Arenadata™ Platform Security

Версия - v1.0.0

Руководство по работе с Apache Ranger

2022 Arenadata™

Оглавление

1 Apache Ranger - Введение **3**
- 1.1 Предварительные требования к установке . . . 3

2 Предварительные требования к установке **5**
- 2.1 Настройка сопоставления групп Hadoop для LDAP/AD . . . 5

3 Установка Ranger **8**
- 3.1 Загрузка бандла Arenadata Platform Security . . . 8
- 3.2 Создание кластера . . . 8
- 3.3 Конфигурирование сервисов . . . 11
- 3.4 Завершение установки . . . 12

4 Включение плагинов Ranger **14**
- 4.1 HDFS . . . 14
- 4.2 YARN . . . 18
- 4.3 Hive . . . 18
- 4.4 HBase . . . 18

5 Управление аудитом в Ranger **23**
- 5.1 Аудит. Введение . . . 23
- 5.2 Вкладка Access . . . 23
- 5.3 Вкладка Admin . . . 24
- 5.4 Вкладка Login Sessions . . . 24
- 5.5 Вкладка Plugins . . . 25
- 5.6 Вкладка Plugins Status . . . 25

В документе приведены настройки функций безопасности Hadoop, авторизация в кластере, установка Apache Ranger и создание HDFS Policy.

Документ может быть полезен администраторам, программистам, разработчикам и сотрудникам подразделений информационных технологий, осуществляющих внедрение кластера.

Important: Перед установкой убедитесь, что версия бандла Arenadata Hadoop не ниже чем 2.1.3.0

Important: Контактная информация службы поддержки – e-mail: info@arenadata.io

Глава 1

Apache Ranger - Введение

Apache Ranger можно установить при помощи пользовательского интерфейса **ADCM**. В отличие от ручного процесса установки, требующего выполнения ряда шагов, установка **Ranger** с использованием интерфейса **ADCM** проще и легче. Опция службы **Ranger** доступна через мастер **Add Service** после инсталляции кластера **ADH** с помощью установщика.

Служба Ranger включает в себя следующие компоненты:

- Ranger Admin
- Ranger UserSync
- Ranger Key Management Service

После установки и запуска этих компонентов можно включить плагины **Ranger**, перейдя к каждому отдельному сервису (**HDFS**, **HBase**, **Hiveserver2**, **Storm**, **Knox**, **YARN** и **Kafka**) и изменив конфигурацию в расширенном режиме *ranger-<service>-plugin-properties*.

Important: При включении плагина Ranger необходимо перезапустить компонент

Important: Включение Apache Kafka требует включения Kerberos

Important: !ВНИМАНИЕ! Компоненты Ranger должны быть установлены на отдельной VM или сервере и не должны использовать существующие узлы кластера Arenadata Hadoop

1.1 Предварительные требования к установке

- Поддерживаются следующие ОС: RedHat/CentOS 7.7,7.8
- Необходимо установить JDK 8+. Поддерживаются как OpenJDK, так и Oracle JDK.

База данных:

- MySQL (5.6+)
- Сервер БД может быть установлен на том же хосте. Или сервисам Ranger необходим доступ к хосту сервера БД.

- Для продуктивного использования необходимо выделить достаточном дискового пространства для служебной БД Ranger.

Журнал логов:

- Для хранения и индексации логов Apache Ranger использует Apache Solr
- Узлы Apache Solr могут быть установлены на те же хосты, что и компоненты Apache Ranger
- Убедитесь что для инстансов Solr выделено достаточно ресурсов из расчета - кластер из 10 узлов, состоящий примерно из 15-20 компонентов, может генерировать 1 ГБ журналов аудита за один день

Ranger Admin:

- Для процесса Ranger Admin требуется выделить минимум 1,5 ГБ ОЗУ.

Глава 2

Предварительные требования к установке

Important: Для установки сервисов необходимы вылеоенный сервер или виртуальная машина, доступная в интерфейсе ADCM

Перед установкой **Ranger** необходимо убедиться, что кластер отвечает следующим требованиям:

- Установлен и настроен кластер Arenadata Hadoop версии не ниже 2.1.3
- Рекомендуется хранить аудиты как в HDFS, так и в Solr. Конфигурация по умолчанию для Ranger Audits в Solr использует общий экземпляр Solr;
- Чтобы обеспечить принудительную авторизацию на уровне групп LDAP/AD в Hadoop, необходимо настроить сопоставление групп Hadoop для LDAP/AD для LDAP (*Настройка сопоставления групп Hadoop для LDAP/AD*);
- При использовании внешней СУБД для хранения метаданных, должен быть запущен и доступен экземпляр базы данных MySQL, который будет использоваться Ranger. Установщик Ranger создаст двух новых пользователей (имена по умолчанию: *rangeradmin* и *rangerlogger*) и две новые базы данных (имена по умолчанию: *ranger* и *ranger_audit*).

2.1 Настройка сопоставления групп Hadoop для LDAP/AD

Для обеспечения принудительной авторизации на уровне групп **LDAP/AD** в **Hadoop**, необходимо настроить сопоставление групп **Hadoop** для **LDAP/AD**.

Important: Доступ к LDAP и сведения о подключении: настройки LDAP могут различаться в зависимости от используемой реализации LDAP

Существует три способа настройки сопоставления групп **Hadoop**.

- **Настройка сопоставления групп Hadoop для LDAP/AD с использованием SSSD (рекомендуется)**

Для сопоставления групп рекомендуется использовать SSSD или один из следующих сервисов подключения ОС **Linux** к **LDAP**:

- Centrify
- NSLCD

- Winbind
- SAMBA

Большинство перечисленных сервисов позволяет не только искать пользователя и перечислять группы, но также выполнять другие действия на хосте. При этом ни одно из этих действий не требуется для сопоставления групп **LDAP** в **Hadoop**. Поэтому, оценивая эти сервисы, необходимо понимать разницу между модулем **NSS** (который выполняет разрешение пользователь/группа) и модулем **PAM** (который выполняет аутентификацию пользователя). Для возможности поиска (или "валидации") пользователя в **LDAP** и перечисления групп требуется **NSS**. А **PAM** может представлять угрозу безопасности.

- **Настройка сопоставления групп Hadoop в файле core-site.xml**

Настройка **Hadoop** для использования сопоставления групп на основе **LDAP** в файле *core-site.xml* осуществляется в следующем порядке:

1. Добавить свойства, показанные в приведенном ниже примере, в файл *core-site.xml*. Необходимо указать значение для привязанного пользователя, его пароль и другие свойства, специфичные для экземпляра LDAP, и убедиться, что фильтры классов объектов, пользователей и групп соответствуют значениям, указанным в экземпляре LDAP.

```
<property>
<name>hadoop.security.group.mapping</name>
<value>org.apache.hadoop.security.LdapGroupsMapping</value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.bind.user</name>
<value>cn=Manager,dc=hadoop,dc=apache,dc=org</value>
</property>

<!-
<property>
<name>hadoop.security.group.mapping.ldap.bind.password.file</name>
<value>/etc/hadoop/conf/ldap-conn-pass.txt</value>
</property>
->

<property>
<name>hadoop.security.group.mapping.ldap.bind.password</name>
<value>hadoop</value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.url</name>
<value>ldap://localhost:389/dc=hadoop,dc=apache,dc=org</value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.url</name>
<value>ldap://localhost:389/dc=hadoop,dc=apache,dc=org</value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.base</name>
<value></value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.search.filter.user</name>
```

```
<value>(&amp;(|(objectclass=person)(objectclass=applicationProcess))(cn={0}))</value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.search.filter.group</name>
<value>(objectclass=groupOfNames)</value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.search.attr.member</name>
<value>member</value>
</property>

<property>
<name>hadoop.security.group.mapping.ldap.search.attr.group.name</name>
<value>cn</value>
</property>
```

2. В зависимости от конфигурации можно обновлять сопоставления пользователей и групп с помощью следующих команд HDFS и YARN:

```
hdfs dfsadmin -refreshUserToGroupsMappings
yarn rmadmin -refreshUserToGroupsMappings
```

3. Проверить сопоставление групп LDAP, выполнив команду *hdfs groups*. Команда отображает группы из LDAP для текущего пользователя. При настроенном сопоставлении групп LDAP разрешения HDFS могут использовать группы, определенные в LDAP для контроля доступа.

- **Ручное создание пользователей и групп в среде Linux**

  Также можно вручную создавать пользователей и группы в среде Linux.

Глава 3

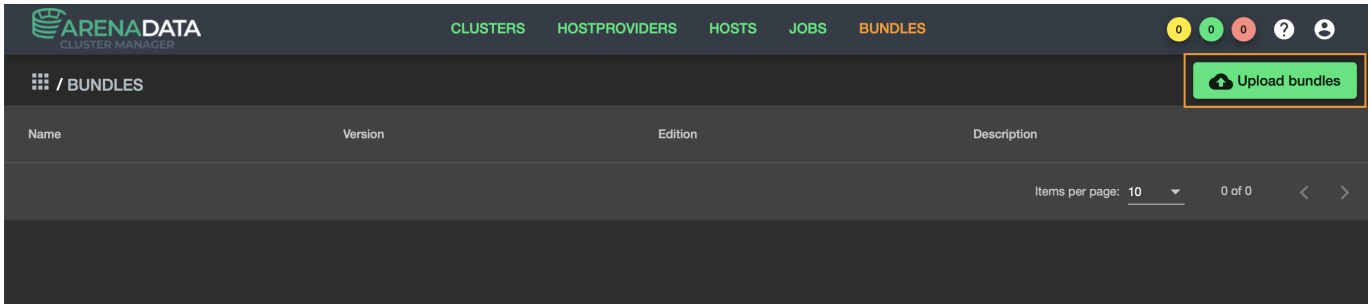
Установка Ranger

Установка **Ranger** с помощью **ADCM** заключается в три этапа:

- *Загрузка бандла Arenadata Platform Security*
- *Создание кластера*
- *Конфигурирование сервисов*
- *Завершение установки*

3.1 Загрузка бандла Arenadata Platform Security

Для начала работы с компонентами Apache Ranger, необходимо загрузить бындл в текущий инстанс ADCM, с помощью действия “Upload Bundle”



Далее необходимо принять соглашение об использовании (EULA)

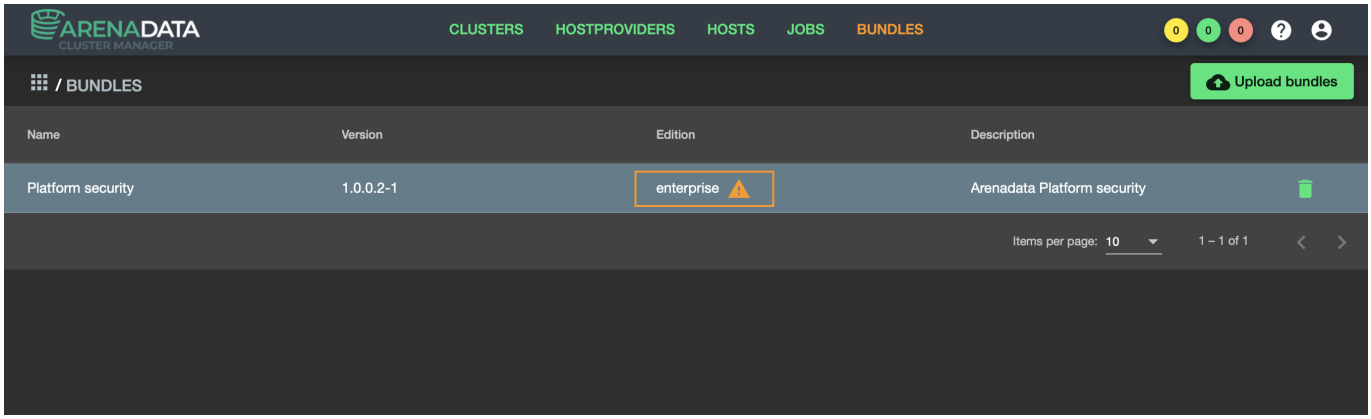
3.2 Создание кластера

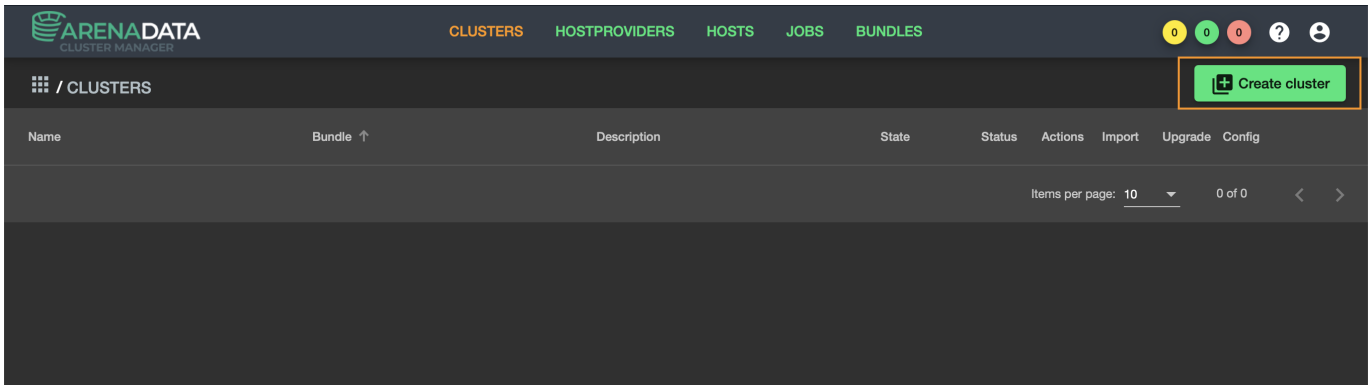
Следующим шагом является создание кластера Arenadata Platform Security с помощью действия “Create cluster” в разделе “Clusters”

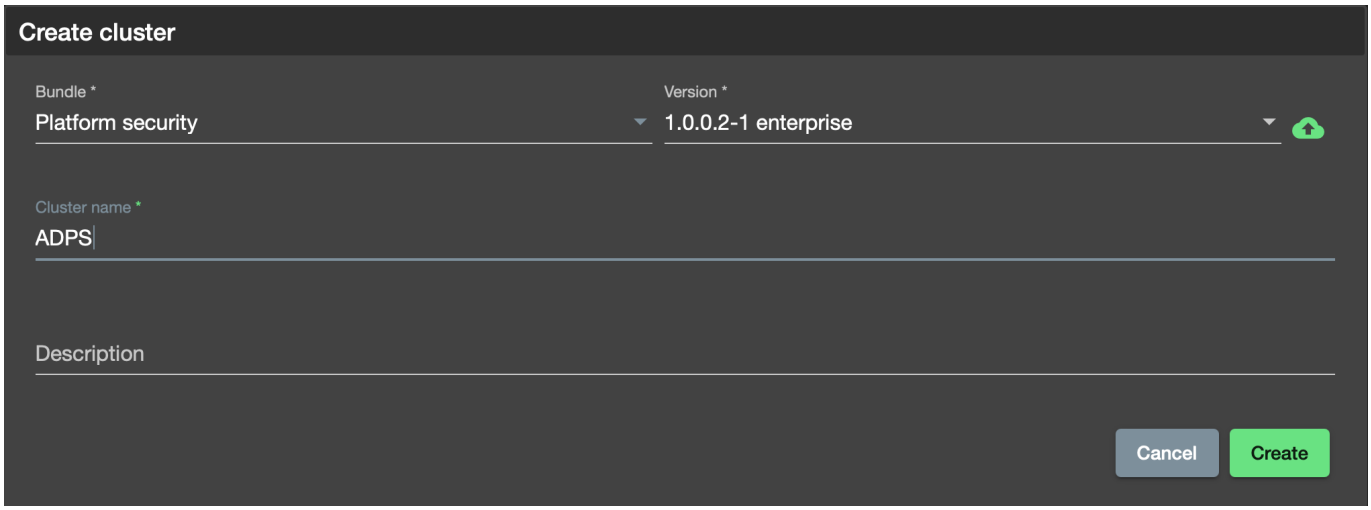
После чего, выберите имя кластера и завершите конфигурацию с помощью кнопки “Create”.

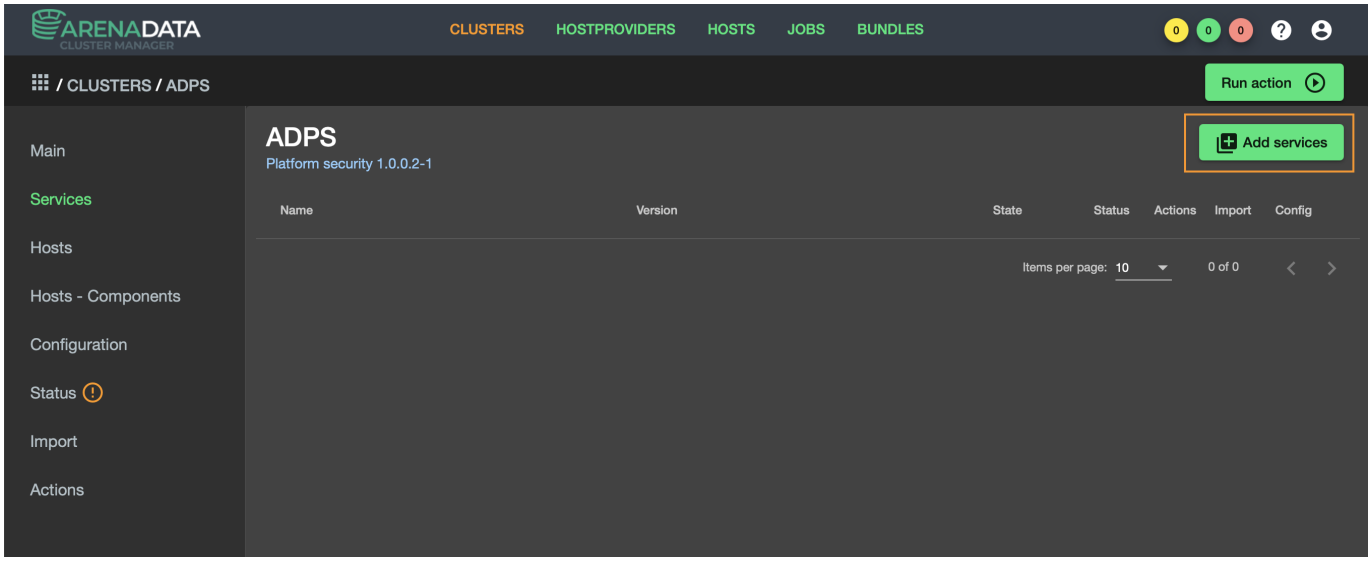
Следующим шагом является ыбор требуемых сервисов и распределение топологии компонентов. Для этого перейдите в конфигурацию кластера и выберите раздел “Services” и нажмите “Add services”

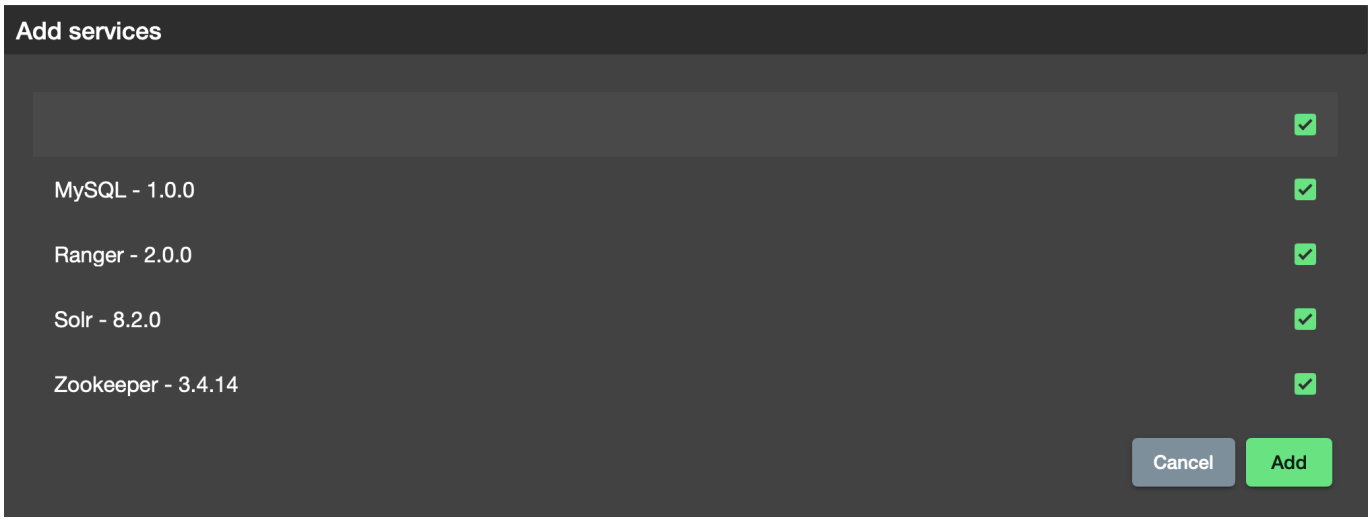
Выберите необходимые компоненты в интерфейсе ADCM


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ BUNDLES
Upload bundles
Name
Version
Edition
Description
Platform security
1.0.0.2-1
enterprise
Arenadata Platform security
Items per page: 10
1 – 1 of 1

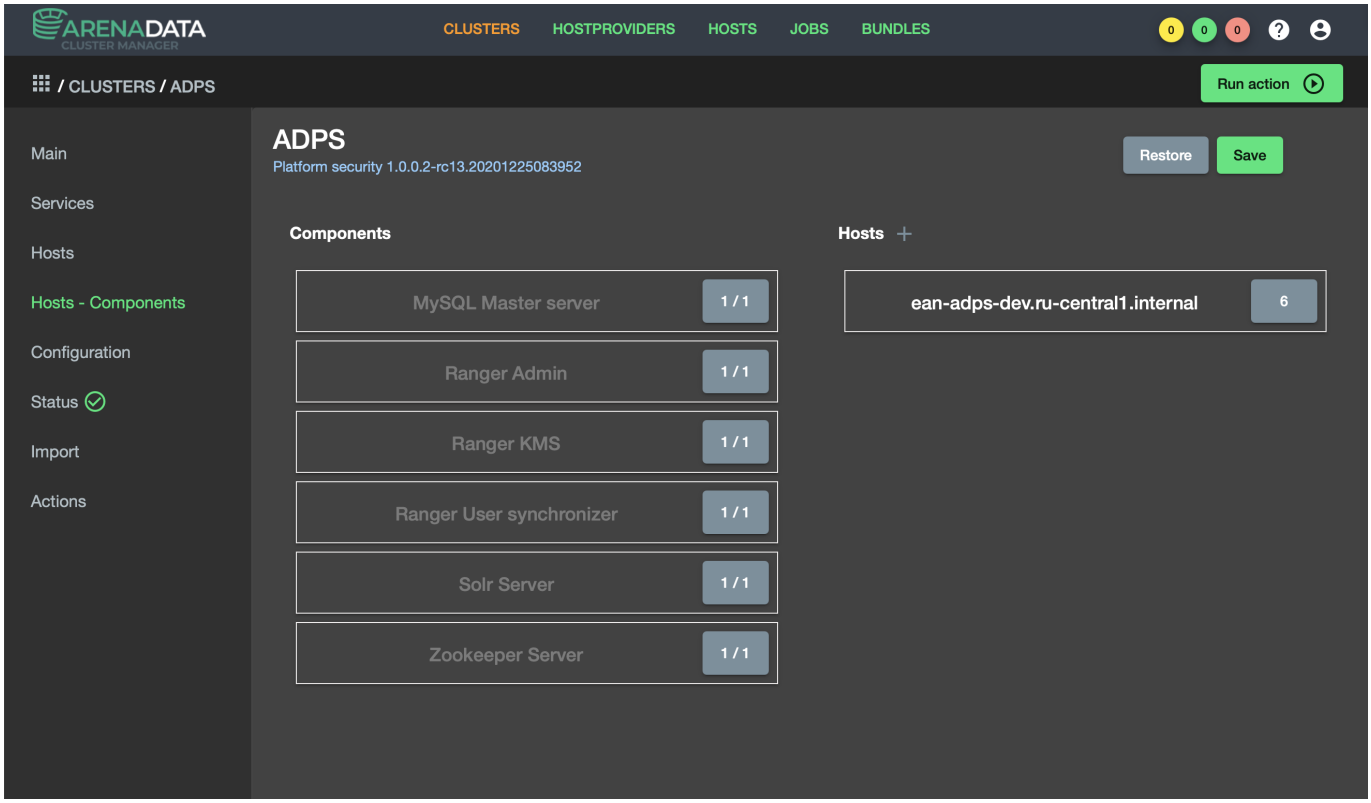

ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ CLUSTERS
Create cluster
Name
Bundle
Description
State
Status
Actions
Import
Upgrade
Config
Items per page: 10
0 of 0


Create cluster
Bundle *
Platform security
Version *
1.0.0.2-1 enterprise
Cluster name *
ADPS
Description
Cancel
Create


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ CLUSTERS / ADPS
Run action
Main
Services
Hosts
Hosts - Components
Configuration
Status
Import
Actions
ADPS
Platform security 1.0.0.2-1
Add services
Name
Version
State
Status
Actions
Import
Config
Items per page: 10
0 of 0


Add services
MySQL - 1.0.0
Ranger - 2.0.0
Solr - 8.2.0
Zookeeper - 3.4.14
Cancel
Add

Далее перейдите в раздел “Host-Components” и распределите компоненты по хостам



Important: Все необходимые хосты должны быть созданы перед установкой компонентов

Important: Решение позволяет произвести установку всех компонентов в рамках одного хоста, но для промышленных инсталляций рекомендуется разнести компоненты между различными хостами для обеспечения большей отказоустойчивости

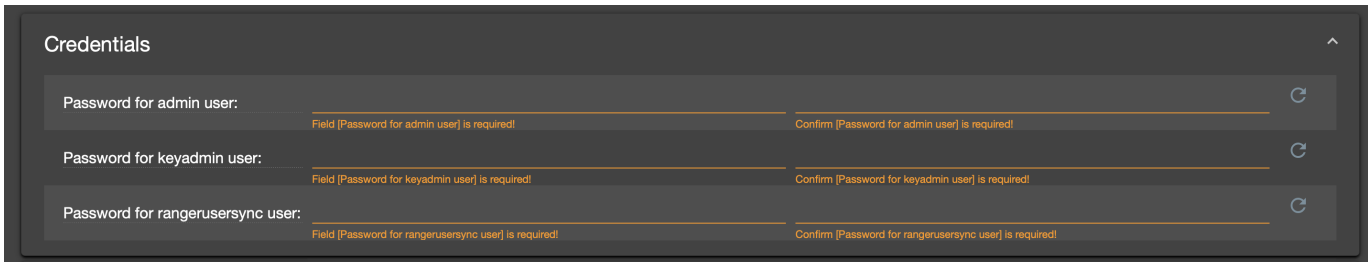
3.3 Конфигурирование сервисов

Следующим шагом в процессе установки **Ranger** является задание настроек на странице сервиса Ranger “Configuration”:

- *Credentials*
- *dbks-site.xml*
- *ranger-admin-site.xml*
- *ranger-ugsync-site.xml*

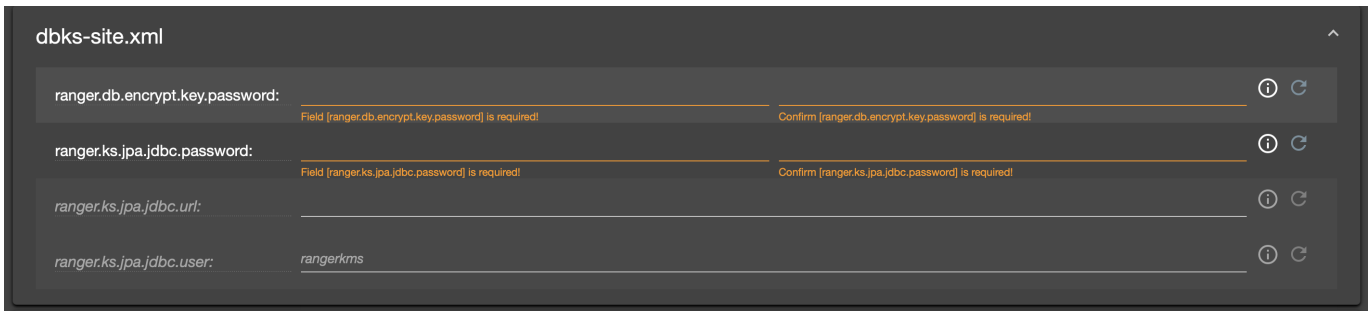
3.3.1 Credentials

В данном разделе необходимо указать учетные данные создаваемых технологических пользователей для доступа к интерфейсу и компонентам сервиса Ranger



3.3.2 dbks-site.xml

В данном разделе необходимо указать пароль доступа для ключей шифрования и пароль подключения к БД



3.3.3 ranger-admin-site.xml

В данном разделе необходимо указать пароль доступа для подключения к БД и инстансу Solr для обеспечения аудита действий пользователей

3.3.4 ranger-ugsync-site.xml

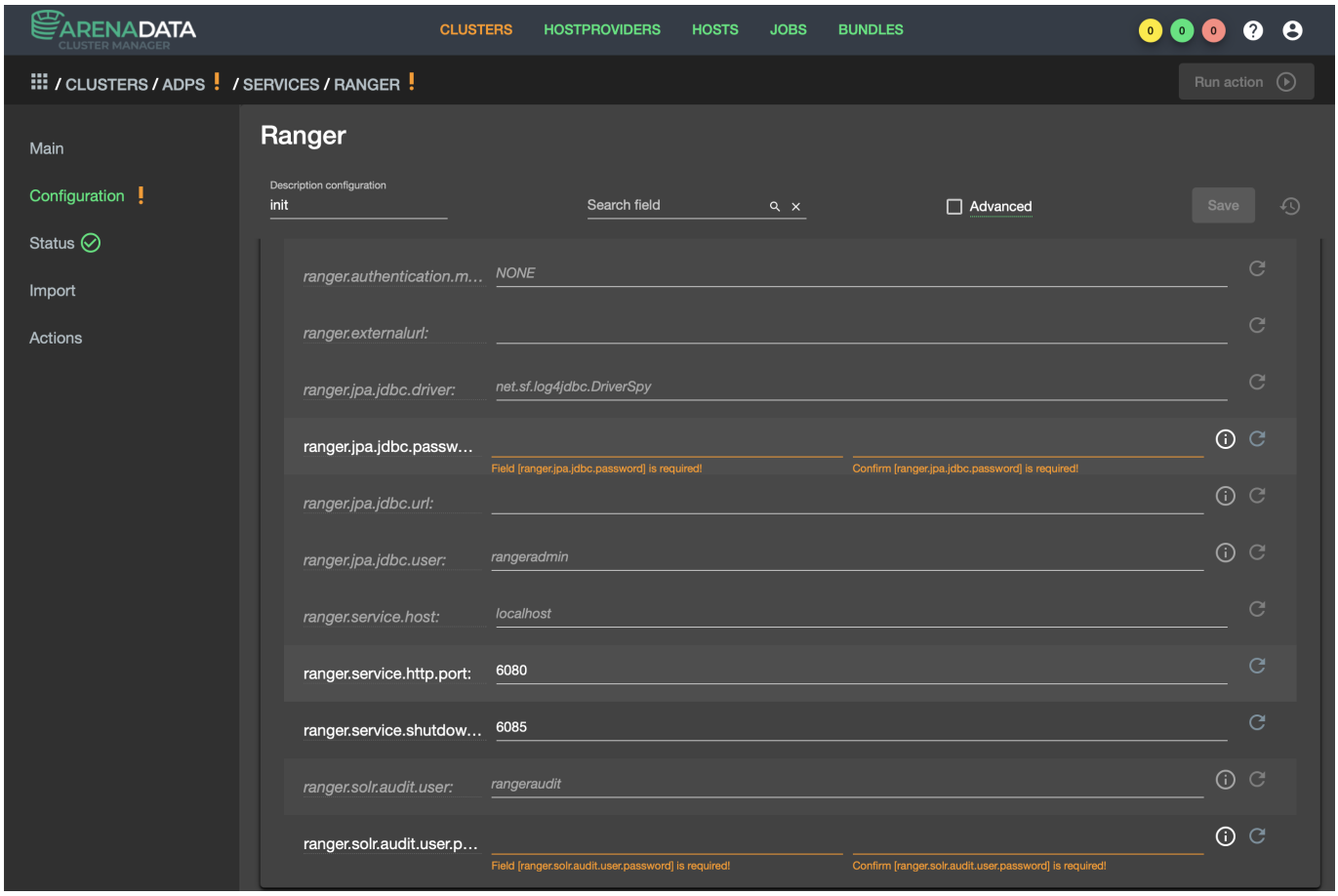
В разделе описывается настройка **Ranger User Sync** для **UNIX** и **LDAP/AD**.

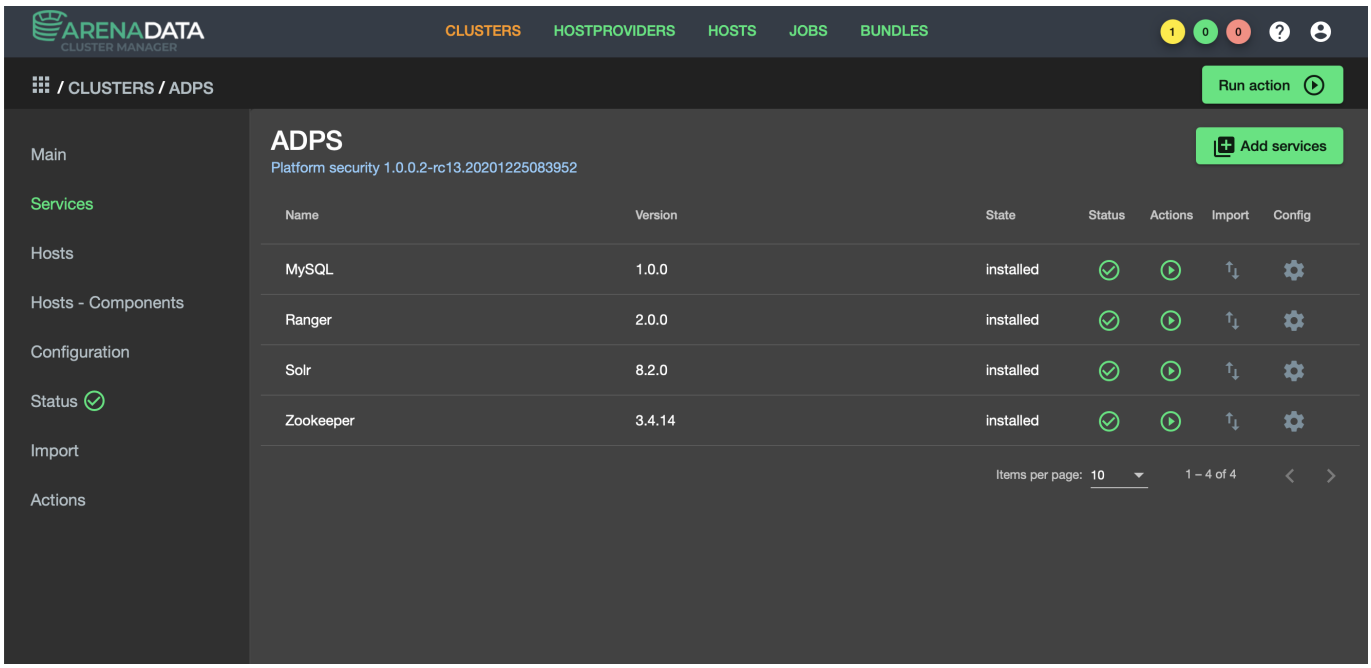
3.4 Завершение установки

Important: Перед запуском установки убедитесь что в интерфейсе более нет предупреждений в части конфигурации сервисов.

Для завершение процесса установки **Ranger** перйдите в раздел Main кластера и выберите действие “Install” в разделе “Run action”

После заершения установки, все компоненты должны иметь “зеленый” статус


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ CLUSTERS / ADPS !
/ SERVICES / RANGER !
Run action
Main
Configuration !
Status
Import
Actions
Ranger
Description configuration
init
Search field
Advanced
Save
ranger.authentication.m...
NONE
ranger.externalurl:
ranger.jpa.jdbc.driver:
net.sf.log4jdbc.DriverSpy
ranger.jpa.jdbc.passw...
Field [ranger.jpa.jdbc.password] is required!
Confirm [ranger.jpa.jdbc.password] is required!
ranger.jpa.jdbc.url:
ranger.jpa.jdbc.user:
rangeradmin
ranger.service.host:
localhost
ranger.service.http.port:
6080
ranger.service.shutdow...
6085
ranger.solr.audit.user:
rangeraudit
ranger.solr.audit.user.p...
Field [ranger.solr.audit.user.password] is required!
Confirm [ranger.solr.audit.user.password] is required!


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ CLUSTERS / ADPS
Run action
Main
Services
Hosts
Hosts - Components
Configuration
Status
Import
Actions
ADPS
Platform security 1.0.0.2-rc13.20201225083952
Add services
Name
Version
State
Status
Actions
Import
Config
MySQL
1.0.0
installed
Ranger
2.0.0
installed
Solr
8.2.0
installed
Zookeeper
3.4.14
installed
Items per page: 10
1 – 4 of 4

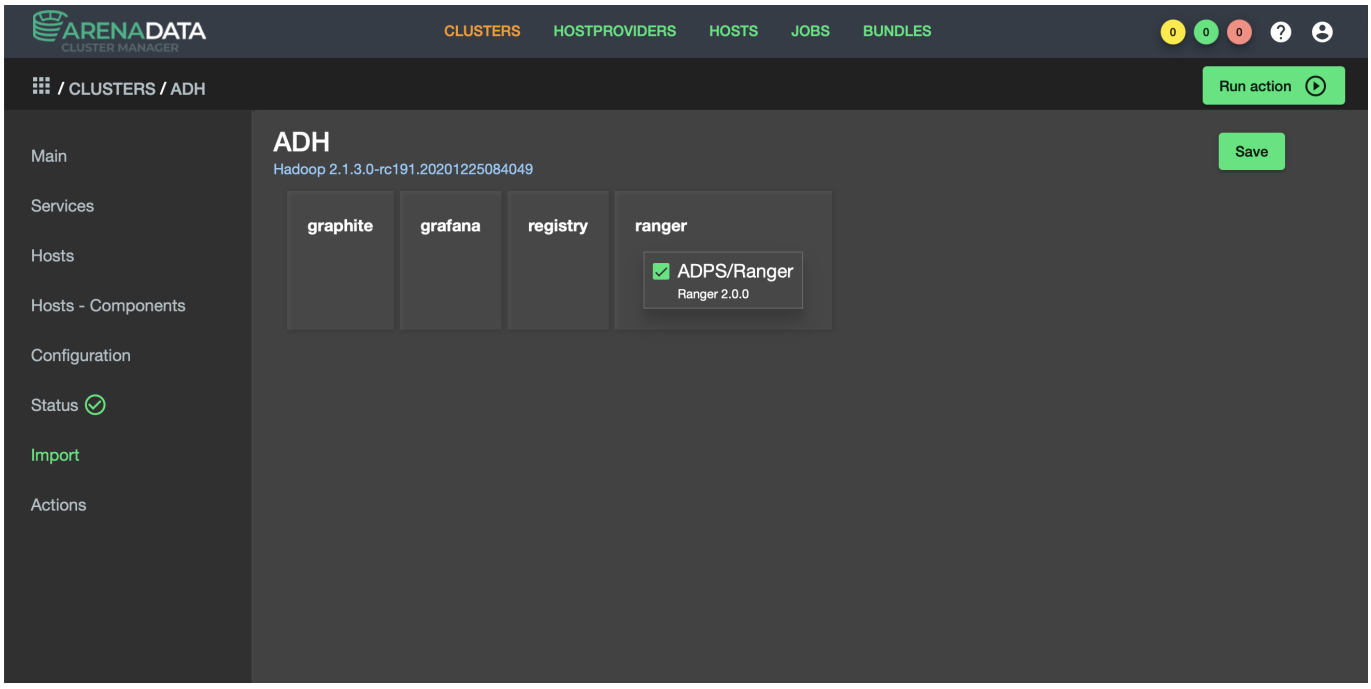
Глава 4

Включение плагинов Ranger

Плагины **Ranger** могут быть включены для нескольких сервисов **ADH**. По соображениям производительности рекомендуется хранить аудиты в **Solr**, а не в базе данных.

Доступны следующие плагины **Ranger**: *HDFS*, **Hive**, **HBase**, **YARN**, **Sqoop**.

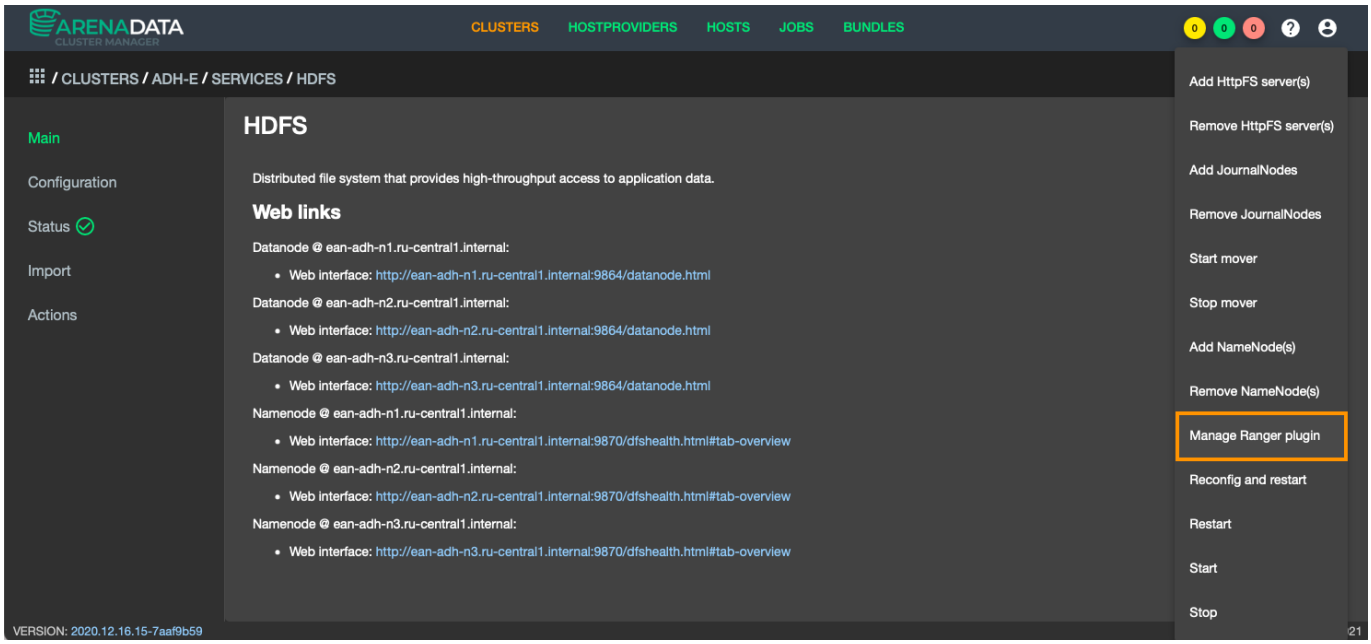
Important: Перед включением плагинов необходимо сделать import в том кластере, который будет интегрирован с ADPS



4.1 HDFS

Для включения плагина **Ranger HDFS** необходимо выполнить следующие действия:

На странице сервиса HDFS кластера ADH в разделе “Run action”, выбрать Manager Ranger Plugin.

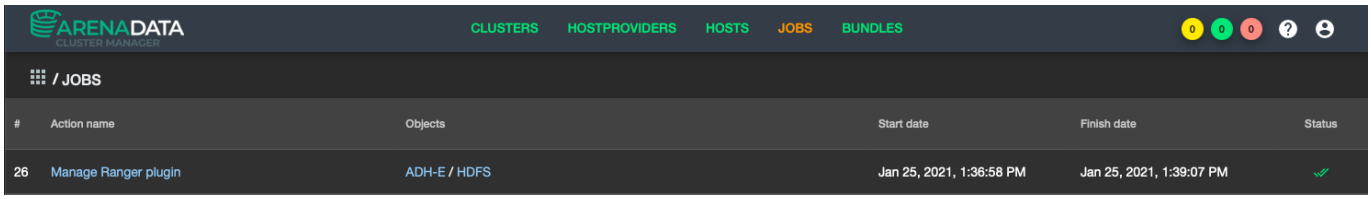


Выберите необходимое состояние (Enabled/Disabled):



После чего запустится процесс активации плагина и создание дефолтной политике на стороне Ranger.

В статусе должно отображаться успешное выполнение.



4.1.1 HDFS Policy

Ranger для авторизации в Hadoop

После проверки подлинности пользователя необходимо определить его права доступа. Права доступа пользователя к ресурсам определяет авторизация. Например, пользователю может быть разрешено создание политики и просмотр отчетов, но не разрешено редактирование пользователей и групп. **Ranger** можно использовать для настройки и управления доступом к сервисам **Hadoop**.

Ranger позволяет создавать сервисы для определенных ресурсов **Hadoop** (**HDFS**, **HBase**, **Hive** и др.) и добавлять права доступа к этим сервисам. Можно также создавать сервисы на основе тегов и добавлять политики доступа к ним. Использование политик на основе тегов позволяет управлять доступом к ресурсам

нескольких компонентов **Hadoop** без создания отдельных сервисов и политик в каждом компоненте. Можно также использовать **Ranger TagSync** для синхронизации хранилища тегов **Ranger** с внешним сервисом метаданных, таким как **Apache Atlas**.

Создание HDFS Policy

Благодаря конфигурации **Apache Ranger** позволяет проверять для запроса пользователя как политики **Ranger**, так и разрешения **HDFS**. Когда **NameNode** получает пользовательский запрос, плагин **Ranger** проверяет политики, установленные через **Ranger Service Manager**, и если их нет, проверяет разрешения, установленные в **HDFS**.

Рекомендуется создавать разрешения в **Ranger Service Manager** и иметь ограниченные разрешения на уровне **HDFS**.

Добавление новой политики к существующему сервису **HDFS** осуществляется по следующему алгоритму:

1. На странице "Service Manager" выбрать существующий сервис в разделе HDFS (`Рис.%s.`).

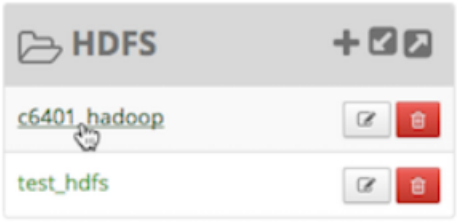


Рис.4.1.: Выбор сервиса HDFS

При этом открывается страница "List of Policies", на которой необходимо нажать кнопку "Add New Policy" (`Рис.%s.`).

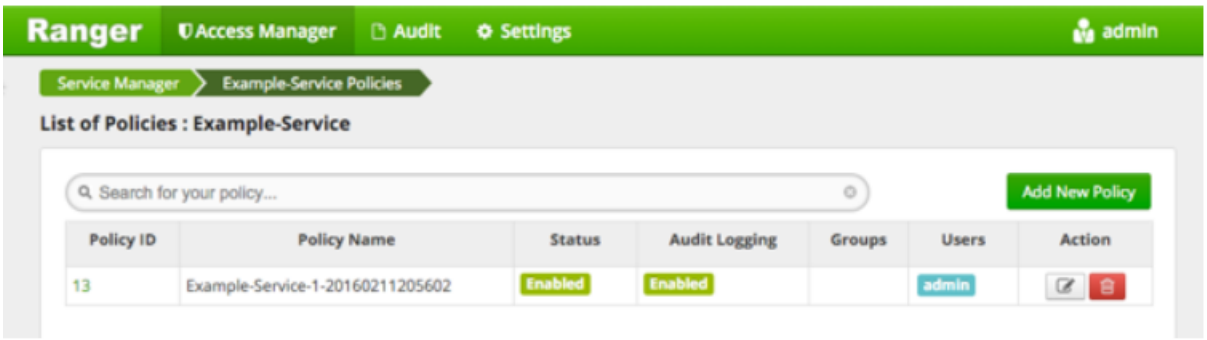


Рис.4.2.: List of Policies

2. Открывается страница "Create Policy" (`Рис.%s.`).

На странице необходимо заполнить поля. Раздел "Policy Details":

- *Policy Name* – ввести уникальное имя для данной политики (имя не может быть продублировано нигде в системе);
- *Resource Path* – определить путь к ресурсу для папки/файла политики. Во избежание необходимости указывать полный путь или включать политику для всех вложенных папок или файлов, можно заполнить это поле с помощью подстановочных знаков (например, /home*) либо указать, что политика должна быть рекурсивной;
  - Подстановочные знаки могут быть включены в путь ресурса, имя базы данных, таблицы или столбца: "*" – указывает ноль или более символов; "?" – указывает один символ;

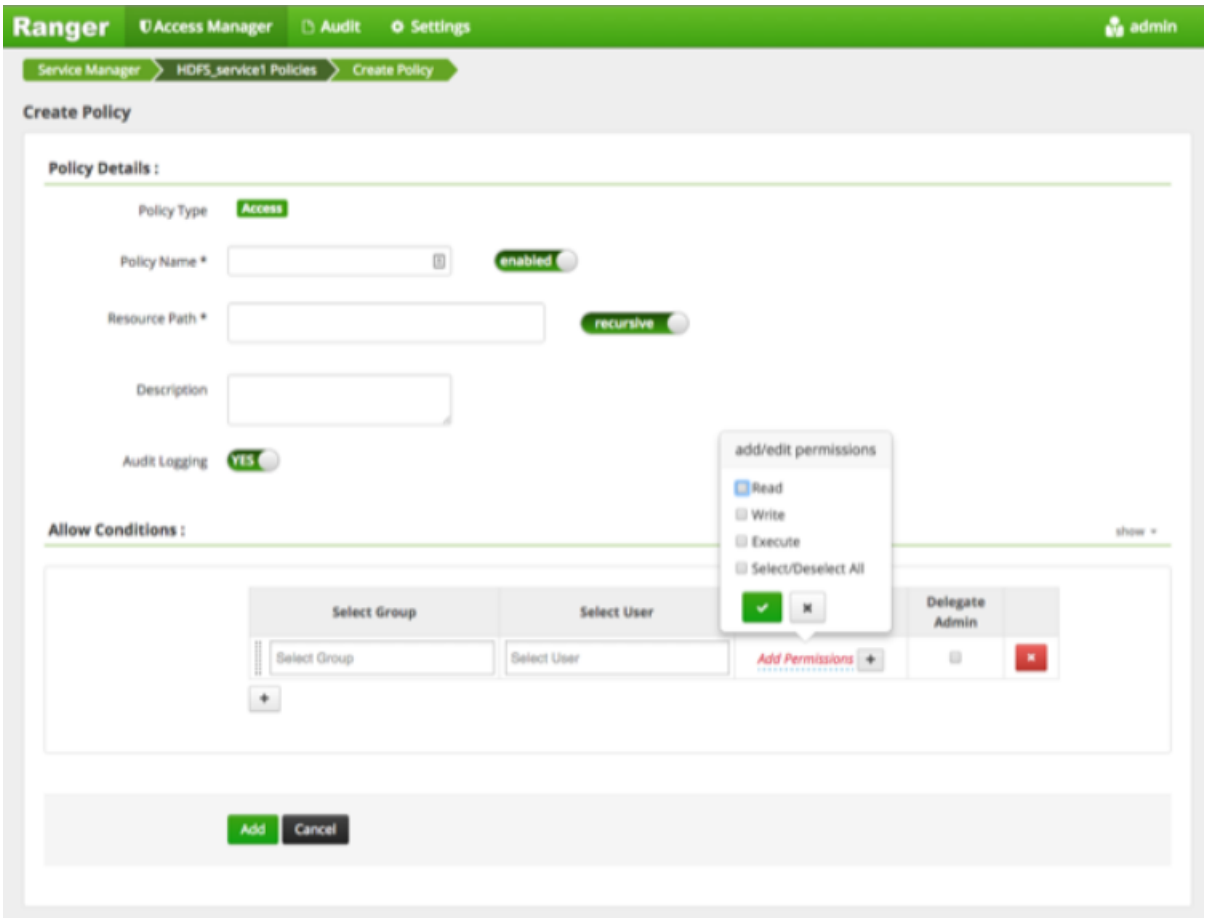


Рис.4.3.: Create Policy

- *Description* – (опционально) указать цель политики;
- *Audit Logging* – указать, выполняется ли аудит данной политики (снять флажок, чтобы отключить аудит).

  Раздел “Allow Conditions”:

- *Select Group* – указать группу, к которой применяется данная политика. Чтобы назначить группу в качестве администратора для выбранного ресурса, выбрать *Admin permissions* (администраторы могут создавать дочерние политики на основе существующих). Группа *public* содержит всех пользователей, поэтому предоставление доступа к ней предоставляет доступ ко всем пользователям;
- *Select User* – указать конкретного пользователя, к которому применяется данная политика (за пределами уже указанной группы), или назначить определенного пользователя администратором данной политики (администраторы могут создавать дочерние политики на основе существующих);
- *Permissions* – добавить или изменить права: *Read* (чтение), *Write* (запись), *Create* (создание), *Admin* (Администратор), *Select/Deselect All* (выбрать/отменить все);
- *Delegate Admin* – когда политика назначается пользователю или группе пользователей, данные пользователи становятся делегированными администраторами. Делегированный администратор может обновлять, удалять политики. Он также может создавать дочерние политики на основе исходной (базовой);

3. Для добавления дополнительных условий можно использовать символ плюс “+”. Условия оцениваются в порядке, указанном в списке – сначала применяется условие в верхней части списка, затем второе, третье и так далее;
4. Нажать кнопку *Add* для сохранения новой политики.

4.2 YARN

Для включения плагина **Ranger YARN** необходимо выполнить следующие действия:

На странице сервиса YARN кластера ADH в разделе “Run action”, выбрать Manager Ranger Plugin.

Выберите необходимое состояние (Enabled/Disabled):

После чего запустится процесс активации плагина и создание дефолтной политике на стороне Ranger.

В статусе должно отображаться успешное выполнение.

4.3 Hive

Для включения плагина **Ranger Hive** необходимо выполнить следующие действия:

На странице сервиса Hive кластера ADH в разделе “Run action”, выбрать Manager Ranger Plugin.

Выберите необходимое состояние (Enabled/Disabled):

После чего запустится процесс активации плагина и создание дефолтной политике на стороне Ranger.

В статусе должно отображаться успешное выполнение.

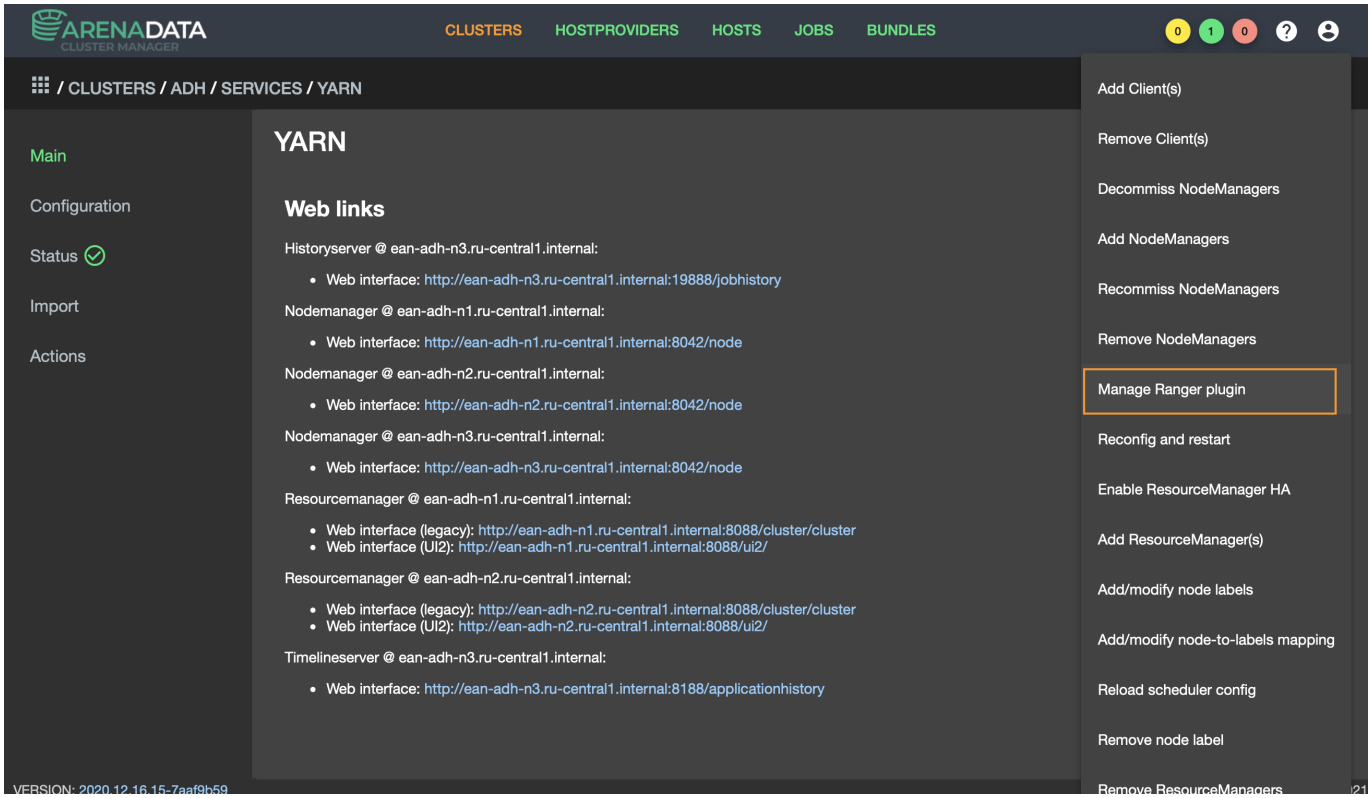
4.4 HBase

Для включения плагина **Ranger HBase** необходимо выполнить следующие действия:

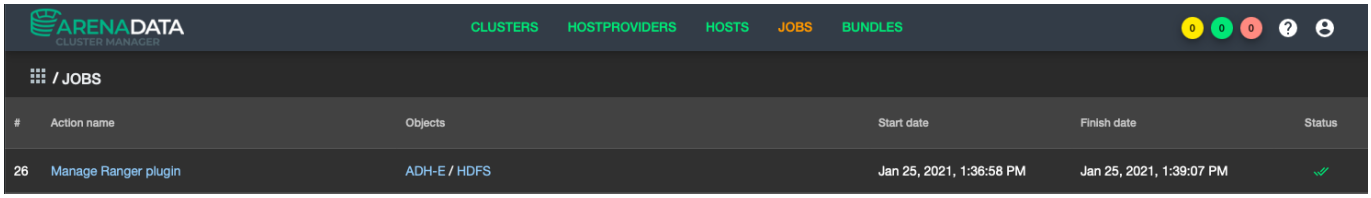
На странице сервиса HBase кластера ADH в разделе “Run action”, выбрать Manager Ranger Plugin.

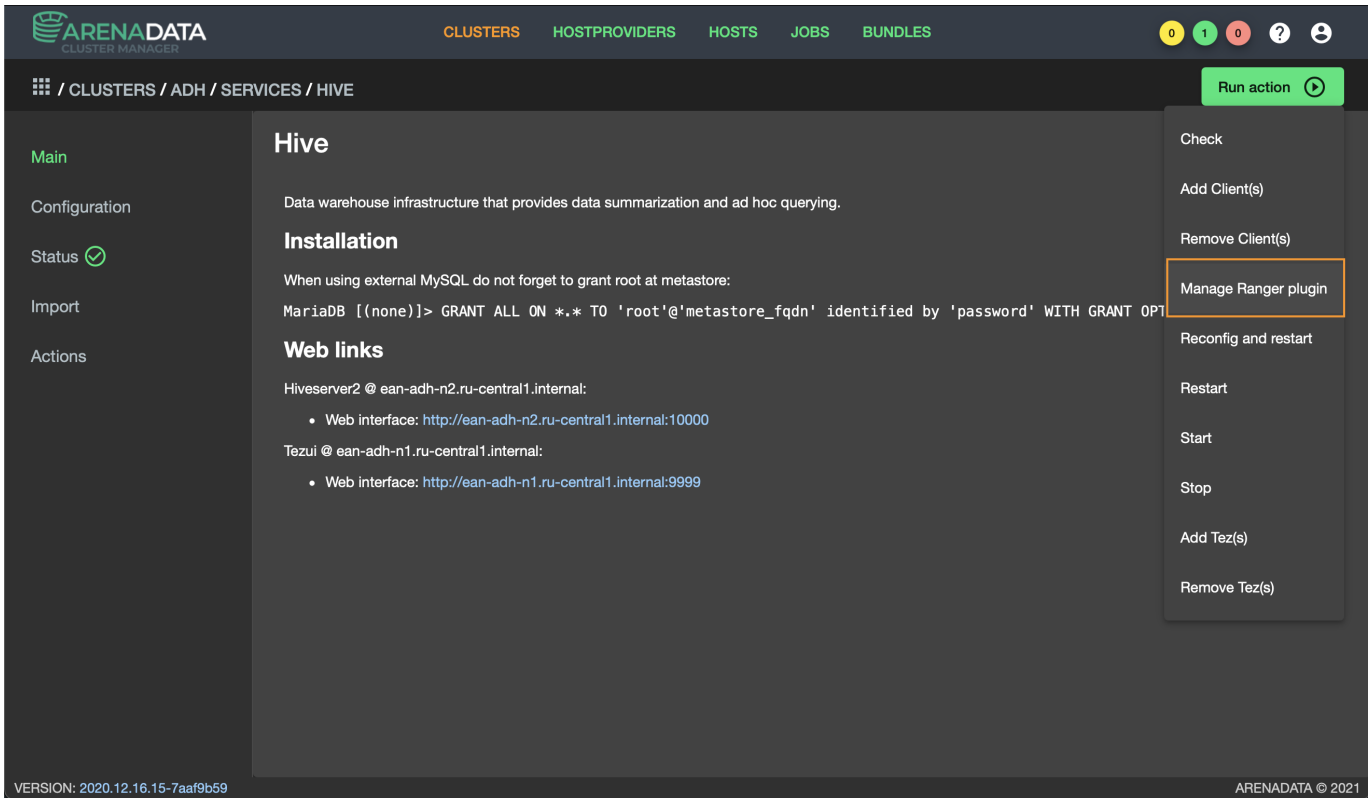
Выберите необходимое состояние (Enabled/Disabled):

После чего запустится процесс активации плагина и создание дефолтной политике на стороне Ranger.

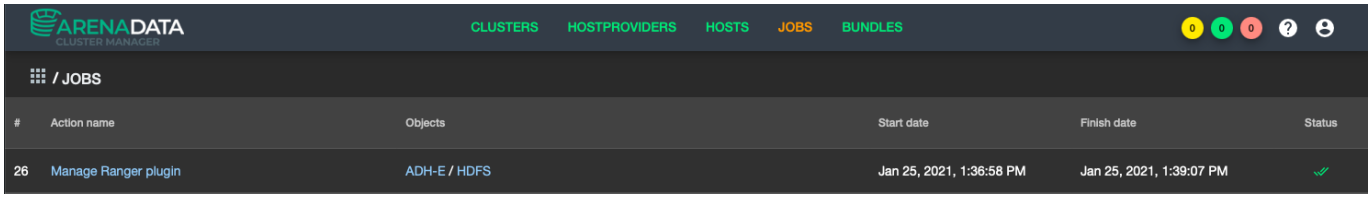

ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ CLUSTERS / ADH / SERVICES / YARN
Main
Configuration
Status
Import
Actions
YARN
Web links
Historyserver @ ean-adh-n3.ru-central1.internal:
Web interface: http://ean-adh-n3.ru-central1.internal:19888/jobhistory
Nodemanager @ ean-adh-n1.ru-central1.internal:
Web interface: http://ean-adh-n1.ru-central1.internal:8042/node
Nodemanager @ ean-adh-n2.ru-central1.internal:
Web interface: http://ean-adh-n2.ru-central1.internal:8042/node
Nodemanager @ ean-adh-n3.ru-central1.internal:
Web interface: http://ean-adh-n3.ru-central1.internal:8042/node
Resourcemanager @ ean-adh-n1.ru-central1.internal:
Web interface (legacy): http://ean-adh-n1.ru-central1.internal:8088/cluster/cluster
Web interface (UI2): http://ean-adh-n1.ru-central1.internal:8088/ui2/
Resourcemanager @ ean-adh-n2.ru-central1.internal:
Web interface (legacy): http://ean-adh-n2.ru-central1.internal:8088/cluster/cluster
Web interface (UI2): http://ean-adh-n2.ru-central1.internal:8088/ui2/
Timelineserver @ ean-adh-n3.ru-central1.internal:
Web interface: http://ean-adh-n3.ru-central1.internal:8188/applicationhistory
Add Client(s)
Remove Client(s)
Decommiss NodeManagers
Add NodeManagers
Recommiss NodeManagers
Remove NodeManagers
Manage Ranger plugin
Reconfig and restart
Enable ResourceManager HA
Add ResourceManager(s)
Add/modify node labels
Add/modify node-to-labels mapping
Reload scheduler config
Remove node label

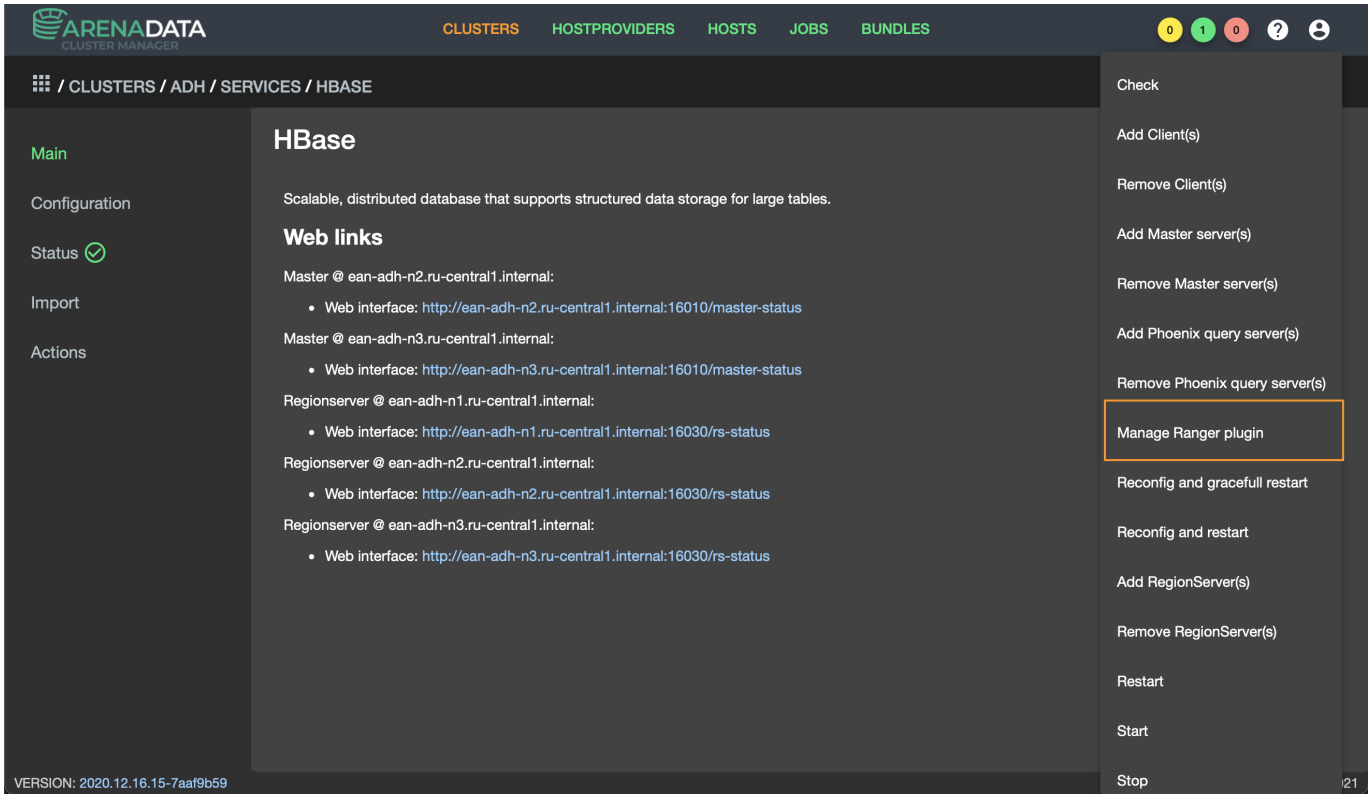

Run an action [Manage Ranger plugin]?
Desired plugin state: enabled ...
Cancel
Run


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ JOBS
Action name Objects Start date Finish date Status
26 Manage Ranger plugin ADH-E / HDFS Jan 25, 2021, 1:36:58 PM Jan 25, 2021, 1:39:07 PM


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ CLUSTERS / ADH / SERVICES / HIVE
Run action
Main
Configuration
Status
Import
Actions
Hive
Data warehouse infrastructure that provides data summarization and ad hoc querying.
Installation
When using external MySQL do not forget to grant root at metastore:
MariaDB [(none)]> GRANT ALL ON *.* TO 'root'@'metastore_fqdn' identified by 'password' WITH GRANT OPT
Web links
Hiveserver2 @ ean-adh-n2.ru-central1.internal:
Web interface: http://ean-adh-n2.ru-central1.internal:10000
Tezui @ ean-adh-n1.ru-central1.internal:
Web interface: http://ean-adh-n1.ru-central1.internal:9999
Check
Add Client(s)
Remove Client(s)
Manage Ranger plugin
Reconfig and restart
Restart
Start
Stop
Add Tez(s)
Remove Tez(s)
VERSION: 2020.12.16.15-7aaf9b59
ARENADATA © 2021

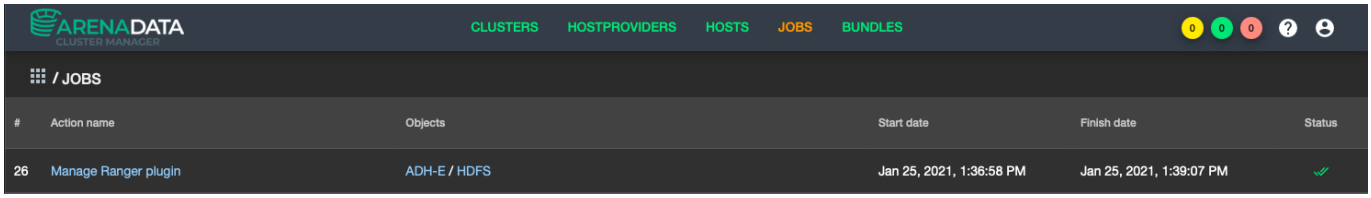

Run an action [Manage Ranger plugin]?
Desired plugin state: enabled ...
Cancel
Run


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ JOBS
Action name Objects Start date Finish date Status
26 Manage Ranger plugin ADH-E / HDFS Jan 25, 2021, 1:36:58 PM Jan 25, 2021, 1:39:07 PM


ARENADATA
CLUSTER MANAGER
CLUSTERS
HOSTPROVIDERS
HOSTS
JOBS
BUNDLES
/ CLUSTERS / ADH / SERVICES / HBASE
Main
Configuration
Status
Import
Actions
HBase
Scalable, distributed database that supports structured data storage for large tables.
Web links
Master @ ean-adh-n2.ru-central1.internal:
Web interface: http://ean-adh-n2.ru-central1.internal:16010/master-status
Master @ ean-adh-n3.ru-central1.internal:
Web interface: http://ean-adh-n3.ru-central1.internal:16010/master-status
Regionserver @ ean-adh-n1.ru-central1.internal:
Web interface: http://ean-adh-n1.ru-central1.internal:16030/rs-status
Regionserver @ ean-adh-n2.ru-central1.internal:
Web interface: http://ean-adh-n2.ru-central1.internal:16030/rs-status
Regionserver @ ean-adh-n3.ru-central1.internal:
Web interface: http://ean-adh-n3.ru-central1.internal:16030/rs-status
Check
Add Client(s)
Remove Client(s)
Add Master server(s)
Remove Master server(s)
Add Phoenix query server(s)
Remove Phoenix query server(s)
Manage Ranger plugin
Reconfig and gracefull restart
Reconfig and restart
Add RegionServer(s)
Remove RegionServer(s)
Restart
Start
Stop
VERSION: 2020.12.16.15-7aaf9b59


Run an action [Manage Ranger plugin]?
Desired plugin state: enabled ...
Cancel
Run

В статусе должно отображаться успешное выполнение.



Глава 5

Управление аудитом в Ranger

5.1 Аудит. Введение

Apache Ranger использует Apache Solr для хранения журналов аудита и обеспечивает поиск пользовательского интерфейса через них. Solr необходимо установить и настроить перед инсталляцией Ranger Admin. Конфигурация по умолчанию для Ranger Audits в Solr использует общий экземпляр Solr, предоставляемый бандлом ADPS. Solr – это и память, и процессор. Если продуктивная система имеет большой объем запросов доступа, необходимо убедиться, что хост Solr имеет достаточную память, процессор и дисковое пространство.

Для доступа к странице Аудита зайдите в основной интерфейс Apache Ranger и затем нажмите «Audit» в верхнем меню.

5.2 Вкладка Access

Предоставляет данные об активности пользователей для всех политик. Политика службы по умолчанию настроена на регистрацию всех действий пользователей в рамках Сервисов. Эта политика по умолчанию не содержит правил доступа для пользователей и групп.

Вы можете фильтровать данные по следующим критериям:

Таблица5.1.: Вкладка Access

Параметр	Описание
Access Enforcer	Ranger (ranger-acl) или Hadoop (hadoop-acl)
Access Type	Тип попытки доступа пользователя (EG, REVOKE, GRANT, OPEN, USE)
Client IP	IP-адрес пользовательской системы, которая пыталась получить доступ к ресурсу
Result	Показывает, была ли операция успешной
Service Name	Имя сервиса, к которой пытался получить доступ пользователь
Service Type	Тип службы, к которой пытался получить доступ пользователь
Start Date, End Date	Фильтрует результаты для определенного диапазона дат
User	Имя пользователя, который пытался получить доступ к ресурсу
Cluster Name	Название кластера

5.3 Вкладка Admin

Вкладка «Admin» содержит все события для аудита веб-интерфейса администрирования безопасности ADH и ADS, включая службу, диспетчер служб, вход в систему и т. Д. (Такие действия, как создание, обновление, удаление, изменение пароля).

Вы можете фильтровать данные по следующим критериям:

Таблица5.2.: Вкладка Admin

Параметр	Описание
Action	Это операции, выполняемые над ресурсами (такие действия, как создание, обновление, удаление, смена пароля)
Audit Type	Существует три значения Resource, asset и xa user в соответствии с операциями, выполняемыми в Service, policy и users
End Date	Время и дата входа в систему сохраняются для каждого сеанса. Диапазон дат используется для фильтрации результатов для этого конкретного диапазона дат
Session ID	Счетчик сеансов увеличивается каждый раз, когда вы пытаетесь войти в систему
Start Date	Время и дата входа в систему сохраняются для каждого сеанса. Диапазон дат используется для фильтрации результатов для этого конкретного диапазона дат
User	Имя пользователя, выполнившего операцию создания, обновления, удаления

5.4 Вкладка Login Sessions

На вкладке «Login Sessions» регистрируется информация, относящаяся к сеансам пользователй для каждого входа в систему.

Вы можете фильтровать данные по следующим критериям:

Таблица5.3.: Вкладка Login Sessions

Параметр	Описание
Login ID	Имя пользователя, под которым кто-то входит в систему
Session-id	Счетчик сеансов увеличивается каждый раз, когда пользователь пытается войти в систему
Start Date, End Date	Указывает, что результаты должны фильтроваться на основе определенной даты начала и даты окончания
Тип входа	Режим, в котором пользователь пытается войти в систему (вводя имя пользователя и пароль)
IP	IP-адрес системы, через которую пользователь вошел в систему
User Agent	Версия браузера или библиотеки, используемая для входа в систему для определенного события (например, Mozilla, Java, Python)
Result	Регистрирует, был ли вход в систему успешным. Возможные результаты: Успех, Неверный пароль, Учетная запись отключена, Заблокирована», Срок действия пароля истек или Пользователь не найден

5.5 Вкладка Plugins

На этой вкладке отображается история и статусы Security Agent. В этом модуле отображаются все службы, экспортированные из системы.

Вы можете фильтровать данные по следующим критериям:

Таблица5.4.: Вкладка Plugins

Параметр	Описание
Plugin IP	IP-адрес агента, который пытался экспортировать службу
Plugin ID	Имя агента, который пытался экспортировать службу
HTTP Response Code	Код HTTP вернулся при попытке экспорта службы
Start Date, End Date	Время и дата экспорта сохраняются для каждого агента. Диапазон дат используется для фильтрации результатов для этого конкретного диапазона дат
Service Name	Имя службы, которую мы пытаемся экспортировать
Cluster Name	Название кластера

5.6 Вкладка Plugins Status

На этой вкладке показаны политики, действующие для каждого плагина. Включает соответствующую информацию о хосте, а также о том, когда плагин загружен и начал применять политики.

Таблица5.5.: Критерии фильтра

Параметр	Описание
Host Name	Имя Хоста
Plugin IP	IP-адрес агента, использующего плагин
Service Name	Имя службы, содержащей политики
Service Type	Компонент