Active Directory Synchronization Tool Architecture and Design

Hosting Controller Cloud Automation Solution

Revised on: November 08, 2016
Version: 1.02

Hosting Controller
www.hostingcontroller.com

Contents

Proprietary Notice

1. Introduction

1.1 About this Guide

This document provides the design for the Hosting Controller Active Directory Synchronization Module. It mainly targets Enterprises, Service Providers and System Integrators responsible for the design, implementation, update and deployment of private/public cloud platforms. This guide provides everything you need to know about the design of HC Active Directory Sync Module.

1.2 Business Requirements

As a design or as a consequence of events beyond the control of an organization, Active Directory Synchronization often becomes inevitable. Synchronization of user data generally is required across different AD forests and may be necessitated by background mergers, acquisitions, divestitures or partnerships. Multi-Forest scenarios are commonplace in a rapidly evolving market. Organizations often require AD objects (users, groups, contacts,) and their passwords to be synchronized between multiple AD forests.

Sometimes organizations housing a hosted infrastructure such as MS Exchange have customers holding their own Active Directories. The primary requirement for such organizations is to have on-premises users somehow synchronized with the hosted environment.

Whatever the reason Cross-Forest synchronization has become a reality, making a very compelling argument for IT departments to be ready may the need arise.

What most businesses require is:

- A lightweight solution for synchronizing users and passwords between two forests.
- Something that does not require a two-way trust relationship to be established between domains.
- A solution that does not involve the added complication and cost of deploying an AD FS infrastructure.
- A tool that provides the flexibility for specific users and groups to be excluded from being synchronized.
- Easy way to synchronize a minimal set of user attributes (having the ability to exclude any unwanted attributes from syncing).
- Interval based synchronization, enabling customers to choose convenient time intervals.

Hosting Controller unifies the convenience of all the above in its Active Directory Synchronization Utility to bring the most effective tool on the market.

1.3 Hosting Controller Experience

Hosting Controller has successfully been providing out of the box solutions to its clientele across the globe since over a decade. The range of products includes solutions for enterprises and telcos.

1.4 Industry Standards and Compliance

Hosting Controller is a control panel validated by Microsoft for both Exchange 2010 and Exchange 2013 installations.

1.5 Support Availability

Hosting Controller Support is available 24 x 7 through its support center from Canada and off-shore locations. Priority phone support and other options are available in the commercial proposal.

2. Hosting Controller Cloud Automation Control Panel

2.1 Overview

Hosting Controller cloud automation solution is a complete control panel product for service providers to automate, manage, provision and administer Microsoft Enterprise applications. Thus, creating a shared multi-tenant environment for automatic provisioning of new accounts, such as Exchange, Lync, SharePoint, Dynamics CRM and Hyper-V. It encompasses a comprehensive self-serve portal for all user levels. Hosting Controller is a validated and recommended control panel by Microsoft for Exchange 2010 and Exchange 2013. The key purpose of using Hosting Controller control panel is:

- To automate provisioning of hosted services.
- To offer comprehensive self-serve portal for end customers to perform routine administration tasks.
- Management of multiple hosted cloud services through single centralized interface.
- Ability to provision multiple shared applications for a single user.
- Option to support distributed environment where different services can be spread across different servers across different OS platforms both Windows & Linux in different data centers within a cluster.

2.2 Key Advantages

Hosting Controller offers central master console with a single database to completely automate servers' infrastructure via single interface. It provides comprehensive self-care portals for administrators, tenants and resellers as per their requirements.

3. HC Active Directory Synchronization Module

For those tenants that have on premise active directory services, the private/public cloud provides directory synchronization facilities to ensure password synchronization, identity information synchronization, user object provisioning as well as object synchronization to ensure consistency in address list.

The directory synchronization is a component, named **HC ADSync Utility**. This component is responsible for:

- User Password synchronization
- User/Group/Contact objects identity information (attributes mentioned below)
- User objects provisioning
- Group objects provisioning
- Contact objects provisioning

This document contains only the detailed design of the HC ADSync component.

3.1 General Design

The following figure illustrates the synchronization workflow.

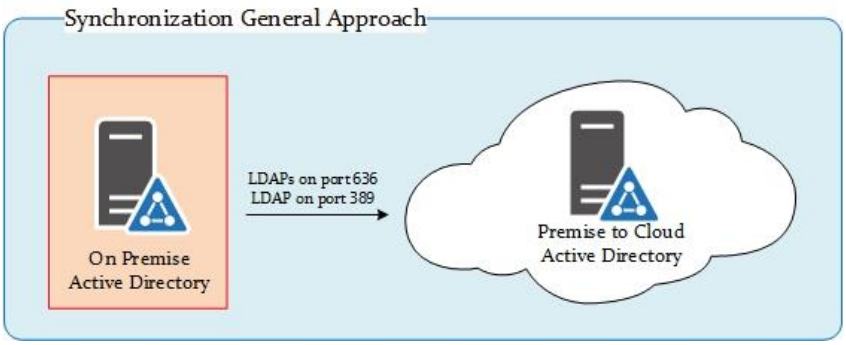

Figure 1: Synchronization General Approach

The overall concept is summarized as follows:

- User object on premise identity information is synchronized through ADSync with related user object within the private/public cloud.
- On premise password change events are intercepted and replicated through ADSync to related user object within the private/public cloud.
- New on premise user objects are provisioned by ADSync into the cloud environment. Within the cloud environment the user objects created without any service offering activated on it.
- Deletion of an on premise user object will result in deletion of the user object and its assigned service offerings in the private/public cloud.
- Resource mailboxes are treated in a similar fashion as user objects.
- Synchronization direction is from on premise to the private/public cloud.

- Once the users are synchronized to the private/public cloud, the HC Import Tool is used to import the objects into HC Control Panel for cloud service offerings through Control Panel.
- Users on premise and in the private/public cloud do not notice any difference in address lists.

3.2 Cloud Control Panel ADSync Utility

HC ADSync Tool is developed as a simple windows service "HCdirSync". This service is deployed onto domain controller in the on-premises AD forest. As changes are made in the on-premises domains, the changes are replicated to the cloud environment using direct LDAP communication. It is strongly recommended to use LDAPs for secure communication.

The ongoing user object identity information (properties and attributes) are synchronized using HC ADSync tool. On premise password changes are intercepted and replicated through HC ADSync to associated user object within the private/public cloud.

Newly created user accounts on the on premises domains are synchronized using HC ADSync Tool. Deletion of an on premises user object will result in deletion of the user object and its assigned service offerings in the private/public cloud. Resource mailboxes are treated in a similar concept as user objects.

Synchronization direction is from on premise to the cloud only, resulting in one way synchronization.

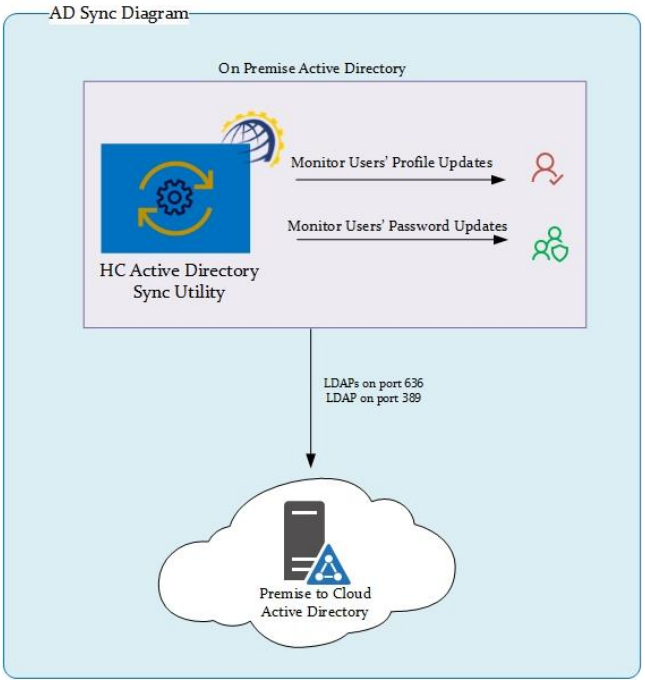

Figure 2: ADSync Diagram

The diagram above shows how changes are detected on the customers' site and synchronized through to the private/public cloud.

3.2.1 Private/Public Cloud AD Secure Requests

Requests are sent to the private/public cloud infrastructure using LDAPs. Its secure request utilizes a combination of a private/public key and a symmetric key (RSA and AES) to securely transfer data and credentials. This ensures the data cannot be intercepted or diverted to another source. Authentication method used is Basic Authentication.

3.2.2 User Object Attributes Synchronization

The following general attributes will be synchronized from a tenant environment into the private/public cloud. Tenant specific attributes are part of the tenant onboarding plan and provided there as such.

Source	Destination	Comments
sAMAccountName	sAMAccountName	
initials	initials	

givenName	givenName	
sn	sn	surname
displayName	displayName	
<password>	<password>	
description	description	
title	title	
thumbnailPhoto	thumbnailPhoto	
telephoneNumber	telephoneNumber	
wWWHomePage	wWWHomePage	
company	company	
manager	manager	
userAccountControl	userAccountControl	only when activated in the cloud
Department	department	
streetAddress	streetAddress	
l	l	location or city
st	st	state
countryCode	countryCode	
postalCode	postalCode	
homePhone	homePhone	
pager	pager	
mobile	mobile	

ipPhone	ipPhone
extensionAttribute1-14	extensionAttribute1-14

Table 1: User object attributes synchronization

3.2.3 HC Control Panel Integration with ADSync

The HC Control Panel user interface has been adapted to assist in the management and deployment of the ADSync utility as well as restricting the changes that can be made for synchronized users.

Users in HC Control Panel that have been synchronized by the ADSync utility are flagged and the control panel user interface will display non-editable user information. This is to avoid user information being updated in control panel and then being overwritten by changes made via the customers Active Directory. HC Control Panel however allows to provision and manage user services.

3.2.4 Installing ADSync on the On-Premise Domain Controllers

The ADSync utility is required to be installed on all on premise domain controllers. The component runs as a hook within the Local Security Authority process of every Domain Controller in the domain. It intercepts all the password change events and replicates the updated password to the private or public cloud environment. For further details, please refer to the following URL: http://help.hostingcontroller.com/enterprise/default.aspx?pageid=active_directory_synchronization

3.2.4.1 ADSync Deployment Scenarios

Following are some scenarios to deploy ADSync:

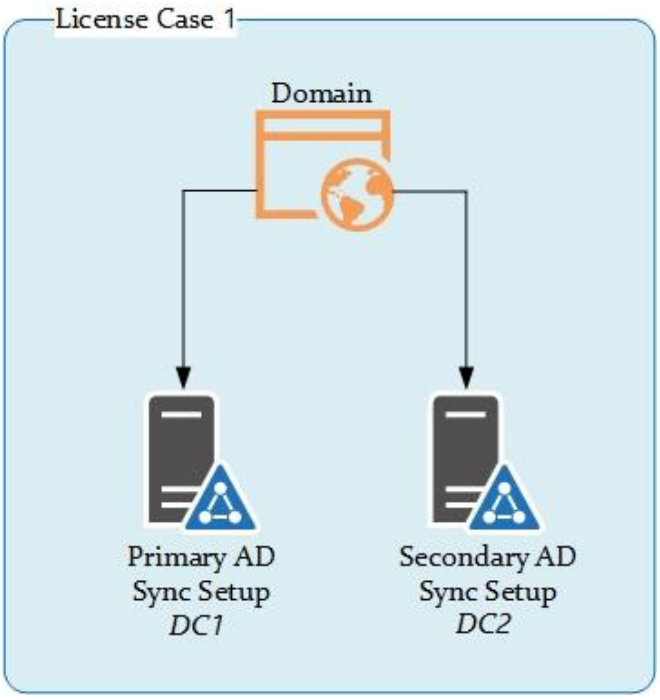

Figure 3: Scenario 1

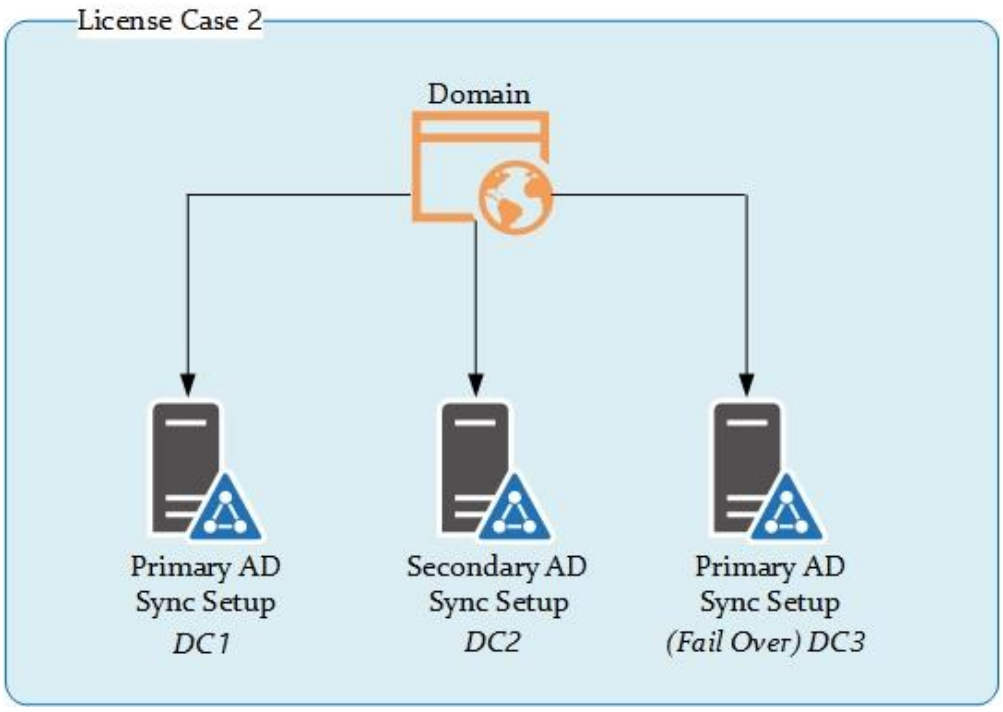

Figure 4: Scenario 2

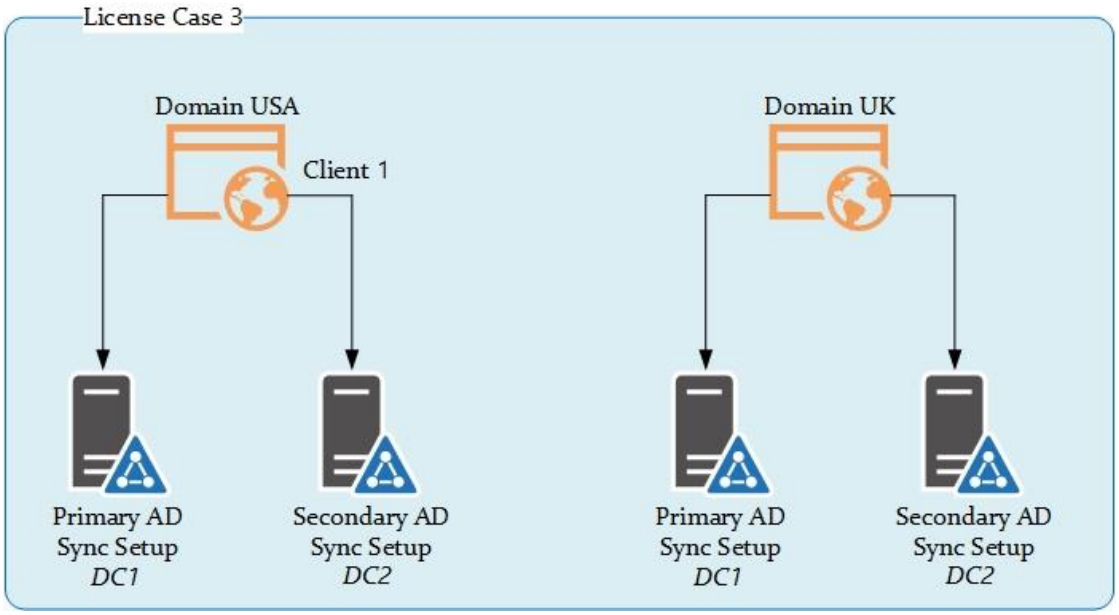

Figure 5: Scenario 3

3.3 HC ADSync Tool Usage Scenarios

The following usage scenarios cover the primary scenarios for the directory synchronization services.

- User Usage Scenarios
  - **User provisioning:** When a new user is created on the on-premise Active Directory, this change is replicated to the cloud.
  - **User property changes:** When properties for user changes those changes are synced to the cloud.
  - **User deletion:** when a user is deleted on the on-premises Active Directory, this change is replicated to the cloud.
  - **Password Changes:** When a user's password is changed, it's replicated to the cloud.
- Distribution Group Usage Scenarios
  - **Distribution group provisioning:** When a new distribution group is created on the on-premise Active Directory, this change is replicated to the cloud.
  - **Distribution group membership changes:** When a user in the tenant organization is added or removed from the distribution group, this change is replicated to the cloud distribution group. This information is visible from the global address list.
  - **Distribution group property changes:** When properties for distribution group changes these changes are synced to the cloud.
  - **Distribution group deletion:** when a distribution group is deleted on the on-premises Active Directory, this change is replicated to the cloud.

- Contact Usage Scenarios
    - **Contact Provisioning:** When a new contact is created on the on-premises Active directory, this change is replicated to the cloud.
    - **Contact Deletion:** When a contact is deleted on the on-premises Active Directory, this change is replicated to the cloud.
    - **Contact Property changes:** When properties of contacts are changed on the on-premises Active Directory these changes are synchronized to the cloud Active Directory.

Contact Us

In case of any ambiguity/query regarding HC Active Directory Sync module, please feel free to contact us at support@hostingcontroller.com.