Integrate with in-prem LDAP server for secure authentication

Overview

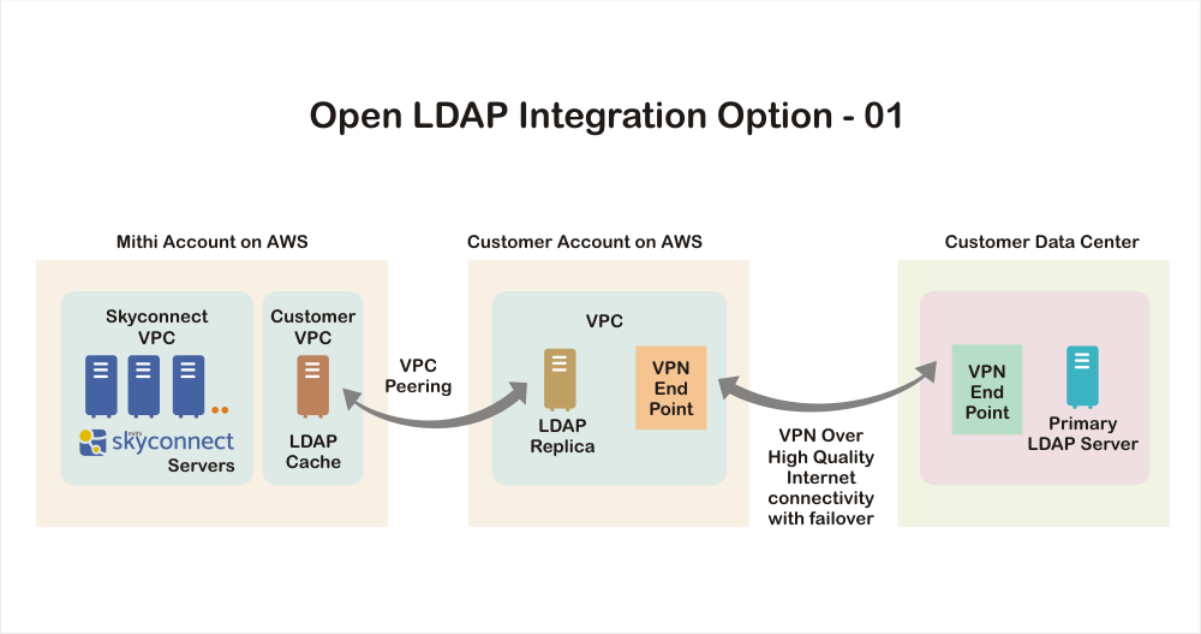
A SkyConnect domain can be setup to authenticate with your in-premise LDAP setup, allowing end users to access the mailboxes and other SkyConnect applications using the domain passwords.

There are two options to setup as follows:

Option 1: Setup with a LDAP replica in the Customer Account on AWS (Recommended when the SkyConnect / Vaultastic users are 500 or above)

In this setup,

1. Customer will have own account on AWS (in the same region as the SkyConnect / Vaultastic domain is hosted for the customer). There will be a LDAP replica and the VPN end point in this account.
2. The Mithi Account where all the SkyConnect & Vaultastic servers are hosted will have a LDAP cache server connecting to the LDAP replica in the Customer account.
3. In the customer's in-premise data center, a VPN end point will be setup to connect to the customer account in AWS.



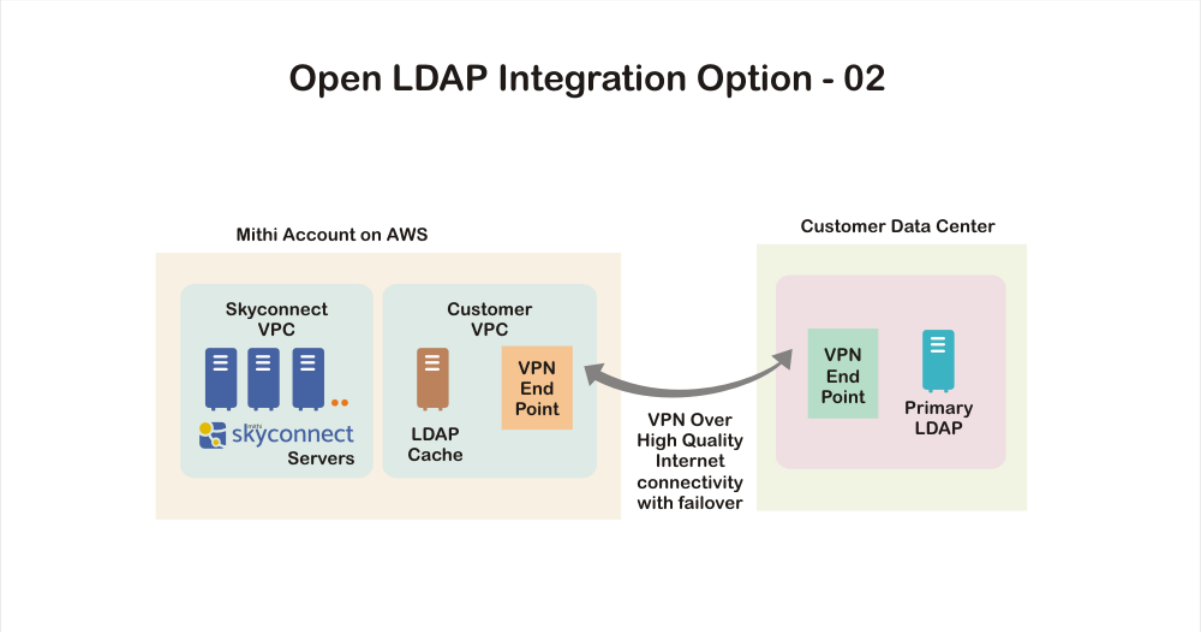
Option 2: Setup without a LDAP replica on AWS

In this setup,

1. There is no LDAP replica on AWS.
2. The Mithi Account where all the SkyConnect & Vaultastic servers are hosted will have a LDAP cache

server connecting to the in-premise LDAP. The VPN end point will be setup to connect to the in-premise servers.

3. In the customer's in-premise data center, a VPN end point will be setup to connect to the customer account in AWS.



Mithi Account Setup on AWS

The components required for the integration with the in-premise LDAP server in the Mithi account are maintained and configured by the Mithi team. These are as follows:

SkyConnect VPC (Virtual Private Cloud)	All the Mithi SkyConnect servers are hosted within this VPC.
Customer VPC (Virtual Private Cloud)	Every customer will have their own VPC within the Mithi account. The LDAP cache server (for both the options) will be in this VPC. For option 2, the VPN end point will also be in this VPC. The range of this VPC will be 100.64 and for option 1, this VPC will be peered with the VPC in the customers AWS account.
LDAP cache	The LDAP cache server will be configured to read and cache authentication information from the in-prem LDAP server for Option 2 or the LDAP replica from the customer account for Option 1.
VPN End point	Only for Option 2. This will be configured to connect to the VPN end point in the customer data center.

Customer account setup on AWS

For Option 1, the LDAP replica and other components required for the integration will be setup and managed by

the customer team. The details are as follows:

VPC (Virtual Private Cloud)	The components required for the integration are setup in this VPC
LDAP replica	A read-only replica of the in-premise LDAP server. **Note**: Setting up the replication of LDAP between the primary and the replica is the responsibility of the customer.
VPN End point	This will be configured to connect to the VPN end point in the customer data center.

Note: The above should be setup in the same region as the SkyConnect domain.

Customer in-premise setup

The LDAP server at the customer location and other components are maintained by the customer. The details are as follows:

Internet connectivity	2 High Quality Internet connections to configure the VPN
VPN End point	This will be configured to connect to the VPN end point in AWS
Primary LDAP server	The primary LDAP server at the customer location.

Availability of the different components and impact on end users

Depending on the state of the VPN connectivity and the availability of the LDAP Replica or primary the primary LDAP server, end users will experience authentication as explained in the table below.

Scenario	Primary LDAP State	VPN State	LDAP cache state	Service Status	User Impact
Business as Usual	Up	Up	Cache is inline with a TTL of 15 minutes	All services up	Change in password on primary will reflect after cache expires (max 15 minutes)
Primary LDAP server is down	Down	Up	Cache is offline	All services up	Users can continue to authenticate with the cached passwords
VPN is down	Up	Down	Cache is offline	All services up	Users can continue to authenticate with the cached passwords. Changes to passwords on the primary server will not be reflected

Scenario	Primary LDAP State	VPN State	LDAP cache state	Service Status	User Impact
VPN changes from down to Up	Up	Up	Cache comes online and starts replicating	All services up	Users can continue to authenticate with cached passwords. There will be a delay in new passwords reflecting in the cache.
Slow connection to the in-prem servers	Up	Slow	Cache is online and can be made offline	Slow access to services if cache is online	Users can continue to authenticate with cached passwords. There will be a delay in new passwords reflecting in the cache.
One of the VPN lines is down	Accessible	Up	Cache is online	All services up	Change in password on primary will reflect after cache expires (max 15 minutes)

Reference links

- https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnections.html
- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#SetUpVPNConnections
-
- http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.html