



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



☰ CoPilot

🔍 Search

🏠 Dashboard

☁️ Cloud Fabric ▾

🌐 Networking ▾

🛡️ Security ▾

📁 SmartGroups

☁️ Cloud Resources ▴

Cloud Account

Cloud Assets

📊 Monitor ▴

FlowIQ

Performance

Cloud Account

+ Cloud Account

⚙️ Audit Settings



Account Name	Cloud ↑	Account Num...	RBAC Group	Audit Status
accounting-aws	AWS	89433732...	admin, + 1 more	● Warning
aws_admin	AWS	66785746...	admin, + 1 more	● Warning
engineering-aws	AWS	88465792...	admin, + 1 more	● Warning
operations-aws	AWS	66785746...	admin, + 1 more	● Warning
marketing-azure	Azure ARM	c6fd7442-...	admin, + 1 more	● Pass
operations-azure	Azure ARM	cb4b4bc0...	admin, + 1 more	● Pass
enterprise-data-gcp	GCP	aviatrix-d...	admin, + 1 more	● Pass
operations-gcp	GCP	aviatrix-d...	admin, + 1 more	● Pass
operations-oci	OCI	ocid1.ten...	admin, + 1 more	● Pass

CSP Assets Inventory



Search

Dashboard

Cloud Fabric

Networking

Security

SmartGroups

Cloud Resources

Cloud Account

Cloud Assets

Monitor

FlowIQ

Performance

Traffic & Latencies

Notifications

Cloud Assets

Virtual Machines

VPC/VNets & Subnets

Actions

<input type="checkbox"/> Name ↑	Cloud	Region	IP Address	CSP Tags	Aviatrix Managed
<input type="checkbox"/> accounting-app-dev	AWS	us-east-1	10.1.2.10	Environment: dev, + 8 more	Yes
<input type="checkbox"/> accounting-app-prod	AWS	us-east-1	10.1.4.10	Environment: p..., + 8 more	Yes
<input type="checkbox"/> accounting-app-qa	AWS	us-east-1	10.1.3.10	Repository: avi... , + 8 more	Yes
<input type="checkbox"/> av-gw-marketing-azure-s...	Azure ARM	northeur...	10.2.2.4, + 1 more	Aviatrix-Create... , + 3 more	Gateways
<input type="checkbox"/> av-gw-operations-oci-spo...	OCI	ap-singap...	10.3.2.51, + 1 more	Aviatrix-Create... , + 3 more	Gateways
<input type="checkbox"/> av-gw-transit-azure-north...	Azure ARM	northeur...	10.2.0.36, + 1 more	Name: Aviatrix-... , + 3 more	Gateways
<input type="checkbox"/> av-gw-transit-oci-ap-sing...	OCI	ap-singap...	10.3.0.13, + 1 more	Aviatrix-Create... , + 3 more	Gateways
<input type="checkbox"/> aviatrix-accounting-aws-...	AWS	us-east-1	10.1.2.97, + 1 more	Name: aviatrix-... , + 4 more	Gateways
<input type="checkbox"/> aviatrix-accounting-aws-s...	AWS	us-east-1	10.1.2.39, + 1 more	Aviatrix-Create... , + 4 more	Gateways
<input type="checkbox"/> aviatrix-accounting-aws-s...	AWS	us-east-1	10.1.4.43, + 1 more	Type: gateway, + 4 more	Gateways
<input type="checkbox"/> aviatrix-accounting-aws-s...	AWS	us-east-1	10.1.3.45, + 1 more	Controller: 54.1..., + 4 more	Gateways

CSP Assets Inventory



Search

Dashboard

Cloud Fabric

Networking

Security

SmartGroups

Cloud Resources

Cloud Account

Cloud Assets

Monitor

Diagnostics

Billing & Cost

Administration

Settings

Cloud Assets

Virtual Machines

VPC/VNets & Subnets

+ VPC/VNet

Actions

Filter

Grid

Download

<input type="checkbox"/> Name ↑	Cloud	Region	IP Address CIDR	CSP Tags	Aviatrix Managed
<div>▼</div> <input type="checkbox"/> AviatrixVPC	AWS	us-east-1	172.16.0.0/16	aws:cloudformation:logical-id: AviatrixVPC, + 4 more	No
<div>▼</div> <input type="checkbox"/> aws-s2c	AWS	us-east-1	10.150.0.0/24	Aviatrix-Created-Resource: Do-Not-Delete-A..., + 1 more	Yes
<div>▼</div> <input type="checkbox"/> azure-s2c	AWS	us-east-1	172.16.0.0/16	Name: azure-s2c, + 1 more	Yes
<div>▼</div> <input type="checkbox"/> spoke-aws-dev	AWS	us-east-1	10.1.2.0/24	Name: spoke-aws-dev, + 1 more	Yes
<div>▼</div> <input type="checkbox"/> spoke-aws-prod	AWS	us-east-1	10.1.3.0/24	Aviatrix-Created-Resource: Do-Not-Delete-A..., + 1 more	Yes
<div>▼</div> <input type="checkbox"/> spoke-azure-all	Azure ARM	westus3	10.2.2.0/24	Aviatrix-Created-Resource: Do-Not-Delete-A..., + 1 more	Yes
<div>▼</div> <input type="checkbox"/> spoke-gcp-dev	GCP				Yes
<div>▼</div> <input type="checkbox"/> spoke-gcp-prod	GCP				Yes
<div>▼</div> <input type="checkbox"/> transit-aws	AWS	us-east-1	10.1.0.0/23	Name: transit-aws, + 1 more	Yes
<div>▼</div> <input type="checkbox"/> transit-azure	Azure ARM	westus3	10.2.0.0/23	Name: transit-azure, + 1 more	Yes
<div>▼</div> <input type="checkbox"/> transit-gcp	GCP				Yes
<div>▼</div> <input type="checkbox"/> vpc-004aa48d53ffb464	AWS	ap-southeast-1	172.31.0.0/16		No
<div>▼</div> <input type="checkbox"/> vpc-03f8740191d7713ce	AWS	sa-east-1	172.31.0.0/16		No
<div>▼</div> <input type="checkbox"/> vpc-09731efe081d0fd13	AWS	ap-northeast-3	172.31.0.0/16		No

←

GCP labels (tags) are NOT available for VPC or VPC Network

←

Default AWS VPC without tag

GCP labels (tags) are NOT available for VPC or VPC Network

Default AWS VPC without tag

Global Routing Inventory – Aviatrix Gateway



<div> Cloud Routes Gateway Routes VPC/VNet Routes External Connections BGP Info </div>						
<div> Filter Grid Download </div>						
Gateway	VPC/VNet	Gateway Status	Tunnel Status	Tunnels	Routes	
accounting-aws-psf-dev	accounting-aws-spoke-dev (10.1.2.0/24)	⊕ Up	⊕ Up	0	5	
accounting-aws-spoke-dev	accounting-aws-spoke-dev (10.1.2.0/24)	⊕ Up	⊕ Up	1	7	
accounting-aws-spoke-prod	accounting-aws-spoke-prod (10.1.4.0/24)	⊕ Up	⊕ Up	1	7	
accounting-aws-spoke-qa	accounting-aws-spoke-qa (10.1.3.0/24)	⊕ Up	⊕ Up	1	7	
engineering-aws-spoke-dev	engineering-aws-spoke-dev (10.5.2.0/24)	⊕ Up	⊕ Up	1	7	
engineering-aws-spoke-dev-vpn	engineering-aws-spoke-dev (10.5.2.0/24)	⊕ Up	⊕ Up	0	7	
engineering-aws-spoke-prod	engineering-aws-spoke-prod (10.5.4.0/24)	⊕ Up	⊕ Up	1	7	
enterprise-data-gcp-spoke-dev	enterprise-data-gcp-spoke-dev (10.4.2.0/24)	⊕ Up	⊕ Up	1	5	
engineering-aws-spoke-qa	engineering-aws-spoke-qa (10.5.3.0/24)	⊕ Up	⊕ Up	1	7	
enterprise-data-gcp-spoke-prod	enterprise-data-gcp-spoke-prod (10.4.4.0/24)	⊕ Up	⊕ Up	1	5	
enterprise-data-gcp-spoke-qa	enterprise-data-gcp-spoke-qa (10.4.3.0/24)	⊕ Up	⊕ Up	1	5	

Global Routing Inventory – Cloud Routes



Cloud Routes

Gateway Routes

VPC/VNet Routes

External Connections

BGP Info



▼ Name	VPC/VNet ↑	Route Table ID	Routes
▼ aviatrix-accounting-aws-spoke-dev	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-0f989b2b17ead...	2 Up
▼ aviatrix-Aviatrix-Ingress-routing	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-06c99baa2682...	3 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 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 Up
▼ aviatrix-Aviatrix-Filter-Gateway	accounting-aws-spoke-dev(vpc-06ca01b0b6488e435) (10.1.2.0/24)	rtb-050e01b8079e...	5 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 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 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 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 Up
▼ aviatrix-accounting-aws-spoke-prod	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-0735497e6a50...	2 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 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:
 1. 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

Instance: i-0380038ff7d66b66f (shopping cart app)

Select an instance above

Details | Security | Networking | Storage | Status checks | Monitoring | **Tags**

Tags



Key

Value

Env

Staging

Name

shopping cart app

Smart Groups Creation

The screenshot illustrates the process of creating a SmartGroup in the Aviatrix CoPilot interface. The left sidebar contains a navigation menu with the following items: CoPilot, Search, Dashboard, Programmable Intent (AirSpace, Networking, Security, SmartGroups), and Operational Visibility (Cloud Resources, Monitor, Troubleshoot, Billing & Cost, Administration, Settings). The 'SmartGroups' option is highlighted with a red box. The main panel shows the 'SmartGroups' section with two buttons: '+ SmartGroup' and 'Refresh CSP Resources', both highlighted with red boxes. A red arrow points from the 'Refresh CSP Resources' button to a notification banner that reads 'Sucessfully refreshed CSP resources' (note the typo). Another red arrow points from the 'Resource Selection (2)' toggle in the 'Create New SmartGroup' modal to a detailed view of the selected resources.

Create New SmartGroup

Name: APACHE-FLEET-SERVERS

Resources: Resource Selection (2) ☒

Name	Type	Cloud	Region
PROD1-APACHE	VM	AWS	eu-central-1
PROD2-APACHE	VM	AWS	eu-central-1

Create New SmartGroup

Name: APACHE-FLEET-SERVERS

Resources: Resource Selection (2) ☒

ⓘ Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.

+ Resource Type

Virtual Machines

Matches all conditions (AND)




Type APACHE

Cancel Save

- 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

SmartGroups

[+ SmartGroup](#) | [Refresh CSP Resources](#) |   | 

Name	Resource Type
Anywhere (0.0.0.0/0)	
Public Internet	

- **Anywhere** → Contains 0.0.0.0/0 CIDR (One member)
- **Public Internet** → Contains Internet CIDRs (total of 31 members)

“Public Internet” SmartGroups Members (31 CIDRS Members)

Type	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		

Type	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 Entities		

Type	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 Entities		

“Anywhere” SmartGroups Members (1 CIDR Member behind the scene)

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

Asset Inventory with SmartGroups



Cloud Assets							
Virtual Machines							
VPC/VNets & Subnets							
Actions ▼ 🔍 📄 ⬇️							
<input type="checkbox"/> Name ↑	Cloud	Region	IP Address	CSP Tags	Aviatrix Managed	SmartGroups	
<input type="checkbox"/> dc-metro-equinix-nost-vm-1	GCP	us-west1	10.50.25... , + 1 more		No		
<input type="checkbox"/> dc-metro-equinix-test-vm	GCP	us-west1	10.50.25... , + 1 more		No		
<input type="checkbox"/> engineering-app-dev	AWS	us-east-2	10.5.2.10	Department: e... , + 8 more	Yes	Dev, dev	
<input type="checkbox"/> engineering-app-prod	AWS	us-east-2	10.5.4.10	Department: e... , + 8 more	Yes	prod	
<input type="checkbox"/> engineering-app-qa	AWS	us-east-2	10.5.3.10	Division: Soluti... , + 8 more	Yes	qa	
<input type="checkbox"/> enterprise-data-dev	GCP	us-west1	10.4.2.10	environment: d... , + 8 more	No	dev-data	
<input type="checkbox"/> enterprise-data-gcp-spok...	GCP	us-west1	10.4.2.2, + 1 more		Gateways		
<input type="checkbox"/> enterprise-data-gcp-spok...	GCP	us-west1	10.4.4.2, + 1 more		Gateways		
<input type="checkbox"/> enterprise-data-gcp-spok...	GCP	us-west1	10.4.3.2, + 1 more		Gateways		
<input type="checkbox"/> enterprise-data-prod	GCP	us-west1	10.4.4.10	infrastructure: ... , + 8 more	No	prod-data	
<input type="checkbox"/> enterprise-data-qa	GCP	us-west1	10.4.3.10	terraform: true, + 8 more	No	qa-data	
<input type="checkbox"/> enterprise-data-qa	GCP	us-west1	10.4.3.10	department: 55... , + 6 more	No		



Aviatrix Certified Engineer (ACE)
<https://aviatrix.com/ACE>



COMMUNITY
<https://community.aviatrix.com>