

Cloud Resource Identification, Inventory and Grouping

Topics Covered



Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

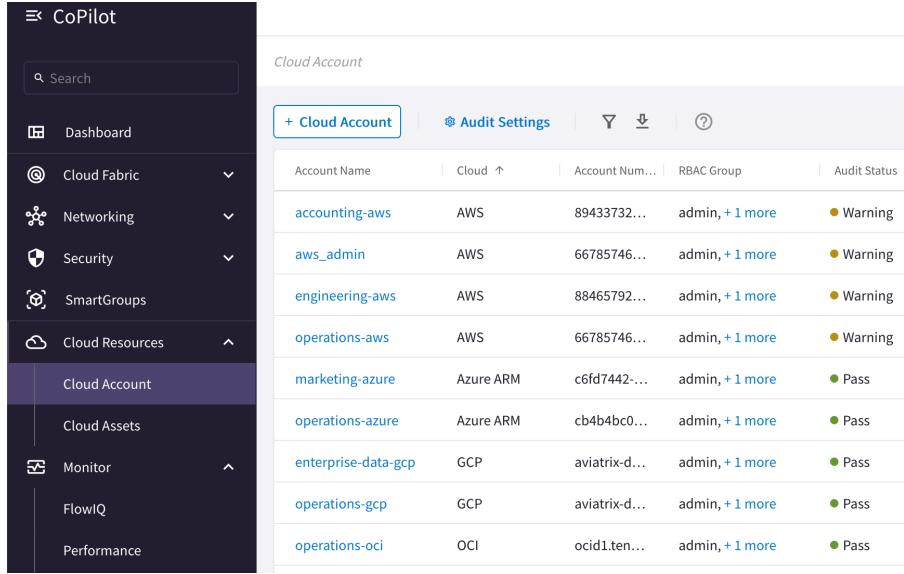
The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

- Asset Inventory using Aviatrix CoPilot Asset Inventory
- Resources identification using tags and other attributes
- Resource Grouping using Aviatrix SmartGroups



CSP Cloud Accounts Inventory

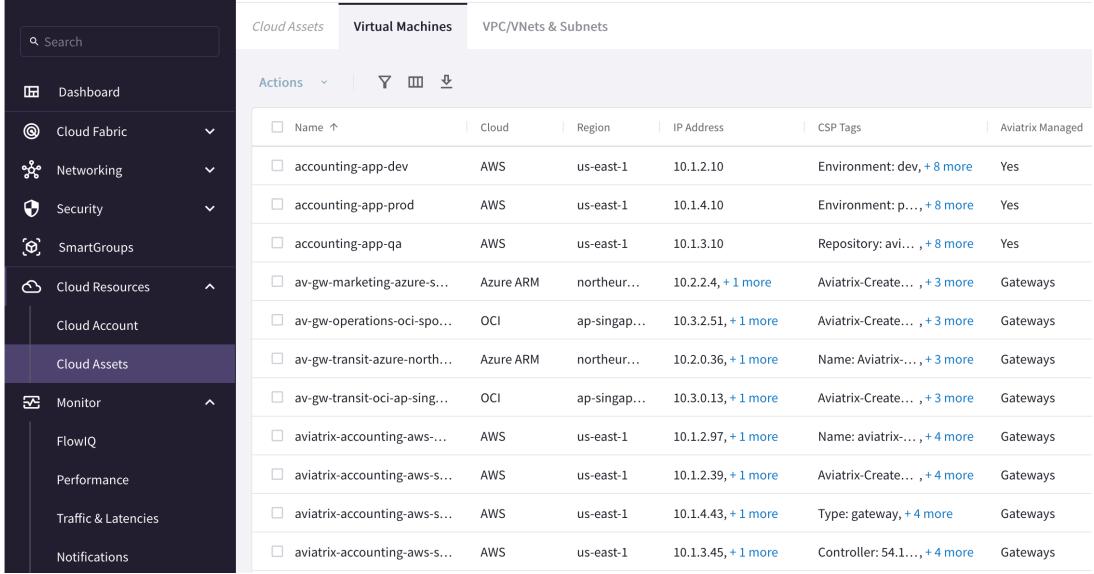






CSP Assets Inventory

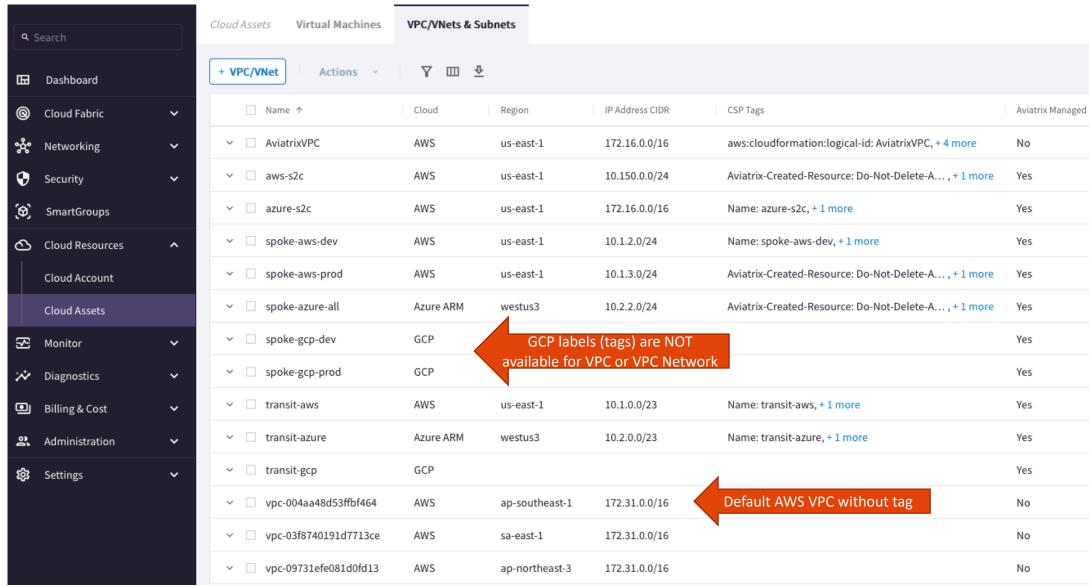






CSP Assets Inventory







Global Routing Inventory – Aviatrix Gateway



Cloud Routes **Gateway Routes VPC/VNet Routes External Connections BGP** Info $\overline{\Phi}$ Ш Tunnel Status VPC/VNet **Gateway Status** Tunnels Routes Gateway ① Up accounting-aws-psf-dev accounting-aws-spoke-dev (10.1.2.0/24) ① Up 0 5 accounting-aws-spoke-dev ① Up ① Up accounting-aws-spoke-dev (10.1.2.0/24) 1 7 accounting-aws-spoke-prod accounting-aws-spoke-prod (10.1.4.0/24) ① Up ① Up 1 7 accounting-aws-spoke-qa accounting-aws-spoke-qa (10.1.3.0/24) ① Up ① Up 1 7 engineering-aws-spoke-dev engineering-aws-spoke-dev (10.5.2.0/24) ① Up ① Up 7 1 engineering-aws-spoke-dev-vpn engineering-aws-spoke-dev (10.5.2.0/24) ① Up ① Up 0 7 engineering-aws-spoke-prod engineering-aws-spoke-prod (10.5.4.0/24) ① Up ① Up 7 1 ① Up ① Up enterprise-data-gcp-spoke-dev enterprise-data-gcp-spoke-dev (10.4.2.0/24) 1 5 ① Up engineering-aws-spoke-qa engineering-aws-spoke-qa (10.5.3.0/24) ① Up 1 7 ① Up ① Up enterprise-data-gcp-spoke-prod enterprise-data-gcp-spoke-prod (10.4.4.0/24) 1 5 enterprise-data-gcp-spoke-qa ① Up enterprise-data-gcp-spoke-qa (10.4.3.0/24) ① Up 1 5



Global Routing Inventory – Cloud Routes



Cloud Routes

Gateway Routes

VPC/VNet Routes

External Connections

BGP Info

7	Ⅲ				
~	Name	VPC/VNet ↑	Route Table ID	Route	es
~	aviatrix-accounting-aws-spoke-dev	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-0f989b2b17ead	2	① Up
~	aviatrix-Aviatrix-Ingress-routing	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-06c99baa2682	3	① Up
~	accounting-aws-spoke-dev-Private-1-us-east-1a-rtb	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-0dacb128698b	5	① Up
~	accounting-aws-spoke-dev-Public-1-us-east-1a-rtb	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-0337086236f40	5	① Up
~	aviatrix-Aviatrix-Filter-Gateway	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-050e01b8079e	5	① Up
~	accounting-aws-spoke-dev-Private-2-us-east-1b-rtb	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-00c7046b5712	5	① Up
~	accounting-aws-spoke-dev-Public-2-us-east-1b-rtb	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-0978035b14e6	5	① Up
~	accounting-aws-spoke-prod-Private-1-us-east-1a-rtb	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-04af5a7543e7c	5	① Up
~	accounting-aws-spoke-prod-Private-2-us-east-1b-rtb	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-00168625453f0	5	① Up
~	aviatrix-accounting-aws-spoke-prod	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-0735497e6a50	2	① Up
~	accounting-aws-spoke-prod-Public-2-us-east-1b-rtb	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-0ecdae864f259	5	① Up



Aviatrix Smart Group



An Aviatrix Smart Group identifies a group of resources with similar policy requirements confined in the same logical container.

- The members of a Smart Group can be classified using *three* methods:
 - CSP Tags (or labels)
 - 2. Resource Attributes
 - 3. CIDR









Classification Methods



CSP Tags (recommended)

- Tags are assigned to:
 - Instance
 - VPC/VNET
 - Subnet
- Tags are {Key, Value} pairs
- Example: A shopping cart app can be tagged with:

{Key: Env, Value: Staging}

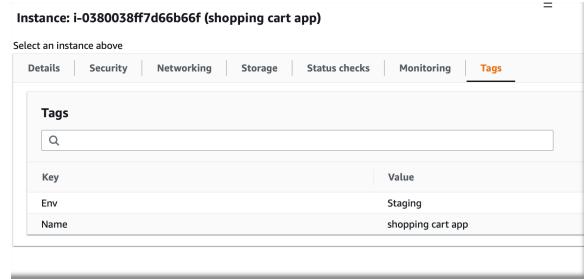
{Key: Name, Value: Shopping cart app}

Resource attribute

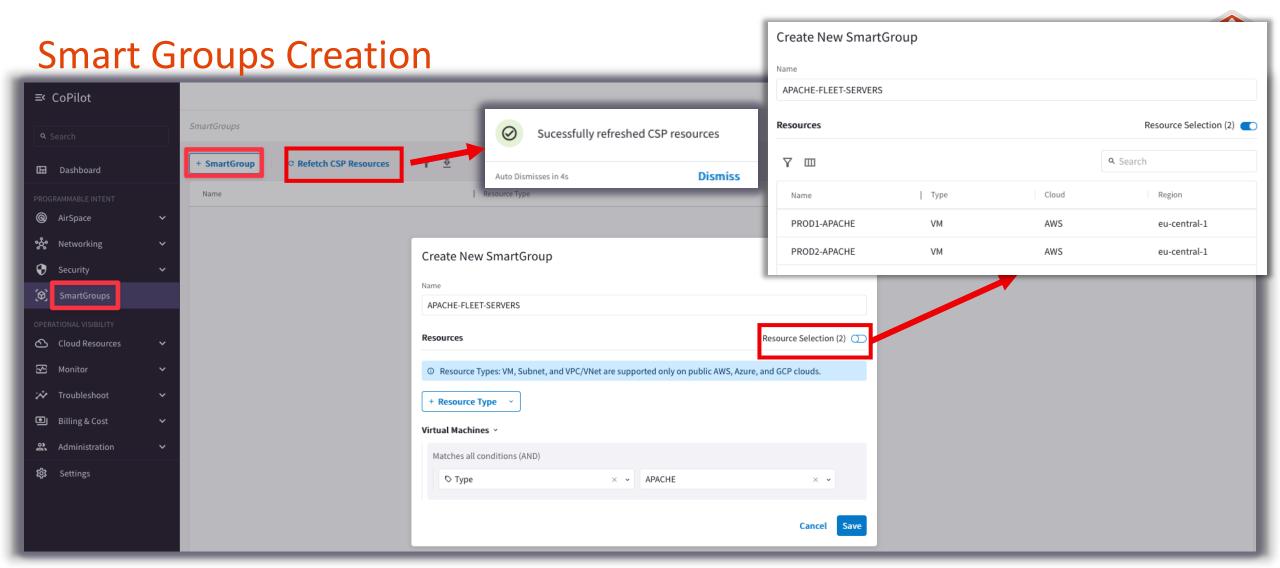
Region Name, Account Name

IP Prefixes

CIDR







- The controller polls the CSPs to retrieve inventory (about VPCs, instances, etc.) every **15 minutes** (can be modified)
- CoPilot queries Controller every 1 hour (can be modified)
- On-demand refresh of tags is available



Pre-defined Smart Groups





- Anywhere → Contains 0.0.0/0 CIDR (One member)
- Public Internet → Contains Internet CIDRs (total of 31 members)



"Public Internet" SmartGroups Members (31 CIDRS Members)



Туре	SmartGroups	IP/CIDRs
CIDR	Public Internet	0.0.0.0/5
CIDR	Public Internet	8.0.0.0/7
CIDR	Public Internet	11.0.0.0/8
CIDR	Public Internet	12.0.0.0/6
CIDR	Public Internet	16.0.0.0/4
CIDR	Public Internet	32.0.0.0/3
CIDR	Public Internet	64.0.0.0/2
CIDR	Public Internet	128.0.0.0/3
CIDR	Public Internet	160.0.0.0/5
CIDR	Public Internet	168.0.0.0/6
CIDR	Public Internet	172.0.0.0/12
Total 31 Destination Entities	5	

Туре	I	SmartGroups	IP/CIDRs
CIDR		Public Internet	172.0.0.0/12
CIDR		Public Internet	172.32.0.0/11
CIDR		Public Internet	172.64.0.0/10
CIDR		Public Internet	172.128.0.0/9
CIDR		Public Internet	173.0.0.0/8
CIDR		Public Internet	174.0.0.0/7
CIDR		Public Internet	176.0.0.0/4
CIDR		Public Internet	192.0.0.0/9
CIDR		Public Internet	192.128.0.0/11
CIDR		Public Internet	192.160.0.0/13
CIDR		Public Internet	192.169.0.0/16
Total 31 Destination Entition	es		

,		
Туре	SmartGroups	IP/CIDRs
CIDR	Public Internet	192.169.0.0/16
CIDR	Public Internet	192.170.0.0/15
CIDR	Public Internet	192.172.0.0/14
CIDR	Public Internet	192.176.0.0/12
CIDR	Public Internet	192.192.0.0/10
CIDR	Public Internet	193.0.0.0/8
CIDR	Public Internet	194.0.0.0/7
CIDR	Public Internet	196.0.0.0/6
CIDR	Public Internet	200.0.0.0/5
CIDR	Public Internet	208.0.0.0/4
CIDR	Public Internet	224.0.0.0/3
Total 31 Destination Enti	ities	



"Anywhere" SmartGroups Members (1 CIDR Member behind the scene)



Туре	I	SmartGroups	IP/CIDRs
CIDR		Anywhere (0.0.0.0/0)	0.0.0.0/0
Total 1 Destination Entity			
Total 1 Destination Entity			



Asset Inventory with SmartGroups



Cloud Assets Virtual Machines	VPC/VNets & Subnets					
Actions Y III 4						
□ Name ↑ □ ac-metro-equinix-nost-vm-1	Cloud	Region us-west1	IP Address 10.50.25, + 1 more	CSP Tags	Aviatrix Managed	SmartGroups
dc-metro-equinix-test-vm	GCP	us-west1	10.50.25, + 1 more		No	
☐ engineering-app-dev	AWS	us-east-2	10.5.2.10	Department: e , + 8 more	Yes	Dev, dev
engineering-app-prod	AWS	us-east-2	10.5.4.10	Department: e , + 8 more	Yes	prod
engineering-app-qa	AWS	us-east-2	10.5.3.10	Division: Soluti, +8 more	Yes	qa
□ enterprise-data-dev	GCP	us-west1	10.4.2.10	environment: d, + 8 more	No	dev-data
□ enterprise-data-gcp-spok	GCP	us-west1	10.4.2.2, + 1 more		Gateways	
□ enterprise-data-gcp-spok	GCP	us-west1	10.4.4.2, + 1 more		Gateways	
□ enterprise-data-gcp-spok	GCP	us-west1	10.4.3.2, + 1 more		Gateways	
□ enterprise-data-prod	GCP	us-west1	10.4.4.10	infrastructure: , + 8 more	No	prod-data
□ enterprise-data-qa	GCP	us-west1	10.4.3.10	terraform: true, +8 more	No	qa-data
	CCD		10 4 2 10	damanturantu FF 1 Curana	N I _	





