02-Lab1 OpenShift 集群命令行访问

目标

- 从集群中找到、下载并安装`oc`命令
- 理解`$HOME/.kube/config`文件的作用
- 找到一个集群的登录URL
- 使用命令行登录到集群中
- 访问不同的群集并在它们之间切换
- 检索关于你的会话的信息：用户名、服务器名称和令牌
- 了解集群凭证和`KUBECONFIG`变量的作用
- 了解如何保护你的OpenShift用户令牌

场景

你是一个应用程序开发人员，你想把你的应用程序部署到一个OpenShift集群。集群管理员向你提供了集群的域名以及你的用户名和密码凭证。你想登录到集群并准备部署应用。

1. 下载并安装命令行工具

从红帽OpenShift容器平台4.6版本开始，你可以直接从集群中下载`oc`命令行工具。这可以确保命令行工具与你的集群的版本相匹配，并省去了搜索适当版本的麻烦。

对于Linux®，默认位置是`https://downloads-openshift-console.apps.${CLUSTER_DOMAIN_NAME}/amd64/linux/oc`。本实验室的集群域名是**shared-na46.openshift.opentlc.com**。在实验室环境之外，这个值可能不同--请向你的集群管理员询问集群域名。

然后你下载命令行工具，并将其移动到包含在你的`$PATH`中的目录。最后，你要确保该文件是可执行的。

1. 使用你喜欢的SSH客户端和你的OPENTLC凭证登录到`student vm`主机。
2. 运行下面的命令，下载`oc`，安装它，并确保它被标记为可执行。

```
$ wget --no-check-certificate https://downloads-openshift-
console.apps.shared-na46.openshift.opentlc.com/amd64/linux/oc
$ sudo mv oc /usr/local/bin/oc
$ sudo chmod a+x /usr/local/bin/oc
```

2. 使用命令行与OpenShift Master进行认证

现在你有了命令行工具，知道了你的集群的域名、你的用户名和密码。

- 集群域名：**shared-na46.openshift.opentlc.com**
- 你的用户名名称：你的*OPENTLC*登录名
- 你的密码：你的*OPENTLC*密码。

1. 显示`oc`命令的帮助信息。

```
$ oc login -h
Log in to your server and save login for subsequent use
```

```
First-time users of the client should run this command to connect to a
server, establish an authenticated session, and
save connection to the configuration file. The default configuration will be
saved to your home directory under
".kube/config".

The information required to login -- like username and password, a session
token, or the server details -- can be
provided through flags. If not provided, the command will prompt for user
input as needed.

Usage:
  oc login [URL] [flags]

Examples:
  # Log in interactively
  oc login

  # Log in to the given server with the given certificate authority file
  oc login localhost:8443 --certificate-authority=/path/to/cert.crt

  # Log in to the given server with the given credentials (will not prompt
interactively)
  oc login localhost:8443 --username=myuser --password=mypass

Options:
  -p, --password='': Password, will prompt if not provided
  -u, --username='': Username, will prompt if not provided      --
certificate-authority='': Path to a cert file for the
certificate authority
      --insecure-skip-tls-verify=false: If true, the server's certificate
will not be checked for validity. This will
make your HTTPS connections insecure
      --token='': Bearer token for authentication to the API server
```

2. 确定用于认证的正确URL。
    - 如果你的集群管理员没有向你提供详细的URL，它很可能是默认的URL。`https://api.${cluster_domain_name}:6443`。要从集群的域名形成URL，在域名的开头加上`https://api.`，在结尾加上`:6443`。
3. 使用适当的认证URL登录到OpenShift主服务器。将`OPENTLC_USERID`替换为**你**的OPENTLC用户ID（例如，`panni-redhat.com`）：

```
$ oc login -u OPENTLC_USERID https://api.shared-
na46.openshift.opentlc.com:6443
The server uses a certificate signed by an unknown authority.
You can bypass the certificate check, but any data you send to the server
could be intercepted by others.
Use insecure connections? (y/n): y

Authentication required for https://api.shared-
na46.openshift.opentlc.com:6443 (openshift)
Username: panni-redhat.com
Password:
Login successful.

You don't have any projects. You can try to create a new project, by running

    oc new-project
```

3. 获取会话信息

1. 确定`oc`命令的版本和服务器的软件版本。

```
$ oc version
Client Version: openshift-clients-4.6.0-202006250705.p0-168-g02c110006
Kubernetes Version: v1.19.0+7070803
```

2. 用各种选项调用`oc whoami`命令，以获得关于你的用户和你的服务器的信息。

```
$ oc whoami
panni-redhat.com
$ oc whoami --show-server
https://api.shared-na46.openshift.opentlc.com:6443
$ oc whoami --show-token
OJbpVRWM4lfOqKfUtefCbdjRlOwQOeACSsxjXoXVT8E
$ oc whoami --show-context
/api-shared-na4-na4-openshift-opentlc-com:6443/panni-redhat.com
```

   - 你可以使用`--show-token`（或`-t`）来获取一些OpenShift服务所需的登录凭证。
   - `--show-context`显示当前项目、集群和用户。(你还没有任何项目，所以第一个字段是空的）。
   - 当你有几个集群或几组凭证并想在它们之间切换时，你可以使用上下文。

4. 探索`.kube/config`文件的内容和作用

当你第一次登录到集群时，一个包含你的会话信息的文件被自动创建。默认情况下，这个文件位于`$HOME/.kube/config`。

1. 查看这个文件的内容。

```
$ cat $HOME/.kube/config
apiVersion: v1
clusters:
- cluster:
    insecure-skip-tls-verify: true
    server: https://api.shared-na46.openshift.opentlc.com:6443
```

```
  name: api.shared-na4.na4.openshift.opentlc.com:6443
contexts:
- context:
    cluster:api-shared-na4-na4-openshift-opentlc-com:6443
    user: panni-redhat.com/api-shared-na4-na4-openshift-opentlc-com:6443
  name: /api-shared-na4-na4-openshift-opentlc-com:6443/panni-redhat.com
current-context: /api-shared-na4-na4-openshift-opentlc-com:6443/panni-
redhat.com
kind: Config
preferences: {}
users:
- name: panni-redhat.com/api-shared-na4-na4-openshift-opentlc-com:6443
  user:
    token: ejOPm9PYhEqryocKv4W6tpOb3ZOqKEu7GOgyLXXXCH8
```

- 如你所见，这是一个典型的OpenShift YAML文件。
- 它有名为`clusters'、contexts'和`users'的列表，记录了你的登录会话信息。
- 当你访问另一个集群时（可能用不同的用户名），它的信息也会记录在这个文件中。

2. 探索如何分离不同群集的登录信息。
   - 用`KUBECONFIG`引用一个新的配置文件，并登录到一个不同的集群。

```
      $ export KUBECONFIG=$HOME/.kube/new-config
      $ oc login -u panni-redhat.com https://api.shared-
na46.openshift.opentlc.com:6443
      The server uses a certificate signed by an unknown authority.
      You can bypass the certificate check, but any data you send to the
server could be intercepted by others.
      Use insecure connections? (y/n): y

      Authentication required for https://api.shared-
na46.openshift.opentlc.com:6443 (openshift)
      Username: panni-redhat.com
      Password:
      Login successful.

      You don't have any projects. You can try to create a new project,
by running

          oc new-project
```

     - 注意，你可以使用`KUBECONFIG`环境变量来指定一个不同的配置文件。
     - 配置文件最初不一定存在，它在你登录时被更新。
     - 因为你登录了同一个集群，所以会创建一个包含相同信息的新文件。
   - 比较这两个配置文件。

```
$ ls -l $HOME/.kube/*config
-rw-------  1 panni  staff  681 May  1 19:05 /Users/panni/.kube/config
-rw-------  1 panni  staff  681 May  2 12:21 /Users/panni/.kube/new-
config
$ diff $HOME/.kube/config $HOME/.kube/new-config
18c18
<     token: ejOPm9PYhEqryocKv4W6tpOb3ZOqKEu7GXXXLJqsCH8
---
>     token: Y7kav_x-yR1zdCXBH2mGFwdvSTjbpsxqdXXXfzv89A4
```

- 注意，会话令牌是不同的。
- 你可以通过改变 `KUBECONFIG` 环境变量在集群和用户之间切换。

  提示：如果你打算从另一台机器上访问同一个集群，你可以把 `config` 文件和你的凭证带到那里。请注意，任何能够访问这个 `config` 文件的人都可以用你的用户名登录到集群。这意味着你必须始终保持它的安全和秘密。注意这个文件的 所有者只读不写 的权限。

  注意：如果你从别人的电脑上登录到集群，你的凭证会记录在那个人的 `$HOME/.kube/config` 文件中（或者在当时 `KUBECONFIG` 指向的文件中）。请确保在离开那台电脑之前，从其他人的电脑上删除你的会话信息，并 `oc logout`。

3. 在你当前的会话中，使用 `oc logout` 并注意在你注销后配置文件的不同。

```
$ oc logout
Logged "panni-redhat.com" out on "https://api.shared-
na46.openshift.opentlc.com:6443"
$ ls -l $HOME/.kube/*config
-rw-------  1 panni  staff  681 May  1 19:05 /Users/panni/.kube/config
-rw-------  1 panni  staff  629 May  2 12:35 /Users/panni/.kube/new-config
$ diff $HOME/.kube/config $HOME/.kube/new-config
17,18c17
<   user:
<     token: ejOPm9PYhEqryocKv4W6tpOb3ZOqKEu7GOgyLJqsCH8
---
>   user: {}
```

   - 请注意，你成功地从 `new-config` 文件中删除了你的会话令牌（目前设置为 `KUBECONFIG` 环境变量的值）。