Kaltura MediaSpace™ LDAP Integration Guide

Last Modified on 05/12/2020 8:12 pm IDT

This guide describes how to implement Lightweight Directory Access Protocol (LDAP) in Kaltura MediaSpace™ (KMS).

Understanding LDAP Implementation in Kaltura MediaSpace

LDAP/AD Authentication in MediaSpace

LDAP authentication in MediaSpace enables users to log into MediaSpace using their credentials from an organizational LDAP or Active Directory (AD) server. A user does not require an additional set of credentials for MediaSpace. LDAP authentication for MediaSpace uses the MediaSpace login window.

When MediaSpace is configured to authenticate using LDAP, other authentication methods are disabled.

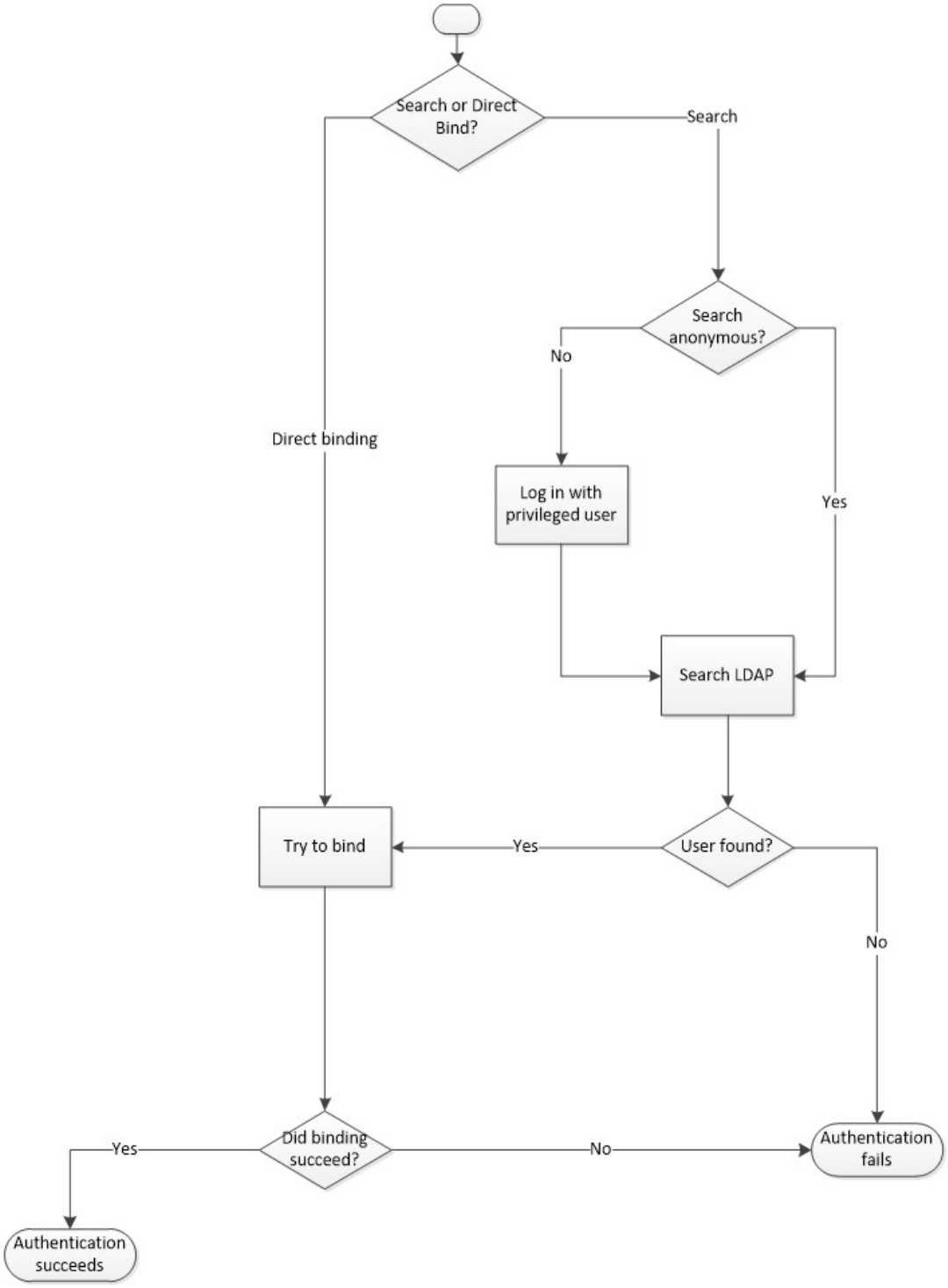
LDAP/AD Authorization in MediaSpace

A user's *application role* determines the MediaSpace actions that the user is authorized to do. When LDAP is used for authorization in MediaSpace, the user's application role is based on membership in organizational groups. The organizational groups are managed in the organization's LDAP server.

To learn more about the MediaSpace application role, refer to Kaltura MediaSpace/Kaltura Application Framework (KAF) Roles and Permissions.

Understanding the LDAP/AD Authentication Flow

The LDAP authentication method implements the following authentication flow:



LDAP server capabilities and MediaSpace LDAP configuration determine whether search for user Distinguished Name (DN) or direct binding is used.

MediaSpace can connect with only one LDAP server.

LDAP/AD Authentication Flow Details

Depending on your MediaSpace LDAP configuration, MediaSpace uses one of the following workflows:

- Search before bind
- Direct bind

"Search before bind" Workflow

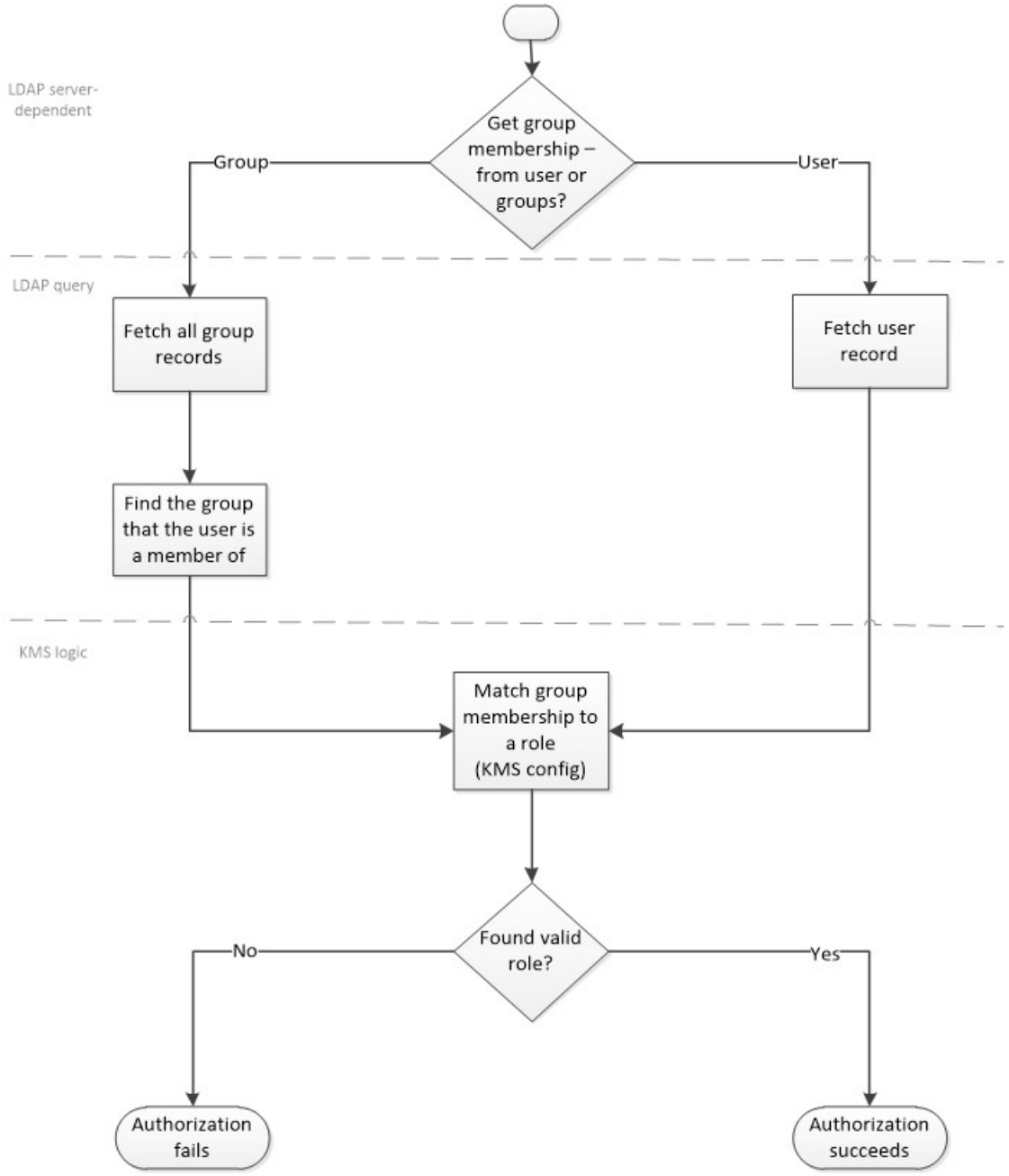
1. MediaSpace connects to the configured LDAP server and binds with a privileged user.
2. MediaSpace queries the LDAP server to find the user's record using a configurable query and the user name entered in the login window.
3. If a record is found, MediaSpace tries to bind the user using the DN that was found and the password entered in the login window.
4. When a user is successfully bound, the user is logged into MediaSpace.

"Direct bind" Workflow:

1. MediaSpace constructs the expected DN of the user using the user name entered in the login window and a configurable pattern of the DN.
2. MediaSpace tries to bind the user using the constructed DN and the password entered in the login window.
3. When a user is successfully bound, the user is logged into MediaSpace.

Understanding the LDAP/AD Authorization Flow

The LDAP authentication method implements the following authorization flow:



LDAP server capabilities and MediaSpace LDAP configuration determine whether group membership is queried based on user or group records.

When an AD server is used and primaryGroupIdAttribute is configured in the MediaSpace Configuration Management panel, the primary group ID is searched for a matching role if no other group matches a role.

Authorization based on nested groups is not supported.

When querying group membership from group objects, using large groups is not recommended since MediaSpace does not support paging when querying LDAP.

LDAP/AD Authorization Flow Details

Depending on your MediaSpace LDAP configuration, MediaSpace queries group membership using one of the following workflows:

- **Get users from groups** – Fetch group records with their *member* attribute
- **Get groups from user** – Fetch the user record with its *memberOf* attribute

"Get users from groups" Workflow

1. Using a single LDAP query, the LDAP authentication method searches for all groups that are preconfigured in a groupàrole mapping setup of MediaSpace and retrieves the configurable membership attribute for the groups that are found.
2. For each group found, the LDAP authentication method:
3. Loops through all members of the group
4. Tries to match the authenticated user DN with the member DN.
   If a match is found, the role mapped to the current group is taken, and the loop ends.

The LDAP query used to search for the groups can be one of the following:

- A preconfigured query defined by the LDAP administrator in your organization
- A preconfigured combination of query patterns that constitutes one query

"Get groups from user" Workflow

1. Using a single LDAP query, the LDAP authentication method fetches the user record including its "memberOf" attribute. The name of the attribute is configurable.
2. For each group found, the LDAP authentication method:
3. Tries to match the group name with one of the groups that are preconfigured in a groupàrole mapping setup of MediaSpace.
   If a match is found, the role mapped to the current group is taken, and the loop ends.

Configuring LDAP in MediaSpace

Configuration settings depend on LDAP server capabilities. Before configuring authentication, determine your LDAP bind method (search before bind or direct bind). Before configuring authorization, determine your LDAP method for user groups searches (get user from groups or get groups from user).

To learn how to configure LDAP for authentication and authorization in MediaSpace, refer to Configuring LDAP Authentication and Authorization.