Integration of LDAP with Sybase Control Center (Sybase Unwired Platform)

Applicable Releases:

Sybase Unwired Platform 2.x

Version 2.0
March 2012
## Document History

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.10</td>
<td>Update for SUP 2.1</td>
</tr>
<tr>
<td>1.00</td>
<td>First official release of this guide</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Business Scenario ........................................................................................................... 2
2. Background Information ..................................................................................................... 3
3. Prerequisites ....................................................................................................................... 4
4. Step-by-Step Procedure ...................................................................................................... 5
   4.1 Creating the LDAP Login Module in SCC ................................................................. 5
   4.2 Configure the Sybase Common Security Infrastructure ........................................... 12
   4.3 Configure the Role Mapping ....................................................................................... 13
   4.4 Map Role(s) to User(s) .............................................................................................. 13
   4.5 Test Configuration ....................................................................................................... 15
5. Appendix .......................................................................................................................... 16
1. Business Scenario

Sybase Control Center is a server application that uses a Web-browser-based client to deliver an integrated solution for monitoring and managing Sybase products. Sybase Control Center provides a single comprehensive Web administration console for real-time performance, status, and availability monitoring of large-scale Sybase enterprise servers. Sybase Control Center combines a modular architecture, a rich client administrative console, agents, common services, and tools for managing and controlling Sybase products. It includes historical monitoring, threshold-based alerts and notifications, alert-based script execution, and intelligent tools for identifying performance and usage trends.

A Sybase Control Center server can support:

- Up to 50 monitored resources (servers)
- Up to 10 users logged in simultaneously

Lightweight Directory Access Protocol (LDAP) is an industry standard for accessing directory services over a network.

The primary benefits of using LDAP to manage users are:

- Centralized password security policies in one authority,
- Centralized identity and passwords across both UNIX and Windows,
- Simplified creation and deletion of users,
- Simplified user password for both the operating system and application, and
- Reduced overall cost of ownership.

The Sybase Control Center security model delegates user authentication to the operating system or to your LDAP server. You can configure Sybase Control Center to authenticate user logins through an LDAP server, the operating system, or both.

- Sybase Control Center can be configured to authenticate through any LDAP server that supports the inetOrgPerson (RFC 2798) schema.
- When Sybase Control Center authenticates through the operating system, it uses the operating system of the Sybase Control Center server machine (not the client).

Sybase strongly recommends that you use a common authentication provider for all Sybase products, including Sybase Control Center. A common authentication provider ensures that single sign-on works for users of Sybase Control Center and its managed servers.
2. Background Information

The SUP/LDAP integration consists of 4 essential steps at runtime:

1. Login to the LDAP server as some user with permission to search the server. (BindDN and BindPassword properties)
2. Perform a search containing the username off a person the SUP is trying to authenticate. The purpose of this search is to look up the fully qualified Distinguished Name (DN) of the user. When the authentication search returns a single match, we can proceed.
3. Login to LDAP with the DN and the user’s password.
4. Perform a Role search to discover the LDAP group this user is a member of. SUP considers a group membership as being a member of a security role.
3. Prerequisites

Prerequisites for the steps described in this How-To Guide are:

- Sybase Unwired Platform 2.x and
- Existing LDAP Server (for this example we will be using the Microsoft Active Directory)
- A user account with access to the LDAP

More information can be found at http://infocenter.sybase.com
4. Step-by-Step Procedure

4.1 Creating the LDAP Login Module in SCC

1. Go to the Sybase Control Center URL: https://<hostname>:8283/scc
2. Login using the SUP admin user credentials and the password that input during the installation of the SUP server.

   ![Authentication Image]

   **Note**

   The “User name” is case sensitive. If you are on Sybase Unwired Platform 2.0 or below than the default password during the installation is “s3pAdmin”.

3. Select the “Security” navigation node as shown below in the figure

   ![Security Image]
4. Create another security profile to be used for the LDAP connection, click on “New...” and input a meaningful name for the profile. For this example, we will be naming it “LDAPConnection”.

5. Click on the “LDAPConnection” icon and then click on the Authentication tab as shown below. The default provider is not what we want but we will change it.
6. Now add the “LDAPLoginModule”. Click on the "New..." button as shown below:

![Image of Sybase Control Center with LDAPModule addition](image1.png)

7. Select “LDAPLoginModule” provider from the list as shown below:

![Image of Add Provider with LDAPLoginModule selection](image2.png)
8. The following default screen will appear:

![Add Provider](image)

**Note**

In order to complete the “LDAPLoginModule”, we will need to have connection properties to the LDAP which your LDAP should be able to provide. Below is a list of properties that one would need in-order to complete this task.

These are the explanation of the above LDAPLoginModule attributes and what we need to provide in order to complete the form.

- **Provider URL**: The LDAP host you are trying to connect to. In our example it is `ldap://<LDAP HOST>[:<LDAP Port>]`
- **Control Flag**: usually we set this to `sufficient`
- **ServerType**: This is the important one. We need to tell SUP what the LDAP server we are talking to. In this document we are going to select Windows LDAP server. So the value should be `msad2k`
- **Authentication Method**: We are going to use `simple`
- **Bind DN**: must be a valid DN (distinguished name) that identifies uniquely the user in the organization.
- **Bind Password**: Your LDAP user password you are using in the Bind DN attribute
- **Authentication Search Base**: Here you are telling LDAP which path to take to perform the search or the lookup: From where LDAP is going to start the base search.
- **Authentication Scope**: We need to tell LDAP how deep to go below the Authentication Search Base. For example the hosts file we used in our example above it was one level below etc. folder. But if we have specified the search base to be `c:\windows\system32`, then the hosts file is located under sub-directories. In LDAP world this is called subtree. (For this example: subtree)
- **Authentication Filter**: This like the where clause of a SQL query to use in LDAP to locate what we need. In our example, we are using Microsoft Windows LDAP and SUP is using your user id to authenticate, so the value for the filter is going to be `(&(sAMAccountName={uid})(objectclass=user))`
- **Role Search Base**: This is used to determine your role in the organization and how to map it to SUP roles.
• Role Scope: This works in conjunction with the Role Search Base, is what we need to find belongs one level below the Role Search Base or more than one level. (For this example: subtree)

• Referral: LDAP supports the ability to have many LDAP servers across the globe. For example, engineers in Waterloo can have an LDAP that is part of the enterprise LDAP server located in Dublin. Instead of going to Dublin to search across the globe, we can contact our local server for the needed path. If someone from a different region tries to login to our server, SCC we need to tell our local LDAP that if the user does not exist on our path, to follow through to figure out on what server this user resides. Therefore the value for this attribute is follow.

Most of the attributes mentioned above need to be added on the provider so the form should look like the example below.

![Edit Provider](image)

Note that when first setting this up, in the above image instead of the ‘Save’ button you will see an ‘OK’ button.

9. Add the properties as below:
   a. Click on <ADD NEW PROPERTY>, you should see this image below
   b. You should see something like the figure below. Select Bind DN attribute:
c. Repeat the same steps to add the rest of the attributes.

10. Once all the attributes value pair has been enter, you can either remove the default provider (“NoSecLoginModule”) or move the new provider to top of the stack.

Example of removing the default provider:

![Example of removing the default provider](image-url)

Example of moving the new provider to the top of the stack:

![Example of moving the new provider](image-url)
11. Once you finish updating the new security profile with a new provider, click on the “General” tab:

![General tab image]

12. Click on the “Validate” button. If everything is correct then you should see a message similar to the screen shot below.

![Validate success message]

13. Click the “Apply” button.
4.2 Configure the Sybase Common Security Infrastructure

At this point, you can update the Sybase CSI to use the LDAP provider as your main source of authentication instead of the default native SCC user account. This file is located in the following directory <installation drive>\Sybase\SCC-<control #>\conf\CSI.properties

1. Make a backup of the file before making the update
2. Open the file in your preferred text editor
3. Locate this section ## SUP Ldap Login module
4. You can uncomment the existing options or add yours as follows below “SUP LDAP Login module”. These value pairs should match what you input in the security profile

   CSI.loginModule.5.options.AuthenticationSearchBase=<CN=……>
   CSI.loginModule.5.options.BindDN=<LDAP service user>
   ## BinPassword must contain your domain password.
   CSI.loginModule.5.options.BindPassword=yourpasswordgoeshere
   CSI.loginModule.5.options.DefaultSearchBase=<CN=......>
   CSI.loginModule.5.options.ProviderURL=ldap://<LDAP host>:<LDAP port>
   CSI.loginModule.5.options.RoleSearchBase=<CN=......>
   CSI.loginModule.5.options.ServerType=msad2k
   CSI.loginModule.5.options.moduleName=SUP LDAP Login Module
   CSI.loginModule.5.provider=com.sybase.ua.services.security.ldap.LDAPWithRoleLogin Module
   CSI.loginModule.5.controlFlag=sufficient
   CSI.loginModule.5.options.Referral=follow
   CSI.loginModule.5.options.RoleScope=subtree
   CSI.loginModule.5.options.AuthenticationScope=subtree

5. Save the file
4.3 Configure the Role Mapping

This part of the guide is a continuation of the previous step if you are planning to use the LDAP as your main source of authentication. This will map the security provider’s physical roles to the logical roles for Sybase Control Center. This file is located in the following directory C:\Sybase\SCC-3_2\conf\roles-map.xml

1. Make a backup of the file before making the update
2. Open the file in your preferred text editor
3. Add the following under the <security-modules> tag and change the value accordingly for the "modRole"

   <module name="SUP LDAP Login Module">
   <role-mapping modRole="<RDN value allow for this role>">
     uafRole="uaAnonymous,uaAgentAdmin,uaPluginAdmin,sccAdminRole,sccUserRole,sccOperRole,sccGuestRole,jmxDirectAccess" />
   </role-mapping>
   <role-mapping modRole="SUP Domain Administrator">
     uafRole="uaAnonymous,uaAgentAdmin,uaPluginAdmin,sccUserRole" />
   </module>

4. Now save the file and restart the Sybase Control Center service

4.4 Map Role(s) to User(s)

Now we need to login back to Sybase Control Center using the default user id and password (see previous section) in order to set the mapping

1. Expand the Domains icon and expand Security icon then highlight admin as shown below

2. All we are interested in right now is to map the SUP Administrator role to the LDAP member of group that we added in the roles-map.xml. If everything is configured correctly should see the group listed as shown in the next step below

3. For the SUP Administrator Role click on MAPPED dropdown list, you should see this
4. Now click on “Map Roles....”
5. You should see the following figure below

6. Locate your Roles under Available Roles, once it is being located, click the “Add>” button
7. Repeat the same steps to add all the roles you put in the roles-map.xml
8. You should see something like this figure
9. Once you are done, click the “OK” button
10. Logout from Sybase Control Center

4.5 Test Configuration

Finally let’s test our configuration

1. Go back to Sybase Control Center by going to the following URL in your browser
   https://<host-name>:8283/scc/#
2. Enter your domain user name credential
3. You should see the following
5. Appendix

Debugging

In order to figure out if the authentication is working or not, we need to turn on the debugging login level within SUP. This is done by turning up the

1. logging level for the SECURITY components and set it to DEBUG
2. And changing the authentication cache timeout to a small value (5 seconds)
3. Finally the log file is located in (..\UnwiredServer\logs\<clusternam>_server.log) so you will be able to see the traces of SUP authentication against the LDAP server

Once you are done with the debugging

1. you need to turn the logging level of security components back down to WARN
2. Bumping the authentication cache timeout back up to 3600 (1 hour)
3. You may need to delete the PreconfiguredLoginModule to disable the supAdmin account.

LDAP Error Code:

When debugging the SUP - LDAP connection with Microsoft AD you may find the following error message in the logs: “The exception is [LDAP: error code 49 - 80090308: LdapErr: DSID-OCxxxxxx, comment: AcceptSecurityContext error, data xxx, vece ].”

Here data xxx refer to the an error code in the following list:

525 – user not found
52e – invalid credentials
530 – not permitted to logon at this time
531 – not permitted to logon at this workstation
532 – password expired
533 – account disabled
701 – account expired
773 – user must reset password
775 – user account locked

Debugging: Step 1

These are the steps to turn on the SECURITY components logging level steps.

1. Expand the Servers icon
2. Expand the cluster or server name
3. Click on Log icon
4. On the right side chose Settings and click on the Security component. Change it from INFO or WARN to DEBUG
5. Once you are done, click Save button
Debugging Step: 2

Changing the authentication cache timeout to a small value (5 seconds)

1. Expand the Security icon
2. Highlight your security module, which in my example is called ‘admin’
3. On the right hand side, click on Settings
4. Change the Authentication cache timeout(seconds): from 3600 to 5
5. Once you are done, click Save button
Note

Just as a reminder once you are done with the debugging

1. Turn the logging level of security components back down to WARN
2. Bumping the authentication cache timeout back up to 3600 (1 hour)
3. May need to disable the supAdmin account