



Red Hat OpenStack Platform 13

リリースノート

Red Hat OpenStack Platform 13 リリースの詳細

Red Hat OpenStack Platform 13 リリースノート

[Red Hat OpenStack Platform 13 リリースの詳細](#)

OpenStack Documentation Team
Red Hat Customer Content Services
rhos-docs@redhat.com

法律上の通知

Copyright © 2018 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

本書には、Red Hat OpenStack Platform の主要機能、機能拡張、既知の問題について記載します。

目次

第1章 はじめに	3
1.1. 本リリースについて	3
1.2. 要件	3
1.3. デプロイメント制限事項	3
1.4. データベースサイズの管理	4
1.5. 認定済みのドライバーとプラグイン	4
1.6. 認定済みゲストオペレーティングシステム	4
1.7. BARE METAL PROVISIONING でサポートされているオペレーティングシステム	4
1.8. ハイパーバイザーのサポート	4
1.9. コンテンツ配信ネットワーク (CDN) のリポジトリ	4
1.10. 製品サポート	6
第2章 最も重要な新機能	7
2.1. RED HAT OPENSTACK PLATFORM DIRECTOR	7
2.2. コンテナ	7
2.3. BARE METAL サービス	7
2.4. CEPH STORAGE	7
2.5. COMPUTE	8
2.6. 高可用性	8
2.7. メトリックとモニタリング	9
2.8. ネットワーク機能仮想化	10
2.9. OPENDAYLIGHT	10
2.10. OPENSTACK NETWORKING	10
2.11. セキュリティ	10
2.12. ストレージ	11
2.13. テクノロジープレビュー	12
2.13.1. 新規テクノロジープレビュー	12
2.13.2. 以前にリリースされたテクノロジープレビュー	12
第3章 リリースの情報	15
3.1. RED HAT OPENSTACK PLATFORM 13 GA	15
3.1.1. 機能拡張	15
3.1.2. テクノロジープレビュー	17
3.1.3. リリースノート	17
3.1.4. 既知の問題	20
第4章 テクニカルノート	29
4.1. RHEA-2018:2086 — RED HAT OPENSTACK PLATFORM 13.0 の機能拡張アドバイザリー	29

第1章 はじめに

1.1. 本リリースについて

Red Hat OpenStack Platform の本リリースは、OpenStack「Queens」リリースをベースとしており、Red Hat OpenStack Platform 固有の追加機能や既知の問題、解決済みの問題が含まれています。

本書には、Red Hat OpenStack Platform 固有の変更のみを記載しています。OpenStack「Queens」のリリースノートは、<https://releases.openstack.org/queens/index.html> で参照してください。

Red Hat OpenStack Platform は、他の Red Hat 製品が提供するコンポーネントを使用します。これらのコンポーネントのサポートに関する詳しい情報は、以下のリンクを参照してください。

<https://access.redhat.com/site/support/policy/updates/openstack/platform/>

Red Hat OpenStack Platform を評価するには、以下のリンク先で登録してください。

<http://www.redhat.com/openstack/>.



注記

Red Hat Enterprise Linux High Availability Add-On は、Red Hat OpenStack Platform の各種ユースケースで利用することができます。このアドオンに関する詳細情報は、<http://www.redhat.com/products/enterprise-linux-add-ons/high-availability/> で参照してください。また、Red Hat OpenStack Platform と併用できるパッケージバージョンに関する情報は、<https://access.redhat.com/site/solutions/509783> を参照してください。

1.2. 要件

Red Hat OpenStack Platform は、Red Hat Enterprise Linux の最新リリースをサポートします。Red Hat OpenStack Platform の本バージョンは、Red Hat Enterprise Linux 7.5 でサポートされています。

Red Hat OpenStack Platform の Dashboard は、OpenStack のリソースやサービスを管理することができる Web ベースのインターフェースです。本リリースの Dashboard は、以下の Web ブラウザーの最新安定版をサポートします。

- Chrome
- Firefox
- Firefox ESR
- Internet Explorer 11 以降 (互換モード が無効な場合)



注記

Red Hat OpenStack Platform をデプロイする前には、利用可能なデプロイメントメソッドの特性を考慮することが重要です。詳しくは、「[Installing and Managing Red Hat OpenStack Platform](#)」の記事を参照してください。

1.3. デプロイメント制限事項

Red Hat OpenStack Platform のデプロイメント制限事項の一覧は、「[Deployment Limits for Red Hat OpenStack Platform](#)」の記事を参照してください。

1.4. データベースサイズの管理

Red Hat OpenStack Platform 環境内における MariaDB データベースのサイズの維持管理に関する推奨プラクティスは、[「Database Size Management for Red Hat Enterprise Linux OpenStack Platform」](#)の記事を参照してください。

1.5. 認定済みのドライバーとプラグイン

Red Hat OpenStack Platform の認定済みドライバー/プラグインの一覧は、[「Component, Plug-In, and Driver Support in Red Hat OpenStack Platform」](#)の記事を参照してください。

1.6. 認定済みゲストオペレーティングシステム

Red Hat OpenStack Platform の認定済みゲストオペレーティングシステムの一覧は、[「Certified Guest Operating Systems in Red Hat OpenStack Platform and Red Hat Enterprise Virtualization」](#)の記事を参照してください。

1.7. BARE METAL PROVISIONING でサポートされているオペレーティングシステム

Bare Metal Provisioning (ironic) で、Red Hat OpenStack Platform のベアメタルノードにインストールすることのできるサポート対象のゲストオペレーティングシステムの一覧は、[「Supported Operating Systems Deployable With Bare Metal Provisioning \(ironic\)」](#)の記事を参照してください。

1.8. ハイパーバイザーのサポート

Red Hat OpenStack Platform は、**libvirt** ドライバーと共に使用する (コンピュートノード上で KVM をハイパーバイザーで使用する) 場合にのみサポート対象となります。

Ironic は、Red Hat OpenStack Platform 7 (Kilo) リリースから完全にサポートされています。Ironic により、一般的なテクノロジー (PXE ブートや IPMI) を使用したベアメタルマシンのプロビジョニングが可能となり、多様なハードウェアに対応する一方で、ベンダー固有の機能を追加するためのプラグ可能なドライバーをサポートすることができます。

Red Hat は、非推奨の VMware の「direct-to-ESX」ハイパーバイザーや KVM 以外の libvirt ハイパーバイザーなど、他の Compute 仮想化ドライバーに対するサポートは提供していません。

1.9. コンテンツ配信ネットワーク (CDN) のリポジトリ

本項では、Red Hat OpenStack Platform 13 のデプロイに必要なリポジトリの設定について説明します。

コンテンツ配信ネットワーク (CDN) から Red Hat OpenStack Platform 13 をインストールすることができます。そのためには、正しいリポジトリを使用するように **subscription-manager** を設定します。

CDN リポジトリを有効にするには、以下のコマンドを実行します。

```
#subscription-manager repos --enable=[reponame]
```

CDN リポジトリを無効にするには、以下のコマンドを実行します。


```
#subscription-manager repos --disable=[reponame]
```

表1.1 必須のリポジトリ (x86_64)

リポジトリ名	リポジトリラベル
Red Hat Enterprise Linux 7 Server (RPMS)	rhel-7-server-rpms
Red Hat Enterprise Linux 7 Server - RH Common (RPMS)	rhel-7-server-rh-common-rpms
Red Hat Enterprise Linux High Availability (for RHEL 7 Server)	rhel-ha-for-rhel-7-server-rpms
Red Hat OpenStack Platform 13 for RHEL 7 (RPMS)	rhel-7-server-openstack-13-rpms
Red Hat Enterprise Linux 7 Server - Extras (RPMS)	rhel-7-server-extras-rpms

表1.2 任意のリポジトリ (x86_64)

リポジトリ名	リポジトリラベル
Red Hat Enterprise Linux 7 Server - Optional	rhel-7-server-optional-rpms
Red Hat OpenStack Platform 13 Operational Tools for RHEL 7 (RPMS)	rhel-7-server-openstack-13-optools-rpms

表1.3 必須のリポジトリ (ppc64le)

リポジトリ名	リポジトリラベル
Red Hat Enterprise Linux for IBM Power, little endian	rhel-7-for-power-le-rpms
Red Hat OpenStack Platform 13 for RHEL 7 (RPMS)	rhel-7-server-openstack-13-for-power-le-rpms

無効にするリポジトリ

以下の表には、Red Hat OpenStack Platform 13 が正常に機能するために無効にする必要のあるリポジトリをまとめています。

表1.4 無効にするリポジトリ

リポジトリ名	リポジトリラベル
Red Hat CloudForms Management Engine	"cf-me-"
Red Hat Enterprise Virtualization	"rhel-7-server-rhev"

リポジトリ名	リポジトリラベル
Red Hat Enterprise Linux 7 Server - Extended Update Support	"*-eus-rpms"



警告

Red Hat OpenStack Platform のリポジトリは、Extra Packages for Enterprise Linux (EPEL) ソフトウェアリポジトリで提供されているパッケージと競合する場合があります。EPEL ソフトウェアリポジトリを有効にしているシステムでの Red Hat OpenStack Platform の使用はサポートされていません。

1.10. 製品サポート

以下のリソースをご利用いただけます。

カスタマーポータル

Red Hat カスタマーポータルでは、OpenStack デプロイメントのプランニング、デプロイ、メンテナンスを支援するために、以下のような幅広いリソースを提供しています。

- ナレッジベース記事およびソリューション
- テクニカルブリーフ
- 製品マニュアル
- サポートケース管理

カスタマーポータルには <https://access.redhat.com/> からアクセスしてください。

メーリングリスト

Red Hat は、OpenStack ユーザーに適した公開メーリングリストを提供しています。

- **rhsa-announce** メーリングリストは、Red Hat OpenStack Platform など、全 Red Hat 製品のセキュリティ関連の修正リリースに関する通知を提供します。

<https://www.redhat.com/mailman/listinfo/rhsa-announce> でサブスクライブしてください。

第2章 最も重要な新機能

本項では、Red Hat OpenStack Platform の今回のリリースにおける最も重要な新機能の概要を説明します。

2.1. RED HAT OPENSTACK PLATFORM DIRECTOR

本項では、director の最も重要な新機能について説明します。

Fast Forward Upgrade

director は、**Red Hat OpenStack Platform 10** から **Red Hat OpenStack Platform 13** までの複数のバージョンをアップグレードする専用の **Fast Forward Upgrade** パスを提供しています。この機能は、**ロングライフバージョン** とされている特定の OpenStack のバージョンの使用を継続し、次のロングライフバージョンが提供された際にアップグレードする機会を提供することを目的としています。詳しい手順は、OpenStack Platform 13 リリースの **Fast Forward Upgrades** ガイドに記載しています。

L3 ルーティング対応のリーフ/スパイン型のネットワーク

director には、プロビジョニングとイントロスペクションのために複数のネットワークを定義する機能が搭載されています。この機能は、コンポーザブルネットワークと併せて使用し、ユーザーがオーバークラウド向けの完全な L3 ルーティング対応のリーフ/スパイン型アーキテクチャーをプロビジョニングおよび設定できるようにします。『**Spine Leaf Networking**』ガイドを参照してください。

Red Hat Virtualization のドライバー

director の OpenStack Bare Metal (ironic) サービスには、Red Hat Virtualization 環境内の仮想ノードを管理するためのドライバーが含まれています。これにより、director は Red Hat Virtualization 内にデプロイされたコントローラーノードを使用するオーバークラウドをプロビジョニングおよびサポートすることができます。

2.2. コンテナ

本項では、Red Hat OpenStack Platform のコンテナ化の最も重要な新機能の概要を説明します。

完全にコンテナ化されたサービス

本リリースでは、Red Hat OpenStack Platform の全サービスをコンテナとして提供しています。これには、以前のバージョンではコンテナ化されていなかった OpenStack Networking (neutron)、OpenStack Block Storage (cinder)、OpenStack Shared File Systems (manila) のサービスが含まれます。オーバークラウドは、完全にコンテナ化されたサービスを使用するようになりました。

2.3. BARE METAL サービス

本項では、Bare Metal (ironic) サービスの最も重要な新機能について説明します。

2.4. CEPH STORAGE

本項には、Ceph Storage の最も重要な新機能について説明します。

Red Hat Ceph Storage 3.0 のサポート

本リリースでは、Red Hat OpenStack でサポートされるデフォルトの Ceph バージョンは、Red Hat Ceph Storage 3.0 (luminous) です。director ではこのバージョンがデフォルトでデプロイされます。Ceph では、バージョン 2.x から 3 へのローリングアップグレードがサポートされるようになりました。

た。director を使用して Ceph クラスタをデプロイしていた場合には、OpenStack を新しいリリースにアップグレードすると、Red Hat Ceph Storage も 3.0 にアップグレードされます。

Ceph Metadata Server と RADOS Gateway ノードのスケールアウト

Red Hat Ceph Storage 3.0 では、Ceph File System (CephFS) を適切に設定すると、複数のメタデータサーバー (MDS) にまたがったメタデータロードのスケールアップがサポートされるようになりました。設定が完了すると、Ceph クラスタ内で利用可能な追加の専用 MDS サーバーは、この追加の負荷を処理するように自動的に割り当てられます。また、新しい専用の Ceph RADOS Gateway (RGW) ノードを追加して、RGW を必要に応じてスケールアップすることができます。

NFS を使用する Manila CephFS ストレージ

Shared File System サービス (manila) は、NFSv4 プロトコルを使用した、Ceph File System (CephFS) によってバックアップされる共有ファイルシステムのマウントをサポートしています。コントローラーノード上で稼働する NFS-Ganesha サーバーを使用して、高可用性 (HA) を使用するテナントに CephFS をエクスポートします。テナントは相互に分離され、提供される NFS ゲートウェイインターフェースを介してのみ CephFS にアクセスすることができます。director には、この新機能は完全に統合されているので、CephFS バックエンドのデプロイと Shared File System サービスの設定が可能です。

Cinder Ceph の複数のプールのサポートの強化

Block Storage (cinder) RADOS Block Device (RBD) バックエンドは、director のテンプレートパラメーター **CinderRbdExtraPools** を使用して、同じ Ceph クラスタ内の異なるプールにマッピングすることが可能です。このパラメーターに関連付けられた各 Ceph プールには、**CinderRbdPoolName** パラメーターに関連付けられた標準の RBD バックエンドに加えて、新規 Block Storage RBD バックエンドが作成されます。

ceph-ansible を使用した RBD mirror デモン

Ceph **rbd-mirror** デモンは、リモートクラスタからイメージの更新をプルして、ローカルクラスタ内のイメージに適用します。RBD mirror は、Red Hat Ceph Storage 3.0 (luminous) では **ceph-ansible** を使用するコンテナとしてデプロイされます。イメージに関連する OpenStack のメタデータは、**rbd-mirror** によってはコピーされません。

2.5. COMPUTE

本項では、Compute サービスの最も重要な新機能について説明します。

リアルタイム KVM の統合

リアルタイム KVM (RT-KVM) と Compute サービスの統合が完全にサポートされるようになりました。RT-KVM には、以下のような利点があります。

- システムコールと中断のレイテンシーは決定論的で平均が低い
- ゲストインスタンスでの Precision Time Protocol (PTP) のサポートにより、クロック同期が正確 (本リリースではコミュニティサポート)

2.6. 高可用性

本項では、高可用性の最も重要な新機能について説明します。

director におけるインスタンス HA の統合

director でインスタンスの HA をデプロイできるようになりました。これにより、手動のステップを使用せずにインスタンスの HA のインストールを設定することができます。



注記

director におけるインスタンスの HA の統合は、バージョン 13 以降でのみ利用可能です。以前のバージョンから 13 にアップグレードするには、インスタンスの HA を予め無効にしておく必要があります。

2.7. メトリックとモニタリング

本項では、メトリックおよびモニタリングのコンポーネントの最も重要な新機能および変更点について説明します。

collectd 5.8 の統合

collectd 5.8 バージョンには、以下の追加プラグインが含まれています。

- **ovs-stats**: OVS で接続されたブリッジとインターフェースの統計を収集するプラグイン
- **ovs-events**: Open vSwitch (OVS) で接続されているインターフェースのリンクステータスをモニタリングして、値を **collectd** にディスパッチし、OVS データベースでリンク状態が変更した場合には常に通知を送信するプラグイン
- **hugepages**: プラットフォーム上の未使用および使用済みのヒュージページを数、バイト、パーセンテージでモニタリングする **hugepages** プラグイン
- **intel-rdt**: Cache Monitoring Technology (CMT) や Memory Bandwidth Monitoring (MBM) などの Intel Resource Director Technology (Intel® RDT) のモニタリング機能によって提供される情報を収集する **intel_rdt** プラグイン。この機能により、Last Level Cache (LLC) の占有率、ローカルメモリー帯域幅の使用率、リモートメモリー帯域幅の使用率、Instructions Per Clock (IPC) などの共有リソースの使用状況に関する情報を提供します。
- **libvirt** プラグイン拡張機能: **libvirt** プラグインが拡張され、プラットフォーム上の CMT、MBM、CPU ピニング、使用状況、状態のメトリックをサポートするようになりました。

collectd および gnocchi の統合

collectd-gnocchi プラグインは、gnocchi にメトリックを送信します。デフォルトでは、**collectd** という名前のリソースタイプと、モニタリング対象の各ホスト用の新規リソースを作成します。

各ホストには、以下の命名規則に従って動的に作成されるメトリック一覧があります。

```
plugin-plugin_instance/type-type_instance-value_number
```

メトリックが適切に作成されるようにするには、アーカイブポリシールールが適合することを確認してください。

複数の RabbitMQ サーバーを使用する sensu のサポート

今回のリリースでは、Red Hat OpenStack Platform は、複数の RabbitMQ サーバーを使用する **sensu** をサポートするようになりました。サポートを有効にするには、**config.yaml** ファイルで **MonitoringRabbitCluster** パラメーターを使用する必要があります。

Intel Resource Director Technology/Memory Bandwidth Monitoring のサポート

Memory Bandwidth Monitoring (MBM) は、Intel® Resource Director Technology (RDT) の不可欠な要素です。スケジューリングに関する意思決定を向上させ、SLA を満たすために、メモリーの使用量および空き容量が全ノードから収集されて OpenStack に提供されます。

2.8. ネットワーク機能仮想化

本項では、ネットワーク機能仮想化 (NFV) の最も重要な新機能について説明します。

NFV ワークロード向けのリアルタイム KVM Compute ロール

RT-KVM Compute ノードロールが追加されて、リアルタイム KVM (RT-KVM) Compute ノードが NFV ワークロードをサポートするようになりました。この新しいロールは、リアルタイム機能を備えた Compute ノードのサブセットを公開し、レイテンシーの要件が厳しいゲストをサポートします。

2.9. OPENDAYLIGHT

本項では、OpenDaylight サービスの最も重要な新機能について説明します。

OpenDaylight の統合

OpenDaylight は、柔軟性の高いモジュール型のオープンな SDN プラットフォームで、今回の Red Hat OpenStack Platform リリースでは完全にサポートされるようになりました。現在の Red Hat のオフリングは、OpenDaylight SDN コントローラーを OpenStack のネットワークバックエンドとして有効化するために設計されている、選択された OpenDaylight コンポーネントを慎重に組み合わせています。このソリューションで使用されている OpenDaylight の主要なプロジェクトは NetVirt で、OpenStack neutron API をサポートしています。

詳しい情報は、『[Red Hat OpenDaylight Product Guide](#)』と『[Red Hat OpenDaylight Installation and Configuration Guide](#)』を参照してください。

2.10. OPENSTACK NETWORKING

本項では、Networking サービスの最も重要な新機能について説明します。

Octavia LBaaS

Octavia が完全にサポートされるようになりました。Octavia はロードバランシング機能を提供する OpenStack の公式プロジェクトで、現行の HAProxy ベースの実装を置き換えることを目的としています。Octavia は LBaaS v2 API を実装しますが、追加の機能も提供します。Octavia には、**amphora** (Compute の仮想マシンとして実装される) を使用して、ロードバランシング機能を提供するリファレンスロードバランシングドライバが含まれています。

Open Virtual Network (OVN)

OVN が完全にサポートされるようになりました。OVN とは、Open vSwitch ベースのネットワーク仮想化ソリューションで、インスタンスにネットワークサービスを提供します。OVN は **neutron** API を完全にサポートします。

2.11. セキュリティー

本項では、セキュリティーコンポーネントの最も重要な新機能について説明します。

Barbican

OpenStack Key Manager (barbican) は Red Hat OpenStack Platform のシークレットマネージャーです。barbican API とコマンドラインを使用して、OpenStack サービスの使用する証明書、キー、パスワードを一元管理することができます。

Barbican: 暗号化ボリュームのサポート

barbican を使用して Block Storage (cinder) の暗号化キーを管理することができます。この設定は、LUKS を使用して、インスタンスに接続されているディスク (ブートディスクを含む) を暗号化します。キー管理の機能は、ユーザーに透過的に行われます。

Barbican: glance イメージの署名

Image Service (glance) を設定して、アップロードしたイメージが改ざんされていないことを検証することができます。イメージは、barbican に保管されているキーで最初に署名され、毎回そのイメージを使用する前に検証されます。

Policy Decision Points (PDP) との統合

Policy Decision Points (PDP) に依存してリソースのアクセス制御を行う場合には、Identity Service (keystone) は、認証の確認を行うための外部の PDP とプロジェクトを統合できます。外部の PDP はアクセス要求を評価して、既定のポリシーに基づいてアクセスを許可または拒否することができます。

インフラストラクチャーおよび仮想化の強化

AIDE Intrusion Detection がテクノロジープレビューとして利用できるようになりました。director の AIDE サービスにより、オペレーターは侵入検出のルールセットの設定と、オーバークラウド上での AIDE のインストールと設定を一元的に行うことができます。

2.12. ストレージ

本項では、ストレージコンポーネントの最も重要な新機能について説明します。

Block Storage: コンテナ化された Block Storage サービスのデプロイ

本リリースでは、コンテナ化された Block Storage サービス (cinder) のデプロイメントはデフォルトになりました。外部のインストールに依存するこれらのサービスのバックエンドを使用する場合には、デプロイメント用にベンダー固有のコンテナを取得する必要があります。

Block Storage: マルチバックエンドアベイラビリティゾーン

Block Storage サービス (cinder) では、設定ファイルのバックエンドセクションの **backend_availability_zone** という新しいドライバーの設定オプションを使用して、バックエンドのアベイラビリティゾーンを定義できるようになりました。以前のバージョンでは、cinder ボリュームで定義されたバックエンドは、同じストレージアベイラビリティゾーンの一部である必要がありました。

Block Storage: OpenStack Key Manager のサポート

Block Storage サービス (cinder) は OpenStack Key Manager (barbican) を使用して、ボリュームの暗号化に使用する暗号化キーを保管するようになりました。この機能は、director で OpenStack Key Manager を設定することによって有効化されます。Identity Service (keystone) で admin または creator ロールが割り当てられているユーザーは、新しいキーを OpenStack Key Manager に追加できます。

Block Storage: RBD ドライバーの暗号化サポート

RBD ドライバーは、LUKS を使用した Block Storage サービス (cinder) ボリュームの暗号化をサポートするようになりました。この機能は、Block Storage サービスおよび Compute サービスを使用する RBD 上のボリュームを暗号化する機能を提供し、data-at-rest をセキュリティ保護します。OpenStack Key Manager (barbican) は RBD ドライバーの暗号化を使用する必要があります。RBD ドライバーの暗号化は、Block Storage サービスでのみサポートされています。

Image サービス: イメージの署名と検証のサポート

Image Service (glance) は、OpenStack Key Manager (barbican) を使用してブート可能なイメージの署名および署名検証の機能を提供するようになりました。イメージの署名は、イメージを保管する前に検証されるようになりました。元のイメージを Image サービスにアップロードする前には、暗号化の署名を追加する必要があります。この署名は、イメージのブート時の検証に使用されます。OpenStack Key Manager は署名するキーのキー管理のサポートを提供します。

Object Storage: at-rest encryption と OpenStack Key Manager のサポート

Object Storage (swift) サービスは、OpenStack Key Manager (barbican) に保管される 256 ビットのキーで、AES の CTR モードを使用する暗号化形式でオブジェクトを保管できるようになりました。director を使用して Object Storage の暗号化を有効化した後は、システムは、クラスター内

の全オブジェクトを暗号化するのに使用する単一のキーを作成します。これにより、Object Storage クラスター内のオブジェクトを保護し、セキュリティコンプライアンスを維持するためのオプションが提供されます。

Shared File System: コンテナ化された Shared File System サービスのデプロイメント

本リリースでは、Shared File System サービス (manila) のコンテナ化されたデプロイメントがデフォルトになりました。外部のインストールに依存関係のあるこれらのサービスにバックエンドを使用する場合には、デプロイメントにベンダー固有のコンテナを取得する必要があります。

Shared File System: NetApp ONTAP cDOT ドライバーでの IPv6 アクセスルールのサポート

Shared File System サービス (manila) は、IPv6 ネットワーク上の NetApp ONTAP バックエンドでバックアップされている共有のエクスポートをサポートするようになりました。エクスポートされた共有へのアクセスは、IPv6 クライアントのアドレスによって制御されます。

2.13. テクノロジープレビュー

本項では、Red Hat OpenStack Platform 13 のテクノロジープレビュー機能について説明します。



注記

テクノロジープレビューと記した機能のサポート範囲についての詳しい情報は、「[テクノロジープレビュー機能のサポート範囲](#)」を参照してください。

2.13.1. 新規テクノロジープレビュー

以下の新機能はテクノロジープレビューとして提供されます。

Ansible ベースの設定 (config download)

director は、オーバークラウドのプランに基づいて、Ansible Playbook のセットを生成できます。これより、オーバークラウドの設定方法は、OpenStack Orchestration (heat) から Ansible ベースの方法に変更されます。アップグレードなど、OpenStack Platform 13 でサポートされている一部の機能は、この機能をプロセスの一部として使用します。ただし、このようなサポート対象の領域外の使用は実稼働環境では推奨されません。この機能は、テクノロジープレビューとしてのみ提供しています。

OVS ハードウェアオフロード

Open vSwitch (OVS) のハードウェアオフロードにより、負荷の高いプロセスが SmartNic 搭載のハードウェアに移行されるので、OVS が加速化されます。これにより、OVS の処理が SmartNIC にオフロードされるので、ホストのリソースが節約されます。

2.13.2. 以前にリリースされたテクノロジープレビュー

以下の機能は引き続きテクノロジープレビューとして提供されています。

Benchmarking サービス

Rally は、マルチノードの OpenStack デプロイメント、クラウドの検証、ベンチマーキング、およびプロファイリングを自動化/統合するためのベンチマーキングツールです。SLA、パフォーマンス、および安定性を継続的に向上させる OpenStack CI/CD システム向けの基本ツールとして使用することができます。Rally は、以下のコアコンポーネントで構成されます。

- サーバードライバー: 異なる仮想化テクノロジー (LXS、Virsh など) およびクラウドサプライヤーと対話するための統合インターフェースを提供します。ssh アクセスを介して、1 つの L3 ネットワーク内で対話を行います。

- デプロイエンジン: サーバープロバイダーから取得したサーバーを使用して、ベンチマーキングの手順が実行される前に OpenStack ディストリビューションをデプロイします。
- 検証: デプロイしたクラウドに対して特定のテストセットを実行して正しく機能するかどうかを確認し、結果を収集してから人間が判読可能な形式で提示します。
- ベンチマークエンジン: パラメーター化されたベンチマークシナリオの書き込みを許可し、クラウドに対して実行します。

Benchmarking サービス: 新しいプラグインタイプの導入

テストシナリオをイテレーションとして実行し、実行されたアクションのタイムスタンプ (およびその他の情報) を Rally のレポートで提供することができます。

Benchmarking サービス: 新しいシナリオ

nova、cinder、magnum、ceilometer、manila、neutron 向けの Benchmarking シナリオが追加されました。

Benchmarking サービス: 検証コンポーネントのリファクタリング

Tempest の起動には、Rally Verify が使用されます。これは、新規モデル (検証機能の種別、検証機能、および検証結果) に対応するためにリファクターされました。

セル

OpenStack Compute には、コンピュートリソースを分割するために **nova-cells** パッケージにより提供されるセルの概念が採用されています。Cells v1 は Cells v2 に置き換えられました。Red Hat OpenStack Platform はデフォルトでは「単一セル」でデプロイし、現時点では複数セルのデプロイメントはサポートしていません。

DNS-as-a-Service (DNSaaS)

Designate としても知られる DNS-as-a-Service (DNSaaS) にはドメインとレコードの管理のための REST API が実装されており、マルチテナントに対応しています。また DNSaaS は OpenStack Identity サービス (keystone) と統合して認証を行います。さらに DNSaaS には Compute (nova) および OpenStack Networking (neutron) の通知と統合するフレームワークが実装されており、DNS レコードの自動生成が可能です。DNSaaS には Bind9 バックエンドとの統合が実装されています。

Firewall-as-a-Service (FWaaS)

Firewall-as-a-Service プラグインは、OpenStack Networking (neutron) に境界ファイアウォール管理機能を提供します。FWaaS は iptables を使用して、ファイアウォールポリシーをプロジェクト内の全仮想ルーターに適用し、1 プロジェクトあたりで1つのファイアウォールポリシーと論理ファイアウォールインスタンスをサポートします。FWaaS は、OpenStack Networking (neutron) ルーターでトラフィックをフィルタリングすることによって境界で稼働します。インスタンスレベルで稼働するセキュリティグループとは、この点が異なります。

Google Cloud Storage バックアップドライバ (Block Storage)

Block Storage (cinder) サービスで、ボリュームのバックアップの保管に Google Cloud Storage を使用するように設定できるようになりました。この機能は、多額な費用のかかるセカンダリークラウドを単に災害復旧の目的で維持管理する方法の代わりとなるオプションを提供します。

ベアメタルノード向けのリンクアグリゲーション

今回のリリースでは、ベアメタルノードのリンクアグリゲーションが導入されました。リンクアグリゲーションにより、ベアメタルノードの NIC に対してボンディングを設定して、フェイルオーバーとロードバランシングをサポートすることができます。この機能には、専用の neutron プラグインから設定可能な特定のハードウェアスイッチベンダーのサポートが必要です。お使いのハードウェアベンダーのスイッチが適切な neutron プラグインをサポートしていることを確認してください。

または、スイッチを手動で事前に設定して、ベアメタルノード用にボンディングを設定することも可能です。ノードが一方のボンディングインターフェースでブートできるようにするには、そのスイッチが LACP と LACP フォールバックの両方をサポートする必要があります (ボンディングが形

成されていない場合には、ボンディングのリンクが個別のリンクにフォールバックする)。そうでない場合には、ノードに別のプロビジョニングおよびクリーニングネットワークも必要となります。

Red Hat OpenStack Platform for POWER

事前にプロビジョニングされたオーバークラウドのコンピュータノードを IBM POWER8 little endian ハードウェアにデプロイできるようになりました。

Red Hat SSO

今回のリリースには、keycloak-httpd-client-install パッケージのバージョンが 1 つ含まれています。このパッケージは、Apache mod_auth_mellon SAML Service Provider を Keycloak SAML IdP のクライアントとして設定するのに役立つコマンドラインツールを提供します。

第3章 リリースの情報

本リリースノートには主に、今回リリースされた Red Hat OpenStack Platform のデプロイメント時に考慮すべきテクノロジープレビューの項目、推奨事項、既知の問題、非推奨となった機能について記載します。

Red Hat OpenStack Platform の本リリースのサポートライフサイクル中にリリースされる更新について情報は、各更新に対応したアドバイザリーの説明に記載されます。

3.1. RED HAT OPENSTACK PLATFORM 13 GA

本リリースノートには主に、今回リリースされた Red Hat OpenStack Platform のデプロイメント時に考慮すべきテクノロジープレビューの項目、推奨事項、既知の問題、非推奨となった機能について記載します。

3.1.1. 機能拡張

Red Hat OpenStack Platform の今回のリリースでは、以下の機能拡張が提供されています。

BZ#[1419556](#)

Object Store サービス (swift) は Barbican を統合して、保管されている (at-rest) オブジェクトを透過的に暗号化/復号化できるようになりました。at-rest 暗号化は、in-transit 暗号化とは異なり、ディスクに保管されている間にオブジェクトが暗号化されることを指します。

Swift のオブジェクトは、ディスク上にクリアテキストとして保管されます。このようなディスクは、ライフサイクル終了に達した時に適切に破棄しなければ、セキュリティリスクをもたらす可能性があります。このリスクは、オブジェクトを暗号化することによって軽減されます。

Swift はこれらの暗号化タスクを透過的に実行し、オブジェクトは swift にアップロードされる際には自動的に暗号化され、ユーザーに提供される際には自動的に復号化されます。この暗号化と復号化は、Barbican に保管されている同じ (対称) キーを使用して処理されます。

BZ#[1540239](#)

今回の機能拡張により、Gnocchi DB インスタンスへのメトリックデータ送信がサポートされるようになりました。

collectd コンポーザブルサービス向けに以下の新しいパラメーターが追加されました。CollectdGnocchiAuthMode が「simple」に設定されると、CollectdGnocchiProtocol、CollectdGnocchiServer、CollectdGnocchiPort、CollectdGnocchiUser が設定に取り入れられます。

CollectdGnocchiAuthMode が「keystone」に設定されている場合には、CollectdGnocchiKeystone* パラメーターが設定に取り入れられます。

追加されたパラメーターに関する詳しい説明は以下のとおりです。

CollectdGnocchiAuthMode:

型: 文字列

説明: >

Gnocchi サーバーが使用する認証のタイプ。

サポートされている値は、「simple」と「keystone」です。

```

    デフォルト: 'simple'
CollectdGnocchiProtocol:
    型: 文字列
    description: Gnocchi サーバーの使用する API プロトコル
    default: 'http'
CollectdGnocchiServer:
    型: 文字列
    説明: >
        メトリックの送信先となる gnocchi エンドポイントの名前またはアドレス
    デフォルト: なし
CollectdGnocchiPort:
    型: 数値
    説明: Gnocchi サーバーに接続するためのポート
    デフォルト: 8041
CollectdGnocchiUser:
    型: 文字列
    説明: >
        簡易認証を使用して、リモートの Gnocchi サーバーに対して認証を行うためのユーザー
名
    デフォルト: なし
CollectdGnocchiKeystoneAuthUrl:
    型: 文字列
    説明: 認証先となる Keystone エンドポイントの URL
    デフォルト: なし
CollectdGnocchiKeystoneUserName:
    型: 文字列
    説明: Keystone に対して認証を行うためのユーザー名
    デフォルト: なし
CollectdGnocchiKeystoneUserId:
    型: 文字列
    説明: Keystone に対して認証を行うためのユーザー ID
    デフォルト: なし
CollectdGnocchiKeystonePassword:
    型: 文字列
    説明: Keystone に対して認証を行うためのパスワード
    デフォルト: なし
CollectdGnocchiKeystoneProjectId:
    型: 文字列
    説明: Keystone に対して認証を行うためのプロジェクト ID
    デフォルト: なし
CollectdGnocchiKeystoneProjectName:
    型: 文字列
    説明: Keystone に対して認証を行うためのプロジェクト名
    デフォルト: なし
CollectdGnocchiKeystoneUserDomainId:
    型: 文字列
    説明: Keystone に対して認証を行うためのユーザードメイン ID
    デフォルト: なし
CollectdGnocchiKeystoneUserDomainName:
    型: 文字列
    説明: Keystone に対して認証を行うためのユーザードメイン名
    デフォルト: なし
CollectdGnocchiKeystoneProjectDomainId:
    型: 文字列
    説明: Keystone に対して認証を行うためのプロジェクトドメイン ID
    デフォルト: なし

```

CollectdGnocchiKeystoneProjectDomainName:
 型: 文字列
 説明: Keystone に対して認証を行うためのプロジェクトドメイン名
 デフォルト: なし

CollectdGnocchiKeystoneRegionName:
 型: 文字列
 説明: Keystone に対して認証を行うためのリージョン名
 デフォルト: なし

CollectdGnocchiKeystoneInterface:
 型: 文字列
 説明: 認証先となる Keystone エンドポイントの種別
 デフォルト: なし

CollectdGnocchiKeystoneEndpoint:
 型: 文字列
 説明: >
 Keystone の値を上書きする場合には、Gnocchi サーバーの URL を明示的に指定します。
 デフォルト: なし

CollectdGnocchiResourceType:
 型: 文字列
 説明: >
 ホストを保管するために Gnocchi によって作成される collectd-gnocchi プラグインのデフォルトのリソースタイプ
 デフォルト: 'collectd'

CollectdGnocchiBatchSize:
 型: 数値
 説明: Gnocchi がバッチ処理すべき値の最小数
 デフォルト: 10

3.1.2. テクノロジープレビュー

本項に記載する項目は、テクノロジープレビューとして提供しています。テクノロジープレビューの適用範囲のステータスに関する詳細情報およびそれに伴うサポートへの影響については、<https://access.redhat.com/support/offerings/techpreview/> を参照してください。

BZ#1488095

RHOS-12 以降では、OpenStack サービスはコンテナ化されています。今回のリリースでは、OpenStack Tempest もコンテナ化されました。コンテナ化された OpenStack Tempest はテクノロジープレビューとして提供されています。

3.1.3. リリースノート

本項では、Red Hat OpenStack Platform の注目すべき変更点や推奨プラクティスなど、今回のリリースに関する重要な情報を記載しています。お使いのデプロイメントに最大限の効果をもたらすために、以下の情報を考慮する必要があります。

BZ#1468020

Shared File System サービス (manila) は、IPv6 環境で manila を使用できるようにする NetApp ONTAP cDOT ドライバーを使用して IPv6 アクセスルールのサポートを提供するようになりました。

その結果、Shared File System サービスは、NetApp IPv6 ネットワーク上で ONTAP バックエンドによってバックアップされる共有のエクスポートをサポートします。エクスポートされた共

有へのアクセスは、IPv6 のクライアントアドレスによって制御されます。

BZ#1469208

Shared File System サービス (manila) は、NFSv4 プロトコルを介して、Ceph File System (CephFS) によってバックアップされる共有ファイルシステムのマウントをサポートしています。コントローラーノード上で稼働する NFS-Ganesha サーバーを使用して、高可用性 (HA) を使用するテナントに CephFS をエクスポートします。テナントは相互に分離され、提供される NFS ゲートウェイインターフェースを介してのみ CephFS にアクセスすることができます。director には、この新機能は完全に統合されているので、CephFS バックエンドのデプロイと Shared File System サービスの設定が可能です。

BZ#1496584

neutron サービスをコンテナ化する場合には、ネットワーク名前空間でコマンドの実行を試みると、以下のようなエラーで操作が失敗する可能性があります。

```
# ip netns exec qrouter...
RTNETLINK answers: Invalid argument
```

ネットワーク名前空間内でコマンドを実行するには、その名前空間を作成した neutron コンテナから操作を行う必要があります。たとえば、l3-agent からルーター用のネットワーク名前空間を作成した場合には、コマンドを以下のように変更します。

```
# docker exec neutron_l3_agent ip netns exec qrouter...
```

同様に、「qdhcp」で始まるネットワーク名前空間の場合には、「neutron_dhcp」コンテナからコマンドを実行してください。

BZ#1503521

本バージョンでは、networking-ovn の内部 DNS 解決のサポートが追加されました。ただし、既知の制限事項が 2 点あり、その 1 つは bz#1581332 で、内部 DNS を介した内部 fqdn 要求が適切に解決されない問題です。

GA リリース版の tripleo は、デフォルトではこの拡張機能を設定しない点に注意してください。bz#1577592 で回避策を参照してください。

BZ#1533206

openstack-gnocchi パッケージは gnocchi という名前に変更されました。アップストリームのスコープが変更されたため、openstack- のプレフィックスは削除されました。Gnocchi は OpenStack の傘下から外れて、スタンドアロンのプロジェクトになりました。

BZ#1556933

python-cryptography は、バージョン 2.1 より、証明書で使用されている CNS 名が IDN 標準に準拠していることを確認するようになりました。検出された名前がこの仕様に従っていない場合には、cryptography はその証明書の検証に失敗し、OpenStack コマンドラインインターフェースを使用する際や OpenStack のサービスログで異なるエラーが見つかる場合があります。

BZ#1563412

OpenStack Compute (nova) に確保されるホストのメモリーが 2048 MB から 4096 MB に

増やされました。これは、環境の容量推定に影響する可能性があります。必要な場合には、環境ファイル内の「NovaReservedHostMemory」パラメーターを使用して確保するメモリーを再設定することができます。以下に例を示します。

```
parameter_defaults:
  NovaReservedHostMemory: 2048
```

BZ#1564176

python-mistralclient は、サポートされているオーバークラウドユースケースのいずれにも属さないため、OSP 13 リリースでは -tools チャンネルから削除されました。

BZ#1567735

OVN をネットワークバックエンドとして使用する OSP13 で、最初のリリースには IPv6 のサポートは含まれません。ゲスト仮想マシンから送信される Neighbor Solicitation 要求への応答に問題があり、デフォルトのルートが失われます。

BZ#1575752

以前のバージョンでは、*NetName パラメーター（例：InternalApiNetName）によってデフォルトのネットワークの名前が変更されていました。これはサポートされなくなりました。

デフォルトのネットワーク名を変更するには、カスタムのコンポーザブルネットワークファイル (network_data.yaml) を使用して、「openstack overcloud deploy」コマンドに「-n」オプションを指定してそのファイルを追加してください。このファイルで、「name_lower」フィールドに変更するネットワークのカスタム net 名を指定します。詳しい情報は、『Advanced Overcloud Customization』ガイドの「Using Composable Networks」を参照してください。

また、ServiceNetMap テーブルのローカルパラメーターを network_environment.yaml に追加して、古いネットワーク名のデフォルト値を新しいカスタム名でオーバーライドする必要があります。デフォルト値は /usr/share/openstack-tripleo-heat-templates/network/service_net_map.j2.yaml にあります。この ServiceNetMap の変更は、今後の OSP-13 リリースでは必要なくなります。

BZ#1577537

OSP 13 ベータ版で一部のコンテナイメージが利用できなかった問題が修正されました。

BZ#1578312

OVSDB サーバーが異なるコントローラーノードにフェイルオーバーする場合に、その状況が検出されなかったため、neutron-server/metadata-agent からの再接続が実行されませんでした。

その結果、metadata-agent が新しいメタデータ名前空間をプロビジョニングせず、クラスターが想定通りに動作しないため、仮想マシンの起動が機能しない場合があります。

回避策としては、新しいコントローラーが OVN データベース向けにマスターとして昇格した後、全コンピュータノードで ovn_metadata_agent コンテナを再起動する方法を使用することができます。また、plugin.ini で ovnsdb_probe_interval の値を 600000 ミリ秒に増やしてください。

BZ#1589849

OVN メタデータエージェントがコンピュートノードで停止すると、そのノード上の全仮想マシンがメタデータサービスにアクセスできなくなります。これにより、新規仮想マシンを起動したり、既存の仮想マシンを再起動したりする場合に、OVN メタデータエージェントが稼働状態に戻るまで仮想マシンはメタデータにアクセスできません。

BZ#[1592528](#)

まれな状況で、コントローラーノードを数回リブートした後に、RabbitMQ の稼働状態が一定しなくなってオーバークラウド上の API 操作がブロックされる場合があります。

この問題には、以下のような症状があります。

- いずれかの OpenStack サービスのログで以下の形式のエントリーが表示される。
DuplicateMessageError: Found duplicate message(629ff0024219488499b0fac0cacao3a5). Skipping it.
- 「openstack network agent list」で一部のエージェントが DOWN と返される。

通常の操作ができる状態に戻すには、いずれかのコントローラーノードで以下のコマンドを実行します（1 台のコントローラーでのみ実行する必要があります）:

```
pcs resource restart rabbitmq-bundle
```

3.1.4. 既知の問題

現時点における Red Hat OpenStack Platform の既知の問題は以下のとおりです。

BZ#[1321179](#)

「python-requests」を使用する OpenStack のコマンドラインクライアントは、現在、IP アドレスが SAN フィールドに記載されている証明書は検証できません。

BZ#[1461132](#)

Cinder ボリュームと Cinder バックアップの両方のブロックストレージバックエンドとして Red Hat Ceph Storage を使用する場合には、差分バックアップの実行を試みると、代わりに完全バックアップが警告なしに実行されます。これは既知の問題です。

BZ#[1508449](#)

OVN は、直接コンピュートノード上で ovn-controller を使用して openflow コントローラーとして DHCP を提供します。ただし、SR-IOV インスタンスは VF/PF を介して直接ネットワークにアタッチされます。そのため、SR-IOV インスタンスは DHCP の応答をどこからも取得することができません。

この問題を回避するには、「OS::TripleO::Services::NeutronDhcpAgent」を以下のように変更してください。

```
OS::TripleO::Services::NeutronDhcpAgent: docker/services/neutron-dhcp.yaml
```

BZ#[1515815](#)

ルーターゲートウェイがクリアされる際には、検出された IP アドレスに関連するレイヤー 3 フローは削除されません。検出される IP アドレスには、PNF と外部ゲートウェイの IP アドレスが含まれます。これによりフローが古くなりますが、機能的には問題ありません。外部ゲートウェイ

イと IP アドレスは頻繁には変わりません。古くなったフローは、外部ネットワークが削除される際に削除されます。

BZ#1518126

Redis は、TLS を有効化した HA デプロイメントでは、ノード間でデータのレプリケーションを正しく行うことができません。Redis のフォロワーノードにはリーダーノードからのデータは全く含まれません。Redis デプロイメントには TLS を無効にすることを推奨します。

BZ#1519783

Neutron は、Neutron Router 作成でクォータを超過していることを示すエラーが表示する場合があります。これは、networking-odl のバグが原因で Neutron DB で単一の作成要求によって複数のルーターリソースが作成される既知の問題です。この問題の回避策は、OpenStack Neutron CLI で重複したルーターを削除して、再度ルーターを 1 つ作成する方法で、これにより単一のインスタンスになります。

BZ#1557794

『Back Up and Restore the Director Undercloud』の手順でリグレッションが確認されました。その結果、同ガイドは変更と確認を行ってから公開する必要があります。

従って、『Back Up and Restore the Director Undercloud』は Red Hat OpenStack Platform 13 の一般提供リリースでは提供されません。この手順の更新は、一般提供リリースの後に優先され、確認が済み次第公開される予定です。

BZ#1559055

OpenDaylight のロギングで前半のログが含まれていない可能性があります。OpenDaylight の journald ロギング (「docker logs opendaylight_api」コマンドを使用) の既知の問題です。現在の回避策としては、OpenDaylight のロギングを「file」メカニズムに切り替えて、コンテナ内の /opt/opendaylight/data/logs/karaf.log にロギングされるようにする方法があります。そのためには、次の heat パラメーターを設定します：
OpenDaylightLogMechanism: 'file'

BZ#1562035

docker-puppet または paunch コンテナの実行中には、nsenter コールのカーネルエラーで Docker run が失敗します。これは、fork 関数の unshare コールの使用と関連したカーネルの問題として確認されました。この問題は、RHEL 7.5.2 リリースに関連付けられた次のカーネルリリースで修正されることになっています (6 月末の予定)。BZ #1577745 と関連付けられたカーネルのホットフィックスがリクエストに応じて提供可能です。

その代わりに、以下の回避策を使用することも可能です。

1) 環境ファイルから「TunedProfileName」パラメーターを削除してデプロイします。cpu-partitioning を使用せずにデプロイした場合には再現性がより低くなることが確認されています。デプロイが完了したら、以下のステップに従って tuned プロファイルを設定します。

- * /etc/tuned/cpu-partitioning-variables.conf で「isolated_cores」を設定します。

- * 「tuned-adm profile cpu-partitioning」のコマンドを実行します。

- * ノードを再起動します。

注記: この回避策を使用すると、問題の発生率が低くなることが確認されています。

2) https://bugzilla.redhat.com/show_bug.cgi?id=1562035#c27 および

https://bugzilla.redhat.com/show_bug.cgi?id=1562035#c31 のコメントで指定されているコマンドに従います。

注記: これにより、ホストの PID がコンテナに公開されてコンテナが実行されることになり、望ましい結果ではありません。「pid=host」回避策を使用しなくても済む方法の詳しい手順は、OSP13 の次のマイナーリリースで提供されます。

BZ#1568012

Floating IP をインスタンスに割り当ててからその Floating IP の割り当てを解除する際に、外部の IP への接続が失敗します。この状況は、テナントの VLAN ネットワークで、NAPT 以外のスイッチ上で起動する仮想マシンに Floating IP が割り当てられ、その後にその Floating IP が削除された場合に発生します。これによって、NAPT スwitchの FIB テーブルでフローが（散発的に）失われます。

失われた FIB テーブルのエントリーが原因で、仮想マシンはパブリックネットワークへの接続を失います。

Floating IP を仮想マシンに割り当てると、パブリックネットワークへの接続が復元されます。その Floating IP が仮想マシンに割り当てられている限りは、インターネットへの接続が可能です。外部ネットワークからのパブリック IP/Floating IP を失います。

BZ#1568311

Floating IP が割り当てられていないインスタンスが別のルーター上の Floating IP が割り当てられているインスタンスに接続を試みると、複数のサブネット全体にわたる Nova インスタンス間のレイヤー 3 接続が失敗する可能性があります。これは、Nova インスタンスが複数の Compute ノードに分散している場合に発生します。この問題には、現在適切な回避策はありません。

BZ#1568976

機能の読み込みのバグが原因で、デプロイメント中に OpenDaylight インスタンスが 1 つまたは複数失敗する場合があります。これによって、デプロイメントまたは機能でエラーが発生する可能性があります。

このような状況では、以下の措置を取ってください。

* In an HA デプロイメントの場合は、少なくとも 2 つの OpenDaylight インスタンスが正しくブートしなければデプロイメントは失敗する場合があります。このような場合には、現在の回避策は、「docker ps」コマンドで各コンテナのヘルスステータスをチェックする方法です。異常な場合には、「docker restart opendaylight_api」でコンテナの再起動を実行します。

* TLS ベースのデプロイメントでは、全 OpenDaylight インスタンスが正しくブートしなければデプロイメントは失敗します。このため、デプロイメントは全 OpenDaylights が正常にブートするまで再起動する必要があります。

BZ#1571864

Fast Forward Upgrade の準備中に Heat stack リソースの一時的に削除されることにより、RHEL が登録解除がトリガーされます。

このような状態になると、Heat ソフトウェアデプロイメントのシグナルが正常に機能しないため、RHEL の登録解除は保留になります。

この問題を回避するには、オーバークラウドがまだ OSP 10 の間に、オーバークラウドの最後のマイナーバージョン更新を実行する準備が整った時点で以下の手順を実行します。

1. テンプレートファイル `/usr/share/openstack-tripleo-heat-templates/extraconfig/pre_deploy/rhel-registration/rhel-registration.yaml` を編集します。
2. そのテンプレートから `RHELUnregistration` および `RHELUnregistrationDeployment` のリソースを削除します。
3. マイナー更新と `Fast Forward Upgrade` の手順を続行します。

BZ#1573597

パフォーマンスの低い Swift クラスターが Gnocchi のバックエンドとして使用されると、`collectd` ログに 503 エラーと、`gnocchi-metricd.conf` に `"ConnectionError: ('Connection aborted.', CannotSendRequest())"` エラーが出力される場合があります。この問題を軽減するには、`CollectdDefaultPollingInterval` パラメーターの値を増やすか、Swift クラスターのパフォーマンスを改善してください。

BZ#1574708

OpenDaylight インスタンスがクラスターから削除されて再接続されると、そのインスタンスがクラスターに正常に参加されない場合があります。ノードは最終的にクラスターに再参加します。

このような場合には、以下のアクションを実行すべきです。

- * 問題の発生したノードを再起動する
- * REST エンドポイントをモニタリングして、クラスターメンバーの正常性を確認します：
`http://$ODL_IP:8081/jolokia/read/org.opendaylight.controller:Category=ShardManager,name=shard-manager-config,type=DistributedConfigDatastore`
 - * 応答には、`"SyncStatus"` のフィールドが含まれるはずで、値が `"true"` の場合には、クラスターメンバーが正常であることを示します。

BZ#1574725

VLAN プロバイダーネットワークの同じサブネット内の複数の仮想マシンが異なる 2 台のコンピュートノードでスケジュールされると、それらの仮想マシン間の ARP が散発的に失敗します。

それらの仮想マシン間の ARP パケット送信は失敗するため、2 つの仮想マシン間には実質的にネットワークがないことになります。

BZ#1575023

`ceph-ansible` の複合 `ceph-keys` 処理により、`/etc/ceph/ceph.client.manila.keyring` ファイルの内容が誤って生成されるため、`manila-share` サービスの初期化が失敗します。

`manila-share` サービスを初期化できるようにするには、以下の手順を実行してください。

1) オーバークラウドのデプロイに使用する `/usr/share/openstack/tripleo-heat-templates` のコピーを作成します。

2) `.../tripleo-heat-templates/docker/services/ceph-ansible/ceph-base.yaml` ファイルを編集して、295 行目の 3 つ並んだバックスラッシュをすべて 1 つのバックスラッシュに変更します。

編集前:

```
mon_cap: 'allow r, allow command \\\\"auth del\\\\" , allow command \\\\"auth caps\\\\" , allow command \\\\"auth get\\\\" , allow command \\\\"auth get-or-create\\\\"'
```

編集後:

```
mon_cap: 'allow r, allow command \\"auth del\\", allow command \\"auth
```

```
caps\", allow command \"auth get\", allow command \"auth get-or-create\"'
```

3) tripleo-heat-templates のコピーのパスを、元の overcloud-deploy コマンドで実行した /usr/share/openstack-tripleo-heat テンプレートの場所に置き換えてオーバークラウドをデプロイします。

ceph キーの /etc/ceph/ceph.client.manila.keyring ファイルには適切な内容が記載されるようになり、manila-share サービスは正常に初期化されるようになります。

BZ#1575118

Ceph リリース 12.2.1 では、各 OSD で許容される PG の最大数が少なくなっています。上限値が低くなったため、モニターが途中で HEALTH_WARN メッセージを発行する場合があります。

モニターの警告の閾値は、1 OSD あたり 300 から 200 PG に削減されています。200 は、一般的な推奨目標値である 1 OSD あたり 100 PG の 2 倍です。この上限は、モニター上の mon_max_pg_per_osd オプションで調整することができます。以前の mon_pg_warn_max_per_osd オプションは削除されています。

プールの消費する PG の量を少なくすることはできません。アップグレードにより既存のデプロイメントが上限に達した場合には、ceph-upgrade のステップを実行中に上限をアップグレード前の値に増やすことができます。環境ファイルで、以下のようなパラメーター設定を追加します。

```
parameter_defaults:
  CephConfigOverrides:
    mon_max_pg_per_osd: 300
```

この設定は ceph.conf に適用されて、クラスターは HEALTH_OK の状態を維持します。

BZ#1575150

OpenDaylight クラスターのメンバーが（エラーなどで）停止した際に OpenDaylight クラスターが最長で 30 分応答しなくなる既知の問題があります。回避策は、クラスターが再度アクティブになるまで待つことです。

BZ#1575496

director で外部ネットワーク用の物理ホストのインターフェースを使用する場合に、そのインターフェースが OVS ブリッジに接続されていなければ、そのインターフェースは OpenDaylight 環境でトラフィックが通過しなくなるので、この種の構成は避けるべきです。

オーバークラウドの外部ネットワーク用の NIC テンプレートでは、常に OVS ブリッジを使用してください。このブリッジは、director ではデフォルトで「br-ex」という名前です（任意の名前を使用可）。外部ネットワークに使用する物理ホストのインターフェースをこの OVS ブリッジに接続する必要があります。

OVS ブリッジに接続したインターフェースを使用すると、デプロイメントは正しく機能し、外部ネットワークからテナントにトラフィックが通過できるようになります。

BZ#1577975

OpenDaylight で CPU の使用率が非常に高くなる期間が発生する場合があります。この問題は、OpenDaylight の機能には影響しませんが、他のシステムのサービスに悪影響を及ぼす可能性があります。

BZ#1579025

OVN pacemaker Resource Agent (RA) のスクリプトは、pacemaker がスレーブノードのプロモーションを試みる際に、プロモーションのアクションが適切に処理されない場合があります。これは、ovsdb-servers が master のステータスを RA スクリプトに報告し、マスターの ip がそのノードに移った場合に発生する問題で、アップストリームでは修正済みです。

問題が発生すると、neutron サーバーは OVN North および South DB サーバーに接続できなくなり、neutron サーバーに対する Create/Update/Delete API はすべて失敗します。

この問題は、ovn-dbs-bundle リソースを再起動すると解決します。以下のコマンドをコントローラーノードで実行してください。

```
「pcs resource restart ovn-dbs-bundle」
```

BZ#1579417

SNAT サポートには、テナントネットワークに使用されているカプセル化に拘らず、VXLAN トンネルを設定する必要があります。また、VLAN テナントネットワークを使用する場合は、VXLAN トンネルのヘッダーがペイロードに追加され、それによってパケットがデフォルトの MTU (1500 バイト) を超過する可能性があるため、MTU を正しく設定する必要があります。

SNAT トラフィックが流れるようにするには、VXLAN トンネルを適切に設定する必要があります。VLAN テナントネットワークを使用する場合は、以下のいずれかの方法で MTU を設定して、SNAT トラフィックが VXLAN トンネルを流れるようにしてください：

- * VLAN テナントベースのネットワークは、ネットワーク構成 1 つにつき 1450 の MTU を使用するよう設定します。
- * heat パラメーターの NeutronGlobalPhysnetMtu を 1450 に設定します。注記：これは、すべての flat/VLAN プロバイダーネットワークが 1450 MTU となることを意味し、望ましい設定ではありません（外部プロバイダーネットワークは特に）。
- * テナントネットワークの下層は、MTU を 1550（またはそれ以上）に設定します。これには、テナントネットワーク用の NIC の NIC テンプレートで MTU を設定する操作が含まれます。

BZ#1581337

PING タイプのヘルスマニターを使用するには、HAProxy（ネットワークロードバランシング用のドライバーで使用するデフォルトのソフトウェア）のバージョンは最小で 1.6 が必要です。古いバージョンの HAProxy を使用すると、ヘルスチェックはユーザーが知らないうちに、TCP 接続となります。

アップストリームのコミュニティでは、使用中の HAProxy のバージョンを確認して、それに応じてアクションを実行するチェックをコードに追加して、問題を修正済みです。

HAProxy バージョン 1.6 以降の場合には、PING を使用できます。

そうでない場合には、引き続き TCP 接続を使用します（それらの haproxy バージョンに他に解決方法がない場合には、全く使えなくなってしまうよりは、TCP 接続を使用した方がよいことになります）。

OSP13 の GA リリースでは、HAProxy が RHEL チャンネルの一部として出荷されており、そのチャンネルでは古いバージョンの HAProxy を使用しているのが問題点です。そのため、OSP13 のユーザーが PING タイプのヘルスマニターを設定すると、代わりに TCP 接続されてしまいます。

BZ#1583541

SRIOV ベースの Compute インスタンスは、異なるネットワーク上にある OVS Compute インスタンスには接続できません。回避策は、両方の VLAN プロバイダーネットワークに接続された外部ルーターを使用することです。

BZ#[1584518](#)

RHOSP では、nova で DifferentHostFilter / SameHostFilter の有無はデフォルトでは設定されません。これらの設定は、一部のテストを適切に完了するために必要です。このため、いくつかのセキュリティーグループのテストが無作為に失敗する可能性があります。

そのようなテストは省略するか、nova の設定にそれらのフィルターを追加する必要があります。

BZ#[1584762](#)

アンダークラウド上で Telemetry が手動で有効化された場合には、各ノードのファイアウォールの間違った設定が原因で「hardware.*」メトリックは機能しません。

回避策としては、以下のようにアンダークラウドデプロイメント用に更にテンプレートを追加することによって、コントロールプレーンネットワークで「snmpd」サブネットを手動で設定する必要があります。

```
parameter_defaults:
    SnmpdIpSubnet: 192.168.24.0/24
```

BZ#[1588186](#)

競合により、Open vSwitch は Opendaylight openflowplugin に接続されません。この問題の修正は、本製品の 13.z リリースで実装される予定です。

BZ#[1590114](#)

アンダークラウド上で Telemetry が手動で有効化された場合には、各ノードのファイアウォールの間違った設定が原因で「hardware.*」メトリックは機能しません。

回避策としては、以下のようにアンダークラウドデプロイメント用に更にテンプレートを追加することによって、コントロールプレーンネットワークで「snmpd」サブネットを手動で設定する必要があります。

```
parameter_defaults:
    SnmpdIpSubnet: 192.168.24.0/24
```

BZ#[1590560](#)

ceph-ansible ユーティリティーは、ceph-create-keys コンテナが作成されたのと同じノードから ceph-create-keys コンテナを必ずしも削除しません。

このため、「Error response from daemon: No such container: ceph-create-keys.」というメッセージが表示されてデプロイメントが失敗する場合があります。これにより、複数のコンピューターノードを使用する新規デプロイメントや、Ceph クライアントとして動作し Ceph を使用するサービスをホスティングするカスタムロールを使用する新規デプロイメントを含む ceph-ansible の実行で影響を受ける場合があります。

BZ#[1590938](#)

-

RHCS3 上に OSD を 3 つ以上デプロイして、pgcalc (<https://access.redhat.com/labs/cephpgc>) により決定されるプールの PG 数を設定する場合は、全 OSD がアクティブになる前に ceph-ansible がプールを作成するため、デプロイメントが失敗します。

この問題を回避するには、デフォルトの PG 数を 32 に設定しておき、デプロイメントの終了時には、『Storage Strategies Guide』の https://access.redhat.com/documentation/en-us/red_hat_ceph_storage/3/html/storage_strategies_guide/placement_groups_pg#set_the_number_of_pgs に記載の手順で PG 数を増やします。

BZ#1590939

ceph-ansible OpenStack プールタスクに誤ったコンテナ名が付いているため、Ceph MON と OSD のコロケーションはまだできません。
標準の HCI (Compute + OSD) には影響ありません。

BZ#1593290

SR-IOV ベースのネットワークインターフェースがアタッチされているゲストを実行中に nova-compute サービスを再起動した後に、そのゲストを削除すると、そのノード上の SR-IOV VF はどのゲストにもアタッチできなくなります。これは、サービスの起動時に利用可能なデバイスが列挙されますが、ゲストにアタッチ済みのデバイスはホストデバイスの一覧に含まれないためです。

ゲストを削除した後は、「nova-compute」サービスを再起動する必要があります。ゲストを削除した後にこのサービスを再起動すると、利用可能な SR-IOV デバイスの一覧が正しくなります。

BZ#1593715

非セキュアなレジストリーの一覧は、メジャーアップグレード中に一部のコンテナイメージがプルされた後に更新されるため、新たに導入された非セキュアなレジストリーからのコンテナイメージは「openstack overcloud upgrade run」コマンドの実行中にダウンロードに失敗します。

以下の回避策を使用することができます。

オプション A: Pacemaker によって管理されているコンテナがあるノード上の `/etc/sysconfig/docker` ファイルを手動で更新して、新たに導入された非セキュアなレジストリーを追加します。

オプション B: アップグレードの直前に「openstack overcloud deploy」コマンドを実行して、環境ファイルの `DockerInsecureRegistryAddress` パラメーターで必要な新しい非セキュアなレジストリーを指定します。

これで、アップグレード中にすべてのコンテナイメージがダウンロードされるようになるはずです。

BZ#1593757

既存のオーバークラウドデプロイメントで Octavia を有効化すると操作が成功したと報告されますが、コントローラーノード上のファイアウォールルールが誤って設定されているため、Octavia API エンドポイントに到達出来ません。

回避策:

全コントローラーノードでファイアウォールルールを追加して、それらが DROP ルールの前に挿入されるようにします。

IPv4:

```
# iptables -A INPUT -p tcp -m multiport --dports 9876 -m state --state
NEW -m comment --comment "100 octavia_api_haproxy ipv4" -j ACCEPT
# iptables -A INPUT -p tcp -m multiport --dports 13876 -m state --state
NEW -m comment --comment "100 octavia_api_haproxy_ssl ipv4" -j ACCEPT
# iptables -A INPUT -p tcp -m multiport --dports 9876,13876 -m state --
state NEW -m comment --comment "120 octavia_api ipv4" -j ACCEPT
```

IPv6:

```
# ip6tables -A INPUT -p tcp -m multiport --dports 9876 -m state --state
NEW -m comment --comment "100 octavia_api_haproxy ipv6" -j ACCEPT
# ip6tables -A INPUT -p tcp -m multiport --dports 13876 -m state --state
NEW -m comment --comment "100 octavia_api_haproxy_ssl ipv6" -j ACCEPT
# ip6tables -A INPUT -p tcp -m multiport --dports 9876,13876 -m state --
state NEW -m comment --comment "120 octavia_api ipv6" -j ACCEPT
```

HAProxy を再起動します:

```
# docker restart haproxy-bundle-docker-0
```

BZ#[1595363](#)

Fast Forward Upgrade の処理中には、アンダークラウドがバージョン 10 から 11 にアップグレードされます。場合によっては、nova-api.log に以下のようなエラーが報告される可能性があります。

```
「Unexpected API Error. Table 'nova_cell0.instances' doesn't exist」
```

このエラーは、以下のコマンドを実行すると解決することができます。

```
$ sudo nova-manage api_db sync
```

この問題はクリティカルではないので、Fast forward Upgrade プロセスを大きく妨げることはありませんはずです。

第4章 テクニカルノート

本章には、コンテンツ配信ネットワークからリリースされる Red Hat OpenStack Platform 「Queens」のエラーアドバイザーの補足情報を記載します。

4.1. RHEA-2018:2086 — RED HAT OPENSTACK PLATFORM 13.0 の機能拡張アドバイザー

本項に記載するバグは、アドバイザー RHEA-2018:2086 に対応しています。このアドバイザーについての詳しい情報は、<https://access.redhat.com/errata/RHEA-2018:2086> を参照してください。

ceph-ansible

BZ#1590560

ceph-ansible ユーティリティーは、ceph-create-keys コンテナが作成されたのと同じノードから ceph-create-keys コンテナを必ずしも削除しません。

このため、「Error response from daemon: No such container: ceph-create-keys.」というメッセージが表示されてデプロイメントが失敗する場合があります。これにより、複数のコンピュータノードを使用する新規デプロイメントや、Ceph クライアントとして動作し Ceph を使用するサービスをホスティングするカスタムロールを使用する新規デプロイメントを含む ceph-ansible の実行で影響を受ける場合があります。

gnocchi

BZ#1533206

openstack-gnocchi パッケージは gnocchi という名前に変更されました。アップストリームのスコープが変更されたため、openstack- のプレフィックスは削除されました。Gnocchi は OpenStack の傘下から外れて、スタンドアロンのプロジェクトになりました。

opendaylight

BZ#1568012

Floating IP をインスタンスに割り当ててからその Floating IP の割り当てを解除する際に、外部の IP への接続が失敗します。この状況は、テナントの VLAN ネットワークで、NAPT 以外のスイッチ上で起動する仮想マシンに Floating IP が割り当てられ、その後にその Floating IP が削除された場合に発生します。これによって、NAPT スwitchの FIB テーブルでフローが（散発的に）失われます。

失われた FIB テーブルのエントリーが原因で、仮想マシンはパブリックネットワークへの接続を失います。

Floating IP を仮想マシンに割り当てると、パブリックネットワークへの接続が復元されます。その Floating IP が仮想マシンに割り当てられている限りは、インターネットへの接続が可能ですが、外部ネットワークからのパブリック IP/Floating IP を失います。

openstack-cinder

BZ#1557331

-

以前のリリースでは、ローリングアップグレードのメカニズムが原因で、オフラインのアップグレードを実行する際に cinder サービスを 2 回再起動する必要がありました。

今回のリリースでは、新しいオプションのパラメーター「--bump-versions」を cinder-manage db sync コマンドに追加すると、2 回のシステム再起動はスキップすることができす。

BZ#1572220

Block Storage service (cinder) は同期ロックを使用してボリュームイメージキャッシュ内のエントリーが重複するのを防ぎます。このロックのスコープは広範過ぎていたため、イメージキャッシュが有効化されていない場合でも、イメージからのボリューム作成の要求が同時に発生すると、それらはロックをめぐって競っていました。

イメージキャッシュが有効化されていない場合のイメージからのボリューム作成の同時要求は、並行して実行するのではなくシリアル化する方が賢明です。

そのため、同期ロックは更新されてロックのスコープは最小限となり、ボリュームイメージキャッシュが有効化されている場合にのみ機能が有効となるようになりました。

今回のリリースでは、イメージからのボリューム作成の同時要求は、ボリュームイメージキャッシュが無効化されている場合には並行して実行されます。ボリュームイメージキャッシュが有効化されている場合にはキャッシュにはエントリーが 1 つしか作成されないようにするロックは最小限に抑えられるようになりました。

openstack-manila

BZ#1468020

Shared File System サービス (manila) は、IPv6 環境で manila を使用できるようにする NetApp ONTAP cDOT ドライバーを使用して IPv6 アクセスルールのサポートを提供するようになりました。

その結果、Shared File System サービスは、NetApp IPv6 ネットワーク上で ONTAP バックエンドによってバックアップされる共有のエクスポートをサポートします。エクスポートされた共有へのアクセスは、IPv6 のクライアントアドレスによって制御されます。

BZ#1469208

Shared File System サービス (manila) は、NFSv4 プロトコルを介して、Ceph File System (CephFS) によってバックアップされる共有ファイルシステムのマウントをサポートしています。コントローラーノード上で稼働する NFS-Ganesha サーバーを使用して、高可用性 (HA) を使用するテナントに CephFS をエクスポートします。テナントは相互に分離され、提供される NFS ゲートウェイインターフェースを介してのみ CephFS にアクセスすることができます。director には、この新機能は完全に統合されているので、CephFS バックエンドのデプロイと Shared File System サービスの設定が可能です。

openstack-neutron

BZ#1552108

ルーターにインターフェースが追加または削除されて DHCP エージェントで分離されたメタデータが有効化となった際に、そのネットワークのメタデータプロキシが更新されません。

そのため、インスタンスがルーターに接続されていないネットワーク上にある場合には、そのインスタンスはメタデータをフェッチできません。

ルーターのインターフェースの追加/削除時には、メタデータプロキシを更新する必要があります。それにより、インスタンスは、使用しているネットワークが分離された場合に DHCP 名前空間からメタデータをフェッチすることができるようになります。

openstack-selinux

BZ#1561711

以前のリリースでは、ゲスト仮想マシンの起動時に、virtlogd サービスがログ記録する AVC 拒否のエラーが重複していました。今回の更新で、virtlogd サービスはシャットダウンを抑制するコールを systemd に送信しなくなり、このエラーが発生しなくなりました。

openstack-swift

BZ#1419556

Object Store サービス (swift) は Barbican を統合して、保管されている (at-rest) オブジェクトを透過的に暗号化/復号化できるようになりました。at-rest 暗号化は、in-transit 暗号化とは異なり、ディスクに保管されている間にオブジェクトが暗号化されることを指します。

Swift のオブジェクトは、ディスク上にクリアテキストとして保管されます。このようなディスクは、ライフサイクル終了に達した時に適切に破棄しなければ、セキュリティリスクをもたらす可能性があります。このリスクは、オブジェクトを暗号化することによって軽減されます。

Swift はこれらの暗号化タスクを透過的に実行し、オブジェクトは swift にアップロードされる際には自動的に暗号化され、ユーザーに提供される際には自動的に復号化されます。この暗号化と復号化は、Barbican に保管されている同じ (対称) キーを使用して処理されます。

openstack-tripleo-common

BZ#1560422

Octavia は、「service」プロジェクトに設定されているデフォルトのクォータによりオーバークラウドで作成可能な Octavia ロードバランサーの数が限定されているため、実用的なワークロードにはスケーリングしません。

この問題を回避するには、オーバークラウドの admin ユーザーとして、必要なクォータを無制限または十分に大きな値に設定します。たとえば、アンダークラウドで以下のコマンドを実行します。

```
# source ~/overcloudrc
# openstack quota set --cores -1 --ram -1 --ports -1 --instances -1 --
  secgroups -1 service
```

BZ#158838

tripleo.plan_management.v1.update_roles ワークフローは、トリガーするサブワークフローに対して、オーバークラウドのプラン名 (swift コンテナ名) または zaqar キュー名を

渡しませんでした。これにより、デフォルト ('overcloud') 以外のオーバークラウドプラン名を使用する場合に誤った動作が発生していました。今回の修正により、それらのパラメーターは正しく渡されるようになり、動作が正しく実行されるようになりました。

BZ#1566463

コンテナが自動的に再起動するように設定されている場合、「docker kill」コマンドは終了しません。ユーザーが「docker kill <container>」の実行を試みると、無期限にハングする場合があります。そのような場合には、CTRL+C でコマンドを停止してください。

この問題を回避するには、(「docker kill」の代わりに)「docker stop」を実行して、コンテナ化されたサービスを停止してください。

BZ#1452979

原因: 「openstack overcloud node configure」コマンドは、「deploy-kernel」および「deploy-ramdisk」のパラメーターにイメージ名だけを取り、イメージ ID は指定できませんでした。今回の修正後にイメージ ID が受け入れられるようになりました。

openstack-tripleo-heat-templates

BZ#1341176

今回の機能拡張により、director から「通常」のコンピュータードとともに、RT 対応のコンピュータードをデプロイする操作がサポートされるようになりました。

1. tripleo-heat-templates/environments/compute-real-time-example.yaml をベースにして、compute-real-time.yaml 環境ファイルを作成します。このファイルは、ComputeRealTime ロールのパラメーターの中で、少なくとも以下のパラメーターを正しい値に設定します。

- * IsolCpusList および NovaVcpuPinSet: real-time ワークロードに確保すべき CPU コアの一覧。これは、real-time コンピュータードの CPU ハードウェアによって異なります。

- * KernelArgs: "default_hugepagesz=1G hugepagesz=1G hugepages=X" に設定します。X はゲストの数と確保するメモリーの量によって異なります。

2. overcloud-realtime-compute イメージをビルドしてアップロードします。

- * リポジトリを準備します (CentOS 用)。
 - sudo yum install -y
- https://trunk.rdoproject.org/centos7/current/python2-tripleo-repos-XXX.el7.centos.noarch.rpm
 - sudo -E tripleo-repos current-tripleo-dev
 - export DIB_YUM_REPO_CONF="/etc/yum.repos.d/delorean*/etc/yum.repos.d/quickstart"
- * openstack overcloud image build --image-name overcloud-realtime-compute --config-file /usr/share/openstack-tripleo-common/image-yaml/overcloud-realtime-compute.yaml --config-file /usr/share/openstack-tripleo-common/image-yaml/overcloud-realtime-compute-centos7.yaml
- * openstack overcloud image upload --update-existing --os-image-name

```
overcloud-realtime-compute.qcow2
```

3. `roles_data.yaml` を `ComputeRealTime` およびその他の必要な全ロールで作成して (例: `openstack overcloud roles generate -o ~/rt_roles_data.yaml Controller ComputeRealTime ...`)、通常の方法のいずれか 1 つで、`ComputeRealTime` ロールを `real-time` ノードに割り当てます。 https://docs.openstack.org/tripleo-docs/latest/install/advanced_deployment/custom_roles.html を参照してください。

4. オーバークラウドをデプロイします。

```
openstack overcloud deploy --templates -r ~/rt_roles_data.yaml -e
./tripleo-heat-templates/environments/host-config-and-reboot.yaml -e
./compute-real-time.yaml [...]
```

BZ#1552583

`glance-direct` メソッドには、HA 構成で使用する場合の共通のステージングエリアが必要です。共通のステージングエリアがない場合には、HA 環境で「`glance-direct`」メソッドを使用したイメージのアップロードが失敗する可能性があります。コントローラーノードで受信する要求は、利用可能なコントローラーノード間で分散されます。1 つのコントローラーが最初のステップを処理し、別のコントローラーが 2 番目の要求を処理し、両コントローラーは異なるステージングエリアにイメージを書き込みます。2 番目のコントローラーは最初のステップを処理するコントローラーが使用するのと同じステージングエリアにはアクセスできません。

Glance は、「`glance-direct`」メソッドを含む複数のイメージインポートメソッドをサポートしています。このメソッドは、3 段階方式を採用しており、イメージレコードを作成し、ステージングエリアにイメージをアップロードしてから、ステージングエリアからストレージバックエンドにイメージを移動して利用できるようにするステップで構成されます。HA の設定の場合は (コントローラー 3 台を使用)、`glance-direct` メソッドでは、全コントローラーノードにまたがった共有ファイルシステムを使用する共通のステージングエリアが必要です。

有効化する Glance インポートメソッドの一覧を設定できるようになりました。デフォルトの設定では、「`glance-direct`」メソッドは有効化されません (Web ダウンロードはデフォルトで有効化)。問題を回避して、HA 環境でイメージを Glance に確実にインポートできるようにするには、「`glance-direct`」メソッドは有効化しないでください。

BZ#1572238

`openvswitch systemd` スクリプトをホストで停止すると、`/run/openvswitch` フォルダが削除されます。

`ovn-controller` コンテナ内の `/run/openvswitch` パスは、古いディレクトリーになります。サービスが再度起動されると、新しいフォルダが再び作成されます。`ovn-controller` がこのフォルダに再度アクセスするには、そのフォルダを再マウントするか、`ovn-controller` コンテナを再起動する必要があります。

BZ#1309550

Cinder 用の RBD バックエンドで使用する Ceph プールの一覧を指定する新しい `CinderRbdExtraPools` Heat パラメーターが追加されました。一覧内の各プール用に追加の Cinder RBD バックエンドドライバーが作成されます。これは、`CinderRbdPoolName` に関連付けられた標準の RBD バックエンドドライバーに追加されます。新しいパラメーターは任意で、デフォルトでは空の一覧となります。すべてのプールが単一の Ceph クラスターに関連付けられます。

BZ#1518126

Redis は、TLS を有効化した HA デプロイメントでは、ノード間でデータのレプリケーションを正しく行うことができません。Redis のフォロワーノードにはリーダーノードからのデータは全く含まれません。Redis デプロイメントには TLS を無効にすることを推奨します。

BZ#1540239

今回の機能拡張により、Gnocchi DB インスタンスへのメトリックデータ送信がサポートされるようになりました。

collectd コンポーザブルサービス向けに以下の新しいパラメーターが追加されました。CollectdGnocchiAuthMode が「simple」に設定されると、CollectdGnocchiProtocol、CollectdGnocchiServer、CollectdGnocchiPort、CollectdGnocchiUser が設定に取り入れられます。

CollectdGnocchiAuthMode が「keystone」に設定されている場合には、CollectdGnocchiKeystone* パラメーターが設定に取り入れられます。

追加されたパラメーターに関する詳しい説明は以下のとおりです。

CollectdGnocchiAuthMode:

型: 文字列

説明: >

Gnocchi サーバーが使用する認証のタイプ。

サポートされている値は、「simple」と「keystone」です。

デフォルト: 'simple'

CollectdGnocchiProtocol:

型: 文字列

description: Gnocchi サーバーの使用する API プロトコル

default: 'http'

CollectdGnocchiServer:

型: 文字列

説明: >

メトリックの送信先となる gnocchi エンドポイントの名前またはアドレス

デフォルト: なし

CollectdGnocchiPort:

型: 数値

説明: Gnocchi サーバーに接続するためのポート

デフォルト: 8041

CollectdGnocchiUser:

型: 文字列

説明: >

簡易認証を使用して、リモートの Gnocchi サーバーに対して認証を行うためのユーザー名

デフォルト: なし

CollectdGnocchiKeystoneAuthUrl:

型: 文字列

説明: 認証先となる Keystone エンドポイントの URL

デフォルト: なし

CollectdGnocchiKeystoneUserName:

型: 文字列

説明: Keystone に対して認証を行うためのユーザー名

デフォルト: なし

CollectdGnocchiKeystoneUserId:

型: 文字列

説明: Keystone に対して認証を行うためのユーザー ID

デフォルト: なし

CollectdGnocchiKeystonePassword:
型: 文字列
説明: Keystone に対して認証を行うためのパスワード
デフォルト: なし

CollectdGnocchiKeystoneProjectId:
型: 文字列
説明: Keystone に対して認証を行うためのプロジェクト ID
デフォルト: なし

CollectdGnocchiKeystoneProjectName:
型: 文字列
説明: Keystone に対して認証を行うためのプロジェクト名
デフォルト: なし

CollectdGnocchiKeystoneUserDomainId:
型: 文字列
説明: Keystone に対して認証を行うためのユーザードメイン ID
デフォルト: なし

CollectdGnocchiKeystoneUserDomainName:
型: 文字列
説明: Keystone に対して認証を行うためのユーザードメイン名
デフォルト: なし

CollectdGnocchiKeystoneProjectDomainId:
型: 文字列
説明: Keystone に対して認証を行うためのプロジェクトドメイン ID
デフォルト: なし

CollectdGnocchiKeystoneProjectDomainName:
型: 文字列
説明: Keystone に対して認証を行うためのプロジェクトドメイン名
デフォルト: なし

CollectdGnocchiKeystoneRegionName:
型: 文字列
説明: Keystone に対して認証を行うためのリージョン名
デフォルト: なし

CollectdGnocchiKeystoneInterface:
型: 文字列
説明: 認証先となる Keystone エンドポイントの種別
デフォルト: なし

CollectdGnocchiKeystoneEndpoint:
型: 文字列
説明: >
Keystone の値を上書きする場合には、Gnocchi サーバーの URL を明示的に指定します。
デフォルト: なし

CollectdGnocchiResourceType:
型: 文字列
説明: >
ホストを保管するために Gnocchi によって作成される collectd-gnocchi プラグインのデフォルトのリソースタイプ
デフォルト: 'collectd'

CollectdGnocchiBatchSize:
型: 数値
説明: Gnocchi がバッチ処理すべき値の最小数
デフォルト: 10

OVN メタデータサービスは、DVR ベースの環境ではデプロイされませんでした。そのため、インスタンスは、メタデータ（例：インスタンス名、公開鍵など）をフェッチできませんでした。

本リリースで提供されているパッチにより、このサービスは有効になり、ブートしたインスタンスはメタデータをフェッチできるようになりました。

BZ#1568120

Cinder バックエンドサービス用の Heat テンプレートは、サービスがコンテナにデプロイされるべきかどうかには拘らず、Puppet をトリガーして cinder-volume サービスをオーバークラウドホストにデプロイしていたので、cinder-volume サービスはコンテナ内とホスト上に 2 回デプロイされていました。

これが原因で、OpenStack ボリュームの操作（ボリュームの作成と接続）は、ホスト上で実行される、正当ではない cinder-volume サービスによって操作が処理される場合に失敗することがありました。

そのため、Cinder バックエンドの heat テンプレートは cinder-volume サービスの 2 番目のインスタンスはデプロイしないように更新されました。

BZ#1573597

パフォーマンスの低い Swift クラスタが Gnocchi のバックエンドとして使用されると、collectd ログに 503 エラーと、gnocchi-metricd.conf に "ConnectionError: ('Connection aborted.', CannotSendRequest())" エラーが出力される場合があります。この問題を軽減するには、CollectdDefaultPollingInterval パラメーターの値を増やすか、Swift クラスタのパフォーマンスを改善してください。

BZ#1575023

ceph-ansible の複合 ceph-keys 処理により、`/etc/ceph/ceph.client.manila.keyring` ファイルの内容が誤って生成されるため、manila-share サービスの初期化が失敗します。

manila-share サービスを初期化できるようにするには、以下の手順を実行してください。

1) オーバークラウドのデプロイに使用する `/usr/share/openstack/tripleo-heat-templates` のコピーを作成します。

2) `.../tripleo-heat-templates/docker/services/ceph-ansible/ceph-base.yaml` ファイルを編集して、295 行目の 3 つ並んだバックスラッシュをすべて 1 つのバックスラッシュに変更します。

編集前:

```
mon_cap: 'allow r, allow command \\\\"auth del\\\\" , allow command \\\\"auth caps\\\\" , allow command \\\\"auth get\\\\" , allow command \\\\"auth get-or-create\\\\"'
```

編集後:

```
mon_cap: 'allow r, allow command \"auth del\", allow command \"auth caps\", allow command \"auth get\", allow command \"auth get-or-create\"'
```

3) `tripleo-heat-templates` のコピーのパスを、元の `overcloud-deploy` コマンドで実行した `/usr/share/openstack-tripleo-heat` テンプレートの場所に置き換えてオーバークラウドをデプロイします。

ceph キーの `/etc/ceph/ceph.client.manila.keyring` ファイルには適切な内容が記載されるようになり、manila-share サービスは正常に初期化されるようになります。

BZ#1552214

cinder-volume サービスを HA 用に設定する場合には、cinder の DEFAULT/host 設定は「hostgroup」に設定されていました。他の cinder サービス (cinder-api、cinder-scheduler、cinder-backup) は、そのサービスを実行しているのがどのオーバークラウドノードであるかに拘らず「hostgroup」をそれらの設定に使っていました。これらのサービスのログメッセージはすべて同じ「hostgroup」ホストから送られたように表示されていたため、どのノードがメッセージを生成したかを判断するのが困難でした。

HA をデプロイする際には、DEFAULT/host がその値に設定されるのではなく、cinder-volume の backend_host が「hostgroup」に設定されます。これにより、各ノードの DEFAULT/host 値が一意となります。

その結果、cinder-api、cinder-scheduler、cinder-backup からのログメッセージはそのメッセージを生成したノードに正しく関連付けられます。

BZ#1578901

以前は、新しいリリースにアップグレードした後も、Block Storage サービス (cinder) は前のリリースの古い RPC バージョンを使用している状態のままとなっていました。このため、最新の RPC バージョンを必要とする cinder API の要求はすべて失敗していました。

新しいリリースにアップグレードすると、cinder RPC バージョンはすべて最新リリースと一致するように更新されるようになりました。

python-cryptography

BZ#1556933

python-cryptography は、バージョン 2.1 より、証明書で使用されている CNS 名が IDN 標準に準拠していることを確認するようになりました。検出された名前がこの仕様に従っていない場合には、cryptography はその証明書の検証に失敗し、OpenStack コマンドラインインターフェースを使用する際や OpenStack のサービスログで異なるエラーが見つかる場合があります。

BZ#1571358

python-cryptography ビルドをインストールした後に、RDO からの最初のインポートは失敗していました。これは、Obsoletes が不足していたためです。また、このパッケージの RHEL 7 ビルドは正しく、適切な Obsoletes エントリーが含まれていました。

今回の修正で python-cryptography に Obsoletes が追加されました。

python-ironic-tests-tempest

BZ#1577982

アップグレードの前にインストールされる tempest のプラグイン (-tests) rpm は、OSP リリース 13 のアップグレードの後に失敗します。初回のアップグレードパッケージには古い RPM を廃止処理するために必要な epoch コマンドが含まれていませんでした。OSP 13 ではサブ

rpm は提供されず、新しいプラグイン rpm 内の Obsoletes は正しい rpm を適切に廃止処理しませんでした。

この問題を修正するには、Obsoletes を修正するか、古い rpm を手動でアンインストールして、代替りとなるプラグイン python2-*--tests-tempest を手動でインストールしてください。

python-networking-ovn

BZ#1433533

neutron と OVN のデータベース間の一貫性を維持するために、設定変更は内部で比較され、バックエンドで検証されます。各設定変更には改訂番号が割り当てられ、スケジュールされたタスクにより、データベースに加えられたすべての作成/更新/削除の操作は検証されます。

BZ#1503521

本バージョンでは、networking-ovn の内部 DNS 解決のサポートが追加されました。ただし、既知の制限事項が 2 点あり、その 1 つは bz#1581332 で、内部 DNS を介した内部 fqdn 要求が適切に解決されない問題です。

GA リリース版の tripleo は、デフォルトではこの拡張機能を設定しない点に注意してください。bz#1577592 で回避策を参照してください。

BZ#1550039

ゲートウェイなしでサブネットを作成すると、DHCP オプションは追加されず、そのようなサブネットを使用するインスタンスは DHCP を取得できません。

代わりに、Metadata/DHCP ポートはがこの目的で使用され、インスタンスは IP アドレスを取得することができます。これには、メタデータサービスを有効化する必要があります。外部ゲートウェイのないサブネット上のインスタンスは、OVN metadata/DHCP ポートを介して、DHCP から IP アドレスを取得できるようになりました。

BZ#1562731

現在の L3 HA スケジューラーはノードの優先度を考慮に入れないため、全ゲートウェイが同じノードでホストされ、負荷は候補間で分散されませんでした。

今回の修正により、ゲートウェイルーターをスケジューリングする際に負荷の最も低いノードを選択するためのアルゴリズムが実装されました。ゲートウェイポートは、最も負荷の低いネットワークノードでスケジュールされ、負荷はノード間で均等に分散されるようになりました。

BZ#1563678

サブポートが別のハイパーバイザー上の異なるトランクに再割り当てされた際に、バインディングの情報が更新されず、サブポートは ACTIVE に切り替わりませんでした。

今回の修正により、バインディング情報は、サブポートがトランクから削除された時に更新されるようになりました。サブポートは、異なるハイパーバイザーにある別のトランクポートに再度割り当てられると、ACTIVE に切り替わりようになりました。

python-os-brick

BZ#[1550974](#)

iSCSI ディスカバリーを使用する際に、ノードの起動設定が「automatic」から「default」にリセットされていたため、リブート時にサービスが起動しない原因となっていました。この問題は、ディスクバリーを実行した後にスタートアップの値をすべて復元することにより修正されます。

python-zaqar-tests-tempest

BZ#[1546285](#)

tempest プラグインのコレクションは、Queens サイクル中の openstack-*-tests rpm のサブパッケージから抽出されるので、アップグレードには依存関係の問題がありました。ただし、すべてのパッケージに Provides と Obsoletes の正しい組み合わせがあるわけではありませんでした。OSP 13 には -tests (未テストのサブ rpm) はありません。

以前のリリースからインストールした -tests を使用してアップグレードを試みると、依存関係の問題により操作は失敗します。

この問題を修正するために、-tests rpm の古いバージョンの Obsoletes が、抽出した先に再度追加されました。