Red Hat OpenStack Platform 17.1

将 DNS 配置为服务

有关如何使用 Red Hat OpenStack Platform 中的 DNS 服务管理域名系统 (DNS) 的信息

Last Updated: 2024-05-23

Red Hat OpenStack Platform 17.1 将 DNS 配置为服务

有关如何使用 Red Hat OpenStack Platform 中的 DNS 服务管理域名系统 (DNS) 的信息

OpenStack Team
rhos-docs@redhat.com

法律通告

摘要

安装、配置、操作、故障排除和升级 RHOSP DNS 服务（指定）的指南。

目录

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 的信息。

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。与我们分享您的成功秘诀。

在 JIRA 中提供文档反馈

使用 Create Issue 表单对文档提供反馈。JIRA 问题将在 Red Hat OpenStack Platform Jira 项目中创建，您可以在其中跟踪您的反馈进度。

1. 确保您已登录到 JIRA。如果您没有 JIRA 帐户，请创建一个帐户来提交反馈。
2. 点击以下链接打开 **Create Issue** 页面： Create Issue
3. 完成 **Summary** 和 **Description** 字段。在 **Description** 字段中，包含文档 URL、章节或章节号以及问题的详细描述。不要修改表单中的任何其他字段。
4. 点 **Create**。

第 1 章 DNS 服务简介

DNS 服务 (designate) 为 Red Hat OpenStack Platform (RHOSP) 部署提供 DNS 即服务实现。

本节简要描述了一些域名系统(DNS)基础知识，描述了 DNS 服务组件，它提供了一个简单的用例，并列出了运行 DNS 服务的各种方法。

本节中包含的主题有：

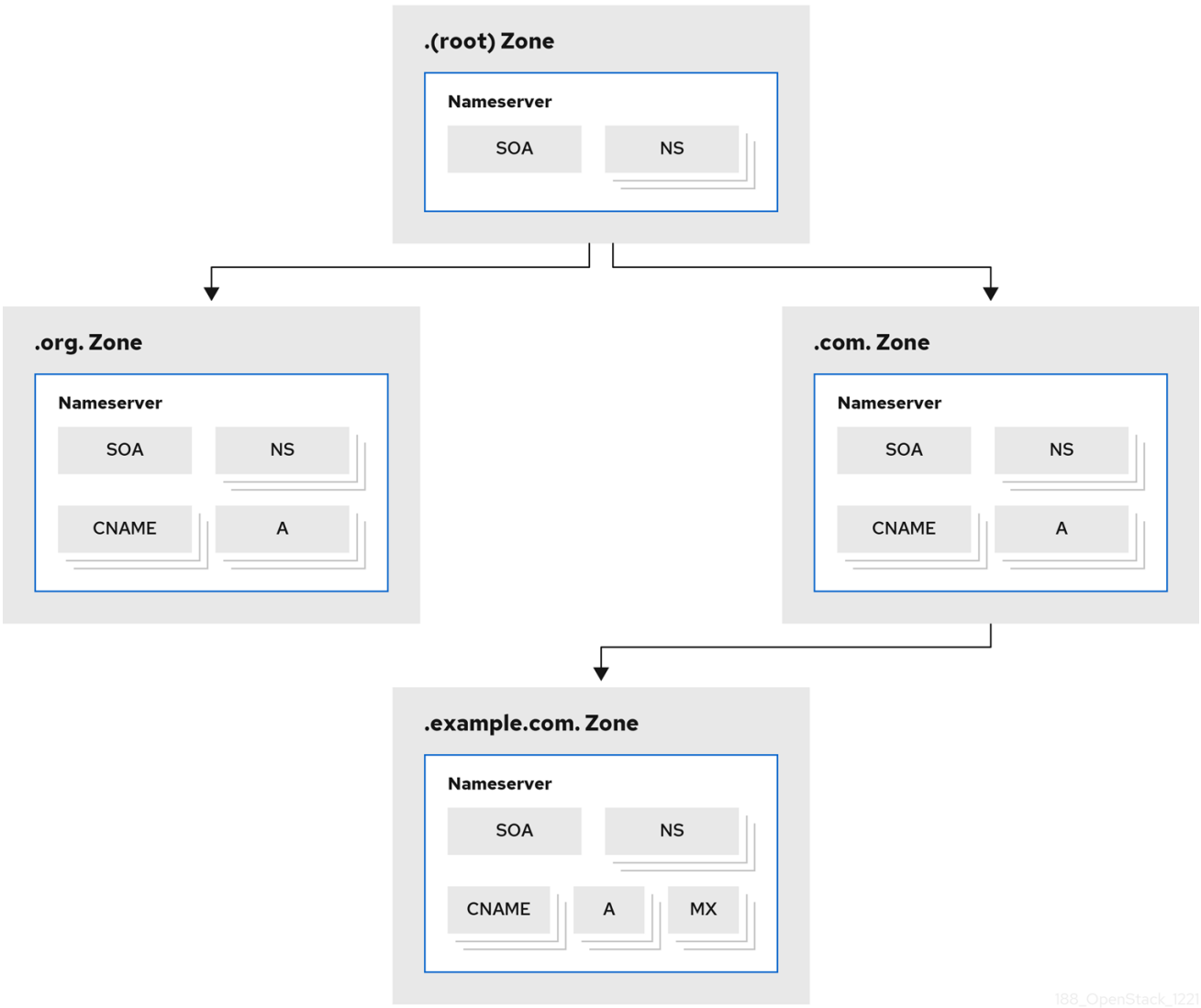
- 第 1.1 节 “域名系统(DNS)的基础知识.”
- 第 1.2 节 “RHOSP DNS 服务简介”
- 第 1.3 节 “DNS 服务组件”
- 第 1.4 节 “DNS 服务的常见部署场景”
- 第 1.5 节 “使用 DNS 服务的不同方法”

1.1. 域名系统(DNS)的基础知识.

域名系统(DNS)是连接到私有或公共网络资源的命名系统。分层的分布式数据库 DNS 将资源与域名相关联的信息，它们被组织到名为 *zone* 的不同组中。权威名称服务器在记录中存储资源和区域信息，这些记录可以通过解析器查找路由网络数据的资源。

名称以区域层次结构的形式进行分隔，并进行委派。单独的名称服务器负责特定的区域。

图 1.1. 域名系统



根区域（即 ）。（点）包含将各种顶级域(TLD)委派给其他名称服务器的记录。这些类型的记录称为名称服务器(NS)记录，并确定哪个 DNS 服务器对特定域具有权威。在存在多个 NS 记录来指示域的主名称服务器和备份名称服务器时，这并不常见。

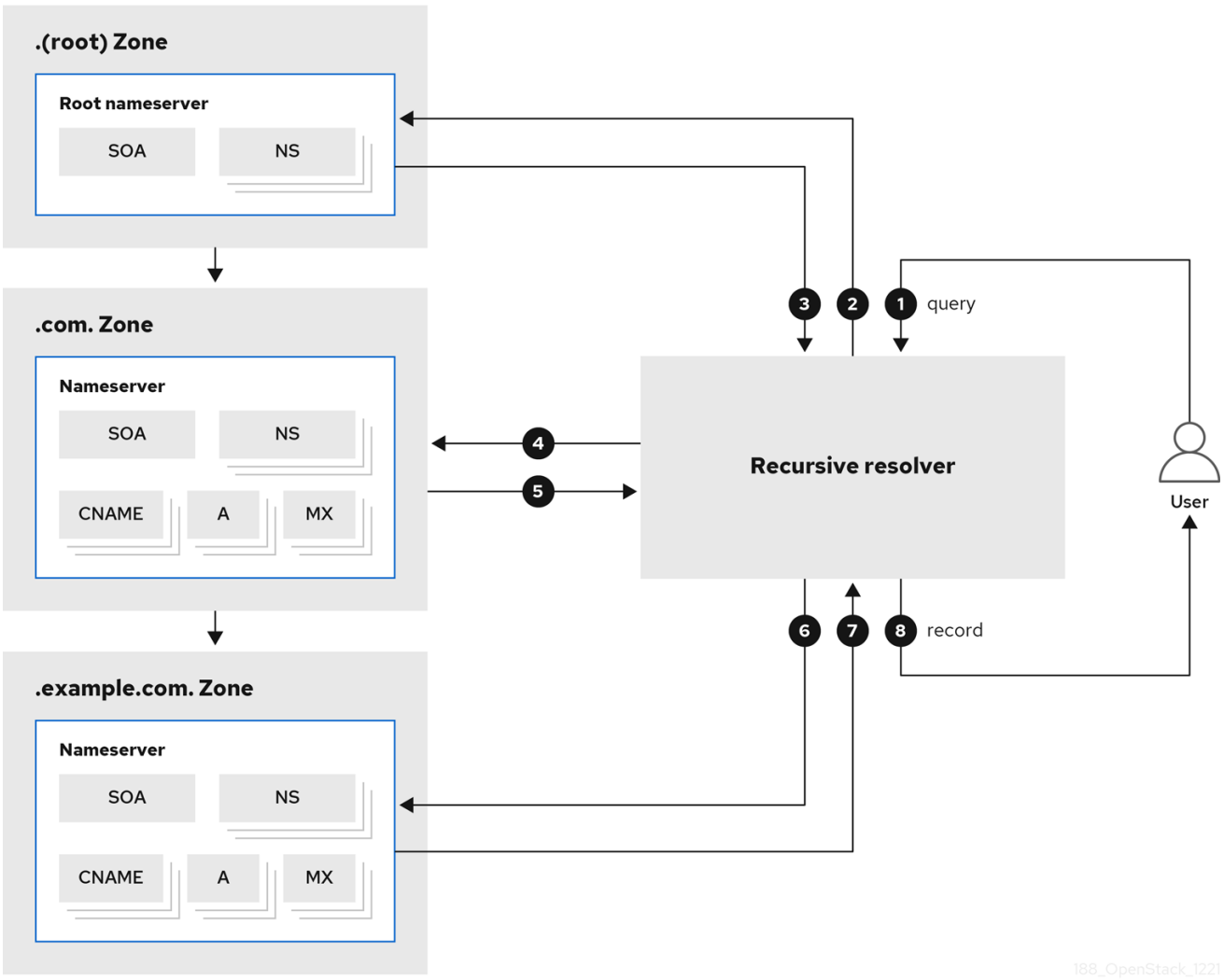
root 区域下是各种 TLD 名称服务器，它们仅包含其 TLD 中域的记录。这些是地址记录和规范名称记录，分别被称为 *A* 和 *CNAME* 记录。

例如，**.com** 名称服务器除将区域委派给其他名称服务器的 NS 记录之外，还包含 **example.com** 的 CNAME 记录。域 **example.com** 可能具有自己的名称服务器，以便它可以创建 **cloud.example.com** 等其他域。

解析器通常分为两部分：*存根解析器* 通常是用户计算机上的库，以及在向用户返回结果之前对名称服务器执行查询的 *递归解析器*。搜索域时，解析器从域末尾开始，并适用于域的开头。

例如，在搜索 **cloud.example.com** 时，解析器以根名称服务器 **.** 开始。root 回复 **.com** 名称服务器的位置。然后，解析器联系 **.com** 名称服务器以获取 **example.com** 名称服务器。最后，解析器查找 **cloud.example.com** 记录并将其返回到用户。

图 1.2. 解析一个 DNS 查询



1	用户查询 **cloud.example.com** 的地址。
2	递归解析器为 **cloud.example.com** 查询 **根** 区域名称服务器。
3	未找到记录，**root** 区域为 **.com** 提供名称服务器。
4	解析器为 **cloud.example.com** 查询 **.com** 名称服务器。
5	未找到记录，**.com** 区域提供 **example.com** 的名称服务器。
6	解析器为 **cloud.example.com** 查询 **example.com** 名称服务器。
7	**example.com** 名称服务器找到 **cloud.example.com**，并向解析器提供 **cloud.example.com** 的 A 记录。
8	解析器将 **cloud.example.com** 的 A 记录转发到用户。

要使此搜索更高效，在解析器上缓存结果，因此在第一个用户请求 **cloud.example.com** 后，解析器可以快速返回后续请求的缓存结果。

其他资源

- https://en.wikipedia.org/wiki/Domain_Name_System
- https://tools.ietf.org/html/rfc1034
- 第 1.2 节 “RHOSP DNS 服务简介”

1.2. RHOSP DNS 服务简介

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)是一个多租户服务，可让您管理 DNS 记录、名称和区域。RHOSP DNS 服务提供 REST API，并与 RHOSP Identity 服务(keystone)集成，以进行用户管理。

使用 RHOSP director，您可以部署 BIND 实例使其包含 DNS 记录，或者您可以将 DNS 服务集成到现有的 BIND 基础架构中。此外，director 可以配置 DNS 服务与 RHOSP 网络服务(neutron)集成，以自动创建计算实例、网络端口和浮动 IP 的记录。

其他资源

- 第 1.1 节 “域名系统(DNS)的基础知识.”
- 第 1.3 节 “DNS 服务组件”

1.3. DNS 服务组件

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)由一个或多个 RHOSP Controller 主机上运行的多个不同服务组成，默认在一个或多个 RHOSP Controller 主机上运行：

指定 API (designate-api 容器)

为用户和 RHOSP 网络服务(neutron)提供 OpenStack 标准 REST API，以便与指定交互。API 通过远程过程调用(RPC)来将它们发送到中央服务来处理请求。

producer (designate-producer container)

编排由指定运行的定期任务。这些任务会长期运行，且潜在可能是大型作业（例如，为 Ceilometer 发出 **dns.zone.exists** ）、从数据库清除已删除的区域，在其刷新间隔上轮询次要区域，生成延迟的 **NOTIFY** 事务，并调用错误状态的定期恢复。

Central (指定中央 容器)

编配区域和记录设置创建、更新和删除。Central 服务接收由 Designate API 服务发送的 RPC 请求，并将必要的业务逻辑应用到数据，同时将其持久存储协调。

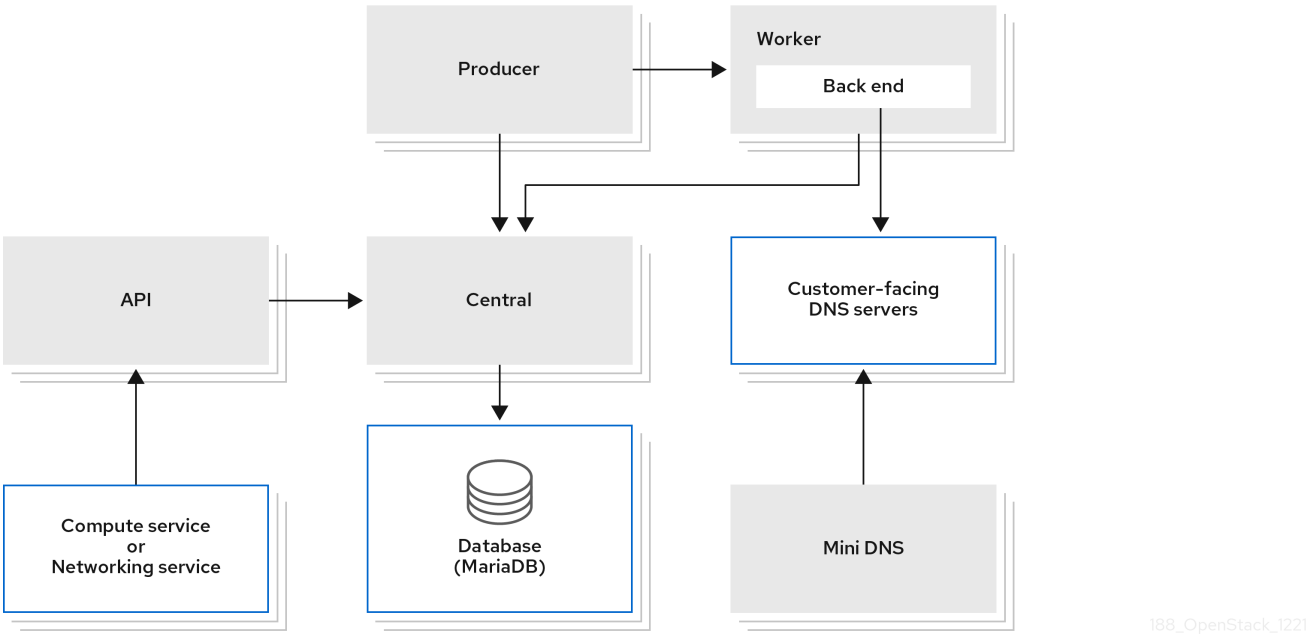
Worker (指定 worker 容器)

为指定管理的 DNS 服务器提供驱动程序的接口。Worker 服务从指定数据库读取服务器配置，还管理 Producer 请求定期任务。

mini DNS (designate-mdns 容器)

管理来自名称服务器的区域权威传输(AXFR)请求。Mini DNS 服务还拉取在指定基础架构外托管的 DNS 区域信息。

图 1.3. DNS 服务架构



在 RHOSP 中，默认情况下，DNS 组件是 BIND 9 和 Unbound：

BIND 9 (绑定 容器)

为 DNS 服务提供 DNS 服务器。BIND 是 DNS 软件的开源套件，特别充当权威名称服务器。

unbound （未绑定容器）

履行 DNS 递归解析器的角色，其启动并分类将 DNS 请求转换为 IP 地址所需的查询。unbound 是一个开源程序，DNS 服务将用作其递归解析器。

DNS 服务使用 oslo 兼容数据库存储数据和 oslo 消息传递，以方便服务间的通信。可以正常运行多个 DNS 服务实例，以促进高可用性部署，API 进程通常位于负载均衡器后面。

其他资源

- 第 1.4 节 “DNS 服务的常见部署场景”
- 第 1.5 节 “使用 DNS 服务的不同方法”

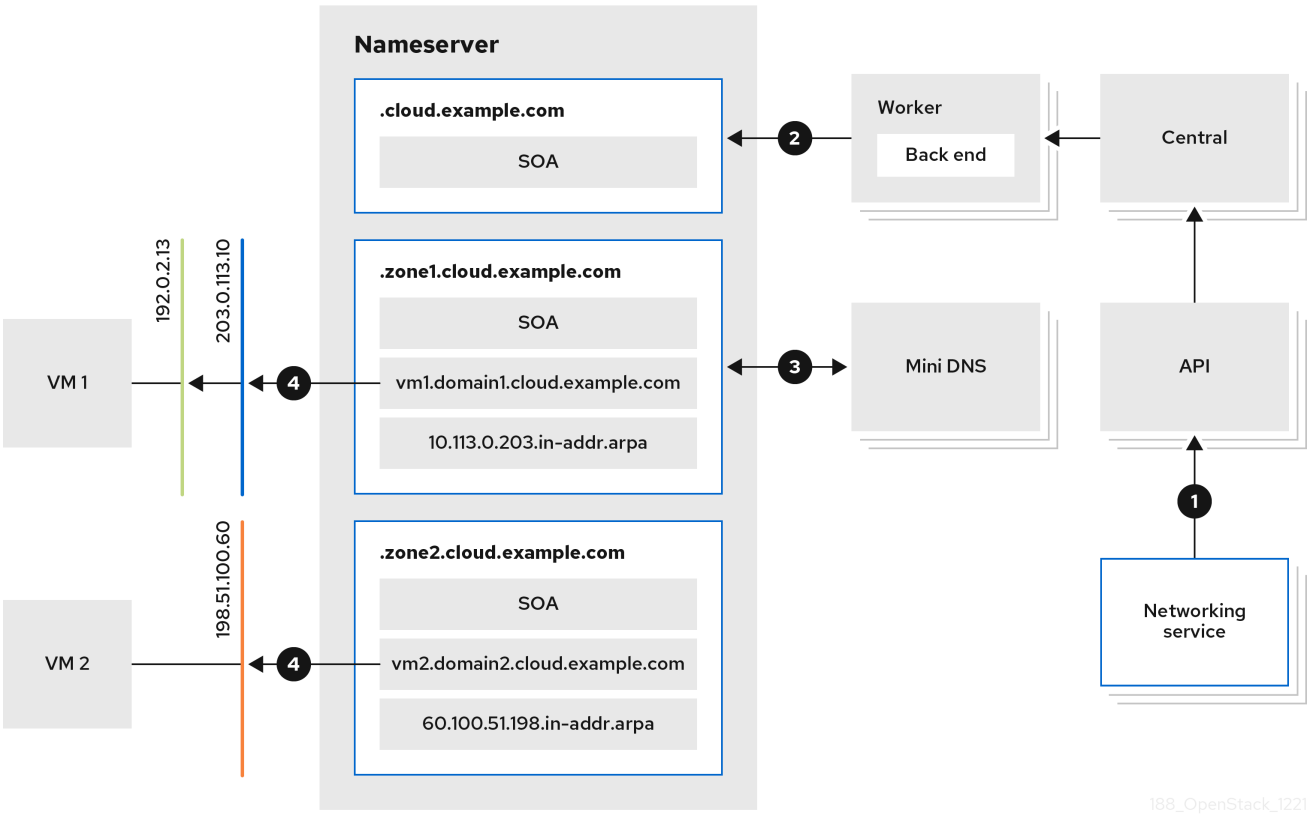
1.4. DNS 服务的常见部署场景

用户创建了两个区域： **zone1.cloud.example.com** 和 **zone2.cloud.example.com**，DNS 服务会添加一个新的授权起始(SOA)记录以及每个新区的新名称服务器(NS)记录。

使用 RHOSP 网络服务，用户会创建一个专用网络，并将它与 **zone1** 和公共网络相关联，并将它与 **zone2** 关联。

最后，用户将虚拟机实例连接到专用网络并附加一个浮动 IP。用户将第二个实例直接连接到公共网络。这些连接会触发网络服务，以请求 DNS 服务代表用户创建记录。DNS 服务将实例名称映射到权威名称服务器上的域，同时创建 PTR 记录以启用反向查找。

图 1.4. 常见 DNS 服务部署



1	您可以将域和名称与 RHOSP 网络服务中的浮动 IP、端口和网络关联。RHOSP 网络服务使用指定的 API 管理端口创建和销毁时的记录。
2	designate Worker 告知名称服务器更新其区域信息。
3	名称服务器从 Mini DNS 请求更新的区域信息。
4	名称服务器同时创建正向和反向记录。

其他资源

- 第 1.2 节 “RHOSP DNS 服务简介”
- 第 1.3 节 “DNS 服务组件”

1.5. 使用 DNS 服务的不同方法

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)提供 REST API，通常以三种方式使用。

- 最常见的方法是使用 RHOSP OpenStack 客户端，一个 python 命令行工具与用于与 RHOSP 服务交互的命令。
- 您还可以通过图形用户界面（RHOSP Dashboard (horizon)使用 DNS 服务。
- 开发人员可以使用 OpenStack SDK 编写应用程序。如需更多信息，请参阅 openstacksdk。

第 2 章 规划 DNS 服务部署

本节讨论在使用 Red Hat OpenStack Platform 规划 DNS 服务（指定）部署时需要考虑的主题。

本节中包含的主题有：

- 第 2.1 节 “DNS 服务器功能支持列表”
- 第 2.2 节 “DNS 服务软件要求”
- 第 2.3 节 “为 DNS 服务配置现有的 BIND 服务器”
- 第 2.4 节 “推荐的 DNS 服务拓扑”
- 第 2.5 节 “关于 DNS 服务高可用性”

2.1. DNS 服务器功能支持列表

下表列出了 Red Hat OpenStack Platform (RHOSP) 17 支持的 DNS 服务（指定）中的功能。

表 2.1. DNS 服务（指定）功能支持列表

功能	RHOSP 17 支持？
x86_64 硬件架构	是
所有其他硬件架构	否
BIND 9 后端	是
所有其他后端	否
Denylists (blacklists)	是
指定 v1 API	否
指定 v2 API	是
指定管理 API	否
指定中央服务	是
指定 Producer 服务	是
指定 Worker 服务	是
指定 miniDNS 服务	是
指定代理服务	否

指定区管理器服务	否
指定池管理器服务	否
指定 OpenStack 客户端插件(CLI)	是
指定客户端(CLI)	否
OpenStack Python SDK （指定）	是
指定客户端(SDK)	否
指定 horizon 仪表板	是
指定 tempest 插件	是
指定数据库 MariaDB/Galera	是
所有其他数据库	否
分布式锁定管理器(Redis)	是
所有其他分布式锁定管理器选项	否
指定 sink	否
指定通知	是
高可用性部署	是
IPv4	是
IPv6	是
Monasca 集成	否
默认池调度程序	是
所有其他池调度程序	否
单个池	是
多个池	否
配额	是
基于角色的访问控制 (RBAC)	是

记录类型 A	是
记录类型 AAAA	是
记录类型 CNAME	是
记录类型 MX	是
记录类型 SRV	是
记录类型 TXT	是
记录类型 SPF	是
记录类型 NS	是
记录类型 PTR	是
记录类型 SSHFP	是
记录类型 SOA	是
记录类型 NAPTR	是
记录类型 CAA	是
所有其他记录类型	否
顶级域(TLD)	是
TSIG 密钥	是
unbound 递归解析器	是
所有其他递归解析器	否
主区域	是
二级区	否
zone 导入和导出	是
zone abandon	否
区域所有权传输	是

2.2. DNS 服务软件要求

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)依赖于以下 RHOSP 核心组件：

- Identity 服务 (keystone)
- RabbitMQ
- MariaDB
- Redis

RHOSP 安装和配置工具集 director 会自动为 DNS 服务配置这些组件。

如果您使用 VLAN 或覆盖网络，您希望 DNS 服务自动为其创建 DNS 记录，请为这些网络设置一些网络分段 ID。DNS 服务不会为其分段 ID 在网络服务(neutron) **ml2_conf.ini** 文件中指定的范围内创建 DNS 记录。

其他资源

- 第 2.4 节 “推荐的 DNS 服务拓扑”
- 为 DNS 集成设置项目

2.3. 为 DNS 服务配置现有的 BIND 服务器

如果您要将 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）与现有 BIND 基础架构集成，则必须执行一些操作以确保 BIND 9 正确配置。

重要

该功能在此发行版本中作为*技术预览*提供，因此不享有红帽的全面支持。它只应用于测试，不应部署在生产环境中。有关技术预览功能的更多信息，请参阅覆盖范围详细信息。

注意

如果您没有现有的 BIND 基础架构，RHOSP director 会自动为您配置 BIND。

先决条件

- 您必须是一个有足够权限才能更改 BIND 9 服务器的用户。
- 确保 BIND 可以访问文件 **/etc/rndc.conf** 和 **/etc/rndc.key**。
- 确保 BIND 能够从 RHOSP DNS 服务(designate)接收 **rndc** 实用程序信息。

流程

1. 登录到您的 BIND 9 服务器。
2. 确保 **/etc/rndc.key** 已正确配置。
   rndc-key 必须有一个基于 Hash 的消息身份验证代码(HMAC)、SHA-256 算法和 Base64 编码的 secret：

```
key "rndc-key" {
    algorithm hmac-sha256;
    secret "<base64-encoded string>";
};
```

3. 如果还没有这么做，请启用 BIND，以使用 **rndc** 程序远程创建和删除区域。
在 **/etc/named.conf** 中，在 选项 **{** 下，确认存在以下行。如果没有，创建一个新行并添加它：

```
allow-new-zones yes;
```

4. 如果还没有，将 BIND 配置为发送最小响应。
另外，在 **/etc/named.conf** 中，在 选项 **{** 下，确认存在以下行。如果没有，创建一个新行并添加它：

```
minimal-responses yes;
```

默认情况下，BIND 9 包括区外记录以及它发送到客户端的响应中的附加部分。将 **minimal-responses** 设置为 **yes** 可防止处理区外的额外信息，并删除对 DNS 缓存中毒攻击的影响。

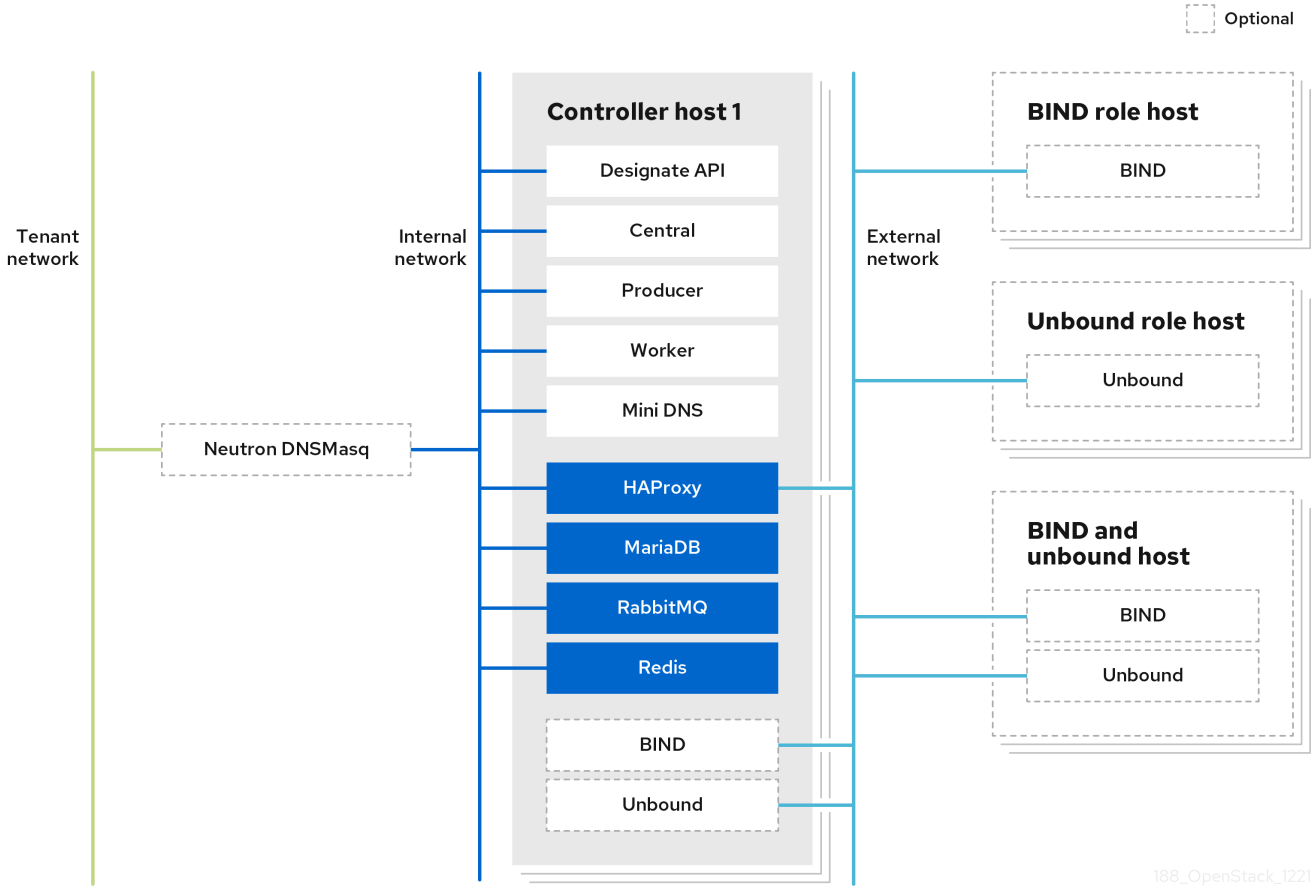
其他资源

- 使用预先存在的 BIND 9 服务器部署 DNS 服务

2.4. 推荐的 DNS 服务拓扑

推荐的拓扑包括在 Red Hat OpenStack Platform (RHOSP) Controller 主机上部署 DNS 服务。如果您的 RHOSP 部署具有高可用性，则至少有三个 RHOSP Controller，各自包含 DNS 服务。

图 2.1. 推荐的 DNS 服务拓扑



在图 2.1 中，DNS 服务组件在其各自的容器中运行。颜色为黑色的容器是 DNS 服务与其他 RHOSP 服务共享的资源。

虚线容器代表 BIND 和 Unbound 的可选放置。如果您的站点具有大量数据流量占用，您可能需要分别使用专用主机来包含 BIND 和 Unbound。

2.5. 关于 DNS 服务高可用性

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)将数据流量和容错的负载平衡整合到称为 *主动-主动高可用性模式的高可用性* 模式中。在主动-主动模式中，DNS 服务在三个或更多个节点上同时运行其组件服务。如果其中一个节点失败，剩余的节点将继续运行，并避免中断和性能下降。DNS 服务会尝试在所有服务实例间负载平衡工作。

DNS 服务组件被归类为使用 RHOSP Controller 角色部署的服务。这意味着，RHOSP 安装和配置工具集 director 会在所有 Controller 主机上自动部署 DNS 服务。因此，如果您在三个或更多不同的主机上部署了三个或更多控制器，则 DNS 服务高度可用。

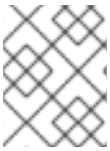
其他资源

- DNS 服务组件

第 3 章 安装和配置 DNS 服务

在部署或重新部署 Red Hat OpenStack Platform (RHOSP)时，您可以通过包含指定环境文件来安装和配置 DNS 服务(designate)。部署 RHOSP 的工具集使用编排服务(heat)环境模板和环境文件，作为有关如何安装和配置 DNS 服务和 RHOSP 部署的其余部分的计划。

在部署 DNS 服务时，director 会自动执行此类操作，如为主动-主动高可用性模式启用 DNS 服务，并激活端口和浮动 IP 地址的自动化。director 还将网络服务(neutron)配置为指向 DNS 服务中包含的 Unbound 解析器。



注意

您可以通过在自定义 heat 环境文件中设置 **UnboundForwardResolvers** 来显式禁用 Unbound 解析器的配置。

您还可以通过为 director 提供所需的 DNS 服务器信息，将 DNS 服务与预先存在的 DNS 基础架构集成。

重要

在 RHOSP 17.1 中，将 DNS 服务与预先存在的 DNS 基础架构集成是一项技术预览功能。

本节中包含的主题有：

- 第 3.1 节 “部署 DNS 服务”
- 第 3.2 节 “使用预先存在的 BIND 9 服务器部署 DNS 服务”
- 第 3.3 节 “更改 DNS 服务默认设置”

3.1. 部署 DNS 服务

您可以使用 Red Hat OpenStack Platform (RHOSP) director 部署 DNS 服务(designate)。director 使用编排服务(heat)模板和环境文件，它们是您的 RHOSP 部署的一组计划。undercloud 导入这些计划，并按照其说明安装和配置 DNS 服务和 RHOSP 部署。

先决条件

- 您必须是有权访问 RHOSP undercloud 的 **stack** 用户。

流程

1. 如果您要将 DNS 服务器与预先存在的 DNS 基础架构集成，请访问 第 3.2 节 “使用预先存在的 BIND 9 服务器部署 DNS 服务”。
2. 以 stack 用户身份登录 undercloud 主机。
3. 提供 undercloud 凭证文件：

```
$ source ~/stackrc
```

4. 创建自定义环境 YAML 文件，其中包含 **DesignateBindNSRecords** 参数的声明，其值为位于 DNS 服务器(designate)池中的子区域的名称服务器记录(NS 记录)：

```
parameter_defaults:
  DesignateBindNSRecords: ['<NS_record_child-zone-1>', '<NS_record_child-zone-2>', '...']
```

示例

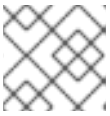
在本例中，DNS 池包含子区域： **ns1.sales.example.org.**、**ns2.sales.example.org.** 和 **ns3.sales.example.org.** 用于父区 **example.org**。

```
parameter_defaults:
  DesignateBindNSRecords: ['ns1.sales.example.org.', 'ns2.sales.example.org.',
'ns3.sales.example.org.']
```

5. 运行部署命令，并包含核心 heat 模板、其他环境文件、**designate.yaml** 环境文件以及包含您的池 NS 记录的文件。

示例

```
$ openstack overcloud deploy --templates \
-e <other_environment_files> \
-e /usr/share/openstack-tripleo-heat-templates/environments/\
services/designate.yaml \
-e /home/stack/my_pool_ns_records.yaml
```



注意

director 在堆栈更新或升级过程中将各种 DNS 服务组件更新至最新的指定镜像。

验证

- 确认已安装 DNS 服务并定义了端点。

```
$ openstack endpoint list -c "Service Name" -c Enabled -c URL
```

输出示例

```
+--------------+---------+-----------------------------------------------+
| Service Name | Enabled | URL                                           |
+--------------+---------+-----------------------------------------------+
| swift        | True    | http://198.51.100.61:8080                     |
| designate    | True    | http://203.0.113.103:9001                     |
| heat-cfn     | True    | http://192.0.2.137:8000/v1                    |
| designate    | True    | http://192.0.2.137:9001                       |
| placement    | True    | http://203.0.113.103:8778/placement           |
| cinderv3     | True    | http://203.0.113.103:8776/v3/%(tenant_id)s    |
| heat         | True    | http://203.0.113.103:8004/v1/%(tenant_id)s    |
| heat-cfn     | True    | http://203.0.113.103:8000/v1                  |
| nova         | True    | http://203.0.113.103:8774/v2.1                |
| heat         | True    | http://192.0.2.137:8004/v1/%(tenant_id)s      |
| glance       | True    | http://203.0.113.103:9292                     |
| heat         | True    | http://203.0.113.103:8004/v1/%(tenant_id)s    |
| glance       | True    | http://203.0.113.103:9292                     |
| neutron      | True    | http://203.0.113.103:9696                     |
| nova         | True    | http://192.0.2.137:8774/v2.1                  |
```

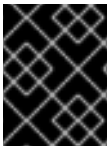
```
| cinderv3     | True    | http://192.0.2.137:8776/v3/%(tenant_id)s        |
| placement    | True    | http://203.0.113.103:8778/placement             |
| keystone     | True    | http://192.168.24.17:35357                      |
| neutron      | True    | http://192.0.2.137:9696                         |
| nova         | True    | http://203.0.113.103:8774/v2.1                  |
| heat-cfn     | True    | http://203.0.113.103:8000/v1                    |
| cinderv3     | True    | http://203.0.113.103:8776/v3/%(tenant_id)s      |
| glance       | True    | http://192.0.2.137:9292                         |
| placement    | True    | http://192.0.2.137:8778/placement               |
| swift        | True    | http://198.51.100.61:8080/v1/AUTH_%(tenant_id)s |
| swift        | True    | http://192.0.2.137:8080/v1/AUTH_%(tenant_id)s   |
| designate    | True    | http://203.0.113.103:9001                       |
| keystone     | True    | http://192.0.2.137:5000                         |
| neutron      | True    | http://203.0.113.103:9696                       |
| keystone     | True    | http://203.0.113.103:5000                       |
+--------------+---------+-------------------------------------------------+
```

其他资源

- *使用 director 安装和管理 Red Hat OpenStack Platform* 指南中的 部署命令选项

3.2. 使用预先存在的 BIND 9 服务器部署 DNS 服务

您可以使用 Red Hat OpenStack Platform (RHOSP) director 来安装和配置 DNS 服务（指定），并将其与预先存在的 BIND 9 DNS 基础架构集成。director 使用编排服务(heat)模板和环境文件，它们是您的 RHOSP 部署的一组计划。您可以将有关 DNS 服务器的具体信息添加到 heat 环境文件中。undercloud 导入这些计划，并按照其说明来安装和配置 RHOSP 和 DNS 服务，并将其与您的 DNS 基础架构集成。



重要

该功能在此发行版本中作为*技术预览*提供，因此不享有红帽的全面支持。它只应用于测试，不应部署在生产环境中。有关技术预览功能的更多信息，请参阅覆盖范围详细信息。

先决条件

- 您有一个已存在的 DNS 基础架构，它依赖于 BIND 9 服务器。
- 确保您的 BIND 9 服务器满足为 DNS 服务 配置现有 BIND 服务器 中描述的配置 。
- 您必须是有权访问 RHOSP undercloud 的 **stack** 用户。

流程

1. 如果您**没有**将 DNS 服务器与预先存在的 DNS 基础架构集成，请访问 第 3.1 节 “部署 DNS 服务”。
2. 以 stack 用户身份登录 undercloud 主机。
3. 提供 undercloud 凭证文件：

```
$ source ~/stackrc
```

4. 创建自定义环境 YAML 文件。

示例

```
$ vi /home/stack/templates/my-designate-environment.yaml
```

5. 您的环境文件必须包含关键字 **parameter_defaults** 和 **DesignateExternalBindServers**。在设计 **ExternalBindServers** 下的新行上，为每个 BIND 9 DNS 服务器添加 IP 地址和 Remote Name Daemon Control (RNDC)密钥。

示例

在本例中，有两个已存在的 BIND 9 服务器，即 **203.0.113.3** 和 **203.0.113.4**，它们分别带有 RNDC 密钥：

```
parameter_defaults:
  DesignateExternalBindServers:
    - host: 203.0.113.3
      rndc_key: "FJOdVqZr5gVXbU9kIagY0IJVDq7CV/mDVb/M7mlLMgY="
    - host; 203.0.113.4
      rndc_key: "QAAACCdIV3KXPJh6U71ImVH0+j4uKRpVV49zVU7A8uvm"
```

6. 为 **DesignateBindNSRecords** 参数添加声明，其值为位于 DNS 服务器(designate)池中的子区域的名称服务器记录(NS 记录)：

```
parameter_defaults:
...
  DesignateBindNSRecords: ['<NS_record_child-zone-1>', '<NS_record_child-zone-2>', '...']
```

示例

在本例中，DNS 池包含子区域：**ns1.sales.example.org.**、**ns2.sales.example.org.** 和 **ns3.sales.example.org.** 用于父区 **example.org。**

```
parameter_defaults:
...
  DesignateBindNSRecords: ['ns1.sales.example.org.', 'ns2.sales.example.org.',
'ns3.sales.example.org.']
```

7. 运行部署命令，并包含核心 heat 模板、其他环境文件、**designate.yaml** 环境文件以及这个新的自定义环境文件。

重要

环境文件的顺序非常重要，因为后续环境文件中定义的参数和资源具有优先权。

示例

```
$ openstack overcloud deploy --templates \
-e <other_environment_files> \
-e /usr/share/openstack-tripleo-heat-templates/environments/\
services/designate.yaml
```

注意

director 在堆栈更新或升级过程中将各种 DNS 服务组件更新至最新的指定镜像。

其他资源

- *使用 director 安装和管理 Red Hat OpenStack Platform* 指南中的 部署命令选项
- *自定义 Red Hat OpenStack Platform 部署* 指南中的环境文件 https://access.redhat.com/documentation/zh-cn/red_hat_openstack_platform/17.1/html/customizing_your_red_hat_openstack_platform_deploy the-overcloud-with-the-orchestration-service#con_environment-files_understanding-heat-templates
- 在自定义 *Red Hat OpenStack Platform 部署* 指南中的 overcloud 创建中包括环境文件

3.3. 更改 DNS 服务默认设置

您可以通过修改 YAML 格式的环境文件并重新部署 RHOSP overcloud，对 Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)进行配置更改。RHOSP director 是一个工具集，它使用编排服务(heat) 模板和环境文件作为配置 DNS 服务的计划。

先决条件

- 您必须是有权访问 RHOSP undercloud 的 **stack** 用户。
- 决定您要修改的 RHOSP DNS 服务参数。
  以下是几个示例：
  - **DesignateRpcResponseTimeout**
    DNS 服务的 RPC 响应超时（以秒为单位）。默认为 60 秒。
  - **DesignateWorkers**
    用于设计服务的 worker 数量。默认值为零(0)，这意味着部署脚本将 RHOSP director 值用于操作系统 worker。

    如需更多信息，*请参阅使用 director 安装和管理 Red Hat OpenStack Platform* 指南中的 确定环境扩展。
  - **DesignateMdnsProxyBasePort**
    MiniDNS 代理端点在外部或公共访问网络上的基本端口。默认端口为 16000。

流程

1. 以 **stack** 用户身份登录 undercloud 主机。
2. 提供 undercloud 凭证文件：

```
$ source ~/stackrc
```

3. 创建自定义 YAML 环境文件。

示例

```
$ vi /home/stack/templates/my-designate-environment.yaml
```

-

您的环境文件必须包含关键字 **parameter_defaults**。将您的参数值对放在 **parameter_defaults** 关键字的后面。

示例

在本例中，RPC 响应超时设置为 120 秒：

```
parameter_defaults:
  DesignateRpcResponseTimeout: '120'
```

4. 运行部署命令，并包含核心 heat 模板、其他环境文件、**designate.yaml** 环境文件以及这个新的自定义环境文件。

重要

环境文件的顺序非常重要，因为后续环境文件中定义的参数和资源具有优先权。

示例

```
$ openstack overcloud deploy --templates \
-e <other_environment_files> \
-e /usr/share/openstack-tripleo-heat-templates/environments/\
services/designate.yaml \
-e /home/stack/templates/my-designate-environment.yaml
```

其他资源

- *Overcloud 参数指南中的 DNS （指定）参数*
- *自定义 Red Hat OpenStack Platform 部署* 指南中的环境文件 https://access.redhat.com/documentation/zh-cn/red_hat_openstack_platform/17.1/html/customizing_your_red_hat_openstack_platform_deploy the-overcloud-with-the-orchestration-service#con_environment-files_understanding-heat-templates
- 在自定义 *Red Hat OpenStack Platform 部署* 指南中的 overcloud 创建中包括环境文件

第 4 章 使用集成的 DNS 服务

Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）与网络服务(neutron)集成，为端口和计算服务(nova)虚拟机实例提供自动记录设置。

云管理员使用 DNS 服务来创建与网络关联的区域。通过使用其云管理员提供的此网络，云用户可以创建虚拟机实例、端口或浮动 IP，DNS 服务会自动创建必要的 DNS 记录。

在 DNS 服务部署安装工具集过程中，RHOSP director 会加载 Networking 服务(neutron)扩展 **dns_domain_ports**。此扩展允许您在 RHOSP 端口、网络和浮动 IP 中添加以下 DNS 属性：

表 4.1. RHOSP 网络和 DNS 服务支持的 DNS 设置

资源	DNS 名称	DNS 域（区）
端口	是	是
网络	否	是
浮动 IP	是	是

注意

对于在网络和浮动 IP 上指定的 DNS 域，浮动 IP 端口上的域优先于网络上设置的域。

重要

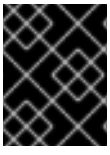
在 Red Hat OpenStack Platform (RHOSP) 17.1 GA 中，提供了一个技术预览，用于在 RHOSP 网络服务(neutron) ML2/OVN 和 RHOSP DNS 服务(designate)之间集成。因此，DNS 服务不会自动为新创建的虚拟机添加 DNS 条目。

本节中包含的主题有：

- 第 4.1 节 “为 DNS 集成设置项目”
- 第 4.2 节 “将虚拟机实例与 DNS 集成”
- 第 4.3 节 “将端口与 DNS 集成”
- 第 4.4 节 “将浮动 IP 与 DNS 集成”

4.1. 为 DNS 集成设置项目

云管理员创建所需的区域、网络和子网，云用户在创建虚拟机实例、端口或浮动 IP 时必须指定它们。因为 RHOSP 网络服务(neutron)与 DNS 服务（指定）集成，所以当云用户创建这些对象时，它们会自动添加到 DNS 服务中。



重要

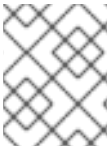
该功能在此发行版本中作为*技术预览*提供，因此不享有红帽的全面支持。它只应用于测试，不应部署在生产环境中。有关技术预览功能的更多信息，请参阅覆盖范围详细信息。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。
- 用于端口和虚拟机的网络无法将属性 **router:external** 设置为 **True**。在创建网络时，必须指定 **--external** 选项。
- 网络必须是以下类型之一：FLAT、VLAN、GRE、VXLAN 或 GENEVE。
- 对于 VLAN、GRE、VXLAN 或 GENEVE 网络，分段 ID 必须在网络服务 **ml2_conf.ini** 文件中配置的范围之外。
  ml2_conf.ini 文件位于 **/var/lib/config-data/puppet-generated/neutron/etc/neutron/plugins/ml2**.+ 中的 Controller 节点主机上，使用下表来确定您的网络分段 ID 范围：

表 4.2. ml2_conf.ini 选项用于设置网络分段 ID

网络类型	节	选项
Geneve	[ml2_type_geneve]	vni_ranges
GRE	[ml2_type_gre]	tunnel_id_ranges
VLAN	[ml2_type_vlan]	network_vlan_ranges
VXLAN	[ml2_type_vxlan]	vni_ranges



注意

如果没有满足这些先决条件，网络服务会使用默认的 **dns_domain** 值(**openstacklocal)在内部解析器中创建一个 DNS 分配。**

流程

1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 创建您希望特定项目中的用户创建 DNS 条目的区域。

   示例

   在本例中，云管理员会创建一个名为 **example.com** 的区域，并指定项目 ID **f75ec24a-d361-ab86-54c0-dfe6093245a3** 中的用户，具有向区添加记录集的权限：

   ```
   $ openstack zone create --email example@example.com example.com. --sudo-project-id
   f75ec24a-d361-ab86-54c0-dfe6093245a3
   ```

注意

DNS 域必须始终是完全限定域名(FQDN)，这意味着它始终以句点结尾。

3. 创建您希望特定项目中的用户创建 DNS 条目的网络。

示例

在本例中，云管理员会创建一个网络 **example-network**，它使用之前创建的区域 **example.com.** 和一个分段 ID **2017**，其位于 ml2_conf.ini 中定义的范围之外：

```
$ openstack network create --dns-domain example.com. \
--provider-segment 2017 --provider-network-type geneve \
example-network
```

4. 在网络上，创建一个子网。

示例

在本例中，云管理员在网络 **example-network** 上创建子网 **example-subnet** ：

```
$ openstack subnet create \
  --allocation-pool start=192.0.2.10,end=192.0.2.200 \
  --network example-network \
  --subnet-range 192.0.2.0/24 \
  example-subnet
```

5. 指示项目中的云用户使用您在添加实例、端口和浮动 IP 时创建的区域和网络。

警告

如果用户创建实例、端口或浮动 IP 没有在区中创建记录集，或者 DNS 服务中不存在该区域，则网络服务执行以下操作：

- 创建带有 **dns_assignment** 字段的端口，使用 **dns_domain** 提供的信息生成。
- 不要在 DNS 服务中创建记录集。
- 记录错误 "Error publish port data in external DNS service"。

验证

- 确认存在您创建的网络。

示例

```
$ openstack network show example-network
```

输出示例

```
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        |                                      |
| created_at                | 2022-09-07T19:03:32Z                 |
| description               |                                      |
| dns_domain                | example.com.                         |
| id                        | 9ae5b3d5-f12c-4a67-b0e5-655d53cd4f7c |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | None                                 |
| is_vlan_transparent       | None                                 |
| mtu                       | 1450                                 |
| name                      | network-example                      |
| port_security_enabled     | True                                 |
| project_id                | f75ec24a-d361-ab86-54c0-dfe6093245a3 |
| provider:network_type     | vxlan                                |
| provider:physical_network | None                                 |
| provider:segmentation_id  | 2017                                 |
| qos_policy_id             | None                                 |
| revision_number           | 3                                    |
| router:external           | Internal                             |
| segments                  | None                                 |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   | 15546c9d-6faf-43aa-83e7-b1e705eed060 |
| tags                      |                                      |
| updated_at                | 2022-09-07T19:03:43Z                 |
+---------------------------+--------------------------------------+
```

其他资源

- *命令行界面参考*中的 zone
- *命令行界面参考*中的 network
- *命令行界面参考*中的subnet

4.2. 将虚拟机实例与 DNS 集成

网络服务(neutron)和 DNS 服务（指定）之间的集成可让您在创建虚拟机实例时自动启用 DNS。

先决条件

- 您的云管理员为您提供了创建启用了 DNS 的实例时要使用的所需网络。

流程

1. 提供您的凭据文件。

   示例

```
$ source ~/overcloudrc
```

2. 使用云管理员提供的网络，创建一个实例。

示例

在本例中，云用户创建一个名为 **my_vm** 的实例：

```
$ openstack server create --image cirros-0.5.2-x86_64-disk --flavor m1.micro --nic net-id=example-network my_vm
```

验证

- 确认您创建的实例的 DNS 服务中存在 记录。

示例

在本例中，DNS 服务会查询 **example.com.** 区域：

```
$ openstack recordset list --type A example.com.
```

输出示例

```
+--------------+--------------------+------+------------+--------+--------+
| id           | name               | type | records    | status | action |
+--------------+--------------------+------+------------+--------+--------+
| 7b8d1be6-1b23 | my_vm.example.com. | A    | 192.0.2.44 | ACTIVE | NONE   |
| -478a-94d5-60 |                    |      |            |        |        |
| b876dca2c8   |                    |      |            |        |        |
+--------------+--------------------+------+------------+--------+--------+
```

其他资源

- *命令行接口参考*中的 server create

4.3. 将端口与 DNS 集成

Networking 服务(neutron)和 DNS 服务（指定）之间的集成可让您在创建端口时自动添加 DNS 记录集。

先决条件

- 在创建启用了 DNS 的端口时，您的云管理员为您提供了要使用的网络。

流程

1. 提供您的凭据文件。

示例

```
$ source ~/overcloudrc
```

2. 使用云管理员提供的区域和网络，创建一个端口。

示例

在本例中，云用户会创建一个端口 **my-port**，其网络(**example-network**)中的 DNS 名称为 **example-port** ：

```
$ openstack port create --network example-network \
--dns-name example-port \
my-port
```

验证

- 确认 DNS 服务中存在您所创建的端口的记录。

示例

在本例中，DNS 服务会查询 **example.com.** 区域：

```
$ openstack recordset list --type A example.com.
```

输出示例

```
+--------------+--------------------------+------+-------------+--------+--------+
| id           | name                     | type | records     | status | action |
+--------------+--------------------------+------+-------------+--------+--------+
| 9ebbe94f-2442 | example-port.example.com. | A    | 192.0.2.149 | ACTIVE | NONE   |
| -4bb8-9cfa-6d |                          |      |             |        |        |
| ca1daba73f    |                          |      |             |        |        |
+--------------+--------------------------+------+-------------+--------+--------+
```

其他资源

- *命令行界面参考*中的 port create

4.4. 将浮动 IP 与 DNS 集成

网络服务(neutron)和 DNS 服务（指定）之间的集成可让您在创建浮动 IP 时自动添加 DNS 记录集。

先决条件

- 您的云管理员为您提供了在创建启用了 DNS 的浮动 IP 时要使用的所需外部网络。

流程

1. 提供您的凭据文件。

示例

```
$ source ~/overcloudrc
```

2. 使用云管理员提供的区域和外部网络，创建一个浮动 IP。

示例

在本例中，云用户在网络(**public**)中创建一个带有 DNS 名称 **example-fip** 的浮动 IP：

```
$ openstack floating ip create --dns-name example-fip \
--dns-domain example.com. \
public
```

验证

- 确认 DNS 服务中存在一条记录，用于您创建的浮动 IP。

  示例

  在本例中，DNS 服务会查询 **example.com.** 区域：

  ```
  $ openstack recordset list --type A example.com.
  ```

  输出示例

  ```
  +--------------+-------------------------+------+-------------+--------+--------+
  | id           | name                    | type | records     | status | action |
  +--------------+-------------------------+------+-------------+--------+--------+
  | e1eca823-169d | example-fip.example.com. | A    | 192.0.2.106 | ACTIVE | NONE   |
  | -4d0a-975e-91 |                         |      |             |        |        |
  | a9907ec0c1    |                         |      |             |        |        |
  +--------------+-------------------------+------+-------------+--------+--------+
  ```

其他资源

- *命令行界面参考中的* floating ip create

第 5 章 管理顶级域名

本节介绍顶级域，并描述了如何在 Red Hat OpenStack Platform DNS 服务（指定）中创建和管理它们。管理允许用户创建哪些域名的方式是通过 denylists。

本节中包含的主题有：

- 第 5.1 节 “关于顶级域”
- 第 5.2 节 “创建顶级域”
- 第 5.3 节 “列出并显示顶级域”
- 第 5.4 节 “修改顶级域”
- 第 5.5 节 “删除顶级域”
- 第 5.6 节 “关于 DNS 服务拒绝列表”
- 第 5.7 节 “关于 denylists 中的 DNS 服务正则表达式”
- 第 5.8 节 “创建 DNS 服务拒绝列表”
- 第 5.9 节 “列出并显示 DNS 服务拒绝列表”
- 第 5.10 节 “修改 DNS 服务拒绝列表”
- 第 5.11 节 “删除 DNS 服务 denylists”

5.1. 关于顶级域

您可以使用顶级域(TLD)来限制用户可以在其下创建区域的域。在域名系统(DNS)术语 *TLD* 是指直接位于 root 下的域集合，如 **.com**。在 Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)中，TLD 可以是任何有效的域。

由于 TLD 定义允许域的集合，因此用户创建的区域必须存在于其中一个 TLD 中。如果在 DNS 服务中没有创建 TLD，则用户可以创建任何区域。TLD 没有允许特权用户在允许的 TLD 之外的区域创建区域的策略。

示例

创建 **.com** TLD 后，如果用户试图创建不包含在 **.com** TLD 中的区域，则尝试会失败。

```
$ openstack zone create --email admin@test.net test.net.
```

输出示例

```
Invalid TLD
```

您可以使用 OpenStack Client **openstack tld** 命令创建、列出、显示、修改和删除 TLD。

其他资源

- *命令行界面参考*中的 tld

- *命令行界面参考*中的 zone

5.2. 创建顶级域

顶级域(TLD)允许您限制用户可以在其下创建区域的域。在 Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)中，TLD 可以是任何有效的域。要创建 TLD，请使用 OpenStack Client **openstack tld create** 命令。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 您可以通过运行 **openstack tld create** 命令创建 TLD。

   示例

   例如，如果需要用户创建以 **.org** 结尾的区域，您可以创建一个 **.org** TLD：

   ```
   $ openstack tld create --name org
   ```

   输出示例

   ```
   +-------------+--------------------------------------+
   | Field       | Value                                |
   +-------------+--------------------------------------+
   | created_at  | 2022-01-10T13:07:33.000000           |
   | description | None                                 |
   | id          | 9fd0a12d-511e-4024-bf76-6ec2e3e71edd |
   | name        | org                                  |
   | updated_at  | None                                 |
   +-------------+--------------------------------------+
   ```

   提示

   使用 **openstack tld 命令**时，请确保输入的完全限定域名(FQDN)没有尾部点，如 **.net**。

验证

- 运行 **openstack tld list** 命令，并确认您的 TLD 存在。

  示例

  ```
  $ openstack tld list --name zone1.cloud.example.com
  ```

其他资源

- *命令行界面参考*中的 tld create

5.3. 列出并显示顶级域

您可以查询 Red Hat OpenStack Platform DNS 服务（指定）数据库并列出所有顶级域(TLD)或显示特定 TLD 的属性。执行此操作的 OpenStack 客户端命令分别是 **openstack tld list** 和 **openstack tld show**。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 使用以下命令列出 DNS 服务数据库中的所有 TLD：

   ```
   $ openstack tld list
   ```

3. 使用 **openstack tld show <TLD_NAME_or_ID** > 命令显示特定 TLD 的属性。

   示例

   ```
   $ openstack tld show org
   ```

其他资源

- *命令行界面参考中的* tld list
- *命令行界面参考中的* tld show

5.4. 修改顶级域

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)可让您更改顶级域(TLD)的各种属性，如其名称。您可以使用 OpenStack Client **openstack tld set** 命令修改 TLD。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

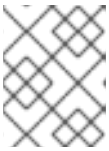
1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 您可以使用以下命令选项以各种方式修改 TLD：

```
openstack tld set [--name NAME] \
                  [--description DESCRIPTION | --no-description] \
                  [TLD_ID | TLD_NAME]
```



注意

之前的语法图不显示 **openstack tld set** 命令的各种格式选项。有关所有命令选项的列表，请参阅"添加资源"中的链接。

在本例中，**openstack tld set** 命令将 **org** TLD 重命名为 **example.net** ：

示例

```
$ openstack tld set org --name example.net
```

输出示例

```
+-------------+--------------------------------------+
| Field       | Value                                |
+-------------+--------------------------------------+
| created_at  | 2022-01-10T13:07:33.000000           |
| description |                                      |
| id          | 9fd0a12d-511e-4024-bf76-6ec2e3e71edd |
| name        | example.net                          |
| updated_at  | 2022-01-10T22:35:20.000000           |
+-------------+--------------------------------------+
```

验证

- 运行 **openstack tld show <TLD_NAME_or_ID** > 命令，并确认您的修改存在。

其他资源

- *命令行界面参考* 中设置的 TLD

5.5. 删除顶级域

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)可让您使用 OpenStack Client **openstack tld delete** 命令删除顶级域(TLD)。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 运行以下命令，获取您要删除的 TLD 的 ID 或名称：

```
$ openstack tld list
```

3. 使用上一步中的名称或 ID，输入以下命令：

```
$ openstack tld delete <TLD_NAME_or_ID>
```

此命令成功时没有输出。

验证

- 运行 openstack **tld show <TLD_NAME_or_ID>** 命令，并验证 TLD 是否已移除。

其他资源

- *命令行界面参考中的* tld delete

5.6. 关于 DNS 服务拒绝列表

Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）有一个 denylist 功能，可让您防止用户创建带有与特定正则表达式匹配的区域。例如，您可以使用 denylist 来防止用户：

- 创建特定区域。
- 创建包含特定字符串的区域。
- 创建特定区的子区。

如果 **example.com.** 是拒绝列表中的成员，一个域或项目用户尝试创建如 **foo.example.com.** 或 **example.com.** 的区，则会遇到错误：

```
$ openstack zone create --email admin@example.com example.com.
Blacklisted zone name
$ openstack zone create --email admin@example.com foo.example.com.
Blacklisted zone name
```

注意

满足 **use_blacklisted_zone** 基于角色的访问控制的用户可以创建具有 denylist 中名称的区域。默认情况下，具有此覆盖的唯一用户是 RHOSP 系统管理员。

您可以使用 OpenStack Client **openstack zone blacklist** 命令创建、列出、显示、修改和删除拒绝列表。

其他资源

- *命令行界面参考中的* zone blacklist create

5.7. 关于 DENYLISTS 中的 DNS 服务正则表达式

在 Red Hat OpenStack Platform DNS 服务（指定）中使用 denylists 的大型部分正在使用正则表达式 (regexes)，这可能很难使用。有关 regex 的 Python 文档可能会作为有用的介绍。在线正则表达式工具可帮助构建和测试用于 denylist API 的正则表达式。

其他资源

- Python 3 文档中的 正则表达式 HOWTO
- 第 5.6 节 "关于 DNS 服务拒绝列表"

5.8. 创建 DNS 服务拒绝列表

Red Hat OpenStack Platform DNS 服务（指定）中的 Denylists 可让您防止用户使用与特定正则表达式匹配的名称创建区域。您可以使用 OpenStack Client **openstack zone blacklist create** 命令创建 denylists。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 使用 **openstack zone blacklist create** 命令创建 denylist。
   在本例中，域 **example.com.** 及其所有子域都添加到 denylist 中。

   示例

   ```
   $ openstack zone blacklist create --pattern ".*example.com."
   ```

   输出示例

   ```
   +-------------+--------------------------------------+
   | Field       | Value                                |
   +-------------+--------------------------------------+
   | created_at  | 2021-10-20T16:15:18.000000           |
   | description | None                                 |
   | id          | 7622e241-8c3d-4c03-a692-8747e3cf2658 |
   | pattern     | .*example.com.                       |
   | updated_at  | None                                 |
   +-------------+--------------------------------------+
   ```

验证

- 运行 **openstack zone blacklist list** 命令，并确认您的 denylist 存在。

其他资源

- *命令行界面参考中的* zone blacklist create
- 第 5.7 节 “关于 denylists 中的 DNS 服务正则表达式”

5.9. 列出并显示 DNS 服务拒绝列表

您可以查询 Red Hat OpenStack Platform DNS 服务（指定）数据库并查看所有拒绝列表，或显示特定 denylist 的属性。执行此操作的 OpenStack 客户端命令是 **openstack zone blacklist list** 和 **openstack zone blacklist show**。

查看所有拒绝列表会很有帮助，因为您必须知道 denylist ID 才能使用其他 denylist 命令。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 使用以下命令列出 DNS 服务数据库中拒绝列表：

   ```
   $ openstack zone blacklist list
   ```

   - 使用上一步中获取的 denylist ID，使用 **openstack zone blacklist show <denylist_ID >** 命令显示特定 denylist 的属性。

     示例

     ```
     $ openstack zone blacklist show 7622e241-8c3d-4c03-a692-8747e3cf2658
     ```

其他资源

- *命令行界面参考中的* 区黑名单列表
- *命令行界面参考中的* 区黑名单显示

5.10. 修改 DNS 服务拒绝列表

Red Hat OpenStack Platform DNS 服务(designate)可让您修改拒绝列表。例如，您可能希望更改 denylist，允许用户创建具有过去限制的特定域名的区域。您可以使用 OpenStack Client **openstack zone blacklist set** 命令修改 denylists。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

1. 作为云管理员，提供您的凭据文件。

   示例

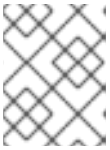
```
$ source ~/overcloudrc
```

2. 运行以下命令，获取您要修改的 denylist 的 ID：

```
$ openstack zone blacklist list
```

3. 您可以使用以下命令选项以各种方式修改 denylist：

```
$ openstack zone blacklist set \
    [--description DESCRIPTION | --no-description] denylist_ID
```



注意

之前的语法图不显示 **openstack zone blacklist set** 命令的各种格式选项。有关所有命令选项的列表，请参阅"添加资源"中的链接。

在本例中，正则表达式(regex)被修改为允许 **web.example.com** 域：

示例

```
$ openstack zone blacklist set 81fbfe02-6bf9-4812-a40e-1522ab6862ca --pattern
".*web.example.com"
```

输出示例

```
+-------------+--------------------------------------+
| Field       | Value                                |
+-------------+--------------------------------------+
| created_at  | 2022-01-08T09:11:43.000000           |
| description | None                                 |
| id          | 81fbfe02-6bf9-4812-a40e-1522ab6862ca |
| pattern     | .*web.example.com                    |
| updated_at  | 2022-01-15T14:26:18.000000           |
+-------------+--------------------------------------+
```

验证

- 运行 **openstack zone blacklist show <denylist_ID** > 命令，并确认您的修改是否存在。

其他资源

- *命令行界面参考* 中设置的区黑名单
- 第 5.7 节 “关于 denylists 中的 DNS 服务正则表达式”

5.11. 删除 DNS 服务 DENYLISTS

Red Hat OpenStack Platform DNS 服务（指定）中的 Denylists 可让您防止用户使用与特定正则表达式匹配的名称创建区域。您可以使用 OpenStack Client **openstack zone blacklist delete** 命令删除拒绝列表。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 运行以下命令，获取您要删除的 denylist 的 ID：

   ```
   $ openstack zone blacklist list
   ```

3. 使用上一步中的 ID，输入以下命令：

   ```
   $ openstack zone blacklist delete <denylist_ID>
   ```

   此命令成功时没有输出。

验证

- 运行 openstack **zone blacklist show <denylist_ID** > 命令，并验证 denylist 已被删除。

其他资源

- *命令行界面参考中的* zone blacklist 删除

第 6 章 查看和管理 DNS 资源的配额

Red Hat OpenStack Platform (RHOSP)提供了一组 DNS 资源配额，云管理员可使用 DNS 服务（指定）进行修改。使用 DNS 配额可帮助您通过设置项目的 DNS 资源限制，从拒绝服务攻击等事件来保护 RHOSP 站点的安全。使用 DNS 配额也可以帮助您跟踪用户的 DNS 资源消耗。云管理员可以设置适用于所有项目的 DNS 配额值，或者根据项目配置一个或多个配额。

本节中包含的主题有：

6.1. 查看 DNS 资源配额

您可以使用 DNS 服务(designate)查看 Red Hat OpenStack Platform (RHOSP)项目的资源配额。

先决条件

- 您必须是您要查看其配额的项目的成员。
- 具有 **admin** 角色的 RHOSP 用户可以查看任何项目的配额。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 查看为项目设置的 DNS 资源配额：

   ```
   $ openstack dns quota list
   ```

   输出示例

   ```
   +-------------------+-------+
   | Field             | Value |
   +-------------------+-------+
   | api_export_size   | 1000  |
   | recordset_records | 20    |
   | zone_records      | 500   |
   | zone_recordsets   | 500   |
   | zones             | 10    |
   +-------------------+-------+
   ```

3. 具有 **admin** 角色的 RHOSP 用户可以查询其他项目的配额：

   a. 获取您要修改其配额的项目的 ID。

请记住该 ID，因为后续步骤需要它。

```
$ openstack project list
```

b. 使用项目 ID，查看为项目设置的 DNS 资源配额。

示例

在本例中，显示项目 ID **ecd4341280d645e5959d32a4b7659da1** 的 DNS 配额：

```
$ openstack dns quota list --project-id ecd4341280d645e5959d32a4b7659da1
```

输出示例

```
+-------------------+-------+
| Field             | Value |
+-------------------+-------+
| api_export_size   | 2500  |
| recordset_records | 25    |
| zone_records      | 750   |
| zone_recordsets   | 750   |
| zones             | 25    |
+-------------------+-------+
```

其他资源

- *命令行界面参考中的*DNS 配额列表

6.2. 修改 DNS 资源配额

您可以使用 DNS 服务(designate)更改 Red Hat OpenStack Platform (RHOSP)项目的 DNS 资源配额。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 获取您要修改其配额的项目的 ID。
   请记住该 ID，因为后续步骤需要它。

   ```
   $ openstack project list
   ```

3. 使用项目 ID，修改项目的 DNS 资源配额。有关可用配额列表，请参阅 第 6.4 节 “DNS 服务配额及其默认值”。

示例

在本例中，**zones** 配额已改变。项目 ID **ecd4341280d645e5959d32a4b7659da1** 的区域总数可以包含 30:

```
$ openstack dns quota set --project-id ecd4341280d645e5959d32a4b7659da1 --zones 30
```

输出示例

```
+-------------------+-------+
| Field             | Value |
+-------------------+-------+
| api_export_size   | 1000  |
| recordset_records | 20    |
| zone_records      | 500   |
| zone_recordsets   | 500   |
| zones             | 30    |
+-------------------+-------+
```

其他资源

- *命令行界面参考*中的 dns quota set
- 第 6.4 节 "DNS 服务配额及其默认值"

6.3. 将 DNS 资源配额重置为默认值

您可以使用 DNS 服务（指定）将 Red Hat OpenStack Platform (RHOSP)项目的 DNS 资源配额重置为默认值。

先决条件

- 您必须是一个具有 **admin** 角色的 RHOSP 用户。

流程

1. 作为云管理员，提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 获取您要重置配额的项目的 ID。
   请记住该 ID，因为后续步骤需要它。

   ```
   $ openstack project list
   ```

3. 使用项目 ID，重置项目的 DNS 资源配额。

   示例

   在本例中，ID 为 **ecd4341280d645e5959d32a4b7659da1** 的项目的配额被重置为默认值：

```
$ openstack dns quota reset --project-id ecd4341280d645e5959d32a4b7659da1
```

成功 **openstack dns quota reset** 命令没有输出。

验证

- 确认已重置了项目的 DNS 资源配额：

  示例

  ```
  $ openstack dns quota list --project-id ecd4341280d645e5959d32a4b7659da1
  ```

  输出示例

  ```
  +-------------------+-------+
  | Field             | Value |
  +-------------------+-------+
  | api_export_size   | 1000  |
  | recordset_records | 20    |
  | zone_records      | 500   |
  | zone_recordsets   | 500   |
  | zones             | 10    |
  +-------------------+-------+
  ```

其他资源

- *命令行界面参考中的*DNS 配额重置
- 第 6.4 节 “DNS 服务配额及其默认值”

6.4. DNS 服务配额及其默认值

Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）有云管理员可以设置的配额来限制所有 RHOSP 项目中的云用户的 DNS 资源消耗。

表 6.1. 区配额

Quota	默认	描述
zones	10	每个项目允许的区域数量。

表 6.2. 记录和记录设置配额

Quota	默认	描述
zone_recordsets	500	每个区允许的记录集数。
zone_records	500	每个区允许的记录数。
recordset_records	20	每个记录集允许的记录数。

表 6.3. zone 导出配额

Quota	默认	描述
api_export_size	1000	区域导出中允许的记录集数。

第 7 章 管理区域

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)使用区将命名空间分成易于管理的内容。用户可以创建、修改、删除、导出和导入区域，只要其 RHOSP 项目拥有该区。

本节中包含的主题有：

7.1. DNS 服务中的区

Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)使用类似的区所有权模型作为 DNS，它有两个主要区别。

例如，在 DNS 中，在根区域（.）中，每个顶级域 (TLD) 如 **.org.** and **.com.** 都有区。在 TLD 区域中，可以委托给其他区域，如 **example.org.** 或 **example.com.** 它们可以由其他机构（或其他名称服务器组）所有和管理。此示例演示了责任层次结构，其中更高级别的区域大部分由委派到低级区域。

与 DNS 类似，使用 RHOSP DNS 服务时，区只能归一个租户所有。但是，与 DNS 不同，DNS 服务不支持租户之间的区域委托。也就是说，租户无法创建父区域归其他租户所有的子区域。

DNS 和 RHOSP DNS 服务之间的第二个区别在于 DNS 服务管理 TLD 与区不同。DNS 服务限制租户创建不在受管 TLD 中的区域。如果 DNS 服务没有管理 TLD，则租户可以创建任何 TLD 和 root 区域以外的任何区域。

7.2. 创建区

zones 可让您更轻松地管理命名空间。默认情况下，任何用户都可以创建 Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)区域。

先决条件

- 您的 RHOSP 项目必须拥有创建子区的区域，或者区必须是允许的 TLD。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

–

2. 通过为区域指定名称和负责该区域的人员的电子邮件地址来创建区域。

示例

```
$ openstack zone create --email dnsprimary@example.com example.com.
```

当您创建区时，DNS 服务会自动创建两个记录集：一个 SOA 记录和 NS 记录。

验证

- 运行 **openstack zone list** 命令确认您的区域已存在。

输出示例

```
+--------------------------------------+-------------+---------+------------+--------+--------+
| id                                   | name        | type    |     serial | status | action |
+--------------------------------------+-------------+---------+------------+--------+--------+
| 14093115-0f0f-497a-ac69-42235e46c26f | example.com. | PRIMARY | 1468421656 |
ACTIVE | NONE   |
+--------------------------------------+-------------+---------+------------+--------+--------+
```

其他资源

- *命令行界面参考*中的 zone create
- *命令行界面参考*中的 zone list

7.3. 更新区

在某些情况下，您必须更新由 Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)管理的区。例如，当您要更改与区域关联的电子邮件地址时，或者您想要更改区域 TTL （生存时间）值时。默认情况下，任何用户都可以修改区。

先决条件

- 您的 RHOSP 项目必须拥有要修改的区。

流程

1. 提供您的凭据文件。

示例

```
$ source ~/overcloudrc
```

2. 通过指定要更改的区域名称和要更改的区属性来修改区：

--email <email_address>

负责区域（所有者）的人员的有效电子邮件地址。

--ttl <seconds>

（实时）持续时间（以秒为单位），即 DNS 客户端- 例如解析器、Web 浏览器，操作系统- 可以在检查检查是否有更新前缓存记录。

--description <string> | --no-description

描述区目的的字符串。

--masters <dns-server> [<dns-server> ...]

DNS 服务器的完全限定域名，即主实例 - 其他 DNS 服务器可以从同步到成为次要服务器的实例。

示例

```
$ openstack zone set example.com. --ttl 3000
```

验证

- 确认您对区域的修改成功。

示例

```
$ openstack zone show example.com.
```

其他资源

- *命令行界面参考*中的 zone set
- *命令行界面参考*中的 zone show

7.4. 删除区

您可以删除由 Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)管理的区域。例如，当区域名称已更改时，您将删除区域。

先决条件

- 您的 RHOSP 项目必须拥有您要删除的区。

流程

1. 提供您的凭据文件。

示例

```
$ source ~/overcloudrc
```

2. 删除区域。

示例

```
$ openstack zone delete example.com.
```

验证

- 运行 **openstack zone list** 命令确认您的区域不再存在。

其他资源

- *命令行界面参考*中的 zone delete
- *命令行界面参考*中的 zone list

7.5. 导出区域

从 Red Hat OpenStack Platform (RHOSP) DNS 服务导出区域数据包括创建 DNS 服务默认在内部存储的区导出资源。例如： **designate://v2/zones/tasks/exports/e75aef2c-b562-4cd9-a426-4a73f6cb82be/export**.创建区导出数据资源后，您可以访问其内容。导出区数据是整个备份策略的一部分，用于保护 RHOSP 部署的 DNS 信息。

先决条件

- 您的 RHOSP 项目必须拥有要从中导出数据的区。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 导出区域。

   示例

   ```
   $ openstack zone export create example.com.
   ```

   输出示例

   ```
   +------------+--------------------------------------+
   | Field      | Value                                |
   +------------+--------------------------------------+
   | created_at | 2022-02-11T02:01:30.000000           |
   | id         | e75aef2c-b562-4cd9-a426-4a73f6cb82be |
   | location   | None                                 |
   | message    | None                                 |
   | project_id | cf5a8f5cc5834d2dacd1d54cd0a354b7     |
   | status     | PENDING                              |
   | updated_at | None                                 |
   | version    | 1                                    |
   | zone_id    | d8f81db6-937b-4388-bfb3-ba620e6c09fb |
   +------------+--------------------------------------+
   ```

   重要

   创建区导出资源后，DNS 服务将继续使用对区域所做的任何更改来更新资源。

3. 记录区域导出 ID (**e75aef2c-b562-4cd9-a426-4a73f6cb82be**)，因为您必须使用它来验证区域导出数据，以及访问区域导出数据。

验证

1. 确认 DNS 服务已成功创建了 zone 导出资源。

示例

```
$ openstack zone export show e75aef2c-b562-4cd9-a426-4a73f6cb82be
```

输出示例

```
+------------+--------------------------------------------------------------------------------+
| Field      | Value                                                                          |
+------------+--------------------------------------------------------------------------------+
| created_at | 2022-02-11T02:01:30.000000                                                     |
| id         | e75aef2c-b562-4cd9-a426-4a73f6cb82be                                           |
| location   | designate://v2/zones/tasks/exports/e75aef2c-b562-4cd9-a426-
4a73f6cb82be/export |
| message    | None                                                                           |
| project_id | cf5a8f5cc5834d2dacd1d54cd0a354b7                                               |
| status     | COMPLETE                                                                       |
| updated_at | 2022-02-11T02:01:30.000000                                                     |
| version    | 2                                                                              |
| zone_id    | d8f81db6-937b-4388-bfb3-ba620e6c09fb                                           |
+------------+--------------------------------------------------------------------------------+
```

zone export create 命令创建 DNS 服务默认在内部存储的资源。

2. 使用您之前获得的区域导出 ID，访问区域导出文件的内容。

提示

使用 **-f value** 选项打印区域文件的内容，而不显示任何 tabulation。您还可以将内容重定向到本地文本文件，如果想要在本地修改导出的区域文件，然后将其导入到 DNS 服务以更新区域，这非常有用。

示例

```
$ openstack zone export showfile e75aef2c-b562-4cd9-a426-4a73f6cb82be -f value
```

输出示例

```
$ORIGIN example.com.
$TTL 3600

example.com.  IN NS ns1.example.com.
example.com.  IN SOA ns1.example.com. admin.example.com. 1624414033 3583 600 86400
3600

www.example.com.  IN A 192.0.2.2
www.example.com.  IN A 192.0.2.1
```

其他资源

- 区文件格式：
  - RFC1034，第 3.6 节
  - RFC1035, 第 5.1 节
- *命令行界面参考中的* zone export create
- *命令行界面参考中的* zone export show
- *命令行界面参考中的* zone export showfile

7.6. 导入区域

将区域数据导入到 Red Hat OpenStack Platform (RHOSP) DNS 服务中包括对符合 DNS 区数据文件格式的文件运行 **openstack zone import** 命令，如从 **openstack zone export showfile** 命令生成的文件。导入数据的一个原因是用户意外删除区。

先决条件

- 您的 RHOSP 项目必须拥有创建子区的区域，或者区必须是允许的 TLD。
- 您要导入的区必须尚不存在。
- 您要导入的区数据必须包含区 TTL （实时）值。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 列出系统中的区：

   ```
   $ openstack zone list
   ```

3. 如果要导入的区域已存在，则必须首先通过运行 **openstack zone delete** 命令删除它。

   示例

   ```
   $ openstack zone delete example.com.
   ```

4. 通过列出系统中的区来确认您的区不再存在：

   ```
   $ openstack zone list
   ```

5. 确认您要导入的区域数据包含区 TTL 值。

   示例

```
$ cat /home/stack/zone_file
```

输出示例

```
$ORIGIN example.com.
$TTL 3000

example.com.  IN NS test.example.com.
example.com.  IN SOA test.example.com. admin.example.com. 1624415706 9000 500 86000
5000
www.example.com.  IN A 192.0.2.2
test.example.com.  IN NS test.example.com.
```

6. 导入有效的区数据文件。

示例

```
$ openstack zone import create /home/stack/zone_file
```

验证

- 确认 DNS 服务已成功导入区域。

示例

```
$ openstack recordset list -c name -c type -c records -c status example.com.
```

输出示例

```
+------------------+------+-------------------------------------------------------------------+--------+
| name             | type | records                                                           | status |
+------------------+------+-------------------------------------------------------------------+--------+
| example.com.     | SOA  | ns1.example.com. admin.example.com. 1624415706 3582 500
86000 3600  | ACTIVE |
| test.example.com. | NS   | test.example.com.                                                 | ACTIVE |
| example.com.     | NS   | ns1.example.com.                                                  | ACTIVE |
| www.example.com.  | A    | 192.0.2.2                                                         | ACTIVE |
+------------------+------+-------------------------------------------------------------------+--------+
```

其他资源

- 区文件格式：
  - RFC1034，第 3.6 节
  - RFC1035, 第 5.1 节
- *命令行界面参考中的* zone import create
- *命令行界面参考*中的 zone list

7.7. 传输区域所有权

您可以将区域的所有权从一个项目传输到另一个项目。例如，财务团队可能希望将 **wow.example.com.** 区域的所有权从其项目传输到销售团队中的项目。

您可以传输区域的所有权，而无需云管理员参与。但是，当前项目区域所有者和接收项目的成员都必须同意转让。

先决条件

- 您的项目必须拥有您要传输的区域。
- 创建转让请求后，接收项目的成员必须接受您要传输的区域。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 获取您要将区域所有权传输到的项目的 ID。

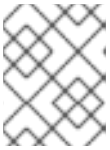
   示例

   ```
   $ openstack project list
   ```

   输出示例

   ```
   +----------------------------------+--------------------+
   | ID                               | Name               |
   +----------------------------------+--------------------+
   | 7af0acba0486472da2447ff55df4a26d | Finance            |
   | 1d12e87fad0d437286c2873b36a12316 | Sales              |
   +----------------------------------+--------------------+
   ```

3. 使用上一步中获取的项目 ID，为您要传输的区域创建一个区域传送请求。

   注意

   在使用目标项目 ID 时，其他项目都不接受区域传送。如果没有提供目标项目 ID，则具有转让请求 ID 及其密钥的任何项目都可以接收区域传送。

   示例

   要将区域 **wow.example.com.** 传送到项目 **1d12e87fad0d437286c2873b36a12316**，您可以运行：

   ```
   $ openstack zone transfer request create --target-project-id
   1d12e87fad0d437286c2873b36a12316 wow.example.com.
   ```

   输出示例

   ```
   +------------------+--------------------------------------------------+
   ```

```
| Field             | Value                                              |
+-------------------+----------------------------------------------------+
| created_at        | 2022-05-26T22:06:39.000000                         |
| description       | None                                               |
| id                | 63cab5e5-65fa-4480-b26c-c16c267c44b2               |
| key               | BIFJIQWH                                           |
| links             | {'self': 'http://127.0.0.1:60053/v2/zones/tasks/tra |
|                   | nsfer_requests/63cab5e5-65fa-4480-b26c-c16c267c44b2 |
|                   | '}                                                 |
| project_id        | 6265985fc493465db6a978b318a01996                   |
| status            | ACTIVE                                             |
| target_project_id | 1d12e87fad0d437286c2873b36a12316                   |
| updated_at        | None                                               |
| zone_id           | 962f08b4-b671-4096-bf24-8908c9d4af0c               |
| zone_name         | wow.example.com.                                   |
+-------------------+----------------------------------------------------+
```

4. 获取区域传送请求 ID 及其密钥。

   示例

   ```
   $ openstack zone transfer request list -c id -c zone_name -c key
   ```

   输出示例

   ```
   +--------------------------------------+-----------------+----------+
   | id                                   | zone_name       | key      |
   +--------------------------------------+-----------------+----------+
   | 63cab5e5-65fa-4480-b26c-c16c267c44b2 | wow.example.com. | BIFJIQWH |
   +--------------------------------------+-----------------+----------+
   ```

5. 将区域传送请求 ID 及其密钥提供给接收项目的成员。

6. 接收项目日志的成员到接收项目，并提供其凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

7. 使用区域传送请求 ID 及其密钥，接受区域传送。

   示例

   ```
   $ openstack zone transfer accept request --transfer-id 63cab5e5-65fa-4480-b26c-
   c16c267c44b2 --key BIFJIQWH
   ```

   输出示例

   ```
   +------------------------+------------------------------------------+
   | Field                  | Value                                    |
   +------------------------+------------------------------------------+
   | created_at             | 2022-05-27T21:37:43.000000               |
   | id                     | a4c4f872-c98c-411b-a787-58ed0e2dce11     |
   ```

```
| key                  | BIFJIQWH                                    |
| links                | {'self': 'http://127.0.0.1:60053/v2/zones/ta |
|                      | sks/transfer_accepts/a4c4f872-c98c-411b-a787 |
|                      | -58ed0e2dce11', 'zone': 'http://127.0.0.1:60 |
|                      | 053/v2/zones/962f08b4-b671-4096-bf24-8908c9d |
|                      | 4af0c'}                                     |
| project_id           | 1d12e87fad0d437286c2873b36a12316            |
| status               | COMPLETE                                    |
| updated_at           | 2022-05-27T21:37:43.000000                  |
| zone_id              | 962f08b4-b671-4096-bf24-8908c9d4af0c        |
| zone_transfer_request_id | 63cab5e5-65fa-4480-b26c-c16c267c44b2    |
+-------------------------+---------------------------------------------+
```

验证

- 使用区域传送接受上一步中的 ID，检查您的区域传送的状态。

  示例

  在本例中，区域状态接受 ID 是 **a4c4f872-c98c-411b-a787-58ed0e2dce11**。

  ```
  $ openstack zone transfer accept show a4c4f872-c98c-411b-a787-58ed0e2dce11
  ```

  输出示例

  ```
  +-------------------------+---------------------------------------------+
  | Field                | Value                                       |
  +-------------------------+---------------------------------------------+
  | created_at           | 2022-05-27T21:37:43.000000                  |
  | id                   | a4c4f872-c98c-411b-a787-58ed0e2dce11        |
  | key                  | None                                        |
  | links                | {'self': 'http://127.0.0.1:60053/v2/zones/ta |
  |                      | sks/transfer_accepts/a4c4f872-c98c-411b-a787 |
  |                      | -58ed0e2dce11', 'zone': 'http://127.0.0.1:60 |
  |                      | 053/v2/zones/962f08b4-b671-4096-bf24-8908c9d |
  |                      | 4af0c'}                                     |
  | project_id           | 1d12e87fad0d437286c2873b36a12316            |
  | status               | COMPLETE                                    |
  | updated_at           | 2022-05-27T21:37:43.000000                  |
  | zone_id              | 962f08b4-b671-4096-bf24-8908c9d4af0c        |
  | zone_transfer_request_id | 63cab5e5-65fa-4480-b26c-c16c267c44b2    |
  +-------------------------+---------------------------------------------+
  ```

其他资源

- *命令行界面参考中的* zone transfer request create
- *命令行界面参考中的* zone transfer accept request

7.8. 修改区传输请求

将区域所有权从一个项目传输到另一个项目的第一步是创建区域传送请求。如果您需要更改或删除区域传送请求，您可以这样做。

先决条件

- 您的项目必须拥有您要修改的传输请求的区域。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 获取您要修改的区域传送请求的 ID。

   示例

   ```
   $ openstack zone transfer request list -c id -c zone_name
   ```

   输出示例

   ```
   +--------------------------------------+------------------+
   | id                                   | zone_name        |
   +--------------------------------------+------------------+
   | 63cab5e5-65fa-4480-b26c-c16c267c44b2 | wow.example.com. |
   +--------------------------------------+------------------+
   ```

3. 使用上一步中获取的区传输请求 ID，您可以更新区域传送请求中的一组有限字段，如描述和目标项目 ID。

   示例

   ```
   $ openstack zone transfer request set --description "wow zone transfer" 63cab5e5-65fa-
   4480-b26c-c16c267c44b2
   ```

   输出示例

   ```
   +--------------------+--------------------------------------------------------+
   | Field              | Value                                                  |
   +--------------------+--------------------------------------------------------+
   | created_at         | 2022-05-26T22:06:39.000000                             |
   | description        | wow zone transfer                                      |
   | id                 | 63cab5e5-65fa-4480-b26c-c16c267c44b2                   |
   | key                | BIFJIQWH                                               |
   | links              | {'self': 'http://127.0.0.1:60053/v2/zones/tasks/tra |
   |                    | nsfer_requests/63cab5e5-65fa-4480-b26c-c16c267c44b2 |
   |                    | '}                                                     |
   | project_id         | 6265985fc493465db6a978b318a01996                       |
   | status             | ACTIVE                                                 |
   | target_project_id  | 1d12e87fad0d437286c2873b36a12316                       |
   | updated_at         | 2022-05-27T20:52:08.000000                             |
   | zone_id            | 962f08b4-b671-4096-bf24-8908c9d4af0c                   |
   | zone_name          | wow.example.com.                                       |
   +--------------------+--------------------------------------------------------+
   ```

4. 使用在第 2 步中获取的区域传送请求 ID，您可以通过删除其区域传送请求来取消待处理的区域传送。

   示例

   ```
   $ openstack zone transfer request delete 63cab5e5-65fa-4480-b26c-c16c267c44b2
   ```

   zone transfer request delete 命令没有输出。运行 **zone transfer request list** 命令来确认区域传送请求已被移除。

其他资源

- 第 7.7 节 “传输区域所有权”
- *命令行界面参考中的* zone transfer request set 命令
- *命令行界面参考中的* zone transfer request delete 命令

第 8 章 管理记录集

Red Hat OpenStack (RHOSP) DNS 服务（指定）在记录集中存储有关区的数据。记录集合由一个或多个 DNS 资源记录组成。除了添加、修改和删除它们外，您还可以查询区来列出其记录集。

本节中包含的主题有：

- 第 8.1 节 “关于 DNS 服务中的记录和记录集”
- 第 8.2 节 “创建记录集”
- 第 8.3 节 “更新记录集”
- 第 8.4 节 “删除记录集”

8.1. 关于 DNS 服务中的记录和记录集

域名系统(DNS)使用资源记录在命名空间内存储区域数据。Red Hat OpenStack (RHOSP) DNS 服务(designate)中的 DNS 记录通过使用记录集进行管理。

每个 DNS 记录都包含以下属性：

- **name** - 指明 DNS 命名空间中位置的字符串。
- **type** - 标识如何使用记录的字母代码集合。例如， **A** 标识地址记录和 **CNAME** 标识规范名称记录。
- **class** - 指定记录命名空间的字母代码集合。通常， 这适用于 互联网，但其他命名空间存在。
- **TTL** - （生存时间）记录有效的持续时间（以秒为单位）。
- **Rdata** - 记录的数据，如 A 记录的 IP 地址或 CNAME 记录的另一个记录名称。

每个区命名空间都必须包含授权起始(SOA)记录，并可具有权威名称服务器(NS)记录和各种其他类型的记录。SOA 记录表明此名称服务器是关于该区域的最佳信息来源。NS 记录标识对区域具有权威的名称服务器。区域的 SOA 和 NS 记录是可读的，但不能修改。

除了所需的 SOA 和 NS 记录外，最常见的三个记录类型是地址(A)、规范名称(CNAME)和指针(PTR)记录。记录将主机名映射到 IP 地址。PTR 记录将 IP 地址映射到主机名。CNAME 记录标识别名的完整主机名。

记录集代表一个或多个具有相同名称和类型的 DNS 记录，但可能存在不同的数据。例如，名为 **web.example.com** 的记录集，类型为 **A**，它包括了数据 **192.0.2.1** 和 **192.0.2.2**，这可能会反映位于这两个 IP 地址的用于托管 **web.example.com** 的两个 Web 服务器。

您必须在区中创建记录集。如果您删除了包含记录集的区，则区中的记录集也会被删除。

考虑使用 **openstack recordset list -c name -c type -c records example.com** 命令查询 **example.com** 区中包括的输出：

```
+-----------------+------+-----------------------------------------+
| name            | type | records                                 |
+-----------------+------+-----------------------------------------+
| example.com.    | SOA  | ns1.example.net. admin.example.com. 16200126 |
|                 |      | 16 3599 600 8640 0 3600                 |
|                 |      |                                         |
```

```
| example.com.     | NS   | ns1.example.net.                          |
|                  |      |                                           |
| web.example.com. | A    | 192.0.2.1                                 |
|                  |      | 192.0.2.2                                 |
|                  |      |                                           |
| www.example.com. | A    | 192.0.2.1                                 |
+------------------+------+-------------------------------------------+
```

在本例中，**example.com.** 区的权威名称服务器是 **ns1.example.net.**，NS 记录。要验证这一点，您可以使用 BIND dig 工具查询 NS 记录的名称服务器：

```
$ dig @ns1.example.net example.com. -t NS +short
ns1.example.net.
```

您还可以验证 A 记录集：

```
$ dig @ns1.example.net web.example.com. +short
192.0.2.2
192.0.2.1
$ dig @ns1.example.net www.example.com. +short
192.0.2.1
```

8.2. 创建记录集

默认情况下，任何用户都可以创建 Red Hat OpenStack Platform DNS 服务(designate)记录集。

先决条件

- 您的项目必须拥有一个要在其中创建记录集的区域。

流程

1. 提供您的凭据文件。

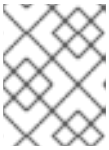
   示例

   ```
   $ source ~/overcloudrc
   ```

2. 您可以使用 **openstack recordset create** 命令创建记录集。记录集需要区域、名称、类型和数据。

   示例

   ```
   $ openstack recordset create --type A --record 192.0.2.1 example.com. www
   ```

   注意

   使用完全限定域名(FQDN)时，需要结尾的点(.)。如果省略尾部点，则区域名称会在生成的记录名称中重复，例如 **www.example.com.example.com。**

在前面的示例中，用户已创建一个名为 **example.com** 的区域。因为记录集名称 **www** 不是 FQDN，所以 DNS 服务会将它添加到区名称中。您可以使用记录设置 name 参数的 FQDN 来达到相同的结果：

```
$ openstack recordset create --type A --record 192.0.2.1 example.com. www.example.com.
```

3. 如果要构建超过字符字符串的最大长度的 TXT 记录集(255 个字符)，那么在创建记录集时，您必须将字符串分成多个更小的字符串。
在本例中，用户通过指定小于 255 个字符的两个字符串，创建一条 410 字符字符串的 TXT 记录集 (**_domainkey.example.com**)：

```
$ openstack recordset create --type TXT --record '"210 characters string" "200 characters string"' example.com. _domainkey
```

4. 您可以多次提供 **--record** 参数，以在记录集中创建多个记录。用于多个 **--record** 参数的典型用途是 round-robin DNS。

示例

```
$ openstack recordset create --type A --record 192.0.2.1 --record 192.0.2.2 example.com. web
```

验证

- 运行 list 命令来验证您创建的记录集是否存在：

示例

```
$ openstack recordset list -c name -c type -c records example.com.
```

输出示例

```
+-----------------+------+---------------------------------------------+
| name            | type | records                                     |
+-----------------+------+---------------------------------------------+
| example.com.    | SOA  | ns1.example.net. admin.example.com 162001261 |
|                 |      | 6 3599 600 86400 3600                       |
|                 |      |                                             |
| example.com.    | NS   | ns1.example.net.                            |
|                 |      |                                             |
| web.example.com. | A    | 192.0.2.1 192.0.2.2                         |
|                 |      |                                             |
| www.example.com. | A    | 192.0.2.1                                   |
+-----------------+------+---------------------------------------------+
```

其他资源

- *命令行界面参考*中的 recordset create
- *命令行界面参考*中的 recordset list
- **dig**的 man page

8.3. 更新记录集

默认情况下，任何用户都可以更新 Red Hat OpenStack Platform DNS 服务(designate)记录集。

先决条件

- 您的项目必须拥有一个区域，在其中更新记录集。

流程

1. 提供您的凭据文件。

   示例

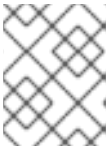
   ```
   $ source ~/overcloudrc
   ```

2. 您可以使用 **openstack recordset set** 命令修改记录集。

   示例

   在本例中，用户正在更新记录集 **web.example.com.** 使其包含两个记录：

   ```
   $ openstack recordset set example.com. web.example.com. --record 192.0.2.5 --record
   192.0.2.6
   ```

   注意

   更新记录集时，您可以通过其 ID 或名称来识别。如果使用其名称，则必须使用完全限定域名(FQDN)。

验证

- 运行 list 命令以确认您的修改。

  示例

  ```
  $ openstack recordset list -c name -c type -c records example.com.
  ```

  输出示例

  ```
  +------------------+------+---------------------------------------------+
  | name             | type | records                                     |
  +------------------+------+---------------------------------------------+
  | example.com.     | SOA  | ns1.example.net. admin.example.com 162001261 |
  |                  |      | 6 3599 600 86400 3600                       |
  |                  |      |                                             |
  | example.com.     | NS   | ns1.example.net.                            |
  |                  |      |                                             |
  | web.example.com. | A    | 192.0.2.5 192.0.2.6                         |
  |                  |      |                                             |
  | www.example.com. | A    | 192.0.2.1                                   |
  +------------------+------+---------------------------------------------+
  ```

其他资源

- *命令行界面参考*中的 recordset create
- *命令行界面参考*中的 recordset list

8.4. 删除记录集

默认情况下，任何用户都可以删除 Red Hat OpenStack Platform DNS 服务(designate)记录集。

先决条件

- 您的项目必须拥有一个区域，您要在其中删除记录集。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 您可以使用 **openstack recordset delete** 命令删除记录集。

   示例

   在本例中，用户从 example. **com. 区域中删除记录集 web.** example.com.：

   ```
   $ openstack recordset delete example.com. web.example.com.
   ```

验证

- 运行 list 命令以确认您的删除。

  示例

  ```
  $ openstack recordset list -c name -c type -c records example.com.
  ```

  输出示例

  ```
  +-----------------+------+---------------------------------------+
  | name            | type | records                               |
  +-----------------+------+---------------------------------------+
  | example.com.    | SOA  | ns1.example.net. admin.example.com 162001261 |
  |                 |      | 6 3599 600 86400 3600                 |
  |                 |      |                                       |
  | example.com.    | NS   | ns1.example.net.                      |
  |                 |      |                                       |
  | www.example.com. | A    | 192.0.2.1                             |
  +-----------------+------+---------------------------------------+
  ```

其他资源

- *命令行界面参考*中的 recordset delete
- *命令行界面参考*中的 recordset list

第 9 章 管理指针记录(PTR)

配置 Red Hat OpenStack Platform (RHOSP) DNS 服务(designate)的步骤是设置 IP 地址到域-name-lookups，也称为反向查找。DNS 资源指针(PTR)记录包含地址到名称映射数据，并存储在反向查找区中。DNS 服务还允许您管理浮动 IP 地址的反向查找。

本节中包含的主题有：

9.1. PTR 记录基础

在 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）中，您可以使用指针(PTR)记录从单个 IP 或一组 IP 地址到完全限定域名(FQDN)创建编号到名称映射（反向映射）。因为域名系统(DNS)将地址查找为名称，所以您可以创建一个包含 IP 地址名称的 PTR 记录。您按照特定惯例形成此名称：反向 IP 地址并附加一个特殊字符串： **in-addr.arpa** 用于 IPv4 地址， **ip6.arpa** 用于 IPv6 地址。

例如，如果 **my-server.example.com** 的 IP 地址为 **198.51.100.42**，则您在反向查找区域中为对应的节点命名 **42.100.51.198.in-addr.arpa**。IP 地址的名称向后列出有助于其查找，因为像标准完全限定域名(FQDN)一样，反向 IP 地址会变得不太具体，因为当您从左侧向右边移动时，反向 IP 地址会较低。

DNS 服务将 PTR 记录的内容写入名为反向查找区的特殊区域，其唯一用途是提供地址到名称查找。因为 PTR 记录包含与标准 FQDN 类似的数据，所以您可以像委派其他区一样委托反向查找区域的子区域。在前面的示例中，hosts **198.51.100.42** 是在 **198.in-addr.arpa** 区域中的节点，此区域可以委派给网络的管理员 **198.51.100.0/8**。

DNS 服务管理浮动 IP 地址的 PTR 记录与标准 IP 地址不同，因为要求用户的 RHOSP 项目拥有包含 IP 地址的区域。在涉及反向名称查找的大多数用例中，可以轻松地满足此要求。在管理标准 IP 地址的反向查找时，您可以在管理其他 DNS 资源记录类型时使用 **openstack recordset** 命令。

但是，在使用浮动 IP 地址时，多个项目通常共享浮动 IP 地址池。要解决地址池的项目所有权问题，您必须在管理浮动 IP 的反向查找时使用不同的命令，即 **openstack ptr record** 命令。

其他资源

- 第 9.3 节 “创建 PTR 记录”
- 第 9.5 节 “为浮动 IP 地址设置 PTR 记录”

9.2. 创建反向查找区域

要正确配置 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定），您必须有一个反向查找区。反向查找区域包含执行地址到名称查找所需的 PTR 记录。您必须按照以下惯例命名反向查找区域：< **backward_IP_address>.in-addr.arpa** 用于 IPv4 地址，< **backward_IP_address>.ip6.arpa** 用于 IPv6 地址。

通常，您可以将 RHOSP 部署中的区与子网计划保持一致。例如，如果您有一个外部网络的 /24 子网，您可以创建一个 /24 子网反向查找区域来包含您的 PTR 记录。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 使用 **openstack zone create** 命令并指定这些所需参数，创建反向查找区域：

   --email <email_address>

   负责区域（所有者）的人员的有效电子邮件地址。

   <name>

   符合惯例的反向查找区的名称：< **backward_IP_address>.in-addr.arpa** 用于 IPv4 地址，< **backward_IP_address>.ip6.arpa** 用于 IPv6 地址。

   示例

   在这个示例中，反向查找区是为 198.51.100.42 地址的一个 PTR 记录设计的：

   ```
   $ openstack zone create --email admin@example.com \
     42.100.51.198.in-addr.arpa.
   ```

   输出示例

   ```
   +----------------+----------------------------------------+
   | Field          | Value                                  |
   +----------------+----------------------------------------+
   | action         | CREATE                                 |
   | attributes     |                                        |
   | created_at     | 2022-02-02T17:32:47.000000             |
   | description    | None                                   |
   | email          | admin@example.com                      |
   | id             | f5546034-b27e-4326-bf9d-c53ed879f7fa   |
   | masters        |                                        |
   | name           | 42.100.51.198.in-addr.arpa.            |
   | pool_id        | 794ccc2c-d751-44fe-b57f-8894c9f5c842   |
   | project_id     | 123d51544df443e790b8e95cce52c285       |
   | serial         | 1591119166                             |
   | status         | PENDING                                |
   | transferred_at | None                                   |
   | ttl            | 3600                                   |
   | type           | PRIMARY                                |
   | updated_at     | None                                   |
   | version        | 1                                      |
   +----------------+----------------------------------------+
   ```

   示例

   在 198.51.100.0/24 子网的反向区的另一个示例中，您可以创建区：

```
$ openstack zone create --email admin@example.com \
  100.51.198.in-addr.arpa.
```

输出示例

```
+----------------+----------------------------------------+
| Field          | Value                                  |
+----------------+----------------------------------------+
| action         | CREATE                                 |
| attributes     |                                        |
| created_at     | 2022-02-02T17:40:23.000000             |
| description    | None                                   |
| email          | admin@example.com                      |
| id             | 5669caad86a04256994cdf755df4d3c1       |
| masters        |                                        |
| name           | 100.51.198.in-addr.arpa.               |
| pool_id        | 794ccc2c-d751-44fe-b57f-8894c9f5c842   |
| project_id     | 123d51544df443e790b8e95cce52c285       |
| serial         | 1739276248                             |
| status         | PENDING                                |
| transferred_at | None                                   |
| ttl            | 3600                                   |
| type           | PRIMARY                                |
| updated_at     | None                                   |
| version        | 1                                      |
+----------------+----------------------------------------+
```

验证

1. 确认您创建的反向查找区已存在：

```
$ openstack zone list -c id -c name -c status
```

输出示例

```
+--------------------------------------+---------------------------+--------+
| id                                   | name                      | status |
+--------------------------------------+---------------------------+--------+
| f5546034-b27e-4326-bf9d-c53ed879f7fa | 42.100.51.198.in-addr.arpa. | ACTIVE |
+--------------------------------------+---------------------------+--------+
```

2. 要完成 address-to-name 映射，forward zone- 包含 IP 地址 的区域必须存在。如果 forward 区域不存在，请立即创建。

其他资源

- 创建区
- *命令行界面参考*中的 zone create

9.3. 创建 PTR 记录

在 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）中，您可以创建 PTR 记录来启用反向查找（地址到名称映射）。启用反向查找是在 RHOSP 部署中正确配置 DNS 服务的一部分。

先决条件

- 您的 RHOSP 项目必须拥有创建 PTR 记录的区域。
- 用于存储 PTR 记录的反向查找区域。更多信息请参阅 第 9.2 节 “创建反向查找区域”。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 使用 **openstack recordset create** 命令并指定这些所需参数来创建 PTR 记录：

   --record <domain_name>

   在执行反向查找时应返回的目标（域名）。

   --type PTR

   您要创建的记录类型 **PTR**。

   <zone_name>

   区域的名称，即记录的反向查找区域。

   <record_name>

   PTR 记录的名称。
   记录名称必须与 <zone_name> 匹配，或者是区的成员。例如，对于反向查找区 **100.51.198.in-addr.arpa.**，它们是有效的 PTR 记录名称：**1.100.51.198.in-addr.arpa.**, **2.100.51.198.in-addr.arpa.**, 以及任何在 **198.51.100.0/24** 子网中的其他反向 IP 地址。

   示例

   ```
   openstack recordset create --record www.example.com. --type PTR \
   42.100.51.198.in-addr.arpa. 42.100.51.198.in-addr.arpa.
   ```

   输出示例

   ```
   +-------------+--------------------------------------+
   | Field       | Value                                |
   +-------------+--------------------------------------+
   | action      | CREATE                               |
   | created_at  | 2022-02-02T19:55:50.000000           |
   | description | None                                 |
   | id          | ca604f72-83e6-421f-bf1c-bb4dc1df994a |
   | name        | 42.100.51.198.in-addr.arpa.          |
   | project_id  | 123d51544df443e790b8e95cce52c285     |
   | records     | www.example.com.                     |
   | status      | PENDING                              |
   | ttl         | 3600                                 |
   | type        | PTR                                  |
   | updated_at  | None                                 |
   ```

```
| version     | 1                                    |
| zone_id     | f5546034-b27e-4326-bf9d-c53ed879f7fa |
| zone_name   | 42.100.51.198.in-addr.arpa.          |
+-------------+--------------------------------------+
```

验证

- 执行反向查找，以确认 IP 地址(**198.51.100.42**)已映射到域名(**www.example.com**)。

  示例

  在本例中，**203.0.113.5** 是部署中的一个 DNS 服务器：

  ```
  $ dig @203.0.113.5 -x 198.51.100.42 +short
  ```

  输出示例

  ```
  www.example.com.
  ```

其他资源

- *命令行界面参考*中的 recordset create
- **dig** 命令 man page.

9.4. 创建多个 PTR 记录

在 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）中，您可以使用更广泛定义的反向查找区将多个 PTR 记录添加到较大的子网中。

先决条件

- 您的 RHOSP 项目必须拥有创建 PTR 记录的区域。
- 用于存储更广泛定义的 PTR 记录的反向查找区域。例如，**198.51.100.0/24** 反向查找区域 **100.51.198.in-addr-arpa**。更多信息请参阅 第 9.2 节 “创建反向查找区域”。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 使用 **openstack recordset create** 命令创建 PTR 记录，并指定这些所需参数：

   --record <domain_name>
   查找的域名。

   --type PTR
   您要创建的记录类型 **PTR**。

<zone_name>

记录所在的反向查找区域的名称。

<record_name>

PTR 记录的名称。
记录名称必须与 <zone_name> 匹配，或者是区的成员。例如，对于反向查找区 **100.51.198.in-addr.arpa.**，它们是有效的 PTR 记录名称：**1.100.51.198.in-addr.arpa.**, **2.100.51.198.in-addr.arpa.**, 以及任何在 **198.51.100.0/24** 子网中的其他反向 IP 地址。

示例

在本例中，反向查找区域更为广泛定义，例如 **100.51.198.0/24** 反向查找区域 **100.51.198.in-addr-arpa** ：

```
$ openstack recordset create --record cats.example.com. --type PTR \
--ttl 3600 100.51.198.in-addr.arpa. 3.100.51.198.in-addr.arpa.
```

输出示例

```
+-------------+--------------------------------------+
| Field       | Value                                |
+-------------+--------------------------------------+
| action      | CREATE                               |
| created_at  | 2022-02-02T20:10:54.000000           |
| description | None                                 |
| id          | c843729b-7aaf-4f99-a40a-d9bf70edf271 |
| name        | 3.100.51.198.in-addr.arpa.           |
| project_id  | 123d51544df443e790b8e95cce52c285     |
| records     | cats.example.com.                    |
| status      | PENDING                              |
| ttl         | 3600                                 |
| type        | PTR                                  |
| updated_at  | None                                 |
| version     | 1                                    |
| zone_id     | e9fd0ced-1d3e-43fa-b9aa-6d4b7a73988d |
| zone_name   | 100.51.198.in-addr.arpa.             |
+-------------+--------------------------------------+
```

验证

1. 执行反向查找，以确认 IP 地址(**198.51.100.3**)已映射到域名(**cats.example.com**)。

   示例

   在本例中，**203.0.113.5** 是部署中的一个 DNS 服务器：

   ```
   $ dig @203.0.113.5 -x 198.51.100.3 +short
   ```

   输出示例

   ```
   cats.example.com.
   ```

2. 执行反向查找，以确认任何其他 IP 地址(**198.51.100.0/24**)已映射到域名(**example.com**)。

示例

在本例中，**203.0.113.5** 是部署中的一个 DNS 服务器：

```
$ dig @203.0.113.5 -x 198.51.100.10 +short
```

输出示例

```
example.com.
```

其他资源

- *命令行界面参考*中的 recordset create
- **dig** 命令 man page.

9.5. 为浮动 IP 地址设置 PTR 记录

在 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）中，您可以为浮动 IP 地址创建 PTR 记录，以允许反向查找。

先决条件

- 定义的一个或多个浮动 IP。
- 要为您要为其创建 PTR 记录的浮动 IP 的反向查找区域。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 确定您要删除 PTR 记录的浮动 IP 地址的 ID。后续步骤中需要此信息。

   ```
   $ openstack floating ip list -c ID -c "Floating IP Address"
   ```

   输出示例

   ```
   +--------------------------------------+---------------------+
   | ID                                   | Floating IP Address |
   +--------------------------------------+---------------------+
   | 5c02c519-4928-4a38-bd10-c748c200912f | 192.0.2.11          |
   | 89532684-13e1-4af3-bd79-f434c9920cc3 | 192.0.2.12          |
   | ea3ebc6d-a146-47cd-aaa8-35f06e1e8c3d | 192.0.2.13          |
   +--------------------------------------+---------------------+
   ```

3. 确定托管浮动 IP 的 neutron 实例的 RHOSP 区域名称。后续步骤中需要此信息。

   ```
   $ openstack endpoint list -c ID -c Region -c "Service Name"
   ```

输出示例

```
+----------------------------------+-----------+--------------+
| ID                               | Region    | Service Name |
+----------------------------------+-----------+--------------+
| 16526452effd467a915155ceccf79dae | RegionOne | placement    |
| 21bf826a62a14456a61bd8f39648e849 | RegionOne | keystone     |
| 9cb1956999c54001a39d11ea14e037a1 | RegionOne | nova         |
| bdeec4e2665d4605bb89e16a8b1bc50d | RegionOne | glance       |
| ced05a1c03ab44caa1a351ace95429e6 | RegionOne | neutron      |
| e79e3113ea544d039b3a6378e60bdf3f | RegionOne | nova         |
| f91ee44123954b6c82162dcd2d4fc965 | RegionOne | designate    |
+----------------------------------+-----------+--------------+
```

4. 使用 **openstack ptr record set** 命令创建 PTR 记录，并指定这些必要的参数：

<floating_IP_ID>

格式的浮动 IP ID：<region_name>:<floating_IP_ID>。

<ptrd_name>

在执行反向查找时应返回的目标（域名）。

示例

```
$ openstack ptr record set RegionOne:5c02c519-4928-4a38-bd10-c748c200912f
ftp.example.com.
```

输出示例

```
+-------------+-------------------------------------------------+
| Field       | Value                                           |
+-------------+-------------------------------------------------+
| action      | CREATE                                          |
| address     | 192.0.2.11                                      |
| description | None                                            |
| id          | RegionOne:5c02c519-4928-4a38-bd10-c748c200912f |
| ptrdname    | ftp.example.com.                                |
| status      | PENDING                                         |
| ttl         | 3600                                            |
+-------------+-------------------------------------------------+
```

验证

- 执行反向查找，以确认浮动 IP 地址(**192.0.2.11**)已映射到域名(**ftp.example.com**)。

示例

在本例中，**203.0.113.5** 是部署中的一个 DNS 服务器：

```
$ dig @203.0.113.5 -x 192.0.2.11 +short
```

输出示例

```
ftp.example.com.
```

其他资源

- *命令行界面参考*中的ptr record set
- **dig** 命令 man page.

9.6. 取消设置浮动 IP 地址的 PTR 记录

在 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）中，您可以删除与浮动 IP 地址关联的 PTR 记录。

先决条件

- 浮动 IP 的 PTR 记录。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 确定您要删除 PTR 记录的浮动 IP 地址的 ID。后续步骤中需要此信息。

   ```
   $ openstack floating ip list -c ID -c "Floating IP Address"
   ```

   输出示例

   ```
   +--------------------------------------+---------------------+
   | ID                                   | Floating IP Address |
   +--------------------------------------+---------------------+
   | 5c02c519-4928-4a38-bd10-c748c200912f | 192.0.2.11          |
   | 89532684-13e1-4af3-bd79-f434c9920cc3 | 192.0.2.12          |
   | ea3ebc6d-a146-47cd-aaa8-35f06e1e8c3d | 192.0.2.13          |
   +--------------------------------------+---------------------+
   ```

3. 确定 RHOSP 区域的名称。后续步骤中需要此信息。

   ```
   $ openstack endpoint list -c ID -c Region -c "Service Name"
   ```

   输出示例

   ```
   +----------------------------------+-----------+--------------+
   | ID                               | Region    | Service Name |
   +----------------------------------+-----------+--------------+
   | 16526452effd467a915155ceccf79dae | RegionOne | placement    |
   | 21bf826a62a14456a61bd8f39648e849 | RegionOne | keystone     |
   | 9cb1956999c54001a39d11ea14e037a1 | RegionOne | nova         |
   | bdeec4e2665d4605bb89e16a8b1bc50d | RegionOne | glance       |
   ```

```
| ced05a1c03ab44caa1a351ace95429e6 | RegionOne | neutron      |
| e79e3113ea544d039b3a6378e60bdf3f | RegionOne | nova         |
| f91ee44123954b6c82162dcd2d4fc965 | RegionOne | designate    |
+----------------------------------+-----------+--------------+
```

4. 使用 **openstack ptr record unset** 命令删除 PTR 记录，并指定这些必要的参数：

   <floating_IP_ID>

   格式的浮动 IP ID：<region>:<floating_IP_ID>。

   示例

   ```
   $ openstack ptr record unset RegionOne:5c02c519-4928-4a38-bd10-c748c200912f
   ```

验证

- 确认删除了 PTR 记录。

  ```
  $ openstack ptr record list
  ```

其他资源

- *命令行界面参考中的*PTR 记录未设置

第 10 章 对 DNS 服务进行故障排除

通过查看 Red Hat OpenStack Platform DNS 服务（指定）日志并使用一些简单命令，您可以验证该服务是否正常运行。这些操作是对 DNS 服务进行故障排除的第一步。

本节中包含的主题有：

10.1. DNS 服务和 BIND 日志

在对问题进行故障排除时，查看 Red Hat OpenStack Platform DNS 服务（指定）日志非常有用。

DNS 服务日志位于 **/var/log/containers/designate** 中。每个组件服务都有一个日志：

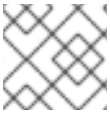
- **central.log**
- **designate-api.log**
- **mdns.log**
- **producer.log**
- **worker.log**

红帽与 RHOSP DNS 服务提供的 BIND 服务器的日志位于 **/var/log/containers/designate/designate-bind** 中：

- **central.log**
- **designate-api.log**

10.2. 导出 DNS 服务池配置

您可以使用 DNS 池配置的副本来对 Red Hat OpenStack Platform (RHOSP) DNS 服务（指定）进行故障排除。



注意

在 RHOSP 17.1 中，不支持多个池。

流程

1. 提供您的凭据文件。

   示例

   ```
   $ source ~/overcloudrc
   ```

2. 您可以从 **designate-central** 容器运行 **designate-manage pool** 命令。首先，获取 control plane 虚拟机实例的 IP 地址。

示例

在本例中，控制器的名称是 **overcloud-controller-0** ：

```
$ CTRL_IP=$(openstack server list -f value -c Networks \
--name overcloud-controller-0 | sed 's/ctlplane=//')
```

3. 登录到其中一个 Controller 节点，并在控制台中显示当前运行的 DNS 服务池配置：

```
$ ssh tripleo-admin@${CTRL_IP} sudo podman exec -i -u root \
designate-central designate-manage pool show_config
```

输出示例

```
Pool Configuration:
--------------------
also_notifies: []
attributes: {}
description: Default Pool
id: 794ccc2c-d751-44fe-b57f-8894c9f5c842
name: default
nameservers:
- host: 192.0.2.111
  port: 53
- host: 192.0.2.109
  port: 53
- host: 192.0.2.131
  port: 53
ns_records:
- hostname: ns2.example.com.
  priority: 2
- hostname: ns1.example.com.
  priority: 1
- hostname: ns3.example.com.
  priority: 3
targets:
- description: BIND9 Server 3
  masters:
  - host: 192.0.2.137
    port: 16002
  - host: 192.0.2.137
    port: 16001
  - host: 192.0.2.137
    port: 16000
  options:
    host: 192.0.2.111
    port: '53'
    rndc_config_file: /etc/designate/private/bind3.conf
    rndc_host: 192.0.2.111
    rndc_port: '953'
  type: bind9
- description: BIND9 Server 2
```

```
  masters:
  - host: 192.0.2.137
    port: 16001
  - host: 192.0.2.137
    port: 16002
  - host: 192.0.2.137
    port: 16000
  options:
    host: 192.0.2.131
    port: '53'
    rndc_config_file: /etc/designate/private/bind2.conf
    rndc_host: 192.0.2.131
    rndc_port: '953'
  type: bind9
- description: BIND9 Server 1
  masters:
  - host: 192.0.2.137
    port: 16002
  - host: 192.0.2.137
    port: 16001
  - host: 192.0.2.137
    port: 16000
  options:
    host: 192.0.2.109
    port: '53'
    rndc_config_file: /etc/designate/private/bind1.conf
    rndc_host: 192.0.2.109
    rndc_port: '953'
  type: bind9
```

4. 如果要将当前池配置导出到文件，请使用 **designate-manage pool generate_file** 命令：

示例

```
$ sudo podman exec -i designate-manage pool generate_file \
--file ~/my_dns_service_config.yaml
```

提示

使用 **podman cp** 命令将文件从容器复制到本地系统。

10.3. 列出可用的 DNS 服务端点

在对问题进行故障排除时，确定 Red Hat OpenStack Platform DNS 服务（指定）端点及其状态很有用。

流程

1. 提供您的凭据文件。

示例

```
$ source ~/overcloudrc
```

2. 列出 RHOSP 服务端点：

```
$ openstack endpoint list -c "Service Name" -c Enabled -c URL
```

输出示例

```
+--------------+---------+-----------------------------------------------+
| Service Name | Enabled | URL                                           |
+--------------+---------+-----------------------------------------------+
| swift        | True    | http://198.51.100.61:8080                     |
| designate    | True    | http://203.0.113.103:9001                     |
| heat-cfn     | True    | http://192.0.2.137:8000/v1                    |
| designate    | True    | http://192.0.2.137:9001                       |
| placement    | True    | http://203.0.113.103:8778/placement           |
| cinderv3     | True    | http://203.0.113.103:8776/v3/%(tenant_id)s    |
| heat         | True    | http://203.0.113.103:8004/v1/%(tenant_id)s    |
| heat-cfn     | True    | http://203.0.113.103:8000/v1                  |
| nova         | True    | http://203.0.113.103:8774/v2.1                |
| heat         | True    | http://192.0.2.137:8004/v1/%(tenant_id)s      |
| glance       | True    | http://203.0.113.103:9292                     |
| heat         | True    | http://203.0.113.103:8004/v1/%(tenant_id)s    |
| glance       | True    | http://203.0.113.103:9292                     |
| neutron      | True    | http://203.0.113.103:9696                     |
| nova         | True    | http://192.0.2.137:8774/v2.1                  |
| cinderv3     | True    | http://192.0.2.137:8776/v3/%(tenant_id)s      |
| placement    | True    | http://203.0.113.103:8778/placement           |
| keystone     | True    | http://192.168.24.17:35357                    |
| neutron      | True    | http://192.0.2.137:9696                       |
| nova         | True    | http://203.0.113.103:8774/v2.1                |
| heat-cfn     | True    | http://203.0.113.103:8000/v1                  |
| cinderv3     | True    | http://203.0.113.103:8776/v3/%(tenant_id)s    |
| glance       | True    | http://192.0.2.137:9292                       |
| placement    | True    | http://192.0.2.137:8778/placement             |
| swift        | True    | http://198.51.100.61:8080/v1/AUTH_%(tenant_id)s |
| swift        | True    | http://192.0.2.137:8080/v1/AUTH_%(tenant_id)s |
| designate    | True    | http://203.0.113.103:9001                     |
| keystone     | True    | http://192.0.2.137:5000                       |
| neutron      | True    | http://203.0.113.103:9696                     |
| keystone     | True    | http://203.0.113.103:5000                     |
+--------------+---------+-----------------------------------------------+
```