Функциональность блокировки по IP

Описание функциональности

Как одно из средств защиты от перебора учетных данных в UIDM реализован механизм блокировки по IP-адресам пользователя.

Если за заданный промежуток времени количество неуспешных попыток аутентификации пользователя с некоторого IP-адреса превысит заданный порог, то все дальнейшие попытки аутентификации пользователя с этого IP будут заблокированы, то есть заканчиваться ошибкой ip blocked. Разблокировка IP произойдет автоматически по истечении заданного промежутка времени.

IP адрес пользователя определяется по HTTP-заголовку `X-Forwarded-For` (может быть настроено использование другого заголовка) в запросах на аутентификацию.

NOTE	В случае, если запросы на аутентификацию приходят не с клиентского устройства, а с сервера, крайне важно, чтобы сервер добавлял в запросы заголовок `X-Forwarded-For` с IP-адресом пользователя. В противном случае UIDM будет в качестве IP получать IP самого сервера, и, как результат - заблокировать все запросы с этого сервера.

Устройство функциональности

Функциональность реализована в основном компоненте - `sso-server` .

В работе функциональность использует 2 структуры данных:

1. Информация о неуспешных попытках аутентификации для заданного IP. По умолчанию эта информация получается из подсистемы аудита, т.к. в аудите протоколируются все неуспешные попытки пользователей. Как альтернативное решение, существует возможность хранения этой информации в Hazelcast. Использование Hazelcast позволяет снизить нагрузку на СУБД, где хранятся данные аудита.
2. Информация о заблокированных IP. Хранится в СУБД в выделенной таблице `BlockedIpAddress`. Основные атрибуты таблицы: `ipAddress` - заблокированный адрес в виде числа, `blockedTo` - время, до которого действует блокировка. Для одного адреса в таблице может существовать несколько записей для разных периодов блокировки.

Настройки функциональности

```
# описание: Использовать ли механизм хранения IP проваливших аутентификацию в
Hazelcast. Если RDBMS -- хранить в БД аудита
# тип даных: string
# единицы измерения: нет
# значение по умолчанию: RDBMS
# ограничения: RDBMS или Hazelcast
com.rooxteam.uidm.blocking.ip.engine=RDBMS
```

Настройки СУБД задаются в стандартных параметрах подключения к СУБД аудита.

При использовании Hazelcast необходимо настроить параметры подключения к нему:

```
# описание: Список инстансов Hazelcast для пдключения
# тип даных: string[]
# единицы измерения: hostname:IP
# ограничения: не пустое, если используем Hazelcast
com.rooxteam.sso.hazelcast.urls=

# описание: Имя "группы серверов", username в терминологии Hazelcast
# тип даных: string
# единицы измерения: нет
# ограничения: не пустое, если используем Hazelcast
com.rooxteam.sso.hazelcast.group.name=

# описание: Пароль для доступа к Hazelcast
# тип даных: string
# единицы измерения: нет
# ограничения: не пустое, если используем Hazelcast
com.rooxteam.sso.hazelcast.group.password=
```

Параметры, управляющие блокировками:

```
# описание: выключатель функциональности блокировки по IP
# тип данных: boolean
# единицы измерения: нет
# значение по умолчанию: true
com.rooxteam.uidm.block.ip.enabled=true

# описание: количество неуспешных попыток аутентификации для блокировки IP-адреса
# тип данных: integer
# единицы измерения: штуки
# ограничения: положительное значение
# значение по умолчанию: 240
com.rooxteam.uidm.auth.fail.ip.block.limit=10000

# описание: длительность интервала, за который подсчитывается число неуспешных попыток
# тип данных: integer
# единицы измерения: секунды
# ограничения: положительное значение
# значение по умолчанию: 86400 (1 сутки)
com.rooxteam.uidm.block.ip.count.period.seconds=86400

# описание: длительность блокировки IP-адреса
# тип данных: integer
# единицы измерения: секунды
# ограничения: положительное значение
# значение по умолчанию: 86400 (1 сутки)
com.rooxteam.uidm.block.ip.seconds=86400
```