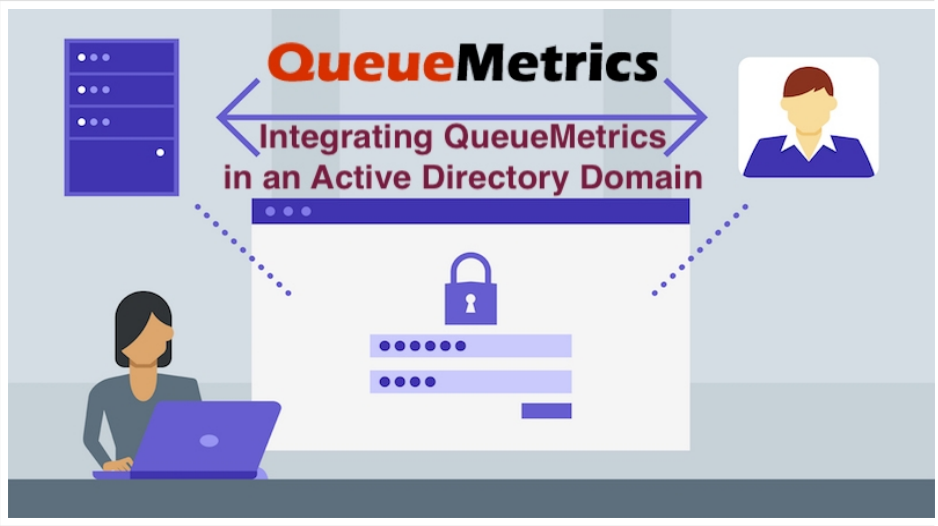
Loway presenta

Integración de QueueMetrics en un dominio de Active Directory



Active Directory (AD) es un servicio de directorio desarrollado por Microsoft para las redes de dominio de Windows. Se basa en el protocolo LDAP y se utiliza ampliamente para proporcionar una gestión centralizada de usuarios en grandes organizaciones, desde el almacenamiento centralizado de contraseñas hasta el aprovisionamiento de todos los servicios de la empresa.

Mediante el uso de Active Directory o soluciones similares basadas en LDAP (por ejemplo, OpenLDAP, Apache Directory Services y muchas otras) su empresa puede gestionar todos los usuarios en todos los servicios y todos los ordenadores de una manera relativamente sencilla: no necesita gestionar las credenciales y el acceso de cada usuario en cada aplicación que ejecute.

QueueMetrics puede integrarse con Active Directory y cualquier otro servidor LDAP aprovechando sus APIs LDAP para verificar las credenciales de los usuarios.

Introducción: credenciales y terminología

Lo primero que tienes que hacer es asegurarte de que tienes un conjunto válido de credenciales en tu mano. Esto es algo que tienes que obtener de tu administrador del sistema de Active Directory.

Necesitas:

- Un URI LDAP para conectarse a su controlador de dominio, por ejemplo `ldap:ad.example.com:389`
- Un Nombre Distinguido LDAP y su contraseña. Un DN es su "login" y suele tener una forma larga como `CN=Peter Parker,CN=Users,DC=example,DC=com` o (en los sistemas de Active Directory) puede ser la

dirección de correo electrónico del usuario. En la terminología de LDAP, el inicio de sesión en el servidor LDAP remoto se llama vinculación.

- Una "base" LDAP, es decir, el punto del árbol LDAP en el que debemos empezar a buscar. En los sistemas ActiveDirectory tiene un aspecto similar al siguiente CN=Users,DC=example,DC=com

En este punto debes instalar una pequeña herramienta llamada ldapsearch; en Linux puedes obtenerlo emitiendo:

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

Una vez hecho esto, puedes comprobar que todo es correcto ejecutando el siguiente comando (sustituye la URI, el DN, la contraseña y la base según corresponda):

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

Si obtienes una lista (posiblemente larga) de objetos impresos, sus credenciales son válidas y puedes ver los usuarios en el directorio de su empresa.

```
# 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:: AQUAAAAAAAUVAAAAeigMKVkbGFLp3j0A9QEAAA==
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
```

Observa cómo cada entrada tiene un montón de atributos; puedes utilizarlos en las consultas para recuperar las entradas exactas del directorio que estás buscando. Si has podido llegar hasta aquí, esto significa que tus credenciales son válidas y puedes empezar a configurar QueueMetrics para acceder a LDAP.

Uso de Active Directory desde QueueMetrics

En general, se necesita una cuenta local de QueueMetrics para cada usuario en AD. Por lo tanto, tienes que crear cuentas "normales", habilitarlas, configurarlas con las clases correctas, etc., y luego establecer una contraseña aleatoria para que no puedan ser utilizadas.

En el caso más sencillo, sólo quiere que QueueMetrics tome el nombre de usuario y la contraseña suministrados por el usuario, intente usarlos para "enlazar" con el servidor, y si el servidor permite un enlace exitoso (es decir, si las credenciales son correctas), cargue el usuario que está definido en QM con el mismo nombre de usuario.

Si el usuario falla en la verificación de AD, puedes decirle a QM que el inicio de sesión debe ser rechazado de plano (y eso es lo predeterminado) o que intente un inicio de sesión "local". Esto se llama autenticación "delegada" porque el servidor LDAP realmente delega a QM para que haga su propio trabajo, y es útil para no tener que definir todos y cada uno de los usuarios en LDAP para que funcionen.

Para que este escenario funcione, basta con añadir las siguientes líneas a su configuration.properties:

```
auth.externalSource=ldap

auth.verboseLog=false



auth.ldapServerUrl=ldap://ad.example.com:389

auth.ldapBind=cn=${login},dc=example,dc=com

auth.ldapFailureDelegates=true
```

Ahora inicia sesión con uno de sus usuarios, y debería funcionar como se espera. Observa cómo los valores, por ejemplo el ldapBind, se construyen reemplazando los marcadores de posición con los valores que su usuario introdujo.

Utilizar diferentes inicios de sesión

A veces, es necesario utilizar usuarios diferentes de los que los usuarios introducen físicamente para iniciar la sesión. Esto es bastante común, ya que tristemente los sistemas de ActiveDirectory son entidades de toda la empresa, y a menudo no se tiene control sobre el formato de los inicios de sesión que se crean allí.

QM es bastante quisquilloso en cuanto a cómo se supone que debe ser el login de un agente, por lo que es necesario decirle a QM que utilice un login diferente. Por suerte, en Active Directory, el esquema de usuario por defecto tiene un conjunto de Atributos de Extensión vacíos que pueden ser configurados libremente para tales fines. Aparecerán en LDAP con un nombre como msDS-cloudExtensionAttribute7. En uno de ellos, se debe especificar el login de QM a utilizar, y esto para cada usuario que necesite acceder a QM.

Así que, digamos que quieres que un usuario se registre con el ID de su empresa (por ejemplo, pparker). Primero añadiremos una parte de dominio para que el usuario sea realmente pparker@example.com, formando así un valor válido para la vinculación. Una vez que la vinculación es exitosa, vamos a buscar un usuario que tenga un nombre de cuenta que coincida con el inicio de sesión introducido, y cuando lo encontramos, leemos su Atributo de Extensión número 7 para determinar el inicio de sesión real que usará QM.

Entonces, si el usuario aparece así en 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
```

Podemos utilizar la siguiente configuración en 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})
```

En este punto, puede iniciar la sesión con `pparker` y QM abrirá la página para `agent/101`.

No funciona: ¿qué puedo hacer?

Asegúrate de establecer `auth.verboseLog=true` e intenta iniciar la sesión, mientras compruebas el archivo `queuemetrics-(date).log`.

Si ves entradas como esta:

```
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]
```

Esto significa que tienes una contraseña incorrecta. Compruébala con `ldapsearch`. Ten en cuenta que cuando utilizas la autenticación delegada, siempre se comprueba primero el LDAP, por lo que obtendrás un error antes de cargar el usuario local.

Cuando todo vaya bien, verás un registro como:

```
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'
```

Si utilizas consultas LDAP personalizadas, asegúrate de probarlas.

Es muy útil revisar los registros de auditoría (Página de inicio -> Administración del sistema -> Registros de auditoría) para poder ver los errores y los inicios de sesión exitosos.

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	

Ten en cuenta que si utilizas la reescritura del login, el login original suministrado por el usuario aparece en la columna 3, mientras que el usuario real que se conectó a QM aparece en la columna 1.

En caso de error, por supuesto, el único nombre de usuario disponible es el que el usuario proporcionó.

Profundizando

¿Qué hay de los servicios web?

En general, todos los servicios web (como cualquier otro inicio de sesión) se comprobarán con ActiveDirectory. Esto puede o no ser lo que deseas, por ejemplo, porque

- algunos servicios (por ejemplo, la carga de datos, con el usuario webqloader utilizado para cargar datos) pueden desencadenar un inicio de sesión varias veces por segundo
- A veces las políticas de la empresa no permiten crear usuarios de servicio en LDAP, ya que no son realmente "empleados", por lo que no pueden pertenecer allí.

Para manejar estos casos, es posible especificar una lista de usuarios que NO deben ser comprobados en LDAP, sino sólo localmente, por ejemplo

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

Y esos sólo tendrán su contraseña comprobada en la base de datos local de usuarios de QM.

¿Seguirán funcionando las tareas cron si cambio a LDAP?

Sí, lo harán. NO realizan un inicio de sesión, sino que sólo "suplantan" al usuario que se supone que los ejecuta.

¿Puedo utilizar Secure LDAP?

LDAP es un protocolo antiguo, y está basado en texto claro; esto lo expone a que se puedan ojear las contraseñas y a otras formas de robo de credenciales.

Puedes utilizar de forma transparente un servidor LDAPS, simplemente sustituyendo `ldap://ad.example.com:389` con `ldaps://ad.example.com:686`, siempre que su DC lo admita.

¿Está disponible en mi sistema QM?

La compatibilidad con LDAP está disponible desde QM 21.04; la reescritura está disponible desde QM 21.04.4

¿Existen otros sistemas de autenticación externos compatibles con QM?

Sí: un controlador HTTP/S JSON (útil para integrarse con cualquier otra cosa, que admite la reescritura, los usuarios ignorados e incluso la creación transparente de usuarios), y un controlador XML-RPC heredado.

Referencias de QueueMetrics

El software QueueMetrics está disponible en las instalaciones o como un servicio alojado en la nube para FreePBX, Yeastar S PBX, Grandstream, Issabel, FusionPBX y muchas otras distribuciones de Asterisk.

Para más información técnica, consulte el Manual del Usuario.

Visita www.queuemetrics.com para obtener una prueba gratuita de 15 días con todas las funciones.

Asiste a nuestros Webinars gratuitos para una demostración en vivo de QueueMetrics.