Configurazione di utenti LDAP su Cisco Meeting Server tramite API

Sommario

Introduzione

In questo documento viene descritta la configurazione del protocollo LDAP (Lightweight Directory Access Protocol) su Cisco Meeting Server tramite API (Application Programming Interface).

Prerequisiti

App PostMan

Cisco Meeting Server (CMS)

Microsoft Active Directory

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Cisco Meeting Server

Microsoft Active Directory

Premesse

Flusso di configurazione di alto livello per sincronizzare LDAP tramite API.

Passaggio 1. Configurare il parametro /ldapServers tramite l'API come descritto di seguito

1. Informazioni porta/indirizzo server LDAP
2. Nome utente e password per accedere al server
3. Protezione di LDAP non sicuro.

Passaggio 2: configurare il parametro /ldapMappings tramite l'API come descritto di seguito

1. Oggetti proprietà utente LDAP per gli oggetti utente corrispondenti cms
2. Esempio l'utente cms jid eseguirà il mapping a $sAMAccountName$@domain.com su cms e così via.

Passaggio 3: configurare i parametri /ldapSources tramite l'API come descritto di seguito per collegare gli oggetti ldapServers e ldapMappings.

Configurazione

Passaggio 1. Configurare /ldapServers

1. Inviare un POST per /ldapServers che creerebbe un ID server LDAP. Utilizzare l'ID univoco /ldapServers per un'ulteriore configurazione.

2. La risposta al POST restituirebbe un formato simile <ldapServer id="7ca32cc4-389f-46f5-a1b0-0a468af291a4">
3. Acquisire le informazioni riportate di seguito per aggiornare l'ID server LDAP in base alla guida di riferimento dell'API CMS

Parameters	Type/Value	Description/Notes
address *	String	The address of the LDAP server to connect to.
portNumber *	Number	The TCP or TLS port number to connect to on the remote LDAP server.
username	String	The username to use when retrieving information from the LDAP server.
password	String	The password of the account associated with username.
secure *	true|false	Whether to make a secure connection to the LDAP server. If "true" then TLS will be used; if "false", TCP will be used.

4. Metodo POST di esempio con parametri

5. Eseguire un'operazione GET per verificare i parametri configurati

Passaggio 2, Configurare /ldapMappings

1. Inviare un POST per /ldapMappings per creare un ID /ldapMappings. Utilizzare l'ID /ldapMappings e configurare i parametri seguenti.

2. Acquisire le informazioni seguenti per aggiornare l'ID mapping LDAP in base alla Guida di riferimento all'API CMS

| Parameters	Type/Value	Description/Notes
jidMapping	String	The template for generating user JIDs from the associated LDAP server's entries, for instance $sAMAccountName$@example.com.
nameMapping	String	The template for generating user names from the associated LDAP server's entries; for instance "cn" to use the common name.
cdrTagMapping	String	The template for generating a users' cdrTag value. Can be set either to a fixed value or be constructed from other LDAP fields for that user. The user's cdrTag is used in callLegStart CDRs. See the Cisco Meeting Server CDR Reference for details.
authenticationIdMapping	String	The template for generating authentication IDs from the associated LDAP server" s entries, for instance " $userPrincipalName$" .
coSpaceUriMapping	String	If these parameters are supplied, they ensure that each user account generated by this LDAP mapping has an associated personal coSpace. The user is automatically added as a member of the coSpace, with permissions defined above
coSpaceSecondaryUriMapping	String	In order for that coSpace to be set up as required, these parameters provide the template for setting the coSpaces' URI, displayed name and configured Call ID. For example, setting coSpaceNameMapping to "cn personal coSpace" ensures that each user's coSpace is labelled with their name followed by "personal coSpace".
coSpaceNameMapping	String	Note that the generated coSpace will have its own cdrTag – and it will be the same as the user's cdrTag and cannot be changed other than by changing the cdrTagMapping above and re-syncing. (The coSpace's cdrTag is used in the callStart CDR. See the Cisco Meeting Server CDR Reference for details.)
coSpaceCallIdMapping	String	Note that the normal uniqueness rules apply to the URI and Call IDs of coSpaces set up in this way: it is not valid to have the same URI or Call ID for more than one coSpace set up by a given LDAP mapping, nor is it valid for such a coSpace URI or Call ID to be the same as one currently in use elsewhere on the Meeting Server.

3. Configurare i parametri seguenti per ldapMappings

4. Eseguire un'operazione GET per verificare i parametri configurati.

Passaggio 3. Configurare /ldapsources

1. Inviare un POST per /ldapsources per creare un ID /ldapsources. Utilizzare l'ID /ldapsources e configurare i parametri seguenti.

2. Acquisire le informazioni seguenti per aggiornare l'ID mapping LDAP in base alla Guida di riferimento all'API CMS

Parameters	Type/Value	Description/Notes
server *	ID	The ID of a previously-configured LDAP server (see above)
mapping *	ID	The ID of a previously-configured LDAP mapping (see above)
baseDn *	String	The distinguished name of the node in the LDAP server's tree from which users should be imported, for instance "cn=Use-ers,dc=<companyname>,dc=com"
filter	String	An LDAP filter string that records must satisfy in order to be imported as users, for instance "(objectClass=person)"
tenant	ID	If supplied, the ID for the tenant to which the LDAP source should be associated. Users imported with this LDAP source will be associated with that tenant
userProfile	ID	If supplied, this is the ID of the user profile to associate with users imported via this LDAP source. This parameter is present from version 2.0 onwards.
nonMemberAccess	true| false	This parameter pre-configures newly created spaces to allow or disallow non-member access. Spaces existing before the LDAP sync are not affected. true - no passcode is required to access the space and non-members are able to access the created spaces. This is the default setting and matches behavior before this parameter was introduced in version 2.0. false - ensures the member must configure non-member access and set a passcode as part of the LDAP sync. This setting allows a company to enforce passcode protection for non-member access to all user spaces. For more information, see Section 1.2.

3. Configurare i parametri seguenti per ldapSources
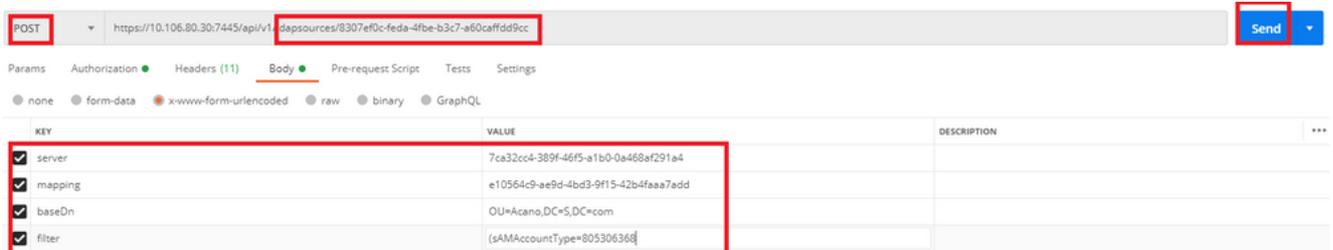
4. Eseguire un'operazione GET per verificare i parametri configurati.
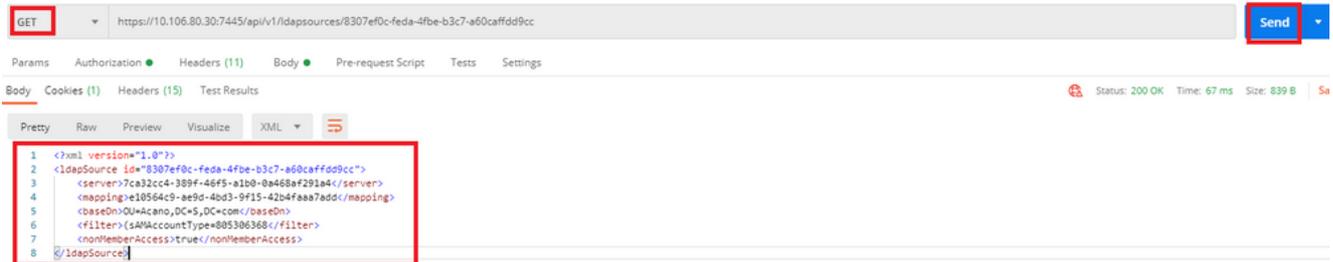
Configurazione completata. Ora è possibile eseguire una sincronizzazione completa.

Verifica

Passaggio 1. Inviare POST per /ldapSyncs dall'API e controllare i registri eventi
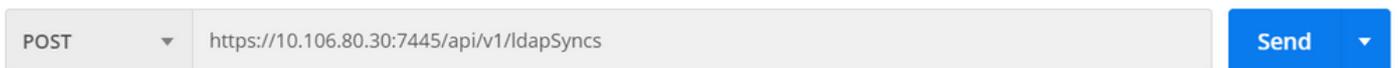
Passaggio 2. Archiviare i registri eventi se la sincronizzazione è stata completata.

10:50:41.225	Info	10.65.86.71: API user "admin" created new LDAP sync operation c02dbb2b-c63e-4bb8-a39f-bbee2cd9611f
10:50:41.225	Info	LDAP sync operation starting
10:50:41.269	Info	LDAP sync operation: finalising
10:50:41.650	Info	LDAP sync operation c02dbb2b-c63e-4bb8-a39f-bbee2cd9611f complete
10:50:55.705	Info	10.65.86.71: web user "admin" logged in
10:50:55.705	Info	web session 1 now in use for user "admin"

10:53:04.331	Info	1103 log messages cleared by "admin"
10:53:07.569	Info	10.65.86.71: web user "admin" created new LDAP sync operation 50c7034c-9aa7-4e81-a304-4113734ffc11
10:53:07.570	Info	LDAP sync operation starting
10:53:07.594	Info	LDAP sync operation: finalising
10:53:07.943	Info	LDAP sync operation complete

Passaggio 3. Verificare che gli utenti siano sincronizzati dall'origine LDAP.

Risoluzione dei problemi

Verificare che i parametri API e gli attributi LDAP siano accurati.

L'acquisizione di pacchetti da Bridge di chiamata consente di isolare i problemi di connettività con LDAP.