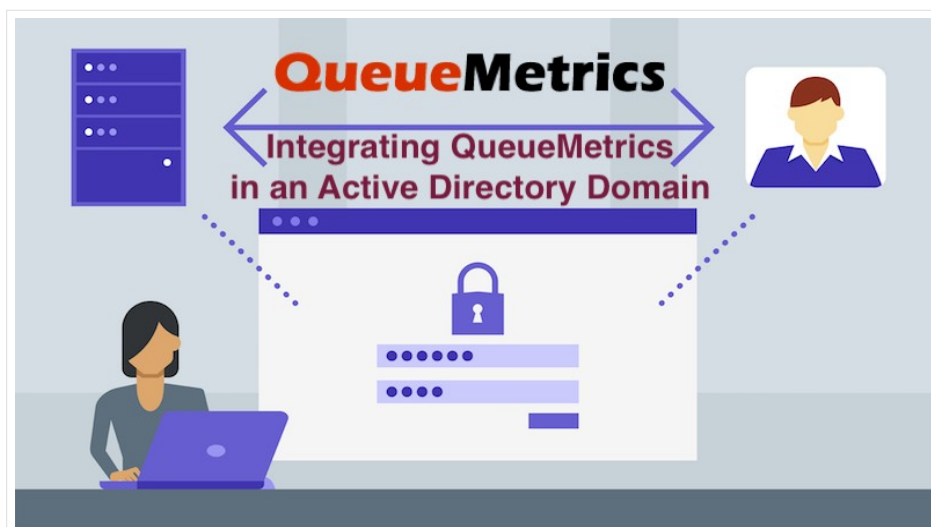


Интеграция QueueMetrics в домен Active Directory



Active Directory (AD) - служба каталогов, разработанная Microsoft для доменной организации сетей Windows. Она базируется на протоколе LDAP и широко используется для централизованного управления пользователями в крупных организациях, от централизованного хранения паролей до управления всеми услугами компании.

Используя Active Directory или аналогичные решения на основе LDAP (например, OpenLDAP, Apache Directory Services и многие другие), компания может управлять всеми пользователями всех служб и всеми компьютерами относительно простым способом - не потребуется управлять учетными данными и доступом для каждого из пользователей в каждом приложении, которое запускается.

QueueMetrics может интегрироваться с Active Directory и любым другим сервером LDAP, используя собственный API LDAP для верификации учетных данных пользователя.

Начало работы: учетные данные и терминология

Первое, что нужно сделать, это убедиться, что есть действующий набор учетных данных. Это то, что необходимо получить от системного администратора Active Directory.

Требуется:

- URI LDAP для подключения к контроллеру домена (Domain Controller), например `ldap:ad.example.com:389`

- Выделенное имя (Distinguished Name, DN) LDAP и его пароль. DN - это ваш «логин» и обычно имеет либо длинную форму, например CN=Peter Parker,CN=Users,DC=example,DC=com либо (в системах Active Directory) может быть адресом электронной почты пользователя. В терминологии LDAP вход на удаленный сервер LDAP называется связыванием.
- «База» LDAP, то есть точка в дереве LDAP, с которой нужно начать поиск. В системах ActiveDirectory это выглядит примерно так CN=Users,DC=example,DC=com

На данном этапе нужно установить небольшой инструмент под названием `ldapsearch`; в Linux его можно получить, выполнив:

```
yum install -y openldap-clients
```

По завершении можно проверить, что все правильно, выполнив следующую команду (замените URI, DN, пароль и базу при необходимости):

```
ldapsearch -H ldap://ad.example.com:389 -x -w 'Spiderman' -D "pparker@example.com" -b "CN=Users,DC=example,DC=com"
```

Если получили распечатанный (возможно, длинный) список объектов, то учетные данные действительны, и можно видеть пользователей в каталоге своей компании.

```
# extended LDIF
#
# LDAPv3
# base <CN=Users,DC=example,DC=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
...many elements skipped...
# Guest, Users, example.com
dn: CN=Guest,CN=Users,DC=example,DC=com
objectClass: top
objectClass: person
```

objectClass: organizationalPerson
objectClass: user
cn: Guest
description: Built-in account for guest access to the computer/domain
distinguishedName: CN=Guest,CN=Users,DC=example,DC=com
instanceType: 4
whenCreated: 20210812150455.0Z
whenChanged: 20210812150455.0Z
uSNCreated: 8197
memberOf: CN=Guests,CN=Builtin,DC=example,DC=com
name: Guest
objectGUID:: P5yymq0Cwkm4w7/5otuyMQ==
userAccountControl: 66082
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 514
objectSid:: AQUAAAAAAAAUAAAAeigMKVkbGFLp3j0A9QEAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Guest
sAMAccountType: 805306368

```
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
isCriticalSystemObject: TRUE
dSCorePropagationData: 20210812150617.0Z
dSCorePropagationData: 16010101000001.0Z

# search result
search: 2
result: 0 Success

# numResponses: 29
# numEntries: 28
```

Как видите, каждая запись имеет множество атрибутов; можно использовать их в запросах для получения точных записей каталога, которые вы ищете. Если удалось это сделать, это означает, что ваши учетные данные действительны, и можно начать настройку QueueMetrics для доступа к LDAP.

Использование Active Directory из QueueMetrics

Вообще говоря, для этого понадобятся локальные учетные записи QueueMetrics для каждого пользователя в AD. Следовательно, нужно создать «нормальные» учетные записи, включить их, установить для них правильные классы и т.д., и затем установить случайный пароль, чтобы их нельзя было использовать.

В простейшем случае, когда просто хотите, чтобы QueueMetrics принимал предоставленные пользователем логин и пароль, пытался использовать их для «привязки» к серверу, и если сервер допускает успешную привязку (то есть, если учетные данные верны), то загрузите пользователя, определенного в QM, с тем же логином.

Если пользователь не проходит верификацию AD, можно сообщить QM, что вход в систему должен быть отклонен сразу (и это значение по умолчанию), или попытаться выполнить «локальный» вход. Это называется «делегированной» аутентификацией, потому что сервер LDAP фактически делегирует QM для выполнения своей собственной работы, и это полезно, так как не нужно определять каждого пользователя в LDAP, чтобы дать всем возможность работать.

Чтобы такой сценарий работал, просто добавляете следующие строки в файл `configuration.properties`:

```
auth.externalSource=ldap
auth.verboseLog=false
```

```
auth.IdapServerUrl=ldap://ad.example.com:389
auth.IdapBind=cn=${login},dc=example,dc=com
auth.IdapFailureDelegates=true
```

Теперь войдите в систему, как один из пользователей, и это должно работать, как ожидалось. Обратите внимание, как значения, например `ldapBind`, создаются путем замены заполнителей значениями, введенными пользователем.

Использование различных входов в систему

Иногда нужно использовать логины, отличных от тех, которые пользователи вводят физически для входа в систему. Это частая ситуация, как это ни печально, поскольку системы ActiveDirectory являются общекорпоративными объектами, и часто вы не можете контролировать формат создаваемых там входов в систему.

QM довольно разборчив с точки зрения того, как должен выглядеть логин агента, поэтому необходимо указать QM использовать другой логин. К счастью, в Active Directory в пользовательской схеме по умолчанию есть набор пустых атрибутов расширения (Extension Attributes), которые можно свободно устанавливать для таких целей. Они появятся в LDAP с именем вроде `msDS-cloudExtensionAttribute7`. В одном из них вы должны указать используемый логин QM, и это для каждого пользователя, которому требуется доступ к QM.

Итак, допустим, вы хотите, чтобы пользователь вошел в систему с идентификатором своей компании (например, `pparker`). Сначала добавим доменную часть, чтобы пользователь на самом деле был `pparker@example.com`, таким образом формируя допустимое значение для связывания. После успешного связывания ищем пользователя с именем учетной записи, совпадающим с введенным логином, и когда его находим, читаем его Атрибут расширения номер 7 (Extension Attribute number 7), чтобы определить фактический логин, который будет использовать QM.

Итак, если пользователь выглядит подобным образом в AD:

```
# Peter Parker, Users, example.com
dn: CN=Peter Parker,CN=Users,DC=example,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Peter Parker
sn: Parker
```

```
givenName: Peter
distinguishedName: CN=Peter Parker,CN=Users,DC=example,DC=com
displayName: Peter Parker
name: Peter Parker
sAMAccountName: pparker
userPrincipalName: pparker@example.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
msDS-cloudExtensionAttribute7: agent/101
mail: pparker@example.com
```

Можно использовать следующую конфигурацию в QM:

```
auth.externalSource=ldap
auth.verboseLog=false

auth.ldapServerUrl=ldap://ad.example.com:389
auth.ldapBind=${login}@example.com
auth.ldapFailureDelegates=true

auth.ldapLoginAttr=msDS-cloudExtensionAttribute7
auth.ldapBase=CN=Users,dc=example,dc=com
auth.ldapQuery=(sAMAccountName=${login})
```

На данном этапе можно войти в систему как `pparker`, и QM откроет страницу для `agent/101`.

Не работает - что делать?

Убедитесь, что установили `auth.verboseLog=true` и попробуйте войти в систему, одновременно проверяя файл `queuemetrics-(date).log`.

Если видите такие записи:

```
it.loway.tpf.transaction.user.AuthOverLDAP.authOverRpc LDAP: Binding 'pparker@example.com' on 'ldap://ad.example.com:389'
```

```
it.loway.tpf.transaction.user.AuthOverLDAP.authOverRpc LDAP auth failed for 'pparker'
```

```
javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090439, comment: AcceptSecurityContext error, data 52e, v4563]
```

Это означает, что введен неправильный пароль. Проверьте это с помощью `ldapsearch`. Обратите внимание, что при использовании делегированной аутентификации LDAP всегда проверяется в первую очередь, поэтому будет получено сообщение об ошибке до того, как будет загружен локальный пользователь.

Когда все идет хорошо, увидите журнал вроде:

```
it.loway.tpf.transaction.user.AuthOverLDAP.authOverRpc LDAP: Binding 'pparker@example.com' on 'ldap://ad.example.com:389'
```

```
it.loway.tpf.transaction.user.AuthOverLDAP.queryLdapAttribute LDAP: Attribute 'msDS-cloudExtensionAttribute7' is set to 'agent/101'
```

Если используете настраиваемые запросы LDAP, обязательно протестируйте их.

Очень полезно проверять журналы аудита (Домашняя страница -> Системное администрирование -> Журналы аудита) (Home Page -> System Administration -> Audit Logs), чтобы видеть ошибки и успешные входы в систему.

Date	User	Session	Action	Text 1	Text 2	Text 3	Text 4
2021-08-23 23:12:37	Agent/101	AC62F6...97576D	Logon	Agent/101	10.0.2.2	pparker	

Обратите внимание, что если используется перезапись имени входа, исходное имя пользователя, предоставленное пользователем, отображается в столбце 3, а фактический пользователь, который вошел в систему QM, отображается в столбце 1.

При ошибках, конечно, доступен только логин, указанный пользователем.

Дальнейшие детали

А как насчет веб-сервисов?

Как правило, все веб-службы (как и любой другой вход в систему) будут проверяться в ActiveDirectory. Это может быть или не быть тем, что вы хотите, например, потому что:

- некоторые службы (например, загрузка данных, когда пользователь `webqloader` используется для загрузки данных) могут запускать вход в систему несколько раз в секунду
- иногда политика компании не позволяет создавать пользователей для служб в LDAP, поскольку они на самом деле не являются «сотрудниками» и не могут относиться к ним.

Для обработки таких случаев можно указать список пользователей, которые НЕ должны проверяться в LDAP, а верифицироваться только локально, например:

```
auth.ldapIgnoreUsers=webqloader,robot
```

И у них будет проверяться только их пароль в локальной базе данных пользователей QM.

Будут ли работать задания cron при переходе на LDAP?

Да, будут. Они НЕ выполняют вход в систему, а только «олицетворяют» пользователя, который должен их запускать.

Можно ли использовать Secure LDAP?

LDAP - старый протокол, основанный на открытом тексте; это открывает доступ к перехвату паролей и другим формам кражи учетных данных.

Можно прозрачно использовать сервер LDAPS, просто заменив <ldap://ad.example.com:389> на <ldaps://ad.example.com:686>, если ваш DC поддерживает его.

Доступно ли это в моей системе QM?

Поддержка LDAP доступна с QM 21.04; перезапись доступна с QM 21.04.4

Поддерживаются ли QM другие внешние системы аутентификации?

Да: драйвер HTTP/S JSON (полезен для интеграции с чем-либо еще, поддерживает перезапись, игнорирование пользователей, и даже прозрачное создание пользователей) и устаревший драйвер XML-RPC.

Ссылки

Программное обеспечение QueueMetrics доступно «on premise» или как облачный хостинг для FreePBX, Yeastar S PBX, Grandstream PBX, Issabel, FusionPBX и других дистрибутивов Asterisk.

Более подробную техническую информацию смотрите в [User Manual](#).

Посетите www.queuemetrics.com для получения 15-дневной бесплатной полнофункциональной пробной версии.

Обратите внимание на [Free Webinars](#) с живой демонстрацией QueueMetrics.