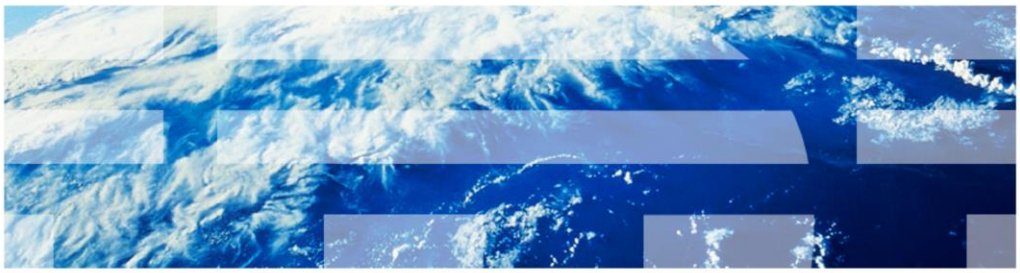
InfoSphere Master Data Management Collaboration Server

How to enable MS Active Directory LDAP integration



This presentation explains how to integrate Microsoft Active Directory to enable LDAP authentication in the IBM InfoSphere® Master Data Management Collaboration Server.

Before going into details, there is some terminology you need to be aware of. The official name of the product referenced in this presentation is IBM InfoSphere Master Data Management Collaboration Server, referred to as MDMCS.

The term $TOP is an environment variable that points to the installation directory of the product.

LDAP refers to the Lightweight Directory Access Protocol and MSAD refers to the Microsoft Active Directory.

Objectives

- Learn how to integrate MSAD with MDMCS for purpose of LDAP user authentication
- Not discussed
  - Detailed setup and configuration of MSAD
  - Other supported LDAP servers

This presentation explains how to integrate Microsoft Active Directory with MDMCS for LDAP user authentication through the product's UI.

This presentation does not cover detailed setup and configuration of Microsoft Active Directory or integration and configuration with other supported LDAP servers.

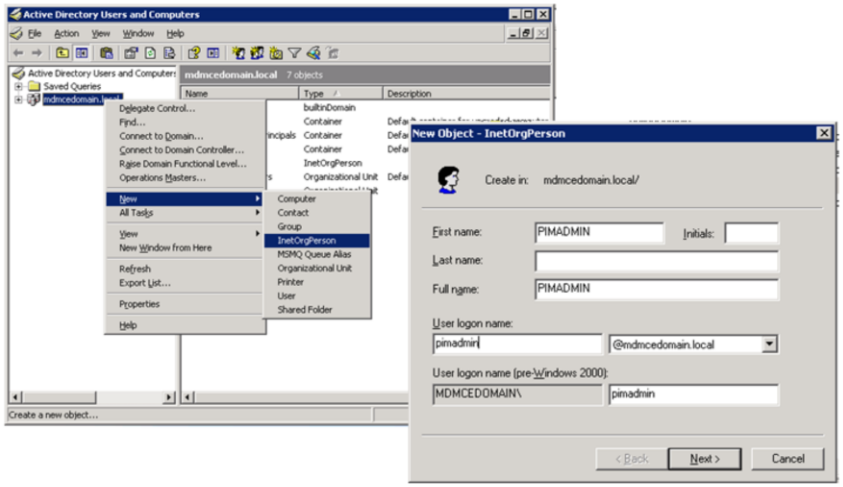
Pre-requisites

- Fully configured and working MSAD
- Fully configured and working MDMCS

This presentation assumes that you have a fully configured and working Microsoft Active Directory and MDMCS instance.

MSAD – Root administrative user

- Root administrative user

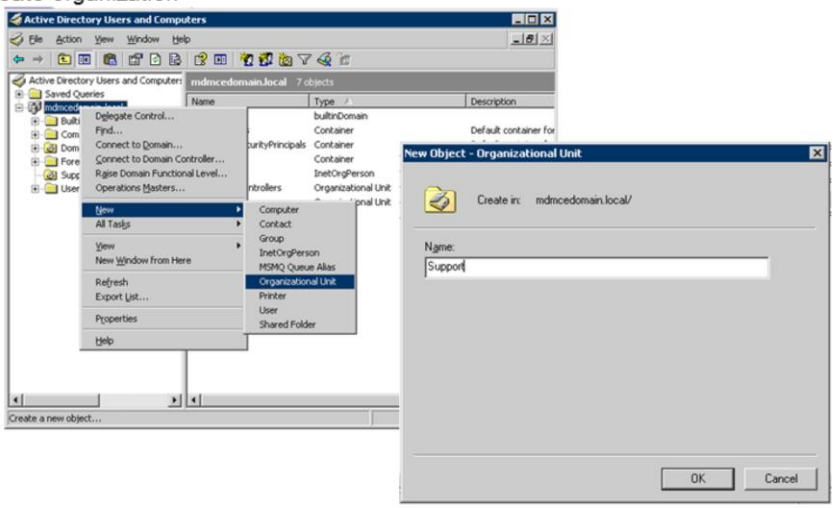


This step is optional if you already have a root administrative user configured. However, it is good practice to have a specific root administrative user for the purposes of MDMCS administration and configuration.

If you do not have an administrative user configured, add a user of type InetOrgPerson at the root of the domain. This user is used as the root user in the MDMCS LDAP lookup table ‘Root Entry DN’ field.

MSAD - Organization

- Create organization

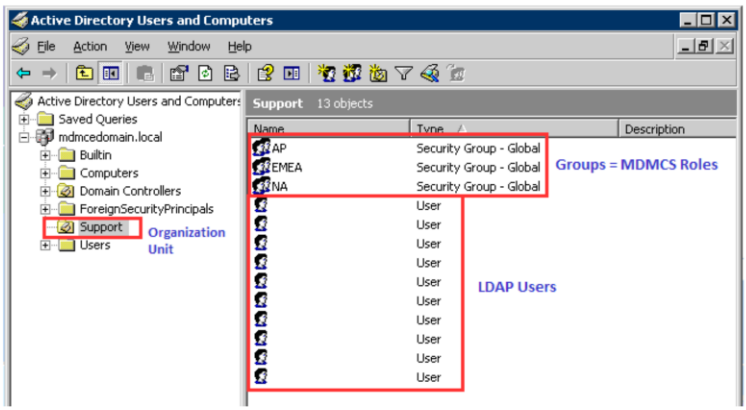


This step is optional if you already have an organization object.

If you do not have an organization object, create a new Organization by choosing a new Organizational Unit. This organization is used as a container to groups that are created to map MDMCS roles.

MSAD – Groups and Users

- Create Groups
- Create Users
- Associate Users to Groups



This step is optional if you already have Groups and Users.

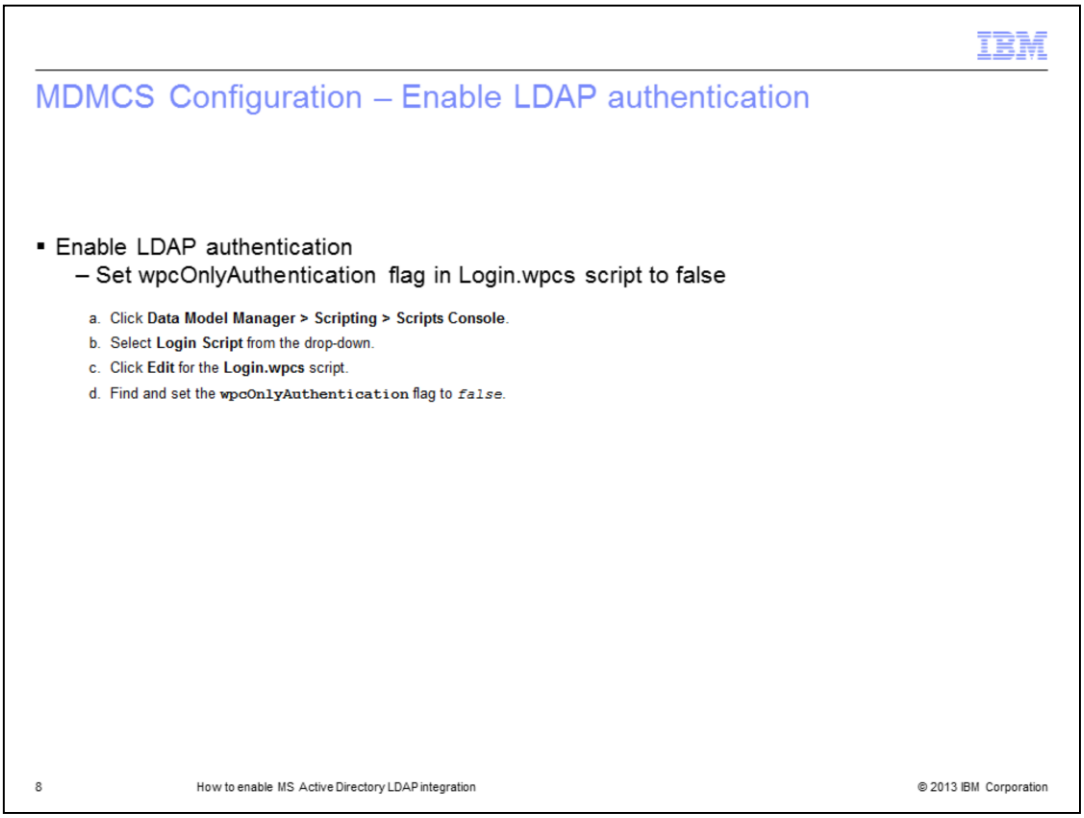
The first step is to create Groups. Create a new Group by selecting the newly created Organizational Unit and right click, choose a new Group and fill in the details.

Create as many Group objects as necessary for all your users based on business needs and on the Roles that are created in MDMCS. Groups have a one-to-one relationship mapping to the MDMCS Roles.

If there are no users, you can add users for the Organizational Unit. For example, here, the organizational unit is Support.

Finally, based on business needs, assign users to a group. For example, if a user is assigned the role of NA then ensure this user is made a member of the NA Group in the MSAD administration.

Once MSAD configuration is finished the setup contains an Organization Unit, Groups that map to MDMCS Roles and Users map to the LDAP users in the MDMCS UI.



In order to enable MSAD users to login through the product's UI, LDAP authentication needs to be enabled on the MDMCS server.

To enable LDAP authentication, login through the product's UI and access the Login Script through the Data Model Manager menu. Click Scripting, then click the Scripts Console menu. Click Edit and find the wpcOnlyAuthentication flag. Set it to false. Save the changes and exit the script.

Configuration – Enable the logger

- Add a logger for LDAP in $TOP/etc/default/log.xml file

```
<appender name="LDAPLOGGER"  class="org.apache.log4j.RollingFileAppender">
<param name="File"    value="/home/cv10FP5/MDMCS10FP5/logs/${svc_name}/ldap.log" />
<param name="Append" value="true" />
<param name="maxFileSize" value="10MB" />
<param name="maxBackupIndex" value="2" />
<param name="encoding" value="UTF-8" />
<layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%d [%t] %-5p %c %x- %m%n"/>
</layout>
</appender>
```

- Set LDAP logger to debug

```
<category name="com.ibm.ccd.wpc_user_scripting.ldap" additivity="false">
   <priority value="debug" />
   <appender-ref ref="LDAPLOGGER" />
 </category>
```

Note: For troubleshooting LDAP issues, review $TOP/logs/appsvr_name/ldap.log

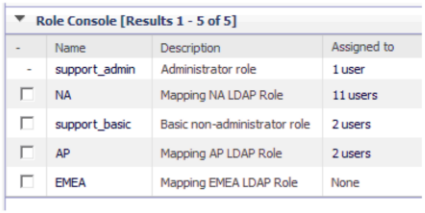
The next step is to configure an additional logger in order to have LDAP related messages written to the product's logs. You need to add a category and appender for this LDAP logger in the $TOP/etc/default/log.xml.

Browse to the $TOP/etc/default/log.xml file and open it. Add the appender and category shown here. Ensure you set the logger value to debug. Save all the changes and exit the file. In order for this change to take effect, restart the product's application server.

When troubleshooting LDAP issues the first place to review is the ldap.log, which is located in the $TOP/logs/appsvr_name directory.

MDMCS configuration – Add MDMCS Roles

- Add MDMCS Roles



Role Console [Results 1 - 5 of 5]

-	Name	Description	Assigned to
-	support_admin	Administrator role	1 user
☐	NA	Mapping NA LDAP Role	11 users
☐	support_basic	Basic non-administrator role	2 users
☐	AP	Mapping AP LDAP Role	2 users
☐	EMEA	Mapping EMEA LDAP Role	None

Create roles in MDMCS with the same name as the groups configured in the Microsoft Active Directory server whose members are to be authenticated. For example, add the role of NA, AP and EMEA as per the earlier image.

MDMCS configuration – LDAP attributes

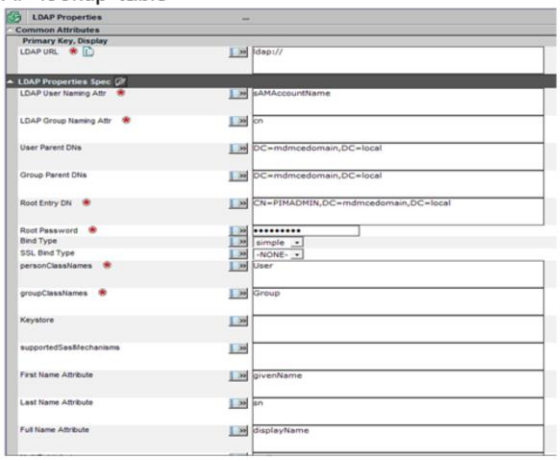
- LDAP server attributes

Attribute name	Description of attribute
LDAP URL	This attribute is the LDAP server URL. The primary key of the lookup table entry. The values are for the LDAP server.
LDAP User Naming Attribute	The naming attribute for the users in this LDAP server.
LDAP Group Naming Attribute	The naming attribute for the groups in this LDAP server.
User Parent DNs	The Pipe (|) delimited Parent DNs where the users are likely to be found. If you do not know the Parent DN, you can set to "".
Group Parent DNs	The Pipe (|) delimited Parent DN where the groups are likely to be found. If you do not know the Parent DN, you can set to "".
Root Entry DN	The root users' Entry DN in this LDAP server.
Root Password	The password of the root user.
Bind Type	The bind type can be one of the following `simple`, `sasl`, or `ssl`. This type is provided as an enum.
SSL Bind Type	The subtypes allowed in `ssl` bind. The `ssl` bind type can be one of the following: `simple` or`DIGEST-MD5`. This type is provided as an enum.
personClassNames	The person class name in the LDAP server.
groupClassNames	The groups class name in the LDAP server.
keystore	The location of the file that was imported in to the JVM.
supportedSaslMechanisms	Subset of server supported `sasl` mechanisms which the customer wants to authenticate LDAP users if the bind type is `sasl`. The list of mechanisms are delimited by a **space character**.
First Name Attribute	The user attribute which represents the first name in LDAP, for example, the `givenname` in Tivoli®.
Last Name Attribute	The user attribute which represents the last name in LDAP, for example, `sn` in Tivoli.
Full Name Attribute	The user attribute which represents the full name in LDAP, for example, `cn` in Tivoli.
Mail ID Attribute	The user attribute which represents the mail ID in LDAP, for example, `mail` in Tivoli.
Telephone Number Attribute	The user attribute which represents the telephone number in LDAP, for example, `telephonenumber` in Tivoli.
FAX Number Attribute	The user attribute which represents the fax number in LDAP, for example, `facsimiletelephonenumber` in Tivoli.
Postal Address Attribute	The user attribute which represents the postal address in LDAP, for example, `postaladdress` in Tivoli.
Title Attribute	The user attribute which represents the title in LDAP, for example, `title` in Tivoli.

The final step is to add values in the MDMCS LDAP lookup table. You will need to provide details for the values described in this table.

MDMCS Configuration – LDAP lookup table

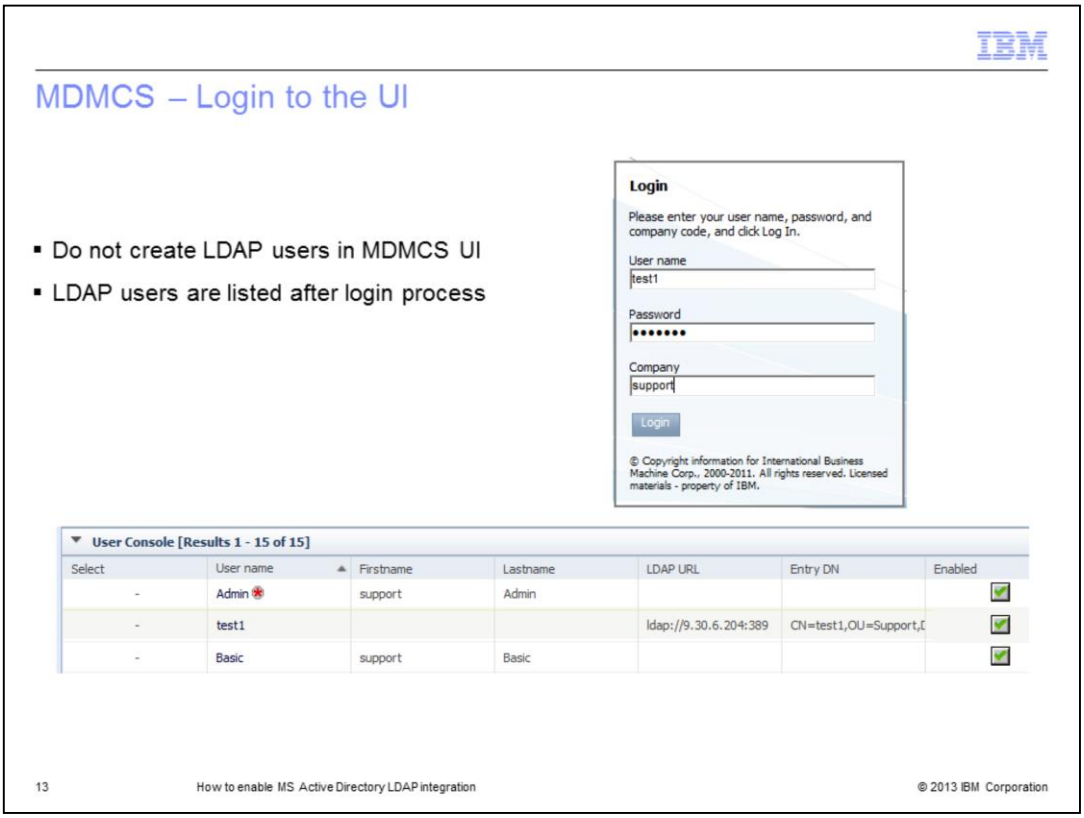
- LDAP lookup table



Displayed on this slide are the values for this configuration. In order to populate the LDAP lookup table you will need to click Product Manager, Lookup Tables and Lookup Table Console menu. Click the magnifying icon to the right of the row for LDAP Properties.

Click the plus sign to add a row and enter the information as per the LDAP configurations from your Microsoft Active Directory server.

Save all changes.



LDAP users should now be able to login through the MCMCS UI.

There is no need to create the LDAP users in MDMCS. Once an LDAP user is able to login successfully, they are listed in the User Console.

Troubleshooting MDMCS LDAP issues (1 of 2)

- Check if Root Administrative user can connect and retrieve users

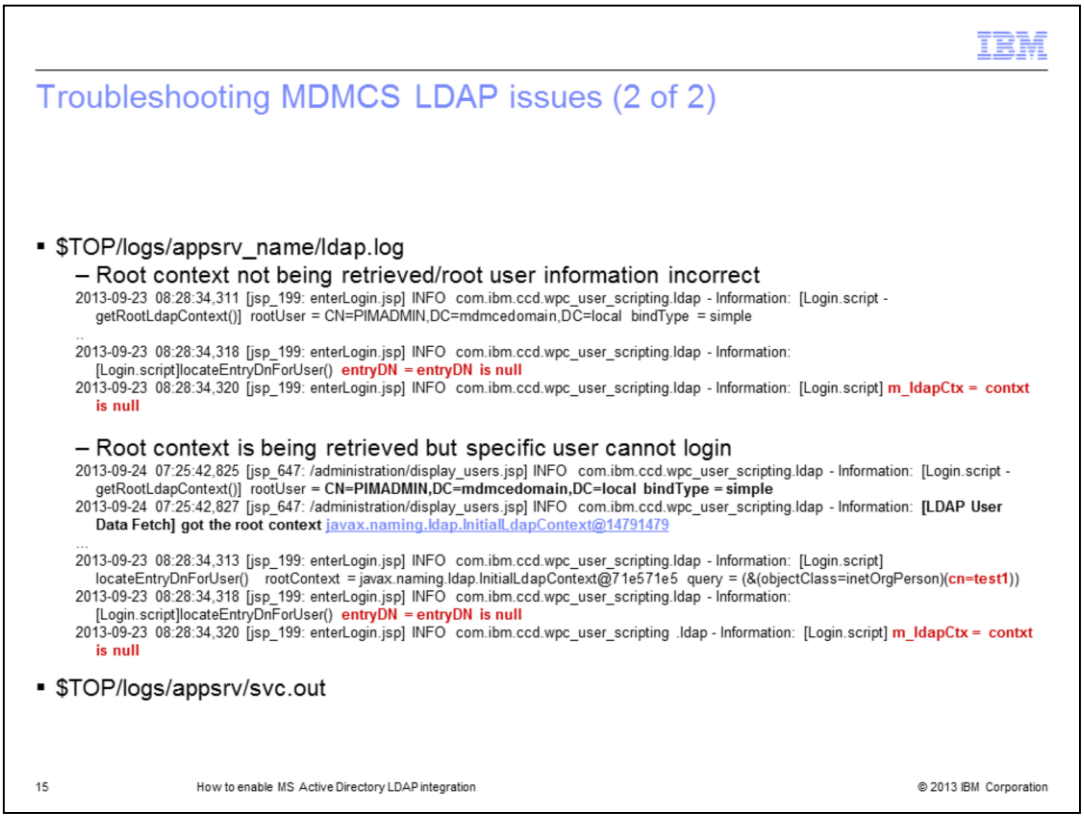
```
var rootUser = "CN=PIMADMIN,DC=mdmcedomain,DC=local";
var rootPassword = "******";
var ldap_url = "ldap://hostname:389" ;
var testUser = "CN=test,OU=Support,DC=mdmcedomain,DC=local";
var ldapUtil = getScriptByPath("scripts/triggers/LDAPLibrary.wpcs");
var function_simpleBind = ldapUtil.getFunctionByName("simpleBind");
var function_search = ldapUtil.getFunctionByName("search"); //function search(m_ctx, searchDN, filter, searchctrl)
var m_ldapCtx = function_simpleBind.invoke(rootUser,rootPassword,ldap_url);
if(m_ldapCtx != null)
{   var filter = "(&(objectclass=group)(|(uniquemember="+testUser+")(member="+testUser+")))";
    var userRoles = function_search.invoke(m_ldapCtx, group_parent_DN, filter, null);
    out.writeln(filter); out.writeln(userRoles); }
else
{   out.writeln("Connection now OK, check the URL, credentials"); }
```

Output:

```
ldap://9.30.6.204:389
CN=PIMADMIN,DC=mdmcedomain,DC=local
******
javax.naming.ldap.InitialLdapContext@599e599e
(&(objectclass=group)(|(uniquemember=CN=ycastane,OU=Support,DC=mdmcedomain,DC=local)(member=CN=ycastane,OU=Support,DC=mdmcedomain,DC=local)))
{}
```


If you are having issues logging in, you can test whether the values entered for Root Entry DN can connect to the LDAP server and retrieve user information.

Update and run the script in the sandbox. Look at the output to see if the information is correct and a connection can be made to the LDAP user.



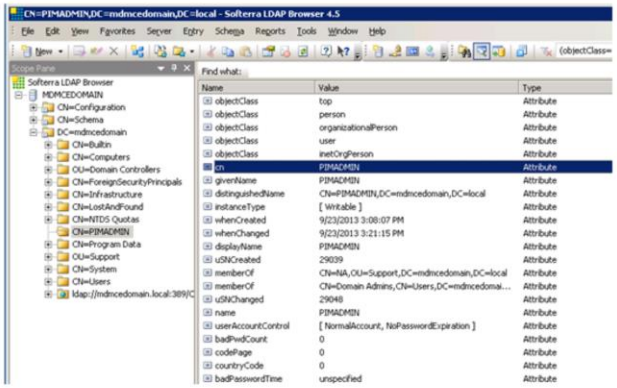
If LDAP users cannot login to MDMCS UI, you can review the LDAP log. The LDAP log is located under $TOP/logs/application server directory. The first thing to check is whether the root context is being retrieved. For example, the information entered in the Root Entry DN value in the LDAP lookup table may be incorrect. A message in the log stating ‘got root context’ indicates the information is correct.

If the root context is being retrieved, perhaps the issue lies with retrieving user information. If so, the context for the specific user might be null, as displayed here. If users are not being retrieved and the root context is being established, there may be incorrect information in the LDAP lookup table values for User Parent DNs or Group Parent DNs.

Another log that can be helpful is svc.out. The svc.out log contains information such as first name, last name, email address and more. If users are able to login through the UI but are reporting some of those values as missing or incorrect, review the values in the LDAP lookup table for attributes for users.

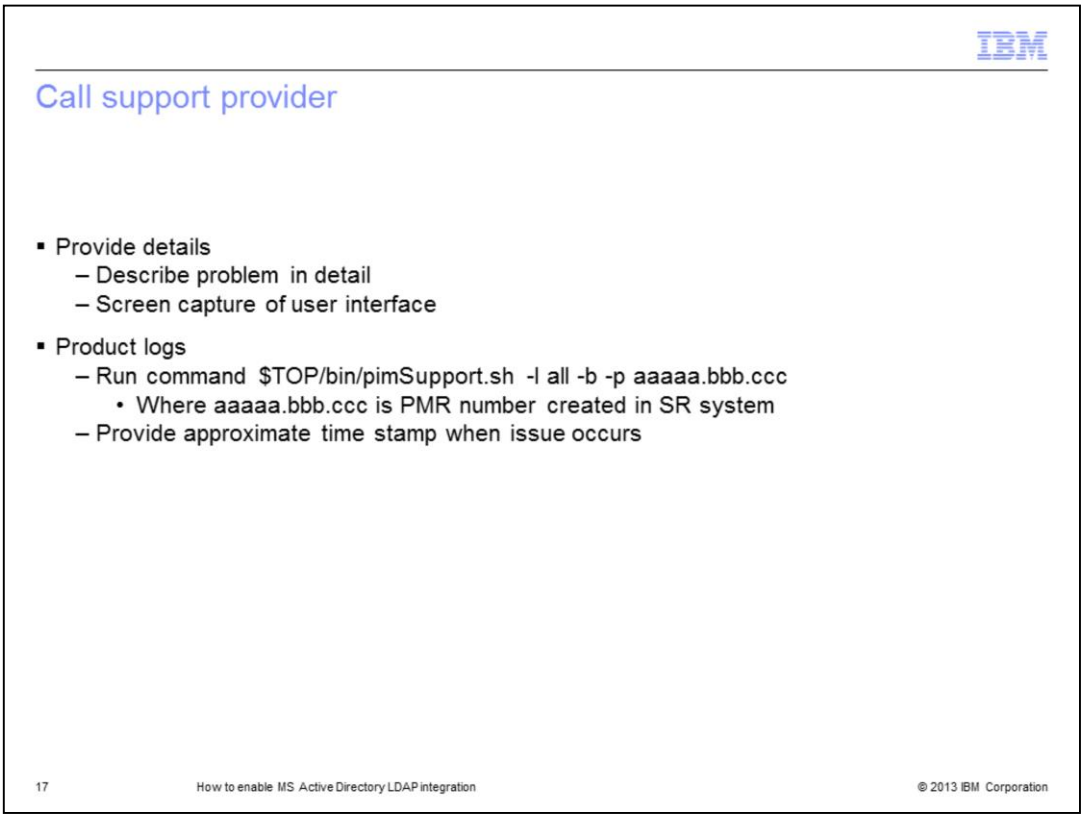
Troubleshooting – Third party tools

- JXplorer
- Softerra LDAP Browser



There are several third party tools that provide a graphical user interface to browse your LDAP directory. When configuring and troubleshooting LDAP issues, these tools can help identify if the values being entered in the MDMCS LDAP lookup table are valid or if proper values are being returned from the MS Active Directory server.

JXExplorer will allow you to browse, search and modify your LDAP directory. Softerra LDAP Browser will allow a read only view of your LDAP directory unless you purchase Softerra LDAP Administrator.



If you need assistance, contact your support provider. Be prepared to provide a detailed problem description, screen captures and the content from the pimSupport.sh script along with an approximate time stamp when the error occurred.

Resources

- Product documentation – Information Center
  - http://pic.dhe.ibm.com/infocenter/mdm/v11r0/topic/com.ibm.pim.adm.doc/sys_admin/pim_con_ldapintegrationcontainer.html
- Technotes
  - Integrating LDAP with the application
    - http://www-01.ibm.com/support/docview.wss?uid=swg21474331
  - WPC LDAP configuration test scripts for Microsoft Active Directory
    - http://www-01.ibm.com/support/docview.wss?uid=swg21291022

For reference, this slide displays links that you might find useful.

Trademarks, disclaimer, and copyright information