forsyte
CLOUD CONNECT

B2B COLLABORATION MADE SIMPLE

An in-depth guide on CloudConnect, the B2B collaboration service powered by Forsyte I.T. Solutions. Learn more at forsyteit.com/cloud-connect.

Table of Contents

Executive Summary

As the need for organizations to seamlessly collaborate across tenants and environments has grown, Forsyte I.T. Solutions identified the need for a tool that makes this easier to manage. Historically, the only way that separate organizations could work together as though in the same environment was to stand up their own complex infrastructures or fully migrate to the same tenant. CloudConnect was built to ease the B2B collaboration burden and uses Azure cloud technology and tools to bridge the gap and create connections. Whether supporting a temporary partnership or longer-term collaboration infrastructure, CloudConnect makes B2B collaboration easy to manage, reducing the roadblocks for growth.

Problem Definition

Organizations often find themselves in situations where they need to frequently collaborate with individuals in outside tenants or environments. This happens for a multitude of reasons, such as:

- Mergers and acquisitions
    - Organizations have a desire to consolidate/migrate into a single tenant in the future but need enhanced collaboration today. Cloud Connect w/B2B accounts can act as a bridge solution. Providing a better experience today with minimal effort during the consolidation/migration process

- Partner organizations
    - Collaborations with other organizations you never intended to migrate or consolidate but need a temporary way to collaborate.
        - Partner Companies
        - University Systems
        - State Departments of Education

- Multiple tenants within the same organization
    - Organizations need to work together without engaging a full migration, B2B accounts offer a viable solution.
    - Students in one tenant and Faculty and Staff in another.
    - Medical school in one tenant and University Campus in another.
- Different platforms utilized within the organization.
    - Google and Microsoft are both utilized
        - i.e. faculty and staff on Office 365 and students in Google

Introduction to CloudConnect

CloudConnect is a SaaS-based service designed by Forsyte I.T. Solutions to accelerate cross-organization collaboration between cloud-based identity/email providers and Microsoft Azure. CloudConnect allows for the mass creation of Azure Business to Business (B2B) accounts across multiple tenants as well as across an Exchange Global Address List (GAL). CloudConnect's collaboration engine can be configured and synchronized in minutes without the need for infrastructure, firewall, or network changes. Organizations of all sizes can effectively manage address list synchronizations and guest accounts in a simple and easy to use interface.

Solution Overview

CloudConnect was born out of the need to connect a large number of loosely affiliated organizations in a quick and efficient manner. Given our extensive identity background, we first looked at traditional solutions but quickly realized that the logistics of making this type of deployment a reality were difficult to overcome. After taking a step back and looking at the problem from a different angle, we decided to create an entirely new and innovative product focused on connecting cloud-based directories. This approach offers a few distinct advantages as they require ZERO networking, ZERO firewall changes and ZERO infrastructure. It also lets us reduce a multi-month deployment to minutes.

Use Case Scenarios

GAL Synchronization

A university system needed unified GAL synchronization. In late Fall of 2018, a university system client began planning to unite its 12 universities for better collaboration, connectivity, and functionality when working together. They wanted to keep their own identities but still seamlessly connect their B2B environments without having the usual common confines.

As a first step, the system wanted to try MIM for the GAL sync between the universities, but only found numerous hurdles and restrictions standing in their way. They specifically ran into roadblocks because they wouldn't open up ports. Forsyte proposed a tool to the organization and a few weeks later, they piloted it.

After years of attempting to set up their university system to easily work together in a B2B environment, it worked with CloudConnect! It was like pushing the EASY button. "It was so easy in comparison with MIM," said one of the project leads.

Teams Access

A large university system needed streamlined access of Teams as though they were on the same environment. The system wanted to remain separate but have access to one tenant so they could collaborate as though on one. In Teams, there is a limitation on what a B2B user can use vs. a full access user. i.e. Guests cannot create their own teams and students will be the guests in the faculty/staff tenant. In this instance, the University system wanted to effectively leverage the use of Teams for collaboration internally and for a council to which they belonged.

The council was comprised of technicians for the 18 major universities in the state. The goal was to create a collaboration platform using Teams that would enhance communication between the technicians and better support the execution of joint projects. Likewise, the goal is to showcase the capabilities of Teams to promote Teams adoption and consumption across the state within higher education.

Forsyte used CloudConnect to assist with the design and deployment of a Teams platform for the council. Emphasis was placed on providing a secure collaboration platform tailored to the needs of the council and to use the opportunity to educate the council members on the capabilities that Teams offers.

Shared Access is a Single Environment

A large consortium needed shared access across one environment for various team members. All colleges are not governed by a central IT and they did not want to be branded as one entity. At the same time, they wished to have the functionality to simplify and foster collaboration broadly as though they were on one tenant.

CloudConnect allowed them to share applications and resources more easily, such as Teams, calendars, and email. Another important factor for the consortium was GAL synchronization.

Features and Benefits

Better Collaboration Experience

Utilizing B2B accounts and CloudConnect lets organizations quickly realize the ROI on their Microsoft investments and provides additional collaboration capabilities between disconnected environments. At its core, organizations are looking for a better collaboration experience, translating into tangible features, such as:

- A unified Global Address List (GAL) across organizations and platforms (Office 365, G Suite, Exchange)
- Calendar sharing between organizations
- Enabling Microsoft Teams Collaboration
- Providing granular access to SharePoint or other Azure based services (VM's, SSO Apps, etc.)
- Create Azure B2B accounts en-masse sourced from Office 365 or G Suite tenants
- Extend Azure B2B account access to on-prem AD
- Enable synchronization in minutes, not weeks
- Manage different entities in one service.

The Hub

CloudConnect was designed to offer ease of functionality and a single-pane view of transacted activities while managing users and activities in an easy to access framework. To accomplish this, Forsyte created a web portal named The Hub..

The Hub makes it easy to track and manage activities within CloudConnect, such as managing error logs and sync logs to maintain clear visibility of the operations of your system. Also found in The Hub is the status of each server, allowing a single pane view of all on-prem agents and their server statuses.

When an activity is transacted in The Hub, a notification will be displayed within The Hub to administrators, alerting on the type of activity. For example, such activities include the addition of new data sources, synched status, share status, server's status, and so on. Any activity will be displayed as alerts in the Hub.

Security First

From a security standpoint, CloudConnect gathers as little information as possible from the client/organization. CloudConnect encodes an organization’s crucial data to be moved by the CloudConnect API and the information is encrypted and protected within Forsyte’s systems.

The different CloudConnect processes completed within The Hub are managed and stored for a simple view into each activity. The information retained by CloudConnect is managed by Forsyte’s own Cosmos DB API, making the information transactions more secure, encoded, protected, and encrypted to avoid exposing the database. This secures the endpoints and code in the database, as the data is processed entirely by Forsyte’s APIs in tightly secured and monitored Azure servers.

Security Posture

- All Application IDs and Keys are stored in FIPS 140-2 Level 2 compliant Hardware Security Modules (HSMs).
- All data synchronizations happen in memory to ensure that no user information is stored in our databases.
- Any metadata that is required to be kept is encrypted at rest.

Technical Configuration

CloudConnect is a cloud-based solution, providing the scalability to synchronize even the largest environments in short order. The following sections outline technical details of the CloudConnect offering. The following key terms will be explained along with a workflow of how the solution works using: Data Sources and Synchronization Policies.

Data Sources

A minimum of two data sources must be configured prior to building synchronization policies. A data source is a connection object consisting of the following information:

- Name
- Tenant ID
- Application ID
- Application Key

Data Sources, explained:

- Name: The Name field is simply a display name for the connection object that will be shown in the portal.
- Tenant ID: This is the tenant ID for the data source.
- Application ID and Key: A service principle[1] is required to manipulate the data sources. Once the service principal is created, the application ID and Key must be associated with the data source. CloudConnect stores the connection information in a secure key vault for access by the service as needed.

[1] The service principal nomenclature is used in Azure AD, the term may differ depending on the data source

Synchronization Policies

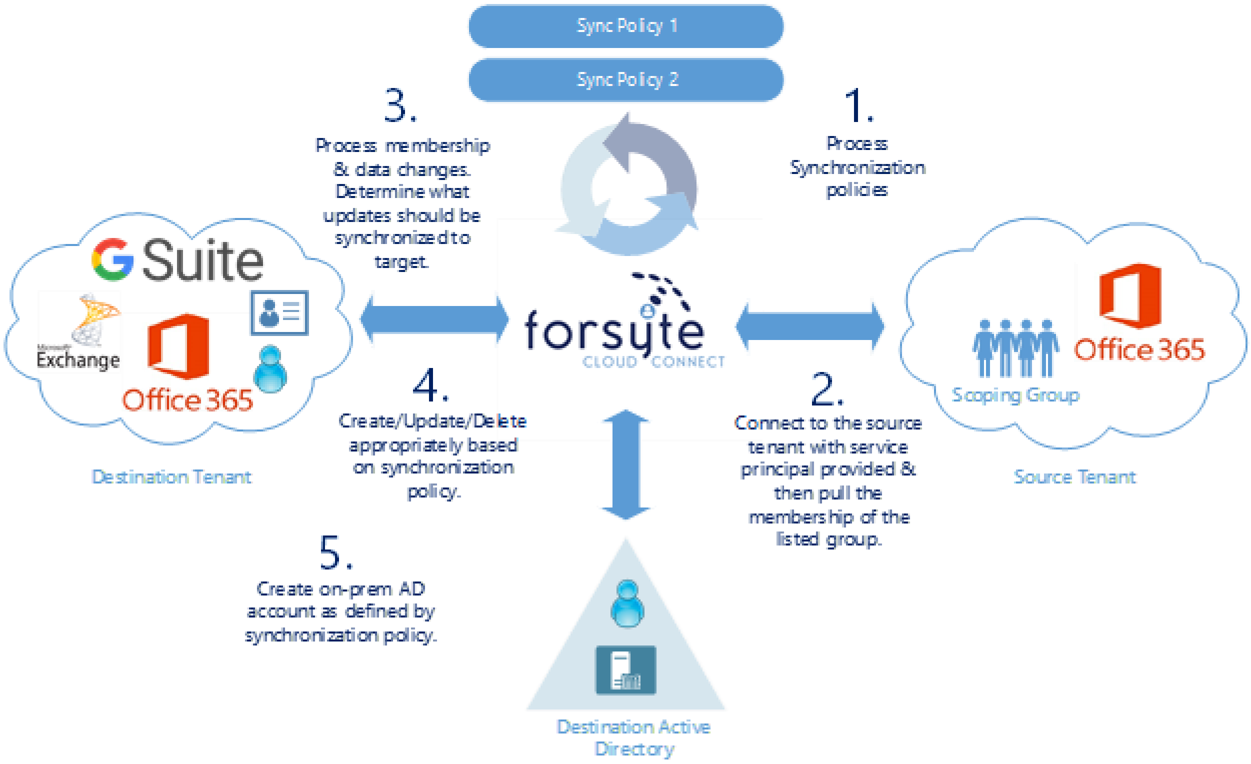
- Synchronization policies are at the core of the CloudConnect tool and determine the:
    - Target and Source data sources
    - Direction of data flow
    - Type of object being managed
    - Scope of objects
    - Attribute flow
- Synchronization policies are processed independently for each customer and are processed in a continuous fashion.

Synchronization Policy Workflow

The following provides the high-level process for synchronization:

1. A rule is selected for processing.
2. Upon selection, the web service determines the source and target data sources for the policy.
3. The web service collects the appropriate service principal information from the key vault.
4. The web service connects to the source directory and enumerate the members of the selected scoping group. Deltas are used when possible
5. Create, Read, Update, Delete (CRUD) operations are performed in the destination data source as necessary depending on the results of the previous step
6. If required by the policy and properly configured on-prem AD accounts can be generated.

Synchronization Diagram


Sync Policy 1
Sync Policy 2
3.
Process membership & data changes. Determine what updates should be synchronized to target.
1.
Process Synchronization policies
G Suite
Exchange
Office 365
Destination Tenant
forsyte CLOUD CONNECT
Office 365
Scoping Group
Source Tenant
4.
Create/Update/Delete appropriately based on synchronization policy.
2.
Connect to the source tenant with service principal provided & then pull the membership of the listed group.
5.
Create on-prem AD account as defined by synchronization policy.
Destination Active Directory

Additional Considerations

- There are no special licensing needs, unless you are using Azure AD Premium features. Learn more: https://docs.microsoft.com/en-us/azure/active-directory/b2b/licensing-guidance.
- When using CloudConnect for Teams connections, there may be a cap on the number of guests you can create.
- Conditional access is not available on the 5:1 premium feature.
- You must have premium licenses to set up dynamic groups. Though there are ways around this, you must have one to turn it on.
- B2B is a 5:1 license. If an organization is hosting it in one tenant, there may not be enough licenses.

Summary

In summary, CloudConnect provides an easy to setup and use solution for organizations looking to engage in collaboration across tenants or environments. For organizations looking to gain a richer collaboration experience across tools such as Teams and provide enriched access to guest users, CloudConnect offers that functionality without the time and expense of network infrastructure changes, tenant consolidation or identity access management typically associated with those efforts. .

Quickly access the data you need in separate tenants and environments. Extend centralized services to partner organizations without standing up your own infrastructure or engaging in complex implementations.

CloudConnect supports multiple platforms and provides an automated method to access internal resources for external organizations and global address list synchronization.

Engage Forsyte I.T. Solutions for additional information and access to CloudConnect:
info@forsyteit.com | 844.587.4535 | forsyteit.com/cloud-connect