



Operational Best Practices

ACE Solutions Architecture Team

CoPilot Syslog Setup (FQDN and Audit data)



- Make sure Logging is enabled on Controller > SETTINGS > Logging > Remote Syslog
 - ❑ Syslog can be exported to up to 9 different servers via Profiles
 - ❑ Make sure to use Profile Index 9 for CoPilot
 - ❑ Edit Options to select a subset of gateways to export
- Make sure, on CSP portal, following port is open on CoPilot instance:
 - ❑ **UDP 5000** (Syslog) – all Gateways

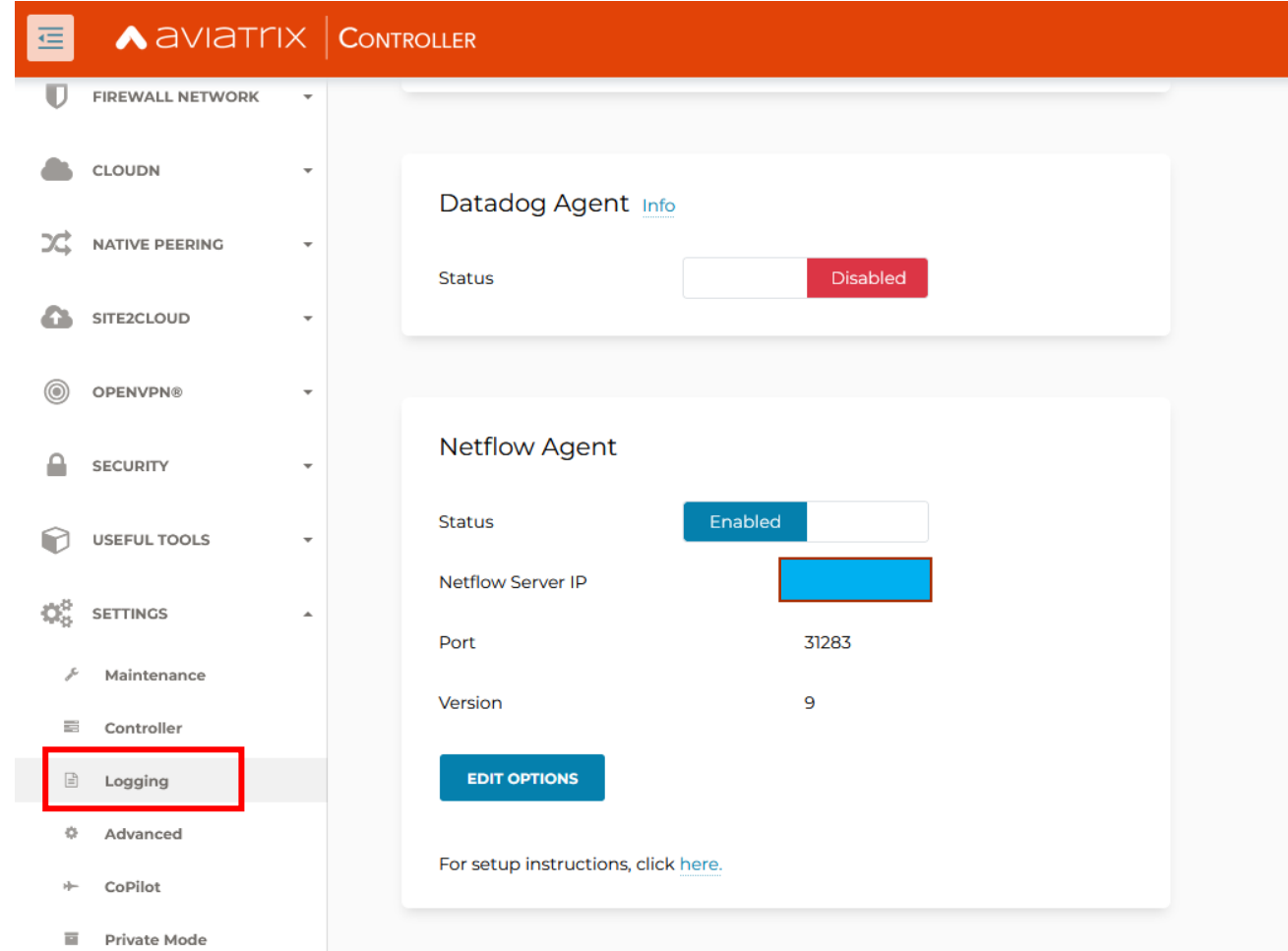
The screenshot shows the Aviatrix Controller web interface. The left sidebar contains a menu with items: FIREWALL NETWORK, CLOUDN, NATIVE PEERING, SITE2CLOUD, OPENVPN®, SECURITY, USEFUL TOOLS, SETTINGS, Maintenance, Controller, **Logging** (highlighted with a red box), Advanced, CoPilot, Private Mode, and User Preference. The main content area is titled 'Remote Syslog' and includes the following configuration details:

- Support up to 10 regional forwarders which can integrate with Splunk, SumoLogic Filebeat and Datadog.
- Enabled Profiles: 0,9
- Profile Index: 0 (dropdown menu)
- Profile Name: Syslog
- Status: Enabled (toggle switch)
- Server: 44.213.0.127
- Port: 5000
- Protocol: UDP
- EDIT OPTIONS button
- For setup instructions, click [here](#).

At the bottom of the main panel, there is a section for 'Datadog Agent' with an 'Info' link.

CoPilot NetFlow Setup (for FlowIQ and ThreatIQ data)

- Make sure NetFlow is enabled on Controller > SETTINGS > Logging > Netflow Agent
 - ❑ If port is changed from default of 31283, it needs to match on CoPilot
 - ❑ Edit Options to select a subset of gateways to export
- Make sure, on CSP portal, following ports are open on CoPilot instance:
 - ❑ UDP 31283 (NetFlow) – all Gateways
 - ❑ TCP 443 (HTTPS) – all clients

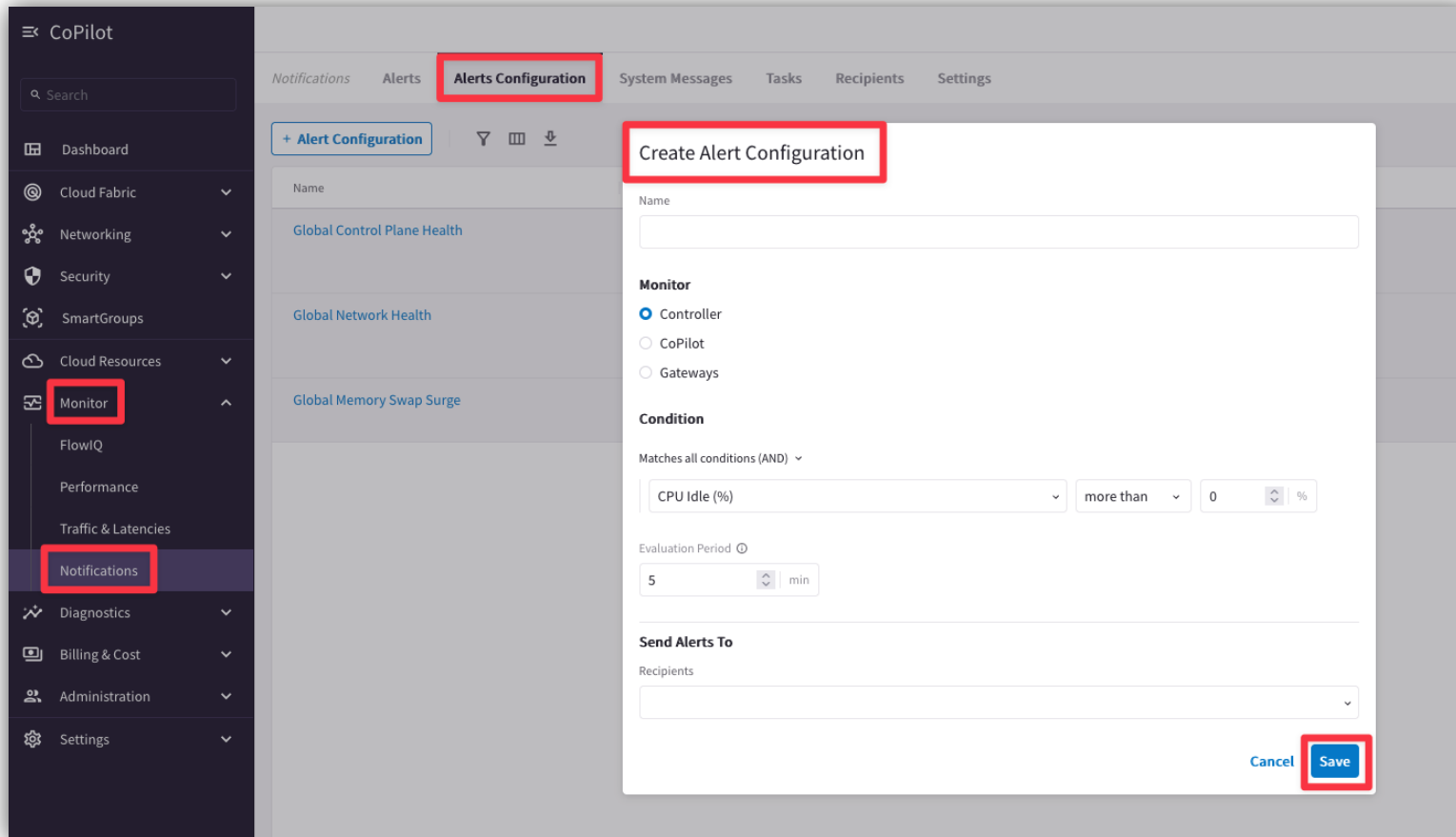


The screenshot shows the Aviatrix Controller interface. The left sidebar contains a menu with the following items: FIREWALL NETWORK, CLOUDN, NATIVE PEERING, SITE2CLOUD, OPENVPN®, SECURITY, USEFUL TOOLS, SETTINGS, Maintenance, Controller, Logging (highlighted with a red box), Advanced, CoPilot, and Private Mode. The main content area displays the 'Datadog Agent' and 'Netflow Agent' settings. The 'Datadog Agent' status is 'Disabled'. The 'Netflow Agent' status is 'Enabled'. The 'Netflow Server IP' field is highlighted with a red box. The 'Port' is set to 31283 and the 'Version' is 9. There is an 'EDIT OPTIONS' button and a link to 'here' for setup instructions.

Agent	Status	Netflow Server IP	Port	Version
Datadog Agent	Disabled			
Netflow Agent	Enabled		31283	9

CoPilot Alerts Configuration

1. Webhooks Integrations work with any 3rd party integration (Slack, PagerDuty, ServiceNow, etc.)
2. Add webhook endpoints (can send payload as JSON or text)
3. Provide custom tags in the payload to classify triggered events and further integrate into your systems
4. Get alerted via webhook and email for the same alert

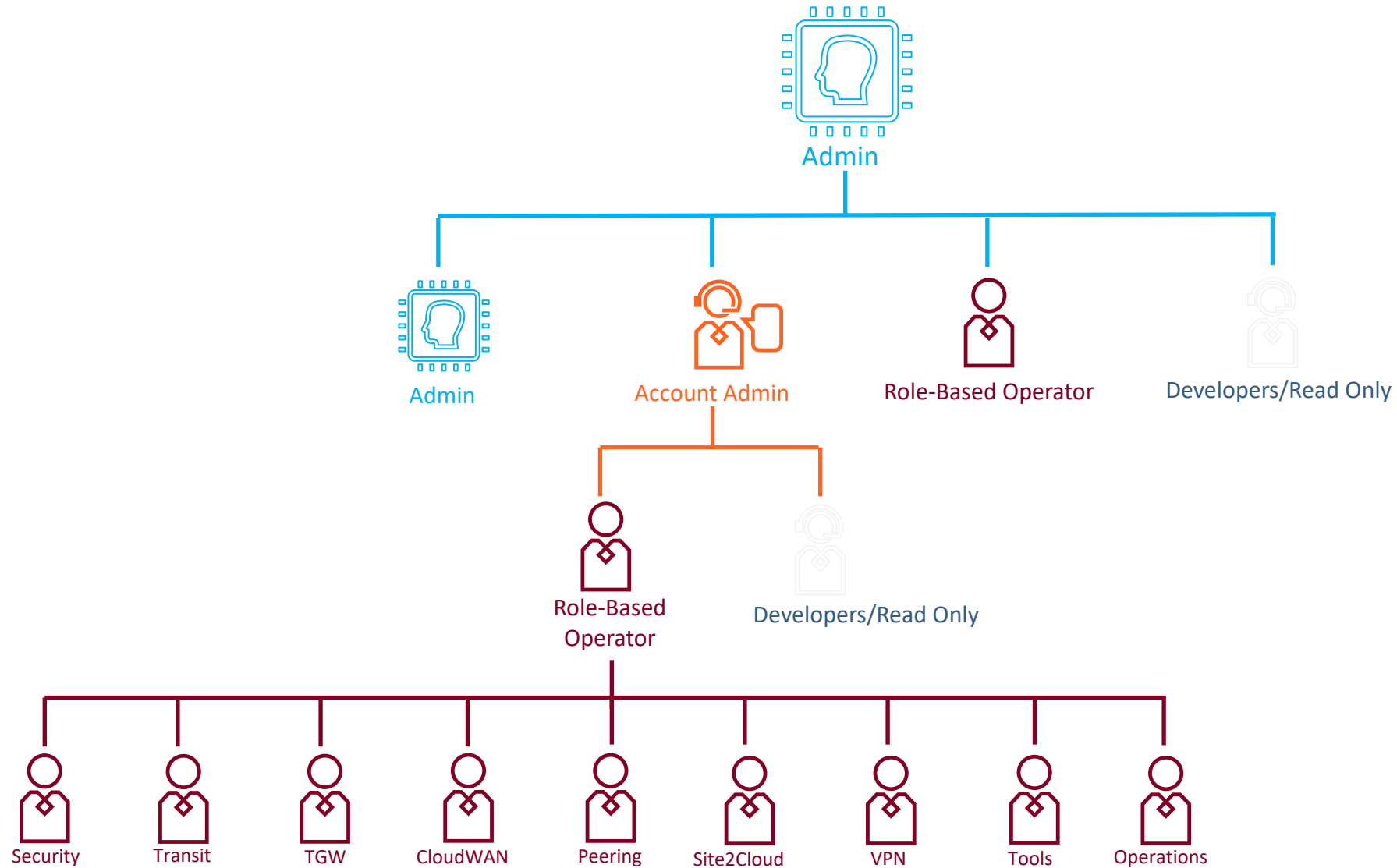


The screenshot shows the CoPilot Alerts Configuration interface. The left sidebar contains a navigation menu with the following items: Dashboard, Cloud Fabric, Networking, Security, SmartGroups, Cloud Resources, Monitor (highlighted with a red box), FlowIQ, Performance, Traffic & Latencies, Notifications (highlighted with a red box), Diagnostics, Billing & Cost, Administration, and Settings. The main content area has a tabbed interface with the following tabs: Notifications, Alerts, Alerts Configuration (highlighted with a red box), System Messages, Tasks, Recipients, and Settings. The Alerts Configuration tab is active, showing a list of alerts: Global Control Plane Health, Global Network Health, and Global Memory Swap Surge. A modal window titled 'Create Alert Configuration' (highlighted with a red box) is open, containing the following fields: Name (text input), Monitor (radio buttons for Controller, CoPilot, and Gateways), Condition (Matches all conditions (AND) dropdown, CPU Idle (%) dropdown, more than dropdown, 0 dropdown, % dropdown), Evaluation Period (5 min), Send Alerts To (Recipients dropdown), and Cancel and Save buttons (the Save button is highlighted with a red box).



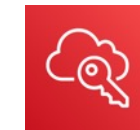
Role-Based Access Control (RBAC)

RBAC: Role-Based Access Control

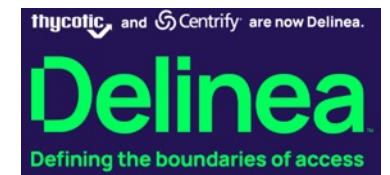


Authentication Phase

- Users can be authenticated:
 - **Locally** on the Aviatrix Controller
 - Onboard Users (Admin, Operators, Developers, Read-Only)
 - Allowed to reset their password
 - Using **SAML IDP**
 - Onboard Users (Admin, Operators, Developers, Read-Only)
 - Other functionality depends on IDP



AWS SSO



User Access- CoPilot



CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

SmartGroups

Cloud Resources

Monitor

Diagnostics

Billing & Cost

Administration

User Access

Reports

Audit

Settings

User Access

Users

Permission Group

Access Management

+ User

Name

Email

Permission Groups

admin	ace.lab@aviatrix.com	admin
copilot_service_account	ace.lab@aviatrix.com	copilot_permission
student	ace.lab@aviatrix.com	admin

Add User

Username

Email

Password

Confirm Password

Permission Groups

Cancel

Save

Permission Sets – CoPilot/Controller



Create Permission Group

Name

Users

Access Accounts

CoPilot Visibility Controller Permissions

[Select All Views](#) [Clear All Views](#)

- ☒ AirSpace
- ☒ Networking
- ☒ Security
- ☒ SmartGroups
- ☒ Cloud Resources
- ☒ Monitor

[Cancel](#) [Save](#)

- ☒ AirSpace
- ☒ Networking
- ☒ Security
- ☒ SmartGroups
- ☒ Cloud Resources
- ☒ Monitor
- ☒ Troubleshoot
- ☒ Billing & Cost
- ☒ Administration
- ☒ Settings

RBAC Example – Okta

 *RBAC User : saad-developer@aviatrix.com*

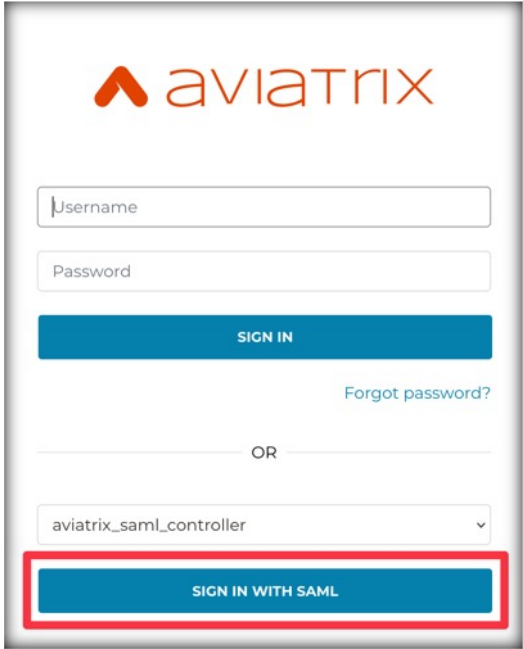
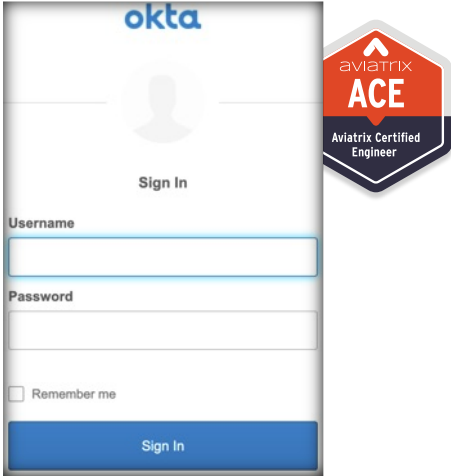
 *RBAC User : saad@aviatrix.com*

 *RBAC User : saad_A-B@aviatrix.com*

 *RBAC User : saad-security@aviatrix.com*

read_only
Super-Users
Account-Admin
Account Admins (A&B)
Account Admins (C&D)
Security-Users

RBAC-User	Permissions
saad-developer	Read Only
saad	Super User (Admin)
saad_A-B	Account Admin for Accounts A&B Only
saad-security	Security User



Admin/Super-Users
Saad



Account Admins
Saad-A&B



Security-Users
Saad-Security



Developers/Read Only
Saad-Developer



Aviatrix Controller High Availability (HA)

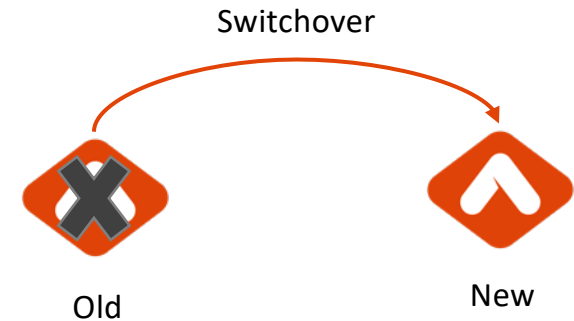
Aviatrix Controller High Availability (HA)

- Very important: Controller is not in the data path
- If Controller is down → Data Plane still functions
- Your cloud network is still up and running
- Do not compare on-prem to cloud
 - Hardware devices cannot be replaced / software is more flexible
 - Cloud operating models are different
 - Cloud processes are different
 - We need a fresh and different look to solve



Aviatrix Controller HA Process

- Takes minutes to switch over to new controller
 - Depends on factors such as AWS latency, instance type, size of the DB, etc.
- Previous controller is terminated
- All existing configuration is restored
- New Private IP is assigned (new AZ)
- New controller stays at the same version as previous

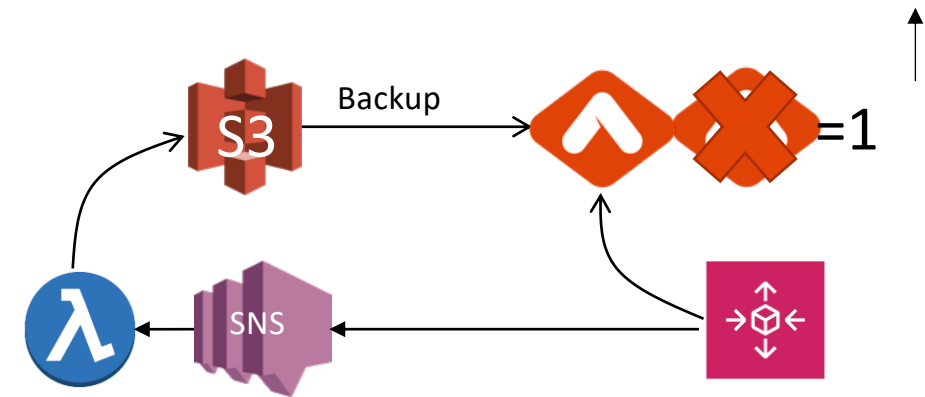


https://docs.aviatrix.com/HowTos/controller_ha.html

<https://github.com/AviatrixSystems/Controller-HA-for-AWS/>

Aviatrix Controller HA Process

- Aviatrix Controller HA operates by relying on an AWS Auto Scaling Group
- The Auto Scaling Group has a desired capacity of 1
- If the Controller EC2 instance is stopped or terminated, it will be automatically re-deployed by the Auto Scaling Group
- An AWS Lambda script is notified via SNS when new instances are launched by the Auto Scaling Group
- This script handles configuration restore using the most recent Controller backup file, stored in S3



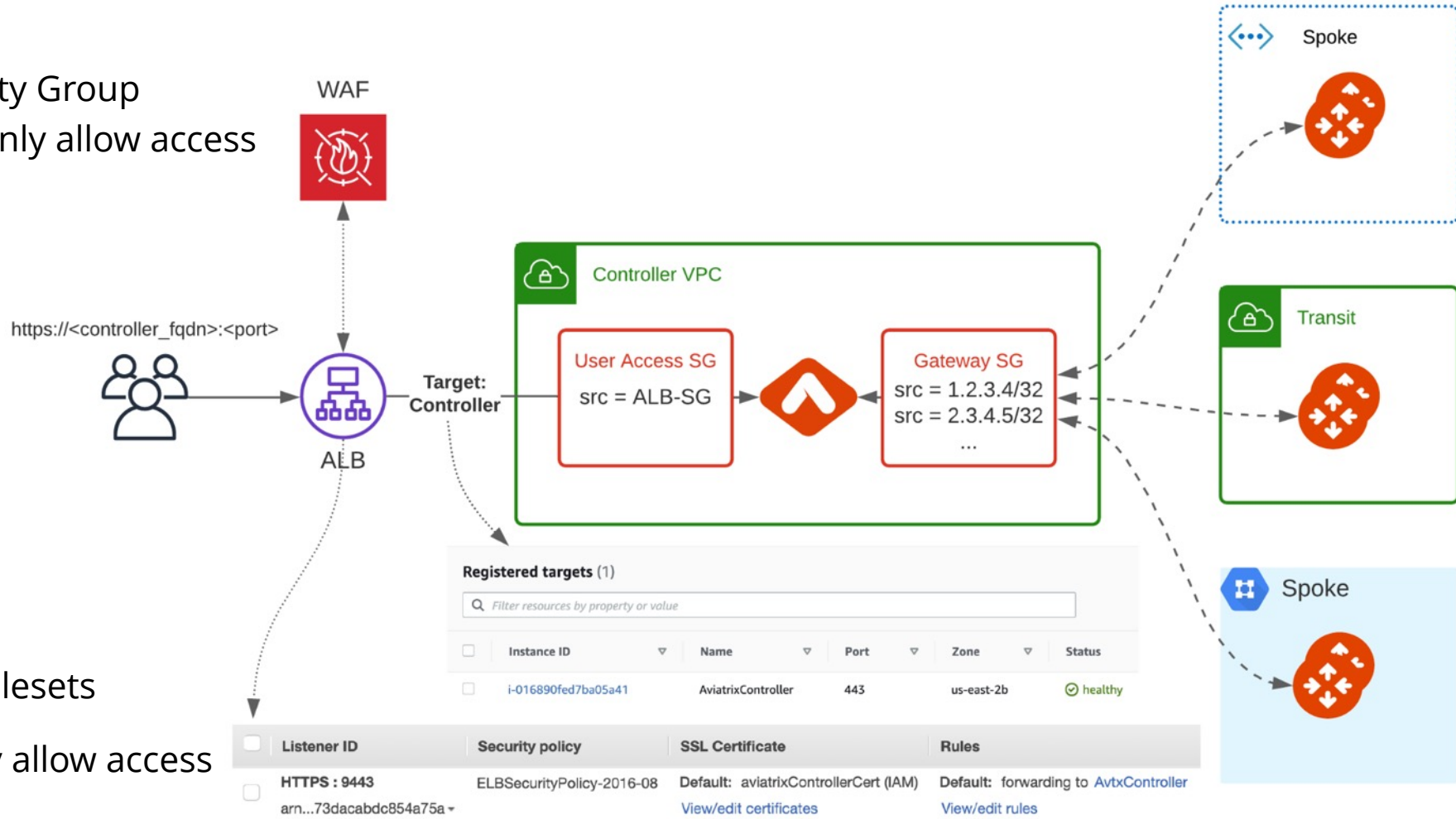


Securing Aviatrix Controller with Application Load Balancer

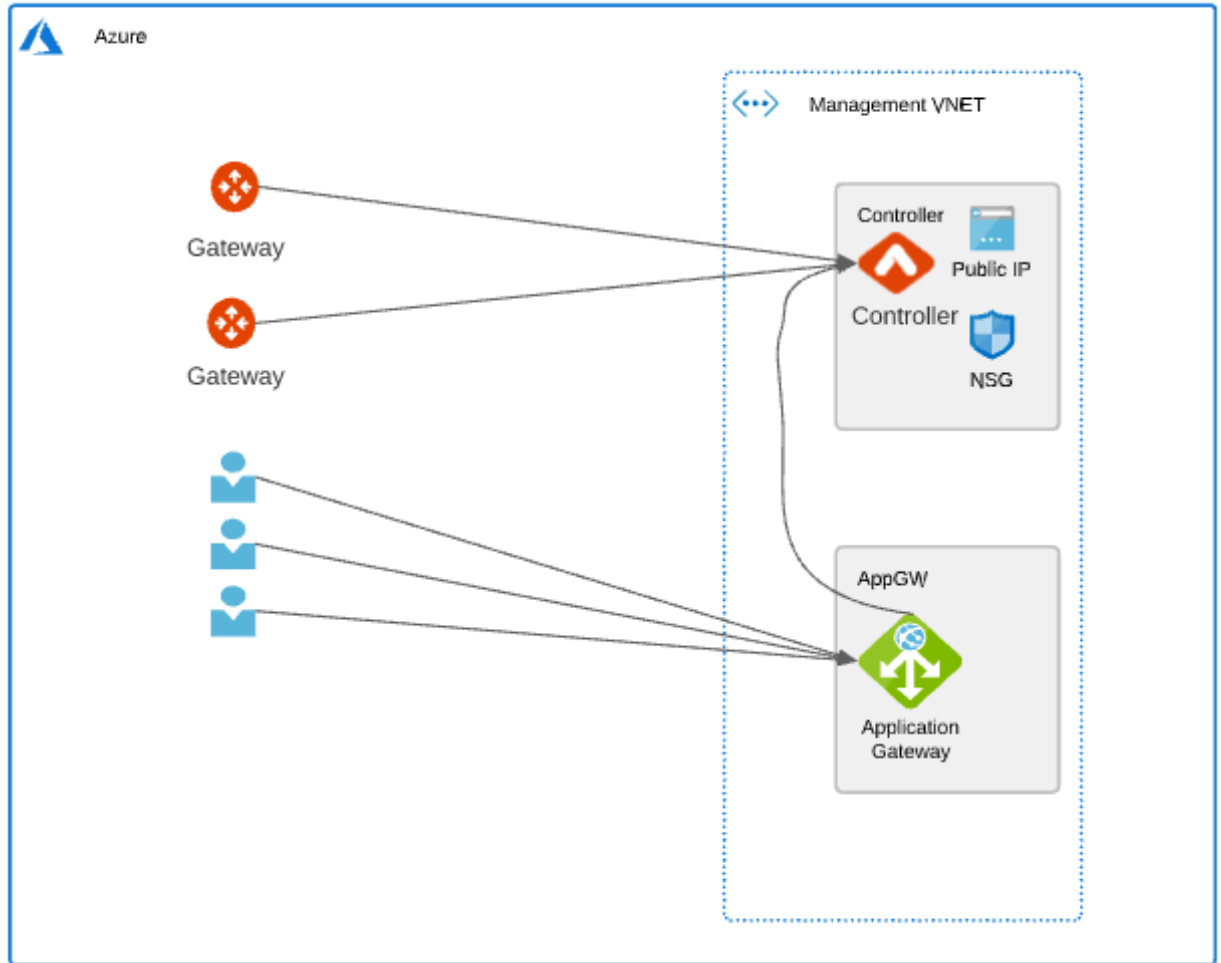
Applies to any cloud



- Confirm that the Controller Security Group Management is NOT disabled to only allow access to the Controller EIP from Aviatrix Gateways
- Create a new internet facing ALB
- Modify main Controller Security Group to only allow access from the ALB Security Group
- Enable WAF on the ALB with AWS Managed Rules
- Adjust ALB idle timeout, modify rulesets
- Modify ALB Security Group to only allow access from the admin user IP



- Use WAF with Azure Managed rules on Application Gateway to limit usual web hacks/attacks against Controller
- Only allow user access from the Application Gateway subnet to Controller on port 443 (Controller Security Groups management feature is a pre-requisite for gateway communication to Controller)
- Allow configuring user access on non-standard HTTPS listener port
- Terminate SSL connection on Application Gateway to leverage cloud native certificate management and WAF capability to inspect and log requests
- L7 health-check on the Controller





Gateway and Controller Sizing

Controller Sizing

- Controller uses multiple cores to handle the API query load generated by CoPilot → **Minimum 4 core instance**
- Resizing:
 - If you do not use User VPN
 - ❑ Stopping the controller to resize does not impact the data traffic
 - ❑ Always good practice to backup controller before performing upgrade
 - If you use User VPN
 - ❑ No impact to connected users, but new connections could not be established during the stop and resize
- Maintenance Windows for resizing usually do not require more than 15 minutes

Gateway Sizing

- Gateway selection affects expected throughput
- If you decide to enable **High Performance Encryption**
 - Use Jumbo MTU and to verify MTU along the path
 - Go to TROUBLESHOOT > Diagnostics > Network
 - Select a gateway and destination IP address, click **Trace Path**
 - It will display MTU of the devices along the path
- **Secure Egress**
 - T2.micro is not adequate, for instance
 - But test it out and adjust accordingly based on CSP quotas*
 - *CSPs have quotas on PPS, but often do not publish them



Gateway and Controller Upgrading & Updating

Types of Upgrades and Updates

- Software Upgrade

- Replaces relevant Platform (i.e., Controller) and **selected** Gateway packages, configuration files, and binaries to Target version
- Part of regular maintenance operations
- Hitless

- Image Upgrade

- Replaces **selected** Gateway cloud image (AMI, VHD, etc.) to the newer version
- Doesn't change Aviatrix software version
- Less frequent
- Incurs traffic disruption

- Security Patches

- Released when security updates to underlying software components become available.
- Most security patches are hitless (review the release notes)

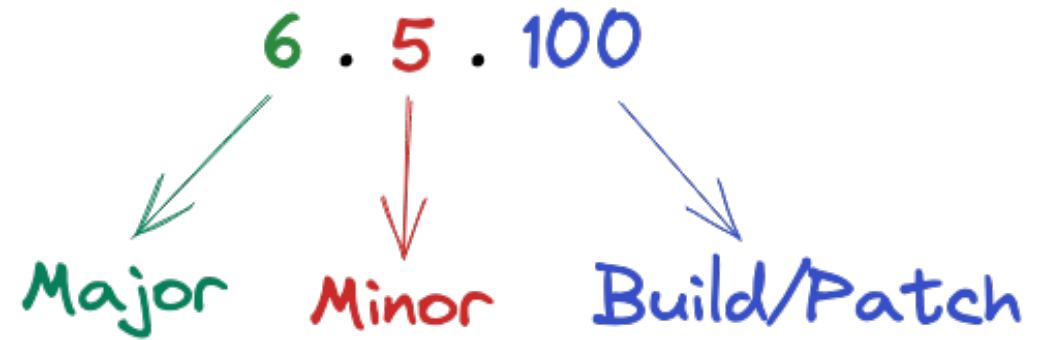
- Software Patches

- Released to address compatibility issues when they arise (if you are using any applications or configurations affected by the patch.
- Most software patches are hitless (review the release notes)

Terminology



- Software Major, Minor, Build Release
 - Numbering convention
 - Example: Aviatrix Release 6.5.100



Supported Upgrade Paths



- Upgrading Builds (within same minor release)

- You automatically get the latest build and cannot select the build number.
- Process might skip over previously released build numbers.



- Upgrading Minor Release Version (within same major release)

- You must upgrade each minor release sequentially.



- Upgrading Major Release Version

- You must upgrade each major release sequentially.



Software Rollback

- Software roll back to Gateway software previous version
- Previous version may or may not be the latest patch/build version available
- Replaces the entire Gateway (image + software) → expect brief disruption
- Gateway Image version may automatically be downgraded if required
- Does not apply to Controller

Upgrade Scenarios

- At any point in time, the Controller supports 2 unique Gateway software versions :
 - **Target Version:** same version as the Controller
 - **Previous:** previous version of the Controller
- Example of supported scenario
 - Upgrade the Controller from 6.5 to 6.5.100
 - Upgrade a group of Gateways to 6.5.100
 - Remaining Gateways run 6.5
- Example of unsupported scenario
 - Upgrade the Controller from 6.5 to 6.5.100
 - Upgrade a group of Gateways to 6.5.100
 - Remaining Gateways run 6.5
 - **Upgrade the Controller to 6.5.200**
 - **Not supported: All Gateways must be upgraded to 6.5.100 before upgrading the Controller to 6.5.200**

Common Scenario – Rolling Upgrades

Upgrade all Secondary Gateways in a particular CSP region

- Upgrade of the Controller has been performed
- Use the Gateway Selective Upgrade capability
 - Add CSP filter
 - Add region filter
 - Add Gateway Type filter
- Optionally perform a dry run upgrade of the selected Gateways

Selective Gateway Upgrade [Info](#)

Total Gateways: 19

Completed: 19

[▶ DRY RUN](#)
[↑ SOFTWARE UPGRADE](#)
[↑ IMAGE UPGRADE](#)
[↓ SOFTWARE ROLLBACK](#)
[↺](#)

Page Size: 50

⌵ COLUMN MENU

<input checked="" type="checkbox"/>	Name	Cloud	Region	Gateway Type	Account	Current Version
<input type="text"/>	▼	<input type="text"/>	▼	<input type="text"/>	▼	<input type="text"/>
<input checked="" type="checkbox"/>	aws-us-east-1-transit2-agw	AWS	us-east-1	Primary	uhoodbhoy	6.5.1922
<input checked="" type="checkbox"/>	aws-us-east-1-transit2-agw-hagw	AWS	us-east-1	Secondary	uhoodbhoy	6.5.1922
<input checked="" type="checkbox"/>	aws-us-east-1-spoke2-agw	AWS	us-east-1	Primary	uhoodbhoy	6.5.1922
<input checked="" type="checkbox"/>	aws-us-east-1-spoke1-agw	AWS	us-east-1	Primary	uhoodbhoy	6.5.1922
<input checked="" type="checkbox"/>	aws-us-east-2-transit1-agw	AWS	us-east-2	Primary	uhoodbhoy	6.5.1922
<input checked="" type="checkbox"/>	aws-us-east-2-transit1-agw-hagw	AWS	us-east-2	Secondary	uhoodbhoy	6.5.1922
<input checked="" type="checkbox"/>	azure-us-west-transit4-agw	Azure ARM	West US	Primary	azure-uhoodbhoy	6.5.1922
<input checked="" type="checkbox"/>	azure-us-west-transit4-agw-hagw	Azure ARM	West US	Secondary	azure-uhoodbhoy	6.5.1922

[↑ APPLY COLUMNS](#)
[⊗ UNSELECT ALL](#)

- ☒ Current Version
- ☒ Target Version
- ☒ Rollback Image Version
- ☒ Previous Image Version
- ☒ Current Image Version
- ☒ Target Image Version
- ☒ Kernel Version
- ☒ Distribution Version
- ☒ Account
- ☒ Cloud
- ☒ Region
- ☒ Gateway Type
- ☒ Gateway Role



Support Resources

Support Portal



- Aviatrix customers may visit Support portal – <https://support.aviatrix.com> to access:
 - Knowledge Base with videos
 - Documentation
 - Community
 - History of tickets
 - CSP outage tracker
- Sign up for Email Notifications from Controller

Email Notifications

Manage the status of your Aviatrix system and ensure your teams receive important notification emails sent by Aviatrix.

Enter email aliases for teams that can respond to each type of alert. If you enter the same email for all four fields, that email account could be overwhelmed. [Read more](#)

The email aliases collected will solely be used for the purpose described here. For more information, please refer to our [Privacy Policy](#)

ACCOUNT AND CERTIFICATE ALERTS

Receive important account and certification information.

Administrator Email Alias

ace.lab@aviatrix.com

VERIFY

SECURITY EVENTS

Receive security and CVE (Common Vulnerabilities and Exposures) notification emails.

Security Admin Email Alias

security-admin-group@yourcompany.com

VERIFY

CRITICAL ALERTS

Receive field notices and **critical** notices. These alerts ensure that you can respond to urgent events.

IT Admin Email Alias

it-support@yourcompany.com

VERIFY

STATUS CHANGE NOTIFICATIONS

Receive system/tunnel status notification emails.

IT Admin Email Alias

it-admin-group@yourcompany.com

VERIFY

Status Change Notification Interval (seconds)

60



Next:

Distributed Cloud Firewall