3~u16.04+mcp134	1:6.3.2-3~u16.04+mcp138
	neutron	2:12.1.1-8~u16.04+mcp407	2:12.1.1-9~u16.04+mcp423
	nova	2:17.0.13-9~u16.04+mcp326	2:17.0.13-9~u16.04+mcp341
	octavia	2.1.2-9~u16.04+mcp126	2.1.2-10~u16.04+mcp129
	python-cryptography	2.1.4-1.1.2~u16.04+mcp1	2.8-1~u16.04+mcp
	python-cryptography-vectors	2.1.4-1.0~u16.04+mcp1	2.8-1~u16.04+mcp
	python-openstackclient	3.14.3-1.0~u16.04+mcp36	3.14.3-1.0~u16.04+mcp40
	python-os-brick	2.3.9-1.0~u16.04+mcp26	2.3.9-1.0~u16.04+mcp31
	python-oslo.cache	1.28.1-1.0~u16.04+mcp9	1.28.1-1.0~u16.04+mcp11
	seabios	1.10.2-1.1~u16.04+mcp2	1.14.0-1.1~u16.04+mcp1
	tempest	1:18.0.0-1~u16.04+mcp42	1:18.0.0-1~u16.04+mcp49
	vmware-nsx	12.0.2-3~u16.04+mcp257	12.0.2-3~u16.04+mcp262
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20201122204910-0	4.1~20210218110907-0
	contrail	4.1~20201122204910-0	4.1~20210218110907-0

	contrail-heat	4.1~20201122204910-0	4.1~20210218110907-0
	contrail-vrouter-dpdk	4.1~20201122204910	4.1~20210218110907
	contrail-web-controller	4.1~20201122204910-0	4.1~20210218110907-0
	contrail-web-core	4.1~20201122204910-0	4.1~20210218110907-0
	neutron-plugin-contrail	4.1~20201122204910-0	4.1~20210218110907-0
Salt formulas	salt-formula-apache	0.2+202003191515.1f81458~xenial1	0.2+202102091417.b7ab9bc~xenial1
	salt-formula-cassandra	0.1+201911071640.af80483~xenial1	0.1+2021021811147.1b589bf~xenial1
	salt-formula-ceilometer	2016.12.1+202009021325.5662655~xenial1	2016.12.1+202102031325.f06bc58~xenial1
	salt-formula-ceph	0.1+202011121413.ec5f052~xenial1	0.1+202101250928.290179e~xenial1
	salt-formula-cinder	2016.12.1+202012021218.5ac8d82~xenial1	2016.12.1+202101251425.ca4467b~xenial1
	salt-formula-dogtag	0.1+202009041057.033c67c~xenial1	0.1+202101221336.9cdc1ea~xenial1
	salt-formula-galera	1.0+202010231127.6427fbb~xenial1	1.0+202101280822.57453da~xenial1
	salt-formula-ironic	0.1+202009031020.c5550c5~xenial1	0.1+202102191402.bb7aaa6~xenial1
	salt-formula-linux	2017.4.1+202010260713.ff40d9e~xenial1	2017.4.1+202102181217.344de40~xenial1
	salt-formula-nginx	0.2+202002071022.df5fd04~xenial1	0.2+202012211735.a30a545~xenial1
	salt-formula-nova	2016.12.1+202011301821.4bb4434~xenial1	2016.12.1+202102121352.d9bab1b~xenial1
	salt-formula-opencontrail	0.2+202010220916.779aab5~xenial1	0.2+202102051450.a1bdd10~xenial1
	salt-formula-oslo-templates	2018.1+202006231140.b3839c0~xenial1	2018.1+202102011510.e24fd64~xenial1

	salt-formula-prometheus	0.1+202010200936.01b3aed~xenial1	0.1+202101291207.8736b2f~xenial1
	salt-formula-rabbitmq	0.2+202007300927.a339125~xenial1	0.2+202102011619.11a6ab9~xenial1
	salt-formula-salt	0.4+202011111100.480bb26~xenial1	0.4+202102022009.9637af2~xenial1
	salt-formula-xtrabackup	0.2+202003231338.2eeeb88~xenial1	0.2+202102050620.b077d2f~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.13 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.13/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.13/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.13/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.13/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.13/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.13/opencontrail-4.1/xenial xenial main
	Salt formulas packages ³⁰	http://mirror.mirantis.com/update/2019.2.13/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.13.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.13.qcow2

	VCP Ubuntu 16.04 image ³⁰	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.13/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.13/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.13/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.13/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.13/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³⁰
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.13/glusterfs-5/xenial xenial main ³⁰
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.13/maas/xenial xenial main ³⁰
	Percona	deb http://mirror.mirantis.com/update/2019.2.13/percona/xenial xenial main ³⁰
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.13/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.13/saltstack-2017.7/xenial xenial main ³⁰ deb http://mirror.mirantis.com/update/2019.2.13/salt-2017.7.8/ xenial xenial main ³⁰

	Upstream Ubuntu system packages ³⁰	deb https://mirror.mirantis.com/update/2019.2.13/ubuntu/xenial/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.13/ubuntu/xenial-updates/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.13/ubuntu/xenial-security/main/restricted/universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.13
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.13
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.13
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.13
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.11 ³⁰
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³⁰
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.13 ³⁰
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.13 ³⁰
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.13 ³⁰
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³⁰
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³⁰
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.9 ³⁰
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ³⁰
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ³⁰
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.10 ³⁰

	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ³⁰
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.13 ³⁰
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.11 ³⁰
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.13 ³⁰
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.13 ³⁰
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.13 ³⁰
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.20 ³⁰
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.10 ³⁰
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ³⁰
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6 ³⁰
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ³⁰
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ³⁰
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³⁰
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.12 ³⁰
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ³⁰

30(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.12 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.12, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	<ol style="list-style-type: none"> 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Ceph updates will be applied during the DriveTrain update.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none">• MCP Operations Guide: Apply security updates using Jenkins• MCP Operations Guide: Apply security updates manually

2019.2.12

The MCP 2019.2.12 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, and StackLight MCP components.

The MCP 2019.2.12 update is available starting from December 11, 2020.

Enhancements

In the MCP 2019.2.12 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.12 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Back up and restore Keystone credential keys

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Back up and restore Keystone credential keys

Implemented the capability to back up and restore the Keystone credential keys in scope of performing the backup and restore procedures using the Backupninja backup pipeline and Backupninja restore pipeline Jenkins pipeline jobs.

Learn more

- [MCP Operations Guide: Create an instant backup using Backupninja pipeline](#)
- [MCP Operations Guide: Restore the services using Backupninja pipeline](#)

OpenStack

In the MCP 2019.2.12 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Cleanup of an OpenStack database

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

Cleanup of an OpenStack database

Implemented the capability to automatically clean up the Nova, Cinder, or Heat database using the Deploy - Openstack Database Cleanup Jenkins pipeline job.

Learn more

[MCP Operations Guide: Clean up an OpenStack database](#)

OpenContrail

In the MCP 2019.2.12 maintenance update, Mirantis introduces the following enhancements for OpenContrail:

- Configuring the VNC API statistics
- Configuring the VMI and VN statistics collection

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

Configuring the VNC API statistics

Implemented the capability to disable or enable sending the Virtual Network Controller (VNC) statistics to the collector service using the `disable_vnc_api_stats` option of the OpenContrail `contrail-api` service through the OpenContrail Salt formula. By default, `disable_vnc_api_stats` is set to True.

Learn more

[MCP Operations Guide: Enable or disable VNC API statistics](#)

Configuring the VMI and VN statistics collection

Implemented the capability to disable or enable the OpenContrail vRouter agent service to collect the virtual machine interfaces (VMIs) and virtual networks (VNs) statistics using the `disable_stats_collection` option through the OpenContrail Salt formula. By default, `disable_stats_collection` is set to True.

Learn more

[MCP Operations Guide: Enable or disable VMI and VN statistics collection](#)

StackLight

In the MCP 2019.2.12 maintenance update, Mirantis introduces the following enhancements for StackLight:

- Disabling of HTTP probes for OpenStack public endpoints

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

Disabling of HTTP probes for OpenStack public endpoints

Added the capability to disable HTTP probes for OpenStack public endpoints. In this case, Telegraf will perform HTTP checks only for the admin and internal OpenStack endpoints.

Learn more

[MCP Operations Guide: Disable HTTP probes for OpenStack public endpoints](#)

Addressed issues

The MCP 2019.2.12 update contains fixes for several MCP components.

DriveTrain

Issues resolutions applied automatically

- [35577] Fixed the issue with the Prometheus Salt formula failing to control permissions on Prometheus configuration. Enhanced the Prometheus Salt formula by adding a default mode for Prometheus files.
- [35510] Fixed the issue with the Salt Master node deployment failing due to an error in `salt.minion.cert`.

- [35773] Extended the txqueuelen parameter for linux.network to fix the issue with inability to set custom_txqueuelen for veth and br interfaces.
- [34400] Fixed the issue causing failure to restart a Salt Minion node.
- [35769] Fixed the issue with inability to use the NumInstancesFilter filter. Now, you can define the maximum number of instances allowed to run on a host using the max_instances_per_host parameter.

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.

- [35705] Improper operation of Galera HA
- [35884] Alerts from Alertmanager are absent in Alerta

[35705] Improper operation of Galera HA

Fixed the issue with Galera and HAProxy using the MySQL health check instead of the Galera health check.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Generate a Galera cluster check password and add it to classes/cluster/<cluster_name>/infra/secrets.yml using the following parameter as described in [MCP Operations Guide: Manage secrets in the Reclass model](#).

```
parameters:
  _param:
    ...
    galera_clustercheck_password: <generated_password>
    ...
```

3. Apply the changes to Galera and HAProxy:

```
salt -C '@galera:master or @galera:slave' saltutil.refresh_pillar
salt -C '@galera:master or @galera:slave' state.apply galera
salt -C '@galera:master or @galera:slave' state.apply haproxy
```

4. Commit the changes to your local repository.

[35884] Alerts from Alertmanager are absent in Alerta

Fixed the issue with Alertmanager failing to send alerts to Alerta.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Generate an Alerta admin API key and add it to `classes/cluster/<cluster_name>/infra/secrets.yml` using the following parameter as described in [MCP Operations Guide: Manage secrets in the Reclass model](#).

```
parameters:
  _param:
  ...
  alerta_admin_api_key_generated: <generated_40_hex_api_key>
  ...
```

3. Add the generated Alerta admin API key to `classes/cluster/<cluster_name>/stacklight/init.yml` using the following parameter.

```
parameters:
  _param:
  ...
  alerta_admin_key: ${_param:alerta_admin_api_key_generated}
  ...
```

4. Apply the changes to Alerta and Alertmanager:

```
salt -C 'l@prometheus:alerta or l@prometheus:alertmanager' saltutil.refresh_pillar
salt -C 'l@prometheus:alerta' state.apply prometheus.alerta
salt -C 'l@prometheus:alertmanager' state.apply prometheus.alertmanager
salt -C 'l@prometheus:alerta or l@prometheus:alertmanager' state.apply docker.client
```

5. Commit the changes to your local repository.

OpenStack

Issues resolutions applied automatically

- [35639][Pike, Queens] Fixed the issue causing live migration and resizing to fail with the Unable to find security driver for model apparmor error message if the Huge Pages feature is enabled. Added the `security_driver: apparmor` parameter to the Nova Salt formula.
- [35129][Queens] Fixed the issue causing inability to define custom filters through the Reclass Model.
- [35834][Queens] Fixed the issue causing Nova and Neutron to incorrectly assign interfaces.

- [35762][Pike, Queens] Fixed the issue with the neutron client state failing with the request() got an unexpected keyword argument ‘__pub_pid’ error message.
- [35763][Pike, Queens] Fixed the issue causing failure to list, create, and delete private Nova flavors through Salt states and modules.
- [35889][Pike, Queens] Updated Django to version 1.11.29 to obtain the latest security fixes.
- [35772][Pike, Queens] Fixed the issue with the creation of an encrypted Cinder volume failing with the ImageCopyFailure: Failed to copy image to volume error message.
- [35902][Pike, Queens] Fixed the issue with Neutron attempting to connect to Designate through an unreachable public endpoint URL.
- [35915][Pike] Disabled the check for bridge creation in case of the Open vSwitch restart. During the Open vSwitch restart, full sync of all bridges is triggered by neutron-ovs-agent.
- [35839][Pike] Fixed the issue causing the IPv6 fixed address of a port to be assigned and listed as belonging to an IPv4 subnet.
- [35673][Pike, Queens] Improved the Octavia Salt formula by adding a mine function to obtain the Octavia amphora owner. The new function allows for better control and properly handles the interface to define what type of Glance endpoint to access.
- [35917][Pike, Queens] Fixed the issue causing novnc to switch to the view-only mode after applying maintenance updates.
- [35657][Queens] Fixed the [community issue](#) causing the designate state to fail due to inability to run the designate-manage database sync command when applying maintenance updates. The issue resolution applies automatically and you do not need to clean up the Designate database manually.
- [35715][Pike, Queens] Updated the QEMU packages to fix the following security vulnerabilities:
 - [CVE-2020-10756](#)
 - [CVE-2020-12829](#)
 - [CVE-2020-13253](#)
 - [CVE-2020-13361](#)
 - [CVE-2020-13362](#)
 - [CVE-2020-13659](#)
 - [CVE-2020-13754](#)
 - [CVE-2020-13765](#)
 - [CVE-2020-15863](#)
 - [CVE-2020-16092](#)

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.

- [35864] Inability to use IPv6 load balancers in active-standby mode

[35864] Inability to use IPv6 load balancers in active-standby mode

Queens

Fixed the issue causing inability to use IPv6 load balancers in the active-standby mode. Updated the Octavia amphora image. To apply the issue resolution, update the [Octavia amphora image](#) in Glance.

OpenContrail

- [35897] In the HAProxy configuration for the contrail-api service, changed the default balance method from roundrobin to leastconn. This prevents a performance issue from occurring if several heavy requests are redirected to the same contrail-api worker. Using the leastconn balancing method, the request is scheduled to a worker with the least active sessions to avoid performance issues when several requests are queueing at one worker.
- [35747] Fixed the issue with an unstable connection between the RabbitMQ server and the OpenContrail controller nodes.

StackLight

- [35949] Fixed the issue causing the Start and End panels of the KPI-Provisioning Grafana dashboard as well as the Notifications Kibana dashboard to display no data.
- [35778] Fixed the issue with Octavia logs being not available in Elasticsearch.
- [35784] Fixed the sf-reporter queries for OpenStack metrics.

Known issues

For MCP known issues applicable to MCP 2019.2.12, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.12 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.11 update. All 2019.2.12 packages are available at <http://mirror.mirantis.com/update/2019.2.12/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.11	2019.2.12
OpenStack Pike	neutron	2:11.0.8-5~u16.04+mcp261	2:11.0.8-5~u16.04+mcp269
	nova	2:16.1.8-6~u16.04+mcp264	2:16.1.8-6~u16.04+mcp271
	novnc	1:0.6.1-1.1~u16.04+mcp5	1:0.6.1-1.1~u16.04+mcp6
	python-castellan	0.12.3-1~u16.04+mcp11	0.12.3-1~u16.04+mcp12
	python-django	1:1.11.22-1~u16.04+mcp1	1:1.11.29-1~u16.04+mcp1
	qemu	1:2.11+dfsg-1.7.13~u16.04+mcp2	1:2.11+dfsg-1.7.31~u16.04+mcp1
	OpenStack Queens	cinder	2:12.0.10-3~u16.04+mcp150
designate		1:6.0.1-1.1~u16.04+mcp31	1:6.0.1-1.1~u16.04+mcp32
horizon-mirantis-theme		0.2.0-1~u16.04+mcp1	0.2.0-1~u16.04+mcp3
ironic		1:10.1.10-1.1~u16.04+mcp75	1:10.1.10-1.1~u16.04+mcp77
keystone		2:13.0.4-4~u16.04+mcp42	2:13.0.4-4~u16.04+mcp44
manila		1:6.3.2-3~u16.04+mcp128	1:6.3.2-3~u16.04+mcp134
neutron		2:12.1.1-8~u16.04+mcp371	2:12.1.1-8~u16.04+mcp407
neutron-dynamic-routing		2:12.0.0-3~u16.04+mcp1	2:12.0.1-1~u16.04+mcp1
nova		2:17.0.13-9~u16.04+mcp289	2:17.0.13-9~u16.04+mcp326
novnc		1:0.6.1-1.1~u16.04+mcp4	1:0.6.1-1.1~u16.04+mcp5
octavia		2.1.2-9~u16.04+mcp125	2.1.2-9~u16.04+mcp126
python-castellan		0.17.0-2.0~u16.04+mcp19	0.17.0-2.0~u16.04+mcp20
python-django		1:1.11.22-1~u16.04+mcp1	1:1.11.29-1~u16.04+mcp1

	python-manilaclient	1.21.1-1.0~u16.04+mcp23	1.21.2-1.0~u16.04+mcp19
	python-oslo.messaging	5.35.6-2~u16.04+mcp29	5.35.6-2~u16.04+mcp31
	python-oslo.policy	1.33.2-1.0~u16.04+mcp6	1.33.2-1.0~u16.04+mcp8
	qemu	1:2.11+dfsg-1.7.13~u16.04+mcp3	1:2.11+dfsg-1.7.31~u16.04+mcp1
	vmware-nsx	12.0.2-3~u16.04+mcp253	12.0.2-3~u16.04+mcp257
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20200905053719-0	4.1~20201122204910-0
	contrail	4.1~20200905053719-0	4.1~20201122204910-0
	contrail-heat	4.1~20200905053719-0	4.1~20201122204910-0
	contrail-vrouter-dpdk	4.1~20200905053719	4.1~20201122204910
	contrail-web-controller	4.1~20200905053719-0	4.1~20201122204910-0
	contrail-web-core	4.1~20200905053719-0	4.1~20201122204910-0
	neutron-plugin-contrail	4.1~20200905053719-0	4.1~20201122204910-0
Salt formulas	salt-formula-ceph	0.1+202008181908.c54081b~xenial1	0.1+202011121413.ec5f052~xenial1
	salt-formula-cinder	2016.12.1+202008310917.59a1f1a~xenial1	2016.12.1+202012021218.5ac8d82~xenial1
	salt-formula-designate	2016.12.1+202008310848.5d51112~xenial1	2016.12.1+202010210932.14dac2e~xenial1
	salt-formula-galera	1.0+201911290842.938c821~xenial1	1.0+202010231127.6427fbb~xenial1
	salt-formula-haproxy	0.2+202008241001.b350fea~xenial1	0.2+202011121320.a2cb999~xenial1
	salt-formula-heat	2016.12.1+202008201010.110b515~xenial1	2016.12.1+202010211317.ec9707f~xenial1

	salt-formula-keystone	2016.12.1+202009091448.2d1373a~xenial1	2016.12.1+202011172142.c7d1c5f~xenial1
	salt-formula-linux	2017.4.1+202008131021.fb2dd0a~xenial1	2017.4.1+202010260713.ff40d9e~xenial1
	salt-formula-neutron	2016.12.1+202009020833.1856c78~xenial1	2016.12.1+202011100915.4ae3012~xenial1
	salt-formula-nova	2016.12.1+202009031017.1abd2cd~xenial1	2016.12.1+202011301821.4bb4434~xenial1
	salt-formula-octavia	2017.6+202008201232.ac4f0c8~xenial1	2017.6+202011111037.c3458cb~xenial1
	salt-formula-opencon trail	0.2+202009041340.16862ad~xenial1	0.2+202010220916.779aab5~xenial1
	salt-formula-prometh eus	0.1+202008181916.6f72eb9~xenial1	0.1+202010200936.01b3aed~xenial1
	salt-formula-salt	0.4+202008181023.e58d897~xenial1	0.4+202011111100.480bb26~xenial1
	salt-formula-telegraf	0.1+202009091226.e3551f3~xenial1	0.1+202010291041.d9d7c86~xenial1

Release artifacts

This section lists the artifacts of the MCP 2019.2.12 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.12/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.12/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.12/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.12/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.12/ceph-nautilus/xenial xenial main

	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.12/opencontrail-4.1/xenial xenial main
	Salt formulas packages ³¹	http://mirror.mirantis.com/update/2019.2.12/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.12.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.12.qcow2
	VCP Ubuntu 16.04 image ³¹	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.12/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.12/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.12/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.12/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.12/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³¹
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.12/glusterfs-5/xenial xenial main ³¹
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable

	MAAS	deb http://mirror.mirantis.com/update/2019.2.12/maas/xenial/xenial main ³¹
	Percona	deb http://mirror.mirantis.com/update/2019.2.12/percona/xenial/xenial main ³¹
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.12/saltstack-2017.7/trusty/trusty main deb http://mirror.mirantis.com/update/2019.2.12/saltstack-2017.7/xenial/xenial main ³¹ deb http://mirror.mirantis.com/update/2019.2.12/salt-2017.7.8/xenial/xenial main ³¹
	Upstream Ubuntu system packages ³¹	deb https://mirror.mirantis.com/update/2019.2.12/ubuntu/xenial/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.12/ubuntu/xenial-updates/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.12/ubuntu/xenial-security/main/restricted/universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.12
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.12
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.12
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.12
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.11 ³¹
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³¹
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.9 ³¹
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.9 ³¹
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.9 ³¹
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³¹

cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³¹
gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.9 ³¹
gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ³¹
gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ³¹
grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.10 ³¹
heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ³¹
jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.9 ³¹
jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.11 ³¹
mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.10 ³¹
openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.11 ³¹
phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.9 ³¹
postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³¹
prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.10 ³¹
prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ³¹
pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6 ³¹
registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ³¹
remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ³¹
sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³¹
telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.12 ³¹

	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ³¹

31(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.11 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.11, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> 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.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	<ol style="list-style-type: none"> 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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Ceph updates will be applied during the DriveTrain update.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.11

The MCP 2019.2.11 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, Ceph, and StackLight MCP components.

The MCP 2019.2.11 update is available starting from September 30, 2020.

Enhancements

In the MCP 2019.2.11 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.11 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Ubuntu security updates
- Security improvement for Docker containers

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Ubuntu security updates

Updated MySQL for Pike and Queens to version 5.6.48-1~u16.04+mcp1 to apply the following Ubuntu security updates:

- [USN-4070-1](#)
 - [USN-4195-1](#)
 - [USN-4250-1](#)
-

Security improvement for Docker containers

Improved the Docker containers security by enhancing the Docker Salt formula to support Docker secrets.

Learn more

[34268] Security improvement for Docker containers

OpenStack

In the MCP 2019.2.11 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Gnocchi and Panko policies configuration

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

Gnocchi and Panko policies configuration

Added the capability to configure custom policies for Gnocchi and Panko through the ReClass model. To set a Gnocchi or Panko policy, use the following pillars:

- For Panko:

```
panko:  
  server:  
    ...  
    policy:  
      'context_is_admin': 'role:admin'  
      'segregation': 'rule:context_is_admin'
```

```
# Add key without value to remove line from policy.json
'telemetry:events:index':
```

- For Gnocchi:

```
gnocchi:
  server:
    ...
    policy:
      'resource_owner': 'project_id:%(project_id)s'
      'get status': 'role:admin'
      # Add key without value to remove line from policy.json
      'list resource type':
```

MCP documentation

In the MCP 2019.2.11 maintenance update, Mirantis introduces the following enhancements for MCP documentation on top of continuous improvements delivered to the existing MCP guides:

- OpenContrail IPv6 capabilities

OpenContrail IPv6 capabilities

Updated the MCP Reference Architecture by describing the IPv6 capabilities available in OpenContrail.

Learn more

[OpenContrail IPv6 support](#)

Addressed issues

The MCP 2019.2.11 update contains fixes for several MCP components.

DriveTrain

Issues resolutions applied automatically

- [35442] Fixed the issue with the Deploy - upgrade control VMs pipeline failing during the packages upgrade of the OpenStack controller nodes with the following error:

```
ERROR: Stage Upgrade OS failed with the following exception:
groovy.lang.MissingMethodException: No signature of method:
```

```
java.lang.Boolean.split() is applicable for argument types: (java.lang.String)
values: []
```

- [35440] Fixed the issue with the RabbitMQ update failing during the rabbitmq_task_upgrade_verify_service test. The issue occurred due to the RabbitMQ cluster using nodes with a long name that caused the cluster status information with running nodes failing to be printed on several lines.
- [33909] Fixed the issue with restoring of Dogtag that led to the Rendering SLS 'base:barbican.server' failed: Jinja variable 'dict object' has no attribute 'key' error.
- [35539] Fixed the issue with the openssh state failing due to the OpenSSH Salt formula using only the RSA key format in known_hosts. The fix adds the possibility to enable the ECDSA key format using known_hosts_use_ecdsa: true.

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.

- [34268] Security improvement for Docker containers

[34268] Security improvement for Docker containers

Enhanced the Docker Salt formula to support Docker secrets and improve the Docker containers security. The improvement applies automatically when applying maintenance updates. However, the secrets are still visible in plain text when running docker service inspect because Docker Swarm keeps the previous specification for a rollback. To remove it, follow the steps below:

To update the Docker Swarm configuration:

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

```
for service in Gerrit_db Gerrit_server Jenkins_slave01 Jenkins_slave02 Jenkins_slave03 ldap_server; do
salt -C '@jenkins:client and @docker:client and not @salt:master' cmd.run "docker service update ${service} --force"
```

```
for service in dashboard_grafana monitoring_alerta; do
salt -C '@docker:swarm:role:master and @prometheus:server' cmd.run "docker service update ${service} --force"
```

OpenStack

Issues resolutions applied automatically

- [35660][Queens] Fixed the issue causing the Neutron Open vSwitch agents to become out of sync during instance launch. In this case, the neutron-openvswitch-agent logs on the OpenStack compute node included the TypeError error messages.
- [35634][Queens] Fixed the issue with inability to create an encrypted volume using public network in the OpenStack environments with Barbican.
- [34972][Queens] Fixed the issue causing Keystone to generate non-existing users in case of LDAP and Federation enabled at the same time.
- [35682][Pike, Queens] Added the VIR_MIGRATE_PARAM_PERSIST_XML to libvirt to fix [CVE-2020-17376](#).
- [35480][Pike] Improved the database retry mechanism to avoid issues with Neutron database errors on port update.
- [35592][Queens] Fixed the issue with parsing of volume attachment events causing the KeyError error when creating or deleting a volume.
- [33882][Pike, Queens] Fixed the issue with a Heat stack deletion failing with the ConcurrentTransaction error.
- [35468][Pike, Queens] Fixed the issue with the Heat stack creation failing with the DBError(pymysql.err.IntegrityError) error while updating or creating values in the database.
- [35361][Salt] Added the project_id parameter to the keystone_user_{{ user_name }}_role_{{ role.name }}_assigned Salt state to fix the issue with conflicting state IDs.
- [35385][Salt] Added the wsgi_processes_count to the Cinder Salt formula to fix the issue with inability to control the number of Cinder WSGI processes.
- [35511][Queens] Improved the Neutron Salt formula to support the integration of Designate with Nova and Neutron. The issue affected only the OpenStack Queens release.
- [35661][Queens] Fixed Ceilometer to perform queries based on the adapted user IDs if implicit tenants are enabled in RADOS Gateway.

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.

- [35657] [Queens] Failure during designate-manage database sync

[35657] [Queens] Failure during designate-manage database sync

When applying MCP 2019.2.11 maintenance updates, the designate state may fail due to inability to run the designate-manage database sync command. For details, see the [community issue](#).

To apply the fix that prevents the issue, manually clean up the Designate database as described below.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Verify that the Designate packages are updated on the primary node. The reported package version must be 1:6.0.1-1.1~u16.04+mcp31.

```
sudo salt -l "designate:server:role:primary" pkg.version designate-central python-designate
```

3. Stop the designate-central service on all nodes:

```
sudo salt -l "designate:server:role:*" service.stop designate-central
```

4. Start the designate-central service on the primary node only:

```
sudo salt -l "designate:server:role:primary" service.start designate-central
```

5. Clean up the duplicated service entries from the Designate database:

```
sudo salt -l "designate:server:role:primary" cmd.run "designate-manage services delete_duplicated_services"
```

6. Start the designate-central service:

```
sudo salt -l "designate:server:role:*" service.start designate-central
```

Once done, continue the update process from the failed step.

OpenContrail

- [35730] Fixed the issue with the `compute_node_address` parameter breaking a vRouter configuration and preventing it from start when switching vRouter from the discovery method to static. The issue affected the OpenContrail 3.2 deployments with the tenant network being used for the OpenStack compute nodes communication with the control plane.
- [35200] Fixed the issue with the Error: 403 Permission Denied displaying on most pages of the OpenContrail 4.1 web UI if a logged user has roles not only in the admin tenant.

StackLight

- [35572] Fixed the issue with Alerta updating incorrectly due to invalid API keys, causing alerts to get stuck.
- [35375] Fixed the memory leak issue causing Prometheus Relay to allocate all available RAM on the node.
- [35533] Fixed the issue with the Nova Compute graph in the Nova - Overview Grafana dashboard displaying incorrect information.
- [35683] Fixed the issue with Telegraf failing to gather the compute quota set metrics.
- [35549] Fixed the issue with improper monitoring of public endpoint certificates. Replaced the unavailability alerts for the OpenStack components endpoints with a generic OpenstackServiceEndpointDown alert. Enhanced the OpenStack Grafana dashboards to display the public endpoint.
- [35536] Improved the GlusterFs monitoring by adding the GlusterfsMountMissing that raises when a GlusterFS mount point is not mounted.
- [35435] To avoid issues with short-living alerts, added the for: 2m clause to the alerts that use the procstat_running metric.
- [35685] Fixed the raise condition of the HaproxyBackendDownMajor alert to properly indicate the number of backends in the DOWN state.
- [35477] To avoid issues with Keystone authorization errors due to keys being out of sync, added the KeystoneKeysRotationFailure alert to monitor the rotation of fernet and credentials Keystone keys.

Ceph

- [35675] Fixed the Ceph - add node, Ceph - add osd (upmap), and Ceph - remove node Jenkins pipeline jobs to enable using them during migration to the ceph-volume tool.
- [35756] Removed the redundant RUNHIGHSTATE parameter from the Ceph - upgrade Jenkins pipeline job to avoid pipeline failure during the Ceph upgrade from Luminous to Nautilus.
- [35668] Fixed the issue with the ceph.osd state failing after a successful deployment in case of persistent device names being used in the deployment model.

Known issues

For MCP known issues applicable to MCP 2019.2.11, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.11 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.10 update. All 2019.2.11 packages are available at <http://mirror.mirantis.com/update/2019.2.11/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.10	2019.2.11
OpenStack Pike	cinder	2:11.2.2-3~u16.04+mcp139	2:11.2.2-3~u16.04+mcp150
	heat	1:9.0.7-2~u16.04+mcp100	1:9.0.7-2~u16.04+mcp105
	keystone	2:12.0.3-5~u16.04+mcp29	2:12.0.3-5~u16.04+mcp38
	mysql-wsrep-5.6	5.6.41-1~u16.04+mcp1	5.6.48-1~u16.04+mcp1
	neutron	2:11.0.8-5~u16.04+mcp249	2:11.0.8-5~u16.04+mcp261
	networking-l2gw	1:11.0.0-1~u16.04+mcp19	1:11.0.0-1~u16.04+mcp23
	nova	2:16.1.8-6~u16.04+mcp240	2:16.1.8-6~u16.04+mcp264
	novnc	1:0.6.1-1.1~u16.04+mcp4	1:0.6.1-1.1~u16.04+mcp5
	panko	3.1.0-2~u16.04+mcp18	3.1.1-2~u16.04+mcp12
	python-os-brick	1.15.9-1~u16.04+mcp8	1.15.9-1~u16.04+mcp11
OpenStack Queens	ceilometer	1:10.0.1-3~u16.04+mcp40	1:10.0.1-3~u16.04+mcp43
	cinder	2:12.0.10-3~u16.04+mcp138	2:12.0.10-3~u16.04+mcp150
	designate	1:6.0.1-1.1~u16.04+mcp27	1:6.0.1-1.1~u16.04+mcp31
	heat	1:10.0.3-1.1~u16.04+mcp113	1:10.0.3-1.1~u16.04+mcp120
	ironic	1:10.1.10-1.1~u16.04+mcp68	1:10.1.10-1.1~u16.04+mcp75

	keystone	2:13.0.4-4~u16.04+mcp40	2:13.0.4-4~u16.04+mcp42
	manila	1:6.3.2-3~u16.04+mcp85	1:6.3.2-3~u16.04+mcp128
	manila-ui	2:13.1-1.0~u16.04+mcp4	2:13.1-1.0~u16.04+mcp6
	mysql-wsrep-5.6	5.6.41-1~u16.04+mcp1	5.6.48-1~u16.04+mcp1
	networking-ovn	4.0.4-1.0~u16.04+mcp97	4.0.4-1.0~u16.04+mcp105
	networking-l2gw	1:12.0.1-1.0~u16.04+mcp17	1:12.0.1-1.0~u16.04+mcp21
	neutron	2:12.1.1-8~u16.04+mcp311	2:12.1.1-8~u16.04+mcp371
	nova	2:17.0.13-9~u16.04+mcp253	2:17.0.13-9~u16.04+mcp289
	novnc	1:0.6.1-1.1~u16.04+mcp3	1:0.6.1-1.1~u16.04+mcp4
	python-castellan	0.17.0-2.0~u16.04+mcp18	0.17.0-2.0~u16.04+mcp19
	python-glance-store	0.23.0-2~u16.04+mcp15	0.23.0-2~u16.04+mcp16
	python-keystonemiddleware	4.22.0-1.0~u16.04+mcp10	4.22.0-1.0~u16.04+mcp13
	python-openstackclient	3.14.3-1.0~u16.04+mcp26	3.14.3-1.0~u16.04+mcp36
	python-os-brick	2.3.9-1.0~u16.04+mcp19	2.3.9-1.0~u16.04+mcp26
	python-oslo.messaging	5.35.6-2~u16.04+mcp27	5.35.6-2~u16.04+mcp29
	vmware-nsx	12.0.2-3~u16.04+mcp238	12.0.2-3~u16.04+mcp253
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20200701204814-0	4.1~20200905053719-0
	contrail	4.1~20200701204814-0	4.1~20200905053719-0
	contrail-heat	4.1~20200701204814-0	4.1~20200905053719-0

	contrail-vrouter-dpdk	4.1~20200701204814	4.1~20200905053719
	contrail-web-controller	4.1~20200701204814-0	4.1~20200905053719-0
	contrail-web-core	4.1~20200701204814-0	4.1~20200905053719-0
	neutron-plugin-contrail	4.1~20200701204814-0	4.1~20200905053719-0
Salt formulas	salt-formula-aodh	0.2+201911290838.15dbddd~xenial1	0.2+202008201111.23a40f7~xenial1
	salt-formula-barbican	2018.1+202002070852.ba74a99~xenial1	2018.1+202008201011.34ba975~xenial1
	salt-formula-ceilometer	2016.12.1+202006160859.d73d127~xenial1	2016.12.1+202009021325.5662655~xenial1
	salt-formula-ceph	0.1+202007090952.f4c8643~xenial1	0.1+202008181908.c54081b~xenial1
	salt-formula-cinder	2016.12.1+202003311421.96c2d46~xenial1	2016.12.1+202008310917.59a1f1a~xenial1
	salt-formula-designate	2016.12.1+202002041545.d6c1c45~xenial1	2016.12.1+202008310848.5d51112~xenial1
	salt-formula-docker	0.1+202003261323.27a65be~xenial1	0.1+202008131329.3623e35~xenial1
	salt-formula-dogtag	0.1+201911081251.ff45cc~xenial1	0.1+202009041057.033c67c~xenial1
	salt-formula-fluentd	0.1+202006030852.cbfa1b5~xenial1	0.1+202009021401.98eb487~xenial1
	salt-formula-glance	2016.12.1+20200620842.3ca281d~xenial1	2016.12.1+202008201233.48392d2~xenial1
	salt-formula-glusterfs	2017.3+202001141131.db7ae3a~xenial1	2017.3+202008180918.cf065bb~xenial1
	salt-formula-haproxy	0.2+202001150929.6f4d961~xenial1	0.2+202008241001.b350fea~xenial1
	salt-formula-heat	2016.12.1+202006010900.7553ea3~xenial1	2016.12.1+202008201010.110b515~xenial1

	salt-formula-ironic	0.1+202003311418.f43a70f~xenial1	0.1+202009031020.c5550c5~xenial1
	salt-formula-keepalived	0.2+201911271107.33c0fb2~xenial1	0.2+202008131016.c2955cd~xenial1
	salt-formula-keystone	2016.12.1+202003180714.918c4b3~xenial1	2016.12.1+202009091448.2d1373a~xenial1
	salt-formula-kibana	0.2+201911071624.5c97b87~xenial1	0.2+202008131019.bd3a3ef~xenial1
	salt-formula-linux	2017.4.1+202006212000.a89140d~xenial1	2017.4.1+202008131021.fb2dd0a~xenial1
	salt-formula-maas	0.0.1+202003241701.55d9d76~xenial1	0.0.1+202008180846.14ccca3~xenial1
	salt-formula-manila	2017.6+202002031333.aa3c3ad~xenial1	2017.6+202008201013.73c004d~xenial1
	salt-formula-mongodb	0.2+201911070927.f14d0a9~xenial1	0.2+202008121308.3a2ea00~xenial1
	salt-formula-neutron	2016.12.1+202006261028.cb0d8fd~xenial1	2016.12.1+202009020833.1856c78~xenial1
	salt-formula-nova	2016.12.1+202006221622.5bbfef3~xenial1	2016.12.1+202009031017.1abd2cd~xenial1
	salt-formula-octavia	2017.6+202004170823.727a8d7~xenial1	2017.6+202008201232.ac4f0c8~xenial1
	salt-formula-opencontrail	0.2+202005250946.18a1ee6~xenial1	0.2+202009041340.16862ad~xenial1
	salt-formula-openssh	0.2+202005250827.13cc6f8~xenial1	0.2+202008281452.d72d1a7~xenial1
	salt-formula-panko	2017.6+201911290835.a8e0f0c~xenial1	2017.6+202008180941.ab341b7~xenial1
	salt-formula-prometheus	0.1+202006251539.e3870e0~xenial1	0.1+202008181916.6f72eb9~xenial1
	salt-formula-rabbitmq	0.2+202006030849.6079bf0~xenial1	0.2+202007300927.a339125~xenial1
	salt-formula-runttest	0.1+202005190810.27eee86~xenial1	0.1+202009031028.1c6013b~xenial1
	salt-formula-salt	0.4+202003301102.521d081~xenial1	0.4+202008181023.e58d897~xenial1

	salt-formula-telegraf	0.1+202005201636. b920a52~xenial1	0.1+202009091226. e3551f3~xenial1
Extra packages	prometheus-relay	0.3-1~u16.04+mcp8	0.3-1~u16.04+mcp9
	telegraf	1:1.9.1-3~u16.04+m cp59	1:1.9.1-3~u16.04+m cp70

Release artifacts

This section lists the artifacts of the MCP 2019.2.11 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.11/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.11/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.11/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.11/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.11/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.11/opencontrail-4.1/xenial xenial main
	Salt formulas packages ³²	http://mirror.mirantis.com/update/2019.2.11/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.11.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.11.qcow2
	VCP Ubuntu 16.04 image ³²	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

Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.11/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.11/elasticsearch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.11/elasticsearch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.11/elasticsearch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.11/elasticsearch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³²
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.11/glusterfs-5/xenial xenial main ³²
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.11/maas/xenial xenial main ³²
	Percona	deb http://mirror.mirantis.com/update/2019.2.11/percona/xenial xenial main ³²
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.11/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.11/saltstack-2017.7/xenial xenial main ³² deb http://mirror.mirantis.com/update/2019.2.11/salt-2017.7.8/ xenial xenial main ³²

	Upstream Ubuntu system packages ³²	deb https://mirror.mirantis.com/update/2019.2.11/ubuntu/xenial/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.11/ubuntu/xenial-updates/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.11/ubuntu/xenial-security/main/restricted/universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.11
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.11
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.11
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.11
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.11 ³²
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³²
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.9 ³²
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.9 ³²
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.9 ³²
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³²
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³²
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.9 ³²
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ³²
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.11 ³²
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.10 ³²

	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ³²
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.9 ³²
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.11 ³²
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.10 ³²
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/openldap:2019.2.11 ³²
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.9 ³²
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³²
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.10 ³²
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.11 ³²
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6 ³²
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ³²
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ³²
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³²
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.11 ³²
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ³²

32(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.10 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.10, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> 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.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	<ol style="list-style-type: none"> 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	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 as described in MCP Operations Guide: Update StackLight LMA .
6	Ceph	Ceph updates will be applied during the DriveTrain update.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso
Known issues

2019.2.10

The MCP 2019.2.10 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, Ceph, and StackLight MCP components.

The MCP 2019.2.10 update is available starting from July 23, 2020.

Enhancements

In the MCP 2019.2.10 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.10 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- LDAP over SSL/TLS

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

LDAP over SSL/TLS

Enhanced the Linux Salt formula to support Lightweight Directory Access Protocol (LDAP) over Transport Layer Security (TLS)/Secure Sockets Layer (SSL).

OpenStack

In the MCP 2019.2.10 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- CpuFlagsFilter filter for live migrations

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

CpuFlagsFilter filter for live migrations

Introduced the capability to add CpuFlagsFilter, a custom Nova scheduler filter for live migrations. The filter ensures that the CPU features of a live migration source host match the target host.

Learn more

- [MCP Deployment Guide: Configure a CPU model](#)
- [MCP Operations Guide: Add the Nova CpuFlagsFilter custom filter](#)

Ceph

In the MCP 2019.2.10 maintenance update, Mirantis introduces the following enhancements for Ceph:

- Restriction of RADOS Gateway capabilities
- Ceph Nautilus support
- RBD monitoring

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

Restriction of RADOS Gateway capabilities

To improve the product security, restricted the RADOS Gateway capabilities to a bare minimum. For the existing environments, perform the steps described in [MCP Operations Guide: Restrict the RADOS Gateway capabilities](#).

Ceph Nautilus support

Introduced support for the Ceph Nautilus 14.2.6 release. The major enhancements include the Messenger v2 protocol and the ceph-volume tool. Added full support for the ceph-volume tool that is now enabled by default for new MCP deployments. For the existing deployments, enable the ceph-volume tool before upgrading Ceph from Luminous to Nautilus.

Learn more

- [Ceph Nautilus 14.2.6 release notes](#)
- [Messenger v2 protocol](#)
- [Ceph-volume tool](#)
- [MCP Operations Guide: Enable the ceph-volume tool](#)
- [MCP Operations Guide: Upgrade Ceph from Luminous to Nautilus](#)

RBD monitoring

TECHNICAL PREVIEW

Implemented the capability to monitor RADOS Block Device (RBD) images using the Ceph RBD Overview Grafana dashboard. RBD monitoring requires Ceph Nautilus and is disabled by default.

Learn more

- [MCP Operations Guide: Enable RBD monitoring](#)
- [MCP Operations Guide: Ceph dashboards](#)

Addressed issues

The MCP 2019.2.10 update contains fixes for several MCP components.

DriveTrain

- [35233] Fixed the SaltStack authentication bypass and directory traversal vulnerabilities. For details, see [CVE-2020-11651](#) and [CVE-2020-11652](#).
- [34662] Fixed the issue affecting the Salt Master node upgrade with `maas_enabled: false`.
- [16569] Fixed the issue causing inability to create flavors with `nova.client` if the OpenStack controller nodes had no access to the proxy network.

- [35257] Fixed the issue with the Nova and Glance Salt formulas attempting to use a public endpoint unavailable from the OpenStack controller nodes.
- [35205] Fixed the issue causing the Deploy - OpenStack Jenkins pipeline job to operate slowly.
- [34962] Fixed the issue with the test=True option being ignored when applying the neutron.client Salt state.
- [35388] Added the missing OpenSSH client example pillar for the .ssh/config configuration missing in the OpenSSH Salt formula.
- [35006] Fixed multiple issues with MAAS machine processing.

OpenStack

- [34900][Pike, Queens] Fixed the issue causing an increase of memory consumption by the neutron-dhcp-agent and memcached processes.
- [35325][Queens] Fixed the issue with snapshots creation getting stuck with the AttributeError: 'NoneType' object has no attribute 'get' exception in the scheduler logs if DriverFilter is enabled in cinder.conf.
- [35127][Pike, Queens] Fixed the issue with the Unable to get Swift service info error message appearing on the Containers page of the Horizon web UI after upgrade of Swift.
- [35252][Queens] Fixed the [community issue](#) causing Horizon to slow down in case of a large number of security groups.
- [35094][Queens] Fixed the issue with the hypervisor host name being exposed only to administrative users of the Horizon web UI.
- [35226][Pike, Queens] Fixed the issue causing failure to update a Heat stack.
- [35349][Pike, Queens] Fixed the issue with instance resize getting stuck in the post-migrating state.
- [35206][Pike, Queens] Fixed the issue occurring in case of port binding failures during instance move operations and causing inability to recover an instance or inability to restart the nova-compute service. Now, binding failures do not affect instance move operations.
- [35308][Pike, Queens] Parameterized the enable_stack_abandon and enable_stack_adapt settings in the Heat Salt formula to allow enabling the stack abandon and stack adopt operations in Heat. Set to False by default.
- [35310][Pike, Queens] Parameterized the extra_event_sources_list and extra_event_sinks_list settings in the Ceilometer Salt formula to allow extending event_sources_list and event_meter_list through the cluster model.
- [35146][Pike, Queens] Fixed the issue with novav21.aggregate_present state ignoring the newly created aggregates and causing the aggregates update failure.
- [35136][Queens] Fixed the issue with random Unexpected API error API error messages, caused by pymysql failures, appearing in the Nova logs.
- [35199][Pike] Updated Manila packages to fix [CVE-2020-9543](#). For details, see [OSSA-2020-002](#).

OpenContrail

- [34442] Fixed the issue with incorrect port ID and subnet ID paths in the Load Balancers tab of the Horizon web UI when using the Neutron LBaaS plugin. The issue affected the OpenStack Queens environments with OpenContrail 4.1.

StackLight

- [35421] Fixed the issue with StackLight sending a large number of duplicated alerts to Salesforce due to false-resolved notifications on the Prometheus side.
 - [35235] Fixed the expression and summary mismatch in the SystemMemoryFullMajor and SystemMemoryFullWarning alerts.
 - [34980] Fixed the issue with parsing of multiline auditd logs in systemd inputs.
 - [34611] Fixed handling of Neutron metrics when using the LinuxBridge networking plugin. Renamed the Neutron Grafana dashboard OpenvSwitch panels to L2 and the Neutron OpenvSwitch Agent panel to Neutron L2 Agent.
 - [35339] Fixed the issue causing the following Salesforce-related services being unavailable due to inability to authenticate to Salesforce:
 - Salesforce notifier for both encrypted and non-encrypted pillar
 - Salesforce reporter (Gainsight) for an encrypted pillar
 - [35346] Fixed the issue with the CVP - StackLight tests Jenkins pipeline job failing when running the test_nova_telegraf_metrics test. The issue occurred due to the max_limit setting, specified in nova.conf, restricting the number of retrieved servers from Nova. Now, this setting is ignored.
 - [35343] Fixed the issue with the CVP - StackLight tests Jenkins pipeline job failing with the TimeoutError: Incorrect image count in metric error message when running the test_glance_metrics test.
 - [35204] Parameterized the --web.cors.origin flag to allow configuring a CORS origin regex for Prometheus.
 - [35022] To avoid misinterpretation, the Telegraf metrics gathering alert was split into two separate alerts:
 - TelegrafGatherErrors - a node-based Fluentd alert
 - TelegrafRemoteGatherErrors - a container-based Fluentd alert, centralized through Docker Swarm
- For details, see [MCP Operations Guide: Telegraf](#).
- [34821] Increased the prometheus-es-exporter per-aggregate result size to avoid situations when some logs are missing in Elasticsearch. Added the ElasticsearchExporterNoDailyLogs alert that raises when no new published logs from a given node are detected by the Elasticsearch exporter.

Ceph

- [35178] Fixed the issue with an associated block_db partition being not removed from the block.db device during the Ceph OSD disk replacement. Added the capability to clean data partitions when running the Ceph - remove node and Ceph - remove OSD Jenkins pipeline jobs.
- [29831] Added the missing capability to apply highstate on nodes when running the Ceph - upgrade and Update Ceph packages Jenkins pipeline jobs.
- [35170] Fixed exception handling by adding the checks of the host parameter to the Ceph - add node, Ceph - remove node, and Ceph - remove OSD Jenkins pipeline jobs.
- [35406] Fixed the issue with the ceph state failing to set up Ceph keyrings on a newly deployed OpenStack compute node.
- [35124] To avoid RADOS Gateway VIP availability-related issues, added the RadosGWOutage and RadosGWDown alerts that raise if a RADOS Gateway endpoint is unreachable. For details, see [MCP Operations Guide: Ceph alerts](#).
- [35111] Refactored and adjusted the Ceph Grafana dashboards.
- [35203] Fixed the issue with the Ceph - add node Jenkins pipeline job failing with the Salt state on node mon03.env.local failed exception.

Known issues

For MCP known issues applicable to MCP 2019.2.10, see Known issues and corresponding sections in the previous maintenance updates.

Updated MCP components

The MCP 2019.2.10 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.9 update. All 2019.2.10 packages are available at <http://mirror.mirantis.com/update/2019.2.10/>.

Note

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

Updated major versions of the MCP components

Component	Application/service	2019.2.9	2019.2.10
OpenStack	RabbitMQ	3.6.15	3.8.2
Distributed storage	Ceph Nautilus	n/a	14.2.6

Updated minor versions of the MCP components

Component	Application/service	2019.2.9	2019.2.10
-----------	---------------------	----------	-----------

OpenStack Pike	erlang	1:20.2.2+dfsg-1.1~u16.04+mcp1	1:22.1.8+dfsg-1.1~u16.04+mcp1
	heat	1:9.0.7-2~u16.04+mcp91	1:9.0.7-2~u16.04+mcp100
	horizon	3:12.0.4-5~u16.04+mcp83	3:12.0.4-5~u16.04+mcp85
	keystone	2:12.0.3-5~u16.04+mcp26	2:12.0.3-5~u16.04+mcp29
	manila	1:5.1.0-2~u16.04+mcp38	1:5.1.0-2~u16.04+mcp42
	neutron	2:11.0.8-5~u16.04+mcp240	2:11.0.8-5~u16.04+mcp249
	nova	2:16.1.8-6~u16.04+mcp234	2:16.1.8-6~u16.04+mcp240
	python-keystoneauth1	3.1.1-1~u16.04+mcp6	3.1.1-1~u16.04+mcp8
	python-openstackclient	3.12.2-1~u16.04+mcp18	3.12.2-1~u16.04+mcp19
	python-oslo.messaging	5.30.8-1~u16.04+mcp18	5.30.8-1~u16.04+mcp19
	python-swiftclient	1:3.4.1-1~u16.04+mcp4	1:3.4.1-1~u16.04+mcp5
	rabbitmq-server	3.6.15-3~u16.04+mcp2	3.8.2-1~u16.04+mcp2
OpenStack Queens	ceilometer	1:10.0.1-3~u16.04+mcp36	1:10.0.1-3~u16.04+mcp40
	cinder	2:12.0.10-3~u16.04+mcp116	2:12.0.10-3~u16.04+mcp138
	designate	1:6.0.1-1.1~u16.04+mcp25	1:6.0.1-1.1~u16.04+mcp27
	erlang	1:20.2.2+dfsg-1.1~u16.04+mcp1	1:22.1.8+dfsg-1.1~u16.04+mcp1
	heat	1:10.0.3-1.1~u16.04+mcp109	1:10.0.3-1.1~u16.04+mcp113
	horizon	3:13.0.3-10~u16.04+mcp90	3:13.0.3-10~u16.04+mcp99
	horizon-contrail-panels	2:0.1.2-1~u16.04+mcp6	2:0.1.2-1~u16.04+mcp14

	ironic	1:10.1.10-1.1~u16.04+mcp57	1:10.1.10-1.1~u16.04+mcp68
	keystone	2:13.0.4-4~u16.04+mcp33	2:13.0.4-4~u16.04+mcp40
	kombu	4.1.0-2~u16.04+mcp2	4.1.0-3~u16.04+mcp2
	manila	1:6.3.2-3~u16.04+mcp52	1:6.3.2-3~u16.04+mcp85
	networking-ovn	4.0.4-1.0~u16.04+mcp68	4.0.4-1.0~u16.04+mcp97
	neutron	2:12.1.1-8~u16.04+mcp243	2:12.1.1-8~u16.04+mcp311
	nova	2:17.0.13-9~u16.04+mcp224	2:17.0.13-9~u16.04+mcp253
	octavia	2.1.2-9~u16.04+mcp116	2.1.2-9~u16.04+mcp125
	python-amqp	2.2.1-1~exp1~u16.04+mcp4	2.3.2-1~exp1~u16.04+mcp4
	python-castellan	0.17.0-2.0~u16.04+mcp17	0.17.0-2.0~u16.04+mcp18
	python-keystonemiddleware	4.22.0-1.0~u16.04+mcp9	4.22.0-1.0~u16.04+mcp10
	python-os-brick	2.3.9-1.0~u16.04+mcp17	2.3.9-1.0~u16.04+mcp19
	python-oslo.utils	3.35.1-1.0~u16.04+mcp5	3.35.1-1.0~u16.04+mcp8
	python-ovsdbapp	0.10.5-1.0~u16.04+mcp8	0.10.5-1.0~u16.04+mcp17
	python-pymysql	0.8.0-1~u16.04+mcp2	0.8.0-3~u16.04+mcp4
	python-swiftclient	1:3.5.0-2~u16.04+mcp11	1:3.5.1-2~u16.04+mcp6
	rabbitmq-server	3.6.15-3~u16.04+mcp2	3.8.2-1~u16.04+mcp2
	tempest	1:18.0.0-1~u16.04+mcp40	1:18.0.0-1~u16.04+mcp42
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20200423160025-0	4.1~20200701204814-0

	contrail	4.1~20200423160025-0	4.1~20200701204814-0
	contrail-heat	4.1~20200423160025-0	4.1~20200701204814-0
	contrail-vrouter-dpdk	4.1~20200423160025	4.1~20200701204814
	contrail-web-controller	4.1~20200423160025-0	4.1~20200701204814-0
	contrail-web-core	4.1~20200423160025-0	4.1~20200701204814-0
	neutron-plugin-contrail	4.1~20200423160025-0	4.1~20200701204814-0
Salt formulas	salt-formula-auditd	0.1+202001141131.421dd28~xenial1	0.1+202006241039.8e4611a~xenial1
	salt-formula-ceilometer	2016.12.1+202001311412.6837bde~xenial1	2016.12.1+202006160859.d73d127~xenial1
	salt-formula-ceph	0.1+202004101023.8b98fd5~xenial1	0.1+202007090952.f4c8643~xenial1
	salt-formula-elasticsearch	0.2+201911071625.289efb4~xenial1	0.2+202005271243.5aab3fc~xenial1
	salt-formula-fluentd	0.1+201911071625.b0428ad~xenial1	0.1+202006030852.cbfa1b5~xenial1
	salt-formula-glance	2016.12.1+202003180711.bac0c36~xenial1	2016.12.1+202006220842.3ca281d~xenial1
	salt-formula-heat	2016.12.1+202003311335.1661fa8~xenial1	2016.12.1+202006010900.7553ea3~xenial1
	salt-formula-linux	2017.4.1+202003311002.527c778~xenial1	2017.4.1+202006212000.a89140d~xenial1
	salt-formula-neutron	2016.12.1+202004221654.71c9950~xenial1	2016.12.1+202006261028.cb0d8fd~xenial1
	salt-formula-nova	2016.12.1+202004011330.747e873~xenial1	2016.12.1+202006221622.5bbfef3~xenial1
	salt-formula-opencontrail	0.2+202004221323.b7e6e8d~xenial1	0.2+202005250946.18a1ee6~xenial1

	salt-formula-openssh	0.2+202003170830.00f178a~xenial1	0.2+202005250827.13cc6f8~xenial1
	salt-formula-oslo-templates	2018.1+202004011100.501debf~xenial1	2018.1+202006231140.b3839c0~xenial1
	salt-formula-prometheus	0.1+202004071634.98108a9~xenial1	0.1+202006251539.e3870e0~xenial1
	salt-formula-rabbitmq	0.2+201911111218.406954d~xenial1	0.2+202006030849.6079bf0~xenial1
	salt-formula-runttest	0.1+201911251542.a7fd395~xenial1	0.1+202005190810.27eee86~xenial1
	salt-formula-telegraf	0.1+202004141310.3afbecf~xenial1	0.1+202005201636.b920a52~xenial1
Extra packages	prometheus-relay	0.3-1~u16.04+mcp5	0.3-1~u16.04+mcp8
	libvirt-exporter	0.1-1~u16.04+mcp6	0.1-1~u16.04+mcp8
	telegraf	1:1.9.1-3~u16.04+mcp57	1:1.9.1-3~u16.04+mcp59

Release artifacts

This section lists the artifacts of the MCP 2019.2.10 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.10/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.10/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.10/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.10/ceph-luminous/xenial xenial main deb http://mirror.mirantis.com/update/2019.2.10/ceph-nautilus/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.10/opencontrail-4.1/xenial xenial main
	Salt formulas packages ³³	http://mirror.mirantis.com/update/2019.2.10/salt-formulas/xenial xenial main

QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.10.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.10.qcow2
	VCP Ubuntu 16.04 image ³³	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.10/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.10/elastics-earch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.10/elastics-earch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.10/elastics-earch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.10/elastics-earch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³³
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.10/glusterfs-5/xenial xenial main ³³
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.10/maas/xenial xenial main ³³
	Percona	deb http://mirror.mirantis.com/update/2019.2.10/percona/xenial xenial main ³³

	SaltStack packages	<p>deb http://mirror.mirantis.com/update/2019.2.10/saltstack-2017.7/trusty trusty main</p> <p>deb http://mirror.mirantis.com/update/2019.2.10/saltstack-2017.7/xenial xenial main ³³</p> <p>deb http://mirror.mirantis.com/update/2019.2.10/salt-2017.7.8/ xenial xenial main ³³</p>
	Upstream Ubuntu system packages ³³	<p>deb https://mirror.mirantis.com/update/2019.2.10/ubuntu/xenial main restricted universe</p> <p>deb https://mirror.mirantis.com/update/2019.2.10/ubuntu/xenial-updates main restricted universe</p> <p>deb https://mirror.mirantis.com/update/2019.2.10/ubuntu/xenial-security main restricted universe</p>
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.10
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.10
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.10
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.10
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.6 ³³
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³³
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.9 ³³
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.9 ³³
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.9 ³³
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³³
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³³
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.9 ³³

	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ³³
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.10 ³³
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.10 ³³
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ³³
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.9 ³³
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.9 ³³
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.10 ³³
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/openldap:1.2.2 ³³
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.9 ³³
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³³
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.10 ³³
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.10 ³³
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6 ³³
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ³³
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ³³
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³³
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.10 ³³
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ³³

33(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content.](#)
 11, 12, 13, 14,
 15, 16, 17, 18,
 19, 20, 21, 22,
 23, 24, 25, 26,
 27, 28, 29, 30,
 31, 32, 33, 34,
 35)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.9 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.9, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages.
3 . 1	Galera cluster	Update the Galera cluster as described in MCP Operations Guide: Update Galera.
3 . 2	RabbitMQ	Update the RabbitMQ component to version 3.8.2 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 as described in MCP Operations Guide: Update StackLight LMA.

6	Ceph	<ol style="list-style-type: none"> 1. Restrict the RADOS Gateway capabilities. 2. Optional. Recommended. Upgrade Ceph from Luminous to Nautilus: <ol style="list-style-type: none"> 1. Enable the ceph-volume tool. 2. Upgrade Ceph from Luminous to Nautilus. 3. Optional. Enable RBD monitoring.
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

2019.2.9

The MCP 2019.2.9 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, Ceph, and StackLight MCP components.

The MCP 2019.2.9 update is available starting from April 30, 2020.

Enhancements

In the MCP 2019.2.9 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.9 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- System packages and applications update

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

System packages and applications update

Added the capability to update the installed applications and system packages, including kernel, when updating StackLight LMA to versions starting from 2019.2.9. Added the OS_DIST_UPGRADE and OS_UPGRADE parameters to the Deploy - upgrade StackLight Jenkins pipeline job.

OpenStack

In the MCP 2019.2.9 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Cross-AZ high availability for Neutron agents

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

Cross-AZ high availability for Neutron agents

Added support for HA with availability zones for Neutron to provide an extra layer of protection by segmenting the Neutron service deployment in isolated failure domains. By deploying HA nodes across different availability zones, the network services remain available in case of zone-wide failures affecting the deployment. If required, you can manually enable Cross-AZ high availability for DHCP and L3 routers.

Learn more

- [MCP Operations Guide: Cross-AZ high availability for Neutron agents](#)
- [OpenStack documentation: Availability zones](#)

StackLight

In the MCP 2019.2.9 maintenance update, Mirantis introduces the following enhancements for StackLight:

- Alertmanager integrations
- Alerts enhancements
- OpenStack metrics enhancements

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

Alertmanager integrations

Enhanced StackLight by adding the capability to enable integration with all notifications receivers supported by Alertmanager, such as PagerDuty, OpsGenie, and others. For a list of supported receivers, see [Prometheus Alertmanager documentation: Receiver](#). Also, added the capability to configure notifications subroutes.

The enhancement is backward compatible with previous MCP releases and does not affect any of the already configured Alertmanager receivers and routes.

Learn more

- [MCP Operations Guide: Configure Alertmanager integrations](#)
- [MCP Operations Guide: Configure notifications subroutes](#)

Alerts enhancements

- Enhanced the Nova alerts by adding the NovaComputeSystemLoadTooHighWarning and NovaComputeSystemLoadTooHighCritical alerts to separate the Nova-related alerts from the system alerts.
- Reconsidered the raise conditions for the DockerService `{{ camel_case_name }}` ReplicasDownMinor, DockerService `{{ camel_case_name }}` ReplicasDownMajor, and DockerService `{{ camel_case_name }}` Outage alerts.
- Removed the inefficient SystemSMARTDisk* alerts.
- Enhanced StackLight LMA to monitor the Reclass model and raise alerts in case of uncommitted changes. The feature is intended for the deployments that have the Reclass model storage set to local.

To verify that the Reclass model storage is local:

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

```
salt-call pillar.get reclass:storage:data_source:engine
```

Example of a positive system response:

```
local:  
  local
```

Learn more

- [MCP Operations Guide: Nova alerts](#)
- [MCP Operations Guide: Reclass alerts](#)

OpenStack metrics enhancements

Implemented the metrics for OpenStack Block Storage quota sets, OpenStack Compute quota sets, as well as OpenStack floating IPs metrics and OpenStack subnet allocation pools metric. To view the metrics, use the Prometheus web UI.

Addressed issues

The MCP 2019.2.9 update contains fixes for several MCP components.

DriveTrain

Issues resolutions applied automatically

- [34940] Fixed the issue with system packages upgrade causing the maas-dhcpd service being non-operational, leading to inability to perform PXE boot.
- [34798] Fixed the issue with DriveTrain update failing with the Error with request: HTTP Error 504: Gateway Time-out error message.
- [34615] Fixed the issue causing the salt-call state.highstate test=true Salt state to update the OpenStack endpoints instead of showing the intended changes.
- [34468] Fixed the issue with several Jenkins pipeline jobs occasionally failing with timeout error when synchronizing Salt modules or refreshing Salt pillars.
- [34861] Fixed the issue with the gnocchi.server Salt state failing to apply changes to policy.json.
- [34848] Fixed the issue with Jenkins slaves being unable to connect to Jenkins master during the update of MCP versions prior to 2019.2.4.
- [34973] Fixed the issue with inability to set the Glance disk and container formats through the Glance Salt formula.
- [34958] Fixed the issue with known_hosts autopopulation getting stuck for more than 30 minutes in case one or more servers are down. Added the capability to modify known_hosts_autopopulation through the OpenSSH Salt formula.
- [34296] Fixed the issue with the CVP - Sanity checks Jenkins pipeline missing support for secured repositories.
- [34651] Updated jenkins-master to version 2.204.3 to obtain the latest security fixes.

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.

- [34894] Apache service failure to start on proxy nodes after reboot
- [34406] Sphinx UI accessibility without authorization
- [28442] Wrong default value for umask causing an exception

[34894] Apache service failure to start on proxy nodes after reboot

Fixed the issue with the apache2 service failing to start after rebooting of any proxy node. The issue occurred due to Apache requiring the certificates placed on the GlusterFS volume, which might not have been mounted before the apache2 service start. To apply the issue resolution, set the dependency between the GlusterFS volume mount and the apache2 service explicitly as described below.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. In `classes/cluster/<cluster_name>/openstack/proxy.yml`, add the following pillar:

```
parameters:
...
apache:
  server:
    wait_for_service:
      - srv-salt-pki.mount
...
```

3. Apply the changes to Apache on the proxy nodes:

```
salt 'prx*' saltutil.refresh_pillar
salt 'prx*' state.apply apache.server
```

[34406] Sphinx UI accessibility without authorization

Fixed the issue with the Sphinx providing Reclaim variables without authorization. The issue occurred due to NGINX being configured without a basic authorization for `reclaim_doc`.

To apply the issue resolution:

1. Log in to the Salt Master node.
2. Generate a Sphinx UI password and add it to `classes/cluster/<cluster_name>/infra/secrets.yml` using the following parameter as described in [MCP Operations Guide: Manage secrets in the Reclaim model](#).

```
parameters:
  _param:
...
  sphinx_proxy_password_generated: <generated_password>
...
```

3. Apply the changes to NGINX and Sphinx:

```
salt -C '@sphinx:server and @nginx:server' saltutil.refresh_pillar
salt -C '@sphinx:server and @nginx:server' state.apply nginx
```

[28442] Wrong default value for umask causing an exception

Fixed the issue with a wrong default value set for umask, which caused the Cannot access storage file: Permission denied exception when running the salt.control state if umask was set to 027.

To apply the issue resolution:

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

```
salt -C '@salt:control' state.apply salt.control
```

OpenStack

- [34884][Queens] Fixed the issue with the SolidFire Cinder volume driver inability to connect to the SolidFire storage.
- [35100][Pike] Fixed the [community issue](#) with incorrect IPv6 lease entries causing the failed to parse lease database, invalid line error when initializing dnsmasq.
- [35035][Pike, Queens] Fixed the issue with the heat-engine service connection timeout when listing all existing security groups during an OpenStack port creation. Now, the security groups are filtered by project ID in list_security_groups.
- [34824][Pike] Fixed the issue with the OpenDaylight password being exposed in the Ceilometer log files.
- [34870][Pike] Fixed the issue with the designate.server Salt state failing to apply changes to policy.json.
- [34059][Queens] Fixed the issue that caused modifying a project through the Horizon web UI to fail with the Quota value(s) cannot be less than the current usage value(s): 2 Instances used. error message. The issue affected deployments with OpenContrail.
- [34843][Queens] Fixed the issue with the Neutron Salt formula being unable to manage the Nova metadata protocol for Neutron.
- [34790][Pike, Queens] Fixed the issue with the novav21 client state removing hosts from aggregates if the hosts were defined within the OpenStack compute node definitions and the aggregates were ensured through a pillar structure on the OpenStack controller node.
- [34111][Pike, Queens] Fixed the issue with inability to use novav21 to set up keypairs and aggregates in nova.client.

- [34616][Pike, Queens] Updated Django to version 1.11.22 to obtain the latest security fixes.

OpenContrail

- [35156] Fixed the issue with the OpenContrail schema-transformer service restart causing loss of SNAT connectivity for the instances without a floating IP.

StackLight

- [34885] Fixed the issue with several Nova dashboards displaying empty panels.
- [32579] Fixed the issue causing several Grafana dashboards with a large number of queries to occasionally display an error and no data after refreshing the dashboard.
- [34663] Fixed the issue with the CinderApiDown and CinderApiOutage alerts randomly raising if Keystone is set up with an additional domain.
- [34715] Fixed the issue with OVS alerts raising if Neutron Open vSwitch is not deployed.
- [34929] Adjusted StackLight LMA to monitor only the pillar-defined interfaces to avoid issues with an excessive amount of useless metrics.
- [34686] Fixed the issue with the Heat Grafana dashboard displaying no data in the Throughput and Latency graphs of the API performance panel.
- [34923] Fix the issue with several Elasticsearch alerts being false-positively generated during the update of StackLight LMA using the Deploy - upgrade StackLight Jenkins pipeline job.

Ceph

Issues resolutions applied automatically

- [32112] Fixed the issue with inability to update and manage Ceph client keyrings.
- [34896] Fixed the issue with the Ceph - add node Jenkins pipeline job failing to add a new Ceph node.
- [34859] Fixed the issue with the Ceph - add node Jenkins pipeline job failing to add the new Ceph OSD node to StackLight.

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.

- [35101] Swift authentication failure

[35101] Swift authentication failure

Fixed the issue causing inability to authenticate to Swift due to a wrong DNS name specified in RADOS Gateway.

To apply the issue resolution:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In cluster/ceph/rwg.yml, specify the following pillar:

```
parameters:
  ceph:
    radosgw:
      hostname: ${_param:ceph_rgw_hostname}.${_param:cluster_domain}
```

3. Log in to the Salt Master node.
4. Apply the RADOS Gateway configuration changes:

```
salt -l 'ceph:radosgw' state.apply ceph.common
```

Known issues

This section contains the description of the MCP 2019.2.9 known issues and workarounds. For other MCP known issues also applicable to MCP 2019.2.9, see Known issues and corresponding sections in the previous maintenance updates.

- [35146] [Queens, Pike] The novav21 state fails to update aggregates
 - [35330] Salesforce-related services unavailability
-

[35146] [Queens, Pike] The novav21 state fails to update aggregates

Fixed in 2019.2.10

While creating an aggregate, the novav21.aggregate_present state outputs IndexError: tuple index out of range. Although an aggregate is created, it is ignored by the Nova state and is never updated.

Identify whether your deployment is affected by the issue:

- New deployments without aggregates are not affected.
- New deployments with defined aggregates are affected and fail to create aggregates. No workaround is currently available for this use case.

- Existing deployments with aggregates fail to update aggregates. The workaround is to create and update aggregates manually using Nova CLI. For details, see [OpenStack documentation](#).

[35330] Salesforce-related services unavailability

Fixed in 2019.2.10

The following Salesforce-related services may be unavailable due to inability to authenticate to Salesforce:

- Salesforce notifier for both encrypted and non-encrypted pillar
- Salesforce reporter (Gainsight) for an encrypted pillar

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In `classes/cluster/<cluster_name>/stacklight/client.yml`, add the following pillar to the parameters section:

```
parameters:
  docker:
    client:
      stack:
        monitoring:
          service:
            sf_notifier:
              ~environment:
                SF_NOTIFIER_WORKERS: "${_param:sf_notifier_workers}"
                SF_NOTIFIER_BUFFER_SIZE: "${_param:sf_notifier_buffer_size}"
                SF_NOTIFIER_APP_PORT: "${prometheus:sf_notifier:uwsgi:bind_port}"
                SF_NOTIFIER_ALERT_ID_HASH_FUNC: "${_param:sf_notifier_alert_id_hash_func}"
                SFDC_AUTH_URL: "${_param:sf_notifier_sf_dc_auth_url}"
                SFDC_USERNAME: "${_param:sf_notifier_sf_dc_username}"
                SFDC_PASSWORD: "${_param:sf_notifier_sf_dc_password}"
                SFDC_ORGANIZATION_ID: "${_param:sf_notifier_sf_dc_organization_id}"
                SFDC_ENVIRONMENT_ID: "${_param:sf_notifier_sf_dc_environment_id}"
                SFDC_SANDBOX_ENABLED: "${_param:sf_notifier_sf_dc_sandbox_enabled}"
            gainsight:
              ~environment:
                CLUSTER_ID: "${_param:gainsight_cluster_id}"
                PROMETHEUS_URL: "${_param:gainsight_prometheus_url}"
                CONFIG_PATH: "${_param:gainsight_config_path}"
                SFDC_AUTH_URL: "${_param:gainsight_sf_dc_auth_url}"
                SFDC_USERNAME: "${_param:gainsight_sf_dc_username}"
                SFDC_PASSWORD: "${_param:gainsight_sf_dc_password}"
                SFDC_ORGANIZATION_ID: "${_param:gainsight_sf_dc_organization_id}"
```

SFDC_ENVIRONMENT_ID: "\${_param:gainsight_sfdc_environment_id}"
SFDC_SANDBOX_ENABLED: "\${_param:gainsight_sfdc_sandbox_enabled}"

3. Log in to the Salt Master node.
4. Verify that the changes render properly:

```
salt 'mon*' state.sls docker.client test=True
```

5. Apply the changes:

```
salt 'mon*' state.sls docker.client
```

Updated MCP components

The MCP 2019.2.9 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.8 update. All 2019.2.9 packages are available at <http://mirror.mirantis.com/update/2019.2.9/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.8	2019.2.9
DriveTrain	jenkins-master	2.150.3	2.204.3
OpenStack Pike	ceilometer	1:9.0.7-3~u16.04+mcp30	1:9.0.7-3~u16.04+mcp31
	designate	1:5.0.3-3~u16.04+mcp16	1:5.0.3-3~u16.04+mcp17
	heat	1:9.0.7-2~u16.04+mcp90	1:9.0.7-2~u16.04+mcp91
	neutron	2:11.0.8-5~u16.04+mcp234	2:11.0.8-5~u16.04+mcp240
	nova	2:16.1.8-6~u16.04+mcp212	2:16.1.8-6~u16.04+mcp234
	python-django	1:1.11.16-1~u16.04+mcp1	1:1.11.22-1~u16.04+mcp1
	python-keystonemiddleware	4.17.1-1~u16.04+mcp5	4.17.1-1~u16.04+mcp9

	python-oslo.db	4.25.2-4~u16.04+mcp11	4.25.2-4~u16.04+mcp12
	python-pyldap	2.4.25.1-2~u16.04+mcp2	2.4.37-2~u16.04+mcp1
OpenStack Queens	ceilometer	1:10.0.1-3~u16.04+mcp33	1:10.0.1-3~u16.04+mcp36
	cinder	2:12.0.10-3~u16.04+mcp101	2:12.0.10-3~u16.04+mcp116
	heat	1:10.0.3-1.1~u16.04+mcp100	1:10.0.3-1.1~u16.04+mcp109
	horizon	3:13.0.3-10~u16.04+mcp86	3:13.0.3-10~u16.04+mcp90
	ironic	1:10.1.9-1.1~u16.04+mcp62	1:10.1.10-1.1~u16.04+mcp57
	keystone	2:13.0.4-4~u16.04+mcp31	2:13.0.4-4~u16.04+mcp33
	networking-ovn	4.0.4-1.0~u16.04+mcp56	4.0.4-1.0~u16.04+mcp68
	neutron	2:12.1.1-8~u16.04+mcp187	2:12.1.1-8~u16.04+mcp243
	nova	2:17.0.13-9~u16.04+mcp198	2:17.0.13-9~u16.04+mcp224
	octavia	2.1.2-9~u16.04+mcp103	2.1.2-9~u16.04+mcp116
	python-amqp	2.2.1-1~exp1~u16.04+mcp3	2.2.1-1~exp1~u16.04+mcp4
	python-cinderclient	1:3.5.0-1.0~u16.04+mcp12	1:3.5.0-1.0~u16.04+mcp15
	python-django	1:1.11.7-1~u16.04+mcp2	1:1.11.22-1~u16.04+mcp1
	python-octaviaclient	1.4.1-3~u16.04+mcp8	1.4.1-3~u16.04+mcp10
	python-openstackclient	3.14.3-1.0~u16.04+mcp25	3.14.3-1.0~u16.04+mcp26
	python-os-brick	2.3.9-1.0~u16.04+mcp12	2.3.9-1.0~u16.04+mcp17
	python-oslo.cache	1.28.1-1.0~u16.04+mcp7	1.28.1-1.0~u16.04+mcp9

	python-oslo.db	4.33.4-1.1~u16.04+mcp8	4.33.4-1.1~u16.04+mcp9
	python-ovsdbapp	0.10.4-1.0~u16.04+mcp6	0.10.5-1.0~u16.04+mcp8
	python-pyldap	2.4.25.1-2~u16.04+mcp2	2.4.37-2~u16.04+mcp1
	tempest	1:18.0.0-1~u16.04+mcp38	1:18.0.0-1~u16.04+mcp40
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20200207111248-0	4.1~20200423160025-0
	contrail	4.1~20200207111248-0	4.1~20200423160025-0
	contrail-heat	4.1~20200207111248-0	4.1~20200423160025-0
	contrail-vrouter-dpdk	4.1~20200207111248	4.1~20200423160025
	contrail-web-controller	4.1~20200207111248-0	4.1~20200423160025-0
	contrail-web-core	4.1~20200207111248-0	4.1~20200423160025-0
	neutron-plugin-contrail	4.1~20200207111248-0	4.1~20200423160025-0
Salt formulas	salt-formula-apache	0.2+201911081257.e5ed4b7~xenial1	0.2+202003191515.1f81458~xenial1
	salt-formula-ceph	0.1+202002191015.5192463~xenial1	0.1+202004101023.8b98fd5~xenial1
	salt-formula-cinder	2016.12.1+201911290903.79f1677~xenial1	2016.12.1+202003311421.96c2d46~xenial1
	salt-formula-docker	0.1+202001141155.2cf83fa~xenial1	0.1+202003261323.27a65be~xenial1
	salt-formula-glance	2016.12.1+202002041454.ae52437~xenial1	2016.12.1+202003180711.bac0c36~xenial1
	salt-formula-gnocchi	2018.1+201911290829.62b51f8~xenial1	2018.1+202003311438.e3d7c09~xenial1
	salt-formula-heat	2016.12.1+202002040951.2f9ba80~xenial1	2016.12.1+202003311335.1661fa8~xenial1

	salt-formula-horizon	2016.12.1+202002171547.74a60a7~xenial1	2016.12.1+202003161223.ecaab0b~xenial1
	salt-formula-ironic	0.1+201911210859.5750eb1~xenial1	0.1+202003311418.f43a70f~xenial1
	salt-formula-jenkins	2017.8+201908051430.bfcd953~xenial1	2017.8+202003311035.1a3adc4~xenial1
	salt-formula-keystone	2016.12.1+202002040951.94bca39~xenial1	2016.12.1+202003180714.918c4b3~xenial1
	salt-formula-linux	2017.4.1+202002130940.4bf99b7~xenial1	2017.4.1+202003311002.527c778~xenial1
	salt-formula-maas	0.0.1+202002111257.91177f5~xenial1	0.0.1+202003241701.55d9d76~xenial1
	salt-formula-neutron	2016.12.1+202002031330.ec9d35d~xenial1	2016.12.1+202004221654.71c9950~xenial1
	salt-formula-nova	2016.12.1+202002181501.a922543~xenial1	2016.12.1+202004011330.747e873~xenial1
	salt-formula-octavia	2017.6+202002030934.8b88460~xenial1	2017.6+202004170823.727a8d7~xenial1
	salt-formula-openssh	0.2+202001141132.715e44d~xenial1	0.2+202003170830.00f178a~xenial1
	salt-formula-oslo-templates	2018.1+202002040949.30119b6~xenial1	2018.1+202004011100.501debf~xenial1
	salt-formula-prometheus	0.1+201911221146.2020c62~xenial1	0.1+202004071634.98108a9~xenial1
	salt-formula-salt	0.4+201911071622.34d31ba~xenial1	0.4+202003301102.521d081~xenial1
	salt-formula-telegraf	0.1+202002251333.4e3edd1~xenial1	0.1+202004141310.3afbecf~xenial1
	salt-formula-xtrabackup	0.2+201911111253.665443e~xenial1	0.2+202003231338.2eeeb88~xenial1
Extra packages	prometheus-relay	0.3-1~u16.04+mcp2	0.3-1~u16.04+mcp5
	python-jenkins	n/a	1.7.0-1~16.04+mcp1

Release artifacts

This section lists the artifacts of the MCP 2019.2.9 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.9/openstack-pike/xenial/xenial/main deb https://mirror.mirantis.com/update/2019.2.9/openstack-queens/xenial/xenial/main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.9/extra/xenial/xenial/main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.9/ceph-luminous/xenial/xenial/main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.9/opencontrail-4.1/xenial/xenial/main
	Salt formulas packages ³⁴	http://mirror.mirantis.com/update/2019.2.9/salt-formulas/xenial/xenial/main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.9.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.9.qcow2
	VCP Ubuntu 16.04 image ³⁴	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial/squeeze/main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty/21x/main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial/21x/main

	Docker	deb http://mirror.mirantis.com/update/2019.2.9/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.9/elasticse-arch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.9/elasticse-arch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.9/elasticse-arch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.9/elasticse-arch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³⁴
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.9/glusterfs-5/xenial xenial main ³⁴
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.9/maas/xenial xenial main ³⁴
	Percona	deb http://mirror.mirantis.com/update/2019.2.9/percona/xenial xenial main ³⁴
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.9/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.9/saltstack-2017.7/xenial xenial main ³⁴
	Upstream Ubuntu system packages ³⁴	deb https://mirror.mirantis.com/update/2019.2.9/ubuntu/xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.9/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.9/ubuntu/xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.9
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.9
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.9
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.9

Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.6 ³⁴
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³⁴
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.9 ³⁴
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.9 ³⁴
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.9 ³⁴
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³⁴
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³⁴
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.9 ³⁴
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ³⁴
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.7 ³⁴
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.6 ³⁴
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ³⁴
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.9 ³⁴
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.9 ³⁴
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.6 ³⁴
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/openldap:1.2.2 ³⁴
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.9 ³⁴
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³⁴
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.6 ³⁴

	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.9 ³⁴
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6 ³⁴
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ³⁴
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ³⁴
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³⁴
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.9 ³⁴
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ³⁴

34(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.8 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.8, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
---	-----------	----------

1	DriveTrain	<ol style="list-style-type: none"> 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.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	<ol style="list-style-type: none"> 1. Update the OpenStack packages as described in MCP Operations Guide: Update OpenStack packages. 2. Optional. Enable Cross-AZ high availability for Neutron agents.
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	<ol style="list-style-type: none"> 1. Update StackLight LMA as described in MCP Operations Guide: Update StackLight LMA. 2. Optional. Configure Alertmanager integrations and Configure notifications subroutes.
6	Ceph	Perform the steps described in Issues resolutions requiring manual application.
7	Ubuntu Xenial packages	<p>Select from the following options:</p> <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

Known issues

2019.2.8

The MCP 2019.2.8 update introduces enhancements and bug fixes for the DriveTrain, OpenStack, OpenContrail, Ceph, and StackLight MCP components.

The MCP 2019.2.8 update is available starting from March 5, 2020.

Enhancements

In the MCP 2019.2.8 update, Mirantis introduces the following enhancements of the MCP 2019.2.0 release version.

DriveTrain

In the MCP 2019.2.8 maintenance update, Mirantis introduces the following enhancements for DriveTrain:

- Update process improvement
- System packages and applications update
- System packages upgrade before deploying an MCP environment
- Automatically apply the cluster model workarounds for DriveTrain

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Update process improvement

Introduced full support for the capability to apply the maintenance update of a particular 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](#).

System packages and applications update

Added the capability to update the installed applications and system packages, including kernel, when updating DriveTrain to a minor version starting from the maintenance update 2019.2.2 to versions starting from 2019.2.8. Added the `OS_DIST_UPGRADE` and `OS_UPGRADE` parameters to the Deploy - upgrade MCP DriveTrain Jenkins pipeline job.

Learn more

[MCP Operations Guide: Update DriveTrain](#)

System packages upgrade before deploying an MCP environment

Implemented the `DIST_UPGRADE_NODES` parameter to the Deploy - OpenStack Jenkins pipeline job to enable or disable `apt-get dist-upgrade` on all cluster nodes before deploying a new MCP environment. Disabled by default.

Learn more

[MCP Deployment Guide: Deploy an OpenStack environment](#)

Automatically apply the cluster model workarounds for DriveTrain

Implemented the `APPLY_MODEL_WORKAROUNDS` parameter to the Deploy - upgrade MCP DriveTrain Jenkins pipeline job to enable or disable automatic application of the Reclass cluster model workarounds when updating DriveTrain to 2019.2.8. Enabled by default.

Learn more

[MCP Operations Guide: Update DriveTrain](#)

OpenStack

In the MCP 2019.2.8 maintenance update, Mirantis introduces the following enhancements for OpenStack:

- Octavia enhancements

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

Octavia enhancements

Added the capability to enable amphora HA mode and define the size of the spare amphorae pool for the Octavia load balancer. You can enable the features when enabling Octavia on a new or existing OpenStack environment as described in [MCP Deployment Guide: Configure load balancing with OpenStack Octavia](#). For existing environments with Octavia already enabled, perform the steps below, as required:

To obtain the enhancements for the deployments with Octavia enabled:

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

2. In `cluster/<cluster_name>/openstack/init.yml`, set `octavia_loadbalancer_topology` to `ACTIVE_STANDBY` to use the amphora HA mode.
3. In `cluster/<cluster_name>/openstack/octavia_manager.yml`, specify the `spare_amphora_pool_size` parameter as required to use a spare amphorae pool for the Octavia load balancer:

```
octavia:  
  manager:  
    house_keeping:  
      spare_amphora_pool_size: 0
```

4. From the Salt Master node, apply the changes:

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

Learn more

- [MCP Deployment Guide: Enable Octavia on a new OpenStack environment](#)
- [MCP Deployment Guide: Enable Octavia on an existing OpenStack environment](#)

StackLight

In the MCP 2019.2.8 maintenance update, Mirantis introduces the following enhancements for StackLight:

- OpenStack availability zones monitoring

To obtain the enhancements, follow the steps described in [Apply maintenance updates](#).

OpenStack availability zones monitoring

Enhanced StackLight to collect the OpenStack availability zones data and implemented the Nova - availability zones Grafana dashboard that visualizes the availability zones statistics.

Learn more

[MCP Operations Guide: OpenStack dashboards](#)

Addressed issues

The MCP 2019.2.8 update contains fixes for several MCP components.

DriveTrain

- [34739] Fixed the shell condition for the verification of a Docker certificate validity period to resolve the issue causing the apt01 node failing to start in case of an offline MCP deployment.
- [34417] Fixed the issue causing Salt Master with 10-14 GB of RAM being unable to apply Salt states on a large number of nodes. Now, batching is by default set to 2/3 of the available Salt Master worker threads.
- [34514] Fixed the issue with the Deploy - upgrade computes Jenkins pipeline job failing during the Upgrade OS stage.
- [34348] Fixed the issue with logrotate parameters missing in the HAProxy Salt formula.
- [34108] Fixed the issue with the Deploy - upgrade MCP Drivetrain Jenkins pipeline job failing due to missing Git authentication parameters.
- [34053] Fixed the issue with Horizon logging a user out with the Unauthorized error due to the Octavia default policy files missing on the ctl nodes. Added the capability to manage the Octavia policy through the Octavia Salt formula.
- [34754] Fixed the linux.system.auth module in the Linux Salt formula.
- [30646] Fixed the issue with the Deploy - upgrade Opencontrail to 4.x Jenkins pipeline job failing during the STAGE_CONTROLLERS_UPGRADE stage.
- [34461] Fixed the issue with the Deploy - upgrade control VMs Jenkins pipeline job failing for the gtw role if OS_DIST_UPGRADE is selected.
- [34385] Fixed the issue with the CVP - Performance tests Jenkins pipeline job failing with the Error: No such container: cvp exception.
- [34528] Fixed the issue with MySQL users being defined only for the db01 node.
- [34252] Fixed the issue with virtual nodes having an old kernel version and some packages being upgradable after deployment. The issue affected new MCP deployments only.
- [29403] Fixed the issue with the Nova Salt formula executing nova-manage without the --by-service argument when Ironic is enabled.
- [34729] Fixed the launch_instance_defaults option in the Horizon Salt formula.
- [34706] Fixed the following issues in the NGINX Salt formula:
 - Unhardcoded the ssl_stapling parameter.
 - Fixed the misconfiguration of the ssl_ciphers and ssl_protocols parameters.
- [34639] Fixed the following issues in the Nova Salt formula:
 - Unhardcoded the use_cow_images, force_raw_images, snapshot_image_format, and images_type Nova parameters.

- Fixed the issue in the Nova Salt formula that caused Nova to use a public endpoint to query the internal API from the OpenStack compute nodes. Added the capability to set the endpoint to public or internal. The default value is internal.

```
nova:  
  compute:  
    identity:  
      interface: 'public'
```

OpenStack

Issues resolutions applied automatically

- [34561] [Pike] Fixed the issue with a Heat stack creation failing with the following error message: Key manager error: You are not authorized to perform the requested action: Using trust-scoped token to create another token. Create a new trust-scoped token instead.
- [34542] [Pike] Fixed the [community issue](#) with Nova skipping the removal of a vhost user from libvirt.
- [34486] [Pike] Fixed the following issues with the glance-cache-manage client commands:
 - Failure to operate if a real IP address of the Glance API, where Apache is listening, is specified instead of the local host.
 - Ignoring the OS_CACERT variable.
- [34485] [Pike, Queens] Fixed the issue with a Heat stack deletion failing with the too many values to unpack error message if the ExtraRoute resource uses IPv6.
- [34479] [Pike] Fixed the Nova commands handling for the Nova API microversion 2.53 or greater.
- [34307] [Pike] Fixed the issue with the NUMA topology of a new flavor being not considered during the resize of an instance.
- [34462] [Queens] Fixed the issue with Horizon logging the user out with the 403 error message after an attempt to delete a public image created by an administrator.
- [34434] [Pike to Queens upgrade] Fixed the issue with the upgrade of OpenStack Pike to Queens failing when running the Deploy - upgrade control VMs Jenkins pipeline job for the mdb role.
- [33897] [Queens] Fixed the issue that caused listing of floating IPs to take a significant amount of time.
- [33865] [Pike, Queens] Fixed the [community issue](#) causing the DBDeadlock error when managing a Neutron port.
- [34250] [Pike] Fixed the issue with logs of the nova-conductor service containing a significant number of pymysql errors.

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.

- [33738] Failure of Ironic Tempest tests for port lists

[33738] Failure of Ironic Tempest tests for port lists

Pike, Queens

Fixed the issue with the `test_list_ports` and `test_list_ports_details` Tempest tests for Ironic failing due to mismatch of URLs in `validate_self_link`. The issue affected MCP deployments with the HTTPS protocol for OpenStack internal endpoints.

To apply the issue resolution:

1. On the cluster level of the ReClass model, open the `openstack/proxy.yml` file for editing.
2. Verify that the `nginx_proxy_headers` parameter is defined. For example:

```
parameters:
  _param:
    ...
  nginx_proxy_headers:
    X-Forwarded-For:
      enabled: true
      value: '$proxy_add_x_forwarded_for'
    X-Forwarded-Proto:
      enabled: true
      value: '$scheme'
    X-Forwarded-Port:
      enabled: true
      value: '$server_port'
    Host:
      enabled: true
```

3. Specify the NGINX proxy configuration for Ironic API:

```
parameters:
  _param:
    ...
```

```
nginx_proxy_openstack_api_ironic:  
  proxy_set_header: ${_param:nginx_proxy_headers}
```

4. Log in to the Salt Master node.
5. Apply the changes on the proxy nodes:

```
salt -C '@nginx:server and !@horizon:server' saltutil.refresh_pillar  
salt -C '@nginx:server and !@horizon:server' state.apply nginx.server
```

OpenContrail

- [34123] Fixed the issue with the contrail-svc-monitor service removing working service instances from vRouter agents.
- [34122] Fixed the issue with the contrail-svc-monitor service adding the default security group upon the start or initialization, which could cause downtime if the default security group was not applied on the instances.
- [33566] Fixed the issue with the OpenContrail web UI randomly crashing with the unknown exception error message.
- [26673] Fixed the issue that caused updating the name of a shared network in the Horizon web UI to fail with the Failed to update network <network_name> error message.

StackLight

- [34584] Fixed the issue with the incorrect definition of the CephOsdSpaceUsageMajor alert.
- [32082] Fixed the issue with the 502 Bad Gateway error occurring when opening a shortened URL with a Kibana query.
- [34330] Fixed the issue with the Top N * filters incorrectly filtering the data records in the Nova - instances, Nova - users, and Nova - tenants Grafana dashboards.
- [34319] Fixed the issue with the openstack_neutron_port_status metric providing an incorrect output.
- [34539] Fixed the issue with Telegraf incorrectly calculating the CPU load average if isolcpus is configured.
- [34261] Fixed the issue with the flapping SystemLoadTooHighWarning and SystemLoadTooHighCritical alerts by changing the average load frequency from 5 to 15 minutes. Additionally, changed the SystemLoadTooHighCritical alert severity from warning to critical.

Ceph

- [34191] Fixed the Ceph Manager update using the Update Ceph packages Jenkins pipeline job.
- [34415] Fixed the OSD devices detection in the Ceph Salt formula.

- [34217] Fixed the Ceph logs rotation.

Known issues

This section contains the description of the MCP 2019.2.8 known issue and its workaround. For other MCP known issues also applicable to MCP 2019.2.8, see Known issues and corresponding sections in the previous maintenance updates.

- [34894] Apache service fails to start after a prx node reboot

[34894] Apache service fails to start after a prx node reboot

Fixed in 2019.2.9

After rebooting a prx node, the Apache service on that node may not start with the SSLCertificateChainFile: '<file>' does not exist or is empty error message. The issue occurs because the apache2 service starts before running the srv-salt-pki GlusterFS mount. The workaround is to manually start the apache2 service on the affected node.

Updated MCP components

The MCP 2019.2.8 update includes the following changes in the minor versions of the MCP components compared to the MCP 2019.2.7 update. All 2019.2.8 packages are available at <http://mirror.mirantis.com/update/2019.2.8/>.

Note

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

Updated minor versions of the MCP components

Component	Application/service	2019.2.7	2019.2.8
Distributed storage	ceph	12.2.11-1	12.2.13-1
OpenStack Pike	cinder	2:11.2.2-3~u16.04+mcp138	2:11.2.2-3~u16.04+mcp139
	glance	2:15.0.2-2~u16.04+mcp16	2:15.0.2-2~u16.04+mcp17
	heat	1:9.0.7-2~u16.04+mcp88	1:9.0.7-2~u16.04+mcp90
	horizon	3:12.0.4-5~u16.04+mcp80	3:12.0.4-5~u16.04+mcp83

	horizon-contrail-panels	1:0.1.1-1~u16.04+mcp7	1:0.1.1-1~u16.04+mcp8
	ironic	1:9.1.6-2~u16.04+mcp54	1:9.1.6-2~u16.04+mcp56
	kombu	4.1.0-2~u16.04+mcp1	4.1.0-2~u16.04+mcp2
	neutron	2:11.0.8-5~u16.04+mcp228	2:11.0.8-5~u16.04+mcp234
	nova	2:16.1.8-6~u16.04+mcp169	2:16.1.8-6~u16.04+mcp212
	openvswitch	2.9.5-1~u16.04+mcp	2.9.5-2~u16.04+mcp
	python-keystoneclient	1:3.13.1-1~u16.04+mcp4	1:3.13.1-1~u16.04+mcp6
	python-openstackclient	3.12.2-1~u16.04+mcp13	3.12.2-1~u16.04+mcp18
OpenStack Queens	cinder	2:12.0.9-3~u16.04+mcp118	2:12.0.10-3~u16.04+mcp101
	designate-dashboard	6.0.1-1.0~u16.04+mcp2	6.0.1-1.0~u16.04+mcp4
	heat	1:10.0.3-1.1~u16.04+mcp93	1:10.0.3-1.1~u16.04+mcp100
	horizon	3:13.0.2-10~u16.04+mcp87	3:13.0.3-10~u16.04+mcp86
	horizon-contrail-panels	2:0.1.2-1~u16.04+mcp5	2:0.1.2-1~u16.04+mcp6
	kombu	4.1.0-2~u16.04+mcp1	4.1.0-2~u16.04+mcp2
	networking-ovn	4.0.3-1.0~u16.04+mcp78	4.0.4-1.0~u16.04+mcp56
	neutron	2:12.1.1-8~u16.04+mcp168	2:12.1.1-8~u16.04+mcp187
	nova	2:17.0.13-9~u16.04+mcp174	2:17.0.13-9~u16.04+mcp198
	octavia	2.1.2-9~u16.04+mcp92	2.1.2-9~u16.04+mcp103
	openvswitch	2.9.5-1~u16.04+mcp	2.9.5-2~u16.04+mcp
	python-cinderclient	1:3.5.0-1.0~u16.04+mcp10	1:3.5.0-1.0~u16.04+mcp12

	python-keystoneauth1	3.4.0-1.0~u16.04+mcp14	3.4.1-1.0~u16.04+mcp7
	python-keystoneclient	1:3.15.0-1.0~u16.04+mcp14	1:3.15.1-1.0~u16.04+mcp6
	python-keystonemiddleware	4.21.0-1.0~u16.04+mcp20	4.22.0-1.0~u16.04+mcp9
	python-openstackclient	3.14.3-1.0~u16.04+mcp24	3.14.3-1.0~u16.04+mcp25
	python-os-brick	2.3.8-1.0~u16.04+mcp10	2.3.9-1.0~u16.04+mcp12
	python-oslo.messaging	5.35.5-2~u16.04+mcp31	5.35.6-2~u16.04+mcp27
	tempest	1:18.0.0-1~u16.04+mcp26	1:18.0.0-1~u16.04+mcp38
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20191127132224-0	4.1~20200207111248-0
	contrail	4.1~20191127132224-0	4.1~20200207111248-0
	contrail-heat	4.1~20191127132224-0	4.1~20200207111248-0
	contrail-vrouter-dpdk	4.1~20191127132224	4.1~20200207111248
	contrail-web-controller	4.1~20191127132224-0	4.1~20200207111248-0
	contrail-web-core	4.1~20191127132224-0	4.1~20200207111248-0
	neutron-plugin-contrail	4.1~20191127132224-0	4.1~20200207111248-0
Salt formulas	salt-formula-aptly	2017.2+201911061606.6260086~xenial1	2017.2+202001141131.4f6a992~xenial1
	salt-formula-auditd	0.1+201911071035.4556d75~xenial1	0.1+202001141131.421dd28~xenial1
	salt-formula-backupninja	0.2+201911080916.73bfad2~xenial1	0.2+202001141131.6301114~xenial1
	salt-formula-barbican	2018.1+201912131604.f16494a~xenial1	2018.1+202002070852.ba74a99~xenial1
	salt-formula-ceilometer	2016.12.1+201911290902.564076f~xenial1	2016.12.1+202001311412.6837bde~xenial1

	salt-formula-ceph	0.1+201912051140.946ac89~xenial1	0.1+202002191015.5192463~xenial1
	salt-formula-cinder	2016.12.1+201911290903.79f1677~xenial1	2016.12.1+202002041307.7307f18~xenial1
	salt-formula-debmirror	2018.1+201911061607.e3cb60f~xenial1	2018.1+202001141154.c6d0304~xenial1
	salt-formula-designate	2016.12.1+201912060858.42c5fae~xenial1	2016.12.1+202002041545.d6c1c45~xenial1
	salt-formula-docker	0.1+201911061610.8370945~xenial1	0.1+202001141155.2cf83fa~xenial1
	salt-formula-gerrit	2017.2+201911141523.521de4f~xenial1	2017.2+202001141131.0f2cf58~xenial1
	salt-formula-glance	2016.12.1+201911290901.61c0802~xenial1	2016.12.1+202002041454.ae52437~xenial1
	salt-formula-glusterfs	2017.3+201907311451.40cec03~xenial1	2017.3+202001141131.db7ae3a~xenial1
	salt-formula-haproxy	0.2+201912031148.80b870a~xenial1	0.2+202001150929.6f4d961~xenial1
	salt-formula-heat	2016.12.1+201911290843.5c800f8~xenial1	2016.12.1+202002040951.2f9ba80~xenial1
	salt-formula-horizon	2016.12.1+201912050925.8870b1b~xenial1	2016.12.1+202002171547.74a60a7~xenial1
	salt-formula-keycloak	2018.1+201911070927.f6c671a~xenial1	2018.1+202001141132.eb59139~xenial1
	salt-formula-keystone	2016.12.1+201912041637.3041257~xenial1	2016.12.1+202002040951.94bca39~xenial1
	salt-formula-linux	2017.4.1+201912100905.cac8946~xenial1	2017.4.1+202002130940.4bf99b7~xenial1
	salt-formula-maas	0.0.1+201912021129.e3183ad~xenial1	0.0.1+202002111257.91177f5~xenial1
	salt-formula-manila	2017.6+201911290843.ffc3f87~xenial1	2017.6+202002031333.aa3c3ad~xenial1

	salt-formula-memcached	0.2+201911070933.73485d1~xenial1	0.2+202001141132.6a0e4f5~xenial1
	salt-formula-neutron	2016.12.1+201912040858.97bd9ba~xenial1	2016.12.1+202002031330.ec9d35d~xenial1
	salt-formula-nginx	0.2+201911121441.e5c8ed3~xenial1	0.2+202002071022.df5fd04~xenial1
	salt-formula-nova	2016.12.1+201912111257.8c124c3~xenial1	2016.12.1+202002181501.a922543~xenial1
	salt-formula-ntp	0.2+201911251436.9ee5a06~xenial1	0.2+202001141132.30ad994~xenial1
	salt-formula-octavia	2017.6+201912230912.0a99e82~xenial1	2017.6+202002030934.8b88460~xenial1
	salt-formula-opencontrail	0.2+201911290902.08c8848~xenial1	0.2+202001271044.a252779~xenial1
	salt-formula-openssh	0.2+201911071624.11eee6e~xenial1	0.2+202001141132.715e44d~xenial1
	salt-formula-oslo-templates	2018.1+201911181043.d24f42d~xenial1	2018.1+202002040949.30119b6~xenial1
	salt-formula-redis	0.2+201908021516.f5478ee~xenial1	0.2+202001271225.f0735e4~xenial1
	salt-formula-telegraf	0.1+201912040912.0b0bfae~xenial1	0.1+202002251333.4e3edd1~xenial1
	salt-formula-watchdog	2018.1+201911071035.24e5a4a~xenial1	2018.1+202001141132.60a5a9c~xenial1
Extra packages	telegraf	1:1.9.1-3~u16.04+mc52	1:1.9.1-3~u16.04+mc57

Release artifacts

This section lists the artifacts of the MCP 2019.2.8 maintenance update.

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.8/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.8/openstack-queens/xenial xenial main

	Extra packages	deb http://mirror.mirantis.com/update/2019.2.8/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.8/ceph-luminous/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.8/opencontrail-4.1/xenial xenial main
	Salt formulas packages ³⁵	http://mirror.mirantis.com/update/2019.2.8/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.8.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.8.qcow2
	VCP Ubuntu 16.04 image ³⁵	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.8/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.8/elasticsearch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.8/elasticsearch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.8/elasticsearch-arch curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.8/elasticsearch-arch curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³⁵

	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.8/glusterfs-5/xenial xenial main ³⁵
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.8/maas/xenial xenial main ³⁵
	Percona	deb http://mirror.mirantis.com/update/2019.2.8/percona/xenial xenial main ³⁵
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.8/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.8/saltstack-2017.7/xenial xenial main ³⁵
	Upstream Ubuntu system packages ³⁵	deb https://mirror.mirantis.com/update/2019.2.8/ubuntu/xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.8/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.8/ubuntu/xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.8
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.8
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.8
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.8
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.6 ³⁵
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³⁵
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.6 ³⁵
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.6 ³⁵
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.6 ³⁵
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³⁵

cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³⁵
gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.4 ³⁵
gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.6 ³⁵
gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.7 ³⁵
grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.6 ³⁵
heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.6 ³⁵
jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.8 ³⁵
jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.8 ³⁵
mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.6 ³⁵
openldap	docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/openldap:1.2.2 ³⁵
phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.5 ³⁵
postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³⁵
prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.6 ³⁵
prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.5 ³⁵
pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6 ³⁵
registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.6 ³⁵
remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.6 ³⁵
sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³⁵
telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.8 ³⁵

	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.6
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ³⁵

35(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34\)](#)

Apply maintenance updates

Caution!

If you are updating from MCP 2019.2.7 maintenance update, proceed with the steps below right away. If you are updating from MCP maintenance update prior to 2019.2.7, first apply all issues resolutions requiring manual application that follow the initial MCP maintenance update applied on your MCP cluster.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes.
3	OpenStack	<ol style="list-style-type: none"> 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. Optional. Obtain the Octavia improvements as described in Octavia enhancements.

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 but in the following stages: <ol style="list-style-type: none"> 1. Run the Deploy - upgrade StackLight Jenkins pipeline job only with the STAGE_UPGRADE_DOCKER_COMPONENTS option enabled. 2. Run the Deploy - upgrade StackLight Jenkins pipeline job with the STAGE_UPGRADE_ES_KIBANA and STAGE_UPGRADE_SYSTEM_PART options enabled.
6	Ceph	Update the Ceph Luminous packages as described in MCP Operations Guide: Update Ceph packages .
7	Ubuntu Xenial packages	Select from the following options: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso
Known issues

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.

Learn more

[MCP Deployment Guide: Manage kernel](#)

Update process improvement

TECHNICAL PREVIEW Fully available in 2019.2.8

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
- Prometheus 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:

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

- [33378][Queens] Fixed the issue with the inability to configure caching of the Cinder SolidFire backend 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:

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

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

```
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 backend.
- [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:

```
system.haproxy.proxy.listen.cid.aptly
```

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

```
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
 - [34790][Pike, Queens] The `novav21` client state removes hosts from aggregates
 - [35156] Loss of SNAT connectivity
-

[34434] Pike to Queens upgrade failure

Fixed in 2019.2.8

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.

[34790][Pike, Queens] The novav21 client state removes hosts from aggregates

Fixed in 2019.2.9

The novav21 client state removes hosts from aggregates if the hosts are defined within the OpenStack compute node definitions and the aggregates are ensured through a pillar structure on the OpenStack controller node.

Workaround:

1. Open your Git project repository with the Reclass model on the cluster level.
2. In openstack/control_init.yml, specify the following pillar:

```
parameters:
nova:
client:
enabled: true
resources:
v21:
admin_identity:
endpoint_type: internalURL
aggregates:
MyAggregateName:
hosts:
- host1
- host2
...
```

3. Apply the changes:

```
salt -C 'I@nova:client' state.apply nova.client
```

[35156] Loss of SNAT connectivity

Fixed in 2019.2.9

Restarting the OpenContrail schema-transformer service may cause loss of SNAT connectivity for the instances without a floating IP. The issue may also occur during the update of OpenContrail 4.1 when applying maintenance updates to 2019.2.7 and newer.

Workaround:

1. Identify the router ID and the external network ID for the instances that lost the SNAT connectivity:
 1. Log in to the OpenContrail web UI.
 2. Go to Configure > Services > Service Instances.
 3. Find the affected SNAT instance.
 4. In the Service Instance Details window, obtain the router and external network IDs.
2. Log in to an OpenStack controller node.
3. Clear the router gateway:

```
neutron router-gateway-clear <router-id>
```

4. Reset the router external gateway:

```
neutron router-gateway-set <router-id> <external-net-id>
```

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

Component	Application/service	2019.2.6	2019.2.7
DriveTrain	Gerrit	2.13.6	2.15.17
System	Kernel	4.15.0.43.64	4.15.0.72.92

Updated packages from the Mirantis and mirrored repositories

Component	Application/service	2019.2.6	2019.2.7
OpenStack Pike	alembic	0.8.10-1.1~u16.04+mcp2	0.8.10-1.2~u16.04+mcp2
	aodh	5.1.0-3~u16.04+mcp16	5.1.0-4~u16.04+mcp16
	barbican	1:5.0.1-3~u16.04+mcp17	1:5.0.1-4~u16.04+mcp17
	ceilometer	1:9.0.7-2~u16.04+mcp30	1:9.0.7-3~u16.04+mcp30
	cinder	2:11.2.2-2~u16.04+mcp135	2:11.2.2-3~u16.04+mcp138
	designate	1:5.0.3-2~u16.04+mcp16	1:5.0.3-3~u16.04+mcp16
	glance	2:15.0.2-1~u16.04+mcp16	2:15.0.2-2~u16.04+mcp16
	gnocchi	4.0.5-2~u16.04+mcp2	4.0.5-3~u16.04+mcp2
	heat	1:9.0.7-1~u16.04+mcp76	1:9.0.7-2~u16.04+mcp88
	ironic	1:9.1.6-1~u16.04+mcp54	1:9.1.6-2~u16.04+mcp54
	ironic-inspector	6.0.0-1~u16.04+mcp2	6.0.0-2~u16.04+mcp2
	keystone	2:12.0.3-4~u16.04+mcp21	2:12.0.3-5~u16.04+mcp26
	kombu	4.1.0-1~u16.04+mcp1	4.1.0-2~u16.04+mcp1
	manila	1:5.1.0-1~u16.04+mcp38	1:5.1.0-2~u16.04+mcp38
	migrate	0.11.0-1~u16.04+mcp2	0.11.0-2~u16.04+mcp2
	networking-baremetal	0.1.1-2~u16.04+mcp5	0.1.1-2~u16.04+mcp7
	networking-bgpvpn	7.0.0-2~u16.04+mcp24	7.0.1-2~u16.04+mcp11
	networking-sfc	5.0.0-1~u16.04+mcp2	5.0.0-2~u16.04+mcp2
	neutron	2:11.0.8-4~u16.04+mcp223	2:11.0.8-5~u16.04+mcp228

	neutron-dynamic-routing	2:11.0.0-1~u16.04+mcp2	2:11.0.0-2~u16.04+mcp2
	neutron-fwaas	2:11.0.2-2~u16.04+mcp10	2:11.0.2-3~u16.04+mcp10
	neutron-lbaas	2:11.0.4-1~u16.04+mcp11	2:11.0.4-2~u16.04+mcp11
	nova	2:16.1.8-5~u16.04+mcp154	2:16.1.8-6~u16.04+mcp169
	octavia	1.0.5-7~u16.04+mcp21	1.0.5-8~u16.04+mcp21
	panko	3.1.0-1~u16.04+mcp18	3.1.0-2~u16.04+mcp18
	python-neutron-lib	1.9.1-1~u16.04+mcp11	1.9.1-2~u16.04+mcp11
	python-oslo.concurrency	3.21.2-1~u16.04+mcp4	3.21.2-2~u16.04+mcp4
	python-oslo.db	4.25.2-3~u16.04+mcp11	4.25.2-4~u16.04+mcp11
	python-pykmp	0.5.0-1.1~u16.04+mcp2	0.5.0-1.2~u16.04+mcp2
	python-sqlalchemy-utils	n/a	0.30.12-3~u16.04+mcp
	python-taskflow	2.14.2-1.1~u16.04+mcp4	2.14.2-1.2~u16.04+mcp4
	sqlalchemy	1.0.13+ds1-1.1~u16.04+mcp2	1.1.11+ds1-1.1~u16.04+mcp1
	vmware-nsx	11.0.2-2~u16.04+mcp42	11.0.2-3~u16.04+mcp42
	websockify	0.8.0+dfsg1-7~u16.04+mcp2	0.8.0+dfsg1-7~u16.04+mcp3
OpenStack Queens	alembic	0.8.10-1.1~u16.04+mcp2	0.8.10-1.2~u16.04+mcp2
	aodh	6.0.1-2~u16.04+mcp15	6.0.1-3~u16.04+mcp15
	barbican	1:6.0.1-5~u16.04+mcp32	1:6.0.1-6~u16.04+mcp32
	ceilometer	1:10.0.1-2~u16.04+mcp31	1:10.0.1-3~u16.04+mcp33

	cinder	2:12.0.9-2~u16.04+mcp118	2:12.0.9-3~u16.04+mcp118
	designate	1:6.0.1-1.0~u16.04+mcp25	1:6.0.1-1.1~u16.04+mcp25
	glance	2:16.0.1-2~u16.04+mcp32	2:16.0.1-3~u16.04+mcp32
	gnocchi	4.2.4-4~u16.04+mcp12	4.2.4-5~u16.04+mcp12
	heat	1:10.0.3-1.0~u16.04+mcp82	1:10.0.3-1.1~u16.04+mcp93
	ironic	1:10.1.9-1.0~u16.04+mcp60	1:10.1.9-1.1~u16.04+mcp62
	ironic-inspector	7.2.0-1.0~u16.04+mcp1	7.2.4-1.2~u16.04+mcp1
	keystone	2:13.0.2-3~u16.04+mcp32	2:13.0.4-4~u16.04+mcp31
	kombu	4.1.0-1~u16.04+mcp1	4.1.0-2~u16.04+mcp1
	manila	1:6.3.1-2~u16.04+mcp60	1:6.3.2-3~u16.04+mcp52
	migrate	0.11.0-1~u16.04+mcp2	0.11.0-2~u16.04+mcp2
	networking-bagpipe	8.0.1-2~u16.04+mcp7	8.0.1-2~u16.04+mcp11
	networking-sfc	6.0.0-1.0~u16.04+mcp1	6.0.0-1.1~u16.04+mcp1
	neutron	2:12.1.0-7~u16.04+mcp204	2:12.1.1-8~u16.04+mcp168
	neutron-dynamic-routing	2:12.0.0-2~u16.04+mcp1	2:12.0.0-3~u16.04+mcp1
	neutron-fwaas	2:12.0.1-1.0~u16.04+mcp13	2:12.0.1-1.1~u16.04+mcp13
	neutron-lbaas	2:12.0.0-2~u16.04+mcp61	2:12.0.0-3~u16.04+mcp61
	neutron-vpnaas	n/a	2:12.0.1-1~u16.04+mcp
	nova	2:17.0.12-8~u16.01+mcp163	2:17.0.13-9~u16.04+mcp174

	octavia	2.1.2-8~u16.04+mcp86	2.1.2-9~u16.04+mcp92
	octavia-dashboard	1.0.2-1.3~u16.04+mcp3	1.0.2-1.3~u16.04+mcp6
	panko	4.0.2-2~u16.04+mcp15	4.0.2-3~u16.04+mcp15
	python-neutron-lib	1.13.0-1.0~u16.04+mcp11	1.13.0-1.1~u16.04+mcp11
	python-neutronclient	1:6.7.0-1.0~u16.04+mcp21	1:6.7.0-1.1~u16.04+mcp22
	python-octaviaclient	1.4.1-3~u16.04+mcp7	1.4.1-3~u16.04+mcp8
	python-openstackclient	3.14.3-1.0~u16.04+mcp19	3.14.3-1.0~u16.04+mcp24
	python-openstacksdk	0.11.3+repack-1.0~u16.04+mcp12	0.11.4-1.0~u16.04+mcp7
	python-osc-placement	n/a	1.0.0-1~u16.04+mcp
	python-oslo.concurrency	3.25.1-1.0~u16.04+mcp5	3.25.1-1.1~u16.04+mcp5
	python-oslo.db	4.33.4-1.0~u16.04+mcp8	4.33.4-1.1~u16.04+mcp8
	python-pykmp	0.7.0-2.0~u16.04+mcp1	0.7.0-2.1~u16.04+mcp1
	python-sqlalchemy-utils	n/a	0.30.12-3~u16.04+mcp
	python-subunit2sql	1.8.0-4.0~u16.04+mcp1	1.8.0-4.1~u16.04+mcp1
	python-swiftclient	1:3.5.0-2~u16.04+mcp9	1:3.5.0-2~u16.04+mcp11
	python-taskflow	3.1.0-1.0~u16.04+mcp13	3.1.0-1.1~u16.04+mcp13
	sqlalchemy	1.0.13+ds1-1.1~u16.04+mcp2	1.1.11+ds1-1.1~u16.04+mcp1
	websockify	0.8.0+dfsg1-7~u16.04+mcp3	0.8.0+dfsg1-7~u16.04+mcp8
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20190927152323-0	4.1~20191127132224-0

	contrail	4.1~20190927152323-0	4.1~20191127132224-0
	contrail-heat	4.1~20190927152323-0	4.1~20191127132224-0
	contrail-vrouter-dpdk	4.1~20190927152323	4.1~20191127132224
	contrail-web-controller	4.1~20190927152323-0	4.1~20191127132224-0
	contrail-web-core	4.1~20190927152323-0	4.1~20191127132224-0
	neutron-plugin-contrail	4.1~20190927152323-0	4.1~20191127132224-0
Salt formulas	salt-formula-aodh	0.2+201910070821.8c5d729~xenial1	0.2+201911290838.15dbddd~xenial1
	salt-formula-apache	0.2+201909260852.9906e3e~xenial1	0.2+201911081257.e5ed4b7~xenial1
	salt-formula-aptly	2017.2+201812071109.fecc379~xenial1	2017.2+201911061606.6260086~xenial1
	salt-formula-auditd	0.1+201907181609.edad457~xenial1	0.1+201911071035.4556d75~xenial1
	salt-formula-backupninja	0.2+201910301541.94eae60~xenial1	0.2+201911080916.73bfad2~xenial1
	salt-formula-barbican	2018.1+201910070822.e46a068~xenial1	2018.1+201912131604.f16494a~xenial1
	salt-formula-bind	0.1+201910081451.e24f7f8~xenial1	0.1+201911061606.820571d~xenial1
	salt-formula-cassandra	0.1+201907151245.95ff7b7~xenial1	0.1+201911071640.af80483~xenial1
	salt-formula-ceilometer	2016.12.1+201910081617.c259581~xenial1	2016.12.1+201911290902.564076f~xenial1
	salt-formula-ceph	0.1+201910081540.dfd11c8~xenial1	0.1+201912051140.946ac89~xenial1
	salt-formula-cinder	2016.12.1+201910091353.8e752af~xenial1	2016.12.1+201911290903.79f1677~xenial1
	salt-formula-collectd	0.2+201811221326.32816c1~xenial1	0.2+201911071620.36f6922~xenial1

	salt-formula-debmirror	2018.1+201909241520.a0366fe~xenial1	2018.1+201911061607.e3cb60f~xenial1
	salt-formula-designate	2016.12.1+201910071506.f914161~xenial1	2016.12.1+201912060858.42c5fae~xenial1
	salt-formula-docker	0.1+201910031453.e9401db~xenial1	0.1+201911061610.8370945~xenial1
	salt-formula-dogtag	0.1+201910301245.d35b0b5~xenial1	0.1+201911081251.fff45cc~xenial1
	salt-formula-elasticsearch	0.2+201908021521.7c08c15~xenial1	0.2+201911071625.289efb4~xenial1
	salt-formula-fluentd	0.1+201905231626.b551708~xenial1	0.1+201911071625.b0428ad~xenial1
	salt-formula-galera	1.0+201908010831.fc18d6b~xenial1	1.0+201911290842.938c821~xenial1
	salt-formula-gerrit	2017.2+201907151001.27a1cc3~xenial1	2017.2+201911141523.521de4f~xenial1
	salt-formula-git	0.2+201811221326.f5c25eb~xenial1	0.2+201911071622.e9fda84~xenial1
	salt-formula-glance	2016.12.1+201910040809.759fdda~xenial1	2016.12.1+201911290901.61c0802~xenial1
	salt-formula-gnocchi	2018.1+201910041916.491b389~xenial1	2018.1+201911290829.62b51f8~xenial1
	salt-formula-grafana	0.1+201909251318.0a8aaf2~xenial1	0.1+201911191341.4a5cfad~xenial1
	salt-formula-haproxy	0.2+201910141532.f7ff475~xenial1	0.2+201912031148.80b870a~xenial1
	salt-formula-heat	2016.12.1+201910040809.0e28c08~xenial1	2016.12.1+201911290843.5c800f8~xenial1
	salt-formula-horizon	2016.12.1+20190721216.7c3e253~xenial1	2016.12.1+201912050925.8870b1b~xenial1
	salt-formula-influxdb	0.1+201811221327.32f8648~xenial1	0.1+201911071624.c118aef~xenial1
	salt-formula-ironic	0.1+201910071620.c61ef1f~xenial1	0.1+201911210859.5750eb1~xenial1
	salt-formula-java	0.2+201811211411.dd3d56a~xenial1	0.2+201911071035.455b2b3~xenial1

	salt-formula-keepalived	0.2+201812152230.9b0688b~xenial1	0.2+201911271107.33c0fb2~xenial1
	salt-formula-keycloak	2018.1+201810261610.4576ba1~xenial1	2018.1+201911070927.f6c671a~xenial1
	salt-formula-keystone	2016.12.1+201910041519.82033dc~xenial1	2016.12.1+201912041637.3041257~xenial1
	salt-formula-kibana	0.2+201905210700.658869f~xenial1	0.2+201911071624.5c97b87~xenial1
	salt-formula-libvirt	0.1+201811221327.2123c5a~xenial1	0.1+201911061608.ccc7754~xenial1
	salt-formula-linux	2017.4.1+201910101244.2e6ad0f~xenial1	2017.4.1+201912100905.cac8946~xenial1
	salt-formula-lldp	0.1+201811221327.e3cad68~xenial1	0.1+201911061608.446069c~xenial1
	salt-formula-logrotate	0.1+201910170929.0ec56cc~xenial1	0.1+201911071036.314279b~xenial1
	salt-formula-maas	0.0.1+201910111546.ec56001~xenial1	0.0.1+201912021129.e3183ad~xenial1
	salt-formula-manila	2017.6+201910071508.3b33943~xenial1	2017.6+201911290843.ffc3f87~xenial1
	salt-formula-memcached	0.2+201910071508.069e5c2~xenial1	0.2+201911070933.73485d1~xenial1
	salt-formula-mongodb	0.2+201908021518.fdde3e3~xenial1	0.2+201911070927.f14d0a9~xenial1
	salt-formula-mysql	0.2+201811221327.ba591ed~xenial1	0.2+201911111532.7acd6b9~xenial1
	salt-formula-neutron	2016.12.1+201910221145.b99face~xenial1	2016.12.1+201912040858.97bd9ba~xenial1
	salt-formula-nginx	0.2+201908211443.23ba335~xenial1	0.2+201911121441.e5c8ed3~xenial1
	salt-formula-nova	2016.12.1+201910041217.8465fae~xenial1	2016.12.1+201912111257.8c124c3~xenial1
	salt-formula-ntp	0.2+201908220911.a61995f~xenial1	0.2+201911251436.9ee5a06~xenial1
	salt-formula-octavia	2017.6+201910251518.e325db6~xenial1	2017.6+201912230912.0a99e82~xenial1

	salt-formula-opencon trail	0.2+201910101508. da53267~xenial1	0.2+201911290902. 08c8848~xenial1
	salt-formula-openlda p	2017.3+2018112213 27.bf63d5e~xenial1	2017.3+2019110709 32.da6d391~xenial1
	salt-formula-opensca p	0.1+201812201717. e74d79d~xenial1	0.1+201911070931. 25fb696~xenial1
	salt-formula-openssh	0.2+201909251506. 474d205~xenial1	0.2+201911071624. 11eee6e~xenial1
	salt-formula-oslo-tem plates	2018.1+2019083009 27.f2d6ba5~xenial1	2018.1+2019111810 43.d24f42d~xenial1
	salt-formula-panko	2017.6+2019082608 59.b4faa32~xenial1	2017.6+2019112908 35.a8e0f0c~xenial1
	salt-formula-postgres ql	2017.4+2019073114 22.6b2c74b~xenial1	2017.4+2019110709 31.8dff18~xenial1
	salt-formula-powerdn s	0.1+201812150647. 97eb6b6~xenial1	0.1+201911070931. 211a69a~xenial1
	salt-formula-prometh eus	0.1+201909251319. db41b21~xenial1	0.1+201911221146. 2020c62~xenial1
	salt-formula-rabbitm q	0.2+201909241136. a2739ee~xenial1	0.2+201911111218. 406954d~xenial1
	salt-formula-reclass	0.2+201908261321. 995c917~xenial1	0.2+201911081404. 07719bf~xenial1
	salt-formula-rsyslog	0.1+201811221328. 1cb1d34~xenial1	0.1+201911071622. 78de5f8~xenial1
	salt-formula-runtest	0.1+201910211338. 4c48ac0~xenial1	0.1+201911251542. a7fd395~xenial1
	salt-formula-salt	0.4+201910300830. 308fccd~xenial1	0.4+201911071622. 34d31ba~xenial1
	salt-formula-telegraf	0.1+201910041104. 4d8f0bb~xenial1	0.1+201912040912. 0b0bfae~xenial1
	salt-formula-tinyprox y	0.1+201811141102. 1f390ef~xenial1	0.1+201911070930. 637ecee~xenial1
	salt-formula-watchdo g	2018.1+2018111413 25.75d7d50~xenial1	2018.1+2019110710 35.24e5a4a~xenial1
	salt-formula-xtraback up	0.2+201909041534. bd7b0c9~xenial1	0.2+201911111253. 665443e~xenial1
Extra packages	jmx-exporter	2:0.3.2-2~u16.04+m cp3	2:0.3.2-2~u16.04+m cp4
	libvirt-exporter	0.1-1~u16.04+mcp1	0.1-1~u16.04+mcp6

	sosreport	n/a	3.8.0-1~u16.04+mcp1
	telegraf	1:1.9.1-3~u16.04+mcp47	1:1.9.1-3~u16.04+mcp52

Note

All 2019.2.7 packages are available at <http://mirror.mirantis.com/update/2019.2.0/>.

Release artifacts

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

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.7/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.7/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.7/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.7/ceph-luminous/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.7/opencontrail-4.1/xenial xenial main
	Salt formulas packages ³⁶	http://mirror.mirantis.com/update/2019.2.7/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.7.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.7.qcow2

	VCP Ubuntu 16.04 image ³⁶	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.7/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.7/elasticse-arch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.7/elasticse-arch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.7/elasticse-arch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.7/elasticse-arch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³⁶
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.7/glusterfs-5/xenial xenial main ³⁶
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.7/maas/xenial xenial main ³⁶
	Percona	deb http://mirror.mirantis.com/update/2019.2.7/percona/xenial xenial main ³⁶
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.7/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.7/saltstack-2017.7/xenial xenial main ³⁶

	Upstream Ubuntu system packages ³⁶	deb https://mirror.mirantis.com/update/2019.2.7/ubuntu/xenial/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.7/ubuntu/xenial-updates/main/restricted/universe deb https://mirror.mirantis.com/update/2019.2.7/ubuntu/xenial-security/main/restricted/universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/ 2019.2.7
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/ 2019.2.7
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model 2019.2.7
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts 2019.2.7
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.7 ³⁶
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³⁶
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.7 ³⁶
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.7 ³⁶
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.7 ³⁶
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³⁶
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³⁶
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.4 ³⁶
	gainsight_elasticsearch	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight_elasticsearch:2019.2.7 ³⁶
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.5 ³⁶
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.7 ³⁶
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.7 ³⁶

	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.5 ³⁶
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.7 ³⁶
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.7 ³⁶
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/openldap:1.2.2 ³⁶
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.5 ³⁶
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³⁶
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.6 ³⁶
	prometheus_relay	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus-relay:2019.2.5 ³⁶
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.6 ³⁶
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.7 ³⁶
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.7 ³⁶
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³⁶
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.6 ³⁶
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.7
Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.6 ³⁶

36(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34\)](#)

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

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> 1. Update DriveTrain as described in MCP Operations Guide: Update DriveTrain to a minor release version. 2. If applicable, Enable authentication for Aptly repositories.
2	OpenContrail	Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes .
3	OpenStack	<ol style="list-style-type: none"> 1. Update the OpenStack packages as described in MCP Operations Guide: 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. 2. Perform the steps described in Issues resolutions requiring manual application. 3. Optional. Set the directory for lock files. 4. Optional. Add availability zone to Gnocchi instance resource.
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	<ol style="list-style-type: none"> 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.
6	Ceph	Ceph updates will be applied during the DriveTrain update. Optional. Technical preview. Enable the ceph-volume tool .
7	Ubuntu Xenial packages	<p>Select from the following options:</p> <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso
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
- Local mirrors update procedure
- Automatic Dogtag backup

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:

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

For example:

```
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:

- DockerdServiceReplicaFlapping
- OVSTooManyPortRunningOnAgent, OVSErrorOnPort, OVSNonInternalPortDown, OVSGatherFailed
- RabbitmqFdUsageWarning and RabbitmqFdUsageCritical
- 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 salt `-C "l@ceph:common" state.apply ceph.setup.keyring` from the Salt Master node.

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 '@jenkins:client and !@haproxy:proxy' saltutil.refresh_pillar
```

4. Apply the changes to HAProxy on the CI/CD nodes:

```
salt -C '@jenkins:client and !@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 backend. 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 backend 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:

```
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:
  barbican:
    server:
    ...
    ks_notifications_topic: barbican
```

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

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

```
salt -C '!@barbican:server:role:primary' state.apply barbican.server
salt -C '!@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:

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

```
metadata:  
  secret: ${_param:openstack_metadata_password_generated}  
{%- endif %}
```

with:

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

3. Apply the opencontrail.compute state:

```
salt -C '@opencontrail:compute' state.apply opencontrail.compute exclude=opencontrail.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_sf_dc_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_sf_dc_sandbox_enabled` value in double quotation marks. For example:

```
parameters:  
  _param:  
    sf_notifier_sf_dc_sandbox_enabled: "True"
```

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

```
salt -C '@prometheus:server and @docker:client' saltutil.refresh_pillar  
salt -C '@prometheus:server and @docker:client' state.apply docker.client
```

Ceph

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 Reclash model on the cluster level.
2. In `classes/cluster/cluster_name/ceph/common.yml`, remove the backslash characters `\` from the caps definitions. For example:

```
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 "l@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

Fixed in 2019.2.11

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:

Note

In the state below, substitute the certificate path with the one you obtained in the previous step.


```
salt -C 'l@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

Component	Application/service	2019.2.5	2019.2.6
Stacklight	Prometheus	2.5.0	2.12.0

Updated packages from the Mirantis and mirrored repositories

Component	Application/service	2019.2.5	2019.2.6
OpenStack Pike	ceilometer	1:9.0.7-2~u16.04+m cp29	1:9.0.7-2~u16.04+m cp30

	cinder	2:11.2.2-2~u16.04+mcp113	2:11.2.2-2~u16.04+mcp135
	glance	2:15.0.2-1~u16.04+mcp14	2:15.0.2-1~u16.04+mcp16
	heat	1:9.0.7-1~u16.04+mcp65	1:9.0.7-1~u16.04+mcp76
	ironic	1:9.1.6-1~u16.04+mcp53	1:9.1.6-1~u16.04+mcp54
	networking-bagpipe	7.0.0-2~u16.04+mcp12	7.0.1-2~u16.04+mcp7
	neutron	2:11.0.8-2~u16.04+mcp204	2:11.0.8-4~u16.04+mcp223
	nova	2:16.1.8-5~u16.04+mcp142	2:16.1.8-5~u16.04+mcp154
	octavia	1.0.4-6~u16.04+mcp16	1.0.5-7~u16.04+mcp21
	python-barbicanclient	4.5.3-1.1~u16.04+mcp9	4.5.3-1.1~u16.04+mcp12
	python-django-opensack-auth	3.6.1-2~u16.04+mcp9	3.6.1-2~u16.04+mcp10
	python-glance-store	0.22.0-3~u16.04+mcp9	0.22.0-3~u16.04+mcp11
	python-openstackclient	3.12.2-1~u16.04+mcp12	3.12.2-1~u16.04+mcp13
	python-oslo.policy	1.25.4-1~u16.04+mcp5	1.25.4-1~u16.04+mcp6
	python-pymysql	0.7.6-1.1~u16.04+mcp2	0.7.6-1.1~u16.04+mcp3
OpenStack Queens	ceilometer	1:10.0.1-2~u16.04+mcp30	1:10.0.1-2~u16.04+mcp31
	cinder	2:12.0.7-2~u16.04+mcp112	2:12.0.9-2~u16.04+mcp118
	designate-dashboard	6.0.0-1.0~u16.04+mcp2	6.0.1-1.0~u16.04+mcp2
	glance	2:16.0.1-2~u16.04+mcp27	2:16.0.1-2~u16.04+mcp32
	heat	1:10.0.3-1.0~u16.04+mcp63	1:10.0.3-1.0~u16.04+mcp82

	horizon	3:13.0.2-10~u16.04+mcp76	3:13.0.2-10~u16.04+mcp87
	ironic	1:10.1.9-1.0~u16.04+mcp43	1:10.1.9-1.0~u16.04+mcp60
	manila	1:6.3.0-2~u16.04+mcp47	1:6.3.1-2~u16.04+mcp60
	networking-bgpvpn	8.0.1-1.0~u16.04+mcp13	8.0.1-1.0~u16.04+mcp15
	networking-ovn	4.0.3-1.0~u16.04+mcp39	4.0.3-1.0~u16.04+mcp78
	neutron	2:12.1.0-5~u16.04+mcp136	2:12.1.0-7~u16.04+mcp204
	neutron-fwaas	2:12.0.1-1.0~u16.04+mcp10	2:12.0.1-1.0~u16.04+mcp13
	neutron-lbaas	2:12.0.0-2~u16.04+mcp53	2:12.0.0-2~u16.04+mcp61
	nova	2:17.0.11-8~u16.01+mcp139	2:17.0.12-8~u16.01+mcp163
	octavia	2.1.1-7~u16.04+mcp76	2.1.2-8~u16.04+mcp86
	octavia-dashboard	1.0.1-1.3~u16.04+mcp9	1.0.2-1.3~u16.04+mcp3
	python-barbicanclient	4.6.1-1.0~u16.04+mcp12	4.6.1-1.0~u16.04+mcp14
	python-glance-store	0.23.0-2~u16.04+mcp13	0.23.0-2~u16.04+mcp15
	python-ironic-inspector-client	3.1.0-1.0~u16.04+mcp2	3.1.2-1.0~u16.04+mcp2
	python-ironic-lib	2.12.2-1.0~u16.04+mcp6	2.12.3-1.0~u16.04+mcp9
	python-keystonemiddleware	4.21.0-1.0~u16.04+mcp17	4.21.0-1.0~u16.04+mcp20
	python-openstackclient	3.14.3-1.0~u16.04+mcp18	3.14.3-1.0~u16.04+mcp19
	python-openstacksdk	0.11.3+repack-1.0~u16.04+mcp10	0.11.3+repack-1.0~u16.04+mcp12
	python-os-brick	2.3.8-1.0~u16.04+mcp8	2.3.8-1.0~u16.04+mcp10

	python-oslo.log	3.36.0-1.0~u16.04+mcp12	3.36.0-1.0~u16.04+mcp15
	python-oslo.messaging	5.35.5-2~u16.04+mcp26	5.35.5-2~u16.04+mcp31
	python-ovsdbapp	0.10.3-1.0~u16.04+mcp6	0.10.4-1.0~u16.04+mcp6
	python-pymysql	0.8.0-1~u16.04+mcp1	0.8.0-1~u16.04+mcp2
	python-swiftclient	1:3.5.0-2~u16.04+mcp7	1:3.5.0-2~u16.04+mcp9
	sushy	1.3.3-1~u16.04+mcp4	1.3.3-1~u16.04+mcp6
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20190723091617-0	4.1~20190927152323-0
	contrail	4.1~20190723091617-0	4.1~20190927152323-0
	contrail-heat	4.1~20190723091617-0	4.1~20190927152323-0
	contrail-vrouter-dpdk	4.1~20190723091617	4.1~20190927152323
	contrail-web-controller	4.1~20190723091617-0	4.1~20190927152323-0
	contrail-web-core	4.1~20190723091617-0	4.1~20190927152323-0
	neutron-plugin-contrail	4.1~20190723091617-0	4.1~20190927152323-0
Salt formulas	salt-formula-aodh	0.2+201908021613.5563c27~xenial1	0.2+201910070821.8c5d729~xenial1
	salt-formula-apache	0.2+201908091710.7e3a90f~xenial1	0.2+201909260852.9906e3e~xenial1
	salt-formula-backports	n/a	0.1+201909271115.a35cfb9~xenial1
	salt-formula-backupninja	0.2+201907311426.26e6d9a~xenial1	0.2+201910301541.94eae60~xenial1
	salt-formula-barbican	2018.1+201908091203.bcadfba~xenial1	2018.1+201910070822.e46a068~xenial1
	salt-formula-baremetal-simulator	0.1+201812270854.79045fe~xenial1	0.1+201908271439.5400e68~xenial1

	salt-formula-bind	0.1+201812201615.c1766d8~xenial1	0.1+201910081451.e24f7f8~xenial1
	salt-formula-ceilometer	2016.12.1+201908021625.122d9a0~xenial1	2016.12.1+201910081617.c259581~xenial1
	salt-formula-ceph	0.1+201908091302.e7208c2~xenial1	0.1+201910081540.dfd11c8~xenial1
	salt-formula-cinder	2016.12.1+201907311843.aca0d9f~xenial1	2016.12.1+201910091353.8e752af~xenial1
	salt-formula-debmirror	2018.1+201812281232.8730773~xenial1	2018.1+201909241520.a0366fe~xenial1
	salt-formula-designate	2016.12.1+201908051616.5d0b0d2~xenial1	2016.12.1+201910071506.f914161~xenial1
	salt-formula-docker	0.1+201905211725.b72da1c~xenial1	0.1+201910031453.e9401db~xenial1
	salt-formula-dogtag	0.1+201907311641.230a470~xenial1	0.1+201910301245.d35b0b5~xenial1
	salt-formula-glance	2016.12.1+201907311658.1de518d~xenial1	2016.12.1+201910040809.759fdda~xenial1
	salt-formula-gnocchi	2018.1+201908080856.5f44a07~xenial1	2018.1+201910041916.491b389~xenial1
	salt-formula-grafana	0.1+201905281140.b39c951~xenial1	0.1+201909251318.0a8aaf2~xenial1
	salt-formula-haproxy	0.2+201907311337.8a8b420~xenial1	0.2+201910141532.f7ff475~xenial1
	salt-formula-heat	2016.12.1+201907311650.4efd963~xenial1	2016.12.1+201910040809.0e28c08~xenial1
	salt-formula-iptables	1.0+201811211247.c60cebc~xenial1	1.0+201910021624.20d1021~xenial1
	salt-formula-ironic	0.1+201905231618.b711aae~xenial1	0.1+201910071620.c61ef1f~xenial1
	salt-formula-keystone	2016.12.1+201907311659.0ae2333~xenial1	2016.12.1+201910041519.82033dc~xenial1

	salt-formula-linux	2017.4.1+201907311654.987ee9a~xenial1	2017.4.1+201910101244.2e6ad0f~xenial1
	salt-formula-logrotate	0.1+201907311335.7cdf15a~xenial1	0.1+201910170929.0ec56cc~xenial1
	salt-formula-maas	0.0.1+201908121804.d7522b3~xenial1	0.0.1+201910111546.ec56001~xenial1
	salt-formula-manila	2017.6+201907080944.d846ee2~xenial1	2017.6+201910071508.3b33943~xenial1
	salt-formula-memcached	0.2+201903250937.08d5fd4~xenial1	0.2+201910071508.069e5c2~xenial1
	salt-formula-neutron	2016.12.1+201907311854.80b9289~xenial1	2016.12.1+201910221145.b99face~xenial1
	salt-formula-nginx	0.2+201907311432.8eee166~xenial1	0.2+201908211443.23ba335~xenial1
	salt-formula-nova	2016.12.1+201907311830.98980e8~xenial1	2016.12.1+201910041217.8465fae~xenial1
	salt-formula-ntp	0.2+201811221327.ad604c8~xenial1	0.2+201908220911.a61995f~xenial1
	salt-formula-octavia	2017.6+201908050949.35c0953~xenial1	2017.6+201910251518.e325db6~xenial1
	salt-formula-opencontrail	0.2+201907191135.26bdf2d~xenial1	0.2+201910101508.da53267~xenial1
	salt-formula-openssh	0.2+201905061452.3cf4cc7~xenial1	0.2+201909251506.474d205~xenial1
	salt-formula-oslo-templates	2018.1+201905201000.3db8426~xenial1	2018.1+201908300927.f2d6ba5~xenial1
	salt-formula-panko	2017.6+201905241116.68551a1~xenial1	2017.6+201908260859.b4faa32~xenial1
	salt-formula-prometheus	0.1+201907111546.2c18561~xenial1	0.1+201909251319.db41b21~xenial1
	salt-formula-rabbitmq	0.2+201908010825.c9b2b7f~xenial1	0.2+201909241136.a2739ee~xenial1
	salt-formula-reclass	0.2+201811221328.bba5167~xenial1	0.2+201908261321.995c917~xenial1
	salt-formula-runttest	0.1+201907190925.ab45b4c~xenial1	0.1+201910211338.4c48ac0~xenial1

	salt-formula-salt	0.4+201908011504.028077c~xenial1	0.4+201910300830.308fccd~xenial1
	salt-formula-shibboleth	n/a	0.0.2+201909240833.f539306~xenial1
	salt-formula-telegraf	0.1+201908021517.b21fffc~xenial1	0.1+201910041104.4d8f0bb~xenial1
	salt-formula-xtrabackup	0.2+201908091632.e95661a~xenial1	0.2+201909041534.bd7b0c9~xenial1
Extra packages	atomic	n/a	1.22-1~u16.04+mcp1
	prometheus-bin	2.5.0-1~u16.04+mcp1	2.12.0-1~u16.04+mcp1
	telegraf	1:1.9.1-3~u16.04+mcp45	1:1.9.1-3~u16.04+mcp47
	telegraf-builddeps	0.0+git20190613-1	0.0+git20190830-1

Note

All 2019.2.6 packages are available at <http://mirror.mirantis.com/update/2019.2.0/>.

Release artifacts

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

MCP release artifacts

Type	Artifact	Path
Mirantis apt/deb packages	OpenStack packages	deb https://mirror.mirantis.com/update/2019.2.0/openstack-pike/xenial xenial main deb https://mirror.mirantis.com/update/2019.2.0/openstack-queens/xenial xenial main
	Extra packages	deb http://mirror.mirantis.com/update/2019.2.0/extra/xenial xenial main
	Ceph	deb http://mirror.mirantis.com/update/2019.2.0/ceph-luminous/xenial xenial main
	OpenContrail packages	deb http://mirror.mirantis.com/update/2019.2.0/opencontrail-4.1/xenial xenial main

	Salt formulas packages ³⁷	http://mirror.mirantis.com/update/2019.2.0/salt-formulas/xenial xenial main
QCOW images	MCP cfg01 day01 image	http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2.md5 http://images.mirantis.com/cfg01-day01-2019.2.0.qcow2
	MCP apt01 offline image	http://images.mirantis.com/mcp-offline-image-2019.2.6.qcow2.md5 http://images.mirantis.com/mcp-offline-image-2019.2.6.qcow2
	VCP Ubuntu 16.04 image ³⁷	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
Upstream mirrors	aptly	deb http://mirror.mirantis.com/2019.2.0/aptly/xenial squeeze main
	Cassandra	deb http://mirror.mirantis.com/2019.2.0/cassandra/trusty 21x main deb http://mirror.mirantis.com/2019.2.0/cassandra/xenial 21x main
	Docker	deb http://mirror.mirantis.com/update/2019.2.0/docker/xenial xenial stable
	Elastic	deb http://mirror.mirantis.com/update/2019.2.0/elasticse arch-5.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.0/elasticse arch-6.x/xenial stable main deb http://mirror.mirantis.com/update/2019.2.0/elasticse arch-curator/xenial stable main deb http://mirror.mirantis.com/update/2019.2.0/elasticse arch-curator-5/xenial stable main
	Fluentd	deb http://mirror.mirantis.com/2019.2.0/td-agent/xenial xenial contrib ³⁷
	GlusterFS	deb http://mirror.mirantis.com/update/2019.2.0/glusterfs-3.8/xenial xenial main ³⁷
	InfluxDB	deb http://mirror.mirantis.com/2019.2.0/influxdb/xenial xenial stable
	MAAS	deb http://mirror.mirantis.com/update/2019.2.0/maas/xenial xenial main ³⁷

	Percona	deb http://mirror.mirantis.com/update/2019.2.0/percona/xenial xenial main ³⁷
	SaltStack packages	deb http://mirror.mirantis.com/update/2019.2.0/saltstack-2017.7/trusty trusty main deb http://mirror.mirantis.com/update/2019.2.0/saltstack-2017.7/xenial xenial main ³⁷
	Upstream Ubuntu system packages ³⁷	deb https://mirror.mirantis.com/update/2019.2.0/ubuntu/xenial main restricted universe deb https://mirror.mirantis.com/update/2019.2.0/ubuntu/xenial-updates main restricted universe deb https://mirror.mirantis.com/update/2019.2.0/ubuntu/xenial-security main restricted universe
MCP Git repositories	Jenkins pipeline library for MCP operations	https://github.com/Mirantis/mk-pipelines/release/2019.2.0
	General Jenkins pipeline library	https://github.com/Mirantis/pipeline-library/release/2019.2.0
	Reclass system level	https://github.com/Mirantis/reclass-system-salt-model/release/2019.2.0
	MCP common scripts	https://github.com/Mirantis/mcp-common-scripts/release/2019.2.0
	MCP offline image model	https://github.com/Mirantis/mcp-offline-model/release/2019.2.0
Docker images	alerta-web	docker-prod-local.artifactory.mirantis.com/mirantis/external/alerta-web:2019.2.0 ³⁷
	alertmanager	docker-prod-local.artifactory.mirantis.com/openstack-docker/alertmanager:2019.2.4 ³⁷
	aptly	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly:2019.2.0 ³⁷
	aptly-api	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-api:2019.2.0
	aptly-public	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-public:2019.2.0 ³⁷
	aptly-publisher	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/aptly-publisher:2019.2.0 ³⁷
	compose	docker-prod-local.artifactory.mirantis.com/mirantis/external/docker/compose:1.17.1 ³⁷
	cvp-rally	docker-prod-local.artifactory.mirantis.com/mirantis/cvp/cvp-rally:2019.2.5 ³⁷

	elasticsearch	docker-prod-local.artifactory.mirantis.com/mirantis/external/elasticsearch:2019.2.0 ³⁷
	gainsight	docker-prod-local.artifactory.mirantis.com/openstack-docker/gainsight:2019.2.4 ³⁷
	gerrit	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/gerrit:2019.2.5 ³⁷
	grafana	docker-prod-local.artifactory.mirantis.com/openstack-docker/grafana:2019.2.0 ³⁷
	heka	docker-prod-local.artifactory.mirantis.com/openstack-docker/heka:2019.2.0 ³⁷
	jenkins	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jenkins:2019.2.5 ³⁷
	jnlp-slave	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/jnlp-slave:2019.2.0 ³⁷
	mysql	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/mysql:2019.2.0 ³⁷
	openldap	docker-prod-local.artifactory.mirantis.com/mirantis/external/osixia/openldap:1.2.2 ³⁷
	phpldapadmin	docker-prod-local.artifactory.mirantis.com/mirantis/cicd/phpldapadmin:2019.2.5 ³⁷
	postgres	docker-prod-local.artifactory.mirantis.com/mirantis/external/library/postgres:9.6.10 ³⁷
	prometheus	docker-prod-local.artifactory.mirantis.com/openstack-docker/prometheus:2019.2.6 ³⁷
	prometheus_relay	docker-prod-local.artifactory.mirantis.com//openstack-docker/prometheus-relay:2019.2.5 ³⁷
	pushgateway	docker-prod-local.artifactory.mirantis.com/openstack-docker/pushgateway:2019.2.0 ³⁷
	registry	docker-prod-local.artifactory.mirantis.com/mirantis/external/registry:2019.2.0 ³⁷
	remote_storage_adapter	docker-prod-local.artifactory.mirantis.com/openstack-docker/remote_storage_adapter:2019.2.0 ³⁷
	sf_notifier	docker-prod-local.artifactory.mirantis.com/openstack-docker/sf_notifier:2019.2.4 ³⁷
	telegraf	docker-prod-local.artifactory.mirantis.com/openstack-docker/telegraf:2019.2.6 ³⁷
	visualizer	docker-prod-local.artifactory.mirantis.com/mirantis/external/visualizer:2019.2.0

Other	octavia	https://artifactory.mirantis.com/artifactory/binary-prod-local/mirantis/openstack/octavia/images/2019.2.0 ³⁷
-------	---------	---

37(1, 2, 3, 4, 5, Available in the MCP offline image in the reduced size. For details, see: [MCP 6, 7, 8, 9, 10, Reference Architecture: Mirror image content. 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34\)](#)

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.

Update procedure workflow

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> 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. 3. Optional. MCP Operations Guide: Configure remote logging for auditd. 4. Optional. MCP Operations Guide: Configure Redis server memory limits. 5. Optional. MCP Operations Guide: Configure multiple NTP servers.
2	OpenContrail	<ol style="list-style-type: none"> 1. Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes. 2. Perform the steps described in Issues resolutions requiring manual application.

3	OpenStack	<ol style="list-style-type: none"> 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. Optional. For environments with Ironic, Enable SSL on Ironic internal API.
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	<ol style="list-style-type: none"> 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. MCP Operations Guide: Enable Ironic monitoring. 4. Customize the <code>SystemCpuStealTimeWarning</code>, <code>SystemCpuStealTimeCritical</code>, <code>RabbitmqFdUsageWarning</code>, <code>RabbitmqFdUsageCritical</code> and <code>OVSTooManyPortRunningOnAgent</code> alerts as described in MCP Operations Guide: Alerts that require tuning.
6	Ceph	<ol style="list-style-type: none"> 1. Perform the steps described in Issues resolutions requiring manual application. 2. Optional. Update Ceph keyring permissions as described in Ceph.
7	Ubuntu Xenial packages	<p>Select from the following options:</p> <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso
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.

Learn more

[MCP Deployment Guide: Configure Galera parameters](#)

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.

Learn more

[MCP Deployment Guide: Configure HAProxy parameters](#)

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.

Learn more

[MCP Operations Guide: Configure Jenkins SSH slaves instead of JNLP](#)

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.

Learn more

[MCP Operations Guide: Cloud verification](#)

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.

OpenContrail

In the MCP 2019.2.5 maintenance update, Mirantis added the capability to enable Secure Sockets Layer (SSL) for the internal endpoint of the OpenContrail 4.1 API. By default, the feature is disabled.

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

Learn more

[MCP Operations Guide: Enable SSL for an OpenContrail API internal endpoint](#)

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.

Learn more

[MCP Operations Guide: Telegraf alerts](#)

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.

Learn more

[MCP Operations Guide: SMART disks](#)

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.

Learn more

[MCP Deployment Guide: Deploy a Ceph cluster](#)

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 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 Reclaim model and use them in URLs to access the required sources. For example:

```
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 'l@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'
```

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:

```
[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

Component	Application/service	2019.2.4	2019.2.5
OpenStack Pike	aodh	5.1.0-3~u16.04+mcp 12	5.1.0-3~u16.04+mcp 16

	barbican	1:5.0.1-3~u16.04+mcp13	1:5.0.1-3~u16.04+mcp17
	ceilometer	1:9.0.6-2~u16.04+mcp22	1:9.0.7-2~u16.04+mcp29
	cinder	2:11.2.2-2~u16.04+mcp104	2:11.2.2-2~u16.04+mcp113
	designate	1:5.0.2-2~u16.04+mcp19	1:5.0.3-2~u16.04+mcp16
	glance	2:15.0.1-1~u16.04+mcp21	2:15.0.2-1~u16.04+mcp14
	heat	1:9.0.7-1~u16.04+mcp44	1:9.0.7-1~u16.04+mcp65
	horizon	3:12.0.4-4~u16.04+mcp69	3:12.0.4-5~u16.04+mcp80
	ironic	1:9.1.6-1~u16.04+mcp49	1:9.1.6-1~u16.04+mcp53
	keystone	2:12.0.2-4~u16.04+mcp14	2:12.0.3-4~u16.04+mcp21
	libvirt	4.0.0-1.8.10~u16.04+mcp1	4.0.0-1.8.10~u16.04+mcp2
	manila	1:5.0.3-1~u16.04+mcp51	1:5.1.0-1~u16.04+mcp38
	manila-ui	2.10.2-1~u16.04+mcp10	2.10.3-1~u16.04+mcp6
	networking-baremetal	0.1.1-2~u16.04+mcp2	0.1.1-2~u16.04+mcp5
	networking-bgpvpn	7.0.0-2~u16.04+mcp18	7.0.0-2~u16.04+mcp24
	networking-generic-switch	0.4.1-1~u16.04+mcp	0.4.1-1~u16.04+mcp11
	networking-l2gw	1:11.0.0-1~u16.04+mcp17	1:11.0.0-1~u16.04+mcp19
	neutron	2:11.0.8-2~u16.04+mcp178	2:11.0.8-2~u16.04+mcp204
	neutron-fwaas	2:11.0.2-2~u16.04+mcp8	2:11.0.2-2~u16.04+mcp10
	neutron-lbaas	2:11.0.3-1~u16.04+mcp15	2:11.0.4-1~u16.04+mcp11

	nova	2:16.1.8-4~u16.04+mcp131	2:16.1.8-5~u16.04+mcp142
	octavia	1.0.3-7~u16.04+mcp15	1.0.4-6~u16.04+mcp16
	openvswitch	2.9.0-0.1~u16.04+mcp	2.9.5-1~u16.04+mcp
	panko	3.1.0-1~u16.04+mcp16	3.1.0-1~u16.04+mcp18
	python-automaton	1.12.1-2~u16.04+mcp2	1.12.2-2~u16.04+mcp4
	python-brick-cinderclient-ext	0.5.0-1~u16.04+mcp5	0.5.1-1~u16.04+mcp2
	python-castellan	0.12.3-1~u16.04+mcp7	0.12.3-1~u16.04+mcp11
	python-ceilometerclient	2.9.0-2~u16.04+mcp2	2.9.0-2~u16.04+mcp3
	python-debtcollector	1.17.1-0.1~u16.04+mcp2	1.17.2-0.1~u16.04+mcp2
	python-designateclient	2.7.0-1~u16.04+mcp8	2.7.1-1~u16.04+mcp4
	python-django-opensack-auth	3.6.1-2~u16.04+mcp6	3.6.1-2~u16.04+mcp9
	python-futurist	1.3.1-1~u16.04+mcp2	1.3.2-1~u16.04+mcp2
	python-glance-store	0.22.0-3~u16.04+mcp7	0.22.0-3~u16.04+mcp9
	python-glanceclient	1:2.8.0-1~u16.04+mcp14	1:2.8.0-1~u16.04+mcp16
	python-heatclient	1.11.1-1~u16.04+mcp4	1.11.1-1~u16.04+mcp6
	python-ironic-lib	2.10.1-1~u16.04+mcp6	2.10.2-1~u16.04+mcp3
	python-ironicclient	1.17.1-1~u16.04+mcp13	1.17.2-1~u16.04+mcp7
	python-keystoneauth1	3.1.0-1~u16.04+mcp12	3.1.1-1~u16.04+mcp6
	python-keystoneclient	1:3.13.0-1~u16.04+mcp9	1:3.13.1-1~u16.04+mcp4

	python-keystonemiddleware	4.17.0-1~u16.04+mcp2	4.17.1-1~u16.04+mcp5
	python-ldappool	2.1.0-1~u16.04+mcp6	2.1.1-1~u16.04+mcp2
	python-manilaclient	1.17.3-1~u16.04+mcp8	1.17.4-1~u16.04+mcp7
	python-neutron-lib	1.9.1-1~u16.04+mcp9	1.9.1-1~u16.04+mcp11
	python-neutronclient	1:6.5.0-1~u16.04+mcp19	1:6.5.0-1~u16.04+mcp23
	python-novaclient	2:9.1.1-1~u16.04+mcp10	2:9.1.2-1~u16.04+mcp9
	python-octaviaclient	1.2.0-1~u16.04+mcp4	1.2.1-1~u16.04+mcp4
	python-openstacksdk	0.9.18-1~u16.04+mcp1	0.9.18-1~u16.04+mcp4
	python-os-brick	1.15.8-1~u16.04+mcp17	1.15.9-1~u16.04+mcp8
	python-os-client-config	1.28.0-1~u16.04+mcp7	1.28.1-1~u16.04+mcp2
	python-os-traits	0.3.3-1~u16.04+mcp3	0.3.3-1~u16.04+mcp5
	python-os-vif	1.7.1-1~u16.04+mcp0	1.7.1-1~u16.04+mcp2
	python-osc-lib	1.7.0-1~u16.04+mcp5	1.7.1-1~u16.04+mcp2
	python-oslo.concurrency	3.21.1-1~u16.04+mcp4	3.21.2-1~u16.04+mcp4
	python-oslo.config	1:4.11.1-1~u16.04+mcp4	1:4.11.2-1~u16.04+mcp4
	python-oslo.db	4.25.2-3~u16.04+mcp8	4.25.2-3~u16.04+mcp11
	python-oslo.i18n	3.17.1-1~u16.04+mcp4	3.17.2-1~u16.04+mcp4
	python-oslo.middleware	3.30.1-1~u16.04+mcp4	3.30.2-1~u16.04+mcp4
	python-oslo.policy	1.25.3-1~u16.04+mcp4	1.25.4-1~u16.04+mcp5

	python-oslo.reports	1.22.1-1.1~u16.04+mcp2	1.22.2-1.1~u16.04+mcp2
	python-oslo.rootwrap	5.9.2-1~u16.04+mcp6	5.9.3-1~u16.04+mcp5
	python-oslo.serialization	2.20.2-1~u16.04+mcp5	2.20.3-1~u16.04+mcp5
	python-oslo.utils	3.28.3-1~u16.04+mcp5	3.28.4-1~u16.04+mcp6
	python-oslo.versionedobjects	1.26.2-1~u16.04+mcp5	1.26.3-1~u16.04+mcp6
	python-pankoclient	0.3.0-2~u16.04+mcp5	0.3.0-2~u16.04+mcp7
	python-pycadf	2.6.0-1~u16.04+mcp4	2.6.1-1~u16.04+mcp2
	python-swiftclient	1:3.4.0-1~u16.04+mcp7	1:3.4.1-1~u16.04+mcp4
	python-taskflow	2.14.1-1.1~u16.04+mcp4	2.14.2-1.1~u16.04+mcp4
	python-tooz	1.58.0-1~u16.04+mcp4	1.58.1-1~u16.04+mcp2
	qemu	1:2.11+dfsg-1.7.13~u16.04+mcp1	1:2.11+dfsg-1.7.13~u16.04+mcp2
	stevedore	1:1.25.1-1~u16.04+mcp5	1:1.25.2-1~u16.04+mcp4
	sushy	1.1.1-1~u16.04+mcp0	1.1.1-1~u16.04+mcp4
OpenStack Queens	cinder	2:12.0.7-2~u16.04+mcp100	2:12.0.7-2~u16.04+mcp112
	designate	1:6.0.1-1.0~u16.04+mcp22	1:6.0.1-1.0~u16.04+mcp25
	heat	1:10.0.3-1.0~u16.04+mcp59	1:10.0.3-1.0~u16.04+mcp63
	horizon	3:13.0.2-10~u16.04+mcp74	3:13.0.2-10~u16.04+mcp76
	ironic	1:10.1.8-1.0~u16.04+mcp57	1:10.1.9-1.0~u16.04+mcp43
	keystone	2:13.0.2-3~u16.04+mcp30	2:13.0.2-3~u16.04+mcp32

	libvirt	4.0.0-1.8.10~u16.04+mcp1	4.0.0-1.8.10~u16.04+mcp2
	networking-ovn	4.0.3-1.0~u16.04+mcp31	4.0.3-1.0~u16.04+mcp39
	neutron	2:12.0.6-5~u16.04+mcp201	2:12.1.0-5~u16.04+mcp136
	neutron-lbaas	2:12.0.0-2~u16.04+mcp50	2:12.0.0-2~u16.04+mcp53
	nova	2:17.0.10-7~u16.01+mcp188	2:17.0.11-8~u16.01+mcp139
	octavia	2.1.0-7~u16.04+mcp78	2.1.1-7~u16.04+mcp76
	python-automaton	1.14.0-1.0~u16.04+mcp6	1.14.0-1.0~u16.04+mcp8
	python-castellan	0.17.0-2.0~u16.04+mcp15	0.17.0-2.0~u16.04+mcp17
	python-octaviaclient	1.4.0-3~u16.04+mcp11	1.4.1-3~u16.04+mcp7
	python-openstacksdk	0.11.3+repack-1.0~u16.04+mcp8	0.11.3+repack-1.0~u16.04+mcp10
	python-os-brick	2.3.7-1.0~u16.04+mcp8	2.3.8-1.0~u16.04+mcp8
	python-os-vif	1.9.1-1.0~u16.04+mcp8	1.9.1-1.0~u16.04+mcp10
	python-oslo.db	4.33.2-1.0~u16.04+mcp10	4.33.4-1.0~u16.04+mcp8
	python-oslo.policy	1.33.2-1.0~u16.04+mcp5	1.33.2-1.0~u16.04+mcp6
	python-taskflow	3.1.0-1.0~u16.04+mcp11	3.1.0-1.0~u16.04+mcp13
	python-vmware-nsxlib	12.0.4-1.0~u16.04+mcp56	12.0.4-1.0~u16.04+mcp59
	stevedore	1:1.28.0-1~u16.04+mcp7	1:1.28.0-1~u16.04+mcp9
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20190620130104-0	4.1~20190723091617-0
	contrail	4.1~20190620130104-0	4.1~20190723091617-0

	contrail-heat	4.1~20190620130104-0	4.1~20190723091617-0
	contrail-vrouter-dpdk	4.1~20190620130104	4.1~20190723091617
	contrail-web-controller	4.1~20190620130104-0	4.1~20190723091617-0
	contrail-web-core	4.1~20190620130104-0	4.1~20190723091617-0
	neutron-plugin-contrail	4.1~20190620130104-0	4.1~20190723091617-0
Salt formulas	salt-formula-aodh	0.2+201905231515.94a8409~xenial1	0.2+201908021613.5563c27~xenial1
	salt-formula-apache	0.2+201905311132.7890680~xenial1	0.2+201908091710.7e3a90f~xenial1
	salt-formula-auditd	0.1+201811291017.11b2d65~xenial1	0.1+201907181609.edad457~xenial1
	salt-formula-backupninja	0.2+201903221820.d4edf22~xenial1	0.2+201907311426.26e6d9a~xenial1
	salt-formula-barbican	2018.1+201906201241.0decab0~xenial1	2018.1+201908091203.bcadfba~xenial1
	salt-formula-cassandra	0.1+201902071030.452ea5a~xenial1	0.1+201907151245.95ff7b7~xenial1
	salt-formula-ceilometer	2016.12.1+201905240824.04a4e57~xenial1	2016.12.1+201908021625.122d9a0~xenial1
	salt-formula-ceph	0.1+201906211030.d55d5da~xenial1	0.1+201908091302.e7208c2~xenial1
	salt-formula-cinder	2016.12.1+201905222058.690c239~xenial1	2016.12.1+201907311843.aca0d9f~xenial1
	salt-formula-designate	2016.12.1+201905262031.4f886d8~xenial1	2016.12.1+201908051616.5d0b0d2~xenial1
	salt-formula-dogtag	0.1+201812171734.dae55d8~xenial1	0.1+201907311641.230a470~xenial1
	salt-formula-elasticsearch	0.2+201906240959.c9a425c~xenial1	0.2+201908021521.7c08c15~xenial1
	salt-formula-galera	1.0+201901161136.1a7d685~xenial1	1.0+201908010831.fc18d6b~xenial1

	salt-formula-gerrit	2017.2+201905280825.0525c11~xenial1	2017.2+201907151001.27a1cc3~xenial1
	salt-formula-glance	2016.12.1+201905211426.ed99e33~xenial1	2016.12.1+201907311658.1de518d~xenial1
	salt-formula-glusterfs	2017.3+201905311341.b8054b0~xenial1	2017.3+201907311451.40cec03~xenial1
	salt-formula-gnocchi	2018.1+201905240806.d51fa27~xenial1	2018.1+201908080856.5f44a07~xenial1
	salt-formula-haproxy	0.2+201905210701.8033bf0~xenial1	0.2+201907311337.8a8b420~xenial1
	salt-formula-heat	2016.12.1+201905222032.5358e48~xenial1	2016.12.1+201907311650.4efd963~xenial1
	salt-formula-horizon	2016.12.1+201905280832.59bcfec~xenial1	2016.12.1+20190721216.7c3e253~xenial1
	salt-formula-jenkins	2017.8+201905211005.e7925af~xenial1	2017.8+201908051430.bfcd953~xenial1
	salt-formula-keystone	2016.12.1+201905281148.ef7061b~xenial1	2016.12.1+201907311659.0ae2333~xenial1
	salt-formula-linux	2017.4.1+201905281653.c37bd4a~xenial1	2017.4.1+201907311654.987ee9a~xenial1
	salt-formula-logrotate	0.1+201811221327.5bea83e~xenial1	0.1+201907311335.7cdf15a~xenial1
	salt-formula-maas	0.0.1+201904041109.bc421d5~xenial1	0.0.1+201908121804.d7522b3~xenial1
	salt-formula-manila	2017.6+201905241158.7df23f4~xenial1	2017.6+201907080944.d846ee2~xenial1
	salt-formula-mongodb	0.2+201902011526.147fde7~xenial1	0.2+201908021518.fdde3e3~xenial1
	salt-formula-neutron	2016.12.1+201906201052.5d63a3e~xenial1	2016.12.1+201907311854.80b9289~xenial1
	salt-formula-nginx	0.2+201905231631.3000e27~xenial1	0.2+201907311432.8eee166~xenial1

	salt-formula-nova	2016.12.1+201905281512.ac2b347~xenial1	2016.12.1+201907311830.98980e8~xenial1
	salt-formula-octavia	2017.6+201905281144.09c4ac6~xenial1	2017.6+201908050949.35c0953~xenial1
	salt-formula-opencontrail	0.2+201905281026.26cf840~xenial1	0.2+201907191135.26bdf2d~xenial1
	salt-formula-postgresql	2017.4+201811221328.6c1d417~xenial1	2017.4+201907311422.6b2c74b~xenial1
	salt-formula-prometheus	0.1+201906251548.b291d2b~xenial1	0.1+201907111546.2c18561~xenial1
	salt-formula-rabbitmq	0.2+201905222031.efe0645~xenial1	0.2+201908010825.c9b2b7f~xenial1
	salt-formula-redis	0.2+201811141313.60f7927~xenial1	0.2+201908021516.f5478ee~xenial1
	salt-formula-runtest	0.1+201906071047.4ab6a8b~xenial1	0.1+201907190925.ab45b4c~xenial1
	salt-formula-salt	0.4+201904171311.0db1ad5~xenial1	0.4+201908011504.028077c~xenial1
	salt-formula-telegraf	0.1+201906131005.8ae18ef~xenial1	0.1+201908021517.b21fffc~xenial1
	salt-formula-xtrabackup	0.2+201906240954.38bd119~xenial1	0.2+201908091632.e95661a~xenial1
Extra packages	apache2	2.4.18-2ubuntu3.10	2.4.18-2.3.10~u16.04+mcp1
	keepalived	1:1.3.9-1.0.18.04.1~u16.04+mcp	1:1.3.9-1.0.18.04.2~u16.04+mcp1
	openscap	1.2.17-2~u16.04+mcp3	1.2.17-2~u16.04+mcp6
	postgresql-9.6	n/a	9.6.13-0+deb9u1
	prometheus-relay	0.3-1~u16.04+mcp0	0.3-1~u16.04+mcp2
	telegraf	1:1.9.1-3~u16.04+mcp44	1:1.9.1-3~u16.04+mcp45
	xccdf-benchmarks	1.0.2-1~u16.04+mcp1	1.1.1-1~u16.04+mcp1

Note

All 2019.2.5 packages are available at <http://mirror.mirantis.com/update/2019.2.0/>.

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

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> 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. 3. Optional. Recommended. MCP Operations Guide: Configure Audit logging in Jenkins. 4. Optional. MCP Operations Guide: Enable HTTPS access from Jenkins to Gerrit. 5. Optional. MCP Operations Guide: Configure Jenkins SSH slaves instead of JNLP. 6. Optional. MCP Operations Guide: Configure audit logging in Gerrit.
2	OpenContrail	<ol style="list-style-type: none"> 1. Update the OpenContrail packages as described in MCP Operations Guide: Update the OpenContrail 4.x nodes. 2. Optional. Enable SSL for an OpenContrail API internal endpoint.

3	OpenStack	<ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • MCP Operations Guide: Apply security updates using Jenkins • MCP Operations Guide: Apply security updates manually

Seealso

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 SaltStack 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:

- CVP - 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 backend 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

Learn more

[MCP Deployment Guide: Enable libvirt control channel over TLS](#)

RabbitMQ upgrade and update

Implemented the Deploy - upgrade RabbitMQ server Jenkins 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](#)

Seealso

[mu4-deprecation](#)

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](#)
- [OVSIInstanceArpingCheckDown 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](#)
 - [OVSIInstanceArpingCheckDown](#)
 - [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:

```
- system.docker.swarm.stack.monitoring.remote_collector
```

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

Note

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

- [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 'l@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 ConnectionForced: 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 keystonecv3, keystonecv 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 keystonecv3.
- [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 backend:
 - 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 backend 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 backend 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 backend 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 'l@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 backend snapshot mechanism

Pike, Queens

Added support for the Ceph backend snapshotting mechanism to the Nova VM live snapshotting feature on the OpenStack environments with Ceph backend 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:

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

3. In `classes/cluster/<cluster_name>/openstack/compute/init.yml`, add the following parameter:

```
nova:  
  compute:  
    workaround:  
      disable_libvirt_livesnapshot: False
```

4. Apply the changes:

```
salt -C '@glance:server' state.sls glance.server  
salt -C '@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:

```
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:

```
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 'l@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 keyspaces 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.tpl` 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:

```
salt -C 'l@grafana:client' 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:

```
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}
```

5. Log in to the Salt Master node.
6. Apply the following states one by one:

```
salt -C '@docker:swarm and @prometheus:server' state.sls prometheus -b 1
salt -C '@salt:minion' state.sls salt.minion.cert -b 50%
```

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:

```
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:

```
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:

```
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 states:

```
salt -C "l@ceph:mon" state.sls ceph.backup
salt "cfg01*" state.sls reclass.storage
```

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 "l@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:

```
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:

```
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:

```
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:

```
keystone:  
  server:  
    notification:  
      topics: "notifications, stacklight_notificaitons, 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                |
+-----+-----+
| 01a8ab06442a4a0193088e9ce112defa | glance              |
| 06367bc2db6e497694279fc87f1b4b91 | nova                |
| 2f80a6609ab1402abd9257cf0e414c97 | neutron             |
| 4e30f3e7d0a045a29094f5fe684dd955 | heat_domain_admin  |
| 9b575cef6b6744fb853fb6ebedfe41f5 | cinder              |
| b6b3f72daaee4b479a90e0a764d9548e | admin               |
| e8a58ebfacab41318709255be6714439 | barbican            |
| fe9cdd9f456844d194682a4d265679be | heat                |
+-----+-----+
```

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:

```
state.sls salt.minion.ca
```

3. Create the CA file:

```
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

Component	Application/service	2019.2.3	2019.2.4
Stacklight	Alertmanager	0.15.3	0.14.0
	Elasticsearch	5.6.12	6.8.0
	Kibana	5.6.12	6.8.0
DriveTrain	GlusterFS	3.8	5.5

Updated packages from the Mirantis and mirrored repositories

Component	Application/service	2019.2.3	2019.2.4
OpenStack Pike	barbican	1:5.0.1-3~u16.04+m cp9	1:5.0.1-3~u16.04+m cp13

	ceilometer	1:9.0.6-2~u16.04+mcp17	1:9.0.6-2~u16.04+mcp22
	cinder	2:11.2.0-2~u16.04+mcp102	2:11.2.2-2~u16.04+mcp104
	dpdk	17.05.2-1~u16.04+mcp2	17.11.3-4~u16.04+mcp1
	galera-3	n/a	25.3.20-1~u16.04+mcp
	heat	1:9.0.5-1~u16.04+mcp54	1:9.0.7-1~u16.04+mcp44
	horizon	3:12.0.3-4~u16.04+mcp67	3:12.0.4-4~u16.04+mcp69
	ironic	1:9.1.6-1~u16.04+mcp36	1:9.1.6-1~u16.04+mcp49
	libvirt	4.0.0-1.8.5~u16.04+mcp1	4.0.0-1.8.10~u16.04+mcp1
	manila	1:5.0.3-1~u16.04+mcp49	1:5.0.3-1~u16.04+mcp51
	networking-bagpipe	7.0.0-2~u16.04+mcp4	7.0.0-2~u16.04+mcp12
	networking-l2gw	1:11.0.0-1~u16.04+mcp12	1:11.0.0-1~u16.04+mcp17
	networking-odl	1:11.0.0-1~u16.04+mcp60	1:11.0.0-1~u16.04+mcp66
	neutron	2:11.0.6-2~u16.04+mcp201	2:11.0.8-2~u16.04+mcp178
	neutron-fwaas	2:11.0.1-2~u16.04+mcp14	2:11.0.2-2~u16.04+mcp8
	neutron-lbaas	2:11.0.3-1~u16.04+mcp13	2:11.0.3-1~u16.04+mcp15
	nova	2:16.1.7-4~u16.04+mcp165	2:16.1.8-4~u16.04+mcp131
	octavia	1.0.3-6~u16.04+mcp15	1.0.3-7~u16.04+mcp15
	openvswitch	2.8.4-0.0.17.10.1~u16.04+mcp	2.9.0-0.1~u16.04+mcp
	panko	3.1.0-1~u16.04+mcp14	3.1.0-1~u16.04+mcp16

	python-amqp	2.2.1-1~exp1~u16.04+mcp1	2.2.1-1~exp1~u16.04+mcp3
	python-aodhclient	0.9.0-1~u16.04+mcp6	0.9.0-1~u16.04+mcp10
	python-barbicanclient	4.5.3-1.1~u16.04+mcp4	4.5.3-1.1~u16.04+mcp9
	python-castellan	0.12.2-1~u16.04+mcp7	0.12.3-1~u16.04+mcp7
	python-cinderclient	1:3.1.0-1~u16.04+mcp7	1:3.1.1-1~u16.04+mcp4
	python-cliff	2.8.2-1~u16.04+mcp1	2.8.3-1~u16.04+mcp4
	python-glance-store	0.22.0-3~u16.04+mcp4	0.22.0-3~u16.04+mcp7
	python-monascaclient	1.7.1-1~u16.04+mcp2	1.7.1-1~u16.04+mcp6
	python-openstackclient	3.12.1-1~u16.04+mcp12	3.12.2-1~u16.04+mcp12
	python-os-brick	1.15.7-1~u16.04+mcp7	1.15.8-1~u16.04+mcp17
	python-oslo.cache	1.25.1-1~u16.04+mcp6	1.25.2-1~u16.04+mcp7
	python-oslo.context	1:2.17.1-1~u16.04+mcp5	1:2.17.2-1~u16.04+mcp5
	python-oslo.db	4.25.1-3~u16.04+mcp9	4.25.2-3~u16.04+mcp8
	python-oslo.log	3.30.2-1~u16.04+mcp7	3.30.3-1~u16.04+mcp9
	python-oslo.messaging	5.30.7-1~u16.04+mcp15	5.30.8-1~u16.04+mcp18
	python-oslo.privsep	1.22.1-1~u16.04+mcp5	1.22.2-1~u16.04+mcp5
	python-oslo.service	1.25.1-1~u16.04+mcp4	1.25.2-1~u16.04+mcp7
	python-ovsdbapp	0.4.3-1~u16.04+mcp3	0.4.3-1~u16.04+mcp7
	python-vmware-nsxlib	11.0.3-1.0~u16.04+mcp8	11.0.3-1.0~u16.04+mcp10

	qemu	1:2.11+dfsg-1.7.3~u16.04+mcp1	1:2.11+dfsg-1.7.13~u16.04+mcp1
	rabbitmq-server	3.6.15-3~u16.04+mcp1	3.6.15-3~u16.04+mcp2
	vmware-nsx	11.0.2-2~u16.04+mcp36	11.0.2-2~u16.04+mcp42
OpenStack Queens	aodh	6.0.1-2~u16.04+mcp9	6.0.1-2~u16.04+mcp15
	barbican	1:6.0.1-4~u16.04+mcp24	1:6.0.1-5~u16.04+mcp32
	ceilometer	1:10.0.1-2~u16.04+mcp18	1:10.0.1-2~u16.04+mcp30
	cinder	2:12.0.5-2~u16.04+mcp89	2:12.0.7-2~u16.04+mcp100
	designate	1:6.0.1-1.0~u16.04+mcp16	1:6.0.1-1.0~u16.04+mcp22
	galera-3	n/a	25.3.20-1~u16.04+mcp
	glance	2:16.0.1-2~u16.04+mcp23	2:16.0.1-2~u16.04+mcp27
	gnocchi	4.2.4-4~u16.04+mcp8	4.2.4-4~u16.04+mcp12
	heat	1:10.0.2-1.0~u16.04+mcp64	1:10.0.3-1.0~u16.04+mcp59
	heat-dashboard	1.0.2-4~u16.04+mcp5	1.0.3-4~u16.04+mcp6
	horizon	3:13.0.1-10~u16.04+mcp89	3:13.0.2-10~u16.04+mcp74
	horizon-contrail-panels	2:0.1.2-1~u16.04+mcp2	2:0.1.2-1~u16.04+mcp5
	ironic	1:10.1.8-1.0~u16.04+mcp32	1:10.1.8-1.0~u16.04+mcp57
	keystone	2:13.0.2-3~u16.04+mcp19	2:13.0.2-3~u16.04+mcp30
	libvirt	4.0.0-1.8.5~u16.04+mcp1	4.0.0-1.8.10~u16.04+mcp1
	manila	1:6.1.0-2~u16.04+mcp52	1:6.3.0-2~u16.04+mcp47

	manila-ui	2.13.0-1.0~u16.04+mcp11	2.13.1-1.0~u16.04+mcp4
	networking-bagpipe	8.0.1-2~u16.04+mcp	8.0.1-2~u16.04+mcp7
	networking-baremetal	1.0.0-1~u16.04+mcp5	1.0.0-1~u16.04+mcp13
	networking-bgpvpn	8.0.1-1.0~u16.04+mcp7	8.0.1-1.0~u16.04+mcp13
	networking-generic-switch	1.0.0-1~u16.04+mcp	1.0.0-1~u16.04+mcp12
	networking-l2gw	1:12.0.1-1.0~u16.04+mcp10	1:12.0.1-1.0~u16.04+mcp17
	networking-odl	1:12.0.0-1.0~u16.04+mcp39	1:12.0.0-1.0~u16.04+mcp45
	networking-ovn	4.0.3-1.0~u16.04+mcp21	4.0.3-1.0~u16.04+mcp31
	neutron	2:12.0.5-5~u16.04+mcp155	2:12.0.6-5~u16.04+mcp201
	neutron-fwaas	2:12.0.1-1.0~u16.04+mcp6	2:12.0.1-1.0~u16.04+mcp10
	neutron-lbaas	2:12.0.0-2~u16.04+mcp34	2:12.0.0-2~u16.04+mcp50
	nova	2:17.0.9-6~u16.01+mcp189	2:17.0.10-7~u16.01+mcp188
	octavia	2.0.4-6~u16.04+mcp51	2.1.0-7~u16.04+mcp78
	octavia-dashboard	1.0.1-1.3~u16.04+mcp3	1.0.1-1.3~u16.04+mcp9
	openvswitch	2.9.0-0.1~u16.04+mcp	2.9.5-1~u16.04+mcp
	panko	4.0.2-2~u16.04+mcp7	4.0.2-2~u16.04+mcp15
	python-amqp	2.2.1-1~exp1~u16.04+mcp1	2.2.1-1~exp1~u16.04+mcp3
	python-aodhclient	1.0.0-1~u16.04+mcp3	1.0.0-1~u16.04+mcp8
	python-automaton	1.14.0-1.0~u16.04+mcp4	1.14.0-1.0~u16.04+mcp6

	python-barbicanclient	4.6.1-1.0~u16.04+mcp8	4.6.1-1.0~u16.04+mcp12
	python-brick-cinderclient-ext	0.8.0-1~u16.04+mcp8	0.8.0-1~u16.04+mcp10
	python-castellan	0.17.0-1.0~u16.04+mcp8	0.17.0-2.0~u16.04+mcp15
	python-cinderclient	1:3.5.0-1.0~u16.04+mcp5	1:3.5.0-1.0~u16.04+mcp10
	python-cliff	2.11.1-1~u16.04+mcp4	2.11.1-1~u16.04+mcp6
	python-cryptography	2.1.4-1.0~u16.04+mcp1	2.1.4-1.1.2~u16.04+mcp1
	python-debtcollector	1.19.0-0.1~u16.04+mcp5	1.19.0-0.1~u16.04+mcp7
	python-designateclient	2.9.0-1.0~u16.04+mcp4	2.9.0-1.0~u16.04+mcp9
	python-futurist	1.6.0-1.0~u16.04+mcp5	1.6.0-1.0~u16.04+mcp7
	python-glance-store	0.23.0-2~u16.04+mcp6	0.23.0-2~u16.04+mcp13
	python-glanceclient	1:2.10.1-1.0~u16.04+mcp4	1:2.10.1-1.0~u16.04+mcp6
	python-heatclient	1.14.0-1.0~u16.04+mcp6	1.14.1-1.0~u16.04+mcp6
	python-ironic-lib	2.12.2-1.0~u16.04+mcp0	2.12.2-1.0~u16.04+mcp6
	python-ironicclient	2.2.1-1.0~u16.04+mcp6	2.2.2-1.0~u16.04+mcp8
	python-keystoneauth1	3.4.0-1.0~u16.04+mcp12	3.4.0-1.0~u16.04+mcp14
	python-keystoneclient	1:3.15.0-1.0~u16.04+mcp12	1:3.15.0-1.0~u16.04+mcp14
	python-keystonemiddleware	4.21.0-1.0~u16.04+mcp12	4.21.0-1.0~u16.04+mcp17
	python-ldappool	2.2.0-1~u16.04+mcp7	2.2.0-1~u16.04+mcp9
	python-manilaclient	1.21.1-1.0~u16.04+mcp6	1.21.1-1.0~u16.04+mcp23

	python-monascaclient	1.10.0-1.0~u16.04+mcp6	1.10.0-1.0~u16.04+mcp10
	python-neutron-lib	1.13.0-1.0~u16.04+mcp9	1.13.0-1.0~u16.04+mcp11
	python-neutronclient	1:6.7.0-1.0~u16.04+mcp17	1:6.7.0-1.0~u16.04+mcp21
	python-novaclient	2:9.1.1-1~u16.04+mcp6	2:10.1.0-1~u16.04+mcp16
	python-octaviaclient	1.4.0-3~u16.04+mcp11	1.4.0-3~u16.04+mcp11
	python-openstackclient	3.14.3-1.0~u16.04+mcp11	3.14.3-1.0~u16.04+mcp18
	python-openstacksdk	0.11.3+repack-1.0~u16.04+mcp4	0.11.3+repack-1.0~u16.04+mcp8
	python-os-brick	2.3.5-1.0~u16.04+mcp4	2.3.7-1.0~u16.04+mcp8
	python-os-client-config	1.29.0-1.0~u16.04+mcp5	1.29.0-1.0~u16.04+mcp7
	python-os-traits	0.5.0-1.0~u16.04+mcp2	0.5.0-1.0~u16.04+mcp5
	python-os-vif	1.9.0-1.0~u16.04+mcp3	1.9.1-1.0~u16.04+mcp8
	python-osc-lib	1.9.0-1.0~u16.04+mcp4	1.9.0-1.0~u16.04+mcp6
	python-oslo.cache	1.28.0-1.0~u16.04+mcp9	1.28.1-1.0~u16.04+mcp7
	python-oslo.concurrency	3.25.1-1.0~u16.04+mcp3	3.25.1-1.0~u16.04+mcp5
	python-oslo.config	1:5.2.0-1.0~u16.04+mcp7	1:5.2.1-2.0~u16.04+mcp12
	python-oslo.context	1:2.20.0-1.0~u16.04+mcp6	1:2.20.0-1.0~u16.04+mcp8
	python-oslo.db	4.33.1-1.0~u16.04+mcp6	4.33.2-1.0~u16.04+mcp10
	python-oslo.i18n	3.19.0-1.0~u16.04+mcp6	3.19.0-1.0~u16.04+mcp8
	python-oslo.log	3.36.0-1.0~u16.04+mcp8	3.36.0-1.0~u16.04+mcp12

	python-oslo.messaging	5.35.4-2~u16.04+mcp18	5.35.5-2~u16.04+mcp26
	python-oslo.middleware	3.34.0-1.0~u16.04+mcp6	3.34.0-1.0~u16.04+mcp8
	python-oslo.policy	1.33.2-1.0~u16.04+mcp3	1.33.2-1.0~u16.04+mcp5
	python-oslo.privsep	1.27.0-1.0~u16.04+mcp5	1.27.0-1.0~u16.04+mcp7
	python-oslo.reports	1.26.0-1.0~u16.04+mcp6	1.26.0-1.0~u16.04+mcp8
	python-oslo.rootwrap	5.13.0-1.0~u16.04+mcp6	5.13.0-1.0~u16.04+mcp8
	python-oslo.serialization	2.24.0-1.0~u16.04+mcp5	2.24.0-1.0~u16.04+mcp7
	python-oslo.service	1.29.0-1.0~u16.04+mcp5	1.29.0-1.0~u16.04+mcp9
	python-oslo.utils	3.35.1-1.0~u16.04+mcp3	3.35.1-1.0~u16.04+mcp5
	python-oslo.versionedobjects	1.31.3-1.0~u16.04+mcp4	1.31.3-1.0~u16.04+mcp8
	python-ovsdbapp	0.10.3-1.0~u16.04+mcp0	0.10.3-1.0~u16.04+mcp6
	python-pankoclient	0.4.0-1.0~u16.04+mcp9	0.4.1-1.0~u16.04+mcp5
	python-pycadf	2.7.0-1~u16.04+mcp3	2.7.0-1~u16.04+mcp5
	python-swiftclient	1:3.5.0-2~u16.04+mcp	1:3.5.0-2~u16.04+mcp7
	python-taskflow	3.1.0-1.0~u16.04+mcp9	3.1.0-1.0~u16.04+mcp11
	python-tooz	1.60.1-1.0~u16.04+mcp2	1.60.2-1.0~u16.04+mcp2
	python-vmware-nsxlib	12.0.4-1.0~u16.04+mcp40	12.0.4-1.0~u16.04+mcp56
	qemu	1:2.11+dfsg-1.4~u16.04+mcp2	1:2.11+dfsg-1.7.13~u16.04+mcp3
	rabbitmq-server	3.6.15-3~u16.04+mcp1	3.6.15-3~u16.04+mcp2

	ryu	4.15-1~u16.04+mcp2	4.32-1~u16.04+mcp
	stevedore	1:1.28.0-1~u16.04+mcp5	1:1.28.0-1~u16.04+mcp7
	sushy	1.3.3-1~u16.04+mcp0	1.3.3-1~u16.04+mcp4
	tempest	1:18.0.0-1~u16.04+mcp24	1:18.0.0-1~u16.04+mcp26
	vmware-nsx	12.0.2-2~u16.04+mcp171	12.0.2-2~u16.04+mcp238
	websockify	0.8.0+dfsg1-7~u16.04+mcp2	0.8.0+dfsg1-7~u16.04+mcp3
OpenContrail 4.1	ceilometer-plugin-contrail	4.1~20190412052601-0	4.1~20190620130104-0
	contrail	4.1~20190412052601-0	4.1~20190620130104-0
	contrail-heat	4.1~20190412052601-0	4.1~20190620130104-0
	contrail-vrouter-dpdk	4.1~20190412052601	4.1~20190620130104
	contrail-web-controller	4.1~20190412052601-0	4.1~20190620130104-0
	contrail-web-core	4.1~20190412052601-0	4.1~20190620130104-0
	neutron-plugin-contrail	4.1~20190412052601-0	4.1~20190620130104-0
Salt formulas	salt-formula-aodh	0.2+201903281534.817dc54~xenial1	0.2+201905231515.94a8409~xenial1
	salt-formula-apache	0.2+201903280900.0af532a~xenial1	0.2+201905311132.7890680~xenial1
	salt-formula-barbican	2018.1+201903281534.04728ab~xenial1	2018.1+201906201241.0decab0~xenial1
	salt-formula-ceilometer	2016.12.1+201812211452.4a0fcb4~xenial1	2016.12.1+201905240824.04a4e57~xenial1
	salt-formula-ceph	0.1+201903271759.6593ac7~xenial1	0.1+201906211030.d55d5da~xenial1

	salt-formula-cinder	2016.12.1+201903291117.44dff27~xenial1	2016.12.1+201905222058.690c239~xenial1
	salt-formula-designate	2016.12.1+201812211940.9e3f42d~xenial1	2016.12.1+201905262031.4f886d8~xenial1
	salt-formula-docker	0.1+201903271546.54b5fa1~xenial1	0.1+201905211725.b72da1c~xenial1
	salt-formula-elasticsearch	0.2+201812131536.694a03c~xenial1	0.2+201906240959.c9a425c~xenial1
	salt-formula-fluentd	0.1+201811261322.27fb826~xenial1	0.1+201905231626.b551708~xenial1
	salt-formula-gerrit	2017.2+201812201722.9d577c4~xenial1	2017.2+201905280825.0525c11~xenial1
	salt-formula-glance	2016.12.1+201904251442.e763427~xenial1	2016.12.1+201905211426.ed99e33~xenial1
	salt-formula-glusterfs	2017.3+201812211714.d628d64~xenial1	2017.3+201905311341.b8054b0~xenial1
	salt-formula-gnocchi	2018.1+201812171745.a5e9aef~xenial1	2018.1+201905240806.d51fa27~xenial1
	salt-formula-grafana	0.1+201903291208.eaaf37f~xenial1	0.1+201905281140.b39c951~xenial1
	salt-formula-haproxy	0.2+201903291617.e16fc6a~xenial1	0.2+201905210701.8033bf0~xenial1
	salt-formula-heat	2016.12.1+201903281532.e265c38~xenial1	2016.12.1+201905222032.5358e48~xenial1
	salt-formula-horizon	2016.12.1+201903261123.85562ce~xenial1	2016.12.1+201905280832.59bcfec~xenial1
	salt-formula-ironic	0.1+201901091031.086ce5f~xenial1	0.1+201905231618.b711aae~xenial1
	salt-formula-jenkins	2017.8+201812261202.e898ea8~xenial1	2017.8+201905211005.e7925af~xenial1
	salt-formula-keystone	2016.12.1+201904251213.31f7c87~xenial1	2016.12.1+201905281148.ef7061b~xenial1
	salt-formula-kibana	0.2+201812101352.c9f1610~xenial1	0.2+201905210700.658869f~xenial1

	salt-formula-kubernetes	2016.12.1+201904150944.c4db762~xenial1	2016.12.1+201905161140.a80fe43~xenial1
	salt-formula-linux	2017.4.1+201904041309.8c7fecf~xenial1	2017.4.1+201905281653.c37bd4a~xenial1
	salt-formula-manila	2017.6+201903281526.915af54~xenial1	2017.6+201905241158.7df23f4~xenial1
	salt-formula-neutron	2016.12.1+201904251835.18fb9d4~xenial1	2016.12.1+201906201052.5d63a3e~xenial1
	salt-formula-nginx	0.2+201903221825.0c00e83~xenial1	0.2+201905231631.3000e27~xenial1
	salt-formula-nova	2016.12.1+201904251755.ad59244~xenial1	2016.12.1+201905281512.ac2b347~xenial1
	salt-formula-octavia	2017.6+201904231159.ccc5e86~xenial1	2017.6+201905281144.09c4ac6~xenial1
	salt-formula-opencon trail	0.2+201904171048.a270379~xenial1	0.2+201905281026.26cf840~xenial1
	salt-formula-openssh	0.2+201904150940.3635139~xenial1	0.2+201905061452.3cf4cc7~xenial1
	salt-formula-oslo-tem plates	2018.1+201903281325.34893c0~xenial1	2018.1+201905201000.3db8426~xenial1
	salt-formula-panko	2017.6+201812141859.b39496d~xenial1	2017.6+201905241116.68551a1~xenial1
	salt-formula-prometh eus	0.1+201903271541.a1c656e~xenial1	0.1+201906251548.b291d2b_xenial1
	salt-formula-rabbitm q	0.2+201903281326.4b1f769~xenial1	0.2+201905222031.efe0645~xenial1
	salt-formula-runtest	0.1+201904171302.a6a9ff8~xenial1	0.1+201906071047.4ab6a8b~xenial1
	salt-formula-telegraf	0.1+201903221357.f14c88c~xenial1	0.1+201906131005.8ae18ef~xenial1
	salt-formula-xtraback up	0.2+201904051040.e94a4d7~xenial1	0.2+201906240954.38bd119~xenial1
Extra packages	atop	n/a	2.3.0-1~u16.04+mcp
	jmx-exporter	1:0.9-2~u16.04+mcp 21	2:0.3.2-2~u16.04+m cp3

	libvirt-exporter	0.1-1~u16.04+mcp0	0.1-1~u16.04+mcp1
	td-agent-additional-plugins	3.1.3-1~u16.04+mcp2	3.1.5-1~u16.04+mcp1
	telegraf	1:1.9.1-1~u16.04+mcp35	1:1.9.1-3~u16.04+mcp44
	telegraf-builddeps	0.0+git20181221-1	0.0+git20190613-1
	xccdf-benchmarks	0.5.5-1~u16.04+mcp1	1.0.2-1~u16.04+mcp1

Note

All 2019.2.4 packages are available at <http://mirror.mirantis.com/update/2019.2.0/>.

Updated Kubernetes components

Component	Application/service	2019.2.3	2019.2.4
Kubernetes	containernetworking-plugins	0.7.2-173-g8db2808	0.8.0-7-g70fb96e
	external-dns	0.5.11-4	0.5.14-5
	hyperkube	1.13.5-3_1553734030770	1.13.6-4_1559029385616
	hyperkube-amd64	1.13.5-3	1.13.6-4
	nginx-ingress-controller-amd64	nginx-0.23.0-4	nginx-0.24.1-5
	pause-amd64	1.13.5-3	1.13.6-4

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

#	Component	Workflow
1	DriveTrain	<ol style="list-style-type: none"> 1. Update DriveTrain to a minor release version. 2. Perform the steps described in Issues resolutions requiring manual application. 3. Optional. Recommended. Remove anonymous access for Jenkins on the Salt Master node. 4. Optional. Recommended. Remove executors on Jenkins Master. 5. Optional. Recommended. Configure allowed and rejected IP addresses for the GlusterFS volumes.
2	OpenContrail	<ol style="list-style-type: none"> 1. Update the OpenContrail packages as described in Update the OpenContrail 4.x nodes. 2. Optional. Define aging time for flow records.
3	OpenStack	<ol style="list-style-type: none"> 1. Update the OpenStack packages as described in Update OpenStack packages. 2. Perform the steps described in Issues resolutions requiring manual application. 3. Optional. Enable Keystone security compliance policies.
3 · 1	Galera cluster	Update the Galera cluster as described in Update Galera.
3 · 2	RabbitMQ	Update the RabbitMQ component as described in Update RabbitMQ.
4	Kubernetes	Update the Kubernetes packages as described in Update or upgrade Kubernetes.

5	StackLight LMA	<ol style="list-style-type: none"> 1. Update StackLight LMA using the Deploy - upgrade StackLight Jenkins pipeline job as described in Update StackLight LMA. 2. Enable CADF notifications handled by Fluentd. 3. Perform the steps described in Issues resolutions requiring manual application. 4. Enable Prometheus Elasticsearch exporter. 5. Optional. Enable TLS for StackLight LMA.
6	Ceph	<ol style="list-style-type: none"> 1. Update the Ceph packages as described in Update Ceph packages. 2. Perform the steps described in Issues resolutions requiring manual application.
7	Ubuntu Xenial packages	<p>Select from the following options:</p> <ul style="list-style-type: none"> • Apply security updates using Jenkins • Apply security updates manually

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.

Learn more

- [MCP Operations Guide: Perform the data plane networking testing with CVP Shaker](#)

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.

Learn more

- [MCP Operations Guide: Enable FQDN on internal endpoints in the Keystone catalog](#)

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.

Learn more

- [MCP Operations Guide: Expose a hardware RNG device to Nova instances](#)

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.

Learn more

[Kubernetes release notes](#)

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/cidc/control/leader.yml` to add the upmap-based pipeline job:

```
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 backend 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] [Pike, Queens] Fixed the issue causing the `heat_tempest_plugin.tests.functional.test_remote_stack.RemoteStackTest` Tempest test to fail.
- [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:

```
cinder:  
controller:  
  enabled: true  
  osapi:  
  host: 127.0.0.1
```

Eventually, the `cinder:controller` block should look like this:

```
cinder:  
controller:  
  enabled: true
```

3. Log in to the Salt Master node.
4. Refresh the pillars:

```
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:

```
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}`:

```
apache_cinder_api_address: ${_param:cluster_local_address}
```

7. Refresh the pillars and apply the apache state:

```
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 'l@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 'l@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

Note

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

[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:

```
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.

```
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 "!@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:

```
salt -C '@opencontrail:control' cmd.run "sed -i '/^AUTHN_URL.*a insecure = true' /etc/contrail/vnc_api_lib.ini"
```

3. Restart all `contrail-api` workers:

```
salt -C '@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:

```
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:

```
salt -C "l@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:

```
salt -C '@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:

```
salt -C '@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

Component	Application/service	2019.2.2	2019.2.3
DriveTrain	jenkins-master	2.138.3	2.150.3
OpenStack Pike	Cinder	2:11.1.1-2~u16.04+mcp152	2:11.2.0-2~u16.04+mcp102
	Heat	1:9.0.5-1~u16.04+mcp50	1:9.0.5-1~u16.04+mcp54
	Horizon	3:12.0.3-4~u16.04+mcp65	3:12.0.3-4~u16.04+mcp67
	Keystone	2:12.0.1-4~u16.04+mcp16	2:12.0.2-4~u16.04+mcp14
	Manila	1:5.0.2-1~u16.04+mcp40	1:5.0.3-1~u16.04+mcp49
	Nova	2:16.1.7-4~u16.04+mcp149	2:16.1.7-4~u16.04+mcp165
OpenStack Networking Pike	Neutron	2:11.0.6-2~u16.04+mcp185	2:11.0.6-2~u16.04+mcp201
OpenStack Queens	Cinder	2:12.0.5-2~u16.04+mcp77	2:12.0.5-2~u16.04+mcp89

	Heat	1:10.0.2-1.0~u16.04+mcp56	1:10.0.2-1.0~u16.04+mcp64
	Horizon	3:13.0.1-10~u16.04+mcp84	3:13.0.1-10~u16.04+mcp89
	Ironic ^{TechPreview}	1:10.1.7-1.0~u16.04+mcp32	1:10.1.8-1.0~u16.04+mcp32
	Keystone	2:13.0.2-3~u16.04+mcp15	2:13.0.2-3~u16.04+mcp19
	Manila	1:6.0.2-2~u16.04+mcp60	1:6.1.0-2~u16.04+mcp52
	Nova	2:17.0.9-6~u16.01+mcp157	2:17.0.9-6~u16.01+mcp189
OpenStack Networking Queens	Neutron	2:12.0.5-5~u16.04+mcp139	2:12.0.5-5~u16.04+mcp155
Kubernetes	CNI-plugins	0.7.2-151	0.7.2-173
	containerd	1.2.1+1-1~u16.04+mcp	1.2.5-2~u16.04+mcp
	CoreDNS	1.2.6-4	1.4.0
	etcd	3.3.10	3.3.12
	ExternalDNS	0.5.9-3	0.5.11
	Helm	n/a	2.12.2
	Kubernetes	1.12.6	1.13.5
	NGINX Ingress controller	0.21.0-3	0.23.0
	Tiller	n/a	2.12.2
	Virtlet	1.4.4	1.5.0
Distributed storage	Ceph	12.2.8-1~u16.04+mcp142	12.2.11-1 ³⁸
System	Open vSwitch	2.8.0-4~u16.04+mcp1	2.8.4-0.0.17.10.1~u16.04 ³⁹ , 2.9.0-0.1~u16.04 ⁴⁰

³⁸ [Luminous v12.2.11 Release Notes](#)

³⁹ For OpenStack Pike

⁴⁰ For OpenStack Queens

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

#	Component	Workflow
1	DriveTrain	Update DriveTrain to a minor release version.
2	OpenContrail	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Update the Kubernetes packages as described in Update or upgrade Kubernetes. 2. Optional. Enable Helm support.
4	StackLight LMA	<ol style="list-style-type: none"> 1. Optional. Enable SMART disks monitoring using the steps 3-4 in MCP Operations Guide: Enable SMART disk monitoring. 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	<ol style="list-style-type: none"> 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	<p>Select from the following options:</p> <ul style="list-style-type: none"> • Apply security updates using Jenkins • Apply security updates manually

Seealso

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_bgpvpn_precommit method did not match the one for networking-bgpvpn 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+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

Component	Application/service	2019.2.1	2019.2.2
Kubernetes	containerd	1.2.1-1~u16.04+mcp	1.2.1+1-1~u16.04+mcp
	Kubernetes	1.12.4	1.12.6
OpenStack Queens	Barbican	1:6.0.1-4~u16.04+mcp14	1:6.0.1-4~u16.04+mcp24
	Cinder	2:12.0.4-2~u16.04+mcp96	2:12.0.5-2~u16.04+mcp77
	Heat	1:10.0.2-1.0~u16.04+mcp54	1:10.0.2-1.0~u16.04+mcp56
	Horizon	3:13.0.1-10~u16.04+mcp70	3:13.0.1-10~u16.04+mcp84
	Neutron	2:12.0.5-5~u16.04+mcp93	2:12.0.5-5~u16.04+mcp139
	Nova	2:17.0.9-6~u16.01+mcp93	2:17.0.9-6~u16.01+mcp157
	Octavia	2.0.2-6~u16.04+mcp69	2.0.4-6~u16.04+mcp51
OpenStack Pike	L2 Gateway	1:11.0.0-1~u16.04+mcp6	1:11.0.0-1~u16.04+mcp12
	ODL ML2 plugin	1:11.0.0-1~u16.04+mcp58	1:11.0.0-1~u16.04+mcp60
	Neutron	2:11.0.6-2~u16.04+mcp181	2:11.0.6-2~u16.04+mcp185
	Nova	2:16.1.7-4~u16.04+mcp136	2:16.1.7-4~u16.04+mcp149
System	MySQL	5.6.35-0.1~u16.04+mcp2	5.6.41-1~u16.04+mcp1
StackLight LMA	Elasticsearch	6.5.2	5.6.12 ⁴¹
	Kibana	6.5.2	5.6.12 ⁴¹

41(1, 2) For details, see StackLight addressed issues.

2019.2.1

The MCP 2019.2.1 update contains bug fixes for the OpenStack Pike release and is available starting from February, 27.

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 iptables 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/>.

Updated major software components from the Mirantis repositories

Component	Application/service	2019.2.0	2019.2.1
OpenStack Pike	Cinder	2:11.1.1-2~u16.04+mcp140	2:11.1.1-2~u16.04+mcp152
	Heat	1:9.0.5-1~u16.04+mcp43	1:9.0.5-1~u16.04+mcp50

	Horizon	3:12.0.3-3~u16.04+mcp63	3:12.0.3-4~u16.04+mcp65
	Ironic ^{Tech Prev}	1:9.1.6-1~u16.04+mcp31	1:9.1.6-1~u16.04+mcp36
	Nova	2:16.1.7-4~u16.04+mcp114	2:16.1.7-4~u16.04+mcp136
OpenStack Networking Pike	Neutron	2:11.0.6-2~u16.04+mcp146	2:11.0.6-2~u16.04+mcp181