

Эксплуатация Apache NiFi на базе платформы Arenadata Streaming



Эксплуатация Arenadata Streaming (Kafka, NiFi)



Agenda

- Основные этапы установки и подготовка инфраструктуры:
- Распределение компонент. Планирование установки. Установка основных компонент. Лабораторная работа.
- Керберизация ADS/ADPS:
 - Распределение компонент. Планирование установки. Установка основных компонент. Лабораторная работа.
- Настройка LDAP sync source для Ranger User synchronizer.
- Настройка SSL/LDAP for ADS NiFi.

Основные этапы установки и подготовка инфраструктуры

Основные компоненты и экосистема. Безопасность кластеров. Сравнение редакций продуктов

Основные этапы установки

- Конфигурирование кластера ADPS
- Настройка Kerberos на кластере ADPS с Active Directory в качестве KDC
- Настройка Kerberos на кластере ADS с Active Directory в качестве KDC
- Включение SSL: NiFi SSL и NiFi LDAP Auth
- Включение ADPS SSL
- Настройка Kerberos на кластере ADPS и включение плагинов Ranger
- Проверка работоспособности сервисов
- Постнастройка сервисов (Ranger Policy, Security Zones, ...)

Распределение компонент ADPS



Кластер	Сервис	Компонент	ads-a-<##>-adps
Arenadata Platform Security	Ranger	Ranger Admin	1
		Ranger KMS	1
		Ranger User Synchronizer	1
	MySQL	MySQL Master Server (БД ranger, rangerkms)	1
	Solr	Solr Server	1
	Zookeeper	Zookeeper Server	1
Всего компонент			6

Установка кластера ADPS

Общая схема установки кластера:

- Создать кластер ADPS.
- Добавить и настроить сервисы кластера: Zookeeper, MySQL, Ranger, Solr.
- Добавить в кластер хосты ADPS и распределить компоненты.

Установка кластера ADPS

- Создаем и настраиваем узел ADPS в ADCM
- Создаем кластер ADPS:

Create cluster

Product
Platform security

Product version
1.0.5_b2-1 (enterprise)

Cluster name
ADPS

Description
Description

☒ I accept [Terms of Agreement](#)

Cancel Create

- Добавляем сервисы кластера: Zookeeper, MariaDB(MySQL), Ranger, Solr:

Add services

☐ All services

Search services

☐ Knox

☒ MariaDB

☐ Monitoring

☒ Ranger

☒ Solr

☒ Zookeeper

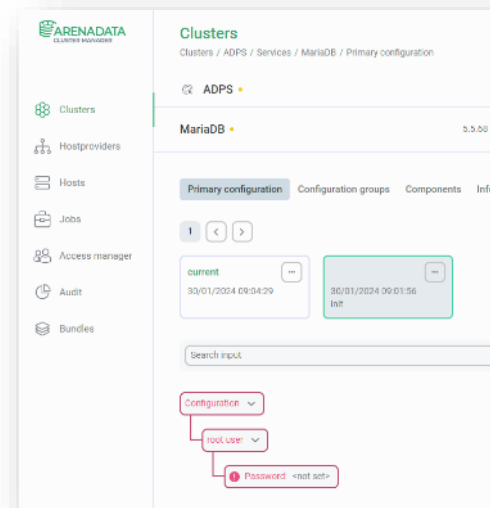
Cancel Add



Name ↓	Version	State	Concerns	Actions
MariaDB	5.5.68	created		
Ranger	2.5.0_arenadata2	created		
Solr	8.11.3	created		
Zookeeper	3.8.4_arenadata1	installed		

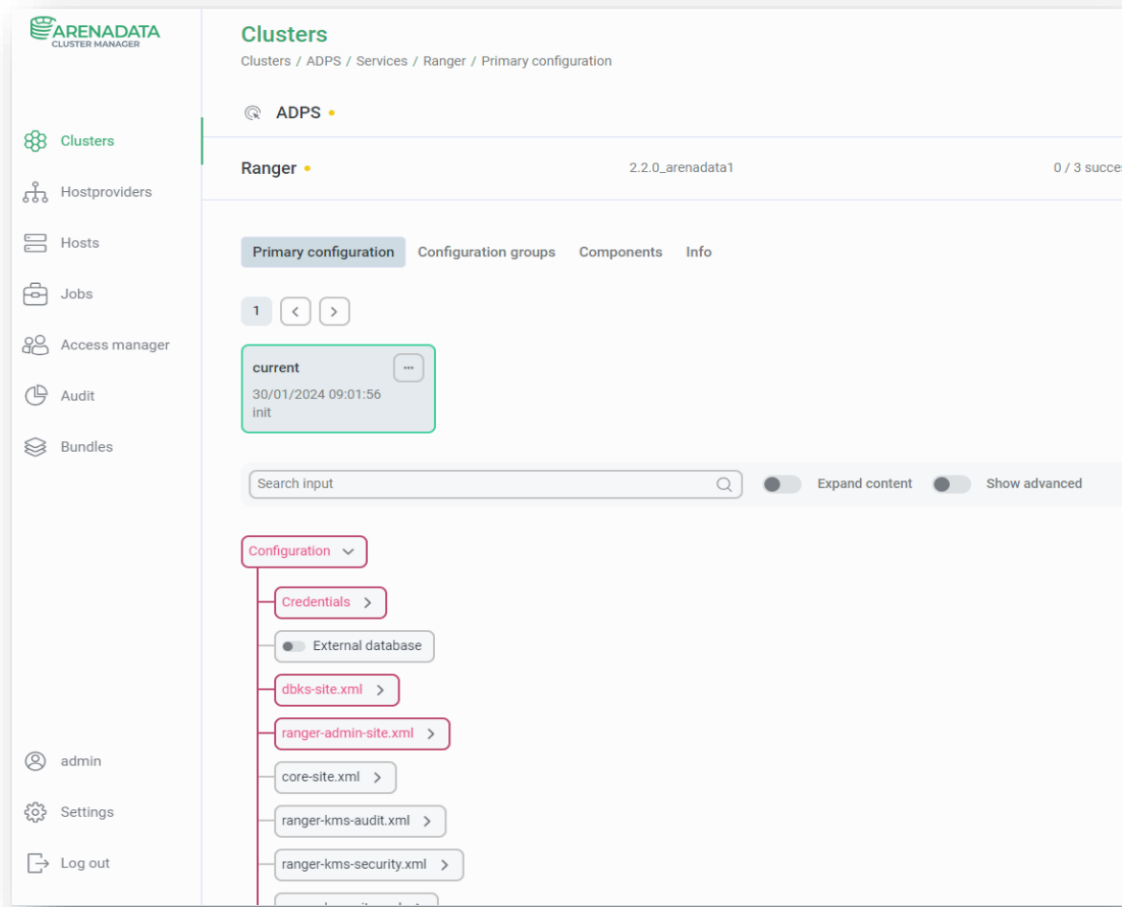
Установка кластера ADPS. MySQL

- Указываем пароль суперпользователя MariaDB(MySQL для версий ADPS старше 1.0.4):



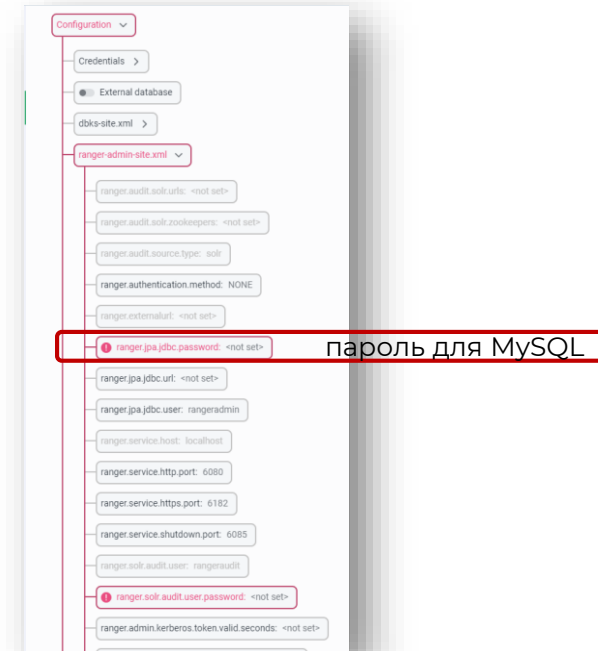
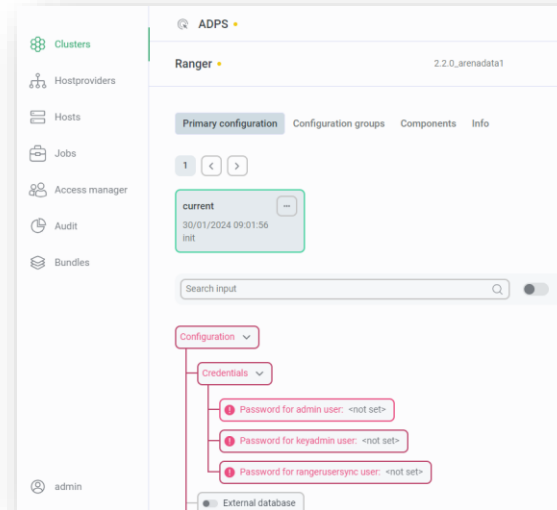
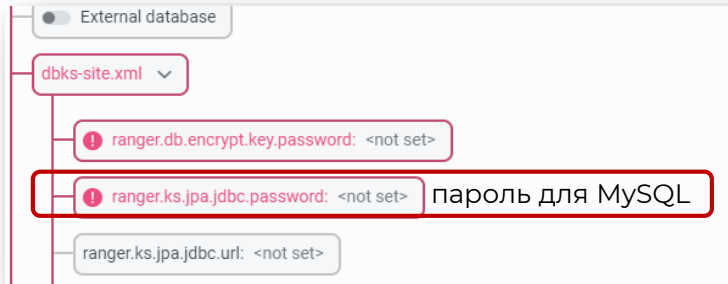
Установка кластера ADPS. Ranger

- Настраиваем сервис **Ranger**, указываем пароли:



Установка кластера ADPS. Ranger

- Настраиваем сервис Ranger, указываем пароли:



Ranger user password requirements:

- Minimum of 8 characters
- Must include at least one alphabetical and one numerical character
- Must not include the following unsupported special characters: " ' \ `

Ranger and Ranger KMS DB user password requirements:

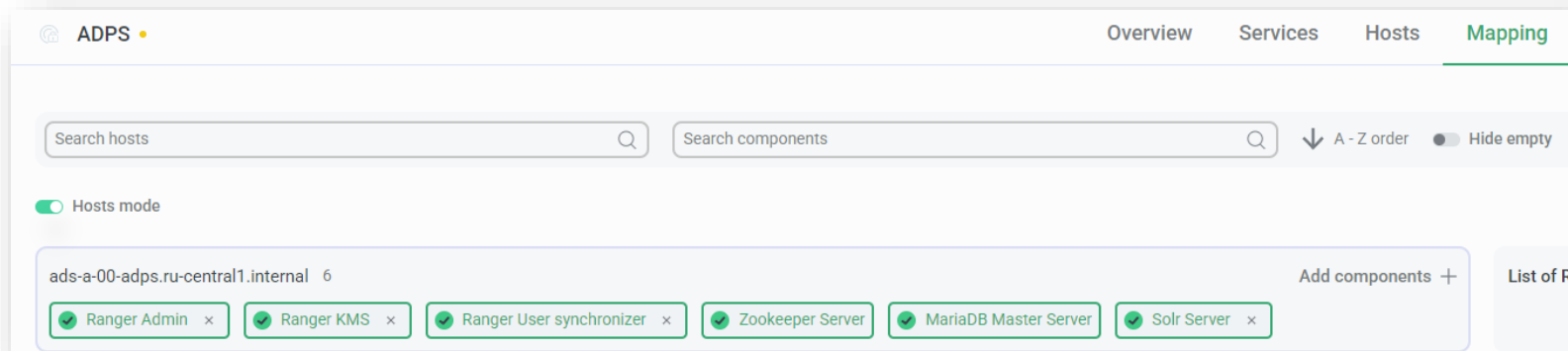
- Must not include the following unsupported special characters: " ' \ `

Ranger database instance password requirements:

- Refer to the password requirements for the applicable database type (MySQL, PostgreSQL, Oracle, etc.)

Установка кластера ADPS. Mapping

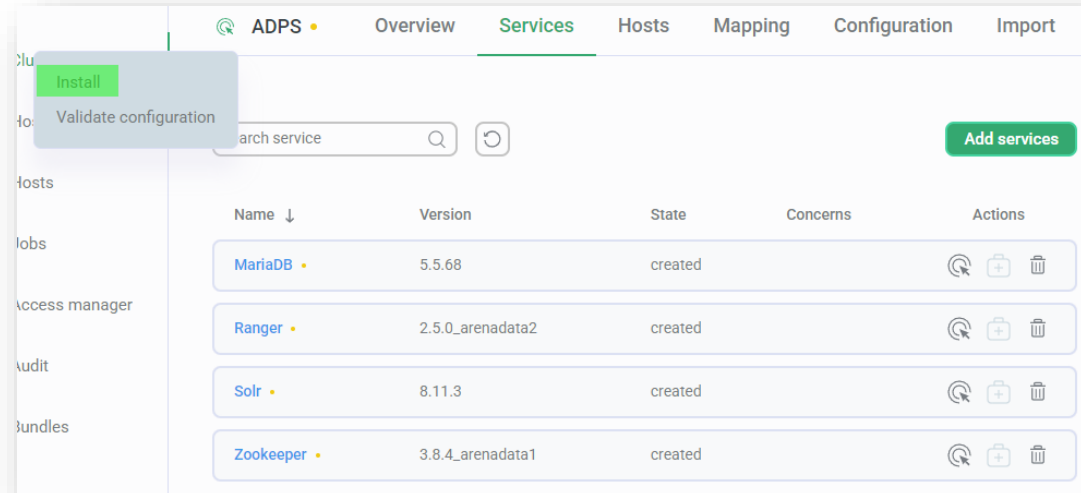
- Добавляем хосты кластера и распределяем компоненты:



***ОБЯЗАТЕЛЬНО ПРОВЕРЬТЕ ПРАВИЛЬНОСТЬ РАСПРЕДЕЛЕНИЯ КОМПОНЕНТ И СРАВНИТЕ ИХ КОЛИЧЕСТВО В СООТВЕТСТВИИ С ПОСЛЕДНЕЙ СТРОКОЙ ТАБЛИЦЫ!!!**

Установка кластера ADPS. Imports

- Запускаем Action Install



Лабораторная работа

1. Выполнить установку кластера через ADPS на узлы:

`ads-a-XX-adps.ru-central1.internal`

2. Проверить работу сервисов.

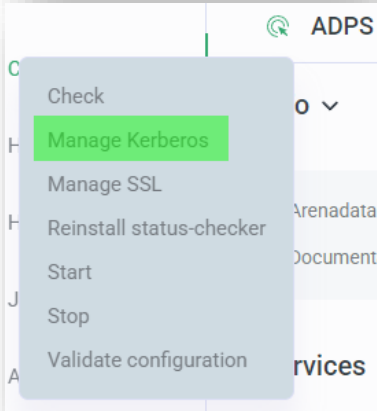
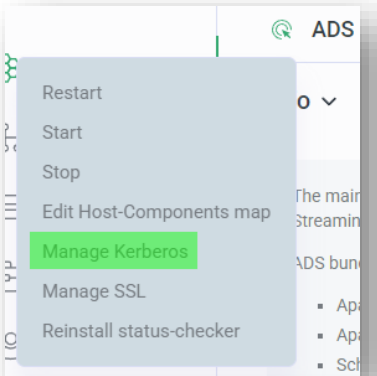
Керберизация ADS/ADPS

Керберизация ADS/ADPS: Active Directory

Для настройки *Kerberos* кластера ADS/ADPS необходимо выбрать действие:

CLUSTERS -> <Кластер> -> Manage Kerberos и заполнить поля:

Поле	Значение
KDC hosts	winda-test-1.adh-sec.com
Realm	ADH-SEC.COM
Domains	adh-sec.com .adh-sec.com
Kadmin server	winda-test-1.adh-sec.com
Kadmin principal	ads-admin XX
Kadmin password	*****
Admin DN	CN=ads-admin XX ,OU=USERS,OU=Student XX ,OU=ADS,OU=Learning,DC=adh-sec,DC=com
LDAP URL	ldaps://winda-test-1.adh-sec.com
Container DN	OU=PRINCIPALS,OU=Student XX ,OU=ADS,OU=Learning,DC=adh-sec,DC=com
TLS CA certificate Path	/usr/local/share/ca-certificates/ca-test.crt
TLS CA certificate (optional)	-----BEGIN CERTIFICATE----- ... -----END CERTIFICATE-----



Run an action: Enable Kerberos

Search input 🔍 Expand

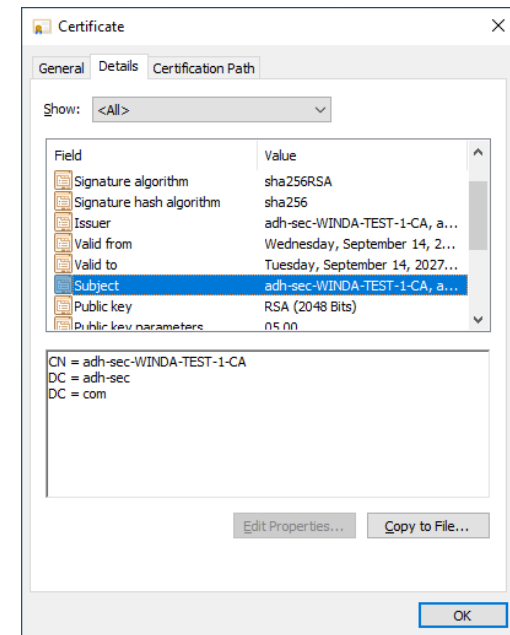
Configuration ▾

- ☐ Existing MIT KDC
- ☒ Existing Active Directory ▾
 - ! KDC hosts: <not set> >
 - ! Realm: <not set>
 - Domains: <not set> >
 - ! Kadmin server: <not set>
 - ! Kadmin principal: <not set>
 - ! Kadmin password: <not set>
 - ! Admin DN: <not set>
 - ! LDAP URL: <not set>
 - ! Container DN: <not set>

Установка CA TLS-сертификата Active Directory

- LDAP:389
- LDAPS:636, over SSL/TLS
- Arenadata Hadoop и Platform Security позволяет использовать сертификаты (самоподписанные) для обеспечения работы по LDAPS.
- Необходимо:
 1. Получить CA сертификат в формате X.509 (*.cer, *.pem).
 2. Добавить полученный сертификат на узлы кластера.

```
# *.cer -> *.pem:  
openssl x509 -inform der -in ca-test.cer -outform pem -out ca-test.pem
```



Установка CA TLS-сертификата Active Directory

Добавление сертификата использованием ADCM:

- Заполнить поля *TLS CA certificate Path* и *TLS CA certificate (optional)*.
- Выполнить Керберизацию кластера.
- После Керберизации кластера будут созданы `/usr/local/share/ca-certificates/ca-test.crt` на всех узлах кластера с содержимым:

```
-----BEGIN CERTIFICATE-----
```

```
MIIDezCCAmOgAwIBAgIQOZQ17d3i8IFHVILb8HdoNjANBgkqhkiG9w0BAQsFADBQ
```

```
...
```

```
-----END CERTIFICATE-----
```

- Необходимо на всех узлах кластера выполнить команду:

```
sudo update-ca-certificates
```

- Проверить настройки файла `/etc/ldap/ldap.conf`:

```
#  
# LDAP Defaults  
#  
...  
SASL_NOCANON    on  
TLS_CACERT /usr/local/share/ca-certificates/ca-test.crt
```

- Проверить наличие сертификата в хранилище.

Лабораторная работа

Выполнить керберизацию (KDC Active Directory) кластеров ADS и ADPS с СА сертификатом ca-test.cer:

```
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIQOZQ17d3i8IFHVILb8HdoNjANBgkqhkiG9w0BAQsFADBQ
MRMwEQYKCZImiZPyLGBGRYDY29tMRcwFQYKCZImiZPyLGBGRYHYWRoLXNIYzEg
MB4GA1UEAxMXYWVwRoLXNIYy1XSU5EQS1URVNULTetQ0EwHhcNMjIwOTE0MTkyMTE0
WhcNMjIwOTE0MTkyMTE0WjBQMwEYKCZImiZPyLGBGRYDY29tMRcwFQYKCZIm
iZPyLGBGRYHYWRoLXNIYzEgMB4GA1UEAxMXYWVwRoLXNIYy1XSU5EQS1URVNULTet
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDNHoZtp2zHmi9r4OYU
yKSG5oVKOsKuaXt1hy2GEBmD1ChQ8IOGidPz4tUxHPPWZ7My8VRLjklrACjq2qRQ
yPb1nPtyhviYocIHUfFuLhNJYx/tX0j9HSrMBTFFr+zq8bSljgDnqtye12xoOwA
RdH2eLIJvPeXWO/owkMS+IX1xsaPfUQZcLVWFwvhjzhUlKpgEz9HeVytIkKF7GhE
YSHLWnk/6tst5+eRvfzCE6+YUydABN4ksnQokyKRkbDnX7ay0Gom2lmcKlhHIW+Q
uVKu7u15tSzPssZhYr+pEmjQbkRtbOGSQQMYDJM8FgqSUBI2APYfdJuREV/5UsR2
dufRAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBIuf4TS/zVzW6MZOSIJF0JNEDCiDAQBgkrBgEEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQsFAAOCAQEAE5TY3VpNtCxzJA09pvJkNK4m417Gcb0EkNcl+fgpxM/T
EV9LdW8cRjrfKH/5E5dpxpPN1GEFdq3JNelurdTsCoOmwv1luxM4u8vPqbPTbfYz
2hb7uFZp48lx8swlVRk2nKfb0u3VBaol6wy10R9EZ9T4/5H9TMAgofcFJcD812K3
FLlxUUR+DzKMHCfekuUcqSI8yRnTvKSGPKPlu3O5dQg4f0iummjd5JqGEb52Qg0G
//zQCllwWSTJ8qb0MDvhGY2tmH4C0Mk17TRZ8W+i/RpBLPjVQ08bl6NR7O2bhFQS
EjOI0fKuB/FPEk2DgGk6iWzm1EGTt4uxOHnTgyqq5w==
-----END CERTIFICATE-----
```

Настройка LDAP sync source для Ranger User synchronizer

Ranger User synchronizer

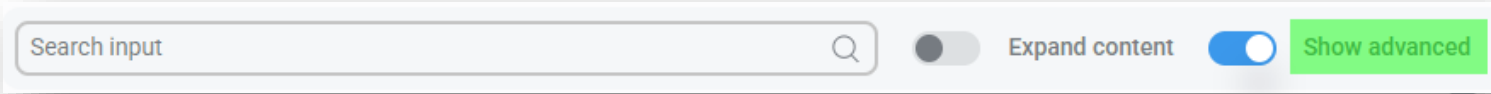
- UserSync позволяет синхронизировать пользователей и группы из Unix, LDAP или Active Directory.
- Информация о пользователях или группах хранится в Ranger Admin.
- Можно настраивать для пользователей и групп политики.

Особенности:

- Синхронизация в «одну сторону». Информация об объектах считывается из внешней системы и загружается в Ranger Admin.
- UserSync не синхронизируется в реальном времени и настраивается отдельно.
- Не поддерживает удаление пользователей из внешней системы. Удаление только из локальной базы данных Ranger Admin

Настройка Ranger User synchronizer

- В ADCM открываем настройки Ranger: CLUSTERS -> ADPS -> Services -> Ranger ->Primary Configuration
- Активировать переключатель Show advanced
- Активизируем переключатель LDAP sync source for User synchronizer и заполняем необходимые поля, остальные можно оставить без изменений:



Поле	Значение
ranger.usersync.ldap.binddn	CN=ads-adminXX,OU=USERS,OU=StudentXX,OU=ADS,OU=Learning,DC=adh-sec,DC=com
ranger.usersync.ldap.deltasync	True
LDAP bind password	ads@2015
ranger.usersync.ldap.searchBase	OU=StudentXX,OU=ADS,OU=Learning,DC=adh-sec,DC=com
ranger.usersync.ldap.url	ldaps://winda-test-1.adh-sec.com
ranger.usersync.ldap.user.searchbase	OU=StudentXX,OU=ADS,OU=Learning,DC=adh-sec,DC=com
ranger.usersync.group.searchenabled	True
ranger.usersync.group.search.first.enabled	false
ranger.usersync.group.usermapsyncenabled	True
ranger.usersync.group.objectclass	group
ranger.usersync.group.searchbase	OU=StudentXX,OU=ADS,OU=Learning,DC=adh-sec,DC=com

Проверка настройки Ranger User synchronizer

- Перейти на узел с установленным Ranger Admin и авторизоваться под локальным пользователем admin.
- Перейти во вкладку Settings → Users
- В строке поиска найти пользователя USER NAME: ads-adminXX.
- Аналогично проверить для групп: Settings → Groups
- Просмотреть информацию в лог-файле
`/var/log/ranger/usersync/usersync-ads-a-XX-adps.ru-central1.internal-ranger.log`

Лабораторная работа

1. Настроить Ranger User synchronizer для ADPS.
2. Проверить синхронизацию.

Настройка LDAP/AD auth для Ranger Admin (опционально)

Настройка Ranger Admin User auth AD

- В ADCM для свойства `ranger.authentication.method(ranger-admin-site.xml)` в конфигурации Ranger выбрать значение **ACTIVE_DIRECTORY**
- В ADCM открываем настройки Ranger: CLUSTERS → ADPS → Services → Ranger → Primary Configuration
- Активируем переключатель Active Directory sync source for Ranger Admin authentication и заполняем необходимые поля, остальные можно оставить без изменений:

Поле	Значение
ranger.ldap.ad.url:	ldaps://winda-test-1.adh-sec.com:636
ranger.ldap.ad.bind.dn	CN=ads-admin XX ,OU=USERS,OU=Student XX ,OU=ADS,OU=Learning,DC=adh-sec,DC=com
ranger.ldap.ad.bind.password	adh@2015
ranger.ldap.ad.base.dn	OU=Student XX ,OU=ADS,OU=Learning,DC=adh-sec,DC=com
ranger.ldap.ad.domain	adh-sec.com

- Выполнить действие Restart для сервиса Ranger.

Проверка настройки Ranger Admin User auth AD

- Перейти на узел с установленным Ranger Admin и авторизоваться пользователем ads-adminXX.
- Проверить на вкладке Rager Admin → Audit → Login Sessions авторизацию пользователей.
- В файле `/var/log/ranger/admin/ranger-admin-ads-a-XX-adps.ru-central1.internal-ranger.log` найти информацию авторизации пользователя:

```
<date>,488 [http-bio-6080-exec-3] INFO  org.apache.ranger.biz.SessionMgr (SessionMgr.java:445) - adminXX is a valid user
```

```
<date>,829 [http-bio-6080-exec-3] INFO  org.apache.ranger.biz.SessionMgr (SessionMgr.java:232) - UserSession Updated to set new Permissions to User: adminXX
```

```
<date>,830 [http-bio-6080-exec-3] INFO  org.apache.ranger.biz.SessionMgr (SessionMgr.java:184) - Login Success: loginId=adminXX, sessionId=329, sessionId=9FE094FAC675621AD120EBB9B7D160EB, requestId=10.129.0.XXX, epoch=1668578296830
```

Замечание. Для синхронизации по LDAPS, на хост Ranger в директорию `/etc/pki/ca-trust/source/anchors/` необходимо скопировать сертификат Active Directory.

Лабораторная работа (опционально)

1. Настроить Ranger User auth AD для ADPS.
2. Проверить синхронизацию.

Присоединение узлов к Active Directory

SSSD

System Security Services Daemon (SSSD) – это пакет приложений для управления аутентификацией и авторизацией

Возможности и особенности:

- Локальное кэширование данных идентификации и информации о группах;
- Стандартные интерфейсы PAM и NSS для клиентов;
- Аутентификация и авторизация;
- Альтернатива **Samba**



https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system-level_authentication_guide/sssd
<https://sssd.io/docs/ad/ad-introdu>

SSSD/realmd. Присоединение узлов

Присоединение клиентов к Active Directory необходимо для корректной работы политик Ranger с группами пользователей и сервисов ADS: Kafka

Основные этапы настройки:

1. Разрешение имён и необходимые пакеты;
2. Присоединение к домену AD;
3. Тестирование аутентификации и авторизации для пользователей и групп;

SSSD/realmd. Присоединение узлов

1. Разрешение имён и необходимые пакеты:

- Изменяем содержимое файла `/etc/resolv.conf`:
`search adh-sec.com`
`nameserver 10.129.0.XXX`
- Проверяем доступность домена `adh-sec.com` и имени контроллера AD (`ping`, `nslookup`);
- Устанавливаем пакеты: `sssd-ad sssd-tools realmd adcli oddjob oddjob-mkhomedir`
- Проверяем наличие домена AD (`realm discover`)

SSSD/realmd. Присоединение узлов

2. Присоединение к домену AD:

- Определяем статус принадлежности к домену каждого клиента (realm list);
- Присоединяем клиента к домену (realm join). Пользователь должен иметь необходимые привилегии в AD;
- Проверяем принадлежность домену AD со стороны клиента и сервера (realm list, ldapsearch);
- Изменяем параметр use_fully_qualified_names = False в /etc/sss/sss.conf
- Перезапускаем сервис Kafka;
- Очищаем кэш (/var/lib/sss/db/*, /var/lib/sss/mc/*) и перезапускаем службу SSSD (stop + clear cache + start)

3. Тестирование аутентификации и авторизации для пользователей и групп:

- Проверка пользователя и его групп (id <username>@adh-sec.com, id <username>, groups <username>).

Лабораторная работа

1. Добавить в домен adh-sec.com узлы:

ads-a-XX-node-1;

ads-a-XX-node-2;

ads-a-XX-node-3.

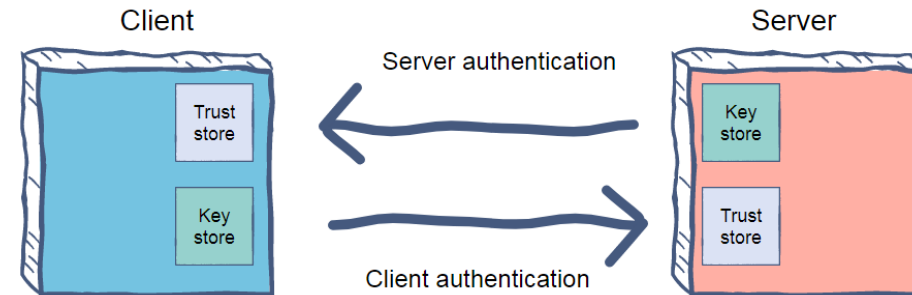
2. Выполнить необходимые проверки и для пользователя ads-adminXX

Настройка SSL/LDAP for ADS NiFi

Шифрование данных

SSL Keystore Management Factory:

- Поддерживает ключи в формате JKS.
- Поддерживает переключение между HTTP и HTTPS.
- Поддерживает двустороннюю проверку сертификата и имени.
- Использует общее расположение хранилища ключей и хранилища доверенных сертификатов, доступное другим службам.
- Позволяет централизованно управлять SSL и распространять изменения на весь кластер и узлы.
- Автоматически перезагружает хранилище ключей и хранилище доверенных сертификатов без перезапуска служб.



Шифрование данных: KeyStore и TrustStore

- KeyStore и TrustStore – это хранилища криптографических публичных и частных ключей и сертификатов. Обычно они представляются файлами формата .jks, .dks, .p12, и другими, в зависимости от типа хранилища.
- KeyStore и TrustStore устроены похоже, но служат разным целям. KeyStore хранит данные о *нашем* приложении, тогда как TrustStore – о других, *которым мы доверяем*.
- По умолчанию в приложении подключен один TrustStore, файл jre/lib/security/cacerts

KEYSTORE

Хранятся ваши приватные ключи и сертификаты (клиентские или серверные)

Необходим для настройки SSL на сервере

Клиент будет хранить свой приватный ключ и сертификат в keystore

javax.net.ssl.keyStore используется для работы с keystore

TRUSTSTORE

Хранятся доверенные сертификаты (корневые самоподписанные CA root)

Необходим для успешного подключения к серверу на клиентской стороне

Сервер будет валидировать клиента при двусторонней аутентификации на основании сертификатов в trustStore

javax.net.ssl.trustStore используется для работы с trustStore

<https://www.pvsm.ru/java/345876>

Шифрование данных: KeyStore и TrustStore

- Формат сертификатов:

.jks — это хранилище ключей Java является наиболее распространенным типом хранилища ключей по умолчанию.

.jseks — это хранилище ключей для расширения криптографии Java (имеет все функции JKS с большим количеством разрешенных алгоритмов).

.p12 или PKCS12 — это тип хранилища ключей для Java и других языков. В отличие от JKS, вы можете извлечь закрытые ключи из PKCS#12.

PKCS11 или .p11 реже используются для доступа к аппаратным криптографическим токенам, таким как сетевые карты.

.bks — это поставщик BouncyCastle, используемый на Android и мобильных устройствах.

Шифрование данных

Основные этапы настройки SSL:

- создать сертификат для каждого узла, используя алгоритм RSA 2048. CN должно быть полным доменным именем соответствующего узла.
- Создать хранилище ключей `trustore.jks`, которое будет содержать необходимые сертификаты. Для запуска SSL необходимо указать путь к этому хранилищу.
- Сертификаты должны быть подписаны ключом, принадлежащим одному из доверенных корневых сертификатов, входящих в хранилище сертификатов Java. Самоподписанные сертификаты поддерживаются. В этом случае корневой сертификат необходимо добавить в хранилище `trustore.jks`.
- Сертификат OpenSSL для вашего имени хоста должен быть добавлен в хранилище `ca-bundle.crt`.
- Учетная запись, используемая для установки сертификатов, должна иметь права на запись:
`/etc/ssl/`

Основные этапы настройки SSL (1,2)

1. Генерируем закрытый ключ на любом узле для дальнейшей подписи запроса:

```
openssl genrsa -aes128 -out private-<host>.key 2048
```

Password: bigdata

private-<host>.key:

```
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4, ENCRYPTED
```

```
DEK-Info: AES-128-CBC, 51EE8122CBDCB3047CF8A4A5F5F372BE
```

```
9EsneNAA+eULAn4eZCwcmIOeE3CsR/NaFop0kggy3aEgFUwe5Bu7Je9axfYaUeus
```

```
...
```

```
SnAKlREmXerP0Rp4F8IL51daR1yY947q6PFz0MDWUaK9nex0TRQMtHZm1t85isb5
```

```
-----END RSA PRIVATE KEY-----
```

2. Генерируем публичный ключ для созданного private.key (опционально):

```
openssl rsa -in private-<host>.key -pubout -out public.key:
```

public.key:

```
-----BEGIN PUBLIC KEY-----
```

```
MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA1I6YAX59mk8fqldckOW9
```

```
RwIDAQAB
```

```
-----END PUBLIC KEY-----
```


Основные этапы настройки SSL (3,4)

3. Создаем файл(csr-<host>.cnf) запроса сертификата. Сформируем данные сертификата и укажем все узлы кластеров ADS, ADPS:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
C = RU
ST = MSK
L = Moscow
O = ARENADATA
OU = ARENADATA
CN = ads-a-XX-<host>.ru-central1.internal
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = ads-a-XX-<host>.ru-central1.internal
```

4. Создадим запрос на подпись сертификата, с использование ранее созданного private.key:

```
openssl req -new -config csr-<host>.cnf -key private-<host>.key
-out cert-<host>.csr -passin pass:bigdata
```

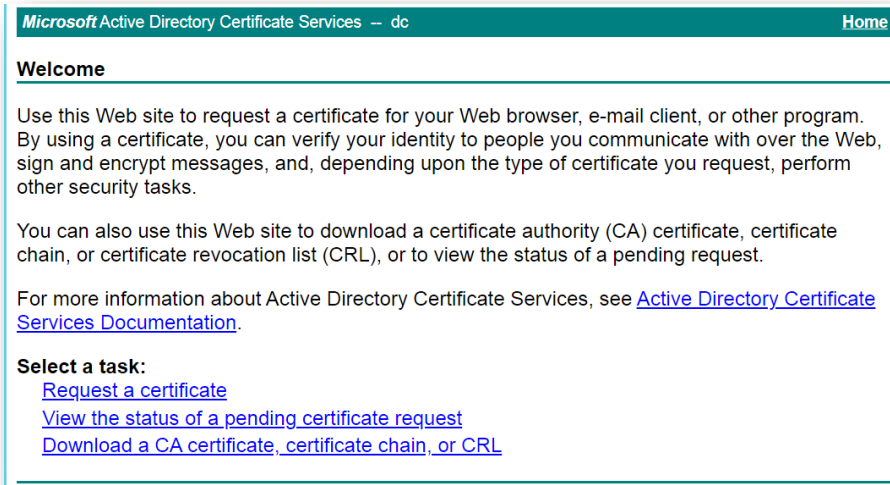
Запрос на подпись cert-.csr:

```
-----BEGIN CERTIFICATE REQUEST-----
MIID9DCCAtwCAQAwZjELMAkGA1UEBhMCU1UxDzANBgNVBAGMBk1PU0NPVzEPMA0G
...
WcZ00JbuHCco8jLaV8ptd6X12FkgAUAi4WTM+Cv1LPYixa8njvypIZ6NcCmnnKFt
m3921PXP2UY=
-----END CERTIFICATE REQUEST-----
```

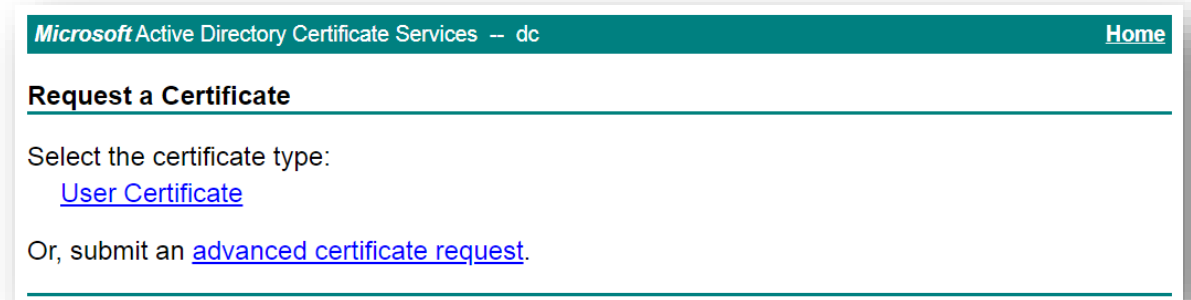
Основные этапы настройки SSL (5)

5. Выпуск подписанного сертификата Microsoft CA:

5.1. Открываем адрес http://<ip_адрес_сервера>/certsrv/:



5.2. Request a certificate -> Or, submit an advanced certificate request:

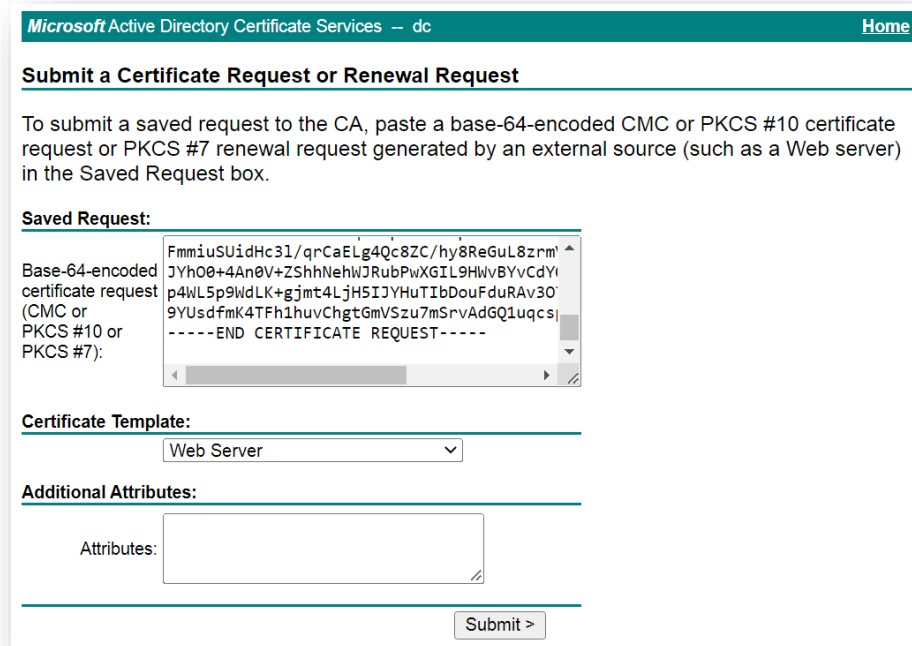


Основные этапы настройки SSL (5)

5. Выпуск подписанного сертификата Microsoft CA:

5.3. Далее **Certificate Template** → **Web Server** и **Submit** и вставляем содержимое файла запроса (cert-<host>.csr) на подпись сертификата в форму:

5.4. Выбираем **Base64 encoded, download certificate and certificate chain** :



Microsoft Active Directory Certificate Services — dc Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
FmmiuSUIdHc3l/qrcAEIg4Qc8ZC/hy8ReGuL8zrm'
JYh00+4An0V+ZShhNehWJRubPwXGIL9HWvBYvCdYf
p4WL5p9WdLK+gjmt4LjH5IJYHuTIbDouFduRAv30'
9YUdfmK4TFh1huvChgtGmVSzu7mSrvAdGQ1uqcsj
-----END CERTIFICATE REQUEST-----
```

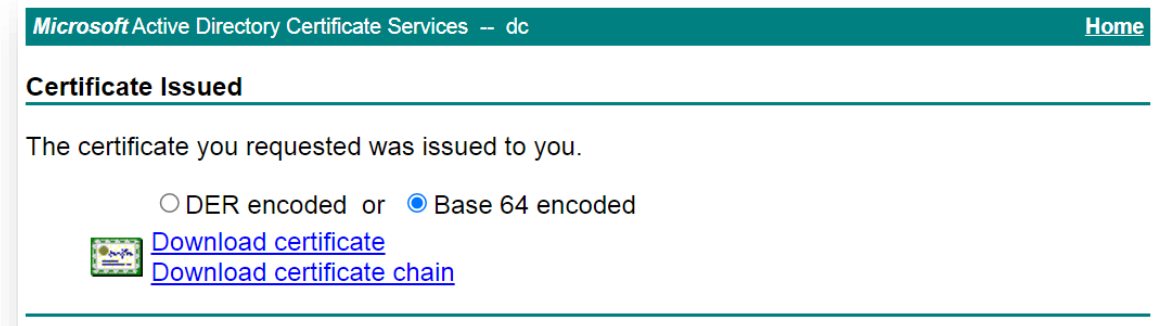
Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >




Microsoft Active Directory Certificate Services — dc Home

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

 [Download certificate](#)

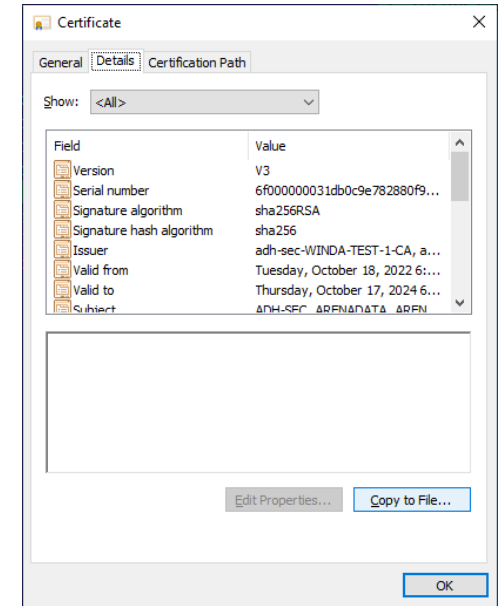
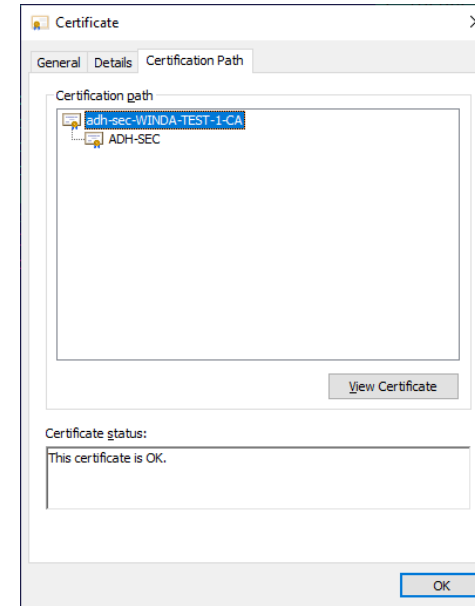
[Download certificate chain](#)

Получили сертификат клиента (cert-<host>.cer) и цепочку сертификатов в формате p7b (cert-chain-<host>.p7b).

Основные этапы настройки SSL (5)

5. Выпуск подписанного сертификата Microsoft CA:

5.5. Сертификат содержит данные цепочки на вкладке Certification Path:



Получение сертификатов в формате .cer:

Способ 1 (опционально). Выгрузить сертификаты можно по отдельности (на вкладке Details → Copy to File...) для каждого элемента в Certification Path

Способ 2. Выгрузить всю цепочку полностью в формат .pem :

```
openssl pkcs7 -in cert-chain-<host>.p7b -print_certs -out chain.pem
```

Основные этапы настройки SSL (6)

6. Создание клиентского и CA сертификатов в формате .cer:

Способ 2. Выгрузить всю цепочку полностью в формат .pem:

```
openssl pkcs7 -in cert-chain.p7b -print_certs -out chain.pem
```

Файл цепочки сертификатов chain.pem:

```
subject=/C=RU/ST=MSK/L=Moscow/O=ARENADATA/OU=ARENADATA/CN=ADH-SEC  
issuer=/DC=com/DC=adh-sec/CN=adh-sec-WINDA-TEST-1-CA
```

```
-----BEGIN CERTIFICATE-----
```

```
MIISPjCCESagAwIBAgITbwAAAAMdsMnngogPkgAAAAAAzANBgkqhkiG9w0BAQsF
```

```
...
```

```
XOHo6+M+ytwnGnd1kX7e17z0/kMjjPcyPf5sAxSmuMlSxQmSMcXu0+skpXH15fT0  
ObXU1D+KQ57x4v4u18tmxR/t
```

```
-----END CERTIFICATE-----
```

```
subject=/DC=com/DC=adh-sec/CN=adh-sec-WINDA-TEST-1-CA
```

```
issuer=/DC=com/DC=adh-sec/CN=adh-sec-WINDA-TEST-1-CA
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIDezCCAmOgAwIBAgIQOZQ17d3i8IFHVILb8HdoNjANBgkqhkiG9w0BAQsFADBQ
```

```
...
```

```
EjOI0fKuB/FPEk2DgGk6iWzm1EGTt4ux0HnTgyqq5w==
```

```
-----END CERTIFICATE-----
```

В цепочке присутствуют клиентский сертификат (большее количество строк) и сертификат корневого сервера.

Основные этапы настройки SSL (6)

6. Создание клиентского и CA сертификатов в формате .cer:

Необходимо создать отдельные файлы для каждого сертификата в таком виде:

Корневой сертификат `ca-<CA-host>.pem` (`ca-<CA-host>.cert`):

```
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIQOZQ17d3i8IFHVILb8HdoNjANBgkqhkiG9w0BAQsFADBQ
...
EjOI0fKuB/FPEk2DgGk6iWzm1EGTt4uxOHnTgyqq5w==
-----END CERTIFICATE-----
```

Клиентский сертификат `cert-<host>.cer`:

```
-----BEGIN CERTIFICATE-----
MIISPjCCESagAwIBAgITbwAAAAMdsMnngogPkgAAAAAAAzANBgkqhkiG9w0BAQsF
...
XOHo6+M+ytwnGndlkX7el7zO/kMjjPcyPf5sAxSmuMISxQmSMcXuO+skpXHl5fTO
ObXU1D+KQ57x4v4ul8tmxR/t
-----END CERTIFICATE-----
```

Замечание. Сертификат `ca-<CA-host>.pem` уже был получен ранее при настройке TLS сертификата для LDAP в разделе Керберизации ADS и ADPS.

Его путь в локальной системе `/usr/local/share/ca-certificates/ca-test.crt` на каждом узле кластера.

Основные этапы настройки SSL (7)

7. Создаем хранилище доверенных сертификатов на ВСЕХ УЗЛАХ КЛАСТЕРА и для ВСЕХ СЕРТИФИКАТОВ.

Пароль для всех пунктов: bigdata

7.1. Сначала импортируем корневой сертификат в формате base64:

```
keytool -import -keystore truststore.jks -noprompt -trustcacerts -alias root -file ca-<CA host>.pem -storetype jks -storepass bigdata
```

7.2. Опционально. Далее импортируем промежуточные сертификаты, если есть (для нашего случая, они отсутствуют).

```
keytool -import -keystore truststore.jks -trustcacerts -alias intermediate -file intermedia.cer -storetype jks
```

7.3. Импортируем клиентские сертификаты cert-<host>'s:

```
keytool -import -keystore truststore.jks -noprompt -trustcacerts -alias ads-a-XX-<host>.ru-central1.internal -file cert-<host>.cer -storetype jks -storepass bigdata
```

7.4. Проверяем хранилище

```
keytool -list -v -keystore truststore.jks -storepass bigdata | grep ads-a
```

Основные этапы настройки SSL (8-10)

8. Создаем хранилище ключей keystore-`<host>`.p12 с паролем bigdata в формате pkcs12:

```
openssl pkcs12 -export -in cert-node-1.cer -inkey private-<host>.key -out keystore-<host>.p12 -name ads-a-XX-<host>.ru-central1.internal -CAfile ca-test.pem -caname root -password pass:bigdata -passin pass:bigdata
```

9. Хранилище ключей keystore-`<host>`.p12 конвертируем в jks:

```
keytool -importkeystore -deststorepass bigdata -destkeypass bigdata -destkeystore keystore-<host>.jks -srckeystore keystore-<host>.p12 -srcstoretype PKCS12 -deststoretype JKS -srcstorepass bigdata -alias ads-a-XX-<host>.ru-central1.internal
```

10. Добавить сертификат в хранилище доверенных сертификатов операционной системы:

```
chmod 777 /etc/ssl/certs/ca-certificates.crt  
cat ca-<CA host>.pem >> /etc/ssl/certs/ca-certificates.crt  
chmod 644 /etc/ssl/certs/ca-certificates.crt
```

Для файла ca-test.pem копирование можно не выполнять, т.к. уже присутствует файл с необходимым содержимым /etc/ssl/certs/ca-certificates.crt после запуска утилиты:

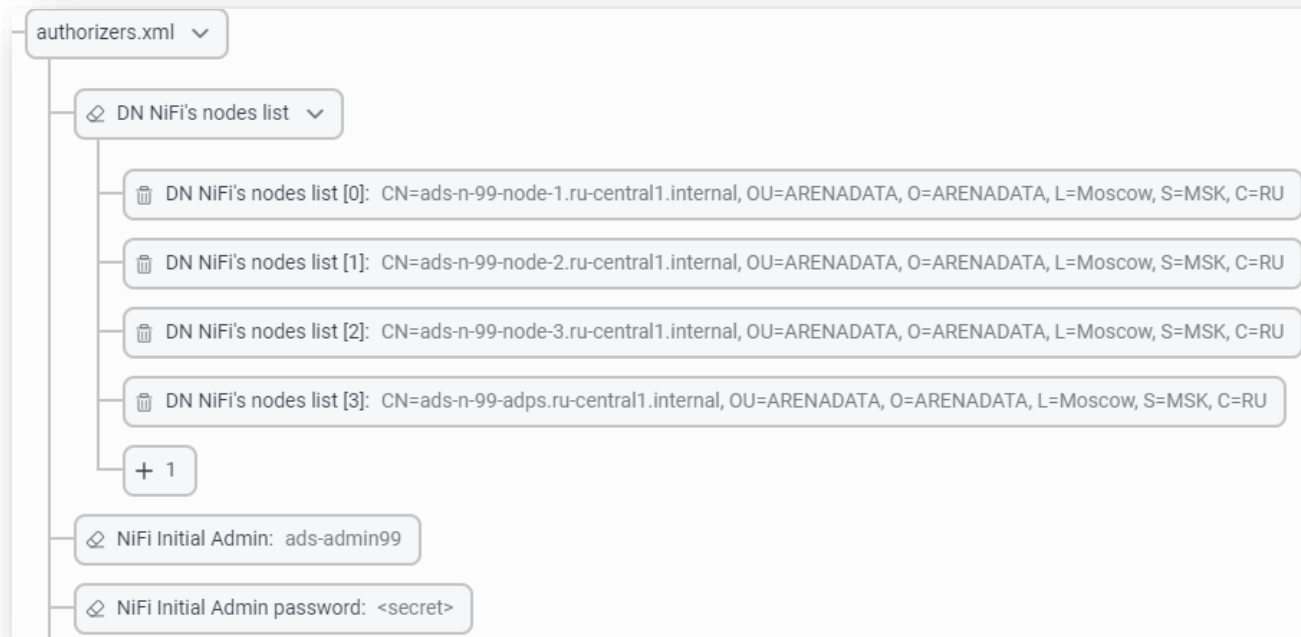
```
sudo update-ca-certificates
```


Основные этапы настройки SSL (11,12)

11. Импортировать сертификаты из хранилища truststore в хранилище Java CA store на каждом узле:

```
sudo keytool -importkeystore -noprompt -srckeystore truststore.jks -destkeystore /etc/ssl/certs/java/cacerts -  
deststorepass changeit -srcstorepass bigdata
```

12. Настроить файл CLUSTERS → ADS → Services → NiFi → Primary Configuration → **authorizers.xml**:



authorizers.xml ▾

- DN NiFi's nodes list ▾
 - DN NiFi's nodes list [0]: CN=ads-n-99-node-1.ru-central1.internal, OU=ARENADATA, O=ARENADATA, L=Moscow, S=MSK, C=RU
 - DN NiFi's nodes list [1]: CN=ads-n-99-node-2.ru-central1.internal, OU=ARENADATA, O=ARENADATA, L=Moscow, S=MSK, C=RU
 - DN NiFi's nodes list [2]: CN=ads-n-99-node-3.ru-central1.internal, OU=ARENADATA, O=ARENADATA, L=Moscow, S=MSK, C=RU
 - DN NiFi's nodes list [3]: CN=ads-n-99-adps.ru-central1.internal, OU=ARENADATA, O=ARENADATA, L=Moscow, S=MSK, C=RU
 - + 1
- NiFi Initial Admin: ads-admin99
- NiFi Initial Admin password: <secret>

Основные этапы настройки SSL (13, 14)

Настроить LDAP NiFi

13.

☒ LDAP Login Identity Provider

Authentication Strategy: LDAPS

Manager DN: CN=ads-admin99,OU=USERS,OU=Student99,OU=ADS,OU=Learning,DC=adh-sec,DC=com

Manager Password: <secret>

TLS - Keystore: <not set>

TLS - Keystore Password: <not set>

TLS - Keystore Type: <not set>

TLS - Truststore: <not set>

TLS - Truststore Password: <not set>

TLS - Truststore Type: <not set>

TLS - Client Auth: NONE

TLS - Protocol: <not set>

TLS - Shutdown Gracefully: <not set>

Referral Strategy: FOLLOW

Connect Timeout: 10 secs

Read Timeout: 10 secs

LDAP URL: ldaps://winda-test-1.adh-sec.com:636

User Search Base: OU=Student99,OU=ADS,OU=Learning,DC=adh-sec,DC=com

User Search Filter: (sAMAccountName={0})

Identity Strategy: USE_USERNAME

Authentication Expiration: 12 hours

14.

☒ LDAP UserGroupProvider

Authentication Strategy: LDAPS

Manager DN: CN=ads-admin99,OU=USERS,OU=Student99,OU=ADS,OU=Learning,DC=adh-sec,DC=com

Manager Password: <secret>

TLS - Keystore: <not set>

TLS - Keystore Password: <not set>

TLS - Keystore Type: <not set>

TLS - Truststore: <not set>

TLS - Truststore Password: <not set>

TLS - Truststore Type: <not set>

TLS - Client Auth: NONE

TLS - Protocol: <not set>

TLS - Shutdown Gracefully: <not set>

Referral Strategy: FOLLOW

Connect Timeout: 10 secs

Read Timeout: 10 secs

LDAP URL: ldaps://winda-test-1.adh-sec.com:636

Page Size: <not set>

Sync Interval: 30 mins

User Search Base: OU=Student99,OU=ADS,OU=Learning,DC=adh-sec,DC=com

User Object Class: person

User Search Scope: ONE_LEVEL

User Search Filter: <not set>

User Identity Attribute: <not set>

User Group Name Attribute: <not set>

User Group Name Attribute - Referenced Group Attribute: <not set>

Group Search Base: OU=Student99,OU=ADS,OU=Learning,DC=adh-sec,DC=com

Group Object Class: group

Group Search Scope: ONE_LEVEL

Group Search Filter: <not set>

Group Name Attribute: <not set>

Group Member Attribute: member

Group Member Attribute - Referenced User Attribute: <not set>

Основные этапы настройки SSL (15)

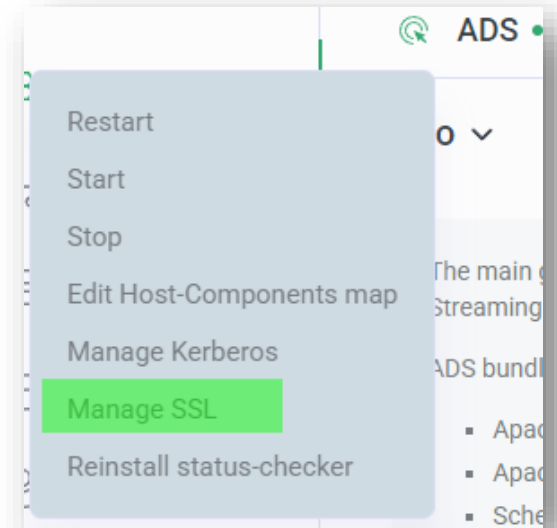
15. Для кластеров ADS и ADPS включаем использование SSL указанием следующих параметров:

Keystore path: /etc/.../keystore.jks

Keystore password: bigdata

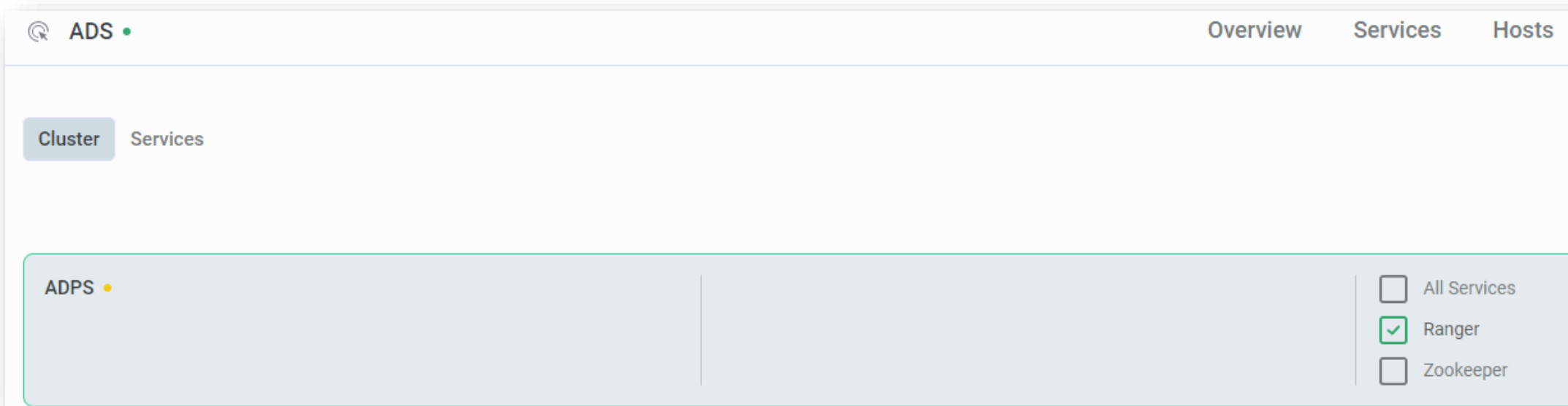
Truststore path: /etc/.../truststore.jks

Truststore password: bigdata

A screenshot of a configuration window titled 'Run an action: Manage SSL'. The window has a close button (X) in the top right corner. It features a progress bar with three steps: '1 Configuration' (active), '2 Raising concerns', and '3 Confirmation'. Below the progress bar are controls for 'Search input', 'Expand content' (disabled), 'Show advanced' (disabled), a refresh icon, and 'Cancel' and 'Next' buttons. The main configuration area is titled 'Configuration' and contains a tree view. The 'Enable SSL' option is checked. Under this, several fields are visible: 'Keystore path: .../keystore.jks', 'Keystore password: <secret>', 'Truststore path: .../truststore.jks' (highlighted with a green border), 'Truststore password: <secret>', 'Force rewrite services SSL configuration: false', and '(DANGEROUS!) Clean nifi users and authorizers: false'.

Интеграция кластера ADPS с кластером ADS

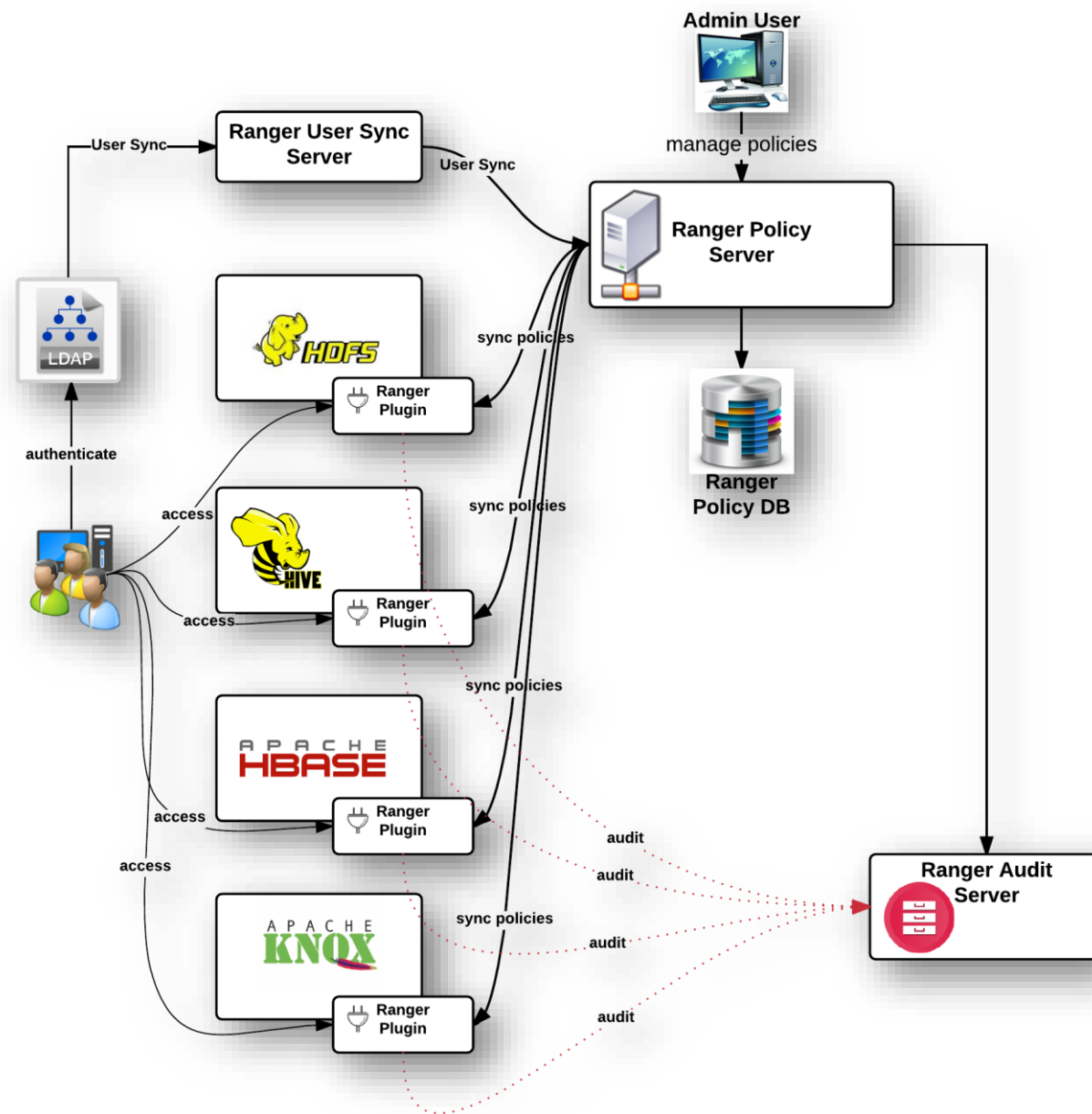
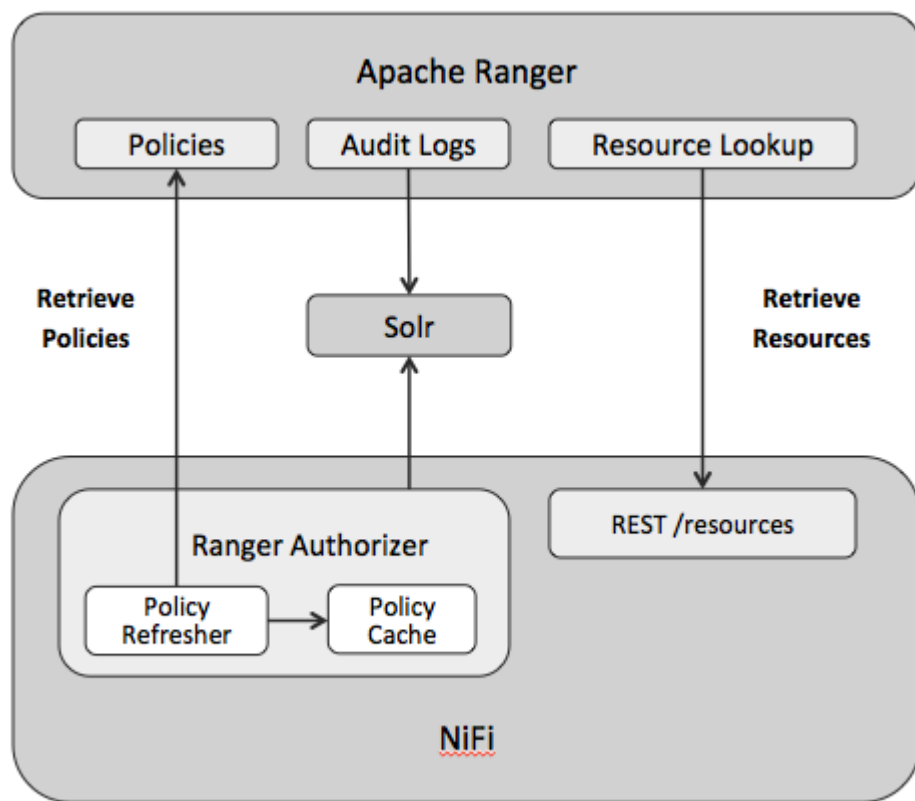
- После включения SSL для кластеров ADS/ADPS можно активировать Ranger-плагин для NiFi!!!
- Для активации Ranger-плагина Kafka, настройка SSL обязательна!
- Для включения плагинов Ranger для сервисов Kafka, NiFi на кластере ADS необходимо перейти на вкладку **Import** кластера ADS и импортировать настройки ADPS/Ranger, установив флажок и нажав кнопку **Save**:



- После импорта настроек ADPS/Ranger необходимо включить плагины Ranger для сервисов (Kafka, NiFi).

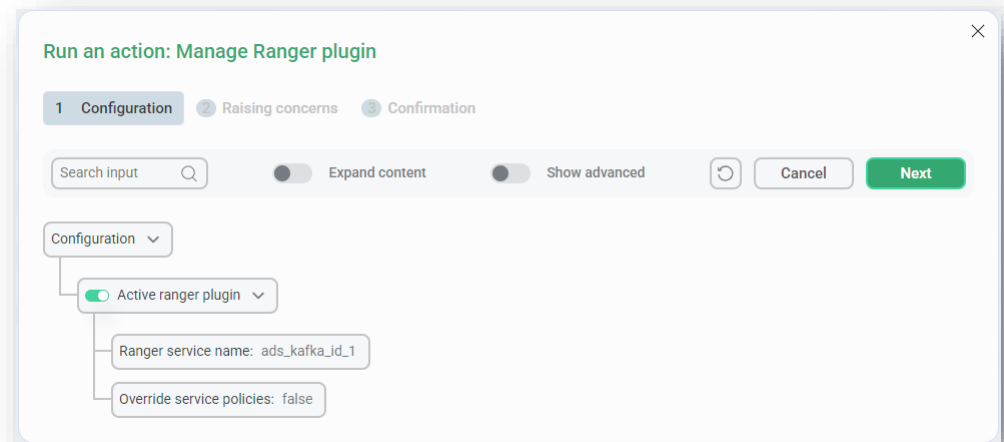
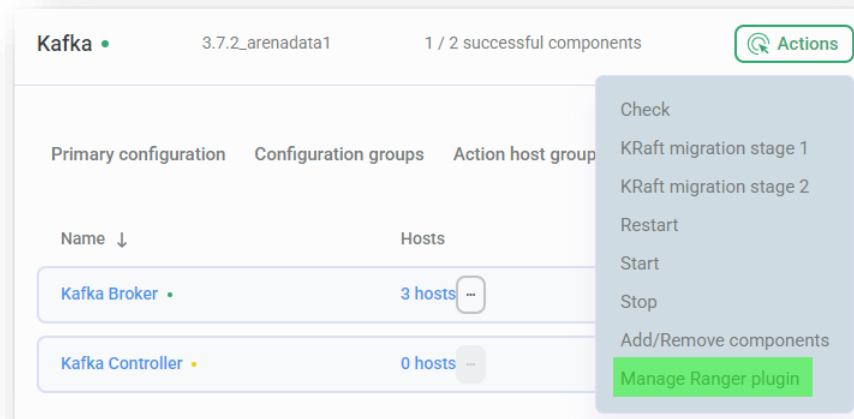
Apache Ranger

- **Ranger** позволяет создавать сервисы для определенных ресурсов ADS (Kafka, NiFi) и добавлять права доступа к этим сервисам.



Kafka Ranger Plugin

- *Kafka*
- ADCM -> Cluster ADS -> Service Kafka -> Actions -> Manage Ranger plugin -> Run



Kafka Ranger Plugin

Service Manager

ads_kafka_id_4 Policies

Edit Policy

Last Response Time : 06/20/2024 12:31:03 AM

Resources :

topic

*

test-topic1

Include

consumerg

*

console-consumer-*

Include

+ Add Resource

Allow Conditions:

Select Role

Select Group

Select User

Policy Conditions

Permissions

admin

Select Roles

nifi-admins99

Select Users

Add Conditions

Consume

Describe

+

Exclude from Allow Conditions:

Select Role

Select Group

Select User

Policy Conditions

Permissions

admin

Select Roles

Select Groups

Select Users

Add Conditions

Add Permissions

add/edit permissions

☐ Publish

☒ Consume

☐ Configure

☒ Describe

☐ Create

☐ Delete

☐ Describe Configs

☐ Alter Configs

☐ Alter

☐ Select/Deselect All

Kafka •

3.7.2_arenadata1

1 / 2 successful components

Actions

Primary configuration

Configuration groups

Action host group

Name ↓	Hosts
Kafka Broker •	3 hosts ...
Kafka Controller •	0 hosts ...

Check

KRaft migration stage 1

KRaft migration stage 2

Restart

Start

Stop

Add/Remove components

Manage Ranger plugin

Run an action: Manage Ranger plugin

1 Configuration

2 Raising concerns

3 Confirmation

Search input

Expand content

Show advanced

Cancel

Next

Configuration

Active ranger plugin

Ranger service name: ads_kafka_id_1










Override service policies: false

Kafka Ranger Plugin

List of Policies : ads_kafka_id_2

Search for your policy...

Add New Policy

Policy ID ▲	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
9	all - topic	--	Enabled	Enabled	--	--	kafka ksql-server schema-registry kafka-rest + More..	  
10	all - cluster	--	Enabled	Enabled	--	--	kafka ksql-server schema-registry kafka-rest + More..	  
11	all - transactionalid	--	Enabled	Enabled	--	--	kafka ksql-server schema-registry kafka-rest + More..	  
12	all - delegationtoken	--	Enabled	Enabled	--	--		
13	all - consumergroup	--	Enabled	Enabled	--	--		



Service Manager > ads_kafka_id_2 Policies > Edit Policy

Policy Name * all - consumergroup Enabled

Policy Label Policy Label

Description Maintained by ADCM

Audit Logging Yes

Resources :

consumerg

topic
transactionalid
cluster
delegationtoken
consumergroup

*

Include

+ Add Resource

NiFi Ranger Permissions

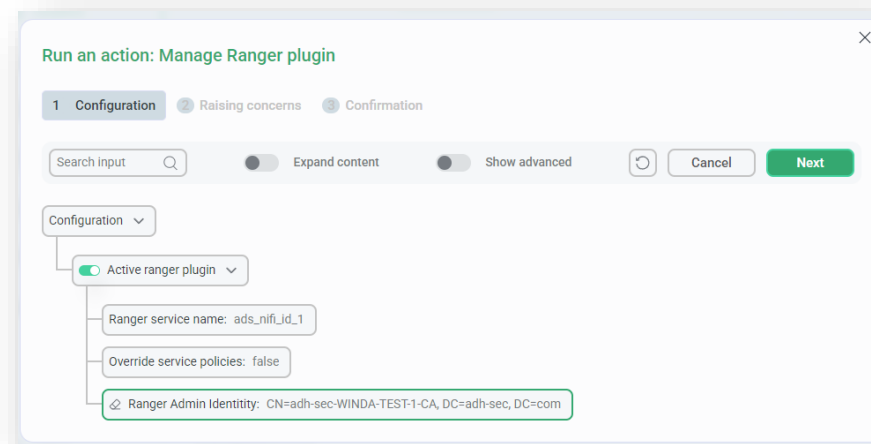
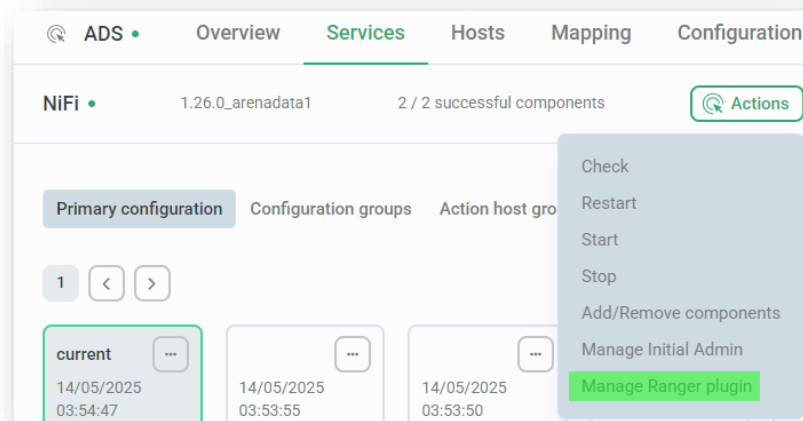
Политики для ресурсов (Write/Modify):

- /resources (Никакие политики не будут доступны, пока эта политика не будет добавлена вручную.)
- /flow
- /system
- /controller
- /counters
- /provenance
- /restricted-components
- /proxy
- /site-to-site
- /parameter-contexts
- /data-transfer/input-ports/<uuid>
- /data-transfer/output-ports/<uuid>
- /process-groups/<uuid>
- /data/process-groups/<uuid>
- /policies/process-groups/<uuid>
- /processors/<uuid>
- /data/processors/<uuid>
- /policies/processors/<uuid>
- ...
- Политики для процессоров (Write/Modify):
 - /restricted-components
 - /restricted-components/read-filesystem - FetchFile, TailFile, GetFile
 - /restricted-components/read-distributed-filesystem - FetchHDFS, FetchParquet, GetHDFS, GetHDFSSequenceFile, MoveHDFS
 - /restricted-components/write-filesystem - FetchFile, GetFile, PutFile
 - /restricted-components/write-distributed-filesystem - DeleteHDFS, GetHDFS, GetHDFSSequenceFile, MoveHDFS, PutHDFS, PutParquet
 - /restricted-components/execute-code - ScriptedReportingTask, ScriptedLookupService, ScriptedReader, ScriptedRecordSetWriter, ExecuteFlumeSink, ExecuteFlumeSource, ExecuteGroovyScript, ExecuteProcess, ExecuteScript, ExecuteStreamCommand, invokeScriptedProcessor,
 - /restricted-components/access-keytab - KeytabCredentialsService
 - /restricted-components/export-nifi-details - SiteToSiteBulletinReportingTask, SiteToSiteProvenanceReportingTask

NiFi Ranger Plugin

- *NiFi*
- ADCM -> Cluster ADS -> Service NiFi -> Actions -> Manage Ranger plugin -> Run

Ranger Admin Identity: CN=adh-sec-WINDA-TEST-1-CA, DC=adh-sec, DC=com



NiFi Registry Ranger Plugin

Service Manager

ads_nifi_registry_id_4 Policies

Edit Policy

Last Response Time : 06/20/2024 12:35:38 AM

Resources :

NiFi Registry Resource Identifier *

✖ / *

+ Add Resource

Allow Conditions:

hide

Select Role	Select Group	Select User	Policy Conditions	Permissions	Delegate Admin	
<div>Select Roles</div>	<div>Select Groups</div>	<div>✖ CN=ads-n-99-node-1.ru-central1.internal, O=ARENADATA, O=ARENADATA, L=Mosc ow, ST=MSK, C=RU</div> <div>✖ CN=ads-n-99-node-2.ru-central1.internal, O=ARENADATA, O=ARENADATA, L=Mosc ow, ST=MSK, C=RU</div> <div>✖ CN=ads-n-99-node-3.ru-central1.internal, O=ARENADATA, O=ARENADATA, L=Mosc ow, ST=MSK, C=RU</div> <div>✖ anonymous</div>	<div>Add Conditions</div> +	<div>Read</div> <div>Write</div> <div>Delete</div> <div></div>	<div><input type="checkbox"/></div>	<div>✖</div>

+

NiFi Ranger Plugin

Service Manager

ads_nifi_id_4 Policies

Edit Policy

Last Response Time : 06/20/2024 12:34:41 A

Policy Details:

Policy Type

Access

Policy ID

9

Policy Name *

denny procgroup

Enabled

Normal

Policy Label

Policy Label

Description

/process-groups/0e928ea8-018f-1000-ffff-ffffc194a93

Audit Logging

Yes

Add Validity Period

Policy Conditions

No Conditions

Resources :

NiFi Resource Identifier *

/process-groups/0e928ea8-018f-1000-ffff-ffffc194a93

Add Resource

Allow Conditions:

Select Role	Select Group	Select User	Policy Conditions	Permissions	Delegate Admin	
Select Roles	Select Groups	nifi-admin99	Add Conditions +	Read Write	<input type="checkbox"/>	

NiFi Ranger Plugin. Flow (main window)

Service Manager > ads_nifi_id_2 Policies > Edit Policy

Last Response Time : 10/15/2024 12:11:47

NiFi Resource Identifier *

/flow

/process-groups/6e4089d4-4a84-3536-b715-4f2f0e4cc208

/processors/2fb2a571-0af9-3b5f-83fe-81e63c542ce7

+ Add Resource

Allow Conditions:

Select Role

Select Group

Select Roles

Select Groups

nifi

3 / 3 0 0 (0 bytes) 0 0 0 45 4 0 0 0 0

Navigate

6b409ef3-0192-1000-d490-6689740f931e

6b409ef3-0192-1000-d490-6689740f931e

6b409ef3-0192-1000-d490-6689740f931e

Operate

6b409ef3-0192-1000-d490-6689740f931e

6b409ef3-0192-1000-d490-6689740f931e

6b409ef3-0192-1000-d490-6689740f931e

File Example

Queued 0 (0 bytes)

In 0 (0 bytes) → 0 5 min

Read/Write 0 bytes / 0 bytes 5 min

Out 0 → 0 (0 bytes) 5 min

Queued 0 (0 bytes)

In 0 (0 bytes) → 0 5 min

Read/Write 0 bytes / 0 bytes 5 min

Out 0 → 0 (0 bytes) 5 min

Queued 0 (0 bytes)

In 0 (0 bytes) → 0 5 min

Read/Write 0 bytes / 0 bytes 5 min

Out 0 → 0 (0 bytes) 5 min

Queued 0 (0 bytes)

In 0 (0 bytes) → 0 5 min

Read/Write 0 bytes / 0 bytes 5 min

Out 0 → 0 (0 bytes) 5 min

6b409ef3-0192-1000-d490-6689740f931e

flow

© Arenadata 2025

62

NiFi Ranger Plugin. Process Group

Service Manager

ads_nifi_id_2 Policies

Edit Policy

Last Response Time : 10/15/2024 12:11:47

NiFi Resource Identifier *

/flow

/process-groups/6e4089d4-4a84-3536-b715-4f2f0e4cc208

/processors/2fb2a571-0af9-3b5f-83fe-81e63c542ce7

+ Add Resource

Allow Conditions:

Select Role

Select Group

Select Roles

Select Groups

nifi

3 / 3

0

0 (0 bytes)

0

0

0

45

4

0

0

0

0

0

0

0

17:03

Navigate

File Example

Process Group

6e4089d4-4a84-3536-b715-4f2f0e4cc208

Operate

File Example

Process Group

6e4089d4-4a84-3536-b715-4f2f0e4cc208

File Example

0 (0 bytes)

0 (0 bytes) → 0

0 bytes / 0 bytes

0 → 0 (0 bytes)

5 min

5 min

5 min

0

0

0

0

0

0

0

0

File Example

0 (0 bytes)

0 (0 bytes) → 0

0 bytes / 0 bytes

0 → 0 (0 bytes)

5 min

5 min

5 min

0

0

0

0

0

0

0

0

File Example

0 (0 bytes)

0 (0 bytes) → 0

0 bytes / 0 bytes

0 → 0 (0 bytes)

5 min

5 min

5 min

0

0

0

0

0

0

0

0

File Example

0 (0 bytes)

0 (0 bytes) → 0

0 bytes / 0 bytes

0 → 0 (0 bytes)

5 min

5 min

5 min

0

0

0

0

0

0

0

0

File Example

0 (0 bytes)

0 (0 bytes) → 0

0 bytes / 0 bytes

0 → 0 (0 bytes)

5 min

5 min

5 min

0

0

0

0

0

0

0

0

File Example

0 (0 bytes)

0 (0 bytes) → 0

0 bytes / 0 bytes

0 → 0 (0 bytes)

5 min

5 min

5 min

0

0

0

0

0

0

0

0

NiFi Ranger Plugin. Processor

Service Manager

ads_nifi_id_2 Policies

Edit Policy

Last Response Time : 10/15/2024 12:11:47

NiFi Resource Identifier *

/flow

/process-groups/6e4089d4-4a84-3536-b715-4f2f0e4cc208

/processors/2fb2a571-0af9-3b5f-83fe-81e63c542ce7

+ Add Resource

Allow Conditions:

Select Role

Select Group

Select Roles

Select Groups

nifi

3 / 3

0

0 (0 bytes)

0

0

0

45

4

0

0

0

0

0

Navigate

+

-

↔

⏮

⏭

↑

Operate

⚙

⚡

✂

▶

■

📄

🔄

📄

📄

🔍

🗑

DELETE

RouteText

Processor

2fb2a571-0af9-3b5f-83fe-81e63c542ce7

In

0 (0 bytes)

5 min

Read/Write

0 bytes / 0 bytes

5 min

Out

0 (0 bytes)

5 min

Tasks/Time

0 / 00:00:00.000

5 min

Queued 0 (0 bytes)

In

0 (0 bytes)

5 min

Read/Write

0 bytes / 0 bytes

5 min

Out

0 (0 bytes)

5 min

Tasks/Time

0 / 00:00:00.000

5 min

Queued 0 (0 bytes)

AD

© Arenadata 2025

64

NiFi Ranger Plugin. Restricted-components: read-filesystem

Ranger

Access Manager

Audit

Security Zone

Settings

Service Manager

ads_nifi_id_2 Policies

Edit Policy

NiFi Resource Identifier *

/flow

/process-groups/6e4089d4-4a84-3536-b715-412f0e4cc208

/processors/2fb2a571-0af9-3b5f-83fe-81e63c542ce7

/restricted-components/read-filesystem

+ Add Resource

Allow Conditions:

Select Role

Select Group

Select User

Select Roles

Select Groups

nifi-admin00

Add Processor

Source

all groups

Displaying 30 of 353

fet

amazon

attributes

aws

azure

cloud

consume

database

delete

fetch

get

google

ingest

json

logs

message

microsoft

pubsub

put

query

record

restricted

source

storage

text

update

Type	Version	Tags
FetchAzureBlobStorage	1.23.2	cloud, blob, storage, microsoft,...
FetchAzureBlobStorage_v12	1.23.2	cloud, blob, storage, microsoft,...
FetchAzureDataLakeStorage	1.23.2	cloud, datalake, storage, micro...
FetchBoxFile	1.23.2	fetch, box, storage
FetchDistributedMapCache	1.23.2	cache, fetch, distributed, map
FetchDropbox	1.23.2	dropbox, fetch, storage
FetchElasticsearchHttp	1.23.2	read, elasticsearch, fetch, get, ...
FetchFTP	1.23.2	input, ftp, get, fetch, retrieve, fil...
FetchFile	1.23.2	ingress, input, restricted, get, f...
FetchGCObject	1.23.2	gcs, google cloud, fetch, googl...
FetchGoogleDrive	1.23.2	fetch, google, storage, drive
FetchGridFS	1.23.2	mongo, fetch, grids

FetchFile 1.23.2

org.apache.nifi - nifi-standard-nar

Reads the contents of a file from disk and streams it into the contents of an incoming FlowFile. Once this is done, the file is optionally moved elsewhere or deleted to help keep the file system organized.

CANCEL

ADD



© Arenadata 2025

65