IBM Content Manager OnDemand
LDAP Sync

9/17/2020

Rob Russell
Software Engineer - Content Manager OnDemand

This article walks through the basics of how to setup, configure and run the Content Manager OnDemand LDAP Sync command.

What is IBM Content Manager OnDemand LDAP Sync?
Content Manager OnDemand LDAP Sync (ARSLSYNC) is a new Content Manager OnDemand command that allows for the synchronization of users and groups between LDAP-compliant directory servers and Content Manager OnDemand. Users, groups, and a user's group membership can be pulled directly from an LDAP-compliant directory server and imported into Content Manager OnDemand. This alleviates the need for the manual creation of users/groups within Content Manager OnDemand.

Prerequisites: This document addresses functionality that is only available in Content Manager OnDemand for Multiplatforms Versions 10.1.0.2 and later. For IBM i and z/OS, this feature is available at Version 10.1.0.3 or later.

OVERVIEW

Prior to Version 10.1.0.2, Content Manager OnDemand only supported authentication to LDAP.

Content Manager OnDemand V10.1.0.2 introduces a new command (ARSLSYNC) which can be configured to run as either a Windows scheduled task, a Unix cron job, or manually from a properly configured Content Manager OnDemand command prompt.

LDAP Sync includes the following functionality:

- Sync users from LDAP to Content Manager OnDemand
- Sync groups from LDAP to Content Manager OnDemand
- Sync group membership from LDAP to Content Manager OnDemand
- Ignore lists for both users and groups
- Creation of a viewable success/failure System Log messages (including manifest file)
- Ability to run in preview mode only
- Option to run with verbose output

To conform to Content Manager OnDemand user and group naming standards, any special characters from LDAP will be converted to the underscore (_) character. This includes the following characters:

- asterisk (*****)
- percent (**%**)
- plus (**+**)
- left bracket (**[**)
- right bracket (**]**)
- double quote (**"**)
- blank

For example, an LDAP user with a samAccountName of 'cmod admin' will be imported into Content Manager OnDemand as 'cmod_admin'. Although this scenario is not common, you should confirm with your LDAP administrator that this conversion will not result in the attempted creation of duplicate IDs.

Preparing your system

The first step in configuring your system to run ARSLSYNC is to ensure LDAP Authentication and Password Case Sensitivity is enabled in the Content Manager OnDemand Administrator client. Refer to the Content Manager OnDemand Knowledge Center for detailed instructions on how to configure LDAP Authentication.

IBM Content Manager OnDemand for Multiplatforms V10.1.0 documentation

Add new configuration parameters

ARSLSYNC introduces the following new parameters:

ARS_LDAP_SERVER_TYPE (required) [AD, SUN, OPEN]: Specifies the type of LDAP repository being configured. Only a single server can be configured per Content Manager OnDemand instance.

ARS_LDAP_USER_FILTER (required): Used to query LDAP for users that will be imported into Content Manager OnDemand. The maximum length for the ARS_LDAP_USER_FILTER parameter is 1024.

For example: (&(objectclass=user)(objectclass=CMODUSER))

ARS_LDAP_GROUP_FILTER (required): Used to query LDAP for groups that will be imported into Content Manager OnDemand. The maximum length for the ARS_LDAP_ GROUP _FILTER parameter is 1024.

For example: (objectclass=group)

ARS_LDAP_GROUP_MAPPED_ATTRIBUTE (required): Used to create the Content Manager OnDemand group name.

ARS_LDAP_IGN_GROUPS: This parameter specifies the user IDs that Content Manager OnDemand ignores when syncing.

You can specify up to 100 group IDs, delimited by a comma.

ARS_LDAP_IGN_USERIDS: This parameter specifies the user IDs that Content Manager OnDemand ignores when syncing. If the parameter does not exist or you do not specify a value, Content Manager OnDemand defaults to ADMIN.

You can specify up to 100 user IDs, delimited by a comma. If you specify a list of user IDs and you want to include ADMIN, you must specify it on the list.

To ease with the configuration, these parameters can be added directly to the ARS.CFG file on UNIX platforms. Windows customers can use the OnDemand Configurator to add these new parameters. Simply select the **Parameters** button from the instance Properties tab and add any entries needed. This alleviates the need from modifying the Windows registry directly.

Once the parameters have been entered, you must restart the ARSSOCKD process in order for the changes to take effect.

Sample LDAP configuration with LDAP Sync parameters (Active Directory)

ARS_LDAP_SERVER**= adserver.yourcompany.com**
ARS_LDAP_PORT**= 3268**
ARS_LDAP_USE_SSL= **FALSE**
ARS_LDAP_BASE_DN= **dc=ondemand,dc=yourdomain,dc=local**
ARS_LDAP_BIND_ATTRIBUTE= **sAMAccountName**
ARS_LDAP_MAPPED_ATTRIBUTE= **sAMAccountName**
ARS_LDAP_ALLOW_ANONYMOUS= **FALSE**
ARS_LDAP_BIND_MESSAGES_FILE=
ARS_LDAP_IGN_USERIDS=**ADMIN**
ARS_LDAP_SERVER_TYPE**=AD**
ARS_LDAP_USER_FILTER**=(objectclass=user)**
ARS_LDAP_GROUP_FILTER**=(objectclass=group)**
ARS_LDAP_GROUP_MAPPED_ATTRIBUTE**=CN**
ARS_LDAP_IGN_GROUPS**=CMOD_ADMINS,CMOD_USERADMINS**

Usage

The ARSLSYNC command must be run as the instance owner. The command usage requires either Sync (-s) or Preview (-t). In preview mode, no changes are made to the server. This should be used during the configuration of ARSLSYNC. Once you are satisfied that your filters are set correctly, you can proceed to run the command in Sync mode.

Usage: arslsync [-I <od_inst>] [-s | -t] [-v]
Version: 10.1.0.2
-h <od_inst> OnDemand Instance Name (same as -I)
-I <od_inst> OnDemand Instance Name (same as -h)
-s Sync
-t Preview
-v Verbose
-1 <trace_file> Trace file
-2 <trace_level> Trace level

ARSLSYNC introduces the following two new System Log messages:

ARS0460I – LDAP Synchronization Success
ARS0461I – LDAP Synchronization Failed

Both message are viewable from within the System Log. The messages will contain a manifest of any changes made to the system.

ARSLSYNC also includes a verbose option (-v) which will output any objects that already exist in Content Manager OnDemand and will remain unchanged.