Red Hat OpenStack Platform 17.0

将 OpenStack 身份与外部用户管理服务集成

使用 Active Directory 或 Red Hat Identity Management 作为外部身份验证后端

Last Updated: 2024-03-23

Red Hat OpenStack Platform 17.0 将 OpenStack 身份与外部用户管理服务集成

使用 Active Directory 或 Red Hat Identity Management 作为外部身份验证后端

OpenStack Team
rhos-docs@redhat.com

法律通告

摘要

将 OpenStack Identity (keystone)服务与 Microsoft Active Directory 域服务(AD DS)、Red Hat Identity Management (IdM)和 LDAP 集成。

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。

第 1 章 将 OPENSTACK 身份(KEYSTONE)与 ACTIVE DIRECTORY 集成

您可以将 OpenStack Identity (keystone)与 Microsoft Active Directory 域服务(AD DS)集成。Identity Service 验证特定的活动目录域服务(AD DS)用户，但在 Identity Service 数据库中保留授权设置和关键服务帐户。因此，Identity Service 对 AD DS 具有对用户帐户身份验证的只读访问权限，并继续管理分配给经过身份验证的帐户的权限。

通过将 Identity 服务与 AD DS 集成，您可以允许 AD DS 用户向 Red Hat OpenStack Platform (RHOSP)进行身份验证来访问资源。RHOSP 服务帐户（如 Identity Service 和 Image 服务）和授权管理保留在 Identity Service 数据库中。使用 Identity Service 管理工具将权限和角色分配给 AD DS 帐户。

将 OpenStack Identity 与 Active Directory 集成的过程包括以下阶段：

1. 配置 Active Directory 凭证并导出 LDAPS 证书
2. 在 OpenStack 中安装和配置 LDAPS 证书
3. 将 director 配置为使用一个或多个 LDAP 后端
4. 配置 Controller 节点以访问 Active Directory 后端
5. 配置 Active Directory 用户或组对 OpenStack 项目的访问权限
6. 验证域和用户列表是否已正确创建
7. 可选：为非管理员用户创建凭证文件。

1.1. 配置 ACTIVE DIRECTORY 凭证

要将 Active Directory 域服务(AD DS)配置为与 OpenStack 身份集成，请为 Identity 服务设置 LDAP 帐户，为 Red Hat OpenStack 用户创建一个用户组，并导出要在 Red Hat OpenStack Platform 部署中使用的 LDAPS 证书公钥。

先决条件

- Active Directory Domain Services 已配置并运行。
- Red Hat OpenStack Platform 已配置和操作。
- DNS 名称解析功能全面，所有主机都被正确注册。
- AD DS 身份验证流量使用 LDAPS 进行加密，使用端口 636。
- 建议：使用高可用性或负载平衡解决方案实施 AD DS，以避免出现单点故障。

流程

在 Active Directory 服务器上执行这些步骤。

1. 创建 LDAP 查找帐户。Identity Service 使用这个帐户查询 AD DS LDAP 服务：

```
PS C:\> New-ADUser -SamAccountName svc-ldap -Name "svc-ldap" -GivenName LDAP -
Surname Lookups -UserPrincipalName svc-ldap@lab.local  -Enabled $false -
PasswordNeverExpires $true -Path 'OU=labUsers,DC=lab,DC=local'
```

2. 为此帐户设置密码，然后启用它。系统将提示您指定一个符合 AD 域复杂性要求的密码：

```
PS C:\> Set-ADAccountPassword svc-ldap -PassThru | Enable-ADAccount
```

3. 为 RHOSP 用户创建一个名为 **grp-openstack** 的组。只有此组的成员才能在 OpenStack Identity 中分配权限。

```
PS C:\> NEW-ADGroup -name "grp-openstack" -groupscope Global -path
"OU=labUsers,DC=lab,DC=local"
```

4. 创建项目组：

```
PS C:\> NEW-ADGroup -name "grp-openstack-demo" -groupscope Global -path
"OU=labUsers,DC=lab,DC=local"
PS C:\> NEW-ADGroup -name "grp-openstack-admin" -groupscope Global -path
"OU=labUsers,DC=lab,DC=local"
```

5. 将 **svc-ldap** 用户添加到 **grp-openstack** 组中：

```
PS C:\> ADD-ADGroupMember "grp-openstack" -members "svc-ldap"
```

6. 从 AD 域控制器，使用证书 **MMC** 将 LDAPS 证书的公钥（而不是私钥）导出为 DER 编码的 **x509** .cer 文件。将此文件发送到 RHOSP 管理员。

7. 检索 AD DS 域的 NetBIOS 名称。

```
PS C:\> Get-ADDomain | select NetBIOSName
NetBIOSName
-----------
LAB
```

将这个值发送到 RHOSP 管理员。

1.2. 安装 ACTIVE DIRECTORY LDAPS 证书

OpenStack Identity (keystone)使用 LDAPS 查询来验证用户帐户。要加密此流量，keystone 使用 **keystone.conf** 定义的证书文件。要配置 LDAPS 证书，请将从 Active Directory 接收的公钥转换为 **.crt** 格式，并将证书复制到 keystone 可以引用它的位置。

注意

当使用多个域进行 LDAP 身份验证时，您可能会收到各种错误，如 **Unable to retrieve authorized projects，或者 Peer 的证书签发者无法识别**。如果 keystone 对某个域使用不正确的证书，会出现这种情况。作为临时解决方案，将所有 LDAPS 公钥合并到单个 **.crt** 捆绑包中，并将所有 keystone 域配置为使用此文件。

先决条件

- 配置了 Active Directory 凭证。
- LDAPS 证书是从 Active Directory 导出的。

流程

1. 将 LDAPS 公钥复制到运行 OpenStack 身份的节点，并将 **.cer** 转换为 **.crt**。这个示例使用名为 **addc.lab.local.cer** 的源证书文件：

```
# openssl x509 -inform der -in addc.lab.local.cer -out addc.lab.local.crt
# cp addc.lab.local.crt /etc/pki/ca-trust/source/anchors
```

2. 可选：如果您需要运行诊断命令，如 **ldapsearch**，您还需要将证书添加到 RHEL 证书存储中：

   a. 将 **.cer** 转换为 **.pem**。这个示例使用名为 **addc.lab.local.cer** 的源证书文件：

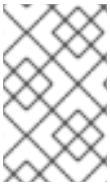
```
# openssl x509 -inform der -in addc.lab.local.cer -out addc.lab.local.pem
```

   b. 在 Controller 节点上安装 **.pem**。例如，在 Red Hat Enterprise Linux 中：

```
# cp addc.lab.local.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust
```

1.3. 配置 DIRECTOR 以使用域特定的 LDAP 后端

要将 director 配置为使用一个或多个 LDAP 后端，请在 heat 模板中将 **KeystoneLDAPDomainEnable** 标志设置为 **true**，并使用每个 LDAP 后端的信息设置环境文件。然后，director 会为每个 keystone 域使用单独的 LDAP 后端。



注意

域配置文件的默认目录设置为 **/etc/keystone/domains/**。您可以使用 **keystone::domain_config_directory** hiera 键设置所需的路径，并将它添加为环境文件中的 **ExtraConfig** 参数来覆盖它。

流程

1. 在部署的 heat 模板中，将 **KeystoneLDAPDomainEnable** 标志设置为 **true**。这会在 **identity** 配置组中的 keystone 中的 **domain_specific_drivers_enabled** 选项。

2. 通过在 **tripleo-heat-templates** 中设置 **KeystoneLDAPBackendConfigs** 参数来添加 LDAP 后端配置的规格，然后您可以指定所需的 LDAP 选项。

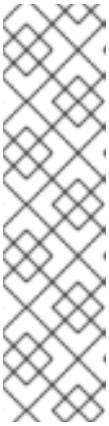
3. 创建 **keystone_domain_specific_ldap_backend.yaml** 环境文件的副本：

```
$ cp /usr/share/openstack-tripleo-heat-
templates/environments/services/keystone_domain_specific_ldap_backend.yaml
/home/stack/templates/
```

4. 编辑 **/home/stack/templates/keystone_domain_specific_ldap_backend.yaml** 环境文件，并设置这些值以适应您的部署。例如，此参数为名为 **testdomain** 的 keystone 域创建 LDAP 配置：

```
parameter_defaults:
  KeystoneLDAPDomainEnable: true
  KeystoneLDAPBackendConfigs:
    testdomain:
      url: ldaps://192.0.2.250
      user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
      password: RedactedComplexPassword
```

```
    suffix: dc=director,dc=example,dc=com
    user_tree_dn: ou=Users,dc=director,dc=example,dc=com
    user_filter: "(memberOf=cn=OSuser,ou=Groups,dc=director,dc=example,dc=com)"
    user_objectclass: person
    user_id_attribute: cn
```



注意

keystone_domain_specific_ldap_backend.yaml 环境文件包含以下已弃用的写入参数：

- **user_allow_create**
- **user_allow_update**
- **user_allow_delete**

这些参数的值对部署没有影响，可以安全地删除。

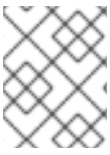
5. 可选：在环境文件中添加更多域。例如：

```
KeystoneLDAPBackendConfigs:
  domain1:
    url: ldaps://domain1.example.com
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
  domain2:
    url: ldaps://domain2.example.com
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
```

这会导致名为 **domain1** 和 **domain2** 的两个域；各自具有不同的 LDAP 域，它们都有自己的配置。

1.4. 授予 ADMIN 用户对 OPENSTACK 身份域的访问权限

要允许 **admin** 用户访问 OpenStack Identity (keystone)域并查看 **Domain** 选项卡，获取域的 ID 和 **admin** 用户，然后将 **admin** 角色分配给域中的用户。



注意

这不会授予 OpenStack admin 帐户对外部服务域的任何权限。在这种情况下，术语 *domain* 指的是 OpenStack 对 keystone 域的使用。

流程

此流程使用 **LAB** 域。使用您要配置的域的实际名称替换域名。

1. 获取 **LAB** 域的 ID：

```
$ openstack domain show LAB
+---------+----------------------------------+
```

```
| Field   | Value                            |
+---------+----------------------------------+
| enabled | True                             |
| id      | 6800b0496429431ab1c4efbb3fe810d4 |
| name    | LAB                              |
+---------+----------------------------------+
```

2. 从 **默认域** 获取 **admin** 用户的 ID：

```
$ openstack user list --domain default | grep admin
| 3d75388d351846c6a880e53b2508172a | admin      |
```

3. 获取 **admin** 角色的 ID：

```
$ openstack role list
```

输出取决于您集成的外部服务：

- Active Directory Domain Service (AD DS)：

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+--------------+
| ID                               | Name         |
+----------------------------------+--------------+
| 544d48aaffde48f1b3c31a52c35f01f9 | SwiftOperator |
| 6d005d783bf0436e882c55c62457d33d | ResellerAdmin |
| 785c70b150ee4c778fe4de088070b4cf | admin        |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_     |
+----------------------------------+--------------+
```

4. 使用 domain 和 admin ID 来构造命令，将 **admin** 用户添加到 keystone **LAB** 域的 **admin** 角色中：

```
# openstack role add --domain 6800b0496429431ab1c4efbb3fe810d4 --user
3d75388d351846c6a880e53b2508172a 785c70b150ee4c778fe4de088070b4cf
```

1.5. 授予外部组对 RED HAT OPENSTACK PLATFORM 项目的访问权限

要授予多个经过身份验证的用户对 Red Hat OpenStack Platform (RHOSP)资源的访问权限，您可以授权外部用户管理服务中的某些组授予 RHOSP 项目的访问权限，而不必要求 OpenStack 管理员手动将每个用户分配到项目中的角色。因此，这些组的所有成员都可以访问预先确定的项目。

先决条件

- 确保外部服务管理员完成以下步骤：
  - 创建名为 **grp-openstack-admin** 的组。
  - 创建名为 **grp-openstack-demo** 的组。
  - 根据需要，将 RHOSP 用户添加到这些组中。
  - 将您的用户添加到 **grp-openstack** 组。
- 创建 OpenStack 身份域。此流程使用 **LAB** 域。
- 创建或选择 RHOSP 项目。这流程使用一个名为 **demo** 的项目，这项目由 **openstack project create --domain default --description "Demo Project" demo** 命令创建。

流程

1. 从 OpenStack 身份域检索用户组列表：

```
# openstack group list --domain LAB
```

命令输出取决于您集成的外部用户管理服务：

- Active Directory Domain Service (AD DS)：

```
+------------------------------------------------------------------+---------------------+
| ID                                                               | Name                |
+------------------------------------------------------------------+---------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-openstack-admin |
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-openstack-demo  |
+------------------------------------------------------------------+---------------------+
```

- Red Hat Identity Manager (IdM):

```
+------------------------------------------------------------------+---------------------+
| ID                                                               | Name                |
+------------------------------------------------------------------+---------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-openstack-admin |
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-openstack-demo  |
+------------------------------------------------------------------+---------------------+
```

2. 检索角色列表：

```
# openstack role list
```

命令输出取决于您集成的外部用户管理服务：

- Active Directory Domain Service (AD DS)：

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+---------------+
```

3. 通过将用户组添加到一个或多个这些角色，来授予用户对 RHOSP 项目的访问权限。例如，如果您希望 **grp-openstack-demo** 组中的用户是 **demo** 项目的普通用户，您必须将该组添加到 **member** 或 **_member_** 角色中，具体取决于您要集成的外部服务：

- Active Directory Domain Service (AD DS)：

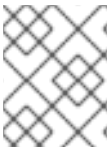
```
# openstack role add --project demo --group
d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8  member
```

- Red Hat Identity Manager (IdM):

```
$ openstack role add --project demo --group
d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8
_member_
```

结果

grp-openstack-demo 的成员可通过输入其用户名和密码并在 **Domain** 字段中输入 **6443** 登录到仪表板：



注意

如果用户收到错误 **Error: Unable to retrieve container list。** 它应该能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 1.6 节 “授予外部用户访问 Red Hat OpenStack Platform 项目”

1.6. 授予外部用户访问 RED HAT OPENSTACK PLATFORM 项目

要从 **grp-openstack** 组中授予特定经过身份验证的用户，您可以向这些用户授予 Red Hat OpenStack Platform (RHOSP)项目的直接访问。如果您要向单个用户授予访问权限，而不是向组授予访问权限，请使用此过程。

先决条件

- 确保外部服务管理员完成以下步骤：
  - 将您的 RHOSP 用户添加到 **grp-openstack** 组中。
  - 创建 OpenStack 身份域.此流程使用 **LAB** 域。
- 创建或选择 RHOSP 项目。这流程使用一个名为 **demo** 的项目，这项目由 **openstack project create --domain default --description "Demo Project" demo** 命令创建。

流程

1. 从 OpenStack 身份域检索用户列表：

```
# openstack user list --domain LAB
 +----------------------------------------------------------------+---------------+
| ID                                                             | Name          |
+----------------------------------------------------------------+---------------+
| 1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e | user1         |
| 12c062faddc5f8b065434d9ff6fce03eb9259537c93b411224588686e9a38bf1 | user2         |
```

```
| afaf48031eb54c3e44e4cb0353f5b612084033ff70f63c22873d181fdae2e73c | user3          |
| e47fc21dcf0d9716d2663766023e2d8dc15a6d9b01453854a898cabb2396826e | user4
|
+------------------------------------------------------------------+----------------+
```

2. 检索角色列表：

```
# openstack role list
```

命令输出取决于您集成的外部用户管理服务：

- Active Directory Domain Service (AD DS)：

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+---------------+
```

3. 通过将他们添加到一个或多个这些角色来授予用户对 RHOSP 项目的访问权限。例如，如果您希望 **user1** 是 **demo** 项目的一个一般用户，您可以将它们添加到**member** 或 **_member_** 角色中（具体取决于您集成的外部服务）。

- Active Directory Domain Service (AD DS)：

```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e member
```

- Red Hat Identity Manager (IdM):

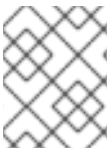
```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e _member_
```

4. 如果您希望 **user1** 是 **demo** 项目的管理用户，请将该用户添加到 **admin** 角色中：

```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e admin
```

结果

user1 用户可以通过输入其外部用户名和密码并在 **Domain** 字段中输入 **LAB** 登录到控制面板：



注意

如果用户收到错误 **Error: Unable to retrieve container list。** 它应该能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 1.5 节 “授予外部组对 Red Hat OpenStack Platform 项目的访问权限”

1.7. 查看 OPENSTACK 身份域和用户列表

使用 **openstack domain list** 命令列出可用条目。在 Identity Service 中配置多个域，可在仪表板登录页面中启用一个新的 **Domain** 字段。用户应输入与其登录凭据匹配的域。

重要

完成集成后，您需要决定是否在 **Default** 域中创建新项目，还是在新创建的 keystone 域中创建新项目。您必须考虑您的工作流以及如何管理用户帐户。如果可能，使用 **Default** 域作为内部域来管理服务帐户和 **admin** 项目，并将外部用户保留在单独的域中。

在本例中，外部帐户需要指定 **LAB** 域。内置的 keystone 帐户（如 **admin**）必须指定 **Default** 作为其域。

流程

1. 显示域列表：

```
# openstack domain list
+----------------------------------+---------+---------+-----------------------------------------------------
--------------+
| ID                               | Name    | Enabled | Description                                         |
+----------------------------------+---------+---------+-----------------------------------------------------
```

```
---------------+
| 6800b0496429431ab1c4efbb3fe810d4 | LAB     | True    |
|
| default                          | Default | True    | Owns users and projects available on Identity API
v2. |
+----------------------------------+---------+---------+-----------------------------------------------------
---------------+
```

2. 显示特定域中的用户列表。这个命令指定了 **--domain** the，并返回属于 **grp-openstack** 组成员的用户，该域中的用户：

```
# openstack user list --domain LAB
```

您还可以附加 **--domain Default** 来显示内置 keystone 帐户：

```
# openstack user list --domain Default
```

1.8. 为非管理员用户创建凭据文件

为 OpenStack 身份配置用户和域后，您可能需要为非管理员用户创建凭据文件。

流程

- 为非管理员用户创建凭证(RC)文件。本例使用文件中的 **user1** 用户。

```
$ cat overcloudrc-v3-user1
# Clear any old environment that may conflict.
for key in $( set | awk '{FS="="}  /^OS_/ {print $1}' ); do unset $key ; done
export OS_USERNAME=user1
export NOVA_VERSION=1.1
export OS_PROJECT_NAME=demo
export OS_PASSWORD=RedactedComplexPassword
export OS_NO_CACHE=True
export COMPUTE_API_VERSION=1.1
export no_proxy=,10.0.0.5,192.168.2.11
export OS_CLOUDNAME=overcloud
export OS_AUTH_URL=https://10.0.0.5:5000/v3
export OS_AUTH_TYPE=password
export PYTHONWARNINGS="ignore:Certificate has no, ignore:A true
SSLContext object is not available"
export OS_IDENTITY_API_VERSION=3
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=LAB
```

1.9. 测试 OPENSTACK IDENTITY 与外部用户管理服务集成

要测试 OpenStack Identity (keystone)是否成功与 Active Directory 域服务(AD DS)集成，请测试用户对仪表板功能的访问权限。

先决条件

- 与外部用户管理服务集成，如 Active Directory (AD)或 Red Hat Identity Manager (IdM)

流程

1. 在外部用户管理服务中创建测试用户，并将用户添加到 **grp-openstack** 组中。
2. 在 Red Hat OpenStack Platform 中，将用户添加到 **demo** 项目的 **_member_** 角色中。
3. 使用 AD 测试用户的凭证登录到控制面板。
4. 单击每个选项卡，以确认它们成功显示且没有错误消息。
5. 使用控制面板构建测试实例。

注意

如果您在这些步骤时遇到问题，请使用 **admin** 帐户登录控制面板，然后以该用户身份执行后续步骤。如果测试成功，这意味着 OpenStack 仍然按预期工作，并且 OpenStack Identity 和 Active Directory 之间的集成设置出现问题。

其他资源

- 第 1.10 节 “Active Directory 集成故障排除”

1.10. ACTIVE DIRECTORY 集成故障排除

如果您在使用 Active Directory 与 OpenStack Identity 集成时遇到问题，您可能需要测试 LDAP 连接或测试证书信任配置。您可能还需要检查 LDAPS 端口是否可以访问。

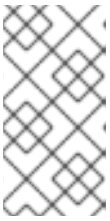
注意

根据错误类型和位置，仅执行此流程中的相关步骤。

流程

1. 使用 **ldapsearch** 命令远程对 Active Directory 域控制器执行测试查询来测试 LDAP 连接。这里有一个成功的结果表示网络连接正在正常工作，AD DS 服务已启动。在本例中，针对服务器 **addc.lab.local** 在端口 **636** 上执行测试查询：

```
# ldapsearch -Z -x -H ldaps://addc.lab.local:636 -D "svc-ldap@lab.local" -W -b
"OU=labUsers,DC=lab,DC=local" -s sub "(cn=*)" cn
```



注意

- **ldapsearch** 是 **openldap-clients** 软件包的一部分。您可以使用 evince **dnf install openldap-clients** 进行安装
- 此命令需要在主机操作系统中找到必要的证书。

2. 如果您在测试 **ldapsearch** 命令时 **无法识别 Peer 的证书签发者** 错误，请确认您的 **TLS_CACERTDIR** 路径设置正确。例如：

```
TLS_CACERTDIR /etc/openldap/certs
```

3. 作为临时解决方案，请考虑禁用证书验证。

重要

不得永久配置此设置。

在 **/etc/openldap/ldap.conf** 中，设置 **TLS_REQCERT** 参数 **以允许** ：

```
TLS_REQCERT allow
```

如果在设置这个值后 **ldapsearch** 查询可以正常工作，您可能需要检查您的证书信任是否正确配置。

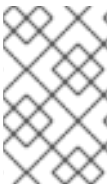
4. 使用 **nc** 命令检查是否远程访问 LDAPS 端口 **636**。在本例中，针对服务器 **addc.lab.local** 执行探测。按 **ctrl-c** 退出提示符。

```
# nc -v addc.lab.local 636
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.200.10:636.
^C
```

如果无法建立连接，这可能表示防火墙配置问题。

第 2 章 将 OPENSTACK 身份(KEYSTONE)与红帽身份管理器(IDM)集成

当您将 OpenStack Identity (keystone)与 Red Hat Identity Manager (IdM)集成时，OpenStack Identity 会验证某些 Red Hat Identity Management (IdM)用户，但在 Identity Service 数据库中保留授权设置和关键服务帐户。因此，Identity Service 对 IdM 具有对 IdM 进行用户帐户身份验证的只读访问权限，同时保留对分配给经过身份验证的帐户的权限的管理。您还可以使用 **novajoin** 将节点注册到 IdM。



注意

此集成的配置文件由 Puppet 管理。因此，您添加的任何自定义配置都会在下次运行 **openstack overcloud deploy** 命令时被覆盖。您可以使用 director 配置 LDAP 身份验证，而不是手动编辑配置文件。

在计划并配置 IdM 集成前，请查看以下关键术语：

- **身份验证** - 使用密码验证用户是否声明的进程。
- **授权** - 验证经过身份验证的用户对试图访问的系统具有适当权限。
- **域** - 请参阅在 Identity Service 中配置的额外后端。例如，可将 Identity Service 配置为从外部 IdM 环境验证用户身份。生成的用户集合可以被视为 *域*。

将 OpenStack 身份与 IdM 集成的过程包括以下阶段：

1. 使用 novajoin 在 IdM 中注册 undercloud 和 overcloud
2. 使用 Ansible 在 undercloud 和 overcloud 中实施 TLS-e
3. 配置 IdM 服务器凭证并导出 LDAPS 证书
4. 在 OpenStack 中安装和配置 LDAPS 证书
5. 将 director 配置为使用一个或多个 LDAP 后端
6. 配置 Controller 节点以访问 IdM 后端
7. 配置 IdM 用户或组对 OpenStack 项目的访问权限
8. 验证域和用户列表是否已正确创建
9. 可选：为非管理员用户创建凭证文件

2.1. 规划 RED HAT IDENTITY MANAGER (IDM)集成

当您计划 OpenStack 身份与红帽身份管理(IdM)集成时，请确保服务都已配置并运行，并查看集成对用户管理和防火墙设置的影响。

先决条件

- 红帽身份管理已配置和操作。
- Red Hat OpenStack Platform 已配置和操作。
- DNS 名称解析功能全面，所有主机都被正确注册。

权限和角色

此集成允许 IdM 用户对 OpenStack 进行身份验证并访问资源。OpenStack 服务帐户（如 keystone 和 glance）和授权管理（权限和角色）将保留在 Identity Service 数据库中。使用 Identity Service 管理工具将权限和角色分配给 IdM 帐户。

高可用性选项

此配置会为单个 IdM 服务器的可用性创建一个依赖项：如果 Identity Service 无法向 IdM 服务器进行身份验证，则项目用户将会受到影响。您可以将 keystone 配置为查询不同的 IdM 服务器，应该不可用，也可以使用负载均衡器。将 IdM 与 SSSD 搭配使用时不要使用负载均衡器，因为此配置已在客户端上实施故障转移。

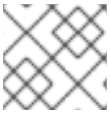
中断要求

- 需要重启 Identity Service 来添加 IdM 后端。
- 在 IdM 中创建帐户之前，用户无法访问控制面板。要减少停机时间，请考虑在此更改前预先执行 IdM 帐户。

防火墙配置

IdM 和 OpenStack 之间的通信包括：

- 验证用户
- IdM 每两小时从控制器检索证书撤销列表(CRL)
- 过期后对新证书的 certmonger 请求



注意

如果初始请求失败，定期 certmonger 任务将继续请求新证书。

如果防火墙在 IdM 和 OpenStack 之间过滤流量，则需要通过以下端口允许访问：

源	目的地	类型	端口
OpenStack Controller 节点	Red Hat Identity Management	LDAPS	TCP 636

2.2. OPENSTACK 的身份管理(IDM)服务器建议

红帽提供了以下信息以帮助您集成 IdM 服务器和 OpenStack 环境。

有关为 IdM 安装准备 Red Hat Enterprise Linux 的详情，请参考 安装身份管理。

运行 **ipa-server-install** 命令来安装和配置 IdM。您可以使用命令参数跳过交互式提示。使用以下建议，以便您的 IdM 服务器可以与您的 Red Hat OpenStack Platform 环境集成：

表 2.1. 参数建议

选项	建议
--admin-password	请注意您提供的值。配置 Red Hat OpenStack Platform 以用于 IdM 时，您将需要此密码。
--ip-address	请注意您提供的值。undercloud 和 overcloud 节点需要网络访问此 ip 地址。
--setup-dns	使用这个选项在 IdM 服务器上安装集成的 DNS 服务。undercloud 和 overcloud 节点使用 IdM 服务器进行域名解析。
--auto-forwarders	使用这个选项使用 **/etc/resolv.conf** 中的地址作为 DNS 转发器。
--auto-reverse	使用这个选项解析 IdM 服务器 IP 地址的反向记录和区域。如果反向记录或区域无法解析，IdM 会创建反向区域。这简化了 IdM 部署。
--ntp-server, **--ntp-pool**	您可以使用这两个选项或其中一个选项来配置 NTP 源。IdM 服务器和 OpenStack 环境必须具有正确的和同步时间。

您必须打开 IdM 所需的防火墙端口，以启用与 Red Hat OpenStack Platform 节点的通信。如需更多信息，请参阅打开 IdM 所需的端口。

其他资源

- 配置和管理身份管理
- Red Hat Identity Management 文档

2.3. 使用 ANSIBLE 实现 TLS-E

您可以使用新的 **tripleo-ipa** 方法在 overcloud 端点上启用 SSL/TLS，在任何位置称为 TLS (TLS-e)。由于所需的证书数量，Red Hat OpenStack Platform 与 Red Hat Identity Management (IdM)集成。当您使用 **tripleo-ipa** 配置 TLS-e 时，IdM 是证书颁发机构。

先决条件

- 确保 undercloud 的所有配置步骤（如创建 stack 用户）已完成。如需了解更多详细信息，请参阅 Director 安装和使用 以了解更多详细信息
- DNS 服务器的 IP 地址在 undercloud 上配置为 IdM 服务器的 IP 地址。**undercloud.conf** 文件中必须配置以下参数之一：
  - **DEFAULT/undercloud_nameservers**
  - **%SUBNET_SECTION%/dns_nameservers**

流程

使用以下步骤在 Red Hat OpenStack Platform 的新安装或您要使用 TLS-e 配置的现有部署中实施 TLS-e。如果在预置备节点中使用 TLS-e 部署 Red Hat OpenStack Platform，则必须使用此方法。

注意

如果您要为现有环境实施 TLS-e，则需要运行命令，如 **openstack undercloud install** 和 **openstack overcloud deploy**。这些过程是幂等的，仅调整现有的部署配置，以匹配更新的模板和配置文件。

1. 配置 **/etc/resolv.conf** 文件：
   在 **/etc/resolv.conf** 中设置 undercloud 上的适当的搜索域和名称服务器。例如，如果部署域是 **example.com**，并且 FreeIPA 服务器的域是 **bigcorp.com**，那么将以下行添加到 /etc/resolv.conf 中：

```
search example.com bigcorp.com
nameserver $IDM_SERVER_IP_ADDR
```

2. 安装所需的软件：

```
sudo dnf install -y python3-ipalib python3-ipaclient krb5-devel
```

3. 使用特定于您的环境的值导出环境变量：

```
export IPA_DOMAIN=bigcorp.com
export IPA_REALM=BIGCORP.COM
export IPA_ADMIN_USER=$IPA_USER (1)
export IPA_ADMIN_PASSWORD=$IPA_PASSWORD (2)
export IPA_SERVER_HOSTNAME=ipa.bigcorp.com
export UNDERCLOUD_FQDN=undercloud.example.com (3)
export USER=stack
export CLOUD_DOMAIN=example.com
```

(1)(2) IdM 用户凭证是一个管理用户，它可以添加新主机和服务。

(3) **UNDERCLOUD_FQDN** 参数的值与 **/etc/hosts** 中的第一个主机名到 IP 地址映射匹配。

4. 在 undercloud 上运行 **undercloud-ipa-install.yaml** ansible playbook：

```
ansible-playbook \
--ssh-extra-args "-o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null" \
/usr/share/ansible/tripleo-playbooks/undercloud-ipa-install.yaml
```

5. 在 undercloud.conf 中添加以下参数

```
undercloud_nameservers = $IDM_SERVER_IP_ADDR
overcloud_domain_name = example.com
```

6. [可选] 如果您的 IPA 域与您的 IPA 域不匹配，请设置 **certmonger_krb_realm** 参数的值：

   a. 在 **/home/stack/hiera_override.yaml** 中设置 **certmonger_krb_realm** 的值：

   -

```
parameter_defaults:
  certmonger_krb_realm = EXAMPLE.COMPANY.COM
```

b. 将 **undercloud.conf** 中的 **custom_env_files** 参数的值设置为 **/home/stack/hiera_override.yaml** ：

```
custom_env_files = /home/stack/hiera_override.yaml
```

7. 部署 undercloud：

```
openstack undercloud install
```

验证

通过完成以下步骤验证 undercloud 是否已正确注册：

1. 列出 IdM 中的主机：

```
$ kinit admin
$ ipa host-find
```

2. 确认 undercloud 上存在 **/etc/novajoin/krb5.keytab**。

```
ls /etc/novajoin/krb5.keytab
```

注意

novajoin 目录名称仅用于传统的命名目的。

在 overcloud 上配置 TLS-e

当您随处使用 TLS 部署 overcloud 时，来自 Undercloud 和 Overcloud 的 IP 地址将自动注册到 IdM。

1. 在部署 overcloud 之前，创建一个 YAML 文件 **tls-parameters.yaml**，其内容类似如下。您选择的值将特定于您的环境：

```
parameter_defaults:
    DnsSearchDomains: ["example.com"]
    CloudDomain: example.com
    CloudName: overcloud.example.com
    CloudNameInternal: overcloud.internalapi.example.com
    CloudNameStorage: overcloud.storage.example.com
    CloudNameStorageManagement: overcloud.storagemgmt.example.com
    CloudNameCtlplane: overcloud.ctlplane.example.com
    IdMServer: freeipa-0.redhat.local
    IdMDomain: redhat.local
    IdMInstallClientPackages: False

resource_registry:
      OS::TripleO::Services::IpaClient: /usr/share/openstack-tripleo-heat-
templates/deployment/ipa/ipaservices-baremetal-ansible.yaml
```

- **OS::TripleO::Services::IpaClient** 参数显示的值会覆盖 **enable-internal-tls.yaml** 文件中的默认设置。您必须确保 **openstack overcloud deploy** 命令中的 **tls-parameters.yaml** 文件遵循 **enable-internal-tls.yaml**。
- 有关用来实现 TLS-e 的参数的更多信息，请参阅 tripleo-ipa 的参数

2. 部署 overcloud。您需要在部署命令中包含 tls-parameters.yaml ：

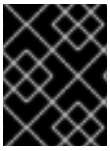
```
DEFAULT_TEMPLATES=/usr/share/openstack-tripleo-heat-templates/
CUSTOM_TEMPLATES=/home/stack/templates

openstack overcloud deploy \
-e ${DEFAULT_TEMPLATES}/environments/ssl/tls-everywhere-endpoints-dns.yaml \
-e ${DEFAULT_TEMPLATES}/environments/services/haproxy-public-tls-certmonger.yaml \
-e ${DEFAULT_TEMPLATES}/environments/ssl/enable-internal-tls.yaml \
-e ${CUSTOM_TEMPLATES}/tls-parameters.yaml \
...
```

3. 通过查询 keystone 获取端点列表来确认每个端点正在使用 HTTPS：

```
openstack endpoint list
```

2.4. 在任何 TLS 下加密 MEMCACHED 流量(TLS-E)



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。

现在，您可以使用 TLS-e 加密 memcached 流量。此功能可用于 novajoin 和 tripleo-ipa ：

1. 创建名为 **memcached.yaml** 的环境文件，其内容如下，以添加对 memcached 的 TLS 支持：

```
parameter_defaults:
  MemcachedTLS: true
  MemcachedPort: 11212
```

2. 在 overcloud 部署过程中包含 **memcached.yaml** 环境文件：

```
openstack overcloud deploy --templates \
-e /usr/share/openstack-tripleo-heat-templates/environments/ssl/enable-internal-tls.yaml \
-e /usr/share/openstack-tripleo-heat-templates/environments/ssl/tls-everywhere-endpoints-dns.yaml \
-e /usr/share/openstack-tripleo-heat-templates/environments/services/haproxy-public-tls-certmonger.yaml \
-e /home/stack/memcached.yaml
...
```

其它资源

- 有关使用 tripleo-ipa 部署 TLSe 的更多信息，请参阅使用 Ansible 实施 TLS-e。

2.5. 配置 RED HAT IDENTITY MANAGER (IDM)服务器凭证

要将 Red Hat Identity Manager (IdM)配置为与 OpenStack 身份集成，请为 Identity 服务设置要使用的 LDAP 帐户，为 Red Hat OpenStack 用户创建一个用户组，并为 lookup 帐户的密码。

先决条件

- Red Hat Identity Manager (IdM)已配置和操作。
- Red Hat OpenStack Platform (RHOSP)已配置和操作。
- DNS 名称解析功能全面，所有主机都被正确注册。
- IdM 身份验证流量使用 LDAPS 加密，使用端口 636。
- 建议：使用高可用性或负载平衡解决方案实施 IdM，以避免出现单点故障。

流程

在 IdM 服务器上执行此步骤。

1. 创建 LDAP 查找帐户，以便在 OpenStack Identity Service 中使用，以查询 IdM LDAP 服务：

```
# kinit admin
# ipa user-add
First name: OpenStack
Last name: LDAP
User  [radministrator]: svc-ldap
```

注意

查看此帐户的密码过期设置，一旦创建。

2. 为 RHOSP 用户创建一个名为 **grp-openstack** 的组。只有此组的成员才能在 OpenStack Identity 中分配权限。

```
# ipa group-add --desc="OpenStack Users" grp-openstack
```

3. 设置 **svc-ldap** 帐户密码并将其添加到 **grp-openstack** 组中：

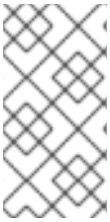
```
# ipa passwd svc-ldap
# ipa group-add-member --users=svc-ldap grp-openstack
```

4. 以 **svc-ldap** 用户身份登录并在提示时更改密码：

```
# kinit svc-ldap
```

2.6. 安装 RED HAT IDENTITY MANAGER (IDM) LDAPS 证书

OpenStack Identity (keystone)使用 LDAPS 查询来验证用户帐户。要加密此流量，keystone 使用 **keystone.conf** 定义的证书文件。要安装 LDAPS 证书，请将证书从 Red Hat Identity Manager (IdM)服务器复制到 keystone 可以引用它的位置，并将证书从 **.crt** 转换为 **.pem** 格式。



注意

当使用多个域进行 LDAP 身份验证时，您可能会收到各种错误，如 **Unable to retrieve authorized projects**，或者 **Peer 的证书签发者无法识别**。如果 keystone 对某个域使用不正确的证书，会出现这种情况。作为临时解决方案，将所有 LDAPS 公钥合并到单个 **.crt** 捆绑包中，并将所有 keystone 域配置为使用此文件。

先决条件

- IdM 服务器凭证已配置。

流程

1. 在您的 IdM 环境中，找到 LDAPS 证书。此文件可以使用 **/etc/openldap/ldap.conf** ：

```
TLS_CACERT /etc/ipa/ca.crt
```

2. 将文件复制到运行 keystone 服务的 Controller 节点。例如， **scp** 命令将 **ca.crt** 文件复制到节点 **node.lab.local** ：

```
# scp /etc/ipa/ca.crt root@node.lab.local:/root/
```

3. 将 **ca.crt** 文件复制到证书目录中。这是 keystone 服务用来访问证书的位置：

```
# cp ca.crt /etc/pki/ca-trust/source/anchors
```

4. 可选：如果您需要运行诊断命令，如 **ldapsearch**，您还需要将证书添加到 RHEL 证书存储中：

   a. 3.在 Controller 节点上，将 **.crt** 转换为 **.pem** 格式：

```
# openssl x509 -in ca.crt -out ca.pem -outform PEM
```

   b. 在 Controller 节点上安装 **.pem**。例如，在 Red Hat Enterprise Linux 中：

```
# cp ca.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust
```

2.7. 配置 DIRECTOR 以使用域特定的 LDAP 后端

要将 director 配置为使用一个或多个 LDAP 后端，请在 heat 模板中将 **KeystoneLDAPDomainEnable** 标志设置为 **true**，并使用每个 LDAP 后端的信息设置环境文件。然后，director 会为每个 keystone 域使用单独的 LDAP 后端。

注意

域配置文件的默认目录设置为 **/etc/keystone/domains/**。您可以使用 **keystone::domain_config_directory** hiera 键设置所需的路径，并将它添加为环境文件中的 **ExtraConfig** 参数来覆盖它。

流程

1. 在部署的 heat 模板中，将 **KeystoneLDAPDomainEnable** 标志设置为 **true**。这会在 **identity** 配置组中的 keystone 中的 **domain_specific_drivers_enabled** 选项。

2. 通过在 **tripleo-heat-templates** 中设置 **KeystoneLDAPBackendConfigs** 参数来添加 LDAP 后端配置的规格，然后您可以指定所需的 LDAP 选项。

3. 创建 **keystone_domain_specific_ldap_backend.yaml** 环境文件的副本：

```
$ cp /usr/share/openstack-tripleo-heat-
templates/environments/services/keystone_domain_specific_ldap_backend.yaml
/home/stack/templates/
```

4. 编辑 **/home/stack/templates/keystone_domain_specific_ldap_backend.yaml** 环境文件，并设置这些值以适应您的部署。例如，此参数为名为 **testdomain** 的 keystone 域创建 LDAP 配置：

```
parameter_defaults:
  KeystoneLDAPDomainEnable: true
  KeystoneLDAPBackendConfigs:
    testdomain:
      url: ldaps://192.0.2.250
      user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
      password: RedactedComplexPassword
      suffix: dc=director,dc=example,dc=com
      user_tree_dn: ou=Users,dc=director,dc=example,dc=com
      user_filter: "(memberOf=cn=OSuser,ou=Groups,dc=director,dc=example,dc=com)"
      user_objectclass: person
      user_id_attribute: cn
```

注意

keystone_domain_specific_ldap_backend.yaml 环境文件包含以下已弃用的写入参数：

- **user_allow_create**
- **user_allow_update**
- **user_allow_delete**

这些参数的值对部署没有影响，可以安全地删除。

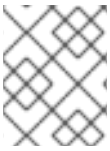
5. 可选：在环境文件中添加更多域。例如：

```
KeystoneLDAPBackendConfigs:
  domain1:
    url: ldaps://domain1.example.com
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
  domain2:
    url: ldaps://domain2.example.com
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
```

这会导致名为 **domain1** 和 **domain2** 的两个域；各自具有不同的 LDAP 域，它们都有自己的配置。

2.8. 授予 ADMIN 用户对 OPENSTACK 身份域的访问权限

要允许 **admin** 用户访问 OpenStack Identity (keystone)域并查看 **Domain** 选项卡，获取域的 ID 和 **admin** 用户，然后将 **admin** 角色分配给域中的用户。



注意

这不会授予 OpenStack admin 帐户对外部服务域的任何权限。在这种情况下，术语 *domain* 指的是 OpenStack 对 keystone 域的使用。

流程

此流程使用 **LAB** 域。使用您要配置的域的实际名称替换域名。

1. 获取 **LAB** 域的 ID：

```
$ openstack domain show LAB
+---------+----------------------------------+
| Field   | Value                            |
+---------+----------------------------------+
| enabled | True                             |
| id      | 6800b0496429431ab1c4efbb3fe810d4 |
| name    | LAB                              |
+---------+----------------------------------+
```

2. 从 **默认域** 获取 **admin** 用户的 ID：

```
$ openstack user list --domain default | grep admin
| 3d75388d351846c6a880e53b2508172a | admin      |
```

3. 获取 **admin** 角色的 ID：

```
$ openstack role list
```

输出取决于您集成的外部服务：

- Active Directory Domain Service (AD DS)：

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+--------------+
| ID                               | Name         |
```

```
+----------------------------------+--------------+
| 544d48aaffde48f1b3c31a52c35f01f9 | SwiftOperator |
| 6d005d783bf0436e882c55c62457d33d | ResellerAdmin |
| 785c70b150ee4c778fe4de088070b4cf | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
+----------------------------------+--------------+
```

4. 使用 domain 和 admin ID 来构造命令，将 **admin** 用户添加到 keystone **LAB** 域的 **admin** 角色中：

```
# openstack role add --domain 6800b0496429431ab1c4efbb3fe810d4 --user
3d75388d351846c6a880e53b2508172a 785c70b150ee4c778fe4de088070b4cf
```

2.9. 授予外部组对 RED HAT OPENSTACK PLATFORM 项目的访问权限

要授予多个经过身份验证的用户对 Red Hat OpenStack Platform (RHOSP)资源的访问权限，您可以授权外部用户管理服务中的某些组授予 RHOSP 项目的访问权限，而不必要求 OpenStack 管理员手动将每个用户分配到项目中的角色。因此，这些组的所有成员都可以访问预先确定的项目。

先决条件

- 确保外部服务管理员完成以下步骤：
  - 创建名为 **grp-openstack-admin** 的组。
  - 创建名为 **grp-openstack-demo** 的组。
  - 根据需要，将 RHOSP 用户添加到这些组中。
  - 将您的用户添加到 **grp-openstack** 组。
- 创建 OpenStack 身份域。此流程使用 **LAB** 域。
- 创建或选择 RHOSP 项目。这流程使用一个名为 **demo** 的项目，这项目由 **openstack project create --domain default --description "Demo Project" demo** 命令创建。

流程

1. 从 OpenStack 身份域检索用户组列表：

```
# openstack group list --domain LAB
```

命令输出取决于您集成的外部用户管理服务：

- Active Directory Domain Service (AD DS)：

```
+------------------------------------------------------------+---------------------+
| ID                                                         | Name                |
+------------------------------------------------------------+---------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-
openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-
openstack-admin |
```

```
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-openstack-demo  |
+----------------------------------------------------------------+---------------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------------------------------------+---------------------+
| ID                                                             | Name                |
+----------------------------------------------------------------+---------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-openstack-admin |
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-openstack-demo  |
+----------------------------------------------------------------+---------------------+
```

2. 检索角色列表：

```
# openstack role list
```

命令输出取决于您集成的外部用户管理服务：

- Active Directory Domain Service (AD DS)：

```
+----------------------------------+-----------------+
| ID                               | Name            |
+----------------------------------+-----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin           |
| 034e4620ed3d45969dfe8992af001514 | member          |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin   |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader          |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator   |
| ef3d3f510a474d6c860b4098ad658a29 | service         |
+----------------------------------+-----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+---------------+
```

3. 通过将用户组添加到一个或多个这些角色，来授予用户对 RHOSP 项目的访问权限。例如，如果您希望 **grp-openstack-demo** 组中的用户是 **demo** 项目的普通用户，您必须将该组添加到 **member** 或 **_member_** 角色中，具体取决于您要集成的外部服务：

- Active Directory Domain Service (AD DS)：

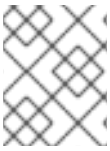
```
# openstack role add --project demo --group
d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8  member
```

- Red Hat Identity Manager (IdM):

```
$ openstack role add --project demo --group
d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8
_member_
```

结果

grp-openstack-demo 的成员可通过输入其用户名和密码并在 **Domain** 字段中输入 **6443** 登录到仪表板：



注意

如果用户收到错误 **Error: Unable to retrieve container list。** 它应该能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 2.10 节 “授予外部用户访问 Red Hat OpenStack Platform 项目”

2.10. 授予外部用户访问 RED HAT OPENSTACK PLATFORM 项目

要从 **grp-openstack** 组中授予特定经过身份验证的用户，您可以向这些用户授予 Red Hat OpenStack Platform (RHOSP)项目的直接访问。如果您要向单个用户授予访问权限，而不是向组授予访问权限，请使用此过程。

先决条件

- 确保外部服务管理员完成以下步骤：
  - 将您的 RHOSP 用户添加到 **grp-openstack** 组中。
  - 创建 OpenStack 身份域.此流程使用 **LAB** 域。

- 创建或选择 RHOSP 项目。这流程使用一个名为 **demo** 的项目，这项目由 **openstack project create --domain default --description "Demo Project" demo** 命令创建。

流程

1. 从 OpenStack 身份域检索用户列表：

```
# openstack user list --domain LAB
 +------------------------------------------------------------------+----------------+
| ID                                                 | Name           |
+------------------------------------------------------------------+----------------+
| 1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e | user1          |
| 12c062faddc5f8b065434d9ff6fce03eb9259537c93b411224588686e9a38bf1 | user2          |
| afaf48031eb54c3e44e4cb0353f5b612084033ff70f63c22873d181fdae2e73c | user3          |
| e47fc21dcf0d9716d2663766023e2d8dc15a6d9b01453854a898cabb2396826e | user4
|
+------------------------------------------------------------------+----------------+
```

2. 检索角色列表：

```
# openstack role list
```

命令输出取决于您集成的外部用户管理服务：

- Active Directory Domain Service (AD DS)：

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+---------------+
```

3. 通过将他们添加到一个或多个这些角色来授予用户对 RHOSP 项目的访问权限。例如，如果您希望 **user1** 是 **demo** 项目的一个一般用户，您可以将它们添加到**member** 或 **_member_** 角色中（具体取决于您集成的外部服务）。

- Active Directory Domain Service (AD DS)：

```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e member
```

- Red Hat Identity Manager (IdM):

```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e _member_
```

4. 如果您希望 **user1** 是 **demo** 项目的管理用户，请将该用户添加到 **admin** 角色中：

```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e admin
```

结果

user1 用户可以通过输入其外部用户名和密码并在 **Domain** 字段中输入 **LAB** 登录到控制面板：

注意

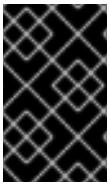
如果用户收到错误 **Error: Unable to retrieve container list。** 它应该能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 2.9 节 “授予外部组对 Red Hat OpenStack Platform 项目的访问权限”

2.11. 查看 OPENSTACK 身份域和用户列表

使用 **openstack domain list** 命令列出可用条目。在 Identity Service 中配置多个域，可在仪表板登录页面中启用一个新的 **Domain** 字段。用户应输入与其登录凭据匹配的域。



重要

完成集成后，您需要决定是否在 **Default** 域中创建新项目，还是在新创建的 keystone 域中创建新项目。您必须考虑您的工作流以及如何管理用户帐户。如果可能，使用 **Default** 域作为内部域来管理服务帐户和 **admin** 项目，并将外部用户保留在单独的域中。

在本例中，外部帐户需要指定 **LAB** 域。内置的 keystone 帐户（如 **admin**）必须指定 **Default** 作为其域。

流程

1. 显示域列表：

```
# openstack domain list
+----------------------------------+---------+---------+-----------------------------------------------------------
--------------+
| ID                               | Name    | Enabled | Description                                                |
+----------------------------------+---------+---------+-----------------------------------------------------------
--------------+
| 6800b0496429431ab1c4efbb3fe810d4 | LAB     | True    |
|
| default                          | Default | True    | Owns users and projects available on Identity API
v2. |
+----------------------------------+---------+---------+-----------------------------------------------------------
--------------+
```

2. 显示特定域中的用户列表。这个命令指定了 **--domain** the，并返回属于 **grp-openstack** 组成员的用户，该域中的用户：

```
# openstack user list --domain LAB
```

您还可以附加 **--domain Default** 来显示内置 keystone 帐户：

```
# openstack user list --domain Default
```

2.12. 为非管理员用户创建凭据文件

为 OpenStack 身份配置用户和域后，您可能需要为非管理员用户创建凭据文件。

流程

- 为非管理员用户创建凭证(RC)文件。本例使用文件中的 **user1** 用户。

```
$ cat overcloudrc-v3-user1
# Clear any old environment that may conflict.
for key in $( set | awk '{FS="="}  /^OS_/ {print $1}' ); do unset $key ; done
export OS_USERNAME=user1
export NOVA_VERSION=1.1
export OS_PROJECT_NAME=demo
export OS_PASSWORD=RedactedComplexPassword
export OS_NO_CACHE=True
export COMPUTE_API_VERSION=1.1
export no_proxy=,10.0.0.5,192.168.2.11
```

```
export OS_CLOUDNAME=overcloud
export OS_AUTH_URL=https://10.0.0.5:5000/v3
export OS_AUTH_TYPE=password
export PYTHONWARNINGS="ignore:Certificate has no, ignore:A true
SSLContext object is not available"
export OS_IDENTITY_API_VERSION=3
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=LAB
```

2.13. 测试 OPENSTACK IDENTITY 与外部用户管理服务集成

要测试 OpenStack Identity (keystone)是否成功与 Active Directory 域服务(AD DS)集成，请测试用户对仪表板功能的访问权限。

先决条件

- 与外部用户管理服务集成，如 Active Directory (AD)或 Red Hat Identity Manager (IdM)

流程

1. 在外部用户管理服务中创建测试用户，并将用户添加到 **grp-openstack** 组中。
2. 在 Red Hat OpenStack Platform 中，将用户添加到 **demo** 项目的 **_member_** 角色中。
3. 使用 AD 测试用户的凭证登录到控制面板。
4. 单击每个选项卡，以确认它们成功显示且没有错误消息。
5. 使用控制面板构建测试实例。

注意

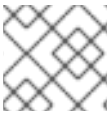
如果您在这些步骤时遇到问题，请使用 **admin** 帐户登录控制面板，然后以该用户身份执行后续步骤。如果测试成功，这意味着 OpenStack 仍然按预期工作，并且 OpenStack Identity 和 Active Directory 之间的集成设置出现问题。

其他资源

- 第 1.10 节 “Active Directory 集成故障排除”

2.14. RED HAT IDENTITY MANAGER (IDM)集成故障排除

如果您在将 Red Hat Identity Manager (IdM)与 OpenStack 身份集成时遇到问题，您可能需要测试 LDAP 连接或测试证书信任配置。您可能还需要检查 LDAPS 端口是否可以访问。



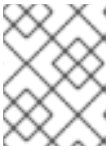
注意

根据错误类型和位置，仅执行此流程中的相关步骤。

流程

1. 使用 **ldapsearch** 命令远程对 IdM 服务器执行测试查询来测试 LDAP 连接。这里有一个成功的结果表示网络连接正在正常工作，IdM 服务已启动。在本例中，针对服务器 **idm.lab.local** 在端口 **636** 上执行测试查询：

```
# ldapsearch -D "cn=directory manager" -H ldaps://idm.lab.local:636 -b "dc=lab,dc=local" -s sub "(objectclass=*)" -w RedactedComplexPassword
```



注意

ldapsearch 是 **openldap-clients** 软件包的一部分。您可以使用 evince **dnf install openldap-clients** 进行安装。

2. 使用 **nc** 命令检查是否远程访问 LDAPS 端口 **636**。在本例中，针对服务器 **idm.lab.local** 执行探测。按 **ctrl-c** 退出提示符。

```
# nc -v idm.lab.local 636
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.200.10:636.
^C
```

如果无法建立连接，这可能表示防火墙配置问题。