



# Operational Best Practices

ACE Solutions Architecture Team

# CoPilot Remote Syslog

- The Syslog server is by default the CoPilot.
  - ❑ When you deploy the CoPilot, automatically the Controller will open the port UDP **5000** (Syslog) on the Security Group attached to the CoPilot instance.
  - ❑ Aviatrix CoPilot Remote Syslog Profile is set to use the Profile **9**.

- In the **CoPilot > Settings > Configuration > Logging Services** page, you can configure the forwarding of logs from the Aviatrix platform to the log servers of well known log management systems.

## Remote Syslog ✔ Enabled

### Aviatrix CoPilot Remote Syslog Profile

Server	[REDACTED]
Protocol	UDP
Port	5000

[Edit Profile](#)

### Manage Remote Syslog

Profile: Profile 2

Profile Name: SolarWinds' Kiwi Syslog

Server: [REDACTED]

Protocol: UDP Port: 5000

▼ Certificate

▼ Custom Template

▼ Advanced Settings

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

# CoPilot NetFlow

- The NetFlow collector is by default the CoPilot.
  - ❑ When you deploy the CoPilot, automatically the Controller will open the port UDP **31283** (NetFlow) on the Security Group attached to the CoPilot instance.
  - ❑ All the Aviatrix Gateways will send NetFlow data to the CoPilot.
  - ❑ As a consequence, FlowIQ feature in Aviatrix CoPilot will start to process the NetFlow information received by the Gateways.

### Netflow Agent ✔ Enabled

Server	██████████
Port	31283
Mode	IPT Mode

[Edit Configuration](#)

- In the **CoPilot > Settings > Configuration > Logging Services** page, you can configure the forwarding of the NetFlow Data from the Aviatrix platform to your designated service point.

### Manage Netflow Agent

Repository

Server  
██████████

Port: 31283      Version: 9

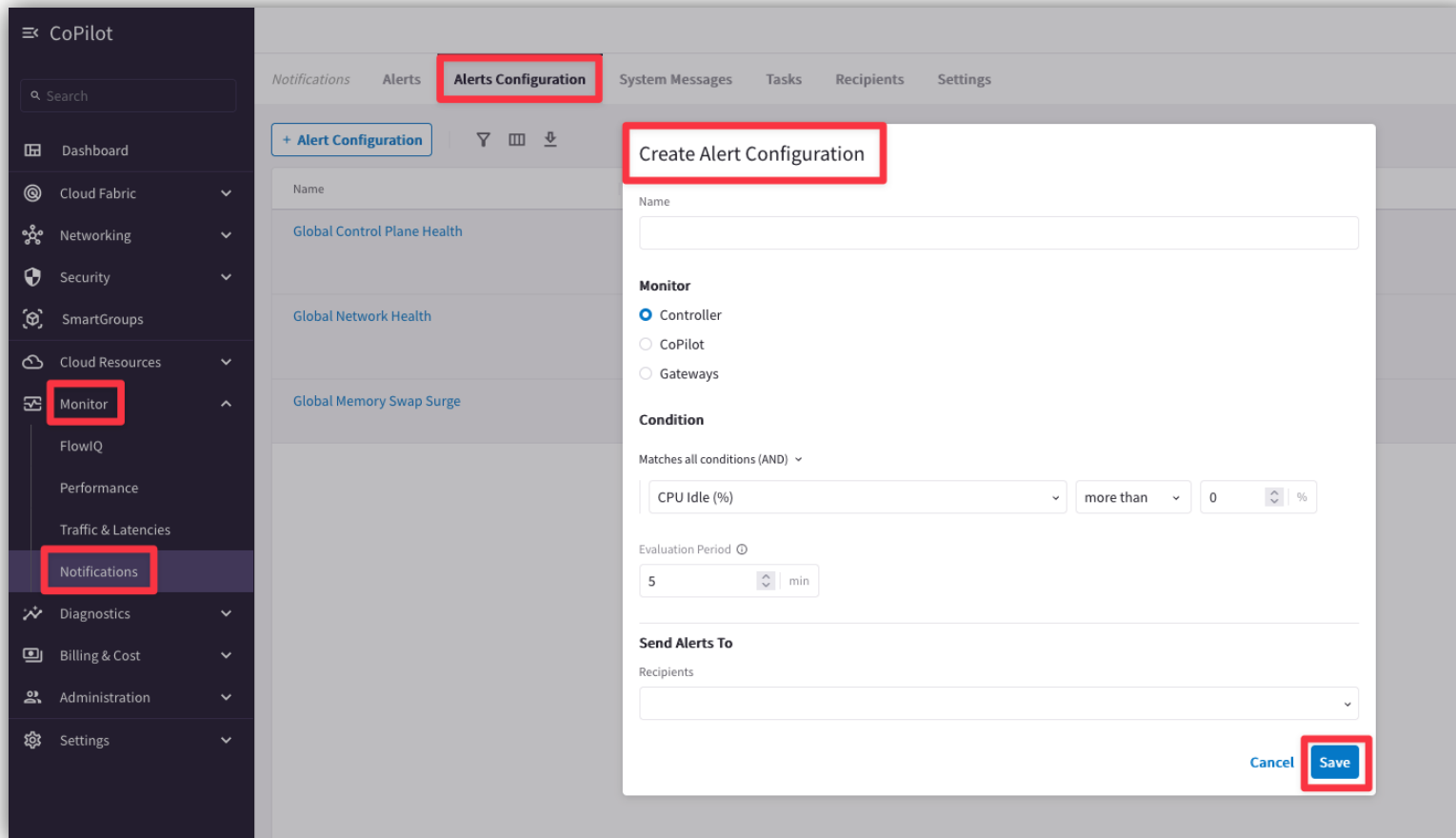
Mode  
 IPT  
 L7 Preview Feature

▼ Advanced Settings

DisableCancelSave

# CoPilot Alerts Configuration

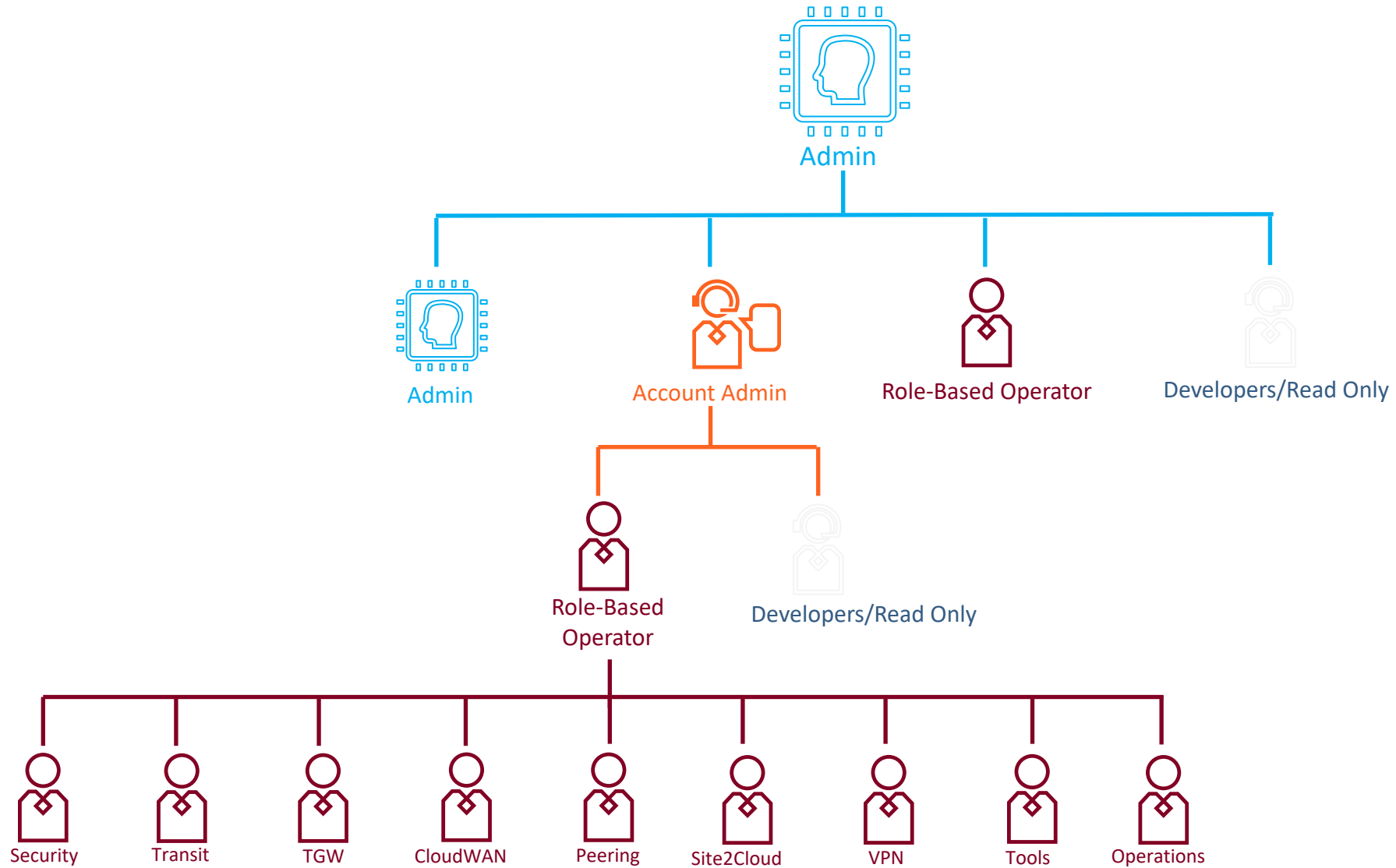
1. Webhooks Integrations work with any 3rd party integration (Slack, PagerDuty, ServiceNow, etc.)
2. Add webhook endpoints (can send payload as JSON or text)
3. Provide custom tags in the payload to classify triggered events and further integrate into your systems
4. Get alerted via webhook and email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

A screenshot of the Aviatrix CoPilot web interface. The left sidebar shows a navigation menu with 'Monitor' and 'Notifications' highlighted with red boxes. The main content area has a tab labeled 'Alerts Configuration' also highlighted with a red box. Below the tab is a list of alerts, including 'Global Control Plane Health', 'Global Network Health', and 'Global Memory Swap Surge'. A modal window titled 'Create Alert Configuration' is open, showing fields for 'Name', 'Monitor' (with 'Controller' selected), 'Condition' (set to 'CPU Idle (%) more than 0 %'), and 'Evaluation Period' (set to '5 min'). The 'Send Alerts To' section has a 'Recipients' dropdown. 'Cancel' and 'Save' buttons are at the bottom right, with 'Save' highlighted by a red box.



## Role-Based Access Control (RBAC)

# RBAC: Role-Based Access Control



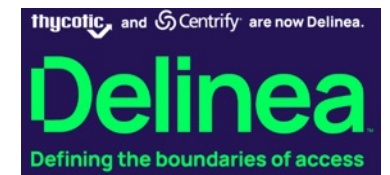
# Authentication Phase



- 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** Filter Grid Download

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 Search and Select

- 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)

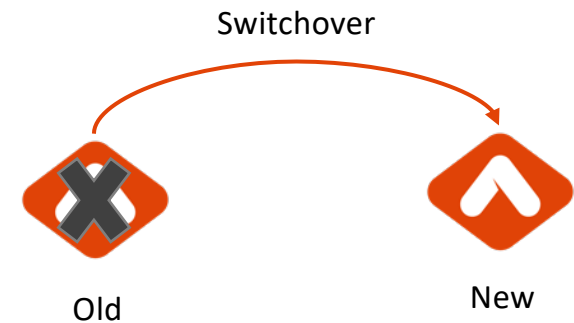


- Very important: Controller is not in the data path
- If Controller is down → Data Plane still functions
- Your cloud network is still up and running
- Do not compare on-prem to cloud
  - Hardware devices cannot be replaced / software is more flexible
  - Cloud operating models are different
  - Cloud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

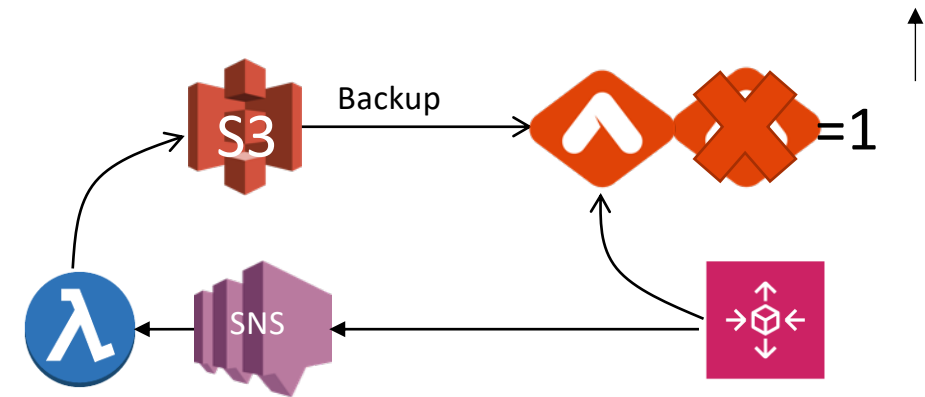


[https://docs.aviatrix.com/HowTos/controller\\_ha.html](https://docs.aviatrix.com/HowTos/controller_ha.html)

<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



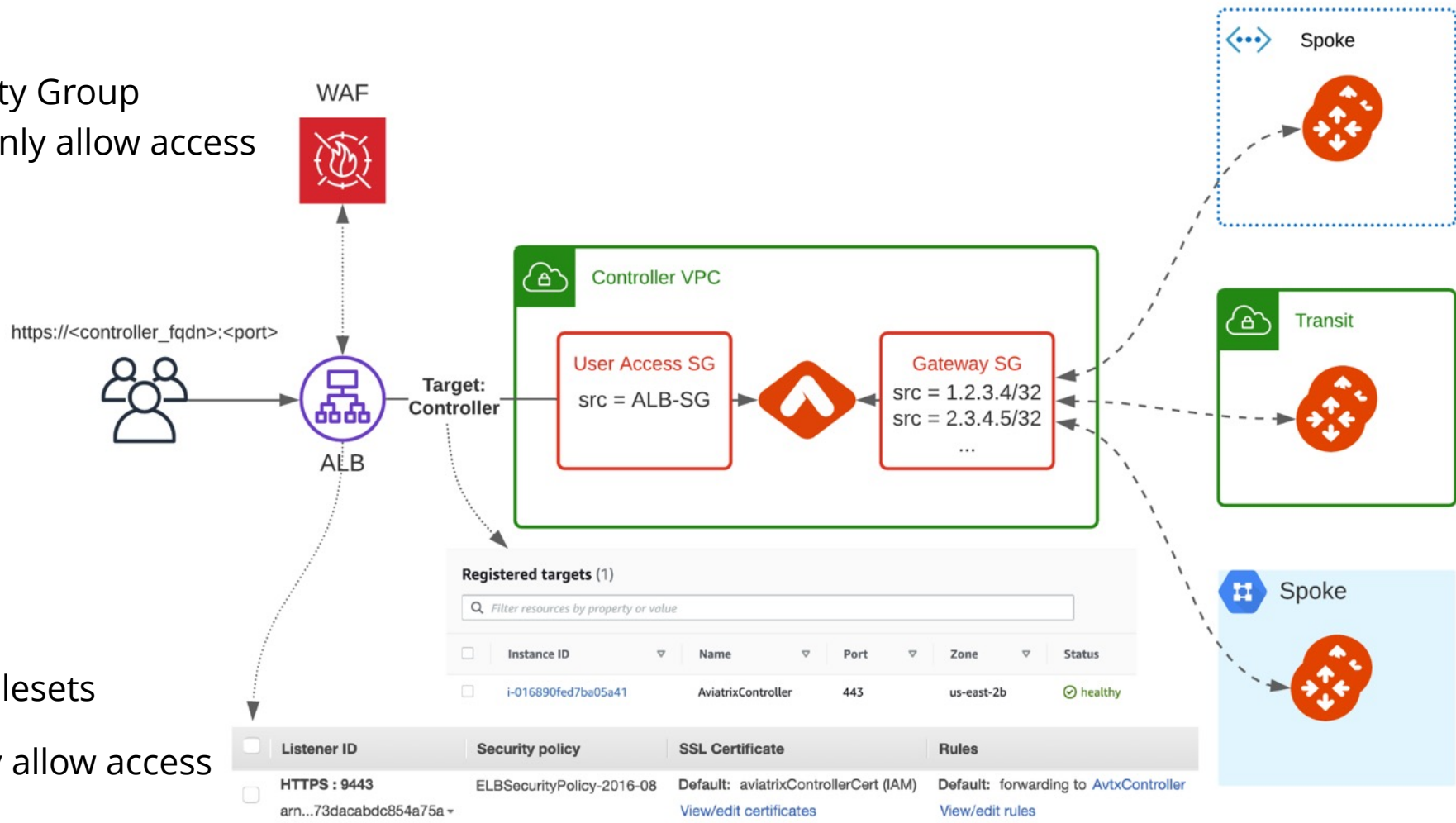


# Securing Aviatrix Controller with Application Load Balancer

# 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

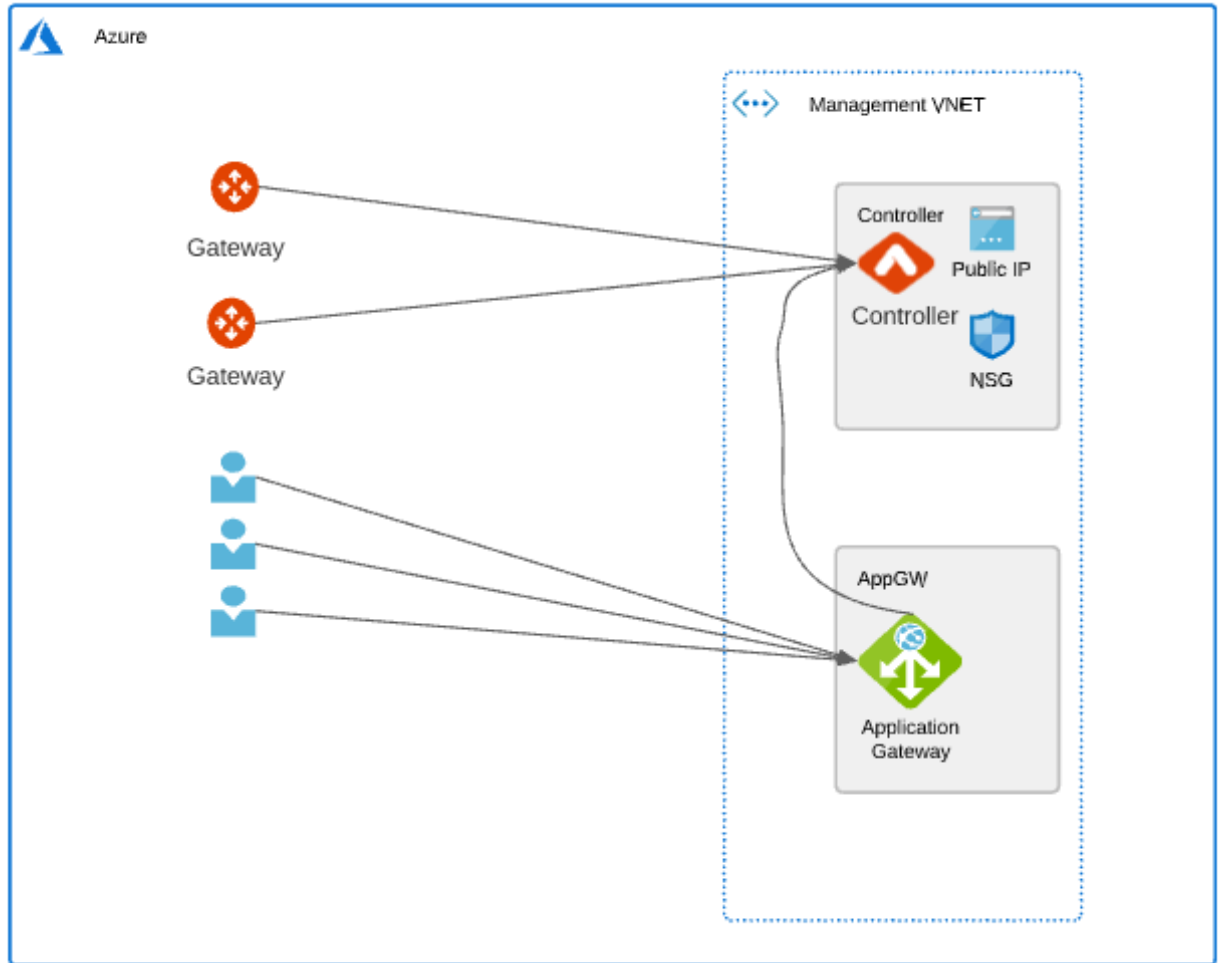




# Azure



- 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)

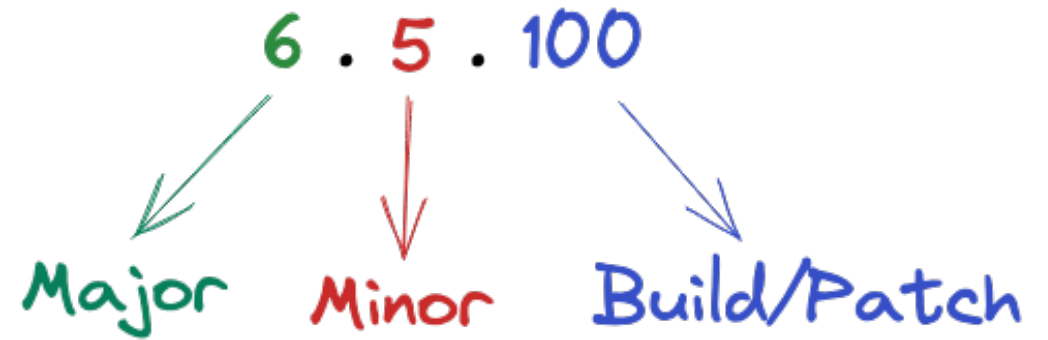
- Software Patches

- 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

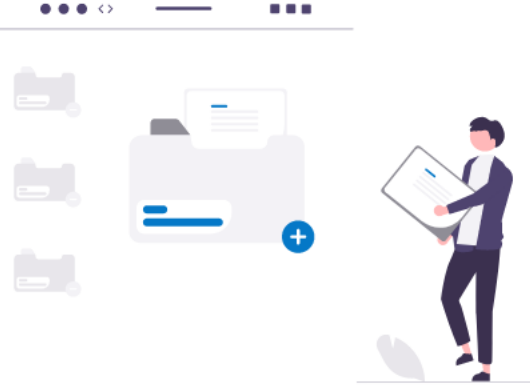
- Software roll back to Gateway software previous version
- Previous version may or may not be the latest patch/build version available
- Replaces the entire Gateway (image + software) → expect brief disruption
- Gateway Image version may automatically be downgraded if required
- Does not apply to Controller

# 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**

# Upgrade Groups (1)

- ❑ Each Upgrade Group that gets created is split up into two groups:
  - **Primary Node Group**
  - **Secondary Nodes Group**
- ❑ If you do want to get around that you will have to, after you have created the group, to manually update it to include additional ones. Likewise, If you want to do both primary and Secondary nodes at the same time.



## Upgrade Plan and Upgrade Groups

You can now create Upgrade Groups of Gateways based on Cloud, Account, Region, or other criteria.

Each Upgrade Group will be automatically divided into two subgroups: one comprising High Availability (HA) instances and another comprising Primary instances.

Reorder the groups based on your preference to create your Upgrade Plan. Applicable for both Software and Image Upgrades.

# Upgrade Groups (2)



CoPilot

Search

- Dashboard
- Cloud Fabric
- Networking
- Security
- SmartGroups
- Cloud Resources
- Monitor
- Diagnostics
- Billing & Cost
- Administration**
  - User Access
  - Reports
  - Audit
  - Upgrade**

Upgrade **Upgrade Plan**

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

**Gateways Requiring Upgrade**

Software Upgrade	Image Upgrade
0	0

[Prepare For Upgrade](#)

[+ Upgrade Group](#) | [Prepare For Upgrade](#) | Filter | List | Download

<input type="checkbox"/>	Name	Gateway Type	Gateway Instance	Software Version
<input type="checkbox"/>	Unassigned HA	Transit, Spoke	3	7.0.2239
<input type="checkbox"/>	Unassigned Primary	Transit, Spoke	6	7.0.2239

Controller Version	Latest Software Version
7.0.2239 <b>Upgrade Controller</b>	7.1.3006

### Upgrade Gateways in All Upgrade Groups

Target Software Version ⓘ	Upgrade Group	Gateway Instances
7.0.2239	Unassigned (HA), <a href="#">+ 1 More</a>	9

**Software Upgrade**

Gateway software upgrades replace the relevant gateway packages, configuration files, and binaries without disrupting network traffic or replacing the gateways. All software upgrades are hitless.

**Image Upgrade**

Aviatrix periodically releases new gateway images that include updates, enhancements, and security improvements. A best practice is to plan to upgrade your gateways at least once a quarter.

#### Software Upgrade Options

Dry Run ⓘ

On  Software Upgrade On

Recommended: On

# Upgrade Groups (3)



Create Upgrade Group

Name

Gateway Selection Preview Gateways (5)

Matches all conditions (AND) ▾  
Gateway Type ▾ Equal ▾ Spoke x ▾  
 Transit  
 Spoke  
 Edge  
 VPN  
 Specialty  
[Select All](#)

Upgrade Group Order  
Place Upgrade Group

- ❑ Assign a name to the Upgrade Group
- ❑ Define the **Matching Condition**
- ❑ **Preview Gateways** toggle allows to see the nodes that exactly match the defined condition

Gateway Selection Preview Gateways (5)

🔍 Search

Gateway	Gateway Type	Cloud	Region	Account	Tags
AVX-AWS-SPOKE-GW-PROD1-1	spoke	AWS	eu-central-1	aws-account	
AVX-AWS-SPOKE-GW-PROD1	spoke	AWS	eu-central-1	aws-account	
AVX-AZURE-SPOKE-GW-PROD3	spoke	Azure ARM	West Europe	Azure-ACCOUNT	
AVX-AWS-SPOKE-GW-TEST	spoke	AWS	eu-central-1	aws-account	
AVX-AWS-SPOKE-GW-PROD2	spoke	AWS	eu-central-1	aws-account	

# Upgrade Groups (4)



<input type="checkbox"/> Name	Gateway Type	Gateway Instance	Software Version	Image Version	Kernel Version	Account	Cloud	Region	Upgrade Group Status	
<input type="checkbox"/> Upgrade-Spoke-GW	Spoke	1	7.0.2239	hvm-cloudx-a...	5.4.0-1096-aw...	aws-account	AWS	eu-central-1	Unknown	↑↓ ✎ 🗑️
<input type="checkbox"/> Upgrade-Spoke-GW	Spoke	4	7.0.2239	[Multiple]	[Multiple]	[Multiple]	[Multiple]	[Multiple]	Unknown	↑↓ ✎ 🗑️
<input type="checkbox"/> Unassigned <span>HA</span>	Transit	2	7.0.2239	[Multiple]	[Multiple]	[Multiple]	[Multiple]	[Multiple]		
<input type="checkbox"/> Unassigned <span>Primary</span>	Transit	2	7.0.2239	[Multiple]	[Multiple]	[Multiple]	[Multiple]	[Multiple]		

- ❑ After the Upgrade Group has been created, it will need to be committed before the upgrade gets started
- ❑ The **Edit** icon allows to modify the groups



# 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