Active Directory Remote Synchronization Implementation Guide

Applications

Document Details

Document #: 160_SG640_190823

Release Version: 06.40.00.00

Version Release Date: March 2019

Overview

Audience: The Operations staff supporting the on-premise CrunchTime Applications.

This document explains how to implement Active Directory Remote Synchronization for the CT Applications.

System Requirements

- CES Release Version 06.40.00 or higher
- Be sure to grab the latest version of this document here: https://links.crunchtime.com/SG-ADRemoteSyncApps

Other Related Documentation

- AD Remote Auth Guide - IT: https://links.crunchtime.com/SG-ADRemoteAuthIT
- AD Remote Sync Guide - IT: https://links.crunchtime.com/SG-ADRemoteSyncIT
- AD Remote Auth Guide - Apps: https://links.crunchtime.com/SG-ADRemoteAuthApps
- AD Remote Sync Guide - CT Admin: https://links.crunchtime.com/SG-ADRemoteSyncCTadmin

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Implementation Steps

1. Make sure the network communication between on-premise CrunchTime Application servers and the in-house Active Directory server works successfully. If this network communication needs to go over the internet (in which case LDAPS will be used), provide to the Active Directory Administrator the block of IPs that will originate from CrunchTime Application servers.

2. Execute the following queries/procedure in CrunchTime Database and commit.

Note: Several of the queries below include values within {braces}, noted in *blue italics*; they are just an example. The actual values will be provided by the Active Directory administrator.

- `update t_application_setting set setting_value = 'true' where setting_name = 'remote.directory.sync.enabled';`
- `update t_application_setting set setting_value = 'Person' where setting_name = 'remote.directory.user.object.class';`
- `update t_application_setting set setting_value = 'memberOf' where setting_name = 'remote.directory.attribute.memberof';`
- `update t_application_setting set setting_value = 'distinguishedName' where setting_name = 'remote.directory.attribute.dn';`
- `update t_application_setting set setting_value = 'sAMAccountName' where setting_name = 'remote.directory.attribute.username';`
- `update t_application_setting set setting_value = 'givenName' where setting_name = 'remote.directory.attribute.first_name';`
- `update t_application_setting set setting_value = 'sn' where setting_name = 'remote.directory.attribute.last_name';`
- `update t_application_setting set setting_value = 'mail' where setting_name = 'remote.directory.attribute.email';`
- `update t_application_setting set setting_value = {'OU=CT_Groups,OU=people,DC=xxx,DC=local'} where setting_name = 'remote.directory.groups_path';`
- `update t_application_setting set setting_value = {'xxx.local'} where setting_name = 'remote.directory.domain_name';`
- `update t_application_setting set setting_value = {'ldap://ip.address/dc=xxx,dc=local'} where setting_name = 'remote.directory.url';`
- `update t_application_setting set setting_value = {'ldap://ip.address/OU=top_search_ou,DC=xxx,DC=local'} where setting_name = 'remote.directory.search_base';`
- `update t_application_setting set setting_value = {'false'} where setting_name = 'remote.directory.search.follow_referral';`
- `update t_application_setting set setting_value = {'computer-user'} where setting_name = 'remote.directory.sync_user.name';`

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Implementation Steps (Continued)

- There are two scenarios for **remote.directory.sync_user.pass**:
  - For Net-Chef/EM Web version 06.00.01.00 and higher, and for TeamworX version 2.4.3 or higher in 2.4.X series, and 2.5.1 or higher in general:

    ```
    exec imf_save_ad_password ({'password'}, 'aD987$iQ3');
    ```

  - For other CrunchTime Application versions:

    ```
    update t_application_setting set setting_value = {'password'} where
    setting_name = 'remote.directory.sync_user.pass';
    ```

3. If using LDAPS, import the certificate provided by the Active Directory Administrator
   - For Servers running Java 8 (Net-Chef/EM Web 06.10.00.xx and lower)
     a. Navigate to the JDK-install-dir/jre/bin directory.
     b. Run: keytool -import -trustcacerts -alias alias -file certificate_filename -keystore cacerts_filename
        - For the -alias option, you can assign any value.
        - For the -file option, specify the fully qualified name of the LDAP server's certificate.
        - For the -keystore option, specify the fully qualified name of the cacerts file. The cacerts file is located in the JDK-install-dir/jre/lib/security directory.
     c. When prompted, enter the keystore password. The default password is *changeit*.
     d. When prompted to trust this certificate, enter *yes*.
   - For Servers running Java 10 (Net-Chef/EM Web 06.30.00.XX and higher)
     a. Navigate to the JDK-install-dir/bin directory.
     b. Run: keytool -import -alias alias -file certificate_filename -cacerts
        - For the -alias option, you can assign any value.
        - For the -file option, specify the fully qualified name of the LDAP server's certificate.
     c. When prompted, enter the keystore password. The default password is *changeit*.
     d. When prompted to trust this certificate, enter *yes*.
4. Restart the CrunchTime Application (Net-Chef/EM Web or TeamworX)
5. Notify the CrunchTime Applications Administrator to test

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Upgrade Notes

Active Directory server certificate consideration

In the case where LDAPS and certificate are used, they need to be considered during some upgrade cases.

- When the CrunchTime Applications upgrade involves moving to new servers, the Active Directory server certificate (imported into cacerts) need to be copied to the new server.
- When upgrading CrunchTime Applications to versions running on a different version of Java than the previous one, the Active Directory server certificate needs to be re-imported into the cacerts file of the new version of Java after the upgrade.
  - Net-Chef/EM Web 06.10.00.xx and earlier run on Java 8
  - Net-Chef/EM Web 06.20.00.xx and newer run on Java 10
  - TeamworX lower than 2.2.0 runs on Java 8
  - TeamworX 2.2.0 and newer run on Java 10

AD Sync-user password encryption consideration

When upgrading CrunchTime Applications from versions that DON'T encrypt the Active Directory password to versions that DO, the following procedure needs to be executed in the CrunchTime Database:

```
exec imf_save_ad_password ({'password'}, 'aD987$iQ3');
```

  - The first argument is the **remote.directory.sync_user.pass** provided by the Active Directory Administrator.
  - The second argument is a hardcoded key.
- App versions that DO NOT encrypt the password: Net-Chef/ EM Web 06.00.00.xx and earlier; TeamworX 2.3.x and lower, 2.4.0, 2.4.1, 2.4.2, 2.5.0
- App versions that DO encrypt the password: Net-Chef/ EM Web 06.00.01.xx and newer; TeamworX 2.4.3 and higher in 2.4.x series; TeamworX 2.5.1 and newer

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com