zentera™
Connect · Protect · Shield

Burst Computing to the Cloud: Use Case Scenario

CoIP™ Platform Enables Secure On-Demand Networked Burst Computing

The CoIP (Cloud over IP) platform supports on-demand bursting of applications to the cloud. CoIP allows customers to spin up virtual machines in the cloud, define and implement overlay network connectivity on a virtual network plane and secure compute resources in the hybrid cloud.

This Use Case scenario describes options for applications to burst to the cloud on demand, utilizing CoIP and the benefits provided by the CoIP solution.

The Opportunity: Leasing On-Demand Computing

Businesses need additional compute capacity, though this occasional or seasonal need typically does not justify investing in a permanent datacenter expansion. More and more companies are turning to the unlimited compute capacity available on demand in the public cloud. By renting compute capacity in the cloud, companies are not only avoiding large capital investments but also converting capital expenses into operating expenses.

The Challenge: On-Demand Secure Networking

Compute capacity in the cloud is available on demand and can be easily set up on public clouds such as Azure and AWS. However, the same is not true for connectivity between compute resources in the cloud and those in the on-premise datacenter. Current connectivity options require companies to set up VPNs between the cloud and the on-premise datacenter. Typically, this requires:

- Setting up VPN gateways in each domain
- Shielding the network in the cloud behind the VPN gateway for security
- Opening the corporate firewall to allow VPN inbound traffic
- Reprogram routing table such that the on-premise access from the cloud is properly routed and restricted

This procedure often causes significant technical difficulties as well as multiple InfoSec (security) reviews, leading to substantial delays. Additionally, it establishes a permanent connection between the cloud and the on-premise datacenter that does not mirror the on-demand operational model of the compute capacity.

The Value of CoIP: True On-Demand Secure Networking for Burst Computing

Conventional		CoIP
Set up VPN Shield network in the cloud Open firewalls Reprogram routing table	**vs.**	Click to set up overlay network
Permanent		On demand
No integration or automation with virtualization or cloud orchestration		Cloud connector allows spinning up VMs in most public clouds and OpenStack from within CoIP
Takes months to complete		Takes minutes

Burst Computing to the Cloud: Use Case Scenario

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. More importantly, since it is quick and easy to provision, it can be set up and torn down on demand along with the compute capacity leased in the public cloud. CoIP creates a virtual network plane that acts as a network security fabric. Additionally, CoIP is integrated with the cloud orchestration API for most popular cloud, via CoIP's Cloud Connectors. Customers can spin up and shut down VMs in these clouds directly from the CoIP interface, with CoIP network properties automatically configured.

- 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.
- Cloud Connectors allow spinning up and shutting down of VMs in most public clouds and OpenStack from within the CoIP network plane.
- The impact to corporate compliance and governance is minimized by maintaining the existing physical security perimeter infrastructure.
- Productivity is enhanced due to fast time-to-trial and time-to-production.

The Example: Subnet Extension to the Cloud Using the CoIP Overlay Network

This section shows how to use the CoIP technology to burst into a public cloud. This can be readily accomplished using a single virtual appliance set up in an AWS or Microsoft Azure cloud datacenter. Optionally, a physical appliance is available that can be installed on the edge of the corporate network. An overlay network and security fabric can be established between the cloud and the on-premise datacenter without VPNs or changes to the physical network infrastructure such as firewalls and subnets.

In this scenario, during a compute burst, instead of deploying six additional servers inside the internal subnet in the enterprise datacenter, the customer deploys the six servers in the cloud. The six servers in the cloud behave as if they are on the enterprise internal subnet, presenting a transparent implementation to users accessing the internal subnet.

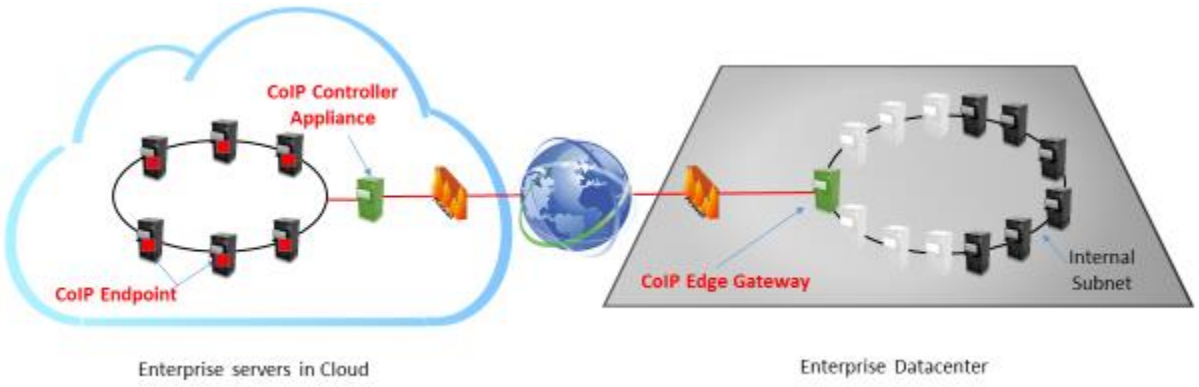

Figure 1. Subnet extension into the cloud during a burst

Burst Computing to the Cloud: Use Case Scenario

Setting up CoIP for burst to the cloud is straightforward, using the following CoIP components (see Fig. 1):

- CoIP Controller Appliance (available as a virtual appliance for use in the Microsoft Azure and Amazon AWS cloud services or a physical appliance in the customer datacenter)
    - 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 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 an 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.

The Conclusion: CoIP Solves the On-Demand Bursting into the Cloud

Using the CoIP approach significantly simplifies enterprises bursting into the cloud by eliminating the need for cumbersome conventional networking techniques. CoIP is decoupled from the underlying physical network and is cloud-agnostic, so it can be quickly used in any environment. With the CoIP platform, an enterprise can quickly spin up virtual machines in the cloud for bursting and securely connect them back to the enterprise in minutes without any changes to any underlying physical network infrastructure in the corporate datacenter or in the public cloud.