Integrating the ovirt-engine to an External Authentication mechanism

Authenticating users from an Active Directory domain

Marcos Sungaila
Sr Principal Technical Product Manager
Oracle Linux & Virtualization
September 2021
Marcos Sungaila

Sr Principal Technical Product Manager
Oracle Linux & Virtualization

- Linux user since 1994
- Professionally working with Linux since 1998
- Started with Virtualization back in 2005
- Virtualization with Open Source tools since 2008
Agenda

1. Pre-requisites
   • Microsoft Windows user account
   • DNS records for plain and secure connections
   • Importing Windows AD-DS CA public key
2. Configuring an External Authentication mechanism
   • Giving permissions to an external user
3. Troubleshooting the AD ldap connection
4. Removing an External Authentication mechanism
Microsoft Windows AD-DS does not allow anonymous LDAP user lookups.

```bash
$ ldapsearch -x -LLL -h 192.168.0.51 -b dc=example,dc=com
Operations error (1)
Additional information: 000004DC: LdapErr: DSID-0C090A22, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v3839
```

In general LDAP lookups occurs through plain text connections.

```bash
$ ldapsearch -x -LLL -h 192.168.0.51 -D cn=administrator,cn=users,dc=example,dc=com \ 
-b dc=example,dc=com
Enter LDAP Password:
dn: DC=example,DC=com
...
distinguishedName: DC=example,DC=com
...
```

**Using administrator account for this operation is not recommended.**
Prerequisites – Windows user account – continuation

Create a user for this specific operation. It can be a service account.

![Image of user creation screen]

- Create in: EXAMPLE.COM/Managed Service Accounts
- First name: Oracle Vtit Svc Integration
- Last name: Account
- Full name: Oracle Vtit Svc Integration Account
- User logon name: oraclesvc01vm
- User logon name (pre-Windows 2000): EXAMPLE\ oraclesvc01vm
Prerequisites – Windows user account – continuation

To connect to the AD-DS server, you will need the user DN or its UPN. Use the `dsquery` command to identify its DN.

If you cannot list a user’s DN, use its UPN for authentication in the form of `<user@domain>`.
You can test user authentication using the ldapsearch command:

```
$ ldapsearch -x -LLL -h 192.168.0.51 -D oraclesvcolvm@example.com -b dc=example,dc=com
```

Enter LDAP Password:

dn: DC=example,DC=com
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=example,DC=com
...

Prerequisites – Windows user account – continuation
Prerequisites – DNS records

Every AD-DS domain server provides SRV DNS records for LDAP service.

This record is in the form of `_ldap._tcp.<domain>`

```
$ host -t srv _ldap._tcp.example.com
Using domain server:
  Name: 192.168.0.51
  Address: 192.168.0.51#53
Aliases:

_ldap._tcp.example.com has SRV record 0 100 389 ad-ds.example.com.
```

This output is the expected behave.
If you receive an error message like this:

$ host -t srv _ldap._tcp.example.com
Host _ldap._tcp.example.com not found: 3(NXDOMAIN)

In general, it means you are using the wrong nameserver for hostname resolution.

Try pointing your command to the AD-DS server as a DNS resolver to confirm:

$ host -t srv _ldap._tcp.example.com <YOUR_AD_DS DOMAIN SERVER>
Using domain server:
  Name: <YOUR_AD_DS DOMAIN SERVER>
  Address: <YOUR_AD_DS DOMAIN SERVER> #53
  Aliases:

  _ldap._tcp.example.com has SRV record 0 100 389 ad-ds.example.com.
Prerequisites – non standard DNS records

There is no SRV predefined DNS record for LDAPS service.

A simple DNS query shows this record does not exist in AD-DS DNS server by default:

```
$ host -t srv _ldaps._tcp.example.com
Host _ldaps._tcp.example.com not found: 3(NXDOMAIN)
```

You need to add this SRV record manually.
Prerequisites – non standard DNS records – continuation

Using the DNS Manager application at your AD-DS Domain server you can confirm this record does not exist.

![DNS Manager screenshot](image)
Prerequisites – non standard DNS records – continuation

You can add this record right clicking the _tcp container and choosing the Service Location record type.
Prerequisites – LDAPS active in AD-DS Domain server

By default, the LDAPS is not configured in AD-DS Domain server, even if 636 port shows in LISTENING state at the server:
Testing LDAPS connection (-H ldaps://) to AD-DS Domain server:

$ ldapsearch -H ldaps://ad-ds.example.com -LLL \
-D cn=administrator,cn=users,DC=example,DC=com \
-W -b DC=example,DC=com

Enter LDAP Password:

ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)

Also, you can test this connection using the openssl command:

$ openssl s_client -connect ad-ds.example.com:636
Prerequisites – StartTLS active in AD-DS Domain server

Testing StartTLS connection (-ZZ -H ldap://) to AD-DS Domain server:

```bash
$ ldapsearch -ZZ -H ldap://ad-ds.example.com -LLL \
    -D cn=administrator,cn=users,DC=example,DC=com \
    -W -b DC=example,DC=com
```

Enter LDAP Password:

```
ldap_start_tls: Server is unavailable (52)
additional info: 00000000: LdapErr: DSID-0C091269, comment: Error initializing SSL/TLS, data 0, v3839
```

To test StartTLS connection using `openssl`, run:

```bash
$ openssl s_client -connect ad-ds.example.com:389 -starttls ldap
```
Ok, my AD has LDAPS/StartTLS active. What now?

Testing connection
Importing Windows AD-DS CA public key and testing connection

Once your Windows AD-DS domain server have LDAPS/StartTLS active, you can add the CA public key used in Windows AD-DS Domain using:

```bash
# cd /etc/pki/ca-trust/source/anchors
# curl -L <Windows-AD_DS-CA-public-key-URL> -o ad-ds-ca.pem
# update-ca-trust extract
```

Make sure LDAPS/StartTLS connections are available using the `ldapsearch` command:

```bash
$ ldapsearch -H ldaps://ad-ds.example.com -x -LLL -D cn=administrator,CN=users,DC=example,DC=com -W -b dc=example,dc=com cn=oraclesvcolvm dn
Enter LDAP Password:
```

```
$ ldapsearch -ZZ -H ldap://ad-ds.example.com -x -LLL -D cn=administrator,CN=users,DC=example,DC=com -W -b dc=example,dc=com cn=oraclesvcolvm dn
Enter LDAP Password:
```

```
$ ldapsearch -ZZ -H ldap://ad-ds.example.com -x -LLL -D cn=administrator,CN=users,DC=example,DC=com -W -b dc=example,dc=com cn=oraclesvcolvm dn
Enter LDAP Password:
```

```
$ ldapsearch -ZZ -H ldap://ad-ds.example.com -x -LLL -D cn=administrator,CN=users,DC=example,DC=com -W -b dc=example,dc=com cn=oraclesvcolvm dn
Enter LDAP Password:
```

Copyright © 2021, Oracle and/or its affiliates

September 14, 2021
Now you can set up an External Authentication mechanism

Using the ovirt-engine-extension-aaa-ldap-setup command
Running ovirt-engine-extension-aaa-ldap-setup

This is a guided script to configure an external authentication mechanism to the ovirt-engine:

   $ ovirt-engine-extension-aaa-ldap-setup

   ... Welcome to LDAP extension configuration program
       Available LDAP implementations:
       1 - 389ds
       2 - 389ds RFC-2307 Schema
       3 - Active Directory

   ... Please select: 3
       Please enter Active Directory Forest name: example.com

   ...
The next step you need to inform how to connect to the AD-DS domain server, and how to obtain the CA public key.

Please select protocol to use (startTLS, ldaps, plain) [startTLS]: startTLS
Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure): URL
URL: http://ad-ds.example.com/ca.pem
[ INFO ] Resolving SRV record 'example.com'
[ INFO ] Connecting to LDAP using 'ldap://ad-ds.example.com:389'
[ INFO ] Executing startTLS
[ INFO ] Connection succeeded
After a successful connection, you need to inform the user DN or UPN to use in LDAP lookups.

Enter search user DN (for example uid=username,dc=example,dc=com or leave empty for anonymous): oraclesvcolvm@example.com
Enter search user password: **********

[ INFO ] Attempting to bind using 'oraclesvcolvm@example.com'
Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]: Yes

NOTE:
Profile name has to match domain name, otherwise Single Sign-On for Virtual Machines will not work.

Please specify profile name that will be visible to users [example.com]: example.com
Running ovirt-engine-extension-aaa-ldap-setup – continuation

At last, the script will connect to the AD-DS domain server to validate configurations:

Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Please provide credentials to test login flow:
Enter user name: oraclesvcolvm
Enter user password: ********

[ INFO ] Executing login sequence...
... (output omitted)
[ INFO ] Login sequence executed successfully

Please make sure that user details are correct and group membership meets expectations (search for PrincipalRecord and GroupRecord titles).
Abort if output is incorrect.
Select test sequence to execute (Done, Abort, Login, Search) [Done]: Done
Finally, after a success connection test, the configuration is saved to `/etc/ovirt-engine/aaa` and `/etc/ovirt-engine/extensions.d` directories:

```
...
CONFIGURATION SUMMARY
    Profile name is: example.com
    The following files were created:
        /etc/ovirt-engine/aaa/example.com.jks
        /etc/ovirt-engine/aaa/example.com.properties
        /etc/ovirt-engine/extensions.d/example.com.properties
        /etc/ovirt-engine/extensions.d/example.com-authn.properties
    Log file is available at /tmp/ovirt-engine-extension-aaa-ldap-setup-20210822141720-5pe7p0.log
...
Restart the `ovirt-engine` service:
    # systemctl restart ovirt-engine.service
```
Finally, after a success connection test, the configuration is saved to /etc/ovirt-engine/aaa and /etc/ovirt-engine/extensions.d directories:

... CONFIGURATION SUMMARY

Profile name is: example.com
The following files were created:
/etc/ovirt-engine/aaa/example.com.jks
/etc/ovirt-engine/aaa/example.com.properties
/etc/ovirt-engine/extensions.d/example.com.properties
/etc/ovirt-engine/extensions.d/example.com-authn.properties

Log file is available at /tmp/ovirt-engine-extension-aaa-ldap-setup-20210822141720-5pe7p0.log

... Restart the ovirt-engine service:

# systemctl restart ovirt-engine.service
Accessing the ovirt-engine dashboard

First access to the ovirt-engine dashboard
Authenticating to the Dashboard

To access the ovirt-engine dashboard, select the appropriate profile:

You can authenticate using AD but will not be authorized to access the dashboard until your user has a role set up.
Giving permissions to AD users to access and manage the ovirt-engine

To configure a role to a user, as admin, access Administration → Configure → System Permissions. Click the Add button and search for the user to configure:
Removing an authentication profile from the ovirt-engine

Active profile is listed in the configuration summary:

```
... CONFIGURATION SUMMARY
  Profile name is: example.com
  The following files were created:
    /etc/ovirt-engine/aaa/example.com.jks
    /etc/ovirt-engine/aaa/example.com.properties
    /etc/ovirt-engine/extensions.d/example.com.properties
    /etc/ovirt-engine/extensions.d/example.com-authn.properties
```

Remove these files and restart the ovirt-engine:

```
# rm -f /etc/ovirt-engine/aaa/example.com.*
# rm -f /etc/ovirt-engine/extensions.d/example.com.*

# systemctl restart ovirt-engine.service
```
Troubleshooting the LDAP connection

Finding errors in LDAP connection using the ldapsearch command
Testing LDAP connections with the ldapsearch command

The main error message in the ldapsearch command does not reflect the real problem:

```
# ldapsearch -x -v -H ldap://ad-ds.example.com -LLL \
    -D oraclesvcolvm@example.com -W \
    -b dc=example,dc=com cn=oraclesvcolvm dn
ldap_initialize( ldap://ad-ds.olpm.lab:389/??base )
ldap_bind: Invalid credentials(49)
additional info: 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error,
data 533, v3839
```
### The real error message in AD LDAP connections from the data field

<table>
<thead>
<tr>
<th>Error code</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>525</td>
<td>User not found</td>
<td>Returned when an invalid username is supplied.</td>
</tr>
<tr>
<td>52e</td>
<td>Invalid credentials</td>
<td>Returned when a valid username is supplied but an invalid password/credential is supplied. If this error is received, it will prevent most other errors from being displayed.</td>
</tr>
<tr>
<td>530</td>
<td>Not permitted to logon at this time</td>
<td>Returned when a valid username and password/credential are supplied during times when login is restricted.</td>
</tr>
<tr>
<td>531</td>
<td>Not permitted to logon from this workstation</td>
<td>Returned when a valid username and password/credential are supplied, but the user is restricted from using the workstation where the login was attempted.</td>
</tr>
<tr>
<td>532</td>
<td>Password expired</td>
<td>Returned when a valid username is supplied, and the supplied password is valid but expired.</td>
</tr>
<tr>
<td>533</td>
<td>Account disabled</td>
<td>Returned when a valid username and password/credential are supplied but the account has been disabled.</td>
</tr>
<tr>
<td>701</td>
<td>Account expired</td>
<td>Returned when a valid username and password/credential are supplied but the account has expired.</td>
</tr>
<tr>
<td>773</td>
<td>User must reset password</td>
<td>Returned when a valid username and password/credential are supplied, but the user must change their password immediately (before logging in for the first time or after the password was reset by an administrator).</td>
</tr>
<tr>
<td>775</td>
<td>Account locked out</td>
<td>Returned when a valid username is supplied, but the account is locked out. Note that this error will be returned regardless of whether or not the password is invalid.</td>
</tr>
</tbody>
</table>
Logs

AAA extensions logs:
  • /var/log/ovirt-engine/engine.log
Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.