Configuration of LDAP on HMC

Table of Contents

Contact:
kumarswamyh@in.ibm.com

LDAP Support on HMC

Since HMC Version 7.3.5.0, you can enable Lightweight Directory Access Protocol (LDAP) authentication on the Hardware Management Console (HMC), to view LDAP servers that are used by the HMC for LDAP remote authentication, to add LDAP servers, or to remove LDAP servers from the HMC.

The HMC authenticates with the LDAP server by means of an anonymous connection by default. You can use the **chhmcldap** command to set the bind distinguished name (DN) and bind password for non-anonymous binding with the LDAP server. You can use the **ldapsearch** command to verify the LDAP setup on the HMC.

The two modes that are supported for LDAP configuration is listed below:

- **LDAP authentication:** The user account is created on the HMC locally. User authentication is done by an LDAP server.
- **LDAP auto-managed** (Remote User Management): The HMC user's information is maintained on the LDAP server. The HMC user account is created automatically when the user logs in for the first time on the HMC. User authentication is done by either an LDAP or a Kerberos server.

Note: The two modes **LDAP authentication** and **LDAP auto-managed** are mutually exclusive and can be configured through the **Enable LDAP for Remote Management** option in the **Configure LDAP** panel or by using the CLI command *chhmcldap -o s --automanage {0|1}.*

Pre-requisites for configuring LDAP remote authentication on HMC

To use LDAP remote authentication for the HMC, you must complete the following prerequisites:

- You must enable LDAP authentication from the LDAP Server Definition window.
- You must define an LDAP server to use for authentication by supplying at least a primary URI for the LDAP server you want.
- You must define the search base (distinguished name tree) for the LDAP server.
- You must set the user profile of each remote user to use LDAP remote authentication instead of local authentication. A user that is set to use LDAP remote authentication will always use LDAP remote authentication, even when the user logs on to the HMC locally. (You do not need to set all users to use LDAP remote authentication. You can set some user profiles so that the users can use local authentication only.)
- You must ensure that a working network connection exists between the HMC and the LDAP servers.

Setting up the LDAP Configuration Data

You can set the LDAP configuration data in the LDAP Server Definition panel. The LDAP administrator provides information about the LDAP client connection data.

- **Enable LDAP**
  Select Enable LDAP to enable LDAP authentication on this HMC by using the LDAP servers that are listed for the primary URI and the backup URI.
  LDAP Connection Configuration:
- **Primary URI**
  Configure an LDAP server for use in authentication on the HMC by specifying the URI. The LDAP server can be Microsoft Active Directory, Tivoli, or Open LDAP.
  Specify the URI in one of the following formats:
  Use the format ldap://ldap.example.com to define a server that uses STARTTLS for SSL encryption.
  Use the format ldaps://ldap.example.com:636 to define a server that uses LDAP over SSL.
  Note: If you use this format, STARTTLS cannot be enabled.
- **Backup URI**
  Configure a backup LDAP server for use in authentication on the HMC by supplying the URI in the one of the following formats:
  Use the format ldap://ldap.example.com to define a server using STARTTLS for SSL encryption.
  Use the format ldaps://ldap.example.com:636 to define a server using LDAP over SSL (Secure LDAP). Note: If you use this format, STARTTLS cannot be enabled.
- **Base DN**: Use this option to locate the user record for the authenticating user. For example, ou=People,dc=example,dc=com.
- **Binddn/Bindpw:** Use this field if the LDAP server requires a bind DN and bind password to connect.
- **Attribute name for user ID:** Use this field to specify the LDAP attribute that identifies the user being authenticated. The attribute that you specify is compared to the user's user ID to locate the correct record to verify the user's provided password. The default attribute is uid. For Microsoft Active Directory, use **sAMAccountName** as the attribute.

Attributes that are specific for LDAP auto-managed mode:

- **Enable LDAP for Remote User Management:**

Select this option to enable LDAP authentication for a remote user of this HMC by using the LDAP servers that are listed for the primary URI and the backup URI.
When you select this option, an LDAP user with properties defined for the HMC can log onto the HMC when the HMC is configured to use an LDAP server. The user account is created automatically and automanage is the specified authentication type based on the user properties retrieved from the attribute that you specify in the LDAP Attributes to Retrieve User Properties field. Each time the user logs on, the user account is refreshed with the current user definition retrieved from the LDAP server.

LDAP Remote User Management Configuration:

- **LDAP Attribute to Retrieve User Properties:**

Use this field to define the LDAP attribute that locates and retrieves the role and authorization properties of the user being authenticated. For example, you might specify a character attribute such as description. The default attribute is ibm-aixAdminPolicyEntry.
The User Properties attribute value is retrieved for the user properties that are used on the HMC. The required user property is taskrole. Other user properties are optional and, if available, are used to create the user account on the HMC automatically when they are applicable.
The user properties which are defined on the LDAP server are specified as key=value pairs that are separated by commas. All user properties, as supported in mkhmcusr and chhmcusr, are applicable to LDAP user with the exception of description, idle_timeout, verify_timeout, authentication_type, passwd, pwage, and min_pwage.
The taskrole is a required property. If you do not specify a taskrole property, the user cannot log on to the HMC. However, the user can still be manually created on the HMC to use the LDAP authentication as it is done in the earlier versions.
The resourcerole property can have multiple roles separated by the '#' character. You can define LDAP users with multiple resource roles by separating each role with the '#' character. If the resourcerole property is defined with multiple roles, the first valid role in the list on the HMC is used for the user. If none of the specified roles are valid, the login is denied.
If the remote_user_name property is specified, and LDAP is configured with Kerberos authentication, the user will be authenticated using Kerberos upon log on to the HMC.
The auto_remove property is applicable for LDAP users only. It can be defined with following values:
0: Do not remove the user account. This is the same as not having the property specified.
1: Remove the user account on HMC if the user record on LDAP server does not exist or has an invalid taskrole.
2: Remove all auto-managed LDAP user account(s) on HMC that does not have a comparable user record on LDAP server or a valid taskrole.

If you are unable to retrieve user properties due to an error, you can use the lshmcldap -r user -v command to validate whether the properties are defined for the user on the LDAP server.

Examples:

The HMC is configured to use LDAP server myldap.company.com to manage LDAP users using the user properties from the attribute description:

```
# lshmcldap -r config
primary=ldap://myldap.company.com,backup=,"basedn=ou=People,dc=company,dc=com",timelimit=30,bindtimelimit=30,referrals=1,ssl=0,loginattribute=uid,hmcauthnameattribute=userPrincipalName,hmcuserpropsattribute=description,binddn,bindpwset=,automanage=1,auth=ldap,searchfilter=,scope=sub
```

To configure HMC user1 with the task role hmcviewer, multiple resource roles role1, role2, role3, the attribute description in user's LDAP record must have the string:

```
taskrole=hmcviewer,resourcerole=role1#role2#role3,..
```

To remove the user account on HMC, if the user is no longer assigned to work on HMC, the attribute description muse have the string:

```
taskrole=hmcviewer,resourcerole=role1#role2#role3,auto_remove=1,..
```

- **Use Kerberos for User Authentication:**

Select this option to specify that the remote user is to be authenticated by Kerberos. This option applies only to remote user management.

- **LDAP Attribute to Retrieve Remote User ID (optional):**

When you select Use Kerberos for User Authentication, you can specify an LDAP attribute to locate and retrieve the remote authentication name from the LDAP server. For example, you might specify an attribute such as userPrincipalName. You also can define the Kerberos remote authentication name by using the attribute remote_user_name in the User Properties field.

Verifying LDAP Server Configuration Information from HMC

You must verify the configuration data by running the *ldapsearch* command from HMC.

For example, if the user sets the LDAP configuration data for **LDAP auto-managed** as given below:

LDAP URI:	*ldaps://example.com*
Base DN:	*ou=People,dc=example,dc=com*
Bind DN:	*cn=HMCAdmin,dc=example,dc=com*
Bind Password:	*abc1234*
Attribute to retrieve user ID:	*Uid*
Attribute to retrieve HMC user properties:	*Description*

The *ldapsearch* command to verify LDAP on HMC is:

```
ldapsearch -h example.com -D cn=HMCAdmin,dc=example,dc=com -w abc1234
     -b ou=People,dc=example,dc=com -x
```

If the *ldapsearch* output does not list the desired user ID(s), it is possible that the base DN is incorrect or at a higher level. In the latter case, rerun *ldapsearch* command with -s sub option to search for all users in sub- directories from the base DN. (Note that setting the search scope to sub-directories will slow down the search, and subsequently the log-in time, therefore it's best to avoid it unless there is a good reason.)

Configure LDAP on HMC

LDAP can be configured on HMC using the UI or CLI *chhmcldap*. With the example above, the following *chhmcldap* and comparable GUI panel is used to configure the LDAP.

LDAP Configuration by using the CLI command:

```
chhmcldap -o s --primary ldaps://example.com --basedn
    u=People,dc=example,dc=com --binddn cn=HMCAdmin,dc=example,dc=com
--bindpw abc1234 --loginattribute uid --hmcuserpropsattribute    description
--automanage 1
```

LDAP Configuration by using the HMC UI:

- Log into HMC.
- Navigate to HMC Management.
- Under Administration, click on **Configure LDAP**.
- The LDAP Server Definition panel opens up for you to configure the LDAP on the HMC.

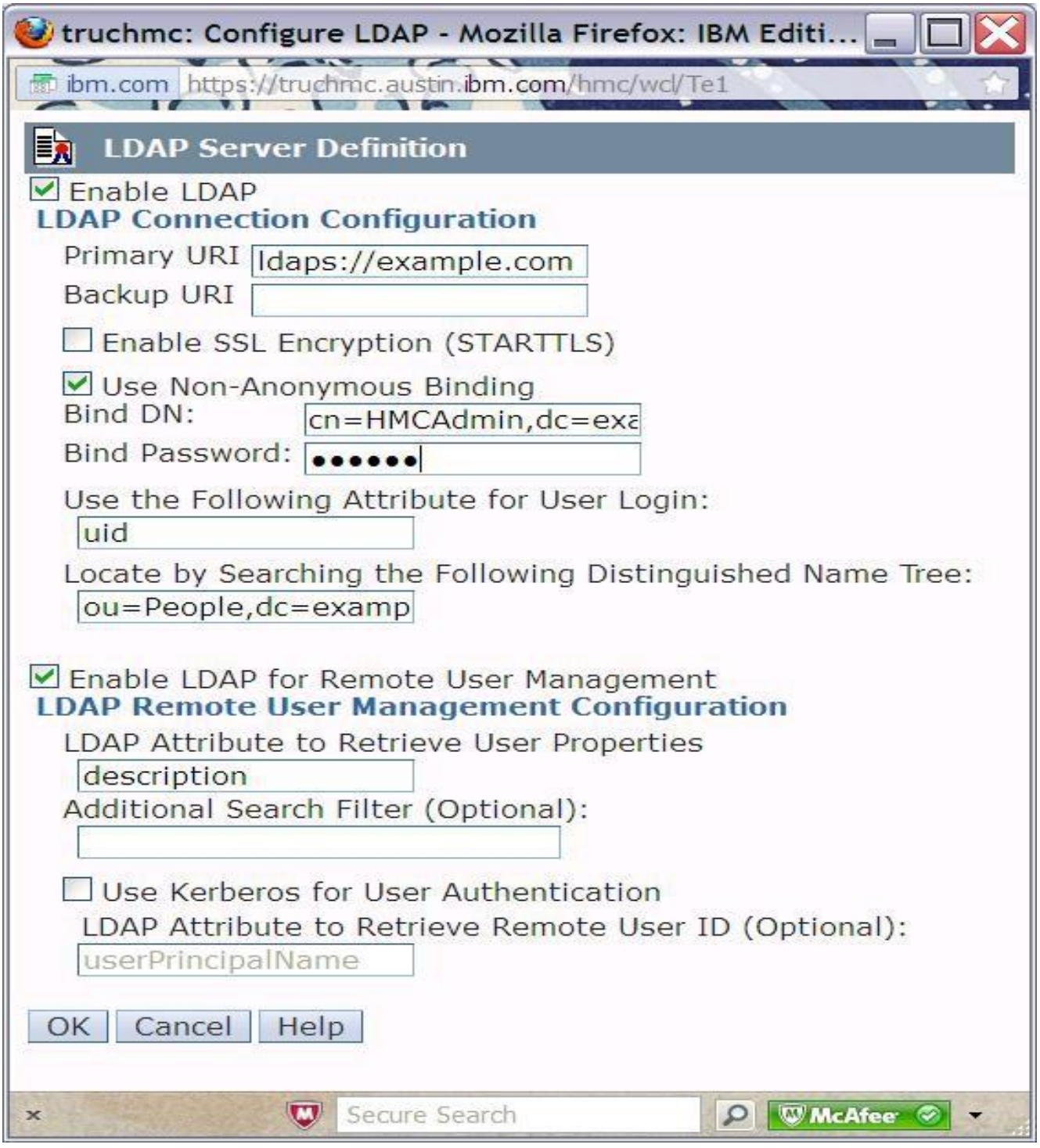

Illustration 1: The LDAP Configuration panel using above example.

Verifying LDAP Setup and User Definition

User does not exist:

If the CLI command *lshmcldap -r user --filter names=<user name>* returns no data, the user is not found or is not defined on the LDAP server.
This could be either the base DN is incorrect or being set at a higher level. Ensure that the search scope is set to sub.

Example:

```
# lshmcldap -r user -v --filter names=user_test
No results were found.
```

 # lshmcldap -r config -v
primary=ldaps://example.com,backup=,"basedn=ou=People,dc=example,dc=co
m",...,loginattribute=uid,hmcauthnameattribute=userPrincipalName,hmcus
erpropsattribute=description,binddn=cn=HMCAdmin,dc=example,dc=com,bind
*pwset=1,automanage=1,auth=ldap,searchfilter=,**scope=sub***

User exists with invalid properties:

If the CLI command *lshmcldap -r user --filter names=<user ID> -v* returns the user with WARNING or ERROR messages, the user is improperly defined to be used with the **auto-managed** feature on HMC.

Example:

myhmc:~ # lshmcldap -r user -v --filter names=test_user
name=test_user,description=,remote_user_name=,user_properties= Details: FOUND USER: test_user
- WARN: An invalid parameter value was entered. The parameter taskrole is empty or not valid. Please check your entry and retry the command.

User exists with valid properties:

If the CLI command *lshmcldap -r user --filter names=<user ID> -v* returns the user with no other message, then the user is able to log into HMC.

myhmc:~ # lshmcldap -r user --filter names=truc
name=truc,"description=""taskrole=hmcviewer,auto_remove=2,remote_webui_access=1""",remote_user_name=,"user_properties=""taskrole=hmcviewer,auto_remove=2,remote_webui_access=1"""

How to Modify LDAP User Record to Allow HMC Log-in

To allow user to log in HMC in auto-managed mode, the user's attribute *hmcuserpropsattribute* must contain the following information:

Required Properties:

taskrole="A valid HMC taskrole"

Optional Properties:

resourcerole="A valid HMC resourcerole"
remove_webui_access={0|1}
remote_ssh_access={0|1}
session_timeout="time-out in minutes"
idle_timeout={time-out in minutes}
inactivity_expiration={number of days}
auto_remove={0|1}
remote_user_name="Kerberos remote user ID"

Example:
If attribute description is to keep the HMC User Properties, it would contain the following string for HMC Log-in.

description="taskrole=hmcviewer"

It could also have all HMC User Properties defined.

description="taskrole=hmcviewer,resourcerole=hmcviewer,session_timeout=20,remote_webui_access=0,remote_ssh_access=1,auto_remove=1,remote_user_name=user@example.com"

chhmc -c kbdcfg	To configure Kerberos configuration.
chhmcldap	To configure or modify LDAP.
chhmcusr	To remove a HMC user account of any authentication type (*local, ldap, kerberos*, and *automanage*).
getfile	To get LDAP or Kerberos CA certificate file and store it on HMC.
ldapserach	To test LDAP configuration data without configuring LDAP on HMC.
lshmc -r	To list Kerberos configuration.
lshmcldap	To list LDAP configuration, retrieve and validate user list from LDAP server. This can be used in conjunction with *ldapsearch* CLI command to verify the LDAP set up on HMC. This can be used to verify if CA certificate is being set up to communicate with LDAP server.

mkhmcusr	To create HMC local user accounts.
rmfile	
rmhmcusr	To remove a HMC user account of any authentication type (*local, ldap, kerberos* and *automanage*).
mkaccfg	To create a custom task role.
chaccfg	To change custom task role.
lsaccfg	To list HMC task roles.

Configuration of Microsoft AD on HMC

Configuration details with Microsoft AD:

Information for bind DN from Microsoft AD (for example, if LDAP server IP is 9.10.10.100). User has referred HMC man pages for *chhmcldap*.

On Microsoft AD (command line)

#**dsquery** user –name **Administrator**
dsquery user CN=Users,dc=corp,dc=ibm,dc=com

Listing subRefs in AD, from remote system using ldapserach *command:*

Kumars-MacBook-Pro:LDAP kumarh$ ldapsearch *-x -h 9.10.10.100 -D "cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com" -w xxxxxxxxx -b "dc=corp,dc=ibm,dc=com" | fgrep subRefs*
subRefs: DC=ibmbase,DC=corp,DC=ibm,DC=com
subRefs: DC=india,DC=corp,DC=ibm,DC=com
subRefs: DC=ForestDnsZones,DC=corp,DC=ibm,DC=com
subRefs: DC=DomainDnsZones,DC=corp,DC=ibm,DC=com
subRefs: CN=Configuration,DC=corp,DC=ibm,DC=com

ldapserach *command to get details of Administrator from Microsoft AD:*

Kumars-MacBook-Pro:LDAP kumarh$ *ldapsearch -x -h 9.10.10.100 -D "cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com" -w xxxxxxxx -b "dc=corp,dc=ibm,dc=com" -s sub "cn=Administrator" dn name description objectCategory*
 # extended LDIF
#
 # LDAPv3

 # base <dc=corp,dc=ibm,dc=com> with scope subtree
 # filter: cn=Administrator
 # requesting: dn name description objectCategory
#

 # Administrator, Users, corp.ibm.com
dn: CN=Administrator,CN=Users,DC=corp,DC=ibm,DC=com
description: Built-in account for administering the computer/domain
name: ***Administrator***
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://ibmbase.corp.ibm.com/DC=ibmbase,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://india.corp.ibm.com/DC=india,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://ForestDnsZones.corp.ibm.com/DC=ForestDnsZones,DC=corp,DC=ibm,DC=com

 # search reference
ref:
ldap://DomainDnsZones.corp.ibm.com/DC=DomainDnsZones,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://corp.ibm.com/CN=Configuration,DC=corp,DC=ibm,DC=com

 # search result
search: 2
result: 0 Success

 # numResponses: 7
 # numEntries: 1
 # numReferences: 5

ldapsearch *command to get LDAP user, whose attribute has HMC properties:*

Kumars-MacBook-Pro:LDAP kumarh$ *ldapsearch -x -h 9.10.10.100 -D "cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com" -w xxxxx -b "dc=corp,dc=ibm,dc=com" -s sub "cn=kumar" dn name description objectCategory*
 # extended LDIF
#
 # LDAPv3
 # base <dc=corp,dc=ibm,dc=com> with scope subtree
 # filter: cn=kumar

 # requesting: dn name description objectCategory
#

 # kumar, Users, corp.ibm.com
dn: CN=kumar,CN=Users,DC=corp,DC=ibm,DC=com
description: ,taskrole=hmcoperator,remote_ssh_access=1
name: kumar
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://ibmbase.corp.ibm.com/DC=ibmbase,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://india.corp.ibm.com/DC=india,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://ForestDnsZones.corp.ibm.com/DC=ForestDnsZones,DC=corp,DC=ibm,DC=com

 # search reference
ref:
ldap://DomainDnsZones.corp.ibm.com/DC=DomainDnsZones,DC=corp,DC=ibm,DC=com

 # search reference
ref: ldap://corp.ibm.com/CN=Configuration,DC=corp,DC=ibm,DC=com

 # search result
search: 2
result: 0 Success

 # numResponses: 7
 # numEntries: 1
 # numReferences: 5

- Run the same *ldapserach* on HMC, and ensure that you get the same output same like that you run on Microsoft AD. If not, check the firewall for connectivity issues. On successful completion, proceed to next step.
- Use the results from the above command to configure LDAP client on HMC side using *chhmcldap* or through the UI.

*chhmcldap –o s –r ldap --primary ldap://9.10.10.100 --binddn "cn=**Administrator**,cn=Users,dc=corp,dc=ibm,dc=com" --bindpw <Administrator's password for bind> --basedn "cn=Users,dc=corp,dc=ibm,dc=com" --automanage 1 --auth ldap --loginattribute **sAMAccountName** --hmcuserpropsattribute **description** --searchfilter <LDAP search filter> --scope [one|sub]*

Note: “sAMAccountName” is used for --loginattribute for Microsoft AD, for OpenLDAP it would be “uid”

Checking configuration using lshmcldap command:

hmc prompt# lshmcldap -r config
primary=ldap://9.10.10.100,backup=,"basedn=CN=Users,dc=corp,dc=ibm,dc=com",timelimit=30,bindtimelimit=30,referrals=1,ssl=0,loginattribute=sAMAccountName,hmcauthnameattribute=userPrincipalName,hmcuserpropsattribute=description,"binddn=cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com",bindpwset=1,automanage=1,auth=ldap,searchfilter=,scope=one,tlscacert=,hmcgroups=

The lshmcldap command *with –*v *option with more verbose information:*

hmc prompt# lshmcldap -r config -v
primary=ldap://9.10.10.100,backup=,"basedn=CN=Users,dc=corp,dc=ibm,dc=com",timelimit=30,bindtimelimit=30,referrals=1,ssl=0,loginattribute=sAMAccountName,hmcauthnameattribute=userPrincipalName,hmcuserpropsattribute=description,"binddn=cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com",bindpwset=1,automanage=1,auth=ldap,searchfilter=,scope=one,tlscacert=,hmcgroups=

Details:

Get LDAP Config:
LdapSettings query primary[ldap://9.10.10.100]
LdapSettings query backup {}
LdapSettings query loginattribute[sAMAccountName]
LdapSettings query basedn[CN=Users,dc=corp,dc=ibm,dc=com]
LdapSettings query timelimit[30]
LdapSettings query timelimit[30]
LdapSettings query referrals[1]
LdapSettings query bindtimelimit[30]
LdapSettings query tlscheckpeer {rc=1, stdOut=0, stdErr=}
LdapSettings query ssl[0]
LdapSettings query binddn[cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com]
LdapSettings query bindpw [**********]
LdapSettings query searchfilter[]
LdapSettings query scope[one]
LdapSettings query tls_cacert[]
LdapSettings query authnameattribute[userPrincipalName]
LdapSettings query propsattribute[description]
LdapSettings query hmcgroups[]

To fetch User details from LDAP on HMC:

hmc prompt# *lshmcldap -r user | grep kumar*
*name=kumar,"description=,taskrole=hmcoperator,remote_ssh_access=1",remote_user_*
name=,"user_properties=,taskrole=hmcoperator,remote_ssh_access=1"

To login to HMC using ssh with the user name.

IBM DEVELOPMENT USE ONLY[hscpe@kumarvhmc850gm ~] $ whoami
hscpe ==========➔ *current user is hscpe*

IBM DEVELOPMENT USE ONLY[hscpe@kumarvhmc850gm ~] $ ssh kumar@<hmcip>
kumar@<hmc ip>'s password:

kumar@kumarvhmc850gm:~> whoami
kumar ==========➔ *now logged with kumar*
kumar@kumarvhmc850gm:~> lshmc -V
"version= Version: 8
Release: 8.5.0
Service Pack: 0
HMC Build level 20160422.1
","base_version=V8R8.5.0
"

Logging into HMC from remote machine using ssh:

Kumars-MacBook-Pro:~ kumarh$ ssh kumar@<hmc ip/host name>
kumar@9.194.250.73's password:xxxxx
kumar@kumarvhmc850gm:~> lshmc -V
"version= Version: 8
Release: 8.5.0
Service Pack: 0
HMC Build level 20160422.1
","base_version=V8R8.5.0
"
kumar@kumarvhmc850gm:~> whoami
kumar

Using LDAP user(in auto-manage mode set to 1).

The user will be automatically created on HMC. Use lshmcusr command to check the user.

IBM DEVELOPMENT USE ONLY[hscroot@kumarvhmc850gm ~] $ lshmcusr --filter "names=kumar"
name=kumar,taskrole=hmcoperator,description=LDAP Managed User,pwage=99999,resourcerole=ALL:,authentication_type=automanage,remote_webui_access=0,remote_ssh_access=1,min_pwage=0,session_timeout=15,verify_timeout=0,idl

e_timeout=0,inactivity_expiration=0,resources=<ResourceID = ALL:><UserDefinedName = AllSystemResources>,disabled=0

==========

NOTE: For the user in non-auto managed mode:

In case where auto-manage is set to zero(0). Then HMC user needs to be created on HMC.

In such case the LDAP configuration on HMC looks like this:

hscroot@kumarvhmc850gm:~> lshmcldap -r config
*primary=ldap://9.10.10.100,backup=,"basedn=cn=Users,dc=corp,dc=ibm,dc=com",timelimit=30,bindtimelimit=30,referrals=1,ssl=0,loginattribute=sAMAccountName,hmcauthnameattribute=userPrincipalName,hmcuserpropsattribute=description,"binddn=cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com",bindpwset=1,**automanage=0**,auth=ldap,searchfilter=,scope=one,tlscacert=,hmcgroups=*

Example: An user with the name "suraj" in LDAP wants to login to HMC.

First check the if the "suraj" name is present in the LDAP server using ldapserach.

```
hscroot@kumarvhmc850gm:~> ldapsearch -x -h 9.10.10.100 -D
"cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com" -w xxxx -b
"dc=corp,dc=ibm,dc=com" -s sub "cn=suraj" | fgrep "suraj"
# filter: cn=suraj
# suraj, Users, corp.ibm.com
dn: CN=suraj,CN=Users,DC=corp,DC=ibm,DC=com
cn: suraj
distinguishedName: CN=suraj,CN=Users,DC=corp,DC=ibm,DC=com
name: suraj
sAMAccountName: suraj
userPrincipalName: suraj@corp.ibm.com
param_cnt=0, i=12: [cn=suraj]
command=[/usr/bin/ldapsearch -x -h 9.10.10.100 -D
cn=Administrator,cn=Users,dc=corp,dc=ibm,dc=com -w xxxx -b
dc=corp,dc=ibm,dc=com -s sub cn=suraj ]
```

Verify that LDAP configuration works using lshmcldap command:

*hscroot@kumarvhmc850gm:~> **lshmcldap -r user | fgrep suraj***
name=suraja,description=00100000000000010000011100000000000000000000000000000000,remote_user_name=,user_properties=00100000000000010000011100000000000000000000000000000000000000000000000000000000

*name=**suraj**,description=Built-in account for administering the computer/domain,remote_user_name=,user_properties=Built-in account for administering the computer/domain*
name=suraj_ad,description=00100000000000010100000000000011111111110000100000000000000000,remote_user_name=,user_properties=0010000000000001010000000000000111111111000010000000000000000

Use mkhmcusr command to create user, present in LDAP server, who wants to manage HMC:

hscroot@kumarvhmc850gm:~> mkhmcusr -i "name=**suraj**,taskrole=hmcviewer,authentication_type=ldap,remote_ssh_access=1"

Verify that the user is created on HMC using the lshmcusr command:

hscroot@kumarvhmc850gm:~> lshmcusr --filter "names=suraj"
*name=**suraj**,taskrole=hmcviewer,description=HMC User,pwage=99999,resourcerole=ALL:,authentication_type=ldap,remote_webui_access=0,remote_ssh_access=1,min_pwage=0,session_timeout=0,verify_timeout=15,idle_timeout=0,inactivity_expiration=0,resources=<ResourceID = ALL:><UserDefinedName = AllSystemResources>,disabled=0*

Logging in with "suraj" user id on HMC.

Kumars-MacBook-Pro:~ kumarh$ ssh suraj@<HMC IP>
suraj@HMCIP's password:
suraj@kumarvhmc850gm:~> lshmc -V
"version= Version: 8
Release: 8.5.0
Service Pack: 0
HMC Build level 20160422.1
","base_version=V8R8.5.0
"
suraj@kumarvhmc850gm:~> whoami
suraj

Note:

- In case there is a firewall between HMC and LDAP server, the firewall has to be broken from both sides.
- The user used for bind must have read access to root domain.

Frequently Asked Questions:

How can I update my LDAP user to be a HMC user?

Yes, any user in LDAP can become HMC user, provided one of the String attribute of User should have mandatory HMC property ",taskrole=hmcoperator" (here hmcoperator is one of the HMC default task-role, for customized HMC user roles, refer man pages of mkaccfg, chaccfg and lsaccfg for details on taskrole)

How does HMC know which field to refer to get the HMC user property details from LDAP?

HMC admin during the configuration of LDAP on HMC, can specify "*—hmcuserpropsattribute*" as part of *chhmcldap* command (similar is present in GUI as well). Here specific the attribute name which holds the HMC properties to be retrieved from LDAP server.
More details can be found in man page for *chhmcldap*.
Extract from Man page:
[--hmcuserpropsattribute

The attribute to use to retrieve the user roles and properties from the LDAP server. These user roles and properties are used when the HMC user is created or updated for an automatically managed LDAP user.

If this option is not specified when LDAP is configured, this attribute is set to ibm-aixAdminPolicyEntry.

This option is only valid for a set operation.]

In a Microsoft AD, Multi domain configuration, for –binddn which domain controller to specify?

Specify the Root Domain in –binddn (refer man page for chhmcldap) If user records are under different sub-domains (a.k.a. directories), the option --scope sub should be included also.

Where can I specify the search details for user?

The –basedn can use to specific all the where to start the search and order to search.

Where can I get sample command to configure LDAP on HMC for auto managed user?

Examples can be got from man page for chhmcldap command.
One ex*: chhmcldap -o s --primary ldaps://example.com –basedn u=People,dc=example,dc=com --binddn cn=HMCAdmin,dc=example,dc=com --bindpw abc1234 --loginattribute sAMAccountName –hmcuserpropsattribute description --automanage 1*

Note: in this example “description” is the LDAP user attribute with contains the “,taskrole=xxx” xxx is valid taskrole.

Apart from taskrole, are there any other HMC attributes that can be added with taskrole?

Yes, there are multiple optional attributes that can be mentioned.
remove_webui_access={0|1}
remote_ssh_access={0|1}
session_timeout="time-out in minutes"
idle_timeout={time-out in minutes}
inactivity_expiration={number of days}
auto_remove={0|1}
remote_user_name="Kerberos remote user ID"
resourcerole="A valid HMC resourcerole"
hmcgroup=" A valid HMC group"

See *mkhmcusr* man page " for more info about *hmcgroup* property and *mkhmcusr* man page for more info about other user properties.

How can I determine the priority of allowing the user to log into HMC if the LDAP server has group of user?

Yes, HMC allows LDAP groups to be used to further control what HMC(s) user(s) can log in. Refer to **chhmcldap** man pages for more info about hmcgroups.

Testing: How can I test my LDAP or AD configuration is correct?

The LDAP configuration and user retrieval can be tested using the following HMC commands

lshmcldap -r config -v
-- To list and validate command configuration errors.

lshmcldap -r user -v
lshmcldap -r user -v --filter "names=ldap_user_id"

-- To test user retrieval from LDAP server and validate HMC user properties. Any failure to retrieval of details implies issue with configuration or communication to LDAP Server from HMC.

Refer to man pages for any other questions on HMC user management or Kerberos or LDAP. Reach out to us in case of any other help required.

==========End of Document==========