Release Notes

Published

2025-08-19

Release Notes: Contrail Cloud

Engineering
Simplicity

Table of Contents

Introduction

Juniper Networks® Contrail® Cloud is an integrated Telco cloud platform built to run high-performance NFV with always-on reliability, allowing service providers to deliver innovative services with greater agility. Contrail Cloud features Red Hat® OpenStack and Red Hat® Ceph combined with Juniper Networks® Contrail™, thereby bridging dynamic cloud orchestration with highly scalable connectivity. Furthermore, Contrail Cloud leverages AppFormix which has a built-in automation capability powered by machine learning to monitor the cloud infrastructure and VNFs in the most optimal manner, and remediating any potential failures to ensure adherence to service-level agreements (SLAs).

These release notes accompany Release 13.7 of Juniper Networks Contrail Cloud. They describe new features, limitations, known problems, and update procedure.

New and Changed Features in Contrail Cloud Release 13.7

IN THIS SECTION

The features listed in this section are new or changed as of Contrail Cloud Release 13.7.

Product Components

- Contrail Networking Release 1912.L4.1
  - You can research limitations that are resolved with this release at:

    Resolved Issues in Contrail Networking Release 1912.L4.1

    Use your Juniper Support login credentials to view the list. If you do not have a Juniper Support account, you can register for one at https://userregistration.juniper.net/.

- AppFormix Release 3.1.25
    - AppFormix Release Notes are available as part of the software download package.
- Red Hat OpenStack 13 – OpenStack Queens Version (Red Hat CDN sync 3-Jul-2022)
    - RHOSP 13 Release Notes.
- RHEL 7.9–Linux kernel 3.10.0-1160.53 (Red Hat CDN sync 3-Jul-2022)
    - RHEL 7.9 Release Notes.
- Red Hat Ceph Storage 3 (Red Hat CDN sync 3-Jul-2022)
    - Ceph 3.3 Release Notes.

New and Changed Features From Previous Contrail Cloud Releases

IN THIS SECTION

This section contains the new or changed features for the specified Contrail Cloud Release.

New and Changed Features in Contrail Cloud 13.6

The features listed in this section are new as of Contrail Cloud Release 13.6. A brief description of each feature is included.

Product Components

- Contrail Networking Release 1912.L4
  - Contrail Networking 1912.L4 Release Notes.
- AppFormix Release 3.1.25
  - AppFormix Release Notes are available as part of the software download package.
- Red Hat OpenStack 13 (z15)–OpenStack Queens Version (Red Hat CDN sync 25-Mar-2021)
  - RHOSP 13 Release Notes.
- RHEL 7.9–Linux kernel 3.10.0-1160.21.1 (Red Hat CDN sync 25-Mar-2021)
  - RHEL 7.9 Release Notes.
- Red Hat Ceph Storage 3 (Red Hat CDN sync 25-Mar-2021)
  - Ceph 3.3 Release Notes.

Contrail Cloud Tuning

- Optional undercloud tuning in the **config/site.yml** configuration file.

  > **NOTE**: Only advanced users with knowledge of TripleO should change these settings.

  Support for additional tuning of the undercloud to match specific settings and requirements. You may use this extra configuration to modify any TripleO parameter documented by Red Hat. See below for a tuning example:

```
undercloud:
  ...
  extra_config: |
      MistralExecutionFieldSizeLimit: 32768
  #hieradata params for undercloud install
```

```
 extra_hieradata: |
   heat::max_json_body_size: 10000000
   heat::rpc_response_timeout: 1200
   heat::max_template_size: 1500000
```

RabbitMQ

- Using a non-default password with RabbitMQ.

  You may set a non-default password for RabbitMQ in your Contrail Cloud environment.

  Configure your RabbitMQ password in the **config/vault-data.yml** file by replacing the default “`c0ntrail123`” password, as seen below:

```
overcloud:
...
  contrail:
    rabbitmq:
      # contrail rabbitmq user name
      user: "contrail_rabbitmq"
      # contrail rabbitmq user password
      password: "c0ntrail123"
```

New and Changed Features in Contrail Cloud 13.5

The features listed in this section are new as of Contrail Cloud Release 13.5. A brief description of each feature is included.

Product Components

- Contrail Networking Release 1912.L3
  - Contrail Networking 1912.L3 Release Notes.
- AppFormix Release 3.1.20
  - AppFormix Release Notes are available as part of the software download package.
- Red Hat OpenStack 13 (z12)–OpenStack Queens Version (Red Hat CDN sync 8-Aug-2020)

  - RHOSP 13 Release Notes.

- RHEL 7.8–Linux kernel 3.10.0-1127.19.1 (Red Hat CDN sync 8-Aug-2020)

  - RHEL 7.8 Release Notes.

- Red Hat Ceph Storage 3 (Red Hat CDN sync 8-Aug-2020)

  - Ceph 3.3 Release Notes.

OpenStack Security

- SSL configuration in the Contrail Cloud undercloud.

  Support for SSL configuration in the Contrail Cloud undercloud. The SSL configuration allows secure communication from the undercloud to OpenStack services, and enables HTTPS service for the endpoints. IdM integration is supported by modifying the SSL configuration in the Contrail Cloud undercloud.

  SSL configuration in the undercloud can be enabled on existing Contrail Cloud environments.

  For additional OpenStack and Red Hat OpenStack Platform information for deploying with SSL, see :

  - https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/13/html/director_installation_and_usage/appe-ssltls_certificate_configuration

  - https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/13/html/advanced_overcloud_customization/sect-enabling_internal_ssltls_on_the_overcloud

- Barbican

  Barbican for Contrail Cloud can be deployed using the standard deployment procedure. Additional parameters are set as described in the Contrail Cloud sample YAML configuration files.

  Barbican can be enabled on existing Contrail Cloud environments. Modify your **site.yml** configuration file and then re-run the **openstack-deploy.sh** script to enable Barbican.

  The Contrail Cloud Barbican features include:

  - Barbican service enablement and secrets management.

  - Block storage encryption using Linux Unified Key Setup-on-disk-format (LUKS) .

  - Tempest automated testing suite.

  For more information regarding Barbican features, See:

  - https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/13/html/manage_secrets_with_openstack_key_manager/managing_secrets_in_barbican

  - https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/13/html/manage_secrets_with_openstack_key_manager/encrypting_cinder_volumes
  - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/encrypting-block-devices-using-luks_security-hardening

Contrail Networking

- Netronome SmartNIC support - Tech Preview

  Support for Netronome with Red Hat OpenStack Platform Director (RHOSPd) 13 environment. This feature will enable increased packets per second (PPS) capacity of the Contrail vRouter datapath allowing applications to reach their full processing capacity. Additionally, it allows reclaiming of CPU cores from Contrail vRouter off-loading, permitting more VMs and VNFs to be deployed per server.

  This feature is a technology preview and not considered production ready. For a list of limitations, see the Known Behavior section.

  For configuration instructions, see Appendix C: Deploying Netronome SmartNIC of the Contrail Cloud Deployment Guide.

- For a NIC compatibility matrix, see the Contrail Networking NIC Support Table.

New and Changed Features in Contrail Cloud 13.4

The features listed in this section are new as of Contrail Cloud Release 13.4. A brief description of each feature is included.

Product Components

- Contrail Networking Release 1912.L2
  - Contrail Networking 1912.L2 Release Notes.
- AppFormix Release 3.1.18
  - AppFormix Release Notes are available as part of the software download package.
- Red Hat OpenStack 13 (z11)–OpenStack Queens Version (Red Hat CDN sync 18-May-2020)
  - RHOSP 13 Release Notes.
- RHEL 7.8–Linux kernel 3.10.0-1127 (Red Hat CDN sync 18-May-2020)

  - RHEL 7.8 Release Notes.
- Red Hat Ceph Storage 3.3.z4 - 3.3.4 (Red Hat CDN sync 18-May-2020)
  - Ceph 3.3 Release Notes.

OpenStack Storage

- Software RAID.

  Additional disk storage configurations for RAID setup. This feature allows for configuration of software RAID for control host virsh storage pools and supports any RAID configuration.

  A RAID configuration sample can be found in: **/var/lib/contrail_cloud/samples/features/label-disk/site.yml**.

Operations

- Multi-Layer Fencing for HA.

  Fact loading has been changed to allow for multi-layered fencing in Contrail Cloud.

  Multi-layer fencing is for high availability environment (HA) multi-node clusters. Problem nodes can be mitigated by establishing fencing policies. Multi-layer fencing adds an additional level of fail over and can happen at the VM level or the hypervisor level. This allows the fencing to kill incompliant VMs and then target the hypervisor is the problem persists. Thus, When a VM can not be fenced the hypervisor can then be fenced.

  For more information, see: Fencing Configuration.

New and Changed Features in Contrail Cloud 13.3

The features listed in this section are new as of Contrail Cloud Release 13.3. A brief description of each feature is included.

Product Components

- Contrail Networking Release 1912.L1
  - Contrail Networking 1912.L1 Release Notes.
- AppFormix Release 3.1.17

  - AppFormix Release Notes are available as part of the software download package.

- Red Hat OpenStack 13 (z10)–OpenStack Queens Version (Red Hat CDN sync 25-Feb-2020)
  - RHOSP 13 Release Notes.
- RHEL 7.7–Linux 3.10.0-1062.12.1.el7 kernel (Red Hat CDN sync 25-Feb-2020)
  - RHEL 7.7 Release Notes.
- Red Hat Ceph Storage 3.3 (Red Hat CDN sync 25-Feb-2020)
  - Ceph 3.3 Release Notes.

Contrail Networking

- For a NIC compatibility matrix, see the Contrail Networking NIC Support Table.

OpenStack Compute

- Host Aggregate configurations.

  Host Aggregate provides an extra level of abstraction to map different workloads to different groups of compute nodes. Compute deployment can be separated into logical groups based on like hardware or software flavors, or other user defined identifiers. Actions can target certain roles or groups using the metadata from the aggregates, as opposed to actions targeting host-by-host, one-by-one. Aggregates and Availability Zone filters can be used simultaneously for scheduling VMs. Availability Zones are created automatically when the metadata is defined. Aggregate management happens during the post-deployment stage, and allows for easy assignment of additional hosts.

  Host Aggregates can also be used to map different groups of hosts to different Availability Zones. Do note though that a host can be in multiple Aggregates but only reside in one Availability Zone.

  For more information, see Managing Host Aggregates.

OpenStack Storage

- Expanded disk labeling.

  Additional disk label configurations allow a disk device to be referenced by its alias and can be used in other configurations. This allows for reliable and predictive naming of disk devices. This is important because during a reboot the OS can rename a disk and break the current disk mapping.

Operations

- IdM support.

An integrated Identity and Authentication solution for Linux and UNIX networked environments. IdM provides centralized authentication, authorization, and account information by storing data about users, groups, hosts, and other objects necessary to manage the security of a network of hosts. Within Contrail Cloud all overcloud nodes and undercloud VM will be joined to the IdM. All certificates for OpenStack and Contrail will be created and managed by IdM. A one time password (OTP) mechanism is used to join the undercloud to IdM.

For more information, see:

- Red Hat Identity Management
- Contrail Certificate Lifecycle Management

- Contrail Cloud Satellite helper scripts have been changed to use the full activation key.
    - scripts/satellite6cleanup.py and scripts/satellite6hosts.py commands now expect the full activation key name to be provided with the `--user` option.

In-place Update Improvements

- Overall improvements to speedup the update process and reduce overall time required to complete an update.
- The state of the update is maintained to ensure that steps are not repeated for each role. A lockfile is created in the **/home/stack/contrail_cloud_update** directory, on the undercloud VM for this purpose.
- Parallel update is used in the step2 script during the overcloud nodes update.
- Parallel update for compute roles is defined by a serial mechanism.
- Roles can be updated in parallel and nodes within each role are updated sequentially.
- Increased the parameter `DockerPuppetProcessCount` from 3 to 8 to speed up Docker Puppet steps.
- Contrail TripleO Heat Template fix for unexpected reboot of computes in Step 3 of the in-place update.
- Computes can be restarted in step2 of the update process, after a successful update. Update reboot behavior is configured in **config/site.yml**.

New and Changed Features in Contrail Cloud 13.2.1 Maintenance Release

The focus of the maintenance release replaces Contrail containers to address security vulnerabilities (CVE-2019-17267 JTAC case: 2020-0116-0248) and CVE-2019-19919 (JTAC Case: 2020-0116-0087)). RHEL and RHOSP components remain the same for this maintenance release. The in-place update procedure remains the same when upgrading from Contrail Cloud 13.2 to Contrail Cloud 13.2.1.

Contrail Cloud 13.2.1 product components:

- Contrail Networking R1912 containers.

  For more information, see Contrail Networking Release R1912.

- AppFormix Release 3.1.6
- Red Hat OpenStack 13 (z8)–OpenStack Queens Version (Red Hat CDN sync 1-October-2019)
- RHEL 7.7–Linux Kernel Version 3.10.0-1062.1.2.el7.x86_64 (Red Hat CDN sync 1-October-2019)
- Red Hat Ceph Storage 3.2 (Red Hat CDN sync 1-October-2019)

The Contrail Cloud 13.2.1 Release includes the following changes:

- Contrail TripleO Heat Templates.
  - Fix for computes rebooting when using **/scripts/contrail-cloud-upgrade-overcloud-step3.sh** in the in-place update procedure.

    Computes are rebooted only when arguments to the kernel are changed in the templates.
- Contrail Cloud Automation.
  - Data collection fix for **collect_data.sh**.

    `hostname` was changed to use `-s`, and files are now created in the **/tmp/** directory as `contrail` user, not `root`.
  - All needed proxy settings are exported by default at the beginning of the post-deploy script run for satellite registration.
  - Fixes for `organization` and `service user` in Ansible when running a fresh install of Contrail Cloud.

New and Changed Features in Contrail Cloud Release 13.2

The features listed in this section are new as of Contrail Cloud Release 13.2. A brief description of each feature is included.

Product Components

- Contrail Networking Release 1910
- AppFormix Release 3.1.6
- Red Hat OpenStack 13 (z9)–OpenStack Queens Version (Red Hat CDN sync 1-October-2019)
- RHEL 7.7–Linux Kernel Version 3.10.0-1062.1.2.el7.x86_64 (Red Hat CDN sync 1-October-2019)
- Red Hat Ceph Storage 3.2 (Red Hat CDN sync 1-October-2019)

Deployment

- Enhancements to `node-configuration.py`. The script will now verify configuration file syntax and schema. For more information, see Contrail Cloud Deployment Guide.
- AppFormix cleanup no longer requires an overcloud redeploy to provision the AppFormix controller VMs.
- The default memory size has been increased from 24 GB to 32 GB ram for the control, contrail-controller and contrail-analytics-database VMs on the control hosts.

New and Changed Features in Contrail Cloud Release 13.1

The features listed in this section are new as of Contrail Cloud Release 13.1. A brief description of each feature is included.

Product Components

- Contrail Networking Release 1908

- AppFormix Release 3.1.0
- Red Hat OpenStack 13—OpenStack Queens Version (Red Hat CDN sync 5-August-2019)
- RHEL7.6—Linux Kernel Version 3.10.0-957.27.2 (Red Hat CDN sync 5-August-2019)
- Red Hat Ceph Storage 3.2 (Red Hat CDN sync 5-August-2019)

OpenStack Compute

- Multiple compute and storage roles allowed for different physical resources.

  A profile is a homogenous group. A role can use multiple profiles as sub-roles to allow heterogeneous hardware to use the same overcloud role.

Ceph Storage

- Ceph Storage 3.2 support with full support for BlueStore Ceph backend.

  For more information, see BlueStore: Improved performance with Red Hat Ceph Storage 3.2
- Encrypted disk contents for Ceph OSD storage.
- Ceph journal device configuration for legacy filestore.
- RGW for Object Store (Swift/S3) backend.
- Allow pools to be disabled.

  Ceph pools for OpenStack services that are not used can be disabled. As an example in Contrail Cloud, Gnocchi and Ceilometer services are disabled by default.
- External Ceph cluster support.

  Contrail Cloud allows for integration of pre-existing Ceph clusters as opposed to creating a new Ceph cluster for deployment.

OpenStack Networking

- IPv6 supported in the overcloud networks.

  The supported networks are:

  - External
  - Storage
  - StorageMgmt

    - Management

  Networks that do not support IPv6 in the overcloud:

    - ControlPlane
    - InternalAPI
    - Tenant

  For more information, see IPV6 NETWORKING FOR THE OVERCLOUD.

- Multiple subnet support for compute and storage.

  This aligns with Red Hat terminology for a Spine/Leaf Architecture. For more information, see SPINE LEAF NETWORKING.

- Changed the default subnet used for the provisioning and controlplane activities from 192.0.2* to 192.168.213*.

    - Changed subnet default decreases the probability of an IP address already being used.
    - The default can be overridden by the user if necessary.

- Sample configs use Linux bond for OVS bridging in the underlay (as opposed to OVS bond in previous Contrail Cloud releases).

Contrail Networking

- TLS encryption certificate management for Sandesh and XMPP Contrail protocols.

- SR-IOV (coexists with either kernel or DPDK vRouter) support using the new role *ComputeSriov*.

- TSN support.

  A new *ContrailTsn* role was added. TSN is a container running in a separate VM added to the Control Host.

- Custom container settings.

  Custom container settings allows passthrough values to set environment properties for Contrail containers

  For more information, see the sample files in the **samples/features/extra-config/** directory.

- Contrail Command UI Integration.

  Only the UI portion of Contrail Command is added in this release. Other capabilities of Contrail Command will be considered in future releases.

- SDN gateway config with FIPs.

  Using the site.yml file, the user can provision SDN gateway configurations.

  For more information, see the sample files in the **samples/features/provision-sdn-gateway/** directory.

Deployment

- Sensitive information at-rest encryption.

  - Supports Ansible Vault for secure storage of sensitive information. All passwords, keys, and other sensitive information are move to an encrypted vault config file.

  - Root password can be changed.

  - SSH keys can have a passphrase.

  - Certificate CA can be imported.

- Automated deployment of compute and storage in small batches.

  In the event of large deployments, updating the entire set of compute and storage nodes can take a very long time. This can potentially lead to timeout errors and a failed deployment. The user can now configure how many nodes are to be deployed/updated in a single batch. The process will cycle through all the batches until the complete set of compute and storage nodes have been deployed.

- Support for custom post-deploy actions.

  Typical actions include system tuning (CPU performance mode, file system tuning), excluding modules, and more.

  These actions can be defined in the **site.yml** file. Examples are provided in the **samples/features/extra-action/** directory

- UEFI boot support.

  Contrail Cloud 13.1 added support for UEFI. Previous versions only supported legacy PXEboot

- LLDP support on the jump host, control host, and all overcloud roles.

  This allows the user to discover server networking info from the switch or from the server. This information makes troubleshooting initial fabric connectivity easier.

- Root disk specification.

  This can be configured in the **site.yml** file. For more information, see Appendix A of the Contrail Cloud Deployment Guide.

- Node configuration validation tools.

  This is a configuration tool to check that physical resources correctly match roles intended for the nodes. The validation tool allows the user to query properties of nodes and compare the differences between nodes.

  For more information, see the Contrail Cloud Deployment Guide.

- TripleO templates are validated before deployment start.

  An error in a TripleO file can take significant time to be found during deployment. This tool checks generated Heat templates for the most common errors before deployment starts. This is intended to save a significant amount of time should error detection occur.

OpenStack Deployment Enhancements

- Admin password can be configured.

- OpenStack CLI bash autocomplete on the undercloud.

- Post deployment validation with Tempest.

  For more information, see the Contrail Cloud Deployment Guide.

- Undercloud/Overcloud RabbitMQ tuning.

  Contrail Cloud applies best practice values to optimize RabbitMQ configuration. RabbitMQ tuning parameters are exposed in the **site.yml** file.

- LDAP integration for Keystone

  LDAP integration for keystone example configuration can be seen in the **site.yml** file in the **samples/features/ldap-backend-for-keystone-domains/** directory.

Operations

- AppFormix.

  For more information, see AppFormix Documentation.

  - AppFormix is now set as an overcloud role.

  - Enable network topology view.

  - Allow virtual IP for the InternalAPI network.

  - Automation the addition of Contrail Config and Analytics REST API endpoints.

  - AppFormix plugin for HEAT overcloud service.

- Custom plugin support.

New and Changed Features in Contrail Cloud Release 13.0.2

The features listed in this section are new as of Contrail Cloud Release 13.0.2.

- Contrail Networking 5.0.2 is now distributed with Contrail Cloud 13.0.2. Contrail Networking 5.0.2 provides many fixes for issues (especially around DPDK). See the Contrail Networking Release Notes.
- Contrail Cloud is delivered through the Contrail Cloud Repository Satellite. The Contrail Cloud Installer script, activation key, satellite DNS name, and satellite organization information is provided through a request to mailto:contrail_cloud_subscriptions@juniper.net.

New and Changed Features in Contrail Cloud Release 13.0

The features listed in this section are new as of Contrail Cloud Release 13.0.

- Support for Red Hat OpenShift Platform 13 based on OpenStack Queens with container-based deployment.
- Support for containerized Contrail Networking Release 5.0.1.
- Support for AppFormix Release 2.16.6.
- Support for Red Hat Enterprise Linux 7.5.
- A single script **site.sh** can be used to launch the 8 playbooks needed for Contrail Cloud deployment.
- Networking layout is simplified and unified by using the os-net-config syntax and utility.
- Disk layout on control-hosts is simplified and fully configuration driven.
- Configuration has a tree structure which provides better logical organization and allows fine-grained overrides of default values.
- Virtual machine(VM) networking layout is now configured in **control-host-nodes.yaml**.

- Virtual machine **(VM) data traffic was moved from the “InternalAPI” network to the “Tenant” network by default**.
- Service user is changed to “contrail” on control-hosts, appformix-nodes, and jumphost.
- MAC addresses are no longer needed in inventory file.
- Support for predictable node placement for control plane VMs.
- Controller fencing support is automatically enabled on HA environments without user intervention.
- Single root input/output virtualization (SR-IOV) supported as a Beta feature.

Supported Hardware

For a list of validated hardware, please refer to the Networking NIC Support Table and the Contrail Cloud Reference Architecture Guide.

Security Advisories

Contrail Cloud 13.7 is released with a Red Hat content sync of 1 Feb 2022. For Red Hat security advisories and CVE database, see: https://access.redhat.com/security/security-updates/#/security-advisories

You can also use the Red Hat REST API to query the CVE database. Adjust the `before` date in the API to match the Contrail Cloud content sync date.

NOTE: This will return all Red Hat products. Not all Red Hat products returned by the REST API query are distributed, or used by Contrail Cloud.

```
https://access.redhat.com/labs/securitydataapi/cve.json?
after=2019-10-01&cvss3_score=7&before=2022-02-01&severity=important
```

```
https://access.redhat.com/labs/securitydataapi/cve.json?
after=2019-10-01&cvss3_score=7&before=2022-02-01&severity=critical
```

Known Behavior

IN THIS SECTION

This section contains the known behavior and limitations for the specified Contrail Cloud Release.

Known Behaviors for Contrail Cloud Release 13.7

This section contains known behaviors and limitations in Contrail Cloud Release 13.7.

- The following capabilities available in Contrail Networking Release 1912.L4.1 are not supported in Contrail Cloud 13.7:
  - Contrail Fabric Management. For more information on fabric management, see:
    - Contrail Networking Fabric Lifecycle Management Guide
    - Data Center: Contrail Enterprise Multicloud for Fabric Management
  - Contrail Enterprise Multicloud support for AWS and Azure.
  - Contrail Command deployment - only the UI is supported for Contrail Cloud Release 13.7.
- Netronome SmartNIC limitations:
  - CC-648 - Compute node network configuration is reset after reboot.

  - CC-673 - Contrail status does not show Netronome Agilio container status.

  - CC-674 - Restart of nova_compute breaks Netronome Agilio container.

  - CC-675 - Hanging vif interfaces

  - CC-678 - VM instances stuck in BUILD state.

  - CC-680 - Connectivity loss after container restarts

- CC-1060/CEM-21860 - Contrail **tf-tripleo-heat-templates** do not pass the `BarbicanPassword` to the Contrail containers. This results in the Barbican user having the same password as the Keystone admin user.

  Additional configuration parameters can be added to the **config/site.yml** file as a workaround to this issue:

  ```
  overcloud:
    extra_config:
      ComputeDpdkParameters:
        ContrailSettings:
          BARBICAN_PASSWORD: <barbican password (default equal to keystone admin password)>
      ComputeKernelParameters:
        ContrailSettings:
          BARBICAN_PASSWORD: <barbican password (default equal to keystone admin password)>
  ```

Known Behaviors for Contrail Cloud Release 13.6

This section contains known behaviors and limitations in Contrail Cloud Release 13.6.

- The following capabilities available in Contrail Networking Release 1912.L4 are not supported in Contrail Cloud 13.6:

  - Contrail Fabric Management. For more information on fabric management, see:

    - Contrail Networking Fabric Lifecycle Management Guide

    - Data Center: Contrail Enterprise Multicloud for Fabric Management

  - Contrail Enterprise Multicloud support for AWS and Azure.

  - Contrail Command deployment - only the UI is supported for Contrail Cloud Release 13.6.

- Netronome SmartNIC limitations:
    - CC-648 - Compute node network configuration is reset after reboot.
    - CC-673 - Contrail status does not show Netronome Agilio container status.
    - CC-674 - Restart of nova_compute breaks Netronome Agilio container.
    - CC-675 - Hanging vif interfaces
    - CC-678 - VM instances stuck in BUILD state.
    - CC-680 - Connectivity loss after container restarts

Known Behaviors for Contrail Cloud Release 13.5

This section contains known behaviors and limitations in Contrail Cloud Release 13.5.

- The following capabilities available in Contrail Networking Release 1912.L3 are not supported in Contrail Cloud 13.5:
    - Contrail Fabric Management. For more information on fabric management, see:
        - Contrail Networking Fabric Lifecycle Management Guide
        - Data Center: Contrail Enterprise Multicloud for Fabric Management
    - Contrail Enterprise Multicloud support for AWS and Azure.
    - Contrail Command deployment - only the UI is supported for Contrail Cloud Release 13.5.
- Netronome SmartNIC limitations:
    - CC-648 - Compute node network configuration is reset after reboot.
    - CC-673 - Contrail status does not show Netronome Agilio container status.
    - CC-674 - Restart of nova_compute breaks Netronome Agilio container.
    - CC-675 - Hanging vif interfaces
    - CC-678 - VM instances stuck in BUILD state.
    - CC-680 - Connectivity loss after container restarts
- CC-697 - SSL for undercloud integration is not working with IDM supplied certificates.

- CC-589 - Using spine/leaf topology with IDM fails to generate leaf certificates.
  - libvirt certificates are not generated for the leaf internalAPI networks, causing deployment failures.
  - Certificates must be manually pre-allocated in IDM for every resource on leaf internalAPI networks.
- Limited Barbican feature support in Contrail Cloud Release 13.5.

  The Barbican features not included in Release 13.5 are as follows:
  - Horizon plugin for Barbican.
  - Barbican object storage encryption.

Known Behaviors for Contrail Cloud Release 13.4

This section contains known behaviors and limitations in Contrail Cloud Release 13.4.

- The following capabilities available in Contrail Networking Release 1912.L2 are not supported in Contrail Cloud 13.4:
  - Contrail Fabric Management. For more information on fabric management, see:
    - Contrail Networking Fabric Lifecycle Management Guide
    - Data Center: Contrail Enterprise Multicloud for Fabric Management
  - Contrail Enterprise Multicloud support for AWS and Azure.
  - Using Contrail Command for Contrail Cloud deployment.
    - Command UI is supported for Contrail Cloud 13.4 Release, but the deployment capability is not compatible with Contrail Cloud deployment.
- Contrail Cloud 13.4 is released with a Red Hat content sync of 18 May 2020. Resolutions for the following security advisories are not yet available with Contrail Cloud 13.4:
  - CVE-2020-8617 Red Hat CVSS v3 Score - 7.5

- CC-473 - Live migration of VMs is broken and is a known issue in OpenStack Queens. The error was reproduced in a lab environment and was tested with kernel compute to kernel compute, and DPDK compute to DPDK compute. The lab testing produced the error shown below:

  ```
  (overcloud) [stack@undercloud ~]$ openstack server migrate  --live overcloud8wq-
  compkernel1hw0-1.cc13-testbed-1.juniper.net kmod0-vm1Migration pre-check error: Instance has
  an associated NUMA topology. Instance NUMA topologies, including related attributes such as
  CPU pinning, huge page and emulator thread pinning information, are not currently
  recalculated on live migration. See bug #1289064 for more information. (HTTP 400) (Request-
  ID: req-27d8710a-7901-41c9-a801-c0f0b6acc5cf)
  ```

  For more information, see: Red Hat Bugzilla - Bug 1196242, and Launchpad Nova Bug 1289064.

- CC-509 - Open vSwitch (OvS) update on control host nodes causes the network connectivity to break. This issue happens during post-deployment activities of the manual yum update and reboot of the control host.

  A workaround for this issue is to temporarily switch the bridge used for the control plane/ provisioning network to Linux bridge. See the procedure below for the workaround.

  On the Control Host node:

  1. Create a backup copy of the devices used in the Control/Provisioning communication: both bridge and bridge interface.

  2. Apply the following changes:

     a. For the bridged interface you will comment out DEVICETYPE, TYPE, and OVS_BRIDGE. Then you will add TYPE=Ethernet.

     ```
     # DEVICETYPE=ovs
     # TYPE=OVSPort
     # OVS_BRIDGE=br-ens2f0
     TYPE=Ethernet
     ```

     b. For the bridge comment out DEVICETYPE and TYPE. Then you will add TYPE=Bridge.

     ```
     # DEVICETYPE=ovs
     # TYPE=OVSBridge
     TYPE=Bridge
     ```

  3. Use tmux, screen, or nohup to separate command execution from ssh connection status.

The commands below will use nohup to remove OvS bridge and apply the new Linux bridge configuration that was completed in the previous step:

```
nohup sh -c  'ovs-vsctl del-port <BRIDGE_NAME> <INTERFACE>; ovs-vsctl del-br
<BRIDGE_NAME>; ifup <BRIDGE_NAME> sudo ifup <INTERFACE>' &
```

4. Check interfaces status (interfaces should be visible as per Linux bridge configuration).
5. Perform the yum update.
6. Restore the backup that were prepared in the first step.
7. Perform a reboot to reload the kernel and OvS configuration.

Known Behaviors for Contrail Cloud Release 13.3

This section contains known behaviors and limitations in Contrail Cloud Release 13.3.

- The following capabilities available in Contrail Networking Release 1912.L1 are not supported in Contrail Cloud 13.3:
    - Contrail Fabric Management.
    - Public cloud deployment and connectivity.
    - Using Contrail Command for Contrail Cloud deployment.
        - Command UI is supported for Contrail Cloud 13.3 Release, but the deployment capability is not compatible with Contrail Cloud deployment.
    - TLS certificate management using IDM for Contrail Services.
- Contrail Cloud 13.3 is released with a Red Hat content sync of 25 Feb 2020. Resolutions for the following security advisories are not yet available with Contrail Cloud 13.3:
    - CVE-2018-1000076 Red Hat CVSS v3 Score - 5.5
    - CVE-2018-1000078 Red Hat CVSS v3 Score - 6.1
    - CVE-2019-14818 Red Hat CVSS v3 Score - 7.5
    - CVE-2019-15605 Red Hat CVSS v3 Score - 7.1
    - CVE-2020-8597 Red Hat CVSS v3 Score - 9.8

- CC-473 - Live migration of VMs is broken and is a known issue in OpenStack Queens. The error was reproduced in a lab environment and was tested with kernel compute to kernel compute, and DPDK compute to DPDK compute. The lab testing produced the error shown below:

  ```
  (overcloud) [stack@undercloud ~]$ openstack server migrate  --live overcloud8wq-
  compkernel1hw0-1.cc13-testbed-1.juniper.net kmod0-vm1Migration pre-check error: Instance has
  an associated NUMA topology. Instance NUMA topologies, including related attributes such as
  CPU pinning, huge page and emulator thread pinning information, are not currently
  recalculated on live migration. See bug #1289064 for more information. (HTTP 400) (Request-
  ID: req-27d8710a-7901-41c9-a801-c0f0b6acc5cf)
  ```

  For more information, see: Red Hat Bugzilla - Bug 1196242, and Launchpad Nova Bug 1289064.

- CC-509 - Open vSwitch (OvS) update on control host nodes causes the network connectivity to break. This issue happens during post-deployment activities of the manual yum update and reboot of the control host.

  A workaround for this issue is to temporarily switch the bridge used for the control plane/ provisioning network to Linux bridge. See the procedure below for the workaround.

  On the Control Host node:

  1. Create a backup copy of the devices used in the Control/Provisioning communication: both bridge and bridge interface.

  2. Apply the following changes:

     a. For the bridged interface you will comment out DEVICETYPE, TYPE, and OVS_BRIDGE. Then you will add TYPE=Ethernet.

     ```
     # DEVICETYPE=ovs
     # TYPE=OVSPort
     # OVS_BRIDGE=br-ens2f0
     TYPE=Ethernet
     ```

     b. For the bridge comment out DEVICETYPE and TYPE. Then you will add TYPE=Bridge.

     ```
     # DEVICETYPE=ovs
     # TYPE=OVSBridge
     TYPE=Bridge
     ```

  3. Use tmux, screen, or nohup to separate command execution from ssh connection status.

The commands below will use nohup to remove OvS bridge and apply the new Linux bridge configuration that was completed in the previous step:

```
nohup sh -c  'ovs-vsctl del-port <BRIDGE_NAME> <INTERFACE>; ovs-vsctl del-br
<BRIDGE_NAME>; ifup <BRIDGE_NAME> sudo ifup <INTERFACE>' &
```

4. Check interfaces status (interfaces should be visible as per Linux bridge configuration).

5. Perform the yum update.

6. Restore the backup that were prepared in the first step.

7. Perform a reboot to reload the kernel and OvS configuration.

- CC-514 - This issue is seen when updating a non-HA topology from CC13.2 or CC13.2.1 to CC13.3. Previous releases assumed fencing was enabled even when HA was not part of the topology. See below for an example of the error output:

```
TASK [overcloud : Run prepare-update.sh] ***************************************
Thursday 30 April 2020  20:18:15 -0700 (0:00:03.928)       0:05:10.076 ********
fatal: [192.168.122.39]: FAILED! => {"changed": true, "cmd": "source /home/stack/stackrc && /
home/stack/prepare-update.sh", "delta": "0:00:03.140025", "end": "2020-04-30
20:18:19.081609", "failed_when_result": true, "msg": "non-zero return code", "rc": 1,
"start": ...
... "Error: The following files were not found: /home/stack/tripleo-heat-templates/
environments/fencing.yaml"]}
```

  Use the CLI input below as a workaround for non-HA updates from CC13.2/CC13.2.1 to CC13.3:

```
sed -i '/^fencing/d' /var/lib/contrail_cloud/facts.d/overcloud.fact
```

Known Behaviors for Contrail Cloud Release 13.2

This section contains known behaviors and limitations in Contrail Cloud Release 13.2.

- The following capabilities available in Contrail Networking Release 1910 are not supported in Contrail Cloud 13.2:

  - Contrail Fabric Management.

  - Public Cloud.
  - Contrail Command Deployment–only the UI is supported for Contrail Cloud 13.2 release.
  - TLS certificate management using IDM for Contrail Services.
- Contrail Cloud 13.2 is released with a Red Hat content sync of 1 Oct 2019. Resolutions for the following security advisories are not yet available with Contrail Cloud 13.2:
  - CVE-2018-1102 Red Hat CVSS v3 Score - 9.9
  - CVE-2018-1002105 Red Hat CVSS v3 Score - 9.8
  - CVE-2019-6778 Red Hat CVSS v3 Score - 7.8
  - CVE-2018-14632 Red Hat CVSS v3 Score - 7.7
  - CVE-2018-20815 Red Hat CVSS v3 Score - 7.0
  - CVE-2018-1127 Red Hat CVSS v3 Score - 4.2
- The deployment of Contrail Command requires connectivity to an external package repository outside of the Contrail Cloud Satellite.
- Setting Linux bridges with DHCP causes race conditions with the underlying bridge interfaces.
- Ceph Pools PGs and replica sets are not updated. After Ceph changes (new OSDs or change in the replicas) TripleO will not make adjustments. These changes must be manually applied post-deployment.
- *ceph-osd fsid* mismatch on redeployed environment due to use of legacy filestore.
  - Cleaning done by Ironic during openstack-deploy-cleanup does not bring osd disk to a usable state.
  - Legacy filestore should not be used. BlueStore with LVM is the recommended approach.
  - For more information, see: Ceph Issue #22354 and Red Hat Bugzilla #1590526.
- Exception is raised when rabbitmq-client tries to delete a queue for which parameters have changed. The following might display when you run `contrail-status` on the Control nodes:

```
control: initializing (Number of connections:2, Expected:3 Missing: Database:Cassandra, IFMap
Server End-Of-RIB not computed, No BGP configuration for self)
```

- Identify the stuck queues by locating which one *<queue_name>* has a large number of messages. To generate the list:

  ```
  sudo docker exec -it contrail_config_rabbitmq rabbitmqctl list_queues | egrep "control|
  collector"
  ```

  Purge each problematic queue by running:

  ```
  sudo docker exec -it contrail_config_rabbitmq rabbitmqctl purge_queue <queue_name>
  ```

  Verify the problem has been fixed by running `contrail-status` on the Control node.

  It might be necessary to restart the RabbitMQ container to fix the issue. To restart the RabbitMQ container:

  ```
  docker restart contrail_config_rabbitmq
  ```

Known Behaviors for Contrail Cloud Release 13.1

This section contains known behaviors and limitations in Contrail Cloud Release 13.1.

- The following capabilities available in Contrail Networking Release 1908 are not supported in Contrail Cloud 13.1:

  - Contrail Fabric Management.

  - Public Cloud.

  - Contrail Command Deployment–only the UI is supported for Contrail Cloud 13.1 release.

  - TLS certificate management using IDM for Contrail Services.

- Contrail Cloud 13.1 is released with a Red Hat content sync of 5-August-2019. The following security advisories were introduced after this date and not included in Contrail Cloud 13.1:

  - RHSA-2019:2002 - Security Advisory.

  - RHSA-2019:2411 - Security Advisory.

  - RHSA-2019:2425 - Security Advisory.

  - RHSA-2019:2029 - Security Advisory.

- Linux bridges can only be configured with static IP.

- *ceph-osd fsid* mismatch on redeployed environment.

  - Cleaning done by Ironic during `openstack-deploy-cleanup` does not bring osd disk to a usable state.

  - BlueStore with LVM is the preferred approach.

  - For more information, see: Ceph Issue #22354 and Red Hat Bugzilla #1590526.

- Ceph Pools PGs and replica sets are not updated. After Ceph changes (new OSDs or change in the replicas) TripleO will not make adjustments. These changes must be manually applied post-deployment.

- Running the `overcloud-validation.sh` script will create objects that are not subsequently cleaned up after the test completes. You must manually remove any remaining objects after the overcloud-validation script completes.

Known Behaviors for Contrail Cloud Release 13.0.2

This section contains known behaviors and limitations in Contrail Cloud Release 13.0.2.

- Only the first element of the **global.ntp** list in **config/site.yml** is used when setting up NTP synchronization in the infrastructure. This entry must be reachable and a fully functional NTP server. The full list is utilized in the overcloud.

- The **samples/site.yml** incorrectly shows the **overcloud.registry**. This should be commented in the deployment **config/site.yml**.

Known Behaviors for Contrail Cloud Release 13.0

This section contains known behaviors and limitations in Contrail Cloud Release 13.0.

- Object storage for Ceph—Rados Gateway is not functional when `ceph.support` is set to enabled.

- Contrail Cloud Release 13 configures only endpoint TLS encryption but not internal Contrail TLS.

Update Instructions

IN THIS SECTION

Instructions for upgrading your Contrail Cloud to the specified release.

Update Your Contrail Cloud to the Current Release

NOTE: Juniper supports a n+1 update path for releases. This procedure remains unchanged and supports update to 13.7.

This is an in place update as defined by RHOSP TripleO model. You now have the option to run a parallel update of roles to complete this update procedure. You must follow a reboot process following the update, if the nodes were not rebooted automatically.

No deployment configurations are required when updating. If deployment configuration changes must be made for any reason, they must be applied to your existing Contrail Cloud deployment before updating to the current version. As a best practice, it is always good to review your configuration files to make sure they adhere to a proper schema and the needs of your deployment environment.

The Contrail Cloud update procedure allows for fine-grained control of the update process. Control of the update process is expressed through configurations in the update plan found in the **config/site.yml** file.

Before You Update

Take these initial steps before starting your Contrail Cloud Update. This will help eliminate possible errors that might occur during the update process and will help ensure expected results. The sections below are a prerequisite to the update of your Contrail Cloud.

Review Your Configuration Files

At this point you want to review your current setup to ensure all configuration settings are accurate and reflect a desired deployment for your Contrail Cloud environment.

- Review all the YAML files in the **/var/lib/contrail_cloud/config** directory and ensure all values match your expected results.

  Compare the old configs against the new Contrail Cloud config schema to check for gaps. To check that the configs are compatible, run:

  ```
  /var/lib/contrail_cloud/scripts/node-configuration.py schema
  ```

Verify Undercloud/Overcloud Health and Service Operations

It is vital that you always check the health of your cloud and the services running in your cloud before attempting any deployment or update activities. You must ensure that the undercloud/overcloud is fully functional, healthy, and that all services are active. Any problems in your cloud health may cause errors during updating. Incorrect settings and configurations will carry over to the updated Contrail Cloud deployment.

1. Check the health of the undercloud, overcloud and the nodes running on them. To verify the health of your cloud and the services, see Node Reboot and Health Check and refer to the “Verify Quorum and Node Health section” in the document.

Back Up Your Undercloud and Overcloud

Make sure to back up your undercloud and overcloud before running the update script. For complete instructions to back up your cloud, see BACK UP AND RESTORE THE DIRECTOR UNDERCLOUD, Backing up the overcloud control plane services, and Backing up Contrail Databases in JSON Format.

Pause and Shutdown Business Services

You must pause or shutdown external business services at this time to ensure a smooth update while preventing possible data loss or workload errors. These business services can include the scope of anything outside of the Contrail Cloud deployment but interacts with Contrail Cloud as a whole. The steps to complete the tasks below are dependent on the specific business service/VM that is running. Please consult the documentation for the specific service you need to pause/shutdown.

- Quiesce all external API requests, for example, Horizon.

- Gracefully shutdown any vulnerable workloads.

- You will want to consider migrating your services/VMs to a different cloud that is outside of the update environment.

Review the Configuration Options

The sample below shows the update configuration options in its entirety and is configured in the **site.yml** file. Use this update configuration sample to determine accurate word spacing and indentations within the configuration hierarchy. Come back and reference this sample as needed to assist you through the update process.

```
update_plan:
  # Directory for lockfiles.
  # Consists all lockfiles created during update. Lockfiles are created
  # for each step, batch name, item from nodes_list if update ends with success.
  lockfile_directory: "/home/{{ undercloud['vm']['user'] }}/contrail_cloud_update"
  # Set how many nodes from role will be updated at the same time
  # If dont set serial for custom role (with profile or/and leaf) we will use from basic
  # role: ComputeKernel/ComputeDpdk/ComputeSriov/CephStorage
  serial:
    Controller: 1
    ContrailController: 1
    ContrailAnalytics: 1
    ContrailAnalyticsDatabase: 1
    AppformixController: 1
    ComputeKernel: 25
    ComputeDpdk: 25
    ComputeSriov: 25
    CephStorage: 1
  # can be parallel or sequence or disabled
  reboot_computes: parallel
  batches:
  # unique batch name
  - name: controller_nodes
    # posssible values: `update_type: parallel` or `update_type: sequence`
    # If parallel: batch will be updated in parallel, all positions from list
    # at the same time.
    # If sequence: all positions from batch list will be processed one by one.
    update_type: parallel
    # nodes_list may contain 'all' word or role or node name from ironic.
    # if set 'all' all overcloud nodes will be upgraded role by role.
    # if set 'all' and serial > 1 for role, more than 1 node from role
    # will be processed at the same time.
    # Nodes list can be listed through command executed on undercloud:
    # `. stackrc && openstack server list -f value -c Flavor | sort -u`
    # node_list should consist all role/nodes used in overcloudi.
    # When on node_list will be a specific Compute node name and node role
    # into which specific Compute node belongs it will be:
    # - updated twice, firstly as a node name, secondly as a part of group
    # - rebooted once as node name
    nodes_list:
      - Controller
      - ContrailController
      - ContrailAnalytics
      - ContrailAnalyticsDatabase
      - AppformixController
  - name: ceph_nodes
    update_type: sequence
    nodes_list:
      - overcloudkt0-cephstorage2hw6-0
      - overcloudkt0-cephstorage1hw7-0
      - overcloudkt0-cephstorage0hw6-0
  - name: compute_nodes
    update_type: sequence
    nodes_list:
      - ComputeKernel
      - ComputeDpdk
      - overcloudkt0-compsriov1hw3-0

# during `contrail-cloud-upgrade-overcloud-step2.sh` step:
# - all nodes from `nodes_list` will be reregistered
# - compute nodes from `nodes_list` restarted
# - during each run, only one batch is processed
# - script need to executed multiple times, to process all batches
# - when all batches will be processed, proper lockfile will be created,
#   you can start with step 3 script
```

Start the Contrail Cloud Update

Time to update your Contrail Cloud Release. The process will deliver updated containers, Red Hat RHEL/RHOSP/Storage content, and kernel version that are associated with the chosen release.

The procedure below will guide you through the update. There is a small disruption in service during the update. However, the update preserves existing overcloud configurations. For example: images, projects, networks, volumes, virtual machines, and so on.

Retrieve Adjusted Keys and Install

Follow these steps to start your update:

1. Send an e-mail message to contrail_cloud_subscriptions@juniper.net and request a Contrail Cloud update. Provide the following information:

    - Include your current activation key in the email request. Your Contrail Cloud activation key will be adjusted to the requested version.

    - Specify the time and date you would like to update your Contrail Cloud. The Contrail Cloud team will prepare the activation for your maintenance window.

2. Refresh your Contrail Cloud subscription on the jump host server by running the `contrail_cloud_installer.sh` from the jump host with the arguments:

```
./contrail_cloud_installer.sh \
--satellite_host ${SATELLITE} \
--satellite_key ${SATELLITE_KEY} \
--satellite_org ${SATELLITE_ORG}
```

Update Contrail Cloud

The following procedure and scripts will update your Contrail Cloud.

As the “`contrail`” user (`su - contrail` from root), execute the following scripts on the jump host to perform the update:

1. update the jump host and the undercloud VM.

```
/var/lib/contrail_cloud/scripts/contrail-cloud-update-undercloud.sh
```

   This will:

    - Update the packages and containers on the jump host and the undercloud VM.

    - Update Red Hat OpenStack Platform Director on the undercloud VM.

    - Update image on the undercloud VM used to provision all new overcloud role instances.

        - overcloud-image-full is updated and used to provision any new overcloud role instance.

2. Prepare the overcloud for update:

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-update-overcloud-step1.sh
   ```

   This will:

   - Publish new containers to the registry on the undercloud VM.
   - Update the overcloud plan on the undercloud VM.
   - Prepare the overcloud nodes for update: `openstack overcloud update prepare`.

3. Perform the overcloud update.

   The overcloud update (`contrail-cloud-update-overcloud-step2.sh`) will:

   - Update all nodes as defined in **config/site.yml** using `nodes_list`.
   - Update packages and containers for each node.
   - Update one node batch per script run.
   - Automatically create a lockfile when the batch has been processed.
   - Reboot the compute nodes, unless manually disabled.

   There are different methods that can be used to complete the overcloud update step. The different methods are listed below (choose one):

   - Default method. All nodes will update in one run.
     - All roles are updated one by one.
     - Within each role the nodes are updated one by one.
   - Targeted method. You have the ability to target roles and even nodes to control the update sequence.
     - Ability to set the desired update targets in the **configs/site.yml** file.
     - Typical to update all control plane roles together with this method.
     - Computes can be updated in small targeted groups.

   If you encounter failures while running the `contrail-cloud-update-overcloud-step2.sh` script, see *If an Update Fails* in the sections below.

NOTE: The overcloud update script `contrail-cloud-update-overcloud-step2.sh` has a hard timeout of 4 hours, which may not be sufficient for complex deployments. Consider using targeted updates to allow for incremental role updates which can complete within that timeframe.

Default Method

To update all the nodes using the default method, run the script below. This will update all nodes in one run and require no additional steps. The update will apply to all roles one at a time and one node at a time within each role.

```
/var/lib/contrail_cloud/scripts/contrail-cloud-update-overcloud-step2.sh
```

Targeted Method

The procedure below allows you to target specific roles and nodes during the update. This approach allows for control and predictability of the update and subsequent compute node reboots. This method is desirable if you want to target specific resources to be updated as workloads are migrated. The roles can now be updated in parallel and the nodes within each role can be updated sequentially.

To complete a targeted update, copy and paste the sample plan **samples/features/update-contrail-cloud/site.yml** into your **config.site.yml**. Edit the sample plan to match your deployment for each targeted group and run the update script for each batch defined within the update plan. The step2 script is run multiple times. You will run step2 once for each defined batch in the update plan. Per-node control allows for planning around node reboot. For how to reboot your compute nodes, see Node Reboot and Health Check and refer to the node reboot section.

NOTE: Compute nodes will automatically reboot as part of the update process, unless manually disabled. Select “disabled” for `reboot_computes:` to stop the automated reboots. You will have to follow the manual reboot procedure after the update is complete for updated packages to take effect (e.g., kernel updates).

- Configure the update plan in your **config/site.yml**. Define how many nodes from each role will be updated at the same time:

```
update_plan:

  serial:
    Controller: 1
    ContrailController: 1
    ContrailAnalytics: 1
    ContrailAnalyticsDatabase: 1
    AppformixController: 1
    ComputeKernel: 25
    ComputeDpdk: 25
    ComputeSriov: 25
    CephStorage: 1
```

- Configure the update plan for the desired reboot behavior:

```
update_plan:

  # can be parallel or sequence or disabled
  reboot_computes: parallel
```

- Now define your batches.

  This is where you define your series of batches. You define the roles and nodes that belong to each unique batch. Other batch update characteristics are set here as well. When the update script is run, the script will identify the first unique batch which has not already been executed and updated. A lockfile is created after each successful batch update to identify it as being completed.

  Name the unique batch and configure the update type with a value of either parallel or sequence. The update will be performed in the batch order you configure in your **site.yml** file. You can also target specific nodes you want to update (e.g. computes) by including the node name. To start, you might configure it to look like this:

```
update_plan:

  batches:

  # unique batch name
  - name: controller_nodes
    update_type: parallel
```

- Set the node types in nodes_list. This list belongs to the unique batch name defined above. In this example, this would be all the node types associated with the batch named controller_nodes:

```
update_plan:

  batches:

  # unique batch name
  - name: controller_nodes
    update_type: parallel
    nodes_list:
      - Controller
      - ContrailController
      - ContrailAnalytics
      - ContrailAnalyticsDatabase
      - AppformixController
```

- Define the specific nodes that are unique within the named node role. Below is an example of defining both storage and compute nodes:

```
update_plan:

  batches:

  # unique batch name
  - name: ceph_nodes
    update_type: sequence
    nodes_list:
      - overcloudkt0-cephstorage2hw6-0
      - overcloudkt0-cephstorage1hw7-0
      - overcloudkt0-cephstorage0hw6-0

  # unique batch name
  - name: compute_nodes
    update_type: sequence
    nodes_list:
      - ComputeKernel
      - ComputeDpdk
      - overcloudkt0-compsriov1hw3-0
```

- Run the update script after you have set your variables for each defined batch in the update plan. Rerun the update script until all batches have successfully updated:

  ```
  /var/lib/contrail_cloud/scripts/contrail-cloud-update-overcloud-step2.sh
  ```

4. Converge the overcloud update. The script below will update Ceph and converges the overcloud heat stack. Note, the `overcloud[‘deployment_timeout’]` value in the **config/site.yml** can be increased to avoid timeouts in the Ceph update.

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-update-overcloud-step3.sh
   ```

   This will:

   - Ensure that the stack resource structure aligns with the new packages and configurations.
   - Update the Ceph cluster configuration: `openstack overcloud ceph-upgrade run`.
   - Run update converge: `openstack overcloud update converge`.
   - Finalize the overcloud update.

Move on to the next sections to update AppFormix and Contrail Command.

Update AppFormix

Update AppFormix for use with Contrail Cloud.

1. As the “`contrail`” user (`su - contrail` from root), execute the following script on the jump host to perform the update:

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-update-appformix.sh
   ```

   This will:

   - Update all packages and containers on the AppFormix nodes.

2. Verify the status of AppFormix.

   Run the following command to view the status AppFormix:

   ```
   ansible -i /usr/bin/tripleo-ansible-inventory AppformixController -m shell -a "curl -s http://
   127.0.0.1:9000/appformix/controller/v2.0/status"
   ```

This will return a 200 on success. Any other code returned should be considered a failure. The API output also contains the AppFormix version. This is helpful to verify the correct version has been installed. See the sample below:

```
{ "Version": "2.19.10-65aa34f7ad", "DBVersion": "70" }
```

Update Contrail Command

Update Contrail Command for use with Contrail Cloud.

1. As the "`contrail`" user (`su - contrail` from root), execute the following script on the jump host to perform the update:

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-update-command.sh
   ```

   This will:

   - Update all packages and containers in the Contrail Command VM.

2. Login to the Contrail Command web UI to verify that it was successfully installed. You access Contrail Command by entering **https://<jumphost>:9091** in your browser.

   Review the **/var/lib/contrail_cloud/config/vault-data.yml** for Contrail Command authentication details.

If an Update Fails

If at any point your update fails you will need to troubleshoot. Follow these basic steps for failure analysis:

- Review the failure output and take screenshots. The screenshots will help others review your failure.

- Review your configuration files. There could be mistakes in your YAML configuration files. Some common configuration errors include (but not limited to): NIC setup, role assignment, network assignment, and networking related errors.

- Gather information to help troubleshoot the problem. One common troubleshooting step is to retrieve the log from a failed node. You do this by ssh to the node and check **/var/log/messages**. Use the following sequence of CLI commands:

  1. Log in to the jump host as the `root` user.

  2. `su - contrail`

3. `ssh undercloud`

4. `source stackrc`

5. Run `openstack stack failures list overcloud` to identify any stack failures to help identify which roles are having issues.

   Nothing will return in the CLI if there are no failures to report.

6. `nova list`

7. `ssh <address>`. Use the list generated in step 6 to identify the node you need to ssh to.

8. `sudo vi /var/log/messages` from within the selected node.

- You must bring all services back to health for the failure to be considered corrected.

  Restore the Pacemaker cluster that was stopped as a result of the failed step in the update procedure (`pcs cluster start` on the controller nodes that have it stopped) to bring the cluster back to healthy state.

  Re-run the failed script only when the failure has been corrected and Pacemaker has been started with the cluster healthy again. Move forward with the update procedure only after the failed playbook runs successfully.

You can safely move on to reboot your nodes if you received no failures during the update process.

Remove Duplicate vRouters

It is possible that duplicate instances of the vRouter might occur during the update process, and it is necessary to remove these duplicates. Access the GUI at this point to identify and remove any duplicate vRouters before continuing with the update process.

Reboot Your Nodes

A Contrail Cloud update will introduce a new RHEL image and kernel. You will now need to reboot your nodes if you chose to disable automatic reboots. You will also need to reboot the control plane, control hosts, and storage at this time. Reboot your nodes as described in, Node Reboot and Health Check.

Update from Contrail Cloud Release 13.1 to 13.2

This is an in place update as defined by Red Hat. You will have to update role-by-role and host-by-host to complete this update. You must follow a reboot process following the update.

There are no changes in the configuration YAML files between Contrail Cloud 13.1 and 13.2. Therefore, You don't need configuration changes between Contrail Cloud 13.1 to 13.2. If configuration changes must be made for any reason, they must be applied to your existing Contrail Cloud 13.1 deployment before updating to Version 13.2. As a best practice, it is always good to review your configuration files to make sure they adhere to a proper schema and the needs of your deployment environment.

Before You Update

Take these initial steps before starting your Contrail Cloud update. This will help eliminate possible errors that might occur during the update process and will help ensure expected results. The sections below are a prerequisite to the update of your Contrail Cloud.

Review Your Configuration Files

At this point you want to review your current setup to ensure all configuration settings are accurate and reflect a desired deployment for your Contrail Cloud environment.

- Review all the YAML files in the **/var/lib/contrail_cloud/config** directory and ensure all values match your expected results.

Verify Undercloud/Overcloud Health and Service Operations

It is vital that you always check the health of your cloud and the services running in your cloud before attempting any deployment or update activities. You must ensure that the undercloud/overcloud is fully functional, healthy, and that all services are active. Any problems in your cloud health may cause errors during updating. Incorrect settings and configurations will carry over to the Contrail Cloud 13.2 deployment.

1. Check the health of the undercloud, overcloud and the nodes running on them. To verify the health of your cloud and the services, see Node Reboot and Health Check and refer to the “Verify Quorum and Node Health section” in the document.

Back Up Your Undercloud and Overcloud

Make sure to back up your undercloud and overcloud before running the update script. For complete instructions to back up your cloud, see BACK UP AND RESTORE THE DIRECTOR UNDERCLOUD, Backing up the overcloud control plane services, and Backing up Contrail Databases in JSON Format.

Pause and Shutdown Business Services

You must pause or shutdown external business services at this time to ensure a smooth update while preventing possible data loss or workload errors. These business services can include the scope of anything outside of the Contrail Cloud deployment but interacts with Contrail Cloud as a whole. The steps to complete the tasks below are dependent on the specific business service/VM that is running. Please consult the documentation for the specific service you need to pause/shutdown.

- Quiesce all external API requests, for example, Horizon.
- Gracefully shutdown any vulnerable workloads.
- You will want to consider migrating your services/VMs to a different cloud that is outside of the update environment.

Start the Update from Contrail Cloud Release 13.1 to 13.2

Time to update to Contrail Cloud Release 13.2. Contrail Cloud 13.2 will deliver updated containers, RHEL image and kernel version that are associated with Release 13.2.

The procedure below will guide you through the update. There is a small disruption in service during the update. However, the update preserves existing overcloud configurations. For example: images, projects, networks, volumes, virtual machines, and so on.

Retrieve Adjusted Keys and Install

Follow these steps to start your update:

1. Send an e-mail message to contrail_cloud_subscriptions@juniper.net to request Contrail Cloud 13.2. Provide the following information:

   - Include your current activation key in the email request. Your Contrail Cloud activation key will be adjusted to Version 13.2.
   - Specify the time and date you would like to update your Contrail Cloud version. The Contrail Cloud team will prepare the activation for your maintenance window.

2. Refresh your Contrail Cloud subscription on the jump host server by running the `contrail_cloud_installer.sh` from the jump host with the arguments:

   ```
   ./contrail_cloud_installer.sh \
   --satellite_host ${SATELLITE} \
   --satellite_key ${SATELLITE_KEY} \
   --satellite_org ${SATELLITE_ORG}
   ```

3. Ensure that all overcloud nodes have valid subscription-manager registrations.

Update to Contrail Cloud 13.2

The following procedure and scripts will update your Contrail Cloud to Version 13.2.

As the “`contrail`” user (`su - contrail` from root), execute the following scripts on the jump host to perform the update:

1. Update the jump host and the undercloud VM.

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-undercloud.sh
   ```

2. Prepare the overcloud for update:

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-overcloud-step1.sh
   ```

3. Perform the overcloud update.

   There are two different methods that can be used to complete this step. The different methods are listed below (choose one):

   - Default method. All nodes will update in one run.
     - All roles are updated one by one.
     - Within each role the nodes are updated one by one.
   - Targeted method. You have the ability to target roles and even nodes to control the update sequence.
     - Ability to set the desired update targets in the **configs/site.yml** file.
     - Typical to update all control plane roles together with this method.
     - Computes can be updated in small targeted groups.

   If you encounter failures while running the `contrail-cloud-upgrade-overcloud-step2.sh` script, see *If an Update Fails* in the sections below.

   > **NOTE**: The overcloud update script `contrail-cloud-upgrade-overcloud-step2.sh` has a hard timeout of 4 hours, which may not be sufficient for complex deployments. Consider using targeted updates to allow for incremental role updates which can complete within that timeframe.

   Default Method

To update all the nodes using the default method, run the script below. This will update all nodes in one run and require no additional steps. The update will apply to all roles one at a time and one node at a time within each role.

-
  ```
  /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-overcloud-step2.sh
  ```

Targeted Method

The procedure below allows you to target specific roles and nodes during the update. This approach allows for control and predictability of the update and subsequent compute node reboots. This method is desirable if you want to update the control plane roles at one time, and then target specific compute resources to be updated as workloads are migrated.

To complete a targeted update, just edit your **/config/site.yml** for each targeted group and rerun the update script each time a change is made. This process can be rerun multiple times if necessary. You can use the name of a specific node, or the name of a specific role to update. Just remember to change your **/config/site.yml** with each update. Per-node control allows for planning around node reboot. It may be desirable to reboot compute nodes as they are updated to avoid disruption later. For how to reboot your compute nodes, see Node Reboot and Health Check and refer to the node reboot section.

NOTE: Compute nodes may automatically reboot as part of the update process.

- You need to configure your **/config/site.yml** to reflect the nodes you want updated. The update will be performed in the order you configure in the **site.yml** file. To start, you might configure it to look like this:

  ```
  upgrade:
    nodes_list:
    - Controller
    - ContrailController
    - ContrailAnalytics
    - ContrailAnalyticsDatabase
    - AppformixController
    - CephStorage
  ```

- Run the update script after you have set your variables:

  ```
  /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-overcloud-step2.sh
  ```

- You can now edit your **/config/site.yml** to target the specific nodes you want to update (e.g. computes). Replace the role names with the node names you want to update. Below is an example targeting specific compute nodes to be updated:

  ```
  upgrade:
    nodes_list:
    - overcloudc54-compkernel1hw0-0
    - overcloudc54-compdpdk0hw0-0
  ```

  Run the update script after all variables have been set:

  ```
  /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-overcloud-step2.sh
  ```

You need to create a flag file to mark `contrail-cloud-upgrade-overcloud-step2.sh` as compete once all overcloud nodes have been updated. The flag file is required before running the next update script. Run the following command:

```
ssh undercloud touch /home/stack/.run-contrail-containers-upgrade
```

4. Converge the overcloud update. The script below will update Ceph and converges the overcloud heat stack. Note, the `overcloud[‘deployment_timeout’]` value in the **config/site.yml** can be increased to avoid timeouts in the Ceph update.

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-overcloud-step3.sh
   ```

Move on to the next sections to update your AppFormix and Contrail Command for Contrail Cloud 13.2.

Update AppFormix

Update to the latest version of AppFormix for use with Contrail Cloud 13.2.

1. As the “`contrail`” user (`su - contrail` from root), execute the following script on the jump host to perform the update:

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-appformix.sh
   ```

2. Verify the status of AppFormix.

Run the following command to view the status AppFormix:

```
ansible -i /usr/bin/tripleo-ansible-inventory AppformixController -m shell -a "curl -s http://
127.0.0.1:9000/appformix/controller/v2.0/status"
```

This will return a 200 on success. Any other code returned should be considered a failure. The API output also contains the AppFormix version. This is helpful to verify the correct version has been installed. See the sample below:

```
{ "Version": "2.19.10-65aa34f7ad", "DBVersion": "70" }
```

Update Contrail Command

Update to the latest version of Contrail Command for use with Contrail Cloud 13.2.

1. As the "`contrail`" user (`su - contrail` from root), execute the following script on the jump host to perform the update:

   ```
   /var/lib/contrail_cloud/scripts/contrail-cloud-upgrade-command.sh
   ```

2. Login to the Contrail Command web UI to verify that it was successfully installed. You access Contrail Command by entering **https://<jumphost>:9091** in your browser.

   Review the **/var/lib/contrail_cloud/config/vault-data.yml** for Contrail Command authentication details.

If an Update Fails

If at any point your update fails you will need to troubleshoot. Follow these basic steps for failure analysis:

- Review the failure output and take screenshots. The screenshots will help others review your failure.

- Review your configuration files. There could be mistakes in your YAML configuration files. Some common configuration errors include (but not limited to): NIC setup, role assignment, and networking related errors.

- Gather information to help troubleshoot the problem. One common troubleshooting step is to retrieve the log from a failed node. You do this by ssh to the node and check **/var/log/messages**. Use the following sequence of CLI commands:

  1. Log in to the jump host as the `root` user.

2. `su - contrail`

3. `ssh undercloud`

4. `source stackrc`

5. Run `openstack stack failures list overcloud` to identify any stack failures to help identify which roles are having issues.

   Nothing will return in the CLI if there are no failures to report.

6. `nova list`

7. `ssh <address>`. Use the list generated in step 6 to identify the node you need to ssh to.

8. `sudo vi /var/log/messages` from within the selected node.

- You must bring all services back to health for the failure to be considered corrected.

  Restore the Pacemaker cluster that was stopped as a result of the failed step in the update procedure (`pcs cluster start` on the controller nodes that have it stopped) to bring the cluster back to healthy state.

  Re-run the failed script only when the failure has been corrected and Pacemaker has been started with the cluster healthy again. Move forward with the update procedure only after the failed playbook runs successfully.

You can safely move on to reboot your nodes if you received no failures during the update process.

Remove Duplicate vRouters

It is possible that duplicate instances of the vRouter might occur during the update process, and it is necessary to remove these duplicates. Access the GUI at this point to identify and remove any duplicate vRouters before continuing with the update process.

Reboot Your Nodes

Contrail Cloud 13.2 introduces a new RHEL image and kernel. You need to reboot the nodes as described in, Node Reboot and Health Check.

Update from Contrail Cloud Release 13.02 to 13.1

Contrail Cloud 13.1 does not support an update path from earlier releases. You must redeploy using adjusted activation keys and retrieve new software packages from the Contrail Cloud Satellite.

1. Send a request to mailto:contrail_cloud_subscriptions@juniper.net regarding the adjustment of your Contrail Cloud keys to Version 13.1.

2. Redeploy Contrail Cloud using the adjusted activation keys.

   For more information, see Deploying Contrail Cloud.

Update from Contrail Cloud Release 13.0.1 to 13.0.2

Update to Contrail Cloud Release 13.0.2 to apply the updated containers that are delivered with Contrail Networking 5.0.2. This update restarts each instance of overcloud roles, one-by-one, so there is a small disruption in service during the update. However, the update preserves existing overcloud configurations. For example: images, projects, networks, volumes, virtual machines, and so on.

To update Contrail Cloud to 13.0.2:

1. Ensure that the overcloud is fully functional and that all services are active.

2. Review the **config/site.yml**.

   a. Remove any **overcloud.registry** configuration

   b. Validate that the control host storage allocations use defined storage pools. If the defaults were not used then it might be necessary to adjust the control-host configuration.

3. Review the **config/overcloud-nics.yml**, **config/control-host-nodes.yml**, and **config/appformix-nodes.yml** to rename all instances of `ControlInterfaceDefaultRoute` to `ControlPlaneDefaultRoute`.

4. Send an e-mail message to mailto:contrail_cloud_subscriptions@juniper.net to coordinate the deployment activation key from Contrail Cloud 13.0.1 to Contrail Cloud 13.0.2. An update script **cc-update.sh** is then provided.

5. Download the **cc-update.sh** script to **/var/lib/contrail_cloud/scripts/cc-upgrade.sh** on the jumphost. Make this file executable:

```
sudo chmod +x /var/lib/contrail_cloud/scripts/cc-upgrade.sh; sudo chown contrail /var/lib/
contrail_cloud/scripts/cc-upgrade.sh
```

6. As the “Contrail” user, execute the following script on the jumphost to perform the update:**/var/lib/contrail_cloud/scripts/cc-upgrade.sh**.

Workaround for DPDK Compute Nodes

The update script does not update the **contrail-vrouter-agent-dpdk** container on the DPDK compute nodes.

Use the instructions below to update the Contrail Cloud 13.0.2 DPDK compute nodes:

1. For each DPDK compute node, update **/etc/sysconfig/network-scripts/network-functions-vrouter-dpdk-env** to the following:

```
#!/bin/bash
CONTRAIL_VROUTER_AGENT_DPDK_DOCKER_IMAGE=192.0.2.1:8787/contrail-vrouter-agent
-dpdk:5.0.2-0.360-rhel-queens-13.0.2
#CONTRAIL_VROUTER_AGENT_DPDK_DOCKER_IMAGE=192.0.2.1:8787/contrail-vrouter-age
nt-dpdk:5.0.1-0.214-rhel-queens
CONTRAIL_VROUTER_AGENT_CONTAINER_NAME=contrail-vrouter-agent
CONTRAIL_VROUTER_AGENT_DPDK_CONTAINER_NAME=contrail-vrouter-agent-dpdk
DPDK_UIO_DRIVER=uio_pci_generic
```

2. Restart the vhost0 interface for the changes to take effect.

```
sudo ifdown vhost0
sudo ifup vhost0
```

Workaround for Kernel vRouter Compute Nodes

The update script does not update the **contrail-vrouter-kernel-init** container on the kernel compute nodes.

Use the instructions below to update the Contrail Cloud 13.0.2 kernel vRouter compute nodes:

1. For each kernel vRouter compute node, pull the latest Docker image:

```
docker pull 192.0.2.1:8787/contrail-vrouter-kernel-init:5.0.2-0.360-rhel-queens-13.0.2
```

2. Find the docker image ID:

```
docker images | grep ker | grep 360
192.0.2.1:8787/contrail-vrouter-kernel-init 5.0.2-0.360-rhel-queens-13.0.2 17c02b0e122d
4weeks ago 1.6 GB
```

3. Run the init container:

```
docker run -v /dev:/dev:rw -v /bin:/host/bin:rw -v /lib/modules:/lib/modules:rw -v
/etc/sysconfig/network-scripts:/etc/sysconfig/network-scripts:rw 17c02b0e122d
```

4. Restart the vRouter agent and vhost0 interface:

```
docker stop contrail_vrouter_agent
ifdown vhost0
ifup vhost0
docker start contrail_vrouter_agent
```

5. Reboot to apply the updates:

```
sudo reboot 0
```