Red Hat OpenStack Platform 17.1

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: 2024-09-05

Red Hat OpenStack Platform 17.1 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

使用联邦或 LDAP 将 OpenStack Identity (keystone)服务与身份提供程序集成。您可以使用 Red Hat Single Sign-On, Microsoft Active Directory Federation Services (AD FS), Microsoft Active Directory Domain Service (AD DS)或 Red Hat Identity Management (IdM)作为身份提供程序。

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 表单在 OpenShift (RHOSO)或更早版本的 Red Hat OpenStack Platform (RHOSP)上提供有关 Red Hat OpenStack Services 文档的反馈。当您为 RHOSO 或 RHOSP 文档创建问题时，这个问题将在 RHOSO Jira 项目中记录，您可以在其中跟踪您的反馈的进度。

要完成 Create Issue 表单，请确保您已登录到 JIRA。如果您没有红帽 JIRA 帐户，您可以在 https://issues.redhat.com 创建一个帐户。

1. 点击以下链接打开 **Create Issue** 页面： Create Issue
2. 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。
3. 点 **Create**。

第 1 章 RED HAT OPENSTACK PLATFORM 身份提供程序

您可以部署两种方法之一，以对用户身份进行身份验证，以向身份提供程序(IdP)进行身份验证：

- 您可以使用 LDAP （轻量级目录访问协议）将 Red Hat OpenStack Platform (RHOSP)身份服务(keystone)连接到 IdP
- 您可以使用联邦，其中 IdP 向身份服务发送断言到授予用户对云的访问权限。

虽然 LDAP 用作身份管理和身份验证的中央授权，但联邦可用于构建单点登录解决方案。

有关使用 Active Directory (AD)或 Red Hat Identity Manager (IdM)将 RHOSP 服务连接到 LDAP 目录服务的详情，请参考以下资源：

- 将 OpenStack Identity (keystone)与 Active Directory 集成
- 将 OpenStack 身份(keystone)与红帽身份管理器(IdM)集成

有关为联邦解决方案使用 Red Hat Single Sign-On 将 RHOSP 连接到 IdM 的详情，请参考以下资源：

- 使用 Red Hat OpenStack Platform 和 Red Hat Single Sign-On 进行联邦
- 使用 Red Hat OpenStack Platform 和 Active Directory Federation Services 进行联邦

第 2 章 使用 RED HAT OPENSTACK PLATFORM 和 RED HAT SINGLE SIGN-ON 进行联邦

红帽支持使用 Red Hat Single Sign-On 作为 Red Hat OpenStack Platform (RHOSP)的身份供应商，以便您可以在更广泛的机构中使用相同的联邦解决方案进行 RHOSP 中的单点登录。

2.1. 使用红帽单点登录部署 RED HAT OPENSTACK PLATFORM

使用 **enable-federation-openidc.yaml** 环境文件来部署 Red Hat OpenStack Platform (RHOSP)，以便它可以集成到您的联邦身份验证解决方案中。联邦允许用户使用单点登录(SSO)登录 OpenStack 控制面板。您必须使用 OpenStack Dashboard for SSO。

先决条件

- 已安装 Red Hat OpenStack Platform director。
- 您的环境中已有 Red Hat Single Sign-On (RH-SSO)联邦身份验证。

流程

1. 记录您的 Identity 服务端点。keystone 端点是您在 **custom-domain.yaml** heat 模板中分配 **CloudName** 参数的 FQDN 值，其中包含的传输和端口号。keystone 端点有以下构造：

```
https://<FQDN>:13000
```

注意

如果没有部署 TLS，您的 Identity 服务 API 端点为 http://<FQDN>:5000。红帽建议使用 RHOSP 的每个生产环境部署 TLS。

2. 为 SSO 管理员提供以下重定向 URI：

```
https://<FQDN>:13000/v3/auth/OS-FEDERATION/identity_providers/kcipaIDP/protocols/openid/websso
https://<FQDN>:13000/v3/auth/OS-FEDERATION/websso/openid
```

作为响应，您的 SSO 管理员为您提供了 **ClientID** 和 **ClientSecret**。

3. 将 **enable-federation-openidc.yaml** heat 模板复制到堆栈主目录中：

```
$ cp /usr/share/openstack-tripleo-heat-templates/environments/enable-federation-openidc.yaml \
/home/stack/
```

4. 编辑 **enable-federation-openidc.yaml** 环境文件的副本。以下是配置示例：

```
parameter_defaults:
  KeystoneAuthMethods: password,token,oauth1,mapped,application_credential,openid (1)
  KeystoneOpenIdcClientId: <ClientID> (2)
  KeystoneOpenIdcClientSecret: <ClientSecret> (3)
  KeystoneOpenIdcCryptoPassphrase: openstack (4)
  KeystoneOpenIdcIdpName: kcipaIDP (5)
```

```
  KeystoneOpenIdcIntrospectionEndpoint: https://rh-
sso.local.com/realms/master/protocol/openid-connect/token/introspect 6
  KeystoneOpenIdcProviderMetadataUrl: https://rh-sso.local.com/realms/master/.well-
known/openid-configuration 7
  KeystoneOpenIdcRemoteIdAttribute: HTTP_OIDC_ISS 8
  KeystoneOpenIdcResponseType: id_token 9
  KeystoneTrustedDashboards: https://overcloud.redhat.local/dashboard/auth/websso/ 10
  WebSSOChoices: [['OIDC', 'OpenID Connect']] 11
  WebSSOIDPMapping: {'OIDC': ['kcipaIDP', 'openid']} 12
  WebSSOInitialChoice: OIDC
  KeystoneFederationEnable: True
  KeystoneOpenIdcEnable: True
  KeystoneOpenIdcEnableOAuth: True
  WebSSOEnable: True
```

1. 以逗号分隔的用于身份验证的可接受的方法列表。
2. 用于 OpenID Connect 供应商握手的客户端 ID。您必须从 SSO 管理员获取此功能
3. 用于 OpenID Connect 供应商握手的客户端 secret。在提供重定向 URL 后，您必须从 SSO 管理员获取此结果。
4. 选择在为 OpenID Connect 握手加密数据时使用的密码短语。
5. 在 Identity 服务(keystone)中与 IdP 关联的名称。对于 RH-SSO，此参数的值始终为 kcipaIDP。
6. Identity 服务内省端点： https://{FQDN}/realms/<realm>/protocol/openid-connect/token/introspect
7. 指向 OpenID Connect 供应商元数据的 URL
8. 要从环境中获取身份提供程序的实体 ID 属性。
9. 预期来自 OpenID Connect 供应商的响应类型。
10. 用于单点登录的仪表板 URL，也可以是以逗号分隔的列表。
11. 指定要安装的 SSO 身份验证选择列表。每个项目都是 SSO 选择标识符和显示消息的列表。
12. 指定从 SSO 身份验证选择到身份提供程序和协议的映射。身份提供程序和协议名称必须与 keystone 中定义的资源匹配。

5. 将 **enable-federation-openidc.yaml** 添加到堆栈中，以及其他环境文件并部署 overcloud：

```
(undercloud)$ openstack overcloud deploy --templates \
-e [your environment files] \
-e /home/stack/templates/enable-federation-openidc.yaml.yaml
```

2.2. 将 RED HAT OPENSTACK PLATFORM 与红帽单点登录集成

使用 Red Hat Single Sign-On (RH-SSO)部署 Red Hat OpenStack Platform (RHOSP)后，您必须将 RH-SSO 与 RHOSP 集成。

流程

1. 创建一个联邦域：

```
$ openstack domain create <federated_domain_name>
```

输出示例：

```
+-------------+----------------------------------+
| Field       | Value                            |
+-------------+----------------------------------+
| description |                                  |
| enabled     | True                             |
| id          | b493634c9dbf4546a2d1988af181d7c9 |
| name        | my_domain                        |
| options     | {}                               |
| tags        | []                               |
+-------------+----------------------------------+
```

2. 设置联邦身份提供程序：

```
$ openstack identity provider create --remote-id https://<rh-sso_fqdn>:9443/realms/<realm> --domain <domain_name> kcipaIDP
```

将 **<rh-sso_fqdn** > 替换为 RH-SSO 的完全限定域名，将 < **realm&** gt; 替换为 RH-SSO 域。默认域是 **master**。将 **<federated_domain_name** > 替换为在第 1 步中创建的联邦域的名称。

输出示例：

```
+-------------------+-------------------------------------------------------+
| Field             | Value                                                 |
+-------------------+-------------------------------------------------------+
| authorization_ttl | None                                                  |
| description       | None                                                  |
| domain_id         | b493634c9dbf4546a2d1988af181d7c9                      |
| enabled           | True                                                  |
| id                | kcipaIDP                                              |
| remote_ids        | https://rh-sso.fqdn.local:9443/realms/master          |
+-------------------+-------------------------------------------------------+
```

3. 创建一个映射文件，它对云的身份需求是唯一的。
Example:

```
 cat > mapping.json << EOF
[
   {
      "local": [
         {
            "user": {
             "name": "{0}"
            },
            "group": {
               "domain": {
                "name": "<federated_domain_name>" 1
```

```
                },
                "name": "<federated_group_name>" 2
            }
        }
    ],
    "remote": [
        {
            "type": "OIDC-preferred_username" 3
        }
    ]
  }
]
EOF
```

1 <federated_domain_name> 是在第 x 步中创建的域。

2 为 **federated_group_name** 选择一个名称。您将在后续步骤中创建此功能

3 您必须使用 **OIDC-preferred_username** 作为 RH-SSO 的声明 ID

1. 使用映射文件为 RHOSP 创建联邦映射规则。在提供的示例中，从 **mapping.json** 文件创建的映射规则命名为 **IPAmap** ：

```
openstack mapping create --rules <file> <name>
```

例如：

```
$ openstack mapping create --rules mapping.json IPAmap
```

2. 创建一个联邦组：

```
$ openstack group create --domain <federation_domain_name>
<federation_group_name>
```

3. 创建 Identity 服务(keystone)项目：

```
$ openstack project create --domain <federation_domain> <federation_project_name>
```

4. 将 Identity 服务联邦组添加到角色中：

```
$ openstack role add --group <federation_group_name> --group-domain
<federation_domain> --project <federation_project_name> --project-domain
<federation_domain> member
```

5. 创建 OpenID 联邦协议：

```
$ openstack federation protocol create openid --mapping IPAmap --identity-provider
kcipaIDP
```

2.3. 其他资源

有关 Red Hat Singe Sign-On 的更多信息，请参阅 入门指南

第 3 章 使用 RED HAT OPENSTACK PLATFORM 和 ACTIVE DIRECTORY FEDERATION SERVICES 进行联邦

红帽支持使用 Microsoft Active Directory Federation Services (AD FS)作为 Red Hat OpenStack Platform (RHOSP)的身份供应商，以便您可以在 RHOSP 中使用相同的联邦解决方案进行 RHOSP 中的单点登录。

3.1. 使用 ACTIVE DIRECTORY FEDERATION SERVICES 部署 RED HAT OPENSTACK PLATFORM

使用 **enable-federation-openidc.yaml** 环境文件来部署 Red Hat OpenStack Platform (RHOSP)，以便它可以集成到您的联邦身份验证解决方案中。联邦允许用户使用单点登录(SSO)登录 OpenStack 控制面板。您必须使用 OpenStack Dashboard for SSO。

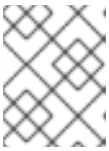
先决条件

- 已安装 Red Hat OpenStack Platform director。
- 您有 Active Directory (c)用于在您的环境中配置的联邦。

流程

1. 记录您的 keystone 端点。keystone 端点是您在 **custom-domain.yaml** heat 模板中分配 **CloudName** 参数的 FQDN 值，其中包含的传输和端口号。keystone 端点有以下构造：

```
https://<FQDN>:13000
```



注意

如果没有部署 TLS，则 keystone 端点为 **http://<FQDN>:5000**。红帽建议使用 RHOSP 的每个生产环境部署 TLS。

2. 为 SSO 管理员提供以下重定向 URI：
重定向 URI：

```
https://<FQDN>:13000/v3/auth/OS-FEDERATION/identity_providers/adfsIDP/protocols/openid/websso
https://<FQDN>:13000/v3/auth/OS-FEDERATION/websso/openid
```

3. 作为响应，您的 SSO 管理员为您提供了 **ClientID** 和 **ClientSecret**。

4. 将 **enable-federation-openidc.yaml** yaml 文件复制到堆栈主目录中：

```
cp /usr/share/openstack-tripleo-heat-templates/environments/enable-federation-openidc.yaml \
/home/stack/
```

5. 编辑 **enable-federation-openidc.yaml** 环境文件的副本。以下是配置示例：

```
parameter_defaults:
  KeystoneAuthMethods: password,token,oauth1,mapped,application_credential,openid
```
(1)

```
  KeystoneOpenIdcClientId: <ClientID> 2
  KeystoneOpenIdcClientSecret: <ClientSecret> 3
  KeystoneOpenIdcCryptoPassphrase: openstack 4
  KeystoneOpenIdcIdpName: adfsIdP 5
  KeystoneOpenIdcIntrospectionEndpoint: https://adfs.local.com/adfs/openid-
connect/token/introspect 6
  KeystoneOpenIdcProviderMetadataUrl: https://adfs.local.com/adfs/.well-known/openid-
configuration 7
  KeystoneOpenIdcRemoteIdAttribute: HTTP_OIDC_ISS 8
  KeystoneOpenIdcResponseType: code 9
  KeystoneTrustedDashboards: https://overcloud.redhat.local/dashboard/auth/websso/ 10
  WebSSOChoices: [['OIDC', 'OpenID Connect']] 11
  WebSSOIDPMapping: {'OIDC': ['adfsIdP', 'openid']} 12
  WebSSOInitialChoice: OIDC
  KeystoneFederationEnable: True
  KeystoneOpenIdcEnable: True
  KeystoneOpenIdcEnableOAuth: True
  WebSSOEnable: True
```

1. 以逗号分隔的用于身份验证的可接受的方法列表。
2. 用于 OpenID Connect 供应商握手的客户端 ID。您必须从 SSO 管理员获取此功能
3. 用于 OpenID Connect 供应商握手的客户端 secret。在提供重定向 URL 后，您必须从 SSO 管理员获取此结果。
4. 选择在为 OpenID Connect 握手加密数据时使用的密码短语。
5. 在 Identity 服务(keystone)中与 IdP 关联的名称。此参数的值始终是 Active Directory Federation Services 的 adfsIDP。
6. Identity 服务内省端点： https://{FQDN}/realms/<realm>/protocol/openid-connect/token/introspect
7. 指向 OpenID Connect 供应商元数据的 URL
8. 要从环境中获取身份提供程序的实体 ID 属性。
9. 预期来自 OpenID Connect 供应商的响应类型。
10. 用于单点登录的仪表板 URL，也可以是以逗号分隔的列表。
11. 指定要安装的 SSO 身份验证选择列表。每个项目都是 SSO 选择标识符和显示消息的列表。
12. 指定从 SSO 身份验证选择到身份提供程序和协议的映射。身份提供程序和协议名称必须与 keystone 中定义的资源匹配。

6. 将 **enable-federation-openidc.yaml** 添加到堆栈中，以及其他环境文件并部署 overcloud：

```
(undercloud)$ openstack overcloud deploy --templates \
-e [your environment files] \
-e /home/stack/templates/enable-federation-openidc.yaml.yaml
```

3.2. 将 RED HAT OPENSTACK PLATFORM 与 ACTIVE DIRECTORY FEDERATION 服务集成

使用 Active Directory Federation Services (ADFS)部署 Red Hat OpenStack Platform (RHOSP)后，您必须完成以下步骤将身份提供程序(IdP)与服务供应商(RHOSP)集成。

流程

1. 创建一个联邦域：

```
openstack domain create <federated_domain_name>
```

输出示例：

```
+-------------+----------------------------------+
| Field       | Value                            |
+-------------+----------------------------------+
| description |                                  |
| enabled     | True                             |
| id          | b493634c9dbf4546a2d1988af181d7c9 |
| name        | my_domain                        |
| options     | {}                               |
| tags        | []                               |
+-------------+----------------------------------+
```

2. 设置联邦身份提供程序。

```
openstack identity provider create --remote-id https://<adfs_fqdn>:9443/adfs --domain
<domain_name> adfsIdP
```

将 **<adfs_fqdn** > 替换为 Active Directory Federation Services 的完全限定域名，将 < **federated_domain_name** > 替换为在第 1 步中创建的联邦域的名称。

输出示例：

```
+-------------------+-----------------------------------------------------+
| Field             | Value                                               |
+-------------------+-----------------------------------------------------+
| authorization_ttl | None                                                |
| description       | None                                                |
| domain_id         | b493634c9dbf4546a2d1988af181d7c9                    |
| enabled           | True                                                |
| id                | adfsIdP                                             |
| remote_ids        | https:/adfs.fqdn.local/adfs/                        |
+-------------------+-----------------------------------------------------+
```

3. 创建映射文件.映射文件对您的云的身份需求是唯一的。
Example:

```
 cat > mapping.json << EOF
[
    {
        "local": [
```

```
        {
            "user": {
             "name": "{0}"
            },
            "group": {
                "domain": {
                 "name": "<federated_domain>" 1
                },
                "name": "<federated_group_name>" 2
            }
        }
    ],
    "remote": [
        {
            "type": "OIDC-upn" 3
        }
    ]
  }
]
EOF
```

1. **federated_domain** 是您在上一步中创建的域。
2. 为 **federated_group_name** 选择一个名称。您将在后续步骤中创建此设置。
3. 您必须使用 'OIDC-upn' 作为 ADFS 的声明 ID。

1. 使用映射文件为 OpenStack 创建联合映射规则。在提供的示例中，从 **mapping.json** 文件创建的映射规则称为 **ADmap** ：

```
openstack mapping create --rules <file> <name>
```

例如：

```
$ openstack mapping create --rules mapping.json ADmap
```

1. 创建一个联邦组：

```
openstack group create --domain <federation_domain> <federation_group_name>
```

2. 创建 Identity 服务(keystone)项目：

```
openstack project create --domain <federation_domain> <federation_project_name>
```

3. 将 Identity 服务联邦组添加到角色。

```
openstack role add --group <federation_group_name> --group-domain <federation_domain> --
project <federation_project_name> --project-domain <federation_domain> member
```

1. 创建 OpenID 联邦协议：

```
openstack federation protocol create openid --mapping ADmap --identity-provider adfsIdP
```

第 4 章 使用 RED HAT OPENSTACK PLATFORM 和其他供应商进行联邦

当与红帽单点登录(RH-SSO)和 Active Directory Federation Services (ADFS)以外的供应商集成时，红帽不提供对联邦的直接支持。如果要使用其他供应商，请联系红帽以获得支持例外。

4.1. 为其他供应商自定义联邦

其他供应商可能有不同的方式来限制 OpenIDC 声明或格式化用户信息，例如：以下是可在 heat 中调整的功能。

先决条件

- 已安装 Red Hat OpenStack Platform (RHOSP) director
- 您在您的环境中提供了一个联合解决方案
- RHOSP 是 17.1.3 或更高版本的版本

流程

1. 为您的 SSO 管理员提供适当的重定向 URI。作为响应，您的 SSO 管理员为您提供了 **ClientID** 和客户端 **secret**。
2. 将 **enable-federation-openidc.yaml** 环境文件 heat 模板复制到 **/home/stack/templates/** 目录并进行配置。
3. 使用以下三个参数来自定义 RHOSP 和联合解决方案之间的交互。

```
parameter_defaults:
  KeystoneOpenIdcClaimDelimiter: ';' (1)
  KeystoneOpenIdcPassUserInfoAs: 'claims' (2)
  KeystoneOpenIdcPassClaimsAs: 'both' (3)
  ...
```

(1) 在设置多值声明时，使用 **KeystoneOpenIdcClaimDelimiter** 参数设置分隔符。默认分隔符为分号。

(2) 使用 **KeystoneOpenIdcPassUserInfoAs** 参数定义在解析后声明传递到联邦应用的方式。允许的值是 **声明**、**json** 和 **jwt**。

(3) 使用 **KeystoneOpenIdcPassClaimsAs** 参数定义声明和令牌传递给应用环境的方式。这些选项是：

- **none** ：声明和令牌不会传递给应用程序。
- **环境** ：声明和令牌作为环境变量传递。
- **标头** ：声明和令牌在标头中传递。
- **：**Claims 和 headers 都作为标头和变量传递。这是默认值。

附加信息

- 使用红帽单点登录部署 Red Hat OpenStack Platform
- 使用 Active Directory Federation Services 部署 Red Hat OpenStack Platform

第 5 章 将 OPENSTACK IDENTITY (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 验证某些 Active Directory 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，身份服务对 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用户。

通过将身份服务与 AD DS 集成，您可以允许 AD DS 用户向 Red Hat OpenStack Platform (RHOSP)进行身份验证以访问资源。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 身份与 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. 配置活动目录用户或组对 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。

5.1. 配置 ACTIVE DIRECTORY 凭证

要配置 Active Directory 域服务(AD DS)，以与 OpenStack 身份集成，为身份服务设置 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 域服务已配置且可操作。
- Red Hat OpenStack Platform 已配置且可操作。
- DNS 名称解析功能全面，所有主机都进行适当注册。
- 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。此帐户供 Identity Service 用于查询 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. 为这个帐户设置密码，然后启用它。系统将提示您指定符合 AD 域复杂性要求的密码：

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

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

```
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（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
```

将此值发送到 RHOSP 管理员。

5.2. 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 能够引用它的位置。

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 project**，或者 **Peer 的证书签发者不能被识别**。如果 keystone 对某个域使用了不正确的证书，则可能会出现这种情况。作为临时解决方案，请将所有 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

- 配置了活动目录凭证。
- LDAPS 证书是从 Active Directory 导出。

流程

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

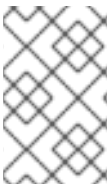
```
# openssl x509 -inform der -in addc.lab.local.cer -out addc.lab.local.pem
```

   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
```

5.3. 将 DIRECTOR 配置为使用域特定的 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 键设置所需的路径来覆盖它，并在环境文件中将它添加为 **ExtraConfig** 参数。

流程

1. 在部署的 heat 模板中，将 **KeystoneLDAPDomainEnable** 标志设为 **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，并将值设置为适合您的部署。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
    ...
```

这会生成两个名为 **domain1** 和 **domain2** 的域；每个域都有一个不同的 LDAP 域，它们都有自己的配置。

5.4. 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 **并查看域** 选项卡，获取域和 **admin** 用户的 ID，然后将 **admin** 角色分配给域中的用户。

注意

这不授予 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 域服务(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
```

5.5. 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，您可以授权来自外部用户管理服务的特定组来授予 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给项目中的角色。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 用户添加到其中一个组中。
  - 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 Identity 域中检索用户组列表：

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

命令输出取决于您与之集成的外部用户管理服务：

- Active Directory 域服务(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
```

命令输出取决于您与之集成的外部用户管理服务：

- Active Directory 域服务(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，授予用户组对 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** 项目的常规用户，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 域服务(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 **Error: Unable to retrieve container list。** 并且希望能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 5.6 节 “授予外部用户对 Red Hat OpenStack Platform 项目的访问权限”

5.6. 授予外部用户对 RED HAT OPENSTACK PLATFORM 项目的访问权限

要从 **grp-openstack** 组授予对 OpenStack 资源的特定经过身份验证的用户，您可以授予这些用户直接访问 Red Hat OpenStack Platform (RHOSP)项目。在您要授予各个用户访问权限而不是授予组访问权限的情况下，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 RHOSP 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 Identity 域中检索用户列表：

```
# 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
```

命令输出取决于您与之集成的外部用户管理服务：

- Active Directory 域服务(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. 通过将用户添加到一个或多个这些角色，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 域服务(AD DS)：

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

- Red Hat Identity Manager (IdM):

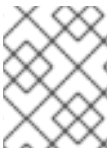
```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e _member_
```

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

```
# 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

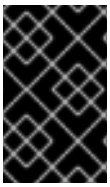
如果用户收到 **Error: Unable to retrieve container list。** 并且希望能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 5.5 节 “授予外部组对 Red Hat OpenStack Platform 项目的访问权限”

5.7. 查看 OPENSTACK 身份域和用户列表

使用 **openstack domain list** 命令列出可用的条目。在 Identity Service 中配置多个域会在仪表板登录页面中启用新的 **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** 域或新创建的 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。此命令示例指定 **--domain LAB**，并返回属于 **grp-openstack** 组成员的用户：

```
# 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
```

5.8. 为非管理员用户创建凭据文件

为 OpenStack Identity 配置用户和域后，您可能需要为非管理员用户创建一个凭据文件。

流程

- 为非管理员用户创建一个凭证(RC)文件。本例在 文件中使用 **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
```

5.9. 测试 OPENSTACK 身份与外部用户管理服务的集成

要测试 OpenStack Identity (keystone)是否已成功与活动目录域服务(AD DS)集成，测试用户对仪表板功能的访问。

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一个测试用户，并将该用户添加到 **grp-openstack** 组。
2. 在 Red Hat OpenStack Platform 中，将用户添加到 **demo** 项目的 **_member_** 角色。
3. 使用 AD 测试用户的凭据登录控制面板。
4. 单击每个选项卡，以确认它们已成功显示，且无错误消息。
5. 使用控制面板构建测试实例。

注意

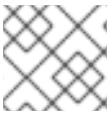
如果您遇到这些步骤的问题，请使用 **admin** 帐户登录控制面板，并以该用户身份执行后续步骤。如果测试成功，这意味着 OpenStack 仍然可以正常工作，并且 OpenStack Identity 和 Active Directory 之间的集成设置中存在问题。

其他资源

- 第 5.10 节 “Active Directory 集成故障排除”

5.10. ACTIVE DIRECTORY 集成故障排除

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



注意

根据错误类型和位置，只执行此流程中的相关步骤。

流程

1. 使用 **ldapsearch** 命令针对 Active Directory 域控制器远程执行测试查询来测试 LDAP 连接。成功结果表示网络连接正常工作，AD DS 服务已启动。在本例中，对端口 **636** 上的服务器 **192.0.2.250** 执行测试查询：

```
# ldapsearch -Z -x -H ldaps://192.0.2.250:636 -D
"cn=openstack,ou=Users,dc=director,dc=example,dc=com" -W -b
"ou=Users,dc=director,dc=example,dc=com" -s sub "
(memberOf=cn=OSuser,ou=Groups,dc=director,dc=example,dc=com)"
```

注意

- **ldapsearch** 是 **openldap-clients** 软件包的一部分。您可以使用 **# dnf install openldap-clients**安装它
- 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's Certificate issuer** 错误，请确认您的 **TLS_CACERTDIR** 路径已被正确设置。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。

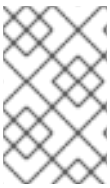
4. 使用 **nc** 命令检查 LDAPS 端口 **636** 是否可以被远程访问。在本例中，对服务器 **addc.lab.local** 执行探测。按 **ctrl-c** 退出提示符。

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

不建立连接时可能表示防火墙配置问题。

第 6 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 验证某些红帽身份管理(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，身份服务对 IdM 具有对用户帐户身份验证的只读访问权限，同时保持对分配给经过身份验证的用户的权限的管理。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 集成前查看以下关键术语：

- **Authentication** - 使用密码验证用户是否声明的身份。
- **授权** - 验证经过身份验证的用户对其试图访问的系统具有正确的权限。
- **域** - 请参阅 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 将 undercloud 和 overcloud 注册到 IdM 中
2. 使用 Ansible 在 undercloud 和 overcloud 上实施 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

6.1. 规划 RED HAT IDENTITY MANAGER (IDM)集成

当您计划 OpenStack 身份与 Red Hat Identity Manager (IdM)集成时，请确保配置并运行这两个服务，并查看集成用户管理和防火墙设置的影响。

先决条件

- Red Hat Identity Management 已配置且可操作。
- Red Hat OpenStack Platform 已配置且可操作。
- DNS 名称解析功能全面，所有主机都进行适当注册。

权限和角色

此集成允许 IdM 用户对 OpenStack 和访问资源进行身份验证。OpenStack 服务帐户（如 keystone 和 glance）以及授权管理（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

此配置会创建对单个 IdM 服务器可用性的依赖项：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，如果不可用，或者您可以使用负载均衡器。在将 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现故障转移。

中断要求

- 需要重启 Identity Service 才能添加 IdM 后端。
- 在 IdM 中创建帐户之前，用户将无法访问仪表板。要减少停机时间，请事先考虑在这个更改前预先尝试 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)
- 过期时对新证书的 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，则需要允许通过以下端口访问：

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

6.2. 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 Red Hat OpenStack Platform 环境集成：

表 6.1. 参数建议

选项	建议
--admin-password	请注意您提供的值。在配置 Red Hat OpenStack Platform 以使用 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	使用这个选项将 **/etc/resolv.conf** 中的地址用作 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。如果无法解析反向记录或区域，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任何一个选项来配置 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

6.3. 使用 ANSIBLE 实施 TLS-E

您可以使用新的 **tripleo-ipa** 方法在 overcloud 端点上启用 SSL/TLS，称为 TLS 随处(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

- 确保完成 undercloud 的所有配置步骤，如创建 stack 用户。如需了解更多详细信息，请参阅使用 director 安装和管理 Red Hat OpenStack Platform。
- DNS 服务器的 IP 地址是在 undercloud 上配置为 IdM 服务器的 IP 地址。以下参数之一必须在 **undercloud.conf** 文件中配置：
  - **DEFAULT/undercloud_nameservers**
  - **%SUBNET_SECTION%/dns_nameservers**

流程

使用以下步骤在新的 Red Hat OpenStack Platform 安装或您要使用 TLS-e 配置的现有部署上实现 TLS-e。如果在预置备节点上部署带有 TLS-e 的 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 **openstack undercloud install**、和 **openstack overcloud deploy** 等命令。这些流程是幂等的，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 上的适当搜索域和名称服务器。例如，如果部署域为 **example.com**，并且 FreeIPA 服务器的域是 **bigcorp.com**，则将以下行添加到 /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

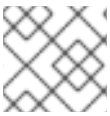
通过完成以下步骤验证 undercloud 是否已正确注册：

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

当您随处部署带有 TLS (TLS-e)的 overcloud 时，Undercloud 和 Overcloud 中的 IP 地址将自动注册到 IdM。

1. 在部署 overcloud 之前，先创建一个 YAML 文件 **tls-parameters.yaml**，其内容类似于以下内容：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 **tls-parameters.yaml** 文件遵循 **openstack overcloud deploy** 命令中的 **enable-internal-tls.yaml**。
- 有关用于实现 TLS-e 的参数的更多信息，请参阅 tripleo-ipa 的参数

2. [可选] 如果您的 IPA 域与您的 IPA 域不匹配，还必须在 **tls-parameters.yaml** 文件中包含 **CertmongerKerberosRealm** 参数的值：

```
    CertmongerKerberosRealm: EXAMPLE.COMPANY.COM
```

3. 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 \
...
```

4. 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
```

6.4. 在 TLS 下加密 MEMCACHED 流量(TLS-E)

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。

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

要将 Red Hat Identity Manager (IdM)配置为与 OpenStack Identity 集成，为身份服务设置 LDAP 帐户，为 Red Hat OpenStack 用户创建一个用户组，并为查找帐户设置密码。

先决条件

- Red Hat Identity Manager (IdM)已配置且可操作。
- Red Hat OpenStack Platform (RHOSP)已配置且可操作。
- DNS 名称解析功能全面，所有主机都进行适当注册。
- 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，以避免单点故障。

流程

在 IdM 服务器上执行此步骤。

1. 创建在 OpenStack Identity Service 中使用的 LDAP 查找帐户来查询 IdM LDAP 服务：

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

注意

创建后，查看此帐户的密码过期设置。

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

```
# 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
```

6.6. 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 能够引用它的位置，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 project**，或者 **Peer 的证书签发者不能被识别**。如果 keystone 对某个域使用了不正确的证书，则可能会出现这种情况。作为临时解决方案，请将所有 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 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 节点上。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
```

6.7. 将 DIRECTOR 配置为使用域特定的 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 键设置所需的路径来覆盖它，并在环境文件中将它添加为 **ExtraConfig** 参数。

流程

1. 在部署的 heat 模板中，将 **KeystoneLDAPDomainEnable** 标志设为 **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，并将值设置为适合您的部署。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
    ...
```

这会生成两个名为 **domain1** 和 **domain2** 的域；每个域都有一个不同的 LDAP 域，它们都有自己的配置。

6.8. 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 **并查看域** 选项卡，获取域和 **admin** 用户的 ID，然后将 **admin** 角色分配给域中的用户。

注意

这不授予 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 域服务(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
```

6.9. 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，您可以授权来自外部用户管理服务的特定组来授予 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给项目中的角色。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 用户添加到其中一个组中。
  - 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 Identity 域中检索用户组列表：

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

命令输出取决于您与之集成的外部用户管理服务：

- Active Directory 域服务(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
```

命令输出取决于您与之集成的外部用户管理服务：

- Active Directory 域服务(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，授予用户组对 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** 项目的常规用户，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 域服务(AD DS)：

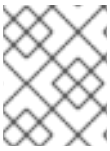
```
# openstack role add --project demo --group
d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8  member
```

- 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 **Error: Unable to retrieve container list。** 并且希望能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 6.10 节 “授予外部用户对 Red Hat OpenStack Platform 项目的访问权限”

6.10. 授予外部用户对 RED HAT OPENSTACK PLATFORM 项目的访问权限

要从 **grp-openstack** 组授予对 OpenStack 资源的特定经过身份验证的用户，您可以授予这些用户直接访问 Red Hat OpenStack Platform (RHOSP)项目。在您要授予各个用户访问权限而不是授予组访问权限的情况下，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 RHOSP 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 Identity 域中检索用户列表：

```
# 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
```

命令输出取决于您与之集成的外部用户管理服务：

- Active Directory 域服务(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. 通过将用户添加到一个或多个这些角色，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 域服务(AD DS)：

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

- Red Hat Identity Manager (IdM):

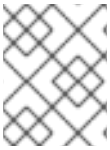
```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e _member_
```

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

```
# 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

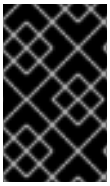
如果用户收到 **Error: Unable to retrieve container list。** 并且希望能够管理容器，则必须将它们添加到 **SwiftOperator** 角色中。

其他资源

- 第 6.9 节 “授予外部组对 Red Hat OpenStack Platform 项目的访问权限”

6.11. 查看 OPENSTACK 身份域和用户列表

使用 **openstack domain list** 命令列出可用的条目。在 Identity Service 中配置多个域会在仪表板登录页面中启用新的 **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** 域或新创建的 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。此命令示例指定 **--domain LAB**，并返回属于 **grp-openstack** 组成员的用户：

```
# 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
```

6.12. 为非管理员用户创建凭据文件

为 OpenStack Identity 配置用户和域后，您可能需要为非管理员用户创建一个凭据文件。

流程

- 为非管理员用户创建一个凭证(RC)文件。本例在 文件中使用 **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
```

6.13. 测试 OPENSTACK 身份与外部用户管理服务的集成

要测试 OpenStack Identity (keystone)是否已成功与活动目录域服务(AD DS)集成，测试用户对仪表板功能的访问。

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一个测试用户，并将该用户添加到 **grp-openstack** 组。
2. 在 Red Hat OpenStack Platform 中，将用户添加到 **demo** 项目的 **_member_** 角色。
3. 使用 AD 测试用户的凭据登录控制面板。
4. 单击每个选项卡，以确认它们已成功显示，且无错误消息。
5. 使用控制面板构建测试实例。

注意

如果您遇到这些步骤的问题，请使用 **admin** 帐户登录控制面板，并以该用户身份执行后续步骤。如果测试成功，这意味着 OpenStack 仍然可以正常工作，并且 OpenStack Identity 和 Active Directory 之间的集成设置中存在问题。

其他资源

- 第 5.10 节 “Active Directory 集成故障排除”

6.14. 对 RED HAT IDENTITY MANAGER (IDM)集成进行故障排除

如果您在将 Red Hat Identity Manager (IdM)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。您可能还需要检查是否可以访问 LDAPS 端口。

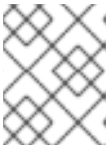
注意

根据错误类型和位置，只执行此流程中的相关步骤。

流程

1. 使用 **ldapsearch** 命令针对 IdM 服务器远程执行测试查询来测试 LDAP 连接。此处成功的结果表示网络连接正常工作，IdM 服务已启动。在本例中，对端口 **636** 上的服务器 **192.0.2.250** 执行测试查询：

```
# ldapsearch -D "cn=directory manager" -H ldaps://192.0.2.250:636 -D
"cn=openstack,ou=Users,dc=director,dc=example,dc=com" -b
"ou=Users,dc=director,dc=example,dc=com" -s sub "
(memberOf=cn=OSuser,ou=Groups,dc=director,dc=example,dc=com)" -w
RedactedComplexPassword
```



注意

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

2. 使用 **nc** 命令检查 LDAPS 端口 **636** 是否可以被远程访问。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
```

未能建立连接时可能会指示防火墙配置问题。