Centralized Credential Management (SSO) for Cloud Authentication Use Case Scenario

CoIP™ Ensures Single Sign-On Across Cloud Ecosystems

The CoIP Platform is purposefully designed to support simple and straightforward connectivity, from outside servers/applications/systems to the Single Sign-On (SSO) services behind the corporate firewall, using CoIP's next-generation virtual overlay network. CoIP allows companies to define and implement on demand virtual overlay network across cloud ecosystems.

This Use Case scenario describes cloud authentication with a centralized LDAP service that sits behind corporate perimeter firewalls, utilizing the benefits provided by the CoIP Platform.

Centralized Credential Management is Needed to Authenticate Resources in the Cloud

A centralized directory service for credential management allows companies to unify authentication and authorization, as well as control provisioning, access rights and related services. LDAP (for Lightweight Directory Access Protocol) is widely used for setting and implementing access permissions, that is, to filter who gets access to what compute resources and data in addition to defining schema and related items.

Companies may have disperse systems that, with the migration of corporate applications to the cloud, could be running on different domains— corporate datacenter, public cloud or private cloud. Each of these systems typically restricts access to users by requiring authentication credentials. A centralized LDAP is required so that all credentials are stored in a single place and in a secure environment (usually behind the corporate firewall) for easy administration and security.

SSO Across Cloud Ecosystems is a Challenge

Servers for SSO services, such as LDAP and AD, are typically hosted behind the corporate firewall to protect critical security information and for central administration. These servers need to be accessed by different servers and applications running inside or outside the corporate firewall (e.g., in the public cloud or hosted environments). Any connectivity to the SSO servers from outside the firewall needs the firewall to be opened and a path to be set up within the corporate network to direct that outside traffic to the SSO servers.

Current connectivity options require companies to set up VPNs from servers residing on different domains to the centralized SSO server. Typically, this requires:

- Setting up VPN gateways in each domain
- Shielding the network in the domain behind the VPN gateway for security
- Opening the corporate firewall to allow VPN inbound traffic
- Reprogramming the corporate firewall to limit the outside servers' access to only the SSO servers

This procedure often causes significant technical difficulties as well as multiple infosec (security) reviews, leading to substantial delays.

Centralized Credential Management (SSO) for Cloud Authentication Use Case Scenario

Benefits of Using CoIP for SSO Across Cloud Ecosystems

Conventional		CoIP
Set up VPN Shield network domain Open firewalls Program firewalls	**vs.**	Click to set up overlay network
Takes months to complete		Takes minutes

The CoIP platform allows companies to define, implement, provision and secure overlay networks within and between on-premise and cloud domains without disrupting the existing enterprise network or perimeter security. CoIP creates a virtual network plane that acts as a network security fabric. To connect the central LDAP authentication server to resources in the cloud, CoIP offers multiple benefits, most importantly:

- The CoIP implementation is easy and quick because overlay network technology does not require physical network changes like setting up VPNs, opening firewalls, redesigning subnets and so on.
- One virtual CoIP appliance can manage numerous remote servers connecting to the central LDAP.
- The impact to corporate compliance and governance is minimized by maintaining the existing physical security perimeter infrastructure.
- Project effort is efficient due to fast time-to-trial and time-to-production.

Example Solution: Centralized LDAP Authentication on a CoIP Overlay Network

This section described how to use CoIP technology to set up centralized LDAP authentication protected behind a corporate firewall. This can be readily accomplished using a single virtual appliance set up in an AWS or Microsoft Azure cloud datacenter. Any number of remote servers can connect to the central LDAP server without VPNs and without any changes to the physical network infrastructure such as firewalls and subnets.

In this scenario, application servers in the public cloud need LDAP authentication services from the corporate datacenter.

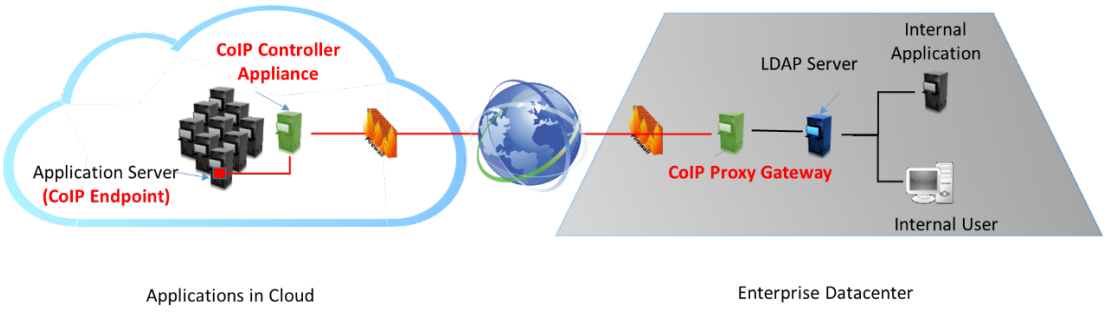

Figure 1. LDAP Implementation without VPNs Using CoIP

Centralized Credential Management (SSO) for Cloud Authentication Use Case Scenario

Setting up the centralized LDAP using CoIP is straightforward, using the following CoIP components as shown in Fig. 1:

- CoIP Network Controller Appliance (available as a virtual appliance for use in the Microsoft Azure and Amazon AWS cloud services)
    - The CoIP management portal, called zCenter, runs on the Controller Appliance. Through zCenter, Application Profiles can be defined that describe policies for CoIP connections and security. CoIP routing and firewalls will be implemented by the system automatically once the endpoints (VM, server, CoIP Edge Gateway) are registered within the Application Profile.
    - zCenter also provides Cloud Connector functions that drive the VM management APIs in the most popular public cloud datacenters, currently including Amazon AWS, Microsoft Azure, Rackspace and HP Cloud.
- CoIP Edge Gateway
    - The CoIP Edge Gateway can be easily implemented using a VM or a physical server. The provisioning for a CoIP Edge Gateway is managed directly from the CoIP zCenter portal.
    - The CoIP Edge Gateway is a CoIP endpoint that bridges IP traffic between the physical network plane and the CoIP plane. As part of the Application Profile policies, a physical IP address or address range can be permitted to connect to the selected CoIP endpoints. Physical IP addresses that are not specified in the Application Profile are not able to route through the CoIP plane.
    - The CoIP Edge Gateway forwards IP packets that are targeted at specific physical IP addresses in the source datacenter to the remote server in the destination datacenter. Those forwarding physical IP addresses need to be configured in the Edge Gateway, which should be deployed in the network at a place where the forwarding packets are routable to the Gateway.
- CoIP Endpoint Clients
    - CoIP endpoint clients are straightforward to install on a VM or a server using the CoIP zCenter portal.

Conclusion – CoIP Solves the SSO Problem Across Cloud Ecosystems

Using the CoIP approach significantly simplifies the establishment of a centralized SSO service, by eliminating the need for cumbersome conventional networking techniques. CoIP is decoupled from the underlying physical network and is domain-agnostic, so it can be used in any environment. With the CoIP platform, a centralized SSO service, such as LDAP or AD, can quickly be connected to any number of remote servers, without any changes to any underlying physical network infrastructure in the corporate datacenter or in the public cloud.