

LDAP for MQTT Clients

Chariot can be configured to use an LDAP server for MQTT client authentication and authorization instead of Chariot's MQTT Credentials.



This feature is available in Chariot v2.4.2 and newer

LDAP Server

- LDAP Server schema and sample data can be found in the following directory:
 - `samples/ldap/ldif/`
- Entries in the LDAP Server used for authentication must support simple bind requests
- Entries in the LDAP Server used for authorization must extend the `cls-mqttCredential` Object Class and use the `cls-subTopicFilter` and `cls-pubTopicFilter` attributes to declare their ACLs (see description below)

LDAP Schema Object Classes

Name	Identifier	Type	Description
cls-mqttCredential	1.3.6.1.4.1.60051.2.2.1	Auxiliary	This class represents ACLs associate with an MQTT client. It may include one or more of either of the attributes <code>cls-subTopicFilter</code> or <code>cls-pubTopicFilter</code>

LDAP Schema Attributes

Name	Identifier	Description
cls-subTopicFilter	1.3.6.1.4.1.60051.2.1.1	An MQTT topic filter to subscribe on
cls-pubTopicFilter	1.3.6.1.4.1.60051.2.1.2	An MQTT topic filter to publish on

Chariot Configuration

The MQTT Accounts LDAP configuration can be found by navigating to the following page on the Chariot UI and selecting the LDAP tab:

Main Menu MQTT Accounts LDAP

The configuration fields are described below. Note that the format of the attributes and object class name might differ in the configuration than the name in the schema (as is the case with Microsoft Active Directory). An administrator for the LDAP directory server should be consulted to fill in the correct values for the configuration (see examples below).

Configuration properties:

 As of release v2.5.0 Chariot will use the supplied login username as the name for the simple bind request with the Microsoft AD server. Additionally the **Domain, Auto Suffix, and/or Username Suffix & Prefix** properties can be configured to support bind requests with a user principal name (UPN) of another form.

Property	Required	Default	Description
Username Attribute Name	yes		The attribute of an entry that represents the username of the MQTT client to authenticate
Sub Topic Attribute Name	yes		The multivalued attribute of an entry that represents a subscription topic filters
Pub Topic Attribute Name	yes		The multivalued attribute of an entry that represents a publish topic filters
Credential Object ClassName	yes		The ObjectClass of an entry that holds the credentials
Host	yes		The URL of the LDAP server
System Username	yes		The distinguished name (DN) that Chariot uses to authenticate with the LDAP server
System Password	yes		The password that Chariot uses to authenticate with the LDAP server
Base DN	yes		The base distinguished name (DN) where entries used for ACLs will be searched for
ACL Check Interval	yes		The interval (in ms) between ACL updates
Domain	no		The Windows Active Directory domain name. Example: "MyDomain.com".
Auto Suffix	no	false	If Chariot should automatically append "@<domain>" to the username when authenticating
Username Suffix	no		A manually specified suffix to append to the username when authenticating
Username Prefix	no		A manually specified prefix to prepend to the username when authenticating

Examples

Example Microsoft Active Directory configuration:

GENERAL

Dashboard

Logging

Alerts

Backup

Web Server

Certificates

Diagnostics

ADMINISTRATIVE

User Accounts

User Sources

MQTT Accounts

License

MQTT

Server Configuration

Client Status

Test Client

Sparkplug

MQTT Accounts

CREDENTIALS

LDAP

Connected

Enabled

Host

chariot-testing-ad.chariot.io

Port

389

Use TLS

System Username

Administrator

System Password

Base DN

CN=Users,DC=chariot,DC=io

Username Attribute Name

sAMAccountName

Sub Topic Attribute Name

clsSubTopicFilter

Pub Topic Attribute Name

clsPubTopicFilter

Credential Object ClassName

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

Saved Queries

chariot.io

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

Keys

LostAndFound

Managed Service Accounts

Program Data

System

Users

NTDS Quotas

TPM Devices

Test Client Properties

Published Certificates Member Of Password Replication Dial-in Object

Security Environment Sessions Remote control

General Address Account

Remote Desktop Services Profile

Attributes:

Attribute	Value
assistant	<not set>
attributeCertificateAttri...	<not set>
audio	<not set>
badPasswordTime	(never)
badPwdCount	0
businessCategory	<not set>
c	<not set>
carLicense	<not set>
clsPubTopicFilter	#
clsSubTopicFilter	a/d/#; a/c/;
cn	Test Client
co	<not set>
codePage	0
comment	<not set>

Edit

Multi-valued String Editor

Attribute: clsSubTopicFilter

Value to add:

Values:

a/b

a/c

a/d/#

Add

Remove

OK

Cancel

Example (OpenDJ) LDAP configuration:

Chariot

Dashboard

GENERAL

Logging

Alerts

Backup

Web Server

Certificates

Diagnostics

ADMINISTRATIVE

User Accounts

User Sources

License

MQTT CLIENT

Client

MQTT SERVER

Status

Configuration

Credentials

Clients

MQTT Accounts

CREDENTIALS

LDAP

Connected

Source Type

LDAP

Enabled

Host

localhost

Port

389

Use TLS

System Username

cn=chariot

System Password

.....

Base DN

ou=credentials,dc=cirruslink,dc=com

Username Attribute

uid

Sub Topic Attribute Name

cls-subTopicFilter