

Lab 3.2. Аутентификация LDAP

Подготовка OpenShift

Цепочка сертификатов для сервера LDAP.

Поскольку FreeIPA выступает в качестве центра сертификации, это необходимо будет указать в окончательной конфигурации.

Скопировать с FreeIPA хоста на хост с кластером OpenShift сертификат

scp [username@dc.corp.local:/etc/ipa/ca.crt](#) .

Прим. В случае хоста Windows и CRC воспользуйтесь WinScp

Создайте проект:

Проект OpenShift - это альтернативное представление пространства имен Kubernetes.

oc project openshift-config

OAuth объект требует Secret для хранения пароля учетной записи от имени которой производится подключение к LDAP:

oc create secret generic ldap-secret --from-literal=bindPassword=пароль

Кроме Secret, цепочка центров сертификации FreeIPA должна находиться в объекте ConfigMap в пространстве имен openshift-config.

Создайте ConfigMap в командной строке:

oc create cm custom-ca-oauth --from-file=ca.crt=ca.crt -n openshift-config

Создайте объекта OAuth

The screenshot shows the 'Add Identity Provider: LDAP' configuration page in the OpenShift console. The left sidebar contains a navigation menu with categories: Networking, Storage, Builds, Observe, Compute, User Management, and Administration. Under Administration, 'Cluster Settings' is selected. The main content area is titled 'Add Identity Provider: LDAP' and includes the instruction 'Integrate with an LDAP identity provider.' The form contains the following fields:

- Name ***: A text input field containing 'ldap'. Below it is a note: 'Unique name of the new identity provider. This cannot be changed later.'
- URL ***: A text input field containing 'ldaps://dc.corp.local/cn=users,cn=accounts,dc=corp,dc=local?uid'. Below it is a note: 'An RFC 2255 URL which specifies the LDAP search parameters to use.'
- Bind DN**: A text input field containing 'uid=admin,cn=users,cn=accounts,dc=corp,dc=local'. Below it is a note: 'DN to bind with during the search phase.'
- Bind password**: A password input field with masked characters '.....'. Below it is a note: 'Password to bind with during the search phase.'

Lab 3.2. Аутентификация LDAP

Email

mail

The list of attributes whose values should be used as the email address.

+ Add more

More options

CA file

ca.crt

Browse...

-----BEGIN CERTIFICATE-----
MIIEiDCCAvcGAWIBAgIBATANBgkqhkiG9w0BAQsFADA1MRMwEQYDVQKDApDT1JQ
LkxPQ0FMMR4wHAYDVQQDBVDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwHhcNMjAy
MTQxMDQ1WWhcNNDQwMzAyMTQxMDQ1WjA1MRMwEQYDVQKDApDT1JQKxPQ0FMMR4w
HAYDVQQDBVDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggGiMA0GCsGSIb3DQEBAQUA
A4IBjwAwggGKAoIBgQCgyyS0uDDMFkhiY4mRSQ92k59DFDETLA58IN+9oxrV/yLP
Y0bwOG/xk9xDkkjwKiM1yGGrMej5TM1ZRNTqL2CRReIJ6S7DYKHEaFy40a6zBTpC0
LJDp/DsR0NArmaL0E0aPcLIqXHPNOHLDBwQSPWOWRw7nLF/OWxkoHm2wgwAq8v/u
E1a5dBR0zkXUyttsh+WNAw0L7UV3eyUQtIKJcwmNnCVcGzKU/f3ISyIJ7rmRGyp5
sf9D9ASR+o8QZP8D1ZkfQVGQFZ02nHIRqi7JxAutVwe/5/IjZ218FLS7jiJxA1J
/hGoIY0uMX2TsM0AYZ1WvOJfmst9jeHeJb5R+30PBIW+YNTCq9WmF/00D9HJrVyO
JDJxdMcHreIuPkrBkESv0vPiTVFS3rEq6C4SVpA0KE4Dio/8XYEeQLnzdeE1kSc6
vbST8u1wG+NopFoY0/1o8ACbB+IEvPZMB2ZtJAVtGUSewHOGWNA16K0qvgv5uKHW
qe2bQWokZWpduP4S8cCAwEAAaOBojCBnzAfBgNVHSMEGDAWgBS3E3KJZYIXyJ

Add Cancel

Откройте на редактирование и приведите значения параметров name для bindPassword и са указанным вами при создании объектов secret и ConfigMap ранее в командной строке:

Configuration > OAuth details

cluster

Details YAML

```
80 - cn
81   preferredUsername:
82   - uid
83   bindDN: "uid=admin,cn=users,cn=accounts,dc=corp,dc=local"
84   bindPassword:
85     name: ldap-secret
86   ca:
87     name: custom-ca-oauth
88   insecure: false
89   url: "ldaps://dc.corp.local/cn=users,cn=accounts,dc=corp,dc=local?uid"
90   mappingMethod: claim
91   name: ldap
92   type: LDAP
93   templates:
94     login:
95       name: login-template
96   tokenConfig:
97     accessTokenMaxAgeSeconds: 0
98
```

Actions

- Edit labels
- Edit annotations
- Edit OAUTH
- Delete OAUTH

Save Reload Cancel Download

Нажмите Save затем Reload.

Lab 3.2. Аутентификация LDAP

Теперь можно войти в веб-консоль <https://oauth-openshift.apps-crc.testing> под новым доменным пользователем:

Log in with

developer

ldap

Log in to your account

Open a terminal and run 'crc console --credentials' to get your credentials.

Username *

ldapuser

Password *

.....

Log in

Если зайти как администратор, то можно увидеть ldapuser в списке пользователей:

Red Hat

OpenShift

Networking >

Storage >

Builds >

Observe >

Compute >

User Management ▾

Users

Users

Users are automatically added the first time they log in.

Name ▾

Search by name... /

Name ⓘ	Full name ⓘ	Identities ⓘ
developer	-	developer:developer ⋮
kubeadmin	-	developer:kubeadmin ⋮
ldapuser	Ldap User	ldap:dWIkPWwkYXB c2VyLGNuPXRvZXJzLGNuPWFjY291bnRzLGRJPWNvcnAsZGM9bG9jYWw ⋮