Active-Active Connectors on AWS

Cloudbrink Connector component is needed for providing secure zero-trust access to private applications hosted inside the customers private networks. Cloudbrink supports access to private networks in a physical on-prem datacenter or virtual CSP hosted datacenter such as VPC/VNET on AWS, Azure or GCP.

From 14.2 release, Cloudbrink will support Connector deployments in Active-Active mode on AWS, apart from the earlier modes of Standalone or Active-Standby. The Active-Active mode of deployment is available on AWS only for the 14.2 release.

Points to note:

- Up to 64 Connector instances can be clustered in one logical Active-Active Connector group.
- All Connector instances must be in the same AWS VPC.
- When a new Connector instance is added to an existing Active-Active Connector group, new user sessions will be loaded on to the new instance until the load is evenly balanced. Existing sessions on the existing instances will not be touched.
- When an existing Connector instance becomes unavailable for any reason, the user sessions on the particular Connector instance will be re-distributed across the remaining available instances.
- When user sessions are re-distributed, user need not re-authenticate to Cloudbrink. The user's authentication session will remain intact.
- The network level TCP connections will be terminated when the user session is re-distributed to other instances. Applications such as SSH or FTP need to be re-established. Web sessions will see short disruption but continue to work after re-distribution.
- User sessions are distributed across Connector instances based on the session load of the Connector instance.

Use Cases:

A. Horizontal Scaling

Customers having high scale requirements can use the Active-Active mode of deployment to support large number of users. With Active-Active mode, customers can start with a limited number of Connector instances and as the users grow, more Connector instances can be added to support the new scale requirements.

B. Availability

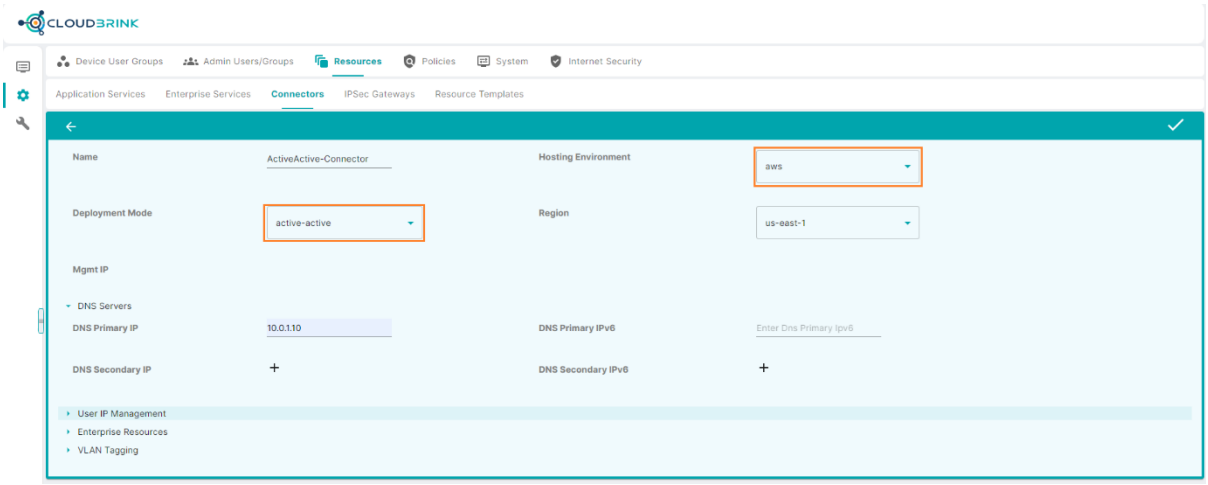
Active-Active mode of Connectors can be used for increasing the availability. When one Connector instance becomes unavailable, the load on that instance will be distributed across all the remaining available instances. This helps in ensuring that in case of an incident, there

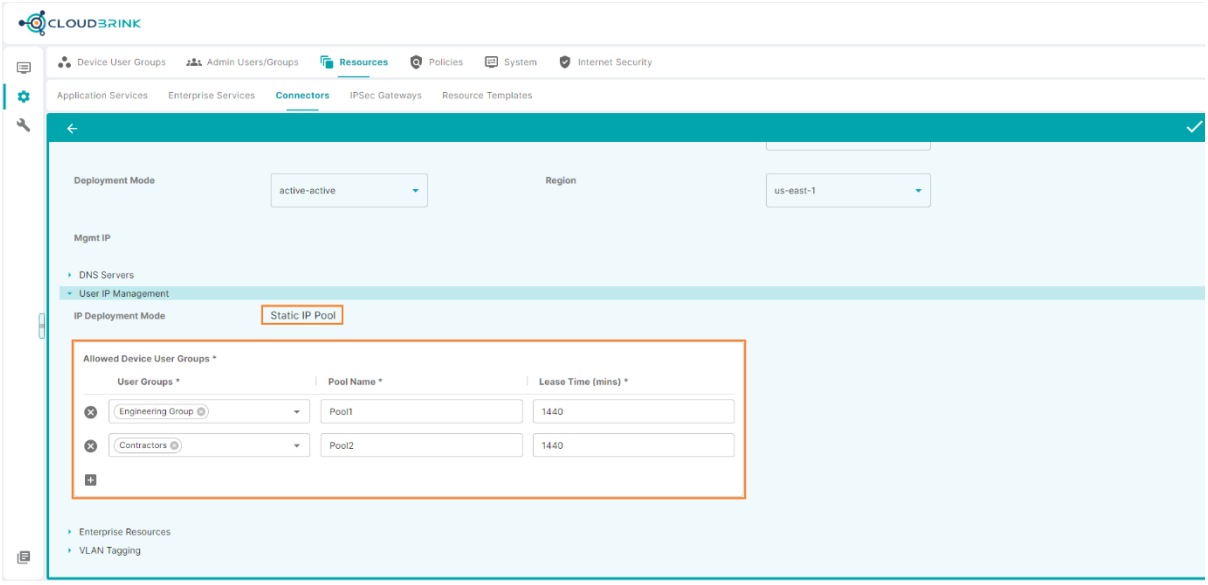
are multiple other instances to take over the load without burdening one single instance (standby).

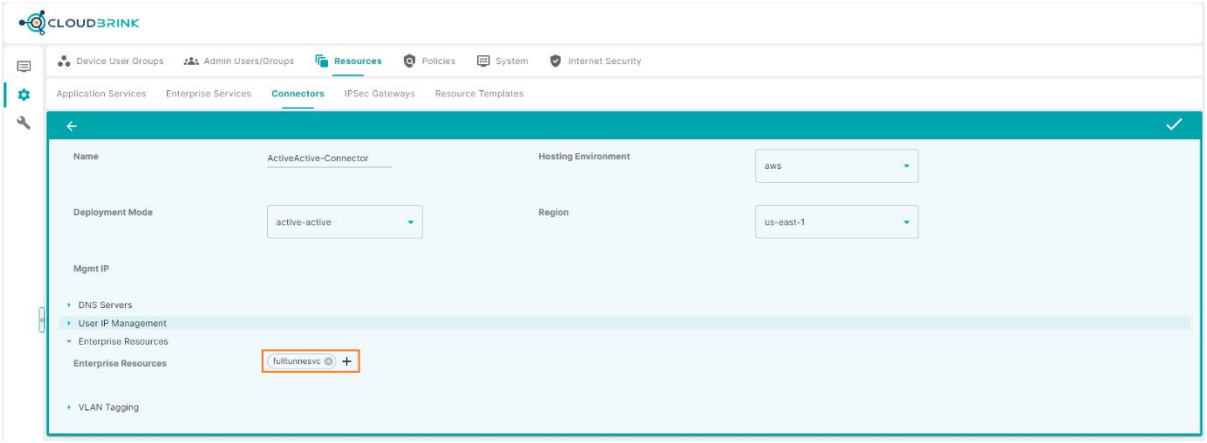
Deployment Steps:

i) **Create Active-Active Connector on Cloudbrink Admin Portal**

a. Navigate to Admin Portal → Configure → Resources → Connectors → Add
b. When adding a new Connector, select “Deployment Mode” as Active-Active. This option will be shown only if “Hosting Environment” is selected as “AWS”
c. Select the list of Device-User-Groups that will use this Connector for accessing private applications. As part of the Device-User-Groups selection, “Pool Names” and “Lease-Time” for each Device-User-Group must be configured.
d. Configure the other parameters (DNS Servers, Enterprise Resources) as usual. “User IP Management” will be pre-selected as “Static IP Pool”
e. Save the Connector



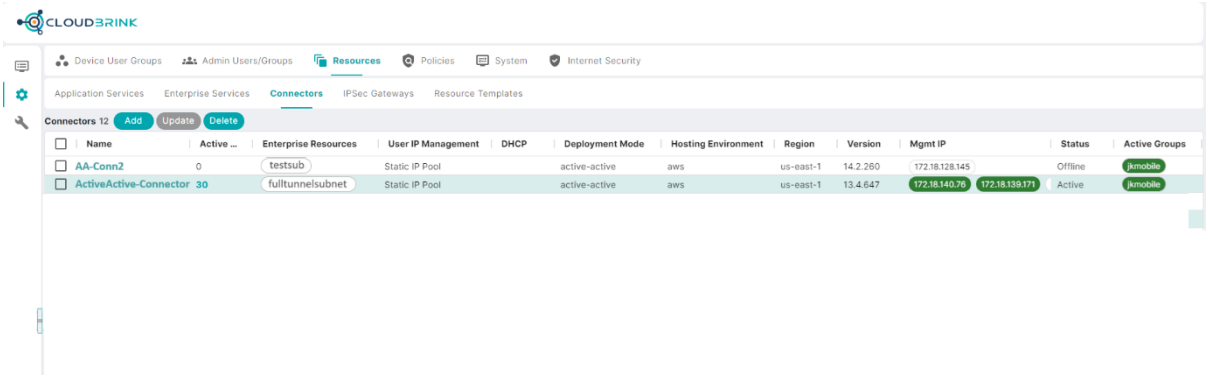




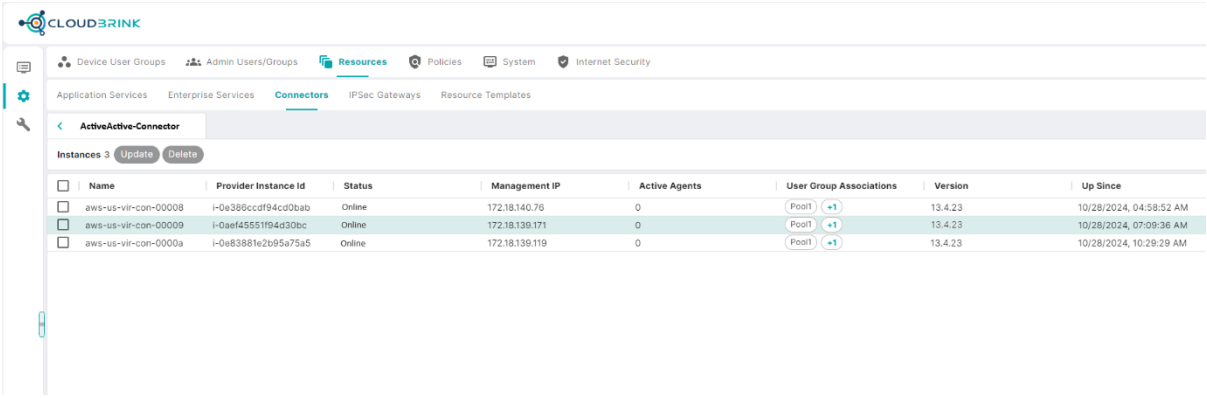
ii) Deploy Connector instances from the AWS Management Console

a. Select the latest Connector AMI from the AWS management console and deploy new instance
b. As part of the cloud-init script, provide correct input parameters such as IP address, Gateway, and the OTP generated from the Cloudbrink Admin Portal for this Connector
c. Once Connector instance deployment is successfully completed on the AWS, Cloudbrink Admin Portal will show the instance in “Online” status

Connector list



Instance level list for each Connector



iii) Configure IP Prefixes for Connector instances on AWS

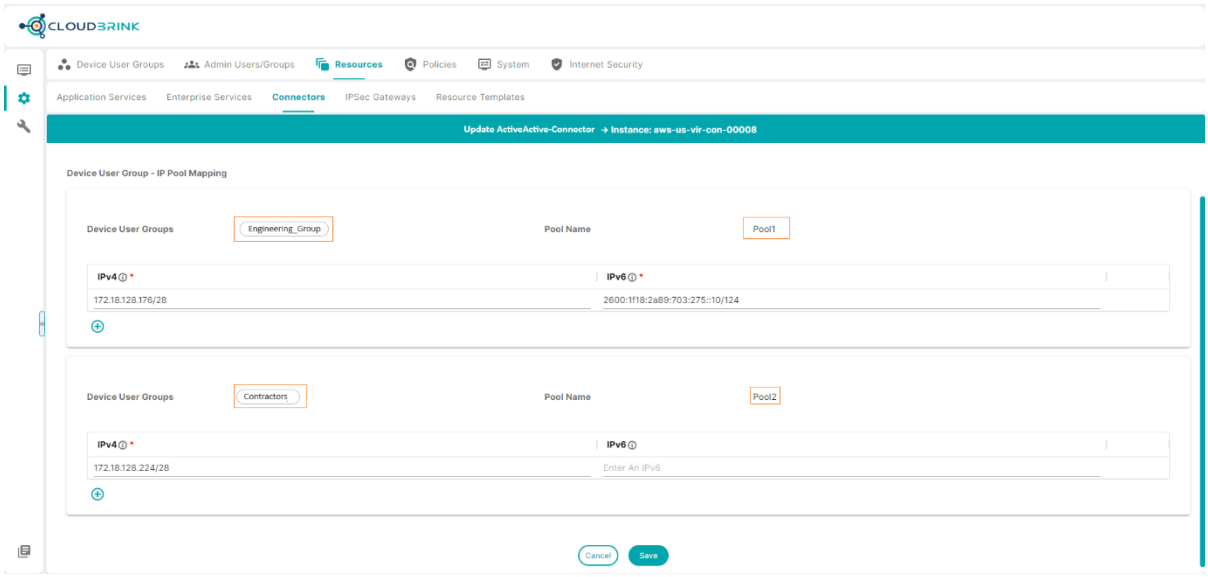
a. From the AWS Management Console, navigate to the Network Interface of each Connector instances and assign IPv4 and/or IPv6 Prefixes. Refer to below documentation https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/work-with-prefixes.html
b. AWS supports /28 for IPv4 prefixes and /80 for IPv6 prefixes
c. Note down the IP Prefixes assigned to the Connector instances because same configuration must be done on the Cloudbrink Admin Portal

iv) Configure Static IP Pools for Connector instances on Cloudbrink Admin Portal

a. Navigate to the Connector instances of the Active-Active Connector by clicking on the Name of the Active-Active Connector
b. Under each Connector instance, the Pool Names that are specified at the Connector level will be prepopulated

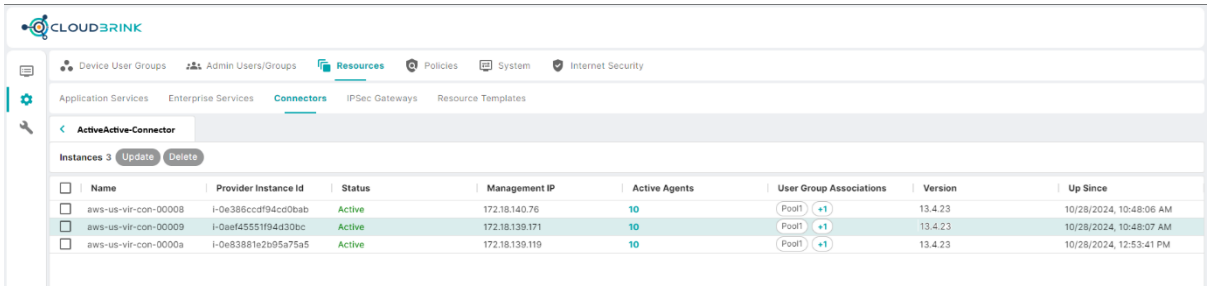
c. For each Pool Name, define the IPv4 and IPv6 Pools. The IP Pools must exactly match the IP Prefixes defined on the respective AWS instances

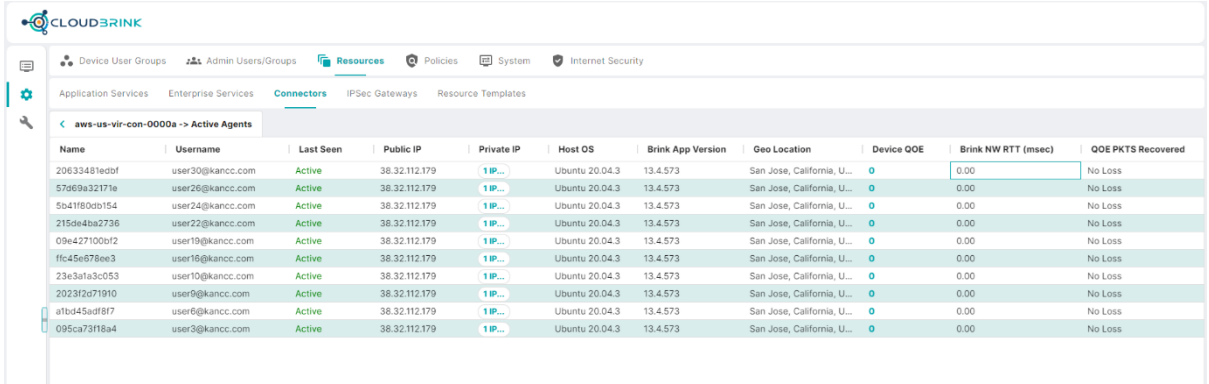
Per instance IP prefix configuration

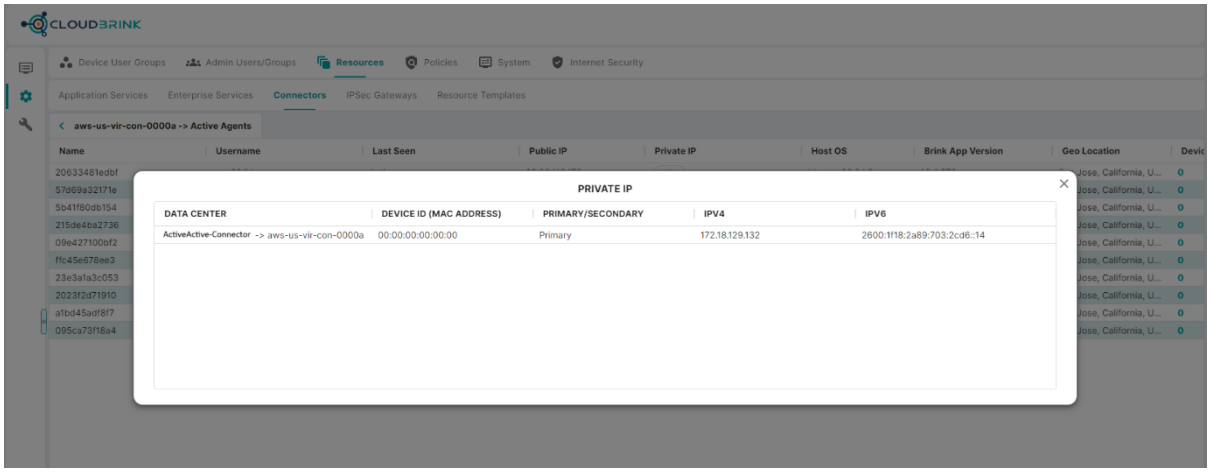


v) Verify the Connector instance status

a. All Connector instances must be in “Active” status. Active status indicates that Connector is ready for handling user traffic to the private applications






CLOUDBRINK
Device User Groups
Admin Users/Groups
Resources
Policies
System
Internet Security
Application Services
Enterprise Services
Connectors
IPSec Gateways
Resource Templates
aws-us-vir-con-0000a -> Active Agents
Name
Username
Last Seen
Public IP
Private IP
Host OS
Brink App Version
Geo Location
PRIVATE IP
DATA CENTER
DEVICE ID (MAC ADDRESS)
PRIMARY/SECONDARY
IPV4
IPV6
ActiveActive-Connector -> aws-us-vir-con-0000a
00:00:00:00:00:00
Primary
172.18.129.132
2600:1f18:2a89:703:2cd6::14