



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

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Release_Notes.ent file |.

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, the Red Hat 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 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

本書は、Red Hat OpenStack Platform の本リリースにおける主要機能、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	5
1.1. 本リリースについて	5
1.2. 要件	5
1.3. デプロイメント制限事項	5
1.4. データベースサイズの管理	6
1.5. 認定済みのドライバーとプラグイン	6
1.6. 認定済みゲストオペレーティングシステム	6
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	6
1.8. ハイパーバイザーのサポート	6
1.9. コンテンツ配信ネットワーク (CDN) のリポジトリ	6
1.10. 製品サポート	8
1.11. サポートされない機能	8
第2章 最も重要な新機能	10
2.1. RED HAT OPENSTACK PLATFORM DIRECTOR	10
2.2. コンテナ	10
2.3. BARE METAL サービス	10
2.4. CEPH STORAGE	10
2.5. COMPUTE	11
2.6. 高可用性	11
2.7. メトリックとモニターリング	12
2.8. ネットワーク機能仮想化	13
2.9. OPENDAYLIGHT	13
2.10. OPENSTACK NETWORKING	13
2.11. セキュリティ	14
2.12. ストレージ	14
2.13. テクノロジープレビュー	15
2.13.1. 新規テクノロジープレビュー	16
2.13.2. 以前にリリースされたテクノロジープレビュー	16
第3章 リリースの情報	18
3.1. RED HAT OPENSTACK PLATFORM 13 GA	18
3.1.1. 機能拡張	18
3.1.2. テクノロジープレビュー	21
3.1.3. リリースノート	21
3.1.4. 既知の問題	24
3.2. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2018 年 7 月 19 日)	31
3.2.1. 機能拡張	31
3.2.2. リリースノート	31
3.2.3. 既知の問題	31
3.3. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2018 年 8 月 29 日)	33
3.3.1. 機能拡張	33
3.3.2. リリースノート	35
3.3.3. 既知の問題	36
3.4. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2018 年 11 月 13 日)	36
3.4.1. 機能拡張	36
3.4.2. リリースノート	38
3.4.3. 既知の問題	38
3.5. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 1 月 16 日)	39
3.5.1. 機能拡張	39
3.5.2. 既知の問題	40

3.6. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 3 月 13 日)	40
3.6.1. 機能拡張	41
3.6.2. リリースノート	42
3.6.3. 既知の問題	42
3.6.4. 廃止された機能	43
3.7. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 4 月 30 日)	43
3.7.1. 機能拡張	43
3.7.2. 既知の問題	44
3.8. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 7 月 10 日)	44
3.8.1. 機能拡張	44
3.8.2. テクノロジーレビュー	45
3.8.3. リリースノート	45
3.8.4. 既知の問題	46
3.9. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 9 月 4 日)	46
3.9.1. 機能拡張	46
3.9.2. テクノロジーレビュー	47
3.9.3. リリースノート	47
3.9.4. 既知の問題	48
3.9.5. 非推奨になった機能	48
3.10. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 11 月 6 日)	49
3.10.1. 機能拡張	49
3.11. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 12 月 19 日)	50
3.11.1. 機能拡張	50
3.11.2. 非推奨になった機能	51
3.12. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 3 月 10 日)	51
3.12.1. 機能拡張	51
3.13. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 6 月 24 日)	52
3.13.1. バグ修正	53
3.13.2. 機能拡張	54
3.13.3. リリースノート	54
3.14. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 10 月 28 日)	54
3.14.1. バグ修正	54
3.14.2. 機能拡張	56
3.14.3. 既知の問題	57
3.15. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 12 月 16 日)	57
3.15.1. バグ修正	58
3.16. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2021 年 3 月 17 日)	58
3.16.1. バグ修正	58
3.16.2. 既知の問題	58
3.17. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2021 年 6 月 16 日)	59
3.17.1. バグ修正	59
3.17.2. 機能拡張	61
3.17.3. リリースノート	61
第4章 テクニカルノート	62
4.1. RHEA-2018:2086: RED HAT OPENSTACK PLATFORM 13.0 の機能拡張アドバイザー	62
4.2. RHSA-2018:2214 (重要): OPENSTACK-TRIPLEO-HEAT-TEMPLATES のセキュリティー更新	72
4.3. RHBA-2018:2215: OPENSTACK-NEUTRON のバグ修正アドバイザー	74
4.4. RHBA-2018:2573: OPENSTACK PLATFORM 13 のバグ修正と機能拡張アドバイザー	76
4.5. RHBA-2018:2574: OPENSTACK DIRECTOR のバグ修正アドバイザー	78
4.6. RHBA-2018:3587: RED HAT OPENSTACK PLATFORM 13.0 DIRECTOR のバグ修正アドバイザー	84
4.7. RHBA-2019:0068: RED HAT OPENSTACK PLATFORM 13 のバグ修正および機能拡張アドバイザー	88
4.8. RHBA-2019:0448: RED HAT OPENSTACK PLATFORM 13 のバグ修正および機能拡張アドバイザー	90

4.9. RHBA-2021:2385 - RED HAT OPENSTACK PLATFORM 13 のバグ修正および機能拡張アドバイザー	93
--	----

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、OpenStackQueens リリースをベースにしています。これには、Red Hat OpenStack Platform 固有の追加機能、既知の問題、および解決済みの問題が含まれます。

本書には、Red Hat OpenStack Platform 固有の変更のみを記載しています。OpenStackQueens 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。

[Red Hat OpenStack Platform のライフサイクル](#)

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。

[OpenStack について理解する](#)



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、[Support for the Pacemaker resource manager in RHEL 6 High Availability clusters](#) を参照してください。

1.2. 要件

Red Hat OpenStack Platform がサポートするのは、Red Hat Enterprise Linux 7 の最新リリースのみです。

Red Hat OpenStack Platform の Dashboard (horizon) 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イスです。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

Internet Explorer 11 を使用して Dashboard を表示することはできますが、ブラウザーは維持されなくなったため、一部機能の低下が予想されます。

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](#) のアート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](#) のアート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](#) のアート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、[Red Hat OpenStack Platform および Red Hat Enterprise Virtualization で認定されたゲストオペレーティングシステム](#) のアート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 \(ironic\)](#) のアート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 (コンピュータノード上で 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 リポジトリを有効化するには、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-*

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



警告

Red Hat OpenStack Platform ソフトウェアリポジトリのパッケージは、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、幅広いリソースを提供しています。カスタマーポータルから、以下のリソースを利用することができます。

- ナレッジベースアトicle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。

[RHSA-announce -- Security announcements for all Red Hat products and services.](#) でサブスクライブしてください。

1.11. サポートされない機能

以下の機能は、Red Hat OpenStack Platform ではサポートされません。

- カスタムポリシー。手動で、または ***Policies** heat パラメーターにより、**policy.json** ファイルの変更が含まれます。ドキュメントに明示的な指示が含まれている場合を除き、デフォルトのポリシーは変更しないでください。

これらの機能のサポートが必要な場合は、[Red Hat Customer Experience and Engagement チーム](#) に連絡してサポート例外を入手してください。

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、[Fast Forward Upgrade](#) に記載しています。

Red Hat Virtualization コントロールプレーン

director は、Red Hat Virtualization にデプロイされたコントローラーノードを使用したオーバークラウドのプロビジョニングをサポートするようになりました。新しい仮想化機能に関する詳しい情報は、[Virtualize your OpenStack control plane with Red Hat Virtualization and Red Hat OpenStack Platform 13](#) を参照してください。

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)、および 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。

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。詳しい手順は、[スパイン/リーフ型ネットワーク](#) 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 (**staging-ovirt**) が含まれています。

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。

2.4. CEPH STORAGE

本項では、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。Red Hat Ceph Storage 2.x (Jewel) を実行する外部クラスター (director によりデプロイされないクラスター) は、より新しい Ceph クライアントとの互換性を維持します。director を使用して Ceph クラスター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 クラスター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イスを介してのみ CephFS にアクセスすることができます。この新機能は director に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 クラスター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 デーモン

Ceph rbd-mirror デーモンは、リモートクラスターからイメージの更新をプルして、ローカルクラスター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 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 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 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 (Fast Forward Upgrade を含む)、インスタンス 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ーリング

本項では、メトリックおよびモニター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イ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イスのリンクステータスをモニターリングして、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ーリングする **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) のモニター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、モニター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ためには、アーカイブポリシールールが適合するようにしてください。

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します。

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。

Telemetry API および ceilometer-collector の廃止

Telemetry API サービスは、**OpenStack Telemetry Metrics** (gnocchi) サービスおよび **OpenStack Telemetry Alarming** (aodh) サービス API に置き換えられています。ceilometer-collector サービスは **ceilometer-notification-agent** デーモンに置き換えられています。Telemetry ポーリングエージェントがサンプルファイルからのメッセージを **ceilometer-notification-agent** デーモンに送付するためです。



注記

ceilometer 全体が非推奨になった訳ではなく、Telemetry API サービスおよび ceilometer-collector サービスが非推奨となっただけです。

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) コンピュートノードが 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。

これに含まれる機能を以下に示します。

- データプレーンの抽象化: プラットフォーム用 P4 プラグイン
- コンテナ: Kubernetes 用プラグイン、および VM/コンテナ混在環境用の Neutron Northbound 機能拡張の開発

詳しい情報は、[Red Hat OpenDaylight Product Guide](#) と [Red Hat OpenDaylight のインストールおよび設定ガイド](#) 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出力ドバイバランシングドライバーが含まれています。

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、保存データを保護します。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: 保存データの暗号化と 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。

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。

Shared File System: 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イスを介してのみ CephFS にアクセスすることができます。この新機能は director に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。

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設定されます。

- サーバープロバイダー: 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イスを提供します。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、コンピュータ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ー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ー (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イ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 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、非推奨に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の情報は、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、非推奨に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

説明: Gnocchi サーバーが使用する API プロトコル

デフォルト: 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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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

BZ#1592823

Ansible Playbook のログに、デプロイメント、更新、アップグレード中のアクションのタイミングに関する情報を提供するタイムスタンプが含まれるようになりました。

3.1.2. テクノロジープレビュー

本セクションに記載する項目は、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ステータスのスコープ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、[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。

BZ#1446311

今回のリリースで、PCI デバイスの NUMA アフィニティーポリシーに対するサポートが追加されました。このポリシーは、[pci]alias の設定オプションの一部として設定します。以下の 3 つのポリシーがサポートされます。

required(必須)、legacy(デフォルト。利用可能な場合には必須)、preferred(あると良い)

いずれの場合も、可能であれば、厳格な NUMA アフィニティーが提供されます。これらのポリシーにより、リソースの使用率を最大化するために、PCI エイリアスごとの NUMA アフィニティーをどの程度厳格にするかを設定できるようになります。これらのポリシー間の主要な相違点は、どれだけの NUMA アフィニティーを破棄するとスケジューリングが失敗するかという点です。

PCI デバイスに preferred ポリシーを設定した場合、PCI デバイスの NUMA ノードとは異なる NUMA ノードが利用できれば、nova はそのノード上の CPU を使用します。これにより、リソースの使用率が高くなりますが、それらのインスタンスのパフォーマンスは低減します。

BZ#1488095

RHOSP 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 クライアントの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イスを介してのみ CephFS にアクセスすることができます。この新機能は director に完全に統合され、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 サービスがコンテナ化されている場合には、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 では、デフォルトではこの拡張機能が設定され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- の接頭辞は削除されました。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イスを使用する際や 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。このパラメーター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、オーバークラウドの高度なカスタマイズのカスタムコンポーザブルネットワーク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に、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タ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、次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 DuplicateMessageError: Found duplicate message(629ff0024219488499b0fac0caciaa3a5). Skipping

it.の形式のエントリーが表示される。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コマンド pcs resource restart rabbitmq-bundle 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)。

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、直接コンピュータノード上で 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

director のアンダークラウドをバックアップおよび復元する手順でリグレッションが確認されました。その結果、手順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、director のアンダークラウドのバックアップと復元は 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、heat パラメーター OpenDaylightLogMechanism: 'file' を設定します。

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、次のような場合にテナントの VLAN ネットワークで発生します。NAPT 以外のスイッチ上で起動する仮想マシンに Floating IP が割り当てられた。その後その Floating IP が削除された。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。ただし、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コンピュータードに分散している場合に発生します。この問題には、適切な回避策はありません。

BZ#1568976

デプロイメント中に、1つまたは複数の OpenDaylight のインスタンスが正しく起動できない場合があります。これは、機能の読み込みのバグが原因です。このために、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。

デプロイメントが合格した場合、そのデプロイメントが正常に実行されるには、3つの OpenDaylight インスタンス中2つが機能している必要があります。3つ目の OpenDaylight インスタンスが正しく起動されていない可能性があります。 **docker ps** コマンドで、各コンテナの正常性ステータスを確認してください。正常でない場合には、 **docker restart opendaylight_api** でそのコンテナを再起動します。

デプロイメントが失敗した場合の唯一のオプションは、そのデプロイメントを再起動することです。TLS ベースのデプロイメントの場合には、OpenDaylight の全インスタンスが正しく起動しないと、デプロイメントは失敗します。

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次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、次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ーリングして、クラスターメンバーの正常性を確認する ([http://\\$ODL_IP:8081/jolokia/read/org.opendaylight.controller:Category=ShardManager,name=shard-manager-config,type=DistributedConfigDatastore](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 台のコンピュータ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となります。

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イスを使用する場合に、そのインターフェイスが OVS ブリッジに接続されていなければ、OpenDaylight 環境のトラフィックはそのインターフェイスを通過しません。したがって、この種の設定は避けるべきです。

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イスをこの 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イスを使用すると、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します。この問題は、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、いずれかの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、次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を、ネットワーク設定 1 つにつき 1450 の MTU を使用するように設定する。NeutronGlobalPhysnetMtu heat パラメーターを 1450 に設定する。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正しくサポートするには、ネットワークの負荷分散に使用される HAProxy はバージョン 1.6 またはそれ以降でなければなりません。

Red Hat OpenStack Platform 13 に含まれる HAProxy は 1.6 より古いバージョンで、PING タイプのヘルスマニターを設定すると TCP 接続が使用されます。

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。この失敗が、ceph-ansible の実行に影響を及ぼす場合があります。これには、複数のコンピュータードを使用している、または 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している新規デプロイメントが含まれます。

BZ#1590938

RHCS3 上に OSD を 4 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 [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イ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ます。したがって、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。

以下の回避策のいずれか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正常にダウンロードされるようになるはずですが。

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。

回避策としては、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する方法があります。

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。ただし、RHOSP 13 では回避策はありません。ただし、RHOSP 14 およびそれ以降のリリースではこの問題は修正されています。

BZ#1790653

OpenStack Networking がポートをバインドする手法により、DVR 環境でネットワークインスタンスのライブマイグレーションを行うと、Floating IP アドレスを使用する既存の接続が切断される場合があります。現在、RHOSP 13 では回避策はありません。ただし、RHOSP 14 およびそれ以降のリリースではこの問題は修正されています。

3.2. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2018年7月19日)

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、非推奨になった機能について記載します。

3.2.1. 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#1592823

Ansible Playbook のログに、デプロイメント、更新、アップグレード中のアクションのタイミングに関する情報を提供するタイムスタンプが含まれるようになりました。

3.2.2. 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#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に、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 ovsdb_probe_interval の値を 600000 ミリ秒に増やしてください。

3.2.3. 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#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#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#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、heat パラメーター OpenDaylightLogMechanism: 'file' を設定します。

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コンピューターノードに分散している場合に発生します。この問題には、適切な回避策はありません。

BZ#1568976

デプロイメント中に、1つまたは複数の OpenDaylight のインスタンスが正しく起動できない場合があります。これは、機能の読み込みのバグが原因です。このために、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。

デプロイメントが合格した場合、そのデプロイメントが正常に実行されるには、3つの OpenDaylight インスタンス中2つが機能している必要があります。3つ目の OpenDaylight インスタンスが正しく起動されていない可能性があります。**docker ps** コマンドで、各コンテナの正常性ステータスを確認してください。正常でない場合には、**docker restart opendaylight_api** でそのコンテナを再起動します。

デプロイメントが失敗した場合の唯一のオプションは、そのデプロイメントを再起動することです。TLS ベースのデプロイメントの場合には、OpenDaylight の全インスタンスが正しく起動しないと、デプロイメントは失敗します。

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#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#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
# iptables -A INPUT -p tcp -m multiport --dports 13876 -m state --state NEW -m comment --
comment "100 octavia_api_haproxy_ssl ipv6" -j ACCEPT
# iptables -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
```

3.3. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2018 年 8 月 29 日)

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、非推奨になった機能について記載します。

3.3.1. 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#1561961

この機能により、PCI デバイスの NUMA アフィニティーポリシーがサポートされるようになりました。このポリシーは、`[pci]alias` の設定オプションの一部として設定します。**required**、**legacy**、**preferred** の3つのポリシーがサポートされています。いずれの場合も、可能であれば、厳格な NUMA アフィニティーが提供されます。これらのポリシー間の主要な相違点は、どれだけの NUMA アフィニティーを破棄するとスケジューリングが失敗するかという点です。これらのポリシーにより、デバイスごとまたはより具体的にするにはデバイスエイリアスごとに、NUMA アフィニティーをどの程度厳格にするかを設定できます。これは、リソース使用率を最大化するのに役立ちます。PCI デバイスに `preferred` ポリシーを設定した場合、PCI デバイスの NUMA ノードとは異なる NUMA ノードしか利用できなければ、nova はそのノード上の CPU を使用するようになります。これにより、リソースの使用率が高くなりますが、それらのインスタンスのパフォーマンスは低減するというマイナス面があります。

BZ#1564918

以前のリリースでは、Ironic は、再試行可能な IPMI エラーのタイプは1つのみと見なしていました。このために、Ironic で不明なエラーが発生する場合があります。今回の機能拡張により、Ironic は、電源管理のハードウェアインターフェイスなど IPMI でバッキングされるハードウェアのインターフェイスでより多くの IPMI エラーメッセージタイプを再試行可能として扱うようになりました。具体的には、Node busy、Timeout、Out of space、および BMC initialization in progress の IPMI エラーが発生すると Ironic が IPMI コマンドを再試行します。その結果、IPMI をベースとする BMC との通信の信頼度が高くなりました。

BZ#1571741

Nova の libvirt ドライバーは、CPU モデルの設定時に、CPU 機能のフラグをより細かく指定できるようになりました。

この変更の1つの利点は、MeltdownCVE の修正を適用した後に、Intel ベースの仮想 CPU モデルで実行しているゲスト上でパフォーマンスの低下が軽減される点が挙げられます。ゲストのパフォーマンスに対する影響は、CPU 機能フラグ PCID(Process-Context ID) を **guest** CPU に公開することによって軽減されます。これは、物理ハードウェア自体の中に PCID フラグが利用可能であることを前提とします。

使用方法についての詳しい情報は、**nova.conf** の **[libvirt]/cpu_model_extra_flags** の説明を参照してください。

BZ#1574349

オーバークラウドをデプロイする前に、クラスター向けに stonith リソースを自動作成することができます。デプロイメントを開始する前に、コマンド `openstack overcloud generate fencing --ipmi-lanplus --output /home/stack/fencing.yaml /home/stack/instackenv.json` を実行します。

次に、デプロイコマンドの引数リストに `-e /home/stack/fencing.yaml` を渡します。これで、クラスターに必要な stonith リソースが自動的に作成されます。

BZ#1578633

rhosp-director-images がマルチアーキテクチャー対応になりました。OSP 13 は、ppc64le 向けのオーバークラウドの完全なイメージと、ironic python エージェントのイメージを使用するようになりました。rhosp-director-images は、この変更に対応するように調整されました。その結果、rhosp-director-images と rhosp-director-images-ipa はメタパッケージとなり、rhosp-director-images-`<arch>` と rhosp-director-images-ipa-`<arch>` の rpm が追加されて、マルチアーキテクチャーをサポートするようになりました。

BZ#1578636

rhosp-director-images がマルチアーキテクチャー対応になりました。OSP 13 は、ppc64le 向けのオーバークラウドの完全なイメージと、ironic python エージェントのイメージを使用するようになりました。rhosp-director-images は、この変更に対応するように調整されました。その結果、rhosp-director-images と rhosp-director-images-ipa はメタパッケージとなり、rhosp-director-images-`<arch>` と rhosp-director-images-ipa-`<arch>` の rpm が追加されて、マルチアーキテクチャーをサポートするようになりました。

BZ#1579691

Nova の libvirt ドライバーは、CPU モデルの設定時に、CPU 機能のフラグをより細かく指定できるようになりました。この変更の1つの利点は、"Meltdown" CVE の修正を適用した後に、Intel ベースの仮想 CPU モデルで実行しているゲスト上でパフォーマンスの低下が軽減される点が挙げられます。ゲストのパフォーマンスに対する影響は、CPU 機能フラグ PCID(Process-Context ID) を **guest** CPU に公開することによって軽減されます。これは、物理ハードウェア自体の中に PCID フラグが利用可能であることを前提とします。この変更により、PCID のみが CPU 機能フラグであった制限がなくなり、複数の CPU フラグの追加/削除が可能となったため、他のユースケースに対応するようになりました。詳しい情報は、**nova.conf** の **[libvirt]/cpu_model_extra_flags** の説明を参照してください。

BZ#1601472

NFV がデプロイされた RHOSP 10 から RHOSP 13 にアップグレードする手順が再テストされ、DPDK および SR-IOV の環境向けに更新されました。

BZ#1606224

今回の更新により、Red Hat のサポートする全 CPU アーキテクチャー上の KVM 仮想化で Ceph Storage がサポートされるようになりました。

BZ#1609352

今回の機能拡張で、nova とユーティリティ用に GA のコンテナと、IBM Power LE 上の Cinder、Glance、Keystone、Neutron、Swift 用にテクノロジープレビューのコンテナが追加されました。

BZ#1619311

rhosp-director-images がマルチアーキテクチャー対応になりました。OSP 13 は、ppc64le 向けのオーバークラウドの完全なイメージと、ironic python エージェントのイメージを使用するようになりました。

た。rhaps-director-images は、この変更に対応するように調整されました。その結果、rhaps-director-images と rhaps-director-images-ipa はメタパッケージとなり、rhaps-director-images-`<arch>` と rhaps-director-images-ipa-`<arch>` の rpm が追加されて、マルチアーキテクチャーをサポートするようになりました。

3.3.2. 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#1523864

今回の更新で、Dell-EMC Unity と VNX バックエンドでの Manila IPv6 エクスポートのロケーションおよびアクセスルールの使用がサポートされるようになりました。

BZ#1549770

コンテナがデフォルトのデプロイメント方法になりました。ベアメタルサービスを environments/baremetal-services.yaml でデプロイする方法はまだ使用できますが、いずれはなくなる見込みです。

environments/services-docker を参照するリソースレジストリーが記載された環境ファイルで、environments/services パスに変更する必要があります。デプロイされているベアメタルサービスを確保する必要がある場合には、最初に配置した environments/services の代わりに environments/services-baremetal に参照を更新してください。

BZ#1565028

OpenDaylight ログの正しいパスが記載された README が /var/log/opendaylight に追加されました。

BZ#1570039

ローテーションされるログをデフォルトで圧縮する、コンテナ化された logrotate サービスの圧縮オプションが追加されました。delaycompress オプションを使用すると、ログファイルの最初のローテーションは圧縮されないようになります。

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。このパラメーター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、オーバークラウドの高度なカスタマイズのカスタムコンポーザブルネットワーク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#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、次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 DuplicateMessageError: Found duplicate message(629ff0024219488499b0fac0caciaa3a5). Skipping

it.の形式のエントリーが表示される。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コマンド pcs resource restart rabbitmq-bundle 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)。

3.3.3. 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#1557794

director のアンダークラウドをバックアップおよび復元する手順でリグレッションが確認されました。その結果、手順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、director のアンダークラウドのバックアップと復元は 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#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します。この問題は、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、いずれかの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#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、次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

3.4. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2018 年 11 月 13 日)

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、非推奨になった機能について記載します。

3.4.1. 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#1466117

OpenStack director の一部として MTU を設定するために、本リリースでは NeutronML2PhysicalNetworkMtus として **neutron::plugins::ml2::physical_network_mtus** が heat テ

ンプレートに追加され、ml2 プラグインの MTU が有効化されるようになりました。`neutron::plugins::ml2::physical_network_mtus` は、TripleO heat テンプレートからの値を元に設定されません。

BZ#1545151

OpenStack が更新またはアップグレードされると、director は最新の amphora イメージを glance にアップロードします。最新の amphora イメージにより、最新の一般バグ修正およびセキュリティー上の修正が適用された状態で amphora インスタンスが実行されます。これには、Octavia エージェントに関する修正だけでなく、オペレーティングシステムに関する修正も含まれます。

今回のリリースで、新たに作成される amphora インスタンスおよび再作成される amphora インスタンスに、最新の amphora イメージが使用されるようになりました。それまでの amphora イメージは、名前を変更して (接尾辞にタイムスタンプを追加) 引き続き glance に保管されます。

BZ#1561961

この機能により、PCI デバイスの NUMA アフィニティーポリシーがサポートされるようになりました。このポリシーは、`[pci]alias` の設定オプションの一部として設定します。`required`、`legacy`、`preferred` の 3 つのポリシーがサポートされています。いずれの場合も、可能であれば、厳格な NUMA アフィニティーが提供されます。これらのポリシー間の主要な相違点は、どれだけの NUMA アフィニティーを破棄するとスケジューリングが失敗するかという点です。これらのポリシーにより、デバイスごとまたはより具体的にするにはデバイスエイリアスごとに、NUMA アフィニティーをどの程度厳格にするかを設定できます。これは、リソース使用率を最大化するのに役立ちます。PCI デバイスに `preferred` ポリシーを設定した場合、PCI デバイスの NUMA ノードとは異なる NUMA ノードしか利用できなければ、nova はそのノード上の CPU を使用するようになります。これにより、リソースの使用率が高くなりますが、それらのインスタンスのパフォーマンスは低減するというマイナス面があります。

BZ#1571286

重み付け関数 `CPUWeigher` を使用して、仮想 CPU の使用状況に応じて負荷をホストに分散する (デフォルト)、または集約することができます。`nova.conf` の `[filter_scheduler] cpu_weight_multiplier` 設定オプションを `-1.0` または `1.0` に設定することができます。このオプションを `1.0` に設定すると、インスタンスはホスト全体に分散されます。このオプションを `-1.0` に設定すると、インスタンスは 1 つのホストに集約されます。値を `0` に設定すると、重み付け関数は無効になります。

BZ#1619485

`multipathd show status` が返すべきエラーコードを返さない状況があります。したがって、`multipathd` がエラー状態にあることを正しく検出するために、この問題の回避策として `stdout` を確認していません。

BZ#1628786

マルチアーキテクチャー環境での Ceph のセットアップ失敗を防ぐために、今回の更新でクライアントユーザー、鍵、およびプールの Ceph セットアップが `x86_64` 以外のシステムでは実行されないようになりました。

Ceph のセットアップは、`x86_64` システムでのみサポートされます。今回の更新以前は、クライアントグループの最初のインベントリ項目が `x86_64` 以外のシステムの場合には、そのシステム上での Ceph セットアップの試みは失敗し、その結果 `ceph-install` が中断していました。

BZ#1629873

iSCSI デバイスの検出では、再スキャンの時間を元にデバイスの有無を確認していました。したがって、スキャンとスキャンの間に利用可能になるデバイスは検出されませんでした。今回のリリースでは、検索と再スキャンは異なるリズムで動作する独立した操作になり、1 秒ごとに確認が行われます。

BZ#1631009

以前のバージョンでは、オーバークラウドと同様に、アンダークラウド hieradata のオーバーライド値を使用して <service>::config オプションにより一部のサービス設定をチューニングすることができました。ただし、この機能はデプロイされたすべての OpenStack サービスで利用可能なわけではありませんでした。今回のバージョンでは、現在利用できないあらゆる設定値を、<service>::config hieradata により更新することができるようになりました。

BZ#1640833

ボリュームのタイプ変更および移行操作のサポートが、Block Storage サービスの HPE Nimble Storage ドライバーに追加されました。

3.4.2. 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#1496584

neutron サービスがコンテナ化されている場合には、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、コマンドは以下のようになります。

```
# 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#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#1589849

OVN メタデータエージェントがコンピューター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。

3.4.3. 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#1621062

octavia-amphora ファイルの名前を変更すると、シンボリックリンクのリンクが切れたり、不適切な名前のシンボリックリンクが生成されたりします。回避策としては、`/usr/sbin/rhosp-director-image-update` を実行する方法があります。これにより問題が解決します。

3.5. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019年1月16日)

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、非推奨になった機能について記載します。

3.5.1. 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#1476282

overcloud-minimal qcow2 イメージを使用して、オーバークラウドの最小バージョンをデプロイできるようになりました。この最小インストールでは、更新のための OpenStack エンタイトルメントは必要ありません。

BZ#1600115

以前のリリースでは、OVN 論理ルーターを使用する新規接続の最初のパケットは、送信先の MAC アドレスを特定するのに使われていました。その結果、新規接続の最初のパケットが失われていました。

今回の機能拡張で、新規接続の最初のパケットを正しくキューに入れる機能が追加され、そのパケットが失われなくなりました。

BZ#1607362

この機能により、IPv6 アドレスへの OpenDaylight (ODL) のデプロイがサポートされるようになりました。

BZ#1635892

従来 Octavia は、VIP および VRRP Amphora ポートに関連付けられたセキュリティーグループに Octavia のプロジェクト ID を割り当てていました。このため、ユーザーはロードバランサーへのアクセスを制限できませんでした。今回の修正で、SG の所有者を変更してユーザープロジェクト (ホワイトリストに登録された特定のプロジェクト) に所属させるオプションが追加され、ユーザーはロードバランサーへのアクセスポリシーを細かく設定できるようになりました。

BZ#1636395

この機能により、信頼済み SR-IOV 仮想機能 (VF) を持つインスタンスの作成が可能になり、VF の MAC アドレスを変更し、ゲストインスタンスから直接プロミスキャスモードを有効にすることができるようになりました。この機能は、インスタンスのフェイルオーバー VF を直接インスタンスから設定するのに役立ちます。

VF を信頼済みモードに設定するには、まず `nova.conf` の `[pci] passthrough_whitelist` JSON 設定オプションの `trusted` の値を設定します。その後、バイndディングプロファイルで `trusted=true` 属性を設定したポートを作成します。`vnictype` 属性の値は、必ず `hw_veb` または `direct` に設定してください。

BZ#1644020

この機能により、新たなパラメーター `NovaLibvirtVolumeUseMultipath` (ブール値) が追加されました。これにより、コンピュータノードの `nova.conf` ファイルでマルチパス設定パラメーター `libvirt/volume_use_multipath` が設定されます。このパラメーターは、Compute ロールごとに設定す

ることができます。デフォルト値は **False** です。

BZ#1646907

この機能により、セキュリティーが強化された完全なイメージを UEFI モードでブートする機能が追加されました。

BZ#1648261

今回の機能拡張で、パラメーター **NeutronOVSTunnelCsum** が追加されました。これにより、heat テンプレートで **neutron::agents::ml2::ovs::tunnel_csum** を設定することができます。このパラメーターにより、OVS エージェントの発信 IP パケットを転送する GRE/VXLAN トンネルのトンネルヘッダーチェックサムを設定または削除します。

BZ#1656495

この機能により、パラメーター **NovaSchedulerWorkers** が追加されました。これにより、スケジューラーノードごとに複数の **nova-schedule** ワーカーを設定することができます。デフォルト値は **1** です。

3.5.2. 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#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。

1. 問題の発生したノードを再起動します。
2. REST エンドポイントをモニターリングして、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](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#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します。この問題は、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、いずれかの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
```

3.6. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 3 月 13 日)

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、非推奨になった機能について記載します。

3.6.1. 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#1636496

今回の更新により、以下のパラメーターを使用して、バックエンドメンバーおよびフロントエンドクライアントのデフォルトの Octavia タイムアウトを設定できるようになりました。

- **OctaviaTimeoutClientData**: フロントエンドクライアントの停止状態タイムアウト
- **OctaviaTimeoutMemberConnect**: バックエンドメンバーの接続タイムアウト
- **OctaviaTimeoutMemberData**: バックエンドメンバーの停止状態タイムアウト
- **OctaviaTimeoutTcpInspect**: コンテンツの検査用に TCP パケットを待機する時間

これらすべてのパラメーターの値は、ミリ秒単位です。

BZ#1636895

今回の更新により、IPv6 アドレスにトンネルエンドポイントを作成できるようになりました。

BZ#1650576

以前のリリースでは、OpenDaylight のパッケージングでは OpenDaylight **log_pattern** のデフォルト値が使用され、PaxOsgi アペンダーが含まれていました。これらのデフォルト値が常にすべてのデプロイメントに適する訳ではなく、カスタムの値を設定することが望ましいこともあります。

今回の更新により、**puppet-.opendaylight** に 2 つの設定変数が追加されています。

- **log_pattern**: この変数を使用して、OpenDaylight ロガー log4j2 で使用するログパターンを設定します。
- **enable_paxosgi_appender**: このブール値フラグを使用して、PaxOsgi アペンダーを有効または無効にします。

puppet-.opendaylight では、OpenDaylight のデフォルト値も変更されています。**puppet-.opendaylight** を使用するデプロイメントは、以下に示す新しいデフォルト値を持ちます。

- **log_pattern**: `%d{ISO8601} | %-5p | %-16t | %-60c{6} | %m%n`
- **enable_paxosgi_appender**: `false`

新たな変数設定オプション

log_pattern

ログ記録に使用するログパターンを指定する文字列

デフォルト: `%d{ISO8601} | %-5p | %-16t | %-60c{6} | %m%n`

有効なオプション: 有効な log4j2 パターンである文字列

enable_paxosgi_logger

ログ記録に PaxOsgi アペンダーを有効にするかどうかを指定するブール値

enable_paxosgi_logger 変数を有効にする場合、追加機能を使用するためにログパターンも変更する必要があります。**log_pattern** 変数を変更し、PaxOsgi トークンが含まれるパターンを含めます。たとえば、**log_pattern** 変数を以下の値が含まれる文字列に設定します。

```
'%X{bundle.id} - %X{bundle.name} -
+
%X{bundle.version}'
```

log_pattern 変数を編集しない場合、PaxOsgi アペンダーは有効で動作を続けますが、ログ記録に追加機能は使用されません。

たとえば、**enable_paxosgi_logger** 変数を **true** に設定し、**log_pattern** 変数を以下の値に設定します。

```
'%d{ISO8601} | %-5p | %-16t | %-32c{1} | %X{bundle.id} - %X{bundle.name} - %X{bundle.version}
| %m%n'
```

デフォルト: **false**

有効なオプション: ブール値 **true** および **false**

3.6.2. 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#1597666

今回の更新により、OpenDaylight のマイナー更新が Red Hat OpenStack Platform のマイナー更新ワークフローに含まれるようになりました。

BZ#1611960

今回の更新により、バックエンドとして OpenDaylight を使用する Red Hat OpenStack Platform 環境のコンピューターノードが、正常にスケーリングできるようになりました。

3.6.3. 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#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 台のコンピューター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となります。

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#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。

3.6.4. 廃止された機能

以下の機能は、Red Hat OpenStack Platform の今回のリリースで廃止されています。

BZ#1431431

Block Storage: 高可用性 Active-Active ボリュームサービスはテクノロジープレビューとしては利用できなくなり、本リリースではサポートされません。

BZ#1683464

Block Storage: RBD Cinder ボリュームレプリケーションはテクノロジープレビューとしては利用できなくなり、サポートされません。

3.7. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 4 月 30 日)

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、非推奨になった機能について記載します。

3.7.1. 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#1654079

以前のリリースでは、オーバークラウドがエラー状態の場合、アンダークラウドのアップグレードに失敗していました。そのため、アンダークラウドを変更してフィックスをデプロイすることができませんでした。

今回の更新により、新しいアンダークラウドのアップグレードオプション **--force** を使用できるようになりました。このオプションを使用すると、アンダークラウドのアップグレードプロセスでオーバークラウドの状態が無視されます。

BZ#1692872

今回の更新により、以下の新たなタグを使用して、設定管理用 Ansible Playbook およびタスクを管理できるようになりました。

- container_config
- container_config_tasks
- container_config_scripts
- container_startup_configs
- host_config
- step1

- step2
- step3
- step4
- step5

3.7.2. 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#1664701

最近の変更により、NUMA トポロジーが設定されたインスタンスのメモリー割り当てに、ページサイズが考慮されるようになりました。この変更で、NUMA トポロジーが設定されたインスタンスのメモリーがオーバーサブスライブできなくなりました。

従来、オーバーサブスクリプションの使用が禁止されていたのは、ヒュージページが設定されたインスタンスだけでしたが、現在は、NUMA トポロジーが設定されたすべてのインスタンスで、メモリーのオーバーサブスクリプションは無効になっています。このことが、明示的な NUMA トポロジーを持つインスタンスおよび暗示的なトポロジーを持つインスタンスに影響を及ぼします。ヒュージページまたは CPU ピニングの使用により、インスタンスに暗示的な NUMA トポロジーが設定される可能性があります。

可能であれば、明示的な NUMA トポロジーの使用を避けてください。CPU ピニングが必要な場合、結果的に暗示的な NUMA トポロジーが生じますが、これに対する回避策はありません。

3.8. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 7 月 10 日)

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、非推奨になった機能について記載します。

3.8.1. 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#1589505

今回の更新により、NUMA アフィニティーを設定して、インスタンスを必ず vSwitch への外部接続を提供する NIC と同じ NUMA ノードに配置できるようになりました。この機能は、種別が flat または vlan のレイヤー 2 ネットワーク、および種別が vxlan、gre、または geneve のレイヤー 3 ネットワークで利用することができます。

BZ#1688461

config-download と共に使用することのできる新たな CLI 引数が 2 つあります。

- **openstack overcloud status:** 別個の CLI セッションで、または API を使用して、デプロイメントを監視します。
- **openstack overcloud failures:** 今後の解析用に、Ansible のエラーをログに記録し保存します。

BZ#1698467

今回の機能拡張により、Octavia Horizon Dashboard に新たな機能が追加され、その操作性が向上しています。

BZ#1698683

今回の更新により、新たな director パラメーター CinderNfsSnapshotSupport が追加されています。これを使用して、NFS バックエンド上の Block Storage サービス (cinder) のスナップショットをコントロールすることができます。

BZ#1701427

以前のリリースでは、環境全体にわたって TLS を有効にすると、haproxy および manila API 等の内部サービス間の通信が維持されませんでした。

今回の更新により、manila API が内部 API ネットワーク上の TLS エンドポイントをサポートするようになりました。

BZ#1714227

今回の更新により、director を通じた第二の Ceph Storage レイヤーデプロイメント機能がサポートされるようになりました。

3.8.2. テクノロジーレビュー

本セクションに記載する項目は、テクノロジーレビューとして提供しています。テクノロジーレビューステータスのスコープ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、[テクノロジーレビュー機能のサポート範囲](#) を参照してください。

BZ#1624971

今回のテクノロジーレビューの更新により、マルチアタッチ機能を使用して、1つのボリュームを複数のホストにアタッチできるようになりました。ボリュームはストレージプロトコルを使用せずに接続され、クラスター化したファイルシステム等の適切なソフトウェアアプリケーションにより、データの一貫性を提供する必要があります。

対象のストレージドライバーが本リリースのマルチアタッチ機能をサポートしているかどうかを判断するには、Red Hat にお問い合わせください。マルチアタッチ機能により接続されたボリュームでは、Cinder ボリュームの暗号化はサポートされません。また、その他の機能上の制約が適用される場合があります。

3.8.3. 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#1651191

今回の更新で、Ansible Networking ML2 プラグインがサポートされるようになりました。これにより、以下の機能が提供されます。

- ironic ベアメタルゲスト用分離テナントネットワーク機能
- ベアメタルノード用自動スイッチ設定
- 複数スイッチプラットフォームでの同一 ML2 ドライバーの使用

BZ#1696332

今回の更新で、IPv6 エンドポイントで OpenStack Messaging サービス (zaqar) がサポートされるようになりました。これにより、IPv6 を使用したアンダークラウドのデプロイが迅速化されます。

BZ#1701425

以前のリリースでは、manila API は Apache httpd サーバーを使用してデプロイされませんでした。今回の更新により、Apache のログは、manila API コンテナのノードの `/var/log/containers/httpd/manila-api` に保存されるようになりました。

3.8.4. 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#1581337

PING タイプのヘルスマニターを正しくサポートするには、ネットワークの負荷分散に使用される HAProxy はバージョン 1.6 またはそれ以降でなければなりません。Red Hat OpenStack Platform 13 に含まれる HAProxy は 1.6 より古いバージョンで、PING タイプのヘルスマニターを設定すると TCP 接続が使用されます。

3.9. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 9 月 4 日)

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、非推奨になった機能について記載します。

3.9.1. 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#1614361

今回の更新により、Fast Forward Upgrade の実行中に Red Hat OpenStack Platform 13 `host-config-and-reboot` 環境ファイルを使用できるようになりました。

1. **first-boot** スクリプトから **NodeUserData** マッピングを削除します。
2. **host-config-and-reboot.yaml** 環境ファイルをデプロイコマンドに追加します。
3. ロール固有のパラメーターを使用して、OVS-DPDK ロールに設定した **KernelArgs** および **TunedProfile** を追加します。
4. **KernelArgs** and **TunedProfile** が OpenStack Platform 10 の値に対応するようにします。違いがあると Fast Forward Upgrade の実行中にノードがリブートし、アップグレードに失敗します。

Ansible は、heat stack 設定により行われるリブートを処理することができません。誤った設定があるとしブートが行われ、Fast Forward Upgrade プロセスが失敗します。

**注記**

新しいパッチがあっても、既存の `first-boot` スクリプトを使用して Fast Forward Upgrade を実行することができます。

BZ#1631107

今回の更新により、Red Hat OpenStack Platform に新しいパラメーター **DnsSearchDomains** が追加

されています。異なる DNS サブドメインを持つ IDM および FreeIPA 環境に、このパラメーターを使用することができます。このパラメーターを環境ファイルの **parameter_defaults** セクションで設定し、**resolv.conf** に DNS サーブドメインの一覧を追加します。

BZ#1679267

以前のリリースでは、既存のデプロイメントで TLS Everywhere にアップグレードすることができませんでした。

今回の更新により、再インストールせずに内部の OpenStack サービス間のインフラ接続を維持することができます。

BZ#1688385

今回の機能拡張により、**tripleo::profile::base::database::mysql::mysql_server_options** hiera ハッシュキーを使用して、任意の mysql 設定オプションをオーバークラウド上の mysql クラスターに渡すことができるようになりました。

BZ#1706992

今回の更新により、インスタンスを移行せずにコンピュートノードがリブートした場合、ノード上のインスタンスを自動的に再起動するように設定できるようになりました。コンピュートノードがリブートする際にインスタンスを正常にシャットダウンして再起動するように、Nova および libvirt-guests エージェントを設定することができます。パラメーター **NovaResumeGuestsStateOnHostBoot** (True/False) および **NovaResumeGuestsShutdownTimeout** (デフォルト: 300s) が新たに Red Hat OpenStack Platform 13 に追加されました。

BZ#1713761

今回の更新により、インターフェイスのキー **domain** を使用して、**ifcfg** 設定のドメインを定義できるようになりました。これにより、異なる DNS サブドメインを持つ IDM および FreeIPA 環境をサポートするのに必要な、DNS 検索のパフォーマンスが向上します。

BZ#1732220

今回の更新により、オーバークラウドのローカルホスト上で **rabbitmq-management** インターフェイスがデフォルトで有効化されるようになりました。したがって、管理 API 経由で **rabbitmq** の状態の監視およびクエリーを容易に行うことができます。

3.9.2. テクノロジープレビュー

本セクションに記載する項目は、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ステータスのスコープ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、[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。

BZ#1700882

今回の更新により、Block Storage サービスのマルチアタッチ機能が、Ceph RBD ドライバーに拡張されています。

3.9.3. 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#1592528

まれな状況で、コントローラーノードを数回リブートすると、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、次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 DuplicateMessageError: Found duplicate message(629ff0024219488499b0fac0cacao3a5). Skipping it. の形式のエントリーが表示される。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コマンド pcs resource restart rabbitmq-bundle を実行します。

BZ#1656978

以前のリリースでは、Neutron SR-IOV エージェントが設定可能な Virtual Function (VF) の状態は、**enable** と **disable** の 2 つでした。そのため、Physical Function (PF) リンクの状態に関わらず、強制的に VF リンクの状態が設定されていました。

今回の更新により、Neutron SR-IOV エージェントは VF を **auto** または **disable** に設定するようになりました。**auto** の状態では、PF の **up** または **down** を自動的に複製します。したがって、PF が **down** の状態にある場合、同じ内蔵スイッチ (NIC) の他の VF とであっても、VF は送受信を行いません。



注記

この動作は標準的ではなく、NIC ベンダーの実装により異なります。PF が **down** の時に、**auto** の状態に設定された VF の実際の動作については、ドライバーのマニュアルを確認してください。

BZ#1708705

今回の更新により、hpe3par ドライバーのマルチアタッチ機能が有効になりました。

3.9.4. 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#1745130

現在、TLS Everywhere のその場アップグレードには、オーバークラウドノードを IdM に登録することができないという既知の問題があります。回避策としては、overcloud deploy を実行する前に、すべてのオーバークラウドノードから `/etc/ipa/ca.crt` を削除する方法があります。詳細は、https://bugzilla.redhat.com/show_bug.cgi?id=1732564 を参照してください。

3.9.5. 非推奨になった機能

本項に記載する項目は、サポートされなくなったか、今後のリリースではサポートされなくなる予定です。

BZ#1541829

Compute REST API からのファイル注入現在、2.56 以前の API マイクロバージョンを使用する場合、この機能は引き続きサポートされます。ただし、将来的には nova のこの機能は廃止されます。変更内容は以下のとおりです。

- **POST /servers** create server API および **POST /servers/{server_id}/action** rebuild server API から、**personality** パラメーターが非推奨になりました。これらの API どちらかへのリクエストボディで **personality** パラメーターを指定すると、**400 Bad Request** エラーが返されます。

- この変更により、rebuild server API に **user_data** を渡すサポートが追加されています。
- **GET /limits** API から **maxPersonality** および **maxPersonalitySize** レスポンス値が返されなくなりました。
- **os-quota-sets** および **os-quota-class-sets** API からの **injected_files**、**injected_file_path_bytes**、**injected_file_content_bytes** を受け入れおよび応答しなくなりました。

3.10. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 11 月 6 日)

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、非推奨になった機能について記載します。

3.10.1. 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#1561961

今回のリリースでは、PCI デバイスの NUMA アフィニティポリシーがサポートされるようになりました。このポリシーは、**[pci]alias** の設定オプションの一部として設定することができます。以下のポリシーがサポートされます。

- **required**
- **legacy**
- **preferred**

いずれの場合も、可能であれば、厳格な NUMA アフィニティが提供されます。これらのポリシー間の主要な相違点は、どれだけの NUMA アフィニティを破棄するとスケジューリングが失敗するかという点です。

これらのポリシーを使用して、デバイスごとまたはより具体的にするにはデバイスエイリアスごとに、NUMA アフィニティをどの程度厳格にするかを設定できます。これは、リソース使用率を最大化するのに役立ちます。

PCI デバイスに preferred ポリシーを設定した場合、PCI デバイスの NUMA ノードとは異なる NUMA ノードしか利用できなければ、nova はそのノード上の CPU を使用するようになります。これにより、リソースの使用率が高くなりますが、それらのインスタンスのパフォーマンスは低減するというマイナス面があります。

BZ#1656292

今回の更新により、Red Hat OpenStack Platform 13 で NVIDIA vGPU GRID ドライバーを使用できるようになりました。Red Hat では、これらのドライバーが含まれるインストール環境を完全にサポートします。ただし、NVIDIA GPU および専用ドライバー周辺のサードパーティーアプリケーションのサポートは除外されます。

BZ#1684421

今回のリリースで、RBD 一時ディスクを持つコンピュートホストのサブセットをデプロイできるように、ロールごとに **NovaEnableRbdBackend** を設定できるようになりました。残りのホストは、引き続きデフォルトのローカル一時ディスクを使用します。

注記: 最高のパフォーマンスを得るためには、RBD 一時コンピュートホストにデプロイするイメージは RAW 形式に、ローカル一時コンピュートホストにデプロイするイメージは QCOW2 形式にする必要があります。

BZ#1726733

今回の更新以前は、デフォルトの amphora タイムアウトの値が実稼働環境には長すぎました。

今回の更新により、実稼働環境により適したデフォルト amphora タイムアウトの値になりました。新しい director パラメーターを使用して、デフォルト値を上書きすることもできます。

BZ#1731210

今回の機能拡張により、facter がバージョン 3 にアップグレードされました。これにより、多数のネットワークインターフェイスを持つシステムで更新をデプロイおよび実行する際のパフォーマンスが向上します。このバージョンの facter は fact のキャッシュに対応し、非常に高速に fact の一覧を生成することができます。

注記: facter バージョン 3 が実装された openstack-tripleo-heat-templates のバージョンを使用する場合、ホストシステムにデプロイする同じコンテナで facter バージョン 3 を実行する必要があります。

BZ#1732220

今回の更新により、オーバークラウドのローカルホスト上で rabbitmq-management インターフェイスがデフォルトで有効化されるようになりました。したがって、管理 API を使用して rabbitmq の状態の監視およびクエリーを容易に行うことができます。

BZ#1733260

今回の更新で **openstack-tripleo-common** の機能が拡張されています。これにより、**openstack overcloud generate fencing** コマンドを実行して、**staging-ovirt** 電源管理ドライバーを使用する ironic ノード用に正しいフェンシング設定を作成することができます。これは、RHV にデプロイする仮想マシンに類似しています。

puppet-tripleo の機能も拡張され、RHV 上の仮想マシン用に pacemaker **fence-rhev** stonith エージェントを正しく設定できるようになりました。

BZ#1746112

今回の更新により、オーバークラウドのロール名を数字で始めることができるようになりました (例: **10Controller**、**99Compute**)。

BZ#1762167

今回の機能拡張で、collectd コンテナにプラグイン connectivity、mysql、ping、procevent、snmp-agent、および sysevent が追加されています。

3.11. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2019 年 12 月 19 日)

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、非推奨になった機能について記載します。

3.11.1. 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#1766735

今回の機能拡張により、OpenStack Image サービス (glance) ボリュームを、コンテナ化されたコントロールプレーンにマウントできるようになりました (ScaleIO の要求に対応)。

3.11.2. 非推奨になった機能

本項に記載する項目は、サポートされなくなったか、今後のリリースではサポートされなくなる予定です。

BZ#1719815

今回、OpenStack Telemetry Event Storage (panko) サービスが非推奨になりました。panko のサポートは、Red Hat Cloudforms からの使用だけに限定されます。Red Hat では、Red Hat Cloudforms のユースケース以外で panko を使用することを推奨しません。panko の使用に代わって、以下のオプションを使用することができます。

- panko に対してポーリングを行う代わりに、OpenStack Telemetry Metrics (gnocchi) サービスに対してポーリングを行う。これにより、リソースの履歴が提供されます。
- OpenStack Telemetry Alarming (aodh) サービスを使用して、これをイベント発生時のアラームのトリガーとする。OpenStack Telemetry Alarming (aodh) サービスがアプリケーションに直接アクセスできない場合には、OpenStack Messaging サービス (zaqar) を使用してアラームをキューに保管することができます。

3.12. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 3 月 10 日)

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、非推奨になった機能について記載します。

3.12.1. 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#1726733

今回の機能拡張により、実稼働環境に適した Octavia タイムアウトのデフォルト値に加えて、デフォルト値を上書きするための以下の新規 heat パラメーターが提供されます。

- OctaviaConnectionMaxRetries
- OctaviaBuildActiveRetries
- OctaviaPortDetachTimeout

BZ#1757886

インスタンスレベルで PCI NUMA アフィニティーを設定できるようになりました。この機能は、SR-IOV ベースのネットワークインターフェイスを持つインスタンスに NUMA アフィニティーを設定する際に必要です。以前のリリースでは、NUMA アフィニティーは PCI パススルーデバイスに対してホストレベルでしか設定することができませんでした。

BZ#1760567

今回の更新で、ceph-ansible が ceph-tools リポジトリからインストールされていることを確認する機能が追加されています。

BZ#1760871

今回の更新で、Octavia keepalived VRRP 設定を細かくチューニングするための以下のパラメーターが追加されています。

octavia::controller::vrrp_advert_int

Amphora ロールおよび優先度通知間隔 (秒単位)。デフォルトは `::os_service_default` です。

octavia::controller::vrrp_check_interval

VRRP ヘルスチェックスクリプトの実行間隔 (秒単位)。デフォルトは `::os_service_default` です。

octavia::controller::vrrp_fail_count

異常レートに移行するまでの連続する失敗の数。デフォルトは `::os_service_default` です。

octavia::controller::vrrp_success_count

正常レートに移行するまでの連続する成功の数。デフォルトは `::os_service_default` です。

octavia::controller::vrrp_garp_refresh_interval

MASTER からの余計な ARP 通知の間隔 (秒単位)。デフォルトは `::os_service_default` です。

octavia::controller::vrrp_garp_refresh_count

各リフレッシュ間隔に送信する余計な ARP 通知の数。デフォルトは `::os_service_default` です。

環境をカスタマイズするには、[オーバークラウドの高度なカスタマイズ](#) を参照してください。

BZ#1766735

今回の機能拡張により、OpenStack Image サービス (glance) ボリュームを、コンテナ化されたコントロールプレーンにマウントできるようになりました (ScaleIO の要求に対応)。

BZ#1777993

今回の更新で、Libvirt OpenStack Nova virt ドライバーに関して、アタッチされているボリュームの拡張がサポートされるようになりました。

BZ#1782229

今回の機能拡張により、イメージのインポートプロセス中に Image サービス (glance) プラグインを有効にするための、新たな2つのパラメーター (**GlanceImageImportPlugins** および **GlanceImageConversionOutputFormat**) が追加されています。

たとえば、**image_conversion** プラグインを有効にすると、以下のコマンドにより qcow2 イメージのインポート、raw 形式での保存、およびインポート後の自動変換が行われます。

```
glance image-create-via-import --disk-format qcow2 --container-format bare --name cirros --import-method web-download --uri http://download.cirros-cloud.net/0.4.0/cirros-0.4.0-x86\_64-disk.img
```

したがって、Image サービスのドライバーに RBD を使用すると、常にイメージを raw 形式で保存することができます。

3.13. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 6 月 24 日)

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、非推奨になった機能について記載します。

3.13.1. バグ修正

以下のバグは、Red Hat OpenStack Platform の本リリースで修正されています。

BZ#1650046

今回の更新以前は、SELinux の制限により、**su** を使用して root としてログインした場合に、RabbitMQ のログがアンダークラウドで正しくローテーションされませんでした。

rabbitmq-server パッケージが更新され、**openstack-selinux** に正しいログローテーションを有効にするポリシールールが新たに追加されました。

BZ#1783210

今回の更新で、cinder-backup コンテナの Pacemaker テンプレートバージョンに正しい ipc:host 設定が配置されるようになりました。

BZ#1805840

今回の更新以前は、Ceph RadosGW をデプロイすると **swiftoperator** ロールが作成されず、**swiftoperator** ロールを持つユーザーには RadosGW Swift エンドポイントの管理権限が付与されませんでした。

今回の更新により、Swift または Ceph RadosGW をデプロイすると **swiftoperator** ロールが自動的に作成され、**swiftoperator** ロールを持つユーザーが RadosGW オブジェクトと Swift オブジェクトを管理できるようになりました。

BZ#1811122

今回の更新以前は、xtremio ドライバーが誤った利用可能な領域容量を報告していたため、ストレージバックエンドに依存する仮想マシンインスタンスは不十分な領域でプロビジョニングすることができませんでした。

今回の更新以降は、xtremio ドライバーが正しい空き領域の容量を報告し、仮想マシンインスタンスが正しくプロビジョニングできるようになりました。

BZ#1813640

今回の更新で、処理中に neutron DHCP エージェントが受信するポート作成および更新メッセージにより高い優先順位が割り当てられ、インスタンスブート時の Failed to allocate network エラーを減らすことができます。

BZ#1813642

今回の更新で、2019 年 7 月 10 日の OpenStack Platform メンテナンスリリース (RHOSP 13.0.7) からのアップグレードに失敗する原因となっていたバグが修正されました。具体的には、OpenStack Compute (nova) のセル管理エラーが修正されました。

これで、2019 年 7 月 10 日の OpenStack Platform メンテナンスリリース (RHOSP 13.0.7) から、より新しい OpenStack バージョンにアップグレードできるようになりました。

BZ#1829284

今回の更新で、cinder ボリュームが対応する VxFlex OS ボリュームに正しく関連付けられ、ボリュームを削除すると、対応するバックエンドボリュームも削除されるようになりました。以前のリリースでは、cinder ボリュームを削除しても対応する VxFlex OS ボリュームの削除がトリガーされませんでした。

BZ#1829765

今回の更新以前は、cinder RBD ドライバーはトリミングまたは破棄操作を実行しなかったため、ユーザーは cinder RBD ボリュームから未使用領域をトリミングすることができませんでした。

今回の更新により、cinder RBD ドライバーがトリミングおよび破棄操作をサポートするようになりました。

BZ#1835870

今回の更新で、HPE 3par ストレージの Cinder オフラインボリューム移行が失敗する原因となっていたバグが修正されました。

3.13.2. 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#1670592

今回の更新により、ハイパーコンバージドインフラストラクチャー (HCI) のデプロイメントと OVS-DPDK の組み合わせがサポートされるようになりました。HCI アーキテクチャーでは、Compute サービスおよび Ceph Storage サービスを同じオーバークラウドノードに配置することができ、より優れたリソース使用率が得られるように設定されています。

BZ#1759254

今回の機能拡張により、**OctaviaConnectionLogging** パラメーターが追加され、接続フローのロギングを無効にできるようになりました。デフォルト設定は **true** で、接続フローがログに記録されることを意味します。

BZ#1823416

今回の機能拡張で、cinder Datera ドライバーがバージョン 2.2 に更新されました。

BZ#1841194

今回の機能拡張により、openvswitch ファイアウォールドライバーでネットワークトラフィックがあふれる原因となっていた状態が修正されました。以前のバージョンでは、該当するパケットの送付先 MAC アドレスに関するフォワーディングデータベース (FDB) エントリーがないため、統合ブリッジ上の特定 VLAN にあるすべてのポートでトラフィックがあふれていました。トラフィックが正しいポートだけに転送されるようになりました。

3.13.3. 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#1804412

今回の更新で、amphora 内での接続のロギングを無効にできるようになりました。

3.14. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 10 月 28 日)

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、非推奨になった機能について記載します。

3.14.1. バグ修正

以下のバグは、Red Hat OpenStack Platform の本リリースで修正されています。

BZ#1723482

今回の更新以前は、コンピュータノードが復元されるまで、Compute (nova) サービスはネットワークポート等のリソースを解放しませんでした。これにより、ダウンしたコンピュータノードのインスタンスからネットワークポートを切り離すことができない場合に、Load-balancing サービス (octavia) がフェイルオーバーに失敗していました。

今回の更新により、Load-balancing サービスのフェイルオーバーフローが更新され、この Compute サービスの問題を回避できるようになりました。Load-balancing サービスは、Compute サービスが解放しないポートを放棄し、コンピュータノードが復元されたら Compute サービスまたは Networking サービスがクリーンアップするように削除待ちの状態のままにするようになりました。これにより問題が解決され、コンピュータノードがまだダウンした状態でもフェイルオーバーが成功します。

BZ#1806975

今回の更新以前は、複数の復元が同時に実行されていると、システムがメモリーを使い果たすため、バックアップサービスが失敗していました。

今回の更新で、データをすぐに参照する回数を減らして、バックアップ/リストア操作時に Python がメモリーを解放する頻度を上げました。これにより、Python は復元が完了するのを待たずに、データが展開されたら直ぐにデータのガベージ収集を行うことができます。これにより問題が解決され、バックアップサービスが複数の復元を同時に処理できるようになりました。

BZ#1841157

今回の更新以前は、FC のライブマイグレーションが失敗していました。今回の更新で、対応するホストの FC の os-brick に正しいデバイス情報が送信されるようになりました。また、コンピュータノードでライブマイグレーションプロセスが失敗した場合に、デバイスが正しいマスキングビューから削除されるようになりました。

BZ#1841866

今回の更新以前は、3PAR ドライバーは可能なボリューム ID の `_name_id` フィールドを調べていなかったため、ライブマイグレーション後にボリュームが使用できなくなりました。今回の更新で、ドライバーはボリューム ID の代替の場所として `_name_id` フィールドを認識し、ライブマイグレーションされたボリュームが想定どおりに機能するようになりました。

BZ#1843196

今回の更新以前は、スナップショットからボリュームを作成する際の非同期移行中に作成された内部の一時スナップショットが、VNX ストレージから削除されませんでした。

たとえば、ボリューム V1 から作成したスナップショット S1 から新規ボリューム V2 を作成する場合、S1 のコピーから内部の一時スナップショット S2 が作成されます。V1 は、2 つのスナップショット S1 および S2 を持つようになります。V1、V2、および S1 を OpenStack Block Storage (cinder) から削除しても、S2 は削除されません。これにより、V1 と S2 の両方が VNX ストレージ上に残ります。

今回の更新で、一時スナップショット S2 が削除され、V1 が正常に削除できるようになりました。

BZ#1854950

今回の更新以前は、RHOSP 10 から RHOSP 13 へのアップグレード後に、インスタンスはそのボリュームにアクセスすることができませんでした。OpenStack Block Storage (cinder) サービスをホストからコンテナに移行する前に、OpenStack Block Storage のバックエンドとして使用されている NFS 共有がアンマウントされないためです。したがって、コンテナ化されたサービスが起動し、OpenStack Block Storage サービスディレクトリー内の全ファイルの所有者を変更すると、NFS 共有上のファイルの所有者も変更されていました。

今回の更新により、コンテナ内で実行されるようにサービスをアップグレードする前に、OpenStack Block Storage NFS 共有がアンマウントされるようになりました。これにより問題が解決され、RHOSP 13 へのアップグレード後にインスタンスがボリュームにアクセスできるようになりました。

BZ#1861084

今回の更新以前は、OpenStack Shared File Systems (manila) サービスが VServer スコープの ONTAP 認証情報で設定されている場合、ファイル共有のプロビジョニングに失敗していました。これは、昨今の NetApp ONTAP ドライバーの変更により、ストレージシステム機能の特定を試みる間、共有マネージャーサービスが再起動ループから抜け出せなくなるためです。

今回の更新により、NetApp ONTAP ドライバーは Vserver スコープの NetApp ユーザーを確認し、ストレージシステム機能を特定するためのフォールバックパスを追加するようになりました。これにより、問題が解決されました。OpenStack Shared File Systems 共有マネージャーサービスはストレージシステム機能を正しく特定し、ファイル共有のプロビジョニングに成功するようになりました。

BZ#1862105

今回の更新以前は、エージェントとの初期接続エラーによりリトライロジックを中断され、エージェントが Ironic サービスとの通信に失敗し、エージェントのコンソールに誤った TypeError が記録されていました。

今回の更新で、既知の接続および検索失敗ケースを明示的に処理するように例外処理が修正され、エージェントで何が生じているかについて明確な情報を提供するようにロギングが更新されました。接続がエージェントの要求どおりにリトライされ、予期しない異常が発生した場合にログが TypeError とだけ報告することがなくなりました。

BZ#1867817

今回の更新以前は、**ceilometer-metrics-qdr.yaml** 環境ファイルを使用すると、OpenStack Telemetry (ceilometer) で必要とされるクラスター化された redis インスタンスではなく、スタンドアロンの Redis 設定が発生していました。今回の更新で、リソースレジストリーの正しいサービスファイルが使用され、問題が解決されています。

BZ#1847305

起動時に、**ironic-conductor** サービスにより、**ironic-conductor** 再起動プロセスの初期段階で受け入れられた作業についてのベアメタルノードの予約ロックが失われる可能性があります。ロックが失われると、**ironic-conductor** サービスの再起動時に OpenStack Bare Metal Provisioning (ironic) デプロイメントに送信された作業に対して競合状態が発生し、要求が NodeNotLocked エラーで失敗していました。

今回の更新により、**ironic-conductor** プロセスで作業を許可する前にデータベースのクリーンアップチェックが実行され、問題が解決されました。

3.14.2. 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#1802038

今回の機能拡張により、外部の Red Hat Ceph Storage 4.1 クラスターがサポートされるようになりました。

BZ#1845802

今回の機能拡張により、Networking (neutron) サービス **http_retries** に新しい設定オプションが追加されました。これを使用して、Compute (nova) サービスまたは OpenStack Bare Metal Provisioning (ironic) サービスへの API 呼び出しの初回試行回数を設定することができます。デフォルトでは、呼び出しに失敗した場合 API コールは 3 回リトライされます。

今回の機能拡張により、Networking サービスは API リクエストをリトライして、インスタンスブート時のエラーを防ぐことができます。たとえば、Compute サービスはポートの使用準備が整っていることを示す通知を受け取るようになります。

BZ#1815202

config-download のテクノロジープレビュー機能を使用する際、生成された Ansible Playbook には **config-download** Playbook に合わせて調整されたデフォルトの **ansible.cfg** が含まれません。デフォルトの Ansible 設定は、大規模なデプロイメントには理想的ではありません。今回の機能拡張により、以下のコマンドを使用して **config-download** Playbook で使用できる **ansible.cfg** を生成できるようになりました。

```
$ openstack tripleo config generate ansible
```

3.14.3. 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#1891014

現在、マイナー更新中にインスタンスのライブマイグレーションを行う際の TLS Everywhere 環境に既知の問題があります。

ライブマイグレーション時の完全な QEMU ネイティブ TLS 暗号化のサポートにより (BZ1754791)、インスタンスを実行中の RHOSP デプロイメントでマイナー更新を実行する際に、インスタンスのライブマイグレーションに失敗します。これは、まだ libvirtd コンテナに存在しない TLS NBD ブロックマイグレーションの証明書が、更新中に作成されるためです。証明書は、ホストから直接バインドマウントされるのではなく、libvirt コンテナの作成時にコンテナのディレクトリツリーにマージされます。したがって、更新中に移行する必要があるインスタンスの QEMU プロセスは新しい証明書を自動的に取得せず、NBD 設定プロセスは以下のエラーと共に失敗します。

```
libvirtError: internal error: unable to execute QEMU command 'object-add': Unable to access credentials /etc/pki/qemu/ca-cert.pem: No such file or directory
```

更新後に作成されたインスタンスに対しては、ライブマイグレーションが機能します。

回避策:

この問題を回避するには、以下のいずれかのオプションを使用することができます。

- 更新の完了後にライブマイグレーションに失敗するインスタンスを停止して起動する。これにより、証明書情報を持つ libvirt コンテナが新たな QEMU プロセスを作成します。
- オーバークラウドに以下の設定を追加して NBD の TLS トランスポートの暗号化を無効にして、オーバークラウドをデプロイする。

```
parameter_defaults:
  UseTLSTransportForNbd: False
```

BZ#1726270

glance db purge コマンドが **IntegrityError** で失敗するという既知の問題があり、関連レコードが他のテーブルからパージされていない場合に、Cannot delete or update a parent row: a foreign key constraint fails のようなメッセージが表示されます。

回避策:

イメージテーブルからレコードを消去する前に、他のテーブルからレコードを手動で削除します。

3.15. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2020 年 12 月 16 日)

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、非推奨になった機能について記載します。

3.15.1. バグ修正

以下のバグは、Red Hat OpenStack Platform の本リリースで修正されています。

BZ#1879531

今回の更新以前は、Red Hat OpenStack Platform (RHOSP)ユーザーがコンテナを **latest** タグを使用するように設定した場合、RHOSP は更新されたコンテナイメージを使用するようにこれらのコンテナをフェッチしたり、再ビルドしたりしませんでした。

今回の更新で、この問題は解決されています。ユーザーがデプロイメントアクション (更新を含む) を実行するたびに、RHOSP は必ずコンテナイメージを取得し、実行中の各コンテナに対してイメージ ID を確認し、最新のイメージが使用されるようにコンテナを再ビルドする必要があるかどうかを判断するようになりました。RHOSP は、更新したすべてのコンテナを再起動します。



重要

この更新は、RHOSP がコンテナ更新をどのように管理するかに関する、以前のバージョンからの変更点です。以前のバージョンでは、RHOSP はイメージが存在するかどうかを確認しませんでした。RHOSP はデプロイメントアクション時に必ずコンテナをリフレッシュし、更新したコンテナを再起動するようになりました。このため、Red Hat Satellite デプロイメントでコンテナタグを制御していない限り、**latest** などのタグを再利用しないでください。

3.16. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース (2021年3月17日)

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、非推奨になった機能について記載します。

3.16.1. バグ修正

以下のバグは、Red Hat OpenStack Platform の本リリースで修正されています。

BZ#1908366

今回の更新で、VxFlex ボリューム切断の試みが失敗する原因となっていた非互換性が解消されました。

昨今の VxFlex cinder ボリュームの認証方法に関する変更は、既存のボリューム接続への後方互換性を持ちませんでした。認証方法の変更前に VxFlex ボリュームを接続した場合、ボリューム切断の試みが失敗していました。

これで、切断に失敗なくなりました。

3.16.2. 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#1841371

スナップショットが含まれるボリュームを別のユーザーに委譲する場合、ボリュームは委譲されませんが、スナップショットは以前のユーザーが所有したままになります。回避策としては、スナップショットを Red Hat Openstack Platform 13 で手動で管理する方法があります。インスタンス&イメージガイドのインスタンスのスナップショットの管理[1]を参照してください。

[1] [インスタンスのスナップショットの管理](#)

3.17. RED HAT OPENSTACK PLATFORM 13 メンテナンスリリース(2021年6月16日)

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、非推奨になった機能について記載します。

3.17.1. バグ修正

以下のバグは、Red Hat OpenStack Platform の本リリースで修正されています。

BZ#1888417

今回の更新以前は、Block Storage サービス(cinder)の NetApp SolidFire バックエンドへの API 呼び出しが **xNotPrimary** エラーで失敗する可能性がありました。このタイプのエラーは、SolidFire が接続を自動的に移動してクラスタのワークロードをリバランスするために、同時に操作がボリュームに追加されたときに発生しました。

今回の更新で、SolidFire ドライバーのパッチが、再試行できる例外のリストに **xNotPrimary** 例外を追加するようになりました。

BZ#1888469

今回の更新以前は、特定の環境でユーザーがタイムアウトしていましたが、大概がボリュームが大きすぎっていました。多くの場合、これらのマルチテラバイトボリュームでは、ネットワークのパフォーマンスが低下したり、SolidFire クラスタに関連するアップグレードの問題が発生したりしていました。

今回の更新で、SolidFire ドライバーに2つのタイムアウト設定が追加され、ユーザーが環境に適切なタイムアウトを設定できるようになりました。

BZ#1914590

今回の更新以前は、Block Storage サービス(cinder) API 応答が失われた場合、NetApp SolidFire バックエンドは未使用の複製ボリュームを作成していました。

今回の更新で、SolidFire ドライバーのパッチは、最初にボリューム名の作成を試みる前に、ボリューム名がすでに存在しているかどうかを確認します。このパッチは、読み取りタイムアウトの検出直後にボリュームの作成をチェックし、無効な API 呼び出しを防ぎます。

BZ#1934440

今回の更新以前は、最新バージョンの Red Hat AMQ Interconnect では CA 証明書のない TLS 接続が許可されないため、Service Telemetry Framework (STF)クライアントは STF サーバーに接続できませんでした。

今回の更新では、新しいオーケストレーションサービス (heat) パラメーター **MetricsQdrSSLProfiles** を提供することで、この問題を修正します。

Red Hat OpenShift TLS 証明書を取得するには、以下のコマンドを入力します。

```
$ oc get secrets
$ oc get secret/default-interconnect-selfsigned -o jsonpath='{.data.ca.crt}' | base64 -d
```

Red Hat OpenShift TLS 証明書の内容を含む **MetricsQdrSSLProfiles** パラメーターをカスタム環境ファイルに追加します。

```
MetricsQdrSSLProfiles:
- name: sslProfile
  caCertFileContent: |
    -----BEGIN CERTIFICATE-----
    ...
    TOpbgNIPcz0sloNK3Be0jUcYHVMPKGMR2kk=
    -----END CERTIFICATE-----
```

次に、**openstack overcloud deploy** コマンドを使用してオーバークラウドを再デプロイします。

BZ#1940153

今回の更新以前は、Block Storage サービス(cinder)を使用して HP3Par Storage バックエンドサーバーのスナップショットから多数のインスタンス（ブート可能なボリューム）を作成すると、タイムアウトが発生していました。HP 変数(**convert_to_base**)が true に設定され、HP3Par が元のボリュームのシックボリュームを作成していました。これは不要で不要なアクションでした。今回の更新により、新しい HP ドライバー(4.0.11)が新しい仕様を含む RHOSP 13 にバックポートされました。

```
hpe3par:convert_to_base=True | False
```

- True（デフォルト）: ボリュームはスナップショット(HOS8 の動作)とは別に作成されません。
- false - ボリュームは、スナップショットの子として作成されます(HOS5 の動作)。

使用方法

cinder type-key コマンドを使用して、HPE3Par ボリュームの新しい仕様を設定できます。

```
cinder type-key <volume-type-name-or-ID> set hpe3par:convert_to_base=False | True
```

例

```
$ cinder type-key myVolType set hpe3par:convert_to_base=False
$ cinder create --name v1 --volume-type myVolType 10
$ cinder snapshot-create --name s1 v1
$ cinder snapshot-list
$ cinder create --snapshot-id <snap_id> --volume-type myVolType --name v2 10
```

注記

v2 のサイズが v1 よりも大きい場合は、ボリュームを拡張することはできません。この場合、エラーを回避するために、v2 はベースボリュームに変換されます (**convert_to_base=True**)。

BZ#1943181

今回の更新以前は、Compute サービス(nova)が Block Storage サービス(cinder)への **終了接続** 呼び出しを行うと、シングルデバイスおよびマルチパスデバイスがフラッシュされず、これらのデバイスが **残り** 状態にあるため、データの損失のリスクがありました。

この問題の原因は、os-brick **disconnect_volume** コードは、**use_multipath** パラメーターに、元の **connect_volume** 呼び出しで使用されたコネクタと同じ値があることを前提としていました。

今回の更新により、Block Storage サービスは接続を解除する方法を変更します。os-brick コードは、インスタンスに接続されているボリュームの Compute サービスのマルチパス設定が変更された場合に、ボリュームを適切にフラッシュおよびデタッチするようになりました。

3.17.2. 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#1875508

今回の機能拡張により、オーバークラウドのデプロイ時に、ロールの Orchestration サービス(heat) パラメーター **ServiceNetMap** をオーバーライドできるようになりました。

TLS を使用するスパイン/リーフ型 (エッジ) デプロイメントでは、階層の補間を使用してロールのネットワークをマッピングする際に問題がありました。ロールごとに ServiceNetMap を上書きすると、TLS-everywhere のデプロイメントで発生する問題が修正され、インターフェイスが容易になり、より複雑な階層の補間の必要性がなくなります。

3.17.3. 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#1924727

Block Storage のバックアップサービスは、ホスト上のファイルにアクセスする必要がある場合がありますが、サービスを実行するコンテナで利用できない場合があります。今回の機能拡張により、**CinderBackupOptVolumes** パラメーターが追加されました。これを使用して、Block Storage のバックアップサービス用に追加のコンテナボリュームマウントを指定することができます。

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 で対応しています。このアドバイザーについての詳しい情報は、[RHEA-2018:2086 - Product Enhancement Advisory](#) 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。この失敗が、ceph-ansible の実行に影響を及ぼす場合があります。これには、複数のコンピューターノードを使用している、または 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している新規デプロイメントが含まれます。

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- の接頭辞は削除されました。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、次のような場合にテナントの VLAN ネットワークで発生します。NAPT 以外のスイッチ上で起動する仮想マシンに Floating IP が割り当てられた。その後その Floating IP が削除された。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。ただし、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ます。

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。このロックの範囲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範囲は最小限となり、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 クライアントの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イスを介してのみ CephFS にアクセスすることができます。この新機能は director に完全に統合され、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イ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イスの追加/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ルアップしません。

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。アンダークラウドで、以下の例に示す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#1588838

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が正しく渡されるようになり、正しい動作に戻りました。

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ノードとともに、RT 対応のコンピュータノ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。

- tripleo-heat-templates/environments/compute-real-time-example.yaml をベースに、ComputeRealTime ロールのパラメーターを設定する compute-real-time.yaml 環境ファイルを作成します。その際、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 and NovaVcpuPinSet: リアルタイム負荷用に確保する CPU コアの一覧。この設定は、実際のリアルタイムコンピュータノードの CPU ハードウェアにより異なります。
 - 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。
- 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
- 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で ComputeRealTime ロールをリアルタイム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。
- 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 設定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、ステージエリアにイメージをアップロードしてから、ステージ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設定されます。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

説明: Gnocchi サーバーが使用する API プロトコル

デフォルト: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:nil

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:nil

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:nil

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:nil

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:nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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: nil

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

BZ#1566376

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することが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ました。そのため、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) がホスト上で実行される正当ではない cinder-volume サービスによって処理される場合、その操作は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、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イスを使用する際や 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、代わ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 では、デフォルトではこの拡張機能が設定され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しません。したがって、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す。

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 (unittest 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。

4.2. RHSA-2018:2214 (重要): OPENSTACK-TRIPLEO-HEAT-TEMPLATES のセキュリティ更新

本項に記載するバグは、アドバイザリー RHSA-2018:2214 で対応しています。このアドバイザリーについての詳しい情報は、[RHSA-2018:2214 - Security Advisory](#) を参照してください。

openstack-tripleo-common

BZ#1592823

Ansible Playbook のログに、デプロイメント、更新、アップグレード中のアクションのタイミングに関する情報を提供するタイムスタンプが含まれるようになりました。

openstack-tripleo-heat-templates

BZ#1586171

以前のリリースでは、OpenDaylight の古いキャッシュが原因でオーバークラウドの更新が失敗していました。今回の更新により、新しいバージョンにアップグレードする前に OpenDaylight が停止されて、古いキャッシュが削除されるようになりました。レベル1の更新は OpenDaylight デプロイメントで機能します。レベル2の更新は現在サポートされていません。

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#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、heat パラメーター OpenDaylightLogMechanism: 'file' を設定します。

BZ#1559105

以前のリリースでは、既存のオーバークラウドに対して overcloud deploy コマンドを再実行すると、pacemaker で管理されているリソースの再起動のトリガーに失敗していました。たとえば、新しいサービスを haproxy に追加すると、haproxy は再起動せず、haproxy pacemaker リソースを手動で再起動するまで新たに設定されたサービスは利用できない状態となっていました。

今回の更新により、pacemaker リソースの設定変更が検出され、pacemaker リソースは自動的に再起動するようになりました。pacemaker で管理されるリソースの設定変更は、いずれもオーバークラウドに反映されるようになりました。

BZ#1589346

以前のリリースでは、Playbook のリストに不要なエントリーが含まれていたため、マイナーな更新のワークフロー内のサービスデプロイメントタスクが 2 回実行されていました。今回の更新により、Playbook の不要なエントリーが削除され、更新された Playbook にはホストの準備のタスクが直接含まれるようになりました。マイナーバージョン更新のアクションは、必要な順序で実行されるようになりました。

BZ#1592424

以前のリリースでは、事前にプロビジョニングされたサーバーにオーバークラウドをデプロイする場合に使用される Heat テンプレートには UpgradeInitCommonCommand のパラメーターがありませんでした。openstack overcloud upgrade prepare コマンドは必要な全操作を実行しなかったため、一部の環境でアップグレード中に問題が発生していました。

今回の更新で、事前プロビジョニング済みのサーバー用のテンプレートに `UpgradelnitCommonCommand` が追加され、`openstack overcloud upgrade prepare` のコマンドが必要なアクションを実行できるようになりました。

BZ#1594328

セキュリティを強化するために、デフォルトの `OpenDaylightPasswordadmin` は無作為に生成される 16 桁の数値に置き換えられました。この無作為に生成されるパスワードは Heat テンプレートでパスワードを指定することによって上書きすることができます。

```
$ cat odl_password.yaml
parameter_defaults:
  OpenDaylightPassword: admin
```

続いて、そのファイルを `overcloud deploy` コマンドで渡します。

```
openstack overcloud deploy <other env files> -e odl_password.yaml
```

puppet-opendaylight

BZ#1594333

以前のリリースでは Karaf シェル (OpenDaylight 用の管理シェル) は、ポート 8101 上の特定の IP アドレスにバインドされていなかったため、Karaf シェルは公開されている外部ネットワーク上でリッスンしていました。そのポートでは、外部ネットワークを使用して OpenDaylight にアクセスすることができるため、セキュリティの脆弱性が発生しました。

今回の更新により、Karaf シェルはデプロイメント中に内部 API ネットワークの IP にバインドされるようになり、Karaf シェルはプライベートの内部 API ネットワークでのみアクセス可能となりました。

4.3. RHBA-2018:2215: OPENSTACK-NEUTRON のバグ修正アドバイザリー

本項に記載するバグは、アドバイザリー RHBA-2018:2215 で対応しています。このアドバイザリーについての詳しい情報は、[RHBA-2018:2215 - Bug Fix Advisory](#) を参照してください。

opendaylight

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コンピュートノードに分散している場合に発生します。この問題には、適切な回避策はありません。

BZ#1568976

デプロイメント中に、1つまたは複数の OpenDaylight のインスタンスが正しく起動できない場合があります。これは、機能の読み込みのバグが原因です。このために、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。

デプロイメントが合格した場合、そのデプロイメントが正常に実行されるには、3つの OpenDaylight インスタンス中2つが機能している必要があります。3つ目の OpenDaylight インスタンスが正しく起動されていない可能性があります。`docker ps` コマンドで、各コンテナの正常性ステータスを確認し

てください。正常でない場合には、**docker restart opendaylight_api** でそのコンテナを再起動します。

デプロイメントが失敗した場合の唯一のオプションは、そのデプロイメントを再起動することです。TLS ベースのデプロイメントの場合には、OpenDaylight の全インスタンスが正しく起動しないと、デプロイメントは失敗します。

BZ#1586169

createFibEntry にパラメーターが不足していたため、NAT セットアップ中に Null Pointer Exception (NPE) が生成されていました。このバグにより、ルーティングテーブルの FIB エントリーが不足して、NAT またはルーティングが失敗する可能性があります。今回の更新で RPC コールに正しいパラメーターが追加されました。NPE は OpenDaylight のログには表示されなくなり、NAT とルーティングが正しく機能するようになりました。

BZ#1587967

VLAN ネットワークにポートがないノード上で NAPT スイッチを選択すると、必要な全フローがプログラムされません。ネットワーク内の Floating IP アドレスを持たない仮想マシンは、すべて外部の接続に失敗します。今回の更新により、ルーターの一部である VLAN の NAPT スイッチ内に VLAN フットプリントを作成するための擬似ポートが追加されました。外部接続は、Floating IP アドレスのない仮想マシンでも機能します。

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#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。

openstack-neutron

BZ#1591206

neutron OVS エージェントに bridge_mac_table_size と呼ばれる新しい設定オプションが追加されました。この値は、openvswitch-neutron-agent によって管理される各ブリッジで other_config:mac-table-size オプションとして設定されます。この値は、ブリッジで学習可能な MAC アドレスの最大数を制御します。この新しいオプションのデフォルト値は 50,000 です。これは、大半のシステムには十分なはずですが、合理的な範囲外の値 (10 から 1,000,000) は OVS によって強制されます。

python-networking-odl

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。

python-networking-ovn

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に、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#1582512

dns_nameservers フィールドがサブセット用に設定されていない場合には、そのサブセットに接続されている仮想マシンの /etc/resolv.conf は空になります。今回の修正により、neutron-server は、仮想マシンを実行しているホストの /etc/resolv.conf から DNS リゾルバーを取得してテナントの仮想マシンのデフォルト dns_nameservers として使用するようになりました。

4.4. RHBA-2018:2573: OPENSTACK PLATFORM 13 のバグ修正と機能拡張アドバイザリー

本項に記載するバグは、アドバイザリー RHBA-2018:2573 で対応しています。このアドバイザリーについての詳しい情報は、[RHBA-2018:2573 - Bug Fix Advisory](#) を参照してください。

openstack-kuryr-kubernetes

BZ#1585237

コントローラーは Nodeport サービスをサポートしないので、ユーザーはそれらを作成すべきではありません。しかし、Nodeport サービスは一部の設定に存在し、そのためにコントローラーがクラッシュしていました。このようなクラッシュを予防するために、コントローラーは Nodeport サービスを無視するようになりました。

openstack-manila

BZ#1523864

今回の更新で、Dell-EMC Unity と VNX バックエンドでの Manila IPv6 エクスポートのロケーションおよびアクセスルールの使用がサポートされるようになりました。

openstack-manila-ui

BZ#1554935

以前のリリースでは、manila-ui プラグイン用の設定ファイルがコピーされていませんでした。そのため、Dashboard で manila のパネルが表示されませんでした。今回の更新で、manila-ui 用の設定ファイルをすべて必要な場所にコピーする手順が含まれるようになりました。ユーザーが Dashboard を有効化すると manila のパネルが表示されます。

openvswitch

BZ#1551016

以前のリリースでは、OVN ポートの作成時間は、システムに存在するポートの数が多いほど長くかかっていました。現在、この作成時間は、クラウド内のポート数に拘らず、一定となりました。

python-eventlet

BZ#1607967

以前のリリースでは、python-eventlet UDP アドレスの処理で問題があり、一部の IPv6 アドレスの処理が正しく行われない場合がありました。その結果、UDP 経由で DNS 応答を受信すると、python-eventlet はその応答を無視して、数秒間停滞し、パフォーマンスに深刻な影響を与えていました。今回のリリースでは、この問題は解決しています。

BZ#1612971

以前のリリースでは、eventlet のバグにより、nameservers を設定していないシステム (または nameservers が到達不可能なシステム) と、名前解決で hosts ファイルのみに依存していたシステムで、インスタンスのブート時に遅延が発生していました。これは、IPv4 ホストだけが指定されている場合でも IPv6 エントリーの解決を試みていたためです。今回の修正により、hosts ファイルに少なくともエントリーが1つある場合には、eventlet はネットワークの解決の使用を試みずに直ちに応答を返すようになりました。

python-oslo-policy

BZ#1600137

以前のリリースでは、neutron でポリシーチェックが実行されるたびにポリシーファイルが再読み込み/再評価されていました。ポリシーファイルが再評価されると、管理者以外のユーザーによる API 操作が大幅に遅くなります。今回の更新により、ポリシーファイルの状態が保存されるようになったため、ルールが変更された場合にのみファイルが再読み込みされます。管理者以外のユーザーによる Neutron API の操作は迅速に解決するようになりました。

python-proliantutils

BZ#1578581

HP Gen10 サーバー上での複数の Sushy オブジェクト作成に伴う問題が原因で、HPE Gen10 サーバーは ID が /redfish/v1/Systems/1 のシステムにアクセスする際に整合性のある応答を提供しませんでした。Sushy のデフォルト認証メソッドであるセッションベースの認証を使用する代わりに、Sushy オブジェクトの作成時に Basic 認証を使用します。これにより、電源状態のリクエストの問題が解決されます。

BZ#1580480

ironic-dbsync ユーティリティーが ironic ドライバーの読み込みを試みて、ドライバーが proliantutils.ilo クライアントモジュールをインポートした場合には、proliantutils ライブラリーがすべての pysnmp MIB の読み込みを試みていました。読み取り不可能な CWD 内で ironic-dbsync プロセスが実行されている場合には、pysnmp は CWD 内の MIB の検索を試みる際に操作が失敗していました。このために、デブロイメント内の ironic-dbsync.log に Unable to load classic driver fake_drac: MIB file pysnmp_mibs/CPQIDA-MIB.pyc access error: [Errno 13] Permission denied: 'pysnmp_mibs': MibLoadError: MIB file pysnmp_mibs/CPQIDA-MIB.pyc access error: [Errno 13] Permission denied: 'pysnmp_mibs' というエラーメッセージが表示されていました。proliantutils の更新によって、モジュールのインポート時に pysnmp は全 MIB を読み込まないようになりました。これにより、アプリケーションにより明示的に要求される前に MIB の検索を試みる状況が防がれるようになりました。

rhosp-release

BZ#1563435

古いイメージのパッケージを削除する際には、ポストスクリプトがイメージパッケージのシンボリックリンクを間違えて更新する場合があります。このスクリプトは更新され、シンボリックリンクの修正に使用されるスクリプトを呼び出すようになりました。

4.5. RHBA-2018:2574: OPENSTACK DIRECTOR のバグ修正アドバイザリー

本項に記載するバグは、アドバイザリー RHBA-2018:2574 で対応しています。このアドバイザリーについての詳しい情報は、[RHBA-2018:2574 - Bug Fix Advisory](#) を参照してください。

instack-undercloud**BZ#1572257**

以前のリリースでは、Red Hat OpenStack のアンダークラウドのアップグレードは、オーバークラウドがエラー状態の時には失敗していました。アップグレードプロセスの設定後のステップでコンバージェンスアーキテクチャーを使用するためにオーバークラウドスタックのマイグレーションを試みる際に暗号化のエラーでかなり遅い段階でエラーが発生していました。今回のリリースでは、エラーは早期に発生し、アンダークラウドのアップグレードは続行されなくなりました。アンダークラウドのアップグレードの最初にエラーが表示されます。ユーザーは、アンダークラウドのアップグレードを行う前にオーバークラウドが *_COMPLETE の状態であることを確認する必要があります。

BZ#1584666

以前のリリースでは、local_mtu のパラメーターが 1900 に設定されていて undercloud.conf に指定されている場合には、アンダークラウドのインストールが失敗していました。local_mtu の値が 1500 よりも大きな場合には、アンダークラウドのインストールが失敗しました。global_physnet_mtu を local_mtu に設定してください。local_mtu の値が 1500 より大きくてもアンダークラウドのインストールは成功します。

BZ#1608173

SSL を有効化したアンダークラウドではインストール中に ERROR: epmd error というエラーメッセージが表示されて操作が失敗する場合があります。このエラーは、ホスト名と一致する仮想 IP が rabbitmq の後に keepalived によって設定されていたためことが原因です。rabbitmq の前に keepalived を設定するようにしてください。これにより、アンダークラウドのインストールは失敗しなくなります。

openstack-tripleo**BZ#1601472**

NFV がデプロイされた RHOSP 10 から RHOSP 13 にアップグレードする手順が再テストされ、DPDK および SR-IOV の環境向けに更新されました。

openstack-tripleo-common**BZ#1594279**

以前のリリースでは、openstack undercloud backup コマンドは、拡張属性をキャプチャーしませんでした。これにより、アンダークラウドの Swift ストレージのオブジェクトメタデータが失われ、レンドリングを使用できませんでした。今回の修正により、バックアップアーカイブの作成時に --xattrs フラ

グが追加されました。アンダークラウドの Swift ストレージのオブジェクトはバックアップ中に拡張属性を維持するようになりました。

BZ#1596763

アンダークラウドが instackenv.json ファイルからベアメタルノードをインポートする場合、UCS ドライバーの設定中に **pm_service_profile** (または **ucs_service_profile**) フィールドのみで一致しない ironic ノードは ironic の設定で相互にオーバーライドしていました。このため、その ironic ノードの1つが設定で指定されていました。openstack-tripleo-common が更新され、**pm_service_profile** (または **ucs_service_profile**) フィールドでのみ一致しない ironic ノードは、引き続き別個とみなされるようになりました。**pm_service_profile** または **ucs_service_profile** のフィールドでのみ異なる ironic ノードはすべて ironic にインポートされます。

BZ#1574349

オーバークラウドをデプロイする前に、クラスター向けに stonith リソースを自動作成することができません。デプロイメントを開始する前に、コマンド `openstack overcloud generate fencing --ipmi-lanplus --output /home/stack/fencing.yaml /home/stack/instackenv.json` を実行します。

次に、デプロイコマンドの引数リストに `-e /home/stack/fencing.yaml` を渡します。これで、クラスターに必要な stonith リソースが自動的に作成されます。

BZ#1575623

派生パラメーターのワークフローで、オーバークラウドノードを特定するための SchedulerHints の使用がサポートされるようになりました。以前のリリースでは、このワークフローでは SchedulerHints を使用して、対応する TripleO オーバークラウドロールに関連付けられたオーバークラウドノードを特定できませんでした。このため、オーバークラウドのデプロイメントは失敗していました。SchedulerHints のサポートにより、このようなエラーが防がれます。

BZ#1577853

OpenDaylight 向けの docker healthcheck では、OpenDaylight で REST インターフェイスと neutron NB コンポーネントのみが正常であることを確認していました。この healthcheck には、ローディングされているすべての OpenDaylight コンポーネントが含まれていなかったため正確ではありませんでした。ローディングされている OpenDaylight コンポーネントをすべてチェックするには、docker healthcheck と共に diagstatus URI を使用してください。これで、OpenDaylight docker コンテナのヘルスステータスはより正確になります。

openstack-tripleo-heat-templates

BZ#1597379

manila-share サービスのコンテナは、コントローラーホストからの PKI トラストストアへのバインドマウントに失敗していました。その結果、manila-share サービスからストレージバックエンドへの接続は SSL を使用して暗号化できませんでした。PKI トラストストアをコントローラーホストから manila-share サービスのコンテナにバインドマウントします。これで、manila-share サービスからストレージバックエンドへの接続は SSL を使用して暗号化できるようになります。

BZ#1597541

libvirtd のライブマイグレーションのポート範囲の変更により、ライブマイグレーションでエラーが発生しないようになりました。以前のリリースでは、libvirtd のライブマイグレーションのポート範囲は qemu.conf ファイルで指定されている 49152 から 49215 まででした。Linux では、この範囲は 32768 から 61000 までのエフェメラルポート範囲のサブセットです。エフェメラル範囲内のポートはいずれ

も他のサービスが使用可能です。その結果、ライブマイグレーションは Live Migration failure: internal error: Unable to find an unused port in range 'migration' (49152-49215) というエラーで失敗していました。libvirtd ライブマイグレーションの新しいポート範囲 (61152 から 61215 まで) はエフェメラル範囲外です。したがって、関連するエラーは発生しなくなりました。

BZ#1500594

以前のリリースでは、オーバークラウドノードから **ceph-osd** パッケージを削除する際に対応する Ceph のプロダクトキーが削除されませんでした。そのため、**subscription-manager** は **ceph-osd** パッケージがまだインストールされていると誤った報告をしていました。今回のリリースでは、**ceph-osd** パッケージの削除を処理するスクリプトにより、対応する Ceph のプロダクトキーも削除されるようになりました。**ceph-osd** パッケージとプロダクトキーを削除するスクリプトは、オーバークラウドの更新中のみ実行されます。その結果、**subscription-manager list** は Ceph OSD がインストールされているという報告をしなくなりました。

BZ#1549770

コンテナがデフォルトのデプロイメント方法になりました。ベアメタルサービスを environments/baremetal-services.yaml でデプロイする方法はまだ使用できますが、いずれはなくなる見込みです。

environments/services-docker を参照するリソースレジストリーが記載された環境ファイルで、environments/services パスに変更する必要があります。デプロイされているベアメタルサービスを確保する必要がある場合には、最初に配置した environments/services の代わりに environments/services-baremetal に参照を更新してください。

BZ#1598469

以前のリリースでは、Sahara 用の Fast Forward Upgrade パスをサポートするコードが含まれていませんでした。その結果、Fast Forward Upgrade で 10 から 13 にアップグレードした後に Sahara のサービスに必要なすべての変更が適用されませんでした。今回の更新で問題が解決し、Sahara サービスは Fast Forward Upgrade を実行した後に正常に機能するようになりました。

BZ#1565028

OpenDaylight ログの正しいパスが記載された README が /var/log/opendaylight に追加されました。

BZ#1567511

CephFS-NFS ドライバーのデプロイメントでは、CephFS によってバッキングされる NFS-Ganesha サーバーが dentry、inode、属性のキャッシュを実行します。これは、libcephfs クライアントによっても実行されます。NFS-Ganesha サーバーの冗長なキャッシュにより、メモリーフットプリントが大きくなり、またキャッシュの一貫性にも影響を及ぼしていました。NFS-Ganesha サーバーの inode、dentry、属性のキャッシュはオフにしてください。これにより、NFS-Ganesha サーバーのメモリーフットプリントが小さくなります。キャッシュの一貫性で問題が発生する可能性も低くなります。

BZ#1567893

TripleO の capabilities-map.yaml は、間違ったファイルの場所で Cinder の Netapp バックエンドを参照していました。UI はケイパビリティマップを使用するので、Cinder の Netapp 設定ファイルにはアクセスできませんでした。capabilities-map.yaml は、Cinder の Netapp 設定の正しい場所を指定するように更新されました。UI の Cinder Netapp バックエンド用のプロパティタブは正常に機能するようになりました。

BZ#1574787

Dell-EMC のストレージシステム (VNX、Unity、VMAX) 用の Manila の設定マニフェストには誤った設定オプションが記載されていました。その結果、オーバークラウドで manila-share を Dell ストレージシステムと共にデプロイすると操作が失敗していました。今回の更新で、Dell-EMC ストレージシステム (VNX、Unity、VMAX) 用の Manila の設定マニフェストは修正されました。オーバークラウドで manila-share サービスを Dell ストレージシステムと共にデプロイする操作は正常に完了するようになりました。

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、次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#1589661

コンテナからの standard_init_linux.go:178: exec user process caused "text file busy" というエラーログで、まれにデプロイメントが失敗する場合があります。競合を回避してデプロイメントが失敗しないようにするには、docker-puppet.sh file を複数回同時に書き出さないようにしてください。

BZ#1590602

IPv6 を無効にするために KernelDisableIPv6 のパラメーターを true に設定すると、デプロイメントは rabbitmq エラーで失敗していました。これは、初期化を正しく行うために、少なくともループバックインターフェイスが IPv6 をサポートしていることが Erlang Port Mapper Daemon の要件であるためです。ipv6 を無効にしている場合にデプロイメントが正常に完了するには、ループバックインターフェイス上で IPv6 を無効にしないでください。

BZ#1597665

Docker が使用していた journald バックエンドは、サイズに基づいてログをロールオーバーしていました。このため、一部の古い OpenDaylight ログが削除されていました。この問題は、コンソールの代わりにファイルにログ記録する方法に移行することで解決し、ロールオーバーは OpenDaylight によって管理できるようになりました。その結果、古いログは以前よりも長い期間保持されます。

BZ#1542493

以前のリリースでは、モニターリング目的の RabbitMQ インスタンス用に標準以外のポートを使用する場合は、コンテナのヘルスチェックでポートの値が反映されなかったために、sensu-client コンテナが unhealthy の状態を報告していました。今回のリリースでは、コンテナのヘルスチェックでポートの値が表示されるようになりました。

BZ#1564519

削除済みのデータベースレコードのデフォルトのページ期間が修正され、Cinder のデータベースから削除済みのレコードがページされるようになりました。以前のリリースでは、Cinder のページ cron ジョブの CinderCronDbPurgeAge 値に誤った値が使用されており、必要なデフォルト期間に達した際に、削除済みのレコードが Cinder の DB からページされませんでした。

BZ#1569515

OSP 13 の TripleO Heat テンプレートの **single-nic-vlans** ネットワークテンプレートでは、Ceph ノード用のブリッジ名が間違っていました。以前のデプロイメントで single-nic-vlans テンプレートが使用されていた場合には、OSP 13 にアップグレードすると Ceph ノードでエラーが発生していました。今

回のリリースでは、Ceph ノードの single-nic-vlans テンプレートで以前のバージョンのブリッジ名と一致する **br-storage** というブリッジ名が使用されるようになりました。single-nic-vlans テンプレートを使用する環境における OSP 13 へのアップグレードは Ceph ノードで正常に実行できるようになりました。

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。このパラメーター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、オーバークラウドの高度なカスタマイズのカスタムコンポーザブルネットワーク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#1576627

以前のリリースでは、yaml-nic-config-2-script.py には対話式のユーザー入力が必要でした。このスクリプトは、自動化目的のために非対話式の方法では呼び出せませんでした。今回のリリースでは --yes のオプションが追加されました。yaml-nic-config-2-script.py に --yes オプションを指定して呼び出すことができるようになり、その場合にはユーザーは対話式の入力を要求されません。

BZ#1593882

以前のリリースでは、tripleo-heat-templates の一部のバージョンで fixed-ips-v6.yaml 環境ファイル内の Redis 仮想 IP ポートの設定にエラーが含まれていました。デプロイメントコマンドラインで network-isolation-v6.yaml の後に fixed-ips-v6.yaml のファイルを指定すると、Redis サービスは正しい IPv6 ネットワークではなく Control Plane ネットワークに配置されていました。今回の更新により、environments/fixed-ips-v6.yaml のファイルには、network/ports/vip.yaml ではなく、正しい network/ports/vip_v6.yaml への参照が含まれるようになりました。fixed-ips-v6.yaml 環境ファイルには正しいリソースレジストリーのエントリーが含まれるので、指定される環境ファイルの順序に拘らず、Redis の仮想 IP は IPv6 アドレスで作成されます。

BZ#1594910

ホスト上で実行されていた Cinder サービスがコンテナ内で実行されるように移行した場合に、TripleO の BlockStorage ロールが更新されませんでした。cinder-volume サービスが BlockStorage ホストにデプロイされていました。今回のリリースでは BlockStorage ロールが更新され、cinder-volume サービスをコンテナ内にデプロイするようになりました。cinder-volume サービスはコンテナ内で正しく実行されます。

BZ#1599329

以前のリリースでは、Manila の設定を変更してオーバークラウドを更新すると、それらの変更は、コンテナ化された Manila share-service にデプロイされませんでした。今回の修正により、変更のデプロイが正常に実行されるようになりました。

BZ#1603538

/var/lib/nova/instances の共有ストレージで、nfs と同様に、任意のコンピュータで nova_compute を再起動すると、インスタンスの仮想一時ディスクと console.log の所有者/グループが変更されていまし

た。その結果、インスタンスは仮想一時ディスクにアクセスできなくなり、機能しなくなっていました。今回の更新で、`/var/lib/nova/instances` 内のインスタンスのファイルの所有権を変更するスクリプトが改善されました。nova compute の再起動中にインスタンスのファイルへのアクセスは失われなくなりました。

BZ#1612342

Cinder の Netapp バックエンドのデプロイに使用されていた TripleO の環境ファイルは古く、誤ったデータが含まれていました。このため、オーバークラウドのデプロイメントが失敗していました。今回のリリースで、Cinder Netapp 環境ファイルが更新されて正しくなりました。オーバークラウドを Cinder Netapp バックエンドと共にデプロイできるようになりました。

BZ#1573787

以前のリリースでは、libvirtd のライブマイグレーションのポート範囲は `qemu.conf` ファイルで指定されている 49152 から 49215 まででした。Linux では、この範囲は 32768 から 61000 までのエフェメラルポート範囲のサブセットです。エフェメラル範囲内のポートはいずれも他のサービスが使用可能です。その結果、ライブマイグレーションは `Live Migration failure: internal error: Unable to find an unused port in range 'migration' (49152-49215)` というエラーで失敗していました。libvirtd ライブマイグレーションの新しいポート範囲 (61152 から 61215 まで) はエフェメラル範囲外です。

BZ#1576572

以前のリリースでは、NIC の設定テンプレートに空白行があり、その後の行頭にコンマがある場合には、`yaml-nic-config-2-script.py` は次の行の最初の列をリセットしませんでした。スクリプトによって変換された NIC の設定テンプレートは無効で、デプロイメントが失敗していました。今回の更新により、スクリプトは空白行を検出した場合にその列の値を正しく設定するようになりました。空白行の後の行頭にコンマがあるテンプレートは正しく変換されるようになりました。

puppet-nova

BZ#1579691

Nova の libvirt ドライバーは、CPU モデルの設定時に、CPU 機能のフラグをより細かく指定できるようになりました。この変更の1つの利点は、"Meltdown" CVE の修正を適用した後に、Intel ベースの仮想 CPU モデルで実行しているゲスト上でパフォーマンスの低下が軽減される点が挙げられます。ゲストのパフォーマンスに対する影響は、CPU 機能フラグ PCID(Process-Context ID) を `guest` CPU に公開することによって軽減されます。これは、物理ハードウェア自体の中に PCID フラグが利用可能であることを前提とします。この変更により、PCID のみが CPU 機能フラグであった制限がなくなり、複数の CPU フラグの追加/削除が可能となったため、他のユースケースに対応するようになりました。詳しい情報は、`nova.conf` の `[libvirt]/cpu_model_extra_flags` の説明を参照してください。

puppet-openshift

BZ#1599805

OpenDaylight は OpenFlow (OF) の統計を定期的にポーリングします。この統計は、現在どこでも使用されていません。この動作は OpenDaylight のパフォーマンスに影響を及ぼします。OF の統計のポーリングを無効にすると、OpenDaylight のパフォーマンスを向上させることができます。

puppet-tripleo

BZ#1598038

以前のリリースでは、競合状態が原因でインスタンス HA デプロイメントが失敗し、`Error: unable to`

get cib というエラーが表示されていました。この競合は、pacemaker クラスタが完全に稼動状態になる前に pacemaker のプロパティが設定されていたために発生し、unable to get cib のエラーで操作が失敗していました。今回の修正により、IHA を使用する場合に、デプロイメントでエラーが発生しなくなりました。

BZ#1564654

以前のリリースでは、stack の名前に大文字を使用するとデプロイメントが失敗していました。今回の更新では、stack の名前に大文字が使用されていてもデプロイメントが成功するようになりました。具体的には、コンテナ内の bootstrap_host スクリプトにより文字列が小文字に変換され、pacemaker プロパティも同じように変換されます。

BZ#1570039

ローテーションされるログをデフォルトで圧縮する、コンテナ化された logrotate サービスの圧縮オプションが追加されました。delaycompress オプションを使用すると、ログファイルの最初のローテーションは圧縮されないようになります。

BZ#1601497

以前のリリースでは、Cinder の Netapp バックエンドの一部の非推奨パラメーターに空の文字列の値を設定すると、Cinder ドライバーの設定が無効となり、Cinder の Netapp バックエンドドライバーの初期化中にエラーが発生していました。今回の更新では、Netapp の非推奨パラメーターの空の文字列の値は、有効な Netapp ドライバーの設定に変換されます。したがって、Cinder の Netapp バックエンドドライバーは正常に初期化されるようになりました。

BZ#1590952

以前のリリースでは、Cinder Netapp バックエンドは CinderNetappNfsMountOptions TripleO Heat パラメーターを無視していたため、TripleO Heat パラメーターによる Netapp NFS のマウントオプションの設定ができませんでした。今回の更新で、Cinder の Netapp の設定を処理するコードは CinderNetappNfsMountOptions パラメーターを無視しないようになりました。CinderNetappNfsMountOptions パラメーターにより、Cinder の Netapp NFS マウントオプションが正しく設定されます。

BZ#1599409

バージョンのアップグレード中に、Cinder のデータベースの同期はブートストラップモードでのみ実行されるようになりました。これにより、全コントローラーノードでデータベースの同期が実行された際に発生していたデータベースの同期およびアップグレードでのエラーが防がれるようになりました。

4.6. RHBA-2018:3587: RED HAT OPENSTACK PLATFORM 13.0 DIRECTOR のバグ修正アドバイザリー

本項に記載するバグは、アドバイザリー RHBA-2018:3587 で対応しています。このアドバイザリーについての詳しい情報は、[RHBA-2018:3587 - Bug Fix Advisory](#) を参照してください。

instack-undercloud

BZ#1627043

IPMI bootdev コマンドを受け取ると、一部のハードウェアでブートデバイスの順序が意図せず変わっていました。そのため、ノードが正しい NIC から起動しなくなったり、PXE がまったく起動しなくなったりすることがありました。本リリースで、ipmi ドライバーに新たな noop 管理インターフェイスが追

加されました。このドライバーを使用すると `bootdev` コマンドは発行されず、現在の起動順が使用されます。ノードは、正しい NIC から PXE ブートを試み、その後ローカルのハードドライブにフォールバックするように設定する必要があります。今回の変更で導入された新たな管理インターフェイスにより、事前に設定された起動順が必ず維持されます。

BZ#1631009

以前のバージョンでは、オーバークラウドと同様に、アンダークラウド `hieradata` のオーバーライド値を使用して `<service>::config` オプションにより一部のサービス設定をチューニングすることができました。ただし、この機能はデプロイされたすべての OpenStack サービスで利用可能なわけではありませんでした。今回のバージョンでは、現在利用できないあらゆる設定値を、`<service>::config hieradata` により更新することができるようになりました。

openstack-tripleo-common

BZ#1631848

Red Hat OpenStack Platform 12 を 13 にアップグレードする際に、`ceph-osd` パッケージが削除されます。パッケージが削除されると、コンテナで動作中であっても OSD が停止していました。本リリースで、アップグレード中にパッケージを削除する Playbook が削除され、アップグレード中 Ceph OSD が意図せず停止することがなくなりました。

BZ#1545151

OpenStack が更新またはアップグレードされると、`director` は最新の `amphora` イメージを `glance` にアップロードします。最新の `amphora` イメージにより、最新の一般バグ修正およびセキュリティー上の修正が適用された状態で `amphora` インスタンスが実行されます。これには、`Octavia` エージェントに関する修正だけでなく、オペレーティングシステムに関する修正も含まれます。

今回のリリースで、新たに作成される `amphora` インスタンスおよび再作成される `amphora` インスタンスに、最新の `amphora` イメージが使用されるようになりました。それまでの `amphora` イメージは、名前を変更して (接尾辞にタイムスタンプを追加) 引き続き `glance` に保管されます。

openstack-tripleo-heat-templates

BZ#1619092

`publicURL keystone` エンドポイントに接続されたインスタンス HA スクリプトの1つ。これが、デフォルトで `internalURL` エンドポイントに移されています。また、`nova.conf` の `[placement]/valid_interfaces` 設定エントリーポイントにより、オペレーターはこの設定をオーバーライドすることができます。

BZ#1624899

本リリース以前は、オンラインデータ移行のトリガーがありませんでした。OSP 13 へのアップグレード後、オーバークラウドの `nova`、`cinder`、および `ironic` のオンラインデータ移行は自動的に実施されないため、手動での対応が必要でした。今回のリリースで、オンラインデータ移行のトリガーに関するロジックが追加されました。OSP 13 にアップグレードする際、**openstack overcloud upgrade converge** コマンドの実行時にオンラインデータ移行がトリガーされます。

BZ#1619104

本リリース以前は、`nova::compute::libvirt::rx_queue_size/nova::compute::libvirt::tx_queue_size` を使用して受信キューのサイズを設定することができました。しかし、専用の TripleO `heat` テンプレートパラメーターはありませんでした。今回のリリースで、以下のようにロールベースで受信キューのサイズ

を設定できるようになりました。

```
parameter_defaults: ComputeParameters: NovaLibvirtRxQueueSize: 1024 NovaLibvirtTxQueueSize: 1024
```

結果的に、rx_queue_size/tx_queue_size は新たなパラメーターを使用して設定されます。

BZ#1466117

OpenStack director の一部として MTU を設定するために、本リリースでは NeutronML2PhysicalNetworkMtus として **neutron::plugins::ml2::physical_network_mtus** が heat テンプレートに追加され、ml2 プラグインの MTU が有効化されるようになりました。neutron::plugins::ml2::physical_network_mtus は、TripleO heat テンプレートからの値を元に設定されま

す。

BZ#1594367

本バージョン以前は、Docker デーモンに再起動が必要かどうかを判断する条件が非常に厳格でした。そのため、Docker 設定の変更や Docker RPM の更新があるたびに、Docker デーモンおよびすべてのコンテナは再起動されていました。今回のリリースで条件が緩和され、コンテナが不必要に再起動されなくなりました。設定の変更にはライブリストア機能を使用してください。これにより、Docker RPM の更新時には Docker デーモンおよびすべてのコンテナは再起動されますが、Docker 設定の変更時には再起動されません。

BZ#1612960

設定変更が一切ない状況でも、再デプロイ時に多くのコンテナが不必要に再起動される場合があります。これは、設定ファイルの md5 変換に多くの不要なファイルが含まれているためでした。今回のリリースで、再デプロイ時にコンテナが不必要に再起動されなくなりました。

BZ#1619663

TripleO CinderNetappBackendName パラメーターが、cinder の Netapp バックエンドのデフォルト値を正しくオーバーライドしませんでした。そのため、cinder の Netapp バックエンドに関連付けられた名前がオーバーライドできませんでした。今回のリリースで、CinderNetappBackendName パラメーターがデフォルトのバックエンド名を正しくオーバーライドするようになりました。

puppet-cinder

BZ#1617199

さまざまな設定設定が cinder から削除されましたが、対応するパラメーターは、cinder 設定設定のための TripleO Puppet モジュールから削除されませんでした。そのため、無効な cinder 設定設定が cinder.conf に追加されていました。今回のリリースで Puppet モジュールが更新され、非推奨の設定が cinder.conf に追加されなくなりました。



注記

更新された Puppet モジュールにより、それまでに cinder.conf に追加された非推奨の設定が削除されることはありません。非推奨の設定は手動で削除する必要があります。

puppet-tripleo

BZ#1628705

システムのシャットダウン時に `rhel-plugin-push.service` と Docker サービスが正常に連携しないため、コントローラーのリブートに長時間を要していました。今回のリリースで、これらの2つのサービスに対して正しいシャットダウン順序が強制的に適用されるようになりました。これで、コントローラーのリブート時間が短縮されました。

BZ#1602833

デプロイメント中、コントローラー3つのうちの2つで、OVS スイッチに誤った OpenFlow コントローラーポート (6653 ではなく 6640) が設定される場合があります。これにより、デプロイメントの失敗や、デプロイメント後の機能不良 (誤ったフローがスイッチにプログラムされる) が生じていました。今回のリリースで、それぞれの OVS スイッチについて、すべての OpenFlow コントローラーポートが正しく 6653 に設定されるようになりました。すべての OVS スイッチが3つの URI で設定される正しい OpenFlow コントローラー設定を持ち、OpenDaylight はポート 6653 をリッスンします。

BZ#1488907

1つの OpenDaylight インスタンスがクラスターから削除されると、インスタンスが分離された状態になり、着信リクエストに対応しなくなります。しかし、HA Proxy は分離された OpenDaylight インスタンスに対してリクエストの負荷分散を続けるため、OpenStack ネットワークコマンドの失敗や、機能不良が生じる場合があります。HA Proxy が、分離された OpenDaylight インスタンスを異常な状態と識別するようになりました。HA Proxy は分離された OpenDaylight にリクエストを転送しません。

python-os-brick

BZ#1631024

特定の状況下で、FibreChannel HBA ホストのスキャンに関する `os-brick` コードが無効な値を返すことがあります。そのため、`cinder` および `nova` 等のサービスが失敗していました。今回のリリースで、FibreChannel HBA スキャンコードが常に有効な値を返すようになりました。FibreChannel HBA ホストをスキャンする際に、`cinder` および `nova` はクラッシュしなくなりました。

BZ#1607196

マルチパス接続の場合、接続が解除される際に、すべてのパスについてデバイスが個別にフラッシュされます。特定のケースでは、あるデバイスのフラッシュ失敗により、接続が解除できない場合があります。マルチパスをフラッシュすることでバッファされたデータが必ずリモートデバイスに書き込まれるので、今回のリリースで個々のパスはフラッシュされなくなりました。実際にデータを喪失した場合に限り、接続の解除に失敗するようになりました。

BZ#1619485

`multipathd show status` が返すべきエラーコードを返さない状況があります。したがって、`multipathd` がエラー状態にあることを正しく検出するために、この問題の回避策として `stdout` を確認していません。

BZ#1628471

本リリース以前は、移行開始時の短時間に単一の iSCSI パスが失敗すると、ボリュームの移行に失敗していました (`VolumePathNotRemoved` エラー)。今回のリリースでは、ボリューム削除の確認がタイムアウトするまでの時間を延長して問題を解決しています。

BZ#1629873

iSCSI デバイスの検出では、再スキャンの時間を元にデバイスの有無を確認していました。したがって、スキャンとスキャンの間に利用可能になるデバイスは検出されませんでした。今回のリリースでは、検索と再スキャンは異なるリズムで動作する独立した操作になり、1秒ごとに確認が行われます。

python-tripleoclient

BZ#1624462

本リリース以前は、カスタムプランを使用すると (デプロイコマンドラインの `-p` オプションを使用)、既存オーバークラウドの再デプロイメント時に多くのパスワード (mysql、horizon、pcsd 等) が新しい値にリセットされていました。このため、再デプロイメントに失敗していました。今回のリリースで、カスタムプランが原因で新しいパスワードが設定されることがなくなりました。

4.7. RHBA-2019:0068: RED HAT OPENSTACK PLATFORM 13 のバグ修正および機能拡張アドバイザリー

本項に記載するバグは、アドバイザリー RHBA-2019:0068 で対応しています。このアドバイザリーについての詳しい情報は、[RHBA-2019:0068 - Bug Fix Advisory](#) を参照してください。

openstack-tripleo-common

BZ#1647931

以前のリリースでは、アンダークラウドからノードを更新すると、**capabilities** フィールドの値が文字列値のタイプに変換されないことがありました。このバグ修正により、ノードの更新時に **capabilities** フィールドが必ず文字列値のタイプに変換されるようになりました。

openstack-tripleo-heat-templates

BZ#1648261

今回の機能拡張で、パラメーター **NeutronOVSTunnelCsum** が追加されました。これにより、heat テンプレートで **neutron::agents::ml2::ovs::tunnel_csum** を設定することができます。このパラメーターにより、OVS エージェントの発信 IP パケットを転送する GRE/VXLAN トンネルのトンネルヘッダーチェックサムを設定または削除します。

BZ#1595114

コントローラーを置き換える際に OpenDaylight (ODL) の設定ファイルは再生成されないため、更新に失敗していました。今回の修正で `/opt/openshift/data` がホストからアンマウントされ、再デプロイメント時に設定ファイルが再生成されるようになりました。

BZ#1641825

以前のリリースでは、OpenStack Platform director は、Block Storage (Cinder) が Nova の要権限 API を使用するボリュームにアクセスするための認証データを設定していませんでした。このため、これらのボリュームに関する操作 (例: 使用中のボリュームの移行) に失敗していました。

今回のバグ修正で、Cinder に Nova の認証データを設定する機能が追加されました。その結果、これらの認証情報により要権限 API を使用するボリュームに関する操作を実施できるようになりました。

BZ#1652544

Ironic が設定されたコンテナ化デプロイメントにアップグレードする際に TFTP サーバーが正しく

シャットダウンせず、アップグレードに失敗していました。今回の修正で TFTP サーバーのシャットダウンプロセスが見直されました。その結果、サーバーがポートをリッスンできるので、アップグレードが正常に完了するようになりました。

BZ#1638021

以前のリリースでは、ODL の Open vSwitch 停止状態検出タイマーの値が大規模なデプロイメントには不十分なため、タイマーのカウントアップ後に ODL L2 エージェントがオフラインと識別されていました。

今回の修正で、停止状態検出タイマーのデフォルト期間が延長され、**OpenDaylightInactivityProbe** heat パラメーターを使用して director からタイマーを設定する機能が追加されました。デフォルト値は 180 秒です。

BZ#1639199

RabbitMQ コンテナの Pacemaker ログファイルの場所が正しく設定されていなかったため、不要なログファイルが /var/log/secure に作成されていました。今回の修正で、RabbitMQ コンテナの起動時に /var/log/btmp パスをマウントするプロセスが追加され、Pacemaker が正しい場所にログを作成できるようになりました。

BZ#1644017

Cinder Dell EMC StorageCenter ドライバーを設定して、ボリューム/イメージ間のデータ転送にマルチパスを使用する機能が追加されました。この機能には、新たなパラメーター **CinderDellScMultipathXfer** (デフォルト値: **True**) が含まれます。マルチパス転送が可能になったことで、ボリューム/イメージ間のデータ転送の合計時間を短縮することができます。

BZ#1644020

この機能により、新たなパラメーター **NovaLibvirtVolumeUseMultipath** (ブール値) が追加されました。これにより、コンピュータードの nova.conf ファイルでマルチパス設定パラメーター **libvirt/volume_use_multipath** が設定されます。このパラメーターは、Compute ロールごとに設定することができます。デフォルト値は **False** です。

BZ#1656495

この機能により、パラメーター **NovaSchedulerWorkers** が追加されました。これにより、スケジューラーノードごとに複数の **nova-schedule** ワーカーを設定することができます。デフォルト値は **1** です。

BZ#1412661

以前のリリースでは、コントローラーノードの再起動後に、LVM ボリュームグループに関連付けられたループバックデバイスが再起動しませんでした。そのため、iSCSI Cinder バックエンドにより使用される LVM ボリュームグループが再起動後に維持されず、新規ボリュームが作成されませんでした。

今回のバグ修正により、コントローラーノードの再起動後にループバックデバイスが復元され、ノードから LVM ボリュームグループにアクセスできるようになりました。

BZ#1642446

今回の機能拡張により Erlang 仮想マシンに **RabbitAdditionalErlArgs** パラメーターが追加され、仮想マシンのカスタム引数を定義できるようになりました。デフォルトの引数は **+sbtw none** で、追加の操作が必要な場合は Erlang スレッドをスリープ状態にします。詳細情報は、Erlang のドキュメント

(<http://erlang.org/doc/man/erl.html#+sbwt>) を確認してください。

openstack-tripleo-heat-templates-compat

BZ#1593774

従来、OpenStack 12 テンプレートからのデプロイでは、OpenStack 13 director は正しい Ceph バージョンを設定しませんでした。このため、オーバークラウドのデプロイメントは失敗していました。

今回のバグ修正により Ceph のバージョンが Jewel に設定され、OpenStack 12 テンプレートから正常にデプロイメントできるようになりました。

puppet-opendaylight

BZ#1607362

この機能により、IPv6 アドレスへの OpenDaylight (ODL) のデプロイがサポートされるようになりました。

4.8. RHBA-2019:0448: RED HAT OPENSTACK PLATFORM 13 のバグ修正 および機能拡張アドバイザリー

本項に記載するバグは、アドバイザリー RHBA-2019:0448 で対応しています。このアドバイザリーについての詳しい情報は、[RHBA-2019:0448 - Bug Fix Advisory](#) を参照してください。

openstack-tripleo-common

BZ#1668774

このバグの原因は、バージョン 3.1 またはそれ以降に更新された dmidecode が小文字でシステム UUID を返すことでした。その結果、上記のバージョン前にノードごとの ceph-ansible カスタマイズを設定してデプロイしたシステムは、UUID に大文字/小文字の不一致があると破損し、デプロイメントに失敗します。今回の修正で **openstack-tripleo-common** パッケージが更新され、大文字および小文字の UUID が受け入れられるようになりました。dmidecode の出力は強制的に小文字表示になるので、コードに大文字/小文字の区別はありません。

openstack-tripleo-heat-templates

BZ#1659077

以前のリリースでは、ファイアウォールによるパケットドロップが原因で、Octavia Health Manager は amphorae からハードビートメッセージを受け取りませんでした。その結果、Octavia コンポーザブルロールデプロイメント上のロードバランサーの **operating_status** は、決して **ONLINE** に変わりませんでした。

今回の更新により、Octavia コンポーザブルロールデプロイメント上のロードバランサーの動作ステータスが、正しく **ONLINE** に変わるようになりました。

BZ#1636496

今回の更新により、以下のパラメーターを使用して、バックエンドメンバーおよびフロントエンドクライアントのデフォルトの Octavia タイムアウトを設定できるようになりました。

- **OctaviaTimeoutClientData**: フロントエンドクライアントの停止状態タイムアウト

- **OctaviaTimeoutMemberConnect**: バックエンドメンバーの接続タイムアウト
- **OctaviaTimeoutMemberData**: バックエンドメンバーの停止状態タイムアウト
- **OctaviaTimeoutTcpsInspect**: コンテンツの検査用に TCP パケットを待機する時間

これらすべてのパラメーターの値は、ミリ秒単位です。

BZ#1655815

以前のリリースでは、コンテナ化された OpenStack サービスが作成する iSCSI 接続は、ホスト上では把握できませんでした。ホストはシャットダウン時にすべての iSCSI 接続を終了する必要があります。ホスト上では接続情報を把握することができないため、ホストがこれらの iSCSI 接続の切断に失敗し、OpenStack 接続の終了に失敗すると、シャットダウンシーケンスがハングアップしていました。

今回の更新により、iSCSI 接続を作成するコンテナ化サービスの接続情報をホスト上で把握することができ、その結果シャットダウンシーケンスはハングアップしなくなりました。

BZ#1597666

今回の更新により、OpenDaylight のマイナー更新が Red Hat OpenStack Platform のマイナー更新ワークフローに含まれるようになりました。

BZ#1611960

今回の更新により、バックエンドとして OpenDaylight を使用する Red Hat OpenStack Platform 環境のコンピュータードが、正常にスケーリングできるようになりました。

BZ#1623123

以前のリリースでは、再デプロイメント後に ODL 設定ファイルが存在しませんでした。

今回の更新により、**/opt/opendaylight/data** がホストにマウントされなくなりました。その結果、再デプロイメント時に ODL 設定ファイルが生成されるようになりました。

BZ#1639203

以前のリリースでは、通常の運用中に rabbitmq pacemaker バンドルが過度にログを記録していました。

今回の更新により、rabbitmq バンドルが過度にログを記録しなくなりました。特に、rabbitmq バンドルは害のないエラー **Failed to connect to system bus: No such file or directory** をログに記録しません。

openstack-tripleo-image-elements

BZ#1646907

今回の更新により、セキュリティーが強化された完全なイメージを UEFI モードでブートできるようになりました。

puppet-opendaylight

BZ#1650576

以前のリリースでは、OpenDaylight のパッケージングでは OpenDaylight **log_pattern** のデフォルト値が使用され、PaxOsgi アペンダーが含まれていました。これらのデフォルト値が常にすべてのデプロイメントに適する訳ではなく、カスタムの値を設定することが望ましいこともあります。

今回の更新により、**puppet-openshift** に 2 つの設定変数が追加されています。

- 1) **log_pattern**: OpenDaylight ロガー log4j2 で使用するログパターンを設定するには、この変数を使用します。
- 2) **enable_paxosgi_appender**: PaxOsgi アペンダーを有効または無効にするには、このブール値フラグを使用します。

puppet-openshift では、OpenDaylight のデフォルト値も変更されています。**puppet-openshift** を使用するデプロイメントは、以下に示す新しいデフォルト値を持ちます。

- **log_pattern**: `%d{ISO8601} | %-5p | %-16t | %-60c{6} | %m%n`
- **enable_paxosgi_appender**: `false`

新たな変数設定オプション

log_pattern

ログ記録に使用するログパターンを指定する文字列

デフォルト: `%d{ISO8601} | %-5p | %-16t | %-60c{6} | %m%n`

有効なオプション: 有効な log4j2 パターンである文字列

enable_paxosgi_logger

ログ記録に PaxOsgi アペンダーを有効にするかどうかを指定するブール値

enable_paxosgi_logger 変数を有効にする場合、追加機能を使用するためにログパターンも変更する必要があります。**log_pattern** 変数を変更し、PaxOsgi トークンが含まれるパターンを含めます。たとえば、**log_pattern** 変数を以下の値が含まれる文字列に設定します。

```
'%X{bundle.id} - %X{bundle.name} - %X{bundle.version}'
```

log_pattern 変数を編集しない場合、PaxOsgi アペンダーは有効で動作を続けますが、ログ記録に追加機能は使用されません。

たとえば、**enable_paxosgi_logger** 変数を **true** に設定し、**log_pattern** 変数を以下の値に設定します。

```
'%d{ISO8601} | %-5p | %-16t | %-32cNORMAL | %X{bundle.id} - %X{bundle.name} - %X{bundle.version} | %m%n'
```

デフォルト: **false**

有効なオプション: ブール値 **true** および **false**

puppet-tripleo

BZ#1600449

以前のリリースでは、BlockStorage ロールを設定してオーバークラウドをデプロイし、BlockStorage ロールに属するノードで pacemaker 属性を設定した場合、デプロイメントに失敗していました。

今回の更新により、pacemaker の管理する cinder-volume リソースは、pacemaker が管理するノードでのみ起動するようになりました。その結果、BlockStorage ロールを設定したオーバークラウドのデプロイメントに成功します。

4.9. RHBA-2021:2385 - RED HAT OPENSTACK PLATFORM 13 のバグ修正および機能拡張アドバイザリー

本項に記載するバグは、アドバイザリー RHBA-2021:2385 で対応しています。このアドバイザリーについての詳しい情報は、RHBA-2021:0817 - Bug Fix Advisory を参照してください。

openstack-cinder コンポーネント

BZ#1914590

今回の更新以前は、Block Storage サービス(cinder) API 応答が失われた場合、NetApp SolidFire バックエンドは未使用の複製ボリュームを作成していました。

今回の更新で、SolidFire ドライバーのパッチは、最初にボリューム名の作成を試みる前に、ボリューム名がすでに存在しているかどうかを確認します。このパッチは、読み取りタイムアウトの検出直後にボリュームの作成をチェックし、無効な API 呼び出しを防ぎます。(BZ#1914590)

BZ#1940153

今回の更新以前は、Block Storage サービス(cinder)を使用して HP3Par Storage バックエンドサーバーのスナップショットから多数のインスタンス（ブート可能なボリューム）を作成すると、タイムアウトが発生していました。HP 変数(**convert_to_base**)が true に設定され、HP3Par が元のボリュームのシックボリュームを作成していました。これは不要で不要なアクションでした。

今回の更新により、新しい HP ドライバー(4.0.11)が新しい仕様を含む RHOSP 13 にバックポートされました。

```
hpe3par:convert_to_base=True | False
```

- True（デフォルト）: ボリュームはスナップショット(HOS8 の動作)とは別に作成されます。
- false - ボリュームは、スナップショットの子として作成されます(HOS5 の動作)。

使用方法

cinder type-key コマンドを使用して、HPE3Par ボリュームの新しい仕様を設定できます。

```
cinder type-key <volume-type-name-or-ID> set hpe3par:convert_to_base=False | True
```

例

```
$ cinder type-key myVolType set hpe3par:convert_to_base=False
$ cinder create --name v1 --volume-type myVolType 10
$ cinder snapshot-create --name s1 v1
$ cinder snapshot-list
$ cinder create --snapshot-id <snap_id> --volume-type myVolType --name v2 10
```

注記

v2 のサイズが v1 よりも大きい場合は、ボリュームを拡張することはできません。この場合、エラーを回避するために、v2 はベースボリュームに変換されます(**convert_to_base=True**)。 (BZ#1940153)

BZ#1888417

今回の更新以前は、Block Storage サービス(cinder)の NetApp SolidFire バックエンドへの API 呼び出しが **xNotPrimary** エラーで失敗する可能性がありました。このタイプのエラーは、SolidFire が接続を自動的に移動してクラスタのワークロードをリバランスするために、同時に操作がボリュームに追加されたときに発生しました。

今回の更新で、SolidFire ドライバーのパッチが、再試行できる例外のリストに **xNotPrimary** 例外を追加するようになりました。 (BZ#1888417)

BZ#1888469

今回の更新以前は、特定の環境でユーザーがタイムアウトしていましたが、大概がボリュームが大きすぎていました。多くの場合、これらのマルチテラバイトボリュームでは、ネットワークのパフォーマンスが低下したり、SolidFire クラスタに関連するアップグレードの問題が発生したりしていました。

今回の更新で、SolidFire ドライバーに 2 つのタイムアウト設定が追加され、ユーザーが環境に適切なタイムアウトを設定できるようになりました。 (BZ#1888469)

openstack-tripleo-heat-templates

BZ#1875508

今回の機能拡張により、オーバークラウドのデプロイ時に、ロールの Orchestration サービス(heat)パラメーター **ServiceNetMap** をオーバーライドできるようになりました。

TLS を使用するスパイン/リーフ型 (エッジ) デプロイメントでは、階層の補間を使用してロールのネットワークをマッピングする際に問題がありました。ロールごとに ServiceNetMap を上書きすると、TLS-everywhere のデプロイメントで発生する問題が修正され、インターフェイスが容易になり、より複雑な階層の補間の必要性がなくなります。 (BZ#1875508)

BZ#1924727

Block Storage のバックアップサービスは、ホスト上のファイルにアクセスする必要がある場合がありますが、サービスを実行するコンテナで利用できない場合があります。今回の機能拡張により、**CinderBackupOptVolumes** パラメーターが追加されました。これを使用して、Block Storage のバックアップサービス用に追加のコンテナボリュームマウントを指定することができます。 (BZ#1924727)

puppet-tripleo

BZ#1934440

今回の更新以前は、最新バージョンの Red Hat AMQ Interconnect では CA 証明書のない TLS 接続が許可されないため、Service Telemetry Framework (STF)クライアントは STF サーバーに接続できませんでした。

今回の更新では、新しいオーケストレーションサービス (heat) パラメーター **MetricsQdrSSLProfiles** を提供することで、この問題を修正します。

Red Hat OpenShift TLS 証明書を取得するには、以下のコマンドを入力します。

```
$ oc get secrets
$ oc get secret/default-interconnect-selfsigned -o jsonpath='{.data.ca\.crt}' | base64 -d
```

Red Hat OpenShift TLS 証明書の内容を含む **MetricsQdrSSLProfiles** パラメーターをカスタム環境ファイルに追加します。

```
MetricsQdrSSLProfiles:
- name: sslProfile
  caCertFileContent: |
    -----BEGIN CERTIFICATE-----
    ...
    TOpbgNIPcz0sloNK3Be0jUcYHVMPKGMR2kk=
    -----END CERTIFICATE-----
```

次に、**openstack overcloud deploy** コマンドを使用してオーバークラウドを再デプロイします。(BZ#1934440)

python-os-brick

BZ#1943181

今回の更新以前は、Compute サービス(nova)が Block Storage サービス(cinder)への **終了接続** 呼び出しを行うと、シングルデバイスおよびマルチパスデバイスがフラッシュされず、これらのデバイスが **残り** 状態にあるため、データの損失のリスクがありました。

この問題の原因は、os-brick **disconnect_volume** コードは、**use_multipath** パラメーターに、元の **connect_volume** 呼び出しで使用されたコネクターと同じ値があることを前提としていました。

今回の更新により、Block Storage サービスは接続を解除する方法を変更します。os-brick コードは、インスタンスに接続されているボリュームの Compute サービスのマルチパス設定が変更された場合に、ボリュームを適切にフラッシュおよびデタッチするようになりました。(BZ#1943181)