Platform Config

Authentication and Sync with Directory Server

Authentication Users with a Directory Server

- So far user authentication has been done via the local Alfresco Database
- This is not the usual case in a production environment where instead user management is centralized with a directory server such OpenLDAP or Active Directory (AD)
- To authenticate against an LDAP compatible directory server a couple of configuration settings need to be done in the **alfresco-global.properties** file that is located in the **tomcat/shared/classes** directory

Authentication Users with a Directory Server Continued

- User authentication is configured like this (example for Microsoft Active Directory (AD))
    - The default authentication configuration assumes users' credentials are in the Alfresco DB:
        - authentication.chain=alfrescoNtlm1:alfrescoNtlm
    - Change this to using AD and local DB:
        - authentication.chain= **companyAD:ldapad**, alfrescoNtlm1:alfrescoNtlm
    - Most properties for the LDAP Active Directory configuration has OK values set by default so no need to change most of them.
    - However, the mapping of the Alfresco user id (%s) to that passed through to AD, and the location of the AD server, need to be updated:
        - ldap.authentication.userNameFormat=%s@domain
        - ldap.authentication.java.naming.provider.url=ldap://domaincontroller.company.com:389

Authentication Users with a Directory Server Continued

- If you don't want unauthenticated users to have access to Alfresco, then set the following property to false:
  - `ldap.authentication.allowGuestLogin`
- If the admin user name is not Administrator in Active Directory, then you need to update the following property:
  - `ldap.authentication.defaultAdministratorUserNames=Administrator`

Authentication Users with a Directory Server Continued

- These values and settings are enough to make alfresco authenticate against your Active Directory
- The first time a user authenticates via AD he or she will also get a skeleton account (Person Object) setup in the Alfresco DB with just the username set
- The Person Object that is setup for the user will not be populated with attributes, such as first name and last name, without user registry export (sync) enabled, which is the next subject

Synchronizing Users and Groups with a Directory server

- Most Alfresco production environments will synchronize users with an external directory server to setup other fields then just user name, such as email
- It is also common to synchronize/import the groups that is in the directory and the members of the groups
- These groups can then be used for Role-based Access Control (RBAC)
- Synchronization is configured in the **alfresco-global.properties** file that is located in the **tomcat/shared/classes** directory

Synchronizing Users and Groups with a Directory server

- User sync is configured like this (example with AD and assumes the authentication configuration is in place)
  - First, configure a directory user that has permission to access users and groups:
    - `ldap.synchronization.java.naming.security.principal=alfresco@mycompany.com`
    - `ldap.synchronization.java.naming.security.credentials=secret`
  - Then check that the directory queries are correct for fetching users and groups (default values usually OK):
    - `ldap.synchronization.groupQuery=(objectclass\=group)`
    - `ldap.synchronization.personQuery=(&(objectclass\=user)(userAccountControl\:1.2.840.113556.1.4.803\:\=512))`

Synchronizing Users and Groups with a Directory server continued

- Then set the search base for users and groups according to where they are in the directory:
  - ldap.synchronization.userSearchBase=ou=User Accounts,ou=Alfresco,dc=domain
  - ldap.synchronization.groupSearchBase=ou=Security Groups,ou=Alfresco,dc=domain
- Then check that the LDAP to Alfresco property mapping is correct for users and groups (default values usually OK):
  - ldap.synchronization.userIdAttributeName=sAMAccountName
  - ldap.synchronization.userFirstNameAttributeName=givenName
  - ldap.synchronization.userLastNameAttributeName=sn
  - ldap.synchronization.userEmailAttributeName=mail
  - ldap.synchronization.userOrganizationalIdAttributeName=company
  - ldap.synchronization.groupIdAttributeName=cn
  - ldap.synchronization.groupDisplayNameAttributeName=displayName
  - ldap.synchronization.groupMemberAttributeName=member

Exercise

We are going to configure Alfresco to talk to a local Apache Directory server