Arenadata™ Streaming

Версия - v1.5-RUS

Руководство администратора по работе с Nifi

2020 Arenadata™

Оглавление

1 Kerberos Service **3**

В руководстве приведены сведения для администраторов системы по работе с платформой ADS в части сервиса Nifi – рекомендации по конфигурации, аутентификация пользователей с настройками их политик и доступа, Kerberos.

Руководство может быть полезно администраторам, программистам, разработчикам и сотрудникам подразделений информационных технологий, осуществляющих сопровождение платформы.

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

Глава 1

Kerberos Service

NiFi может быть настроен для использования Kerberos SPNEGO (или “Kerberos Service”) для аутентификации. В таком случае пользователи попадают в конечную точку REST */access/kerberos*, и сервер отвечает кодом состояния *401* с заголовком задачи *WWW-Authenticate: Negotiate*. Далее сервер связывается с браузером для использования GSS-API и загрузки тикета пользователя Kerberos с указанием его в качестве заголовка *Base64* в последующем запросе. Он принимает форму *Authorization: Negotiate YII...*, и **NiFi** пробует подтвердить этот билет с помощью KDC. В случае успеха принципал пользователя возвращается как подлинный, и поток следует аутентификации login/credential, в результате которой в ответ выдается JWT для предотвращения ненужных издержек аутентификации Kerberos при каждом последующем запросе. В случае если билет пользователя не подтверждается, то он возвращается с соответствующим кодом ошибки. После чего пользователь может предоставить свои учетные данные для формы регистрации Kerberos при условии настроенного *KerberosLoginIdentityProvider*. Дополнительную информация приведена в главе Kerberos.

NiFi отвечает на запросы Kerberos SPNEGO только по соединению HTTPS, поскольку незащищенные запросы никогда не проходят проверку подлинности.

Для включения аутентификации службы Kerberos в *nifi.properties* должны быть настроены следующие свойства:

Таблица1.1.: Свойства для включения аутентификации Kerberos Service

Свойство	Значаение	Описание
Service Principal	true	Принципал сервиса, используемый NiFi для связи с KDC
Keytab Location	true	Путь к файлу keytab, содержащему принципал сервиса

Примечания:

- Kerberos чувствителен к регистру во многих местах, и сообщения об ошибках (или их отсутствие) могут быть недостаточно понятны. Рекомендуется проверить у службы чувствительность к регистру в конфигурационных файлах. Конвенция – *HTTP/fully.qualified.domain@REALM*;
- Браузеры имеют разные уровни ограничений при работе с SPNEGO. Некоторые из них предоставляют локальный тикет Kerberos в любой запрашиваемый домен, в то время как другие выдают пустой список доверенных доменов. Справочная информация для общих браузеров приведена по ссылке;
- Некоторые браузеры (например, устаревший IE) не поддерживают последние алгоритмы шифрования, такие как AES, и ограничены устаревшими алгоритмами (например, DES). Это следует учитывать при создании keytabs;

- Должен быть настроен KDC, определен принципал сервиса для NiFi и экспортирован keytab. Подробные инструкции по настройке и администрированию Kerberos Service выходят за рамки данного документа (MIT Kerberos Admin Guide), но далее приведен пример.

  Пример добавления принципала для сервера на *nifi.nifi.apache.org* и экспорта ключа из KDC:

```
root@kdc:/etc/krb5kdc# kadmin.local
Authenticating as principal admin/admin@NIFI.APACHE.ORG with password.
kadmin.local:  listprincs
K/M@NIFI.APACHE.ORG
admin/admin@NIFI.APACHE.ORG
...
kadmin.local:  addprinc -randkey HTTP/nifi.nifi.apache.org
WARNING: no policy specified for HTTP/nifi.nifi.apache.org@NIFI.APACHE.ORG; defaulting to no␣
↪policy
Principal "HTTP/nifi.nifi.apache.org@NIFI.APACHE.ORG" created.
Principal "HTTP/nifi.nifi.apache.org@NIFI.APACHE.ORG" created.
kadmin.local:  ktadd -k /http-nifi.keytab HTTP/nifi.nifi.apache.org
Entry for principal HTTP/nifi.nifi.apache.org with kvno 2, encryption type des3-cbc-sha1 added to␣
↪keytab WRFILE:/http-nifi.keytab.
Entry for principal HTTP/nifi.nifi.apache.org with kvno 2, encryption type des-cbc-crc added to␣
↪keytab WRFILE:/http-nifi.keytab.
kadmin.local:  listprincs
HTTP/nifi.nifi.apache.org@NIFI.APACHE.ORG
K/M@NIFI.APACHE.ORG
admin/admin@NIFI.APACHE.ORG
...
kadmin.local: q
root@kdc:~# ll /http*
-rw------- 1 root root 162 Mar 14 21:43 /http-nifi.keytab
root@kdc:~#
```