



## 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
- Kubernetes Clusters discovery
- Resource Grouping using Aviatrix SmartGroups

## Use Cases:

Zero Trust Network Access  
(Cloud Firewalling)

Secure B2B  
Connectivity

Secure High-Performance Data  
Connectivity for LLMS

Secure High-Performance  
Datacenter Edge

Cloud Visibility and  
Tooling

# CSP Cloud Accounts Inventory



☰ CoPilot

🔍 Search

🏠 Dashboard

☁️ Cloud Fabric ▾

🌐 Networking ▾

🛡️ Security ▾

👤 Groups

☁️ Cloud Resources ▴

Cloud Account

☁️ Cloud Assets

📊 Monitor ▾

🔧 Diagnostics ▾

💰 Billing & Cost ▾

👤 Administration ▾

⚙️ Settings ▾

Cloud Account

+ Cloud Account

Actions ▾

⚙️ Audit Settings

🔍

⬇️

<input type="checkbox"/> Account Name	Cloud	Account Number / ID	RBAC Group	Audit Status
<input type="checkbox"/> <a href="#">accounting-aws</a>	AWS	894337324417	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">aws_admin</a>	AWS	667857464789	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">engineering-aws</a>	AWS	884657925782	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">enterprise-data-gcp</a>	GCP	aviatrix-demo-dev	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">marketing-azure</a>	Azure ARM	c6fd7442-2813-4056-ae02-c029a4263885	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">operations-aws</a>	AWS	667857464789	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">operations-azure</a>	Azure ARM	cb4b4bc0-a245-42e1-8381-f602ca428232	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">operations-gcp</a>	GCP	aviatrix-demo-stg	admin, <a href="#">+ 3 more</a>	✔️ Pass
<input type="checkbox"/> <a href="#">operations-oci</a>	OCI	ocid1.tenancy.oc1..aaaaaaaawgcwwwxnmuhnjezj	admin, <a href="#">+ 3 more</a>	✔️ Pass

# CSP Assets Inventory



☰ CoPilot

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Cloud Account

Cloud Assets

Monitor

Diagnostics

Billing & Cost

Administration

Settings

Cloud Assets

**Virtual Machines**

VPC/VNets & Subnets

Actions

Filter

Grid

Download

<input type="checkbox"/> Name ↑	Cloud ↑	Region	IP Address	Tags
<input type="checkbox"/> aviatrix-accounting-aws-psf-dev	AWS	us-east-1	10.1.2.97, <a href="#">+ 1 more</a>	Name: aviatrix-accountin... , <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-accounting-aws-spoke-dev	AWS	us-east-1	10.1.2.37, <a href="#">+ 1 more</a>	Controller: 54.148.104.116, <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-accounting-aws-spoke-prod	AWS	us-east-1	10.1.4.43, <a href="#">+ 1 more</a>	HA: False, <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-accounting-aws-spoke-qa	AWS	us-east-1	10.1.3.45, <a href="#">+ 1 more</a>	Name: aviatrix-accountin... , <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-engineering-aws-spoke-dev	AWS	us-east-2	10.5.2.143, <a href="#">+ 6 more</a>	H... , Name: aviatrix-engi... , <a href="#">+ 3 more</a>
<input type="checkbox"/> aviatrix-engineering-aws-spoke-dev-vpn	AWS	us-east-2	10.5.2.42, <a href="#">+ 1 more</a>	Controller: 54.148.104.116, <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-engineering-aws-spoke-prod	AWS	us-east-2	10.5.4.140, <a href="#">+ 6 more</a>	Name: aviatrix-engineerin..., <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-engineering-aws-spoke-qa	AWS	us-east-2	10.5.3.152, <a href="#">+ 6 more</a>	Type: gateway, <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-operations-aws-spoke-landing-zone	AWS	us-east-1	10.7.2.44, <a href="#">+ 1 more</a>	Type: gateway, <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-sampe	AWS	us-east-2	172.31.1..., <a href="#">+ 1 more</a>	Name: aviatrix-sampe, <a href="#">+ 4 more</a>
<input type="checkbox"/> aviatrix-Test-Spoke-GW	AWS	us-east-1	10.101.1..., <a href="#">+ 1 more</a>	Aviatrix-Created-Resource..., <a href="#">+ 4 more</a>

# CSP Assets Inventory



☰ CoPilot

🔍 Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Cloud Account

Cloud Assets

Monitor

Diagnostics

Billing & Cost

Administration

Settings

Cloud AssetsVirtual MachinesVPC/VNets & Subnets

+ VPC/VNet

Actions

🔍 1

📄

⬇️

▼ <input type="checkbox"/>	Name	Cloud <input type="text"/>	Region	IP Address CIDR	VMs	Cloud Tags
▼ <input type="checkbox"/>	operations-oci-spoke-shared	OCI	ap-singap...	10.3.2.0/24	operations-...	+ 2 more
▼ <input type="checkbox"/>	vpc-0973731e7edccad8e	AWS	ap-south...	172.31.0.0/16		
▼ <input type="checkbox"/>	vpc-035a29b19cf1c35c3	AWS	ap-northe...	172.31.0.0/16		
▼ <input type="checkbox"/>	vpc-083207269810ef3c9	AWS	ap-south-1	172.31.0.0/16		
▼ <input type="checkbox"/>	vpc-0dbeaedadec8302dd	AWS	ap-northe...	172.31.0.0/16		
▼ <input type="checkbox"/>	vpc-0b3fedb4a46af12f3	AWS	ap-south-1	172.31.0.0/16		
▼ <input type="checkbox"/>	engineering-aws-spoke-dev	AWS	us-east-2	10.5.2.0/24	engineering-web-dev	Aviatrix-Cre... , + 1 more
▼ <input type="checkbox"/>	example-gcp-spoke-vpc	GCP				
▼ <input type="checkbox"/>	lv-metro-megaport-vpc	GCP				
▼ <input type="checkbox"/>	engineering-aws-spoke-prod	AWS	us-east-2	10.5.4.0/24	engineering-app-prod	Aviatrix-Cre... , + 1 more
▼ <input type="checkbox"/>	vpc-008989747c199f28d	AWS	eu-west-1	172.31.0.0/16		

Default AWS VPC without tag

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

# Kubernetes Assets Inventory



CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Cloud Account

Cloud Assets

Monitor

Diagnostics

Cloud Assets Virtual Machines VPC/VNets & Subnets **Kubernetes Clusters**

⚠ Kubernetes is in Preview. Preview features are not safe for deployment in production environments.

ⓘ Only publicly accessible Kubernetes Clusters are supported. Clusters with Overlay Networks have limited support for Distributed Cloud Firewall.

Manually Onboard Cluster

Filter Grid Download Help

Search

Name	Cloud Account	VPC/VNets	Namespaces	Services	Pods	Onboarded
shared-north-europe-aks-cluster	operations-azure	operations-azure-spoke-k8s	7	8	18	✔ Yes
shared-us-east-1-eks	operations-aws	vpc-03bca47bf62b22bf3	7	7	8	✔ Yes

# Global Routing Inventory (i.e Cloud Routes): Aviatrix Gateways' RTBs

Cloud Routes

Gateway Routes

VPC/VNet Routes

External Connections

BGP Info

More Specific Routes injected by the Controller

Gateway	VPC/VNet	Gateway Status	Tunnel Status	Tunnels	Routes		
accounting-aws-psf-dev	accounting-aws-spoke-dev (10.1.2.0/24)	Up	Unknown	0	4		
accounting-aws-spoke-dev	accounting-aws-spoke-dev (10.1.2.0/24)	Up	Up	1	7		
ROUTE	SOURCE	INTERFACE	VIA	NEXT HOP IP	NEXT HOP GATEWAY	METRIC	
default, 10.1.2.2/32	10.1.2.37	eth0 (INF2)	10.1.2.33	10.1.2.33		100	
default		eth0 (INF2)	10.1.2.33	10.1.2.33		400	
10.1.0.13/32	10.1.2.37	tun-2CCD3F57-0 (INF9)		44.205.63.87	transit-aws-us-east-1	0	
10.1.2.0/24		eth0 (INF2)	10.1.2.33	10.1.2.33		0	
10.1.2.32/28, 10.1.2.33/32	10.1.2.37	eth0 (INF2)				100	
10.2.2.0/24, 10.3.2.0/24, + 230 more	10.1.2.37	tun-2CCD3F57-0 (INF9)		44.205.63.87	transit-aws-us-east-1	100	
accounting-aws-spoke-prod	accounting-aws-spoke-prod (10.1.4.0/24)	Up	Up	1	7		

# Global Routing Inventory (i.e Cloud Routes): CSPs' Routers RTBs

Cloud Routes Gateway Routes <b>VPC/VNet Routes</b> External Connections BGP Info			
<div> <div> <div></div> <div></div> <div></div> </div> <div> <div></div> <div></div> <div></div> </div> </div>			
^ Name	VPC/VN		
^ accounting-aws-spoke-prod-Private-1-us-east-1a-rtb	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-04af5a7543e7c5a38	5
ROUTE	GATEWAY	TARGET	
10.1.4.0/24	local	local	
192.168.0.0/16	aviatrix-accounting-aws-spoke-prod	i-0abc894bf28fd199c	
172.16.0.0/12	aviatrix-accounting-aws-spoke-prod	i-0abc894bf28fd199c	
10.0.0.0/8	aviatrix-accounting-aws-spoke-prod	i-0abc894bf28fd199c	
0.0.0.0/0	aviatrix-accounting-aws-spoke-prod	i-0abc894bf28fd199c	
^ accounting-aws-spoke-prod-Private-2-us-east-1b-rtb	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-00168625453f0490a	5
^ aviatrix-accounting-aws-spoke-prod	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-0735497e6a502311c	2
^ accounting-aws-spoke-prod-Public-2-us-east-1b-rtb	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-0ecdae864f2592abd	5
^ accounting-aws-spoke-prod-Public-1-us-east-1a-rtb	accounting-aws-spoke-prod(vpc-0048eff309de2a237) (10.1.4.0/24)	rtb-0951896b8db8489b2	5

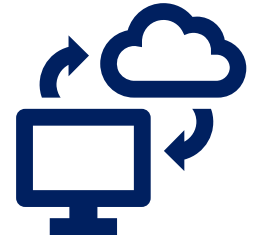
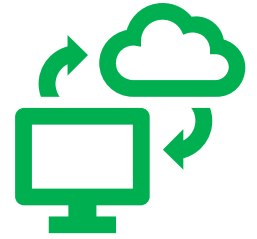
Summary Routes (rfc1918 routes), local cidr, default route... injected by the Controller



# 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 SmartGroup can be classified using *different* methods:
  - CSP Tag
  - Subnets
  - VPC/Vnets
  - Kubernetes
  - Hostnames
  - External Connections (S2C)



# 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



**CoPilot**

Search

Dashboard

Cloud Fabric

Networking

Security

**Groups**

Cloud Resources

Monitor

Diagnostics

Billing & Cost

Administration

Settings

Groups SmartGroups WebGroups Settings

+ SmartGroup

Refetch CSP Resources

Name

Anywhere (0.0.0.0/0)

Public Internet

Create SmartGroup

Name

APACHE

Resource Selection

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

Preview (3)

Create New SmartGroup

Name

APACHE

Resources

Resource Selection (3)

Name	Type	Cloud	Region
PROD1-APACHE	VM	AWS	eu-central-1
PROD2-APACHE	VM	AWS	eu-central-1
prod3-apache	VM	Azure ARM	westeurope

Successfully refreshed CSP resources

Auto Dismisses in 4s

Dismiss

- 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

Groups	SmartGroups	WebGroups	Settings
<div> <span>+ SmartGroup</span> <span>⌂ Refetch CSP Resources</span> <span>⌵</span> <span>⬇</span> <span>?</span> </div>			
Name		Resource Type	
Anywhere (0.0.0.0/0)			
Public Internet			

- **Anywhere (0.0.0.0/0)** → RFC1918 routes + Default Route (IGW)
- **Public Internet** → Default Route (IGW)

## “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 <span>▼</span>   <span>🔍</span> <span>📄</span> <span>⬇️</span>							
<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... , <a href="#">+ 1 more</a>		No		
<input type="checkbox"/> dc-metro-equinix-test-vm	GCP	us-west1	10.50.25... , <a href="#">+ 1 more</a>		No		
<input type="checkbox"/> engineering-app-dev	AWS	us-east-2	10.5.2.10	Department: e... , <a href="#">+ 8 more</a>	Yes	Dev, dev	
<input type="checkbox"/> engineering-app-prod	AWS	us-east-2	10.5.4.10	Department: e... , <a href="#">+ 8 more</a>	Yes	prod	
<input type="checkbox"/> engineering-app-qa	AWS	us-east-2	10.5.3.10	Division: Soluti... , <a href="#">+ 8 more</a>	Yes	qa	
<input type="checkbox"/> enterprise-data-dev	GCP	us-west1	10.4.2.10	environment: d... , <a href="#">+ 8 more</a>	No	dev-data	
<input type="checkbox"/> enterprise-data-gcp-spok...	GCP	us-west1	10.4.2.2, <a href="#">+ 1 more</a>		Gateways		
<input type="checkbox"/> enterprise-data-gcp-spok...	GCP	us-west1	10.4.4.2, <a href="#">+ 1 more</a>		Gateways		
<input type="checkbox"/> enterprise-data-gcp-spok...	GCP	us-west1	10.4.3.2, <a href="#">+ 1 more</a>		Gateways		
<input type="checkbox"/> enterprise-data-prod	GCP	us-west1	10.4.4.10	infrastructure: ... , <a href="#">+ 8 more</a>	No	prod-data	
<input type="checkbox"/> enterprise-data-qa	GCP	us-west1	10.4.3.10	terraform: true, <a href="#">+ 8 more</a>	No	qa-data	
<input type="checkbox"/> ...	GCP	us-west1	10.4.3.10	department: EE... , <a href="#">+ 6 more</a>	No		



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



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