

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

The screenshot displays the Cloudbrink Admin Portal interface. The top navigation bar includes the Cloudbrink logo and several menu items: Device User Groups, Admin Users/Groups, Resources (highlighted), Policies, System, and Internet Security. Below this, a sub-navigation bar shows Application Services, Enterprise Services, Connectors (highlighted), IPsec Gateways, and Resource Templates. The main content area is a form for creating a new connector. The form has a teal header with a back arrow and a checkmark. The fields are as follows:

Name	ActiveActive-Connector	Hosting Environment	aws
Deployment Mode	active-active	Region	us-east-1
Mgmt IP			
DNS Servers			
DNS Primary IP	10.0.1.10	DNS Primary IPv6	Enter Dns Primary ipv6
DNS Secondary IP	+	DNS Secondary IPv6	+
User IP Management			
Enterprise Resources			
VLAN Tagging			

Cloudbrink Admin Portal - Connectors configuration page.

Deployment Mode: active-active | Region: us-east-1

Mgmt IP: [Empty]

DNS Servers: [Empty]

User IP Management: [Expanded]

IP Deployment Mode: Static IP Pool

User Groups *	Pool Name *	Lease Time (mins) *
Engineering Group	Pool1	1440
Contractors	Pool2	1440

Enterprise Resources: [Empty]

VLAN Tagging: [Empty]

Cloudbrink Admin Portal - Connectors configuration page.

Name: ActiveActive-Connector | Hosting Environment: AWS

Deployment Mode: active-active | Region: us-east-1

Mgmt IP: [Empty]

DNS Servers: [Empty]

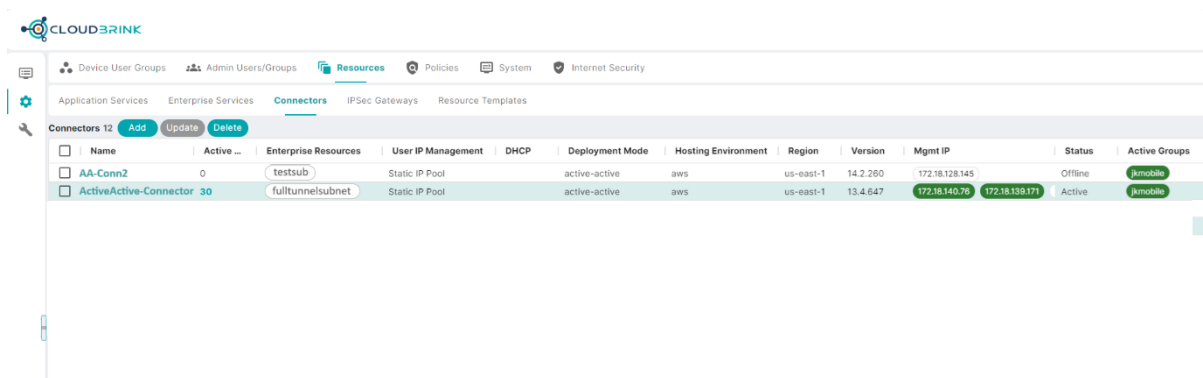
User IP Management: [Expanded]

Enterprise Resources: [Empty] +

VLAN Tagging: [Empty]

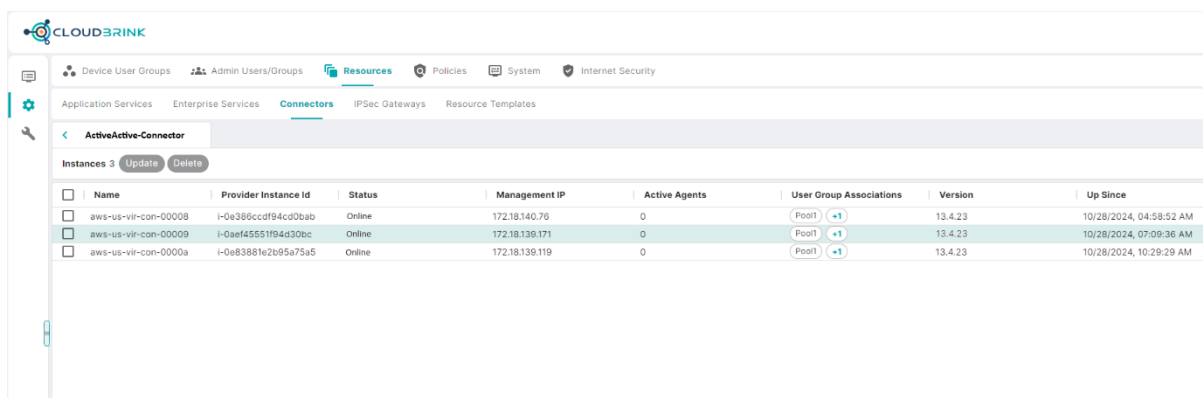
- ii) **Deploy Connector instances from the AWS Management Console**
- Select the latest Connector AMI from the AWS management console and deploy new instance
 - As part of the cloud-init script, provide correct input parameters such as IP address, Gateway, and the OTP generated from the Cloudbrink Admin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

Connector list



	Name	Active ...	Enterprise Resources	User IP Management	DHCP	Deployment Mode	Hosting Environment	Region	Version	Mgmt IP	Status	Active Groups
<input type="checkbox"/>	AA-Conn2	0	testsub	Static IP Pool		active-active	aws	us-east-1	14.2.260	172.18.128.145	Offline	Amobile
<input type="checkbox"/>	ActiveActive-Connector 30		fulltunnelsubnet	Static IP Pool		active-active	aws	us-east-1	13.4.647	172.18.140.76 172.18.139.171	Active	Amobile

Instance level list for each Connector



	Name	Provider Instance Id	Status	Management IP	Active Agents	User Group Associations	Version	Up Since
<input type="checkbox"/>	aws-us-vir-con-00008	i-0e386ccdf94cd0bab	Online	172.18.140.76	0	(Pool) +1	13.4.23	10/28/2024, 04:58:52 AM
<input type="checkbox"/>	aws-us-vir-con-00009	i-0aef45551f94d30bc	Online	172.18.139.171	0	(Pool) +1	13.4.23	10/28/2024, 07:09:36 AM
<input type="checkbox"/>	aws-us-vir-con-0000a	i-0e83881e2b95a75a5	Online	172.18.139.119	0	(Pool) +1	13.4.23	10/28/2024, 10:29:29 AM

iii) Configure IP Prefixes for Connector instances on AWS

- 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>
- AWS supports /28 for IPv4 prefixes and /80 for IPv6 prefixes
- 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

- Navigate to the Connector instances of the Active-Active Connector by clicking on the Name of the Active-Active Connector
- 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

Update ActiveConnector -> Instance: aws-us-vir-con-00008

Device User Group - IP Pool Mapping

Device User Groups: **Engineering_Group** Pool Name: **Pool1**

IPv4: 172.18.128.176/28 | IPv6: 2600:1f18:2a89:703:275:10/124

Device User Groups: **Contractors** Pool Name: **Pool2**

IPv4: 172.18.128.224/28 | IPv6: Enter An IPv6

Cancel **Save**

- 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

Name	Provider Instance Id	Status	Management IP	Active Agents	User Group Associations	Version	Up Since
aws-us-vir-con-00008	i-0e386ccdf94cd0bab	Active	172.18.140.76	10	Pool1	13.4.23	10/28/2024, 10:48:06 AM
aws-us-vir-con-00009	i-0ae45551f94d30bc	Active	172.18.139.171	10	Pool1	13.4.23	10/28/2024, 10:48:07 AM
aws-us-vir-con-0000a	i-0e83881e2b95a75a5	Active	172.18.139.119	10	Pool1	13.4.23	10/28/2024, 12:53:41 PM

Name	Username	Last Seen	Public IP	Private IP	Host OS	Brink App Version	Geo Location	Device QOE	Brink NW RTT (msec)	QOE PKTS Recovered
20633481edof	user30@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
57969a32171e	user26@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
5b41f80db154	user24@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
215de4ba2736	user22@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
09e427100bf2	user19@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
ffc45e978ee3	user18@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
23e3afa3c053	user10@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
2023f2a71910	user9@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
a1bd45edf8f7	user6@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss
095ca73f18a4	user3@kancc.com	Active	38.32.112.179	1P...	Ubuntu 20.04.3	13.4.573	San Jose, California, U...	0	0.00	No Loss

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	Devic
20633481edbf							Jose, California, U...	0
57069a32171e							Jose, California, U...	0
5b41f90db154							Jose, California, U...	0
215de4ba2736							Jose, California, U...	0
09e427100bf2							Jose, California, U...	0
ffc45e678ae3							Jose, California, U...	0
23e3afa3c053							Jose, California, U...	0
2023f2d71010							Jose, California, U...	0
a1bd45ad7817							Jose, California, U...	0
095ca73f18a4							Jose, California, U...	0

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