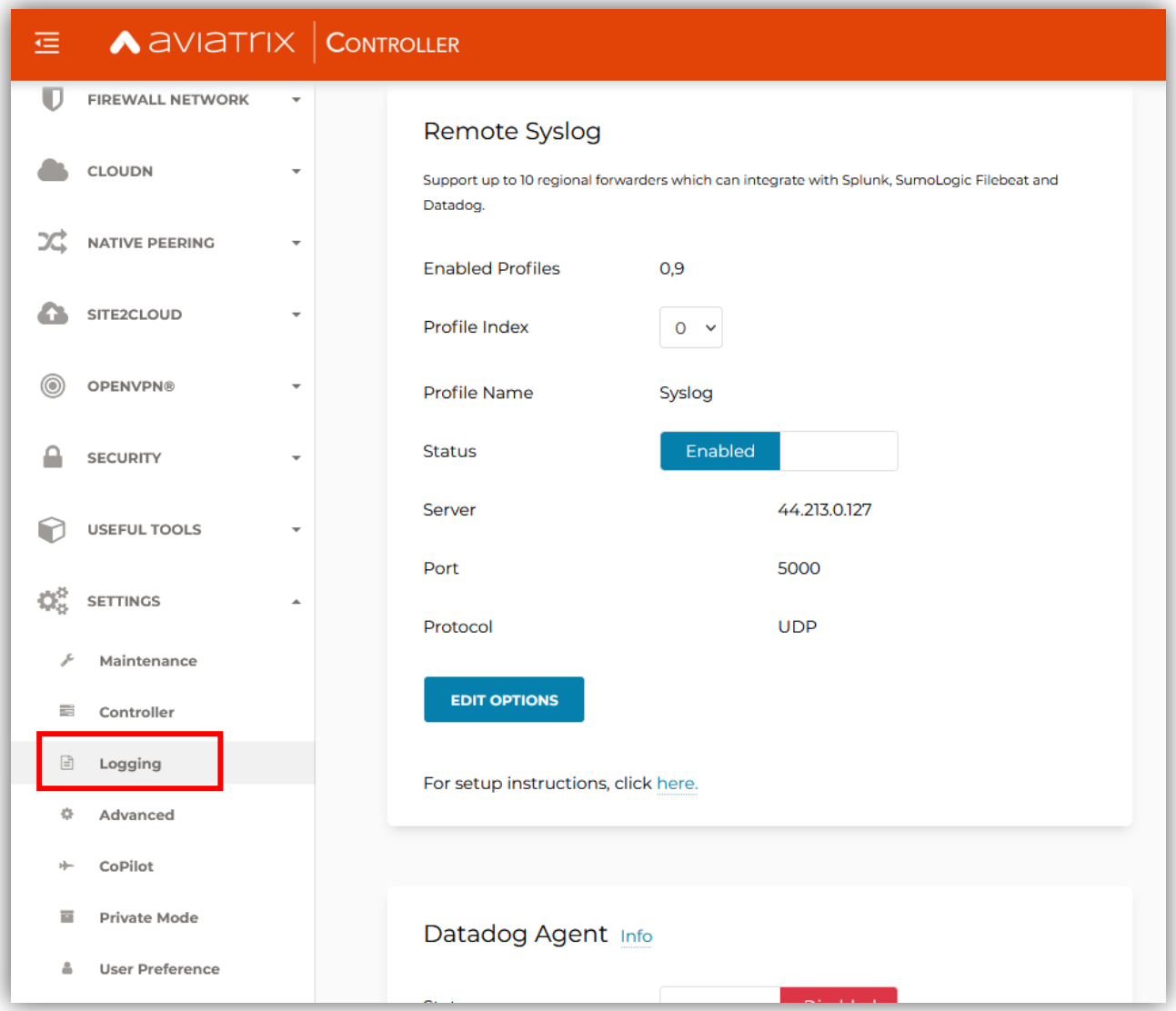
aviatrix

Operational Best Practices

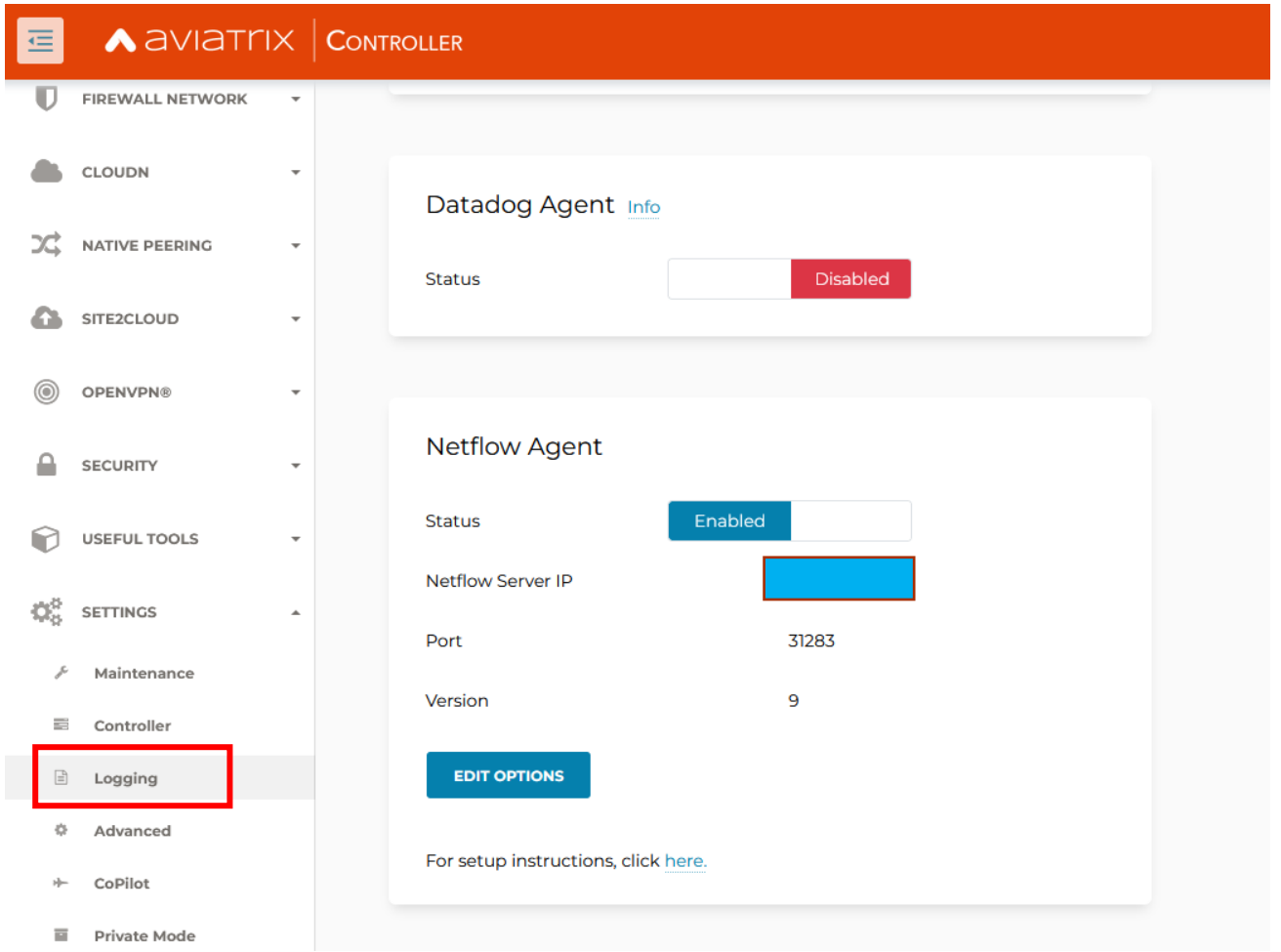
CoPilot Syslog Setup (FQDN and Audit data)

- 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



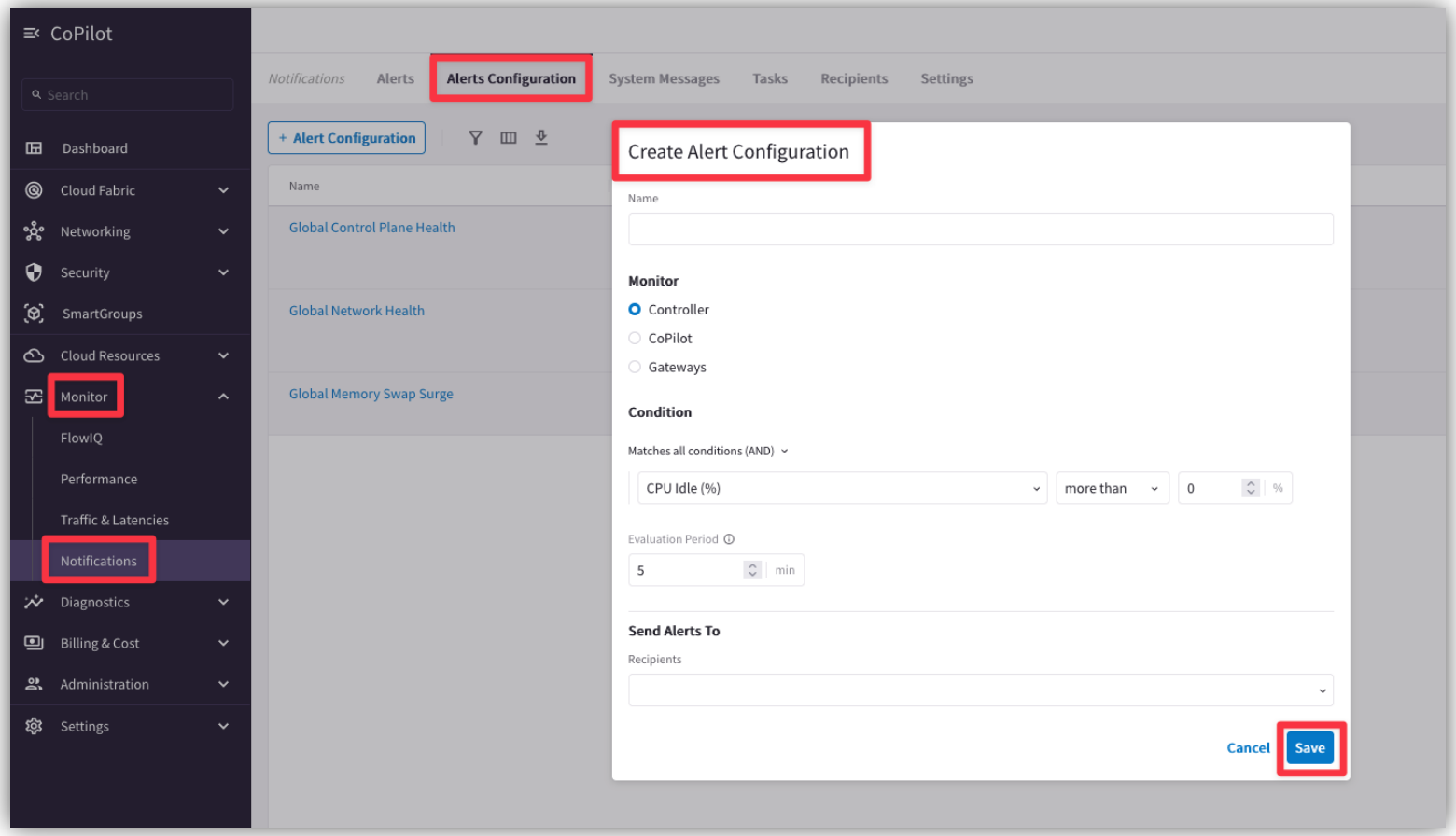
CoPilot NetFlow Setup (for FlowIQ and ThreatIQ data)

- 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



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



Role-Based Access Control (RBAC)

aviatrix

RBAC Permission Groups

- Allows for Roles (Permission Groups) to be created
- Permission Groups have a set of permissions
- Permission Groups are given access to a set of cloud accounts
- Users are added to Permission Groups
- Users can be authenticated in 2 ways:
  - 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

RBAC Permissions

Permission	Description
all_write	Full access except Settings
all_dashboard_write	All read/write for Dashboard
all_accounts_write	All read/write for Accounts
all_gateway_write	All read/write for Gateway
all_tgw_orchestrator_write	All read/write for TGW Orchestrator
all_transit_network_write	All read/write for Transit Network. Also requires Gateway permissions
all_firewall_network_write	All read/write for Firewall Network. Also requires Gateway, Transit Network and TGW orchestrator permissions
all_cloudn_write	All read/write for CloudN. Also requires TGW orchestrator and Transit network permissions
all_peering_write	All read/write for Peering
all_site2cloud_write	All read/write for Site2Cloud
all_openvpn_write	All read/write for OpenVPN
all_security_write	All read/write for Security
all_useful_tools_write	All read/write for Useful Tools
all_troubleshoot_write	All read/write for Troubleshoot

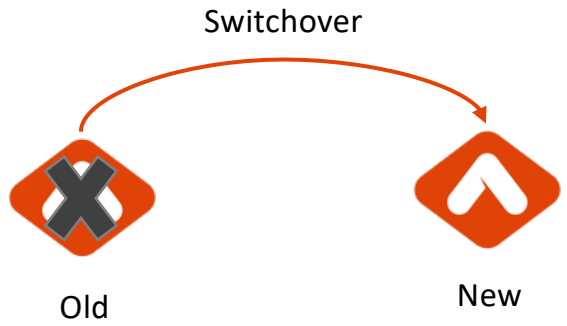
Aviatrix Controller High Availability (HA)

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

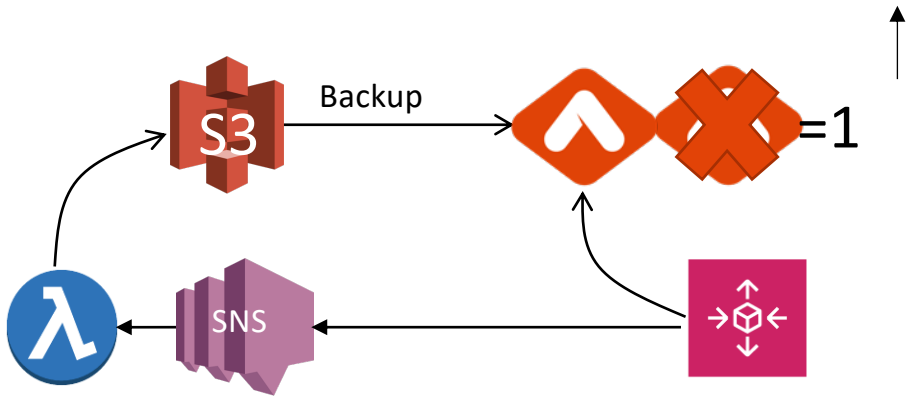
- Takes minutes to switch over to new controller
  - Depends on factors such as AWS latency, instance type, size of the DB, etc.
- Previous controller is terminated
- All existing configuration is restored
- New Private IP is assigned (new AZ)
- New controller stays at the same version as previous



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

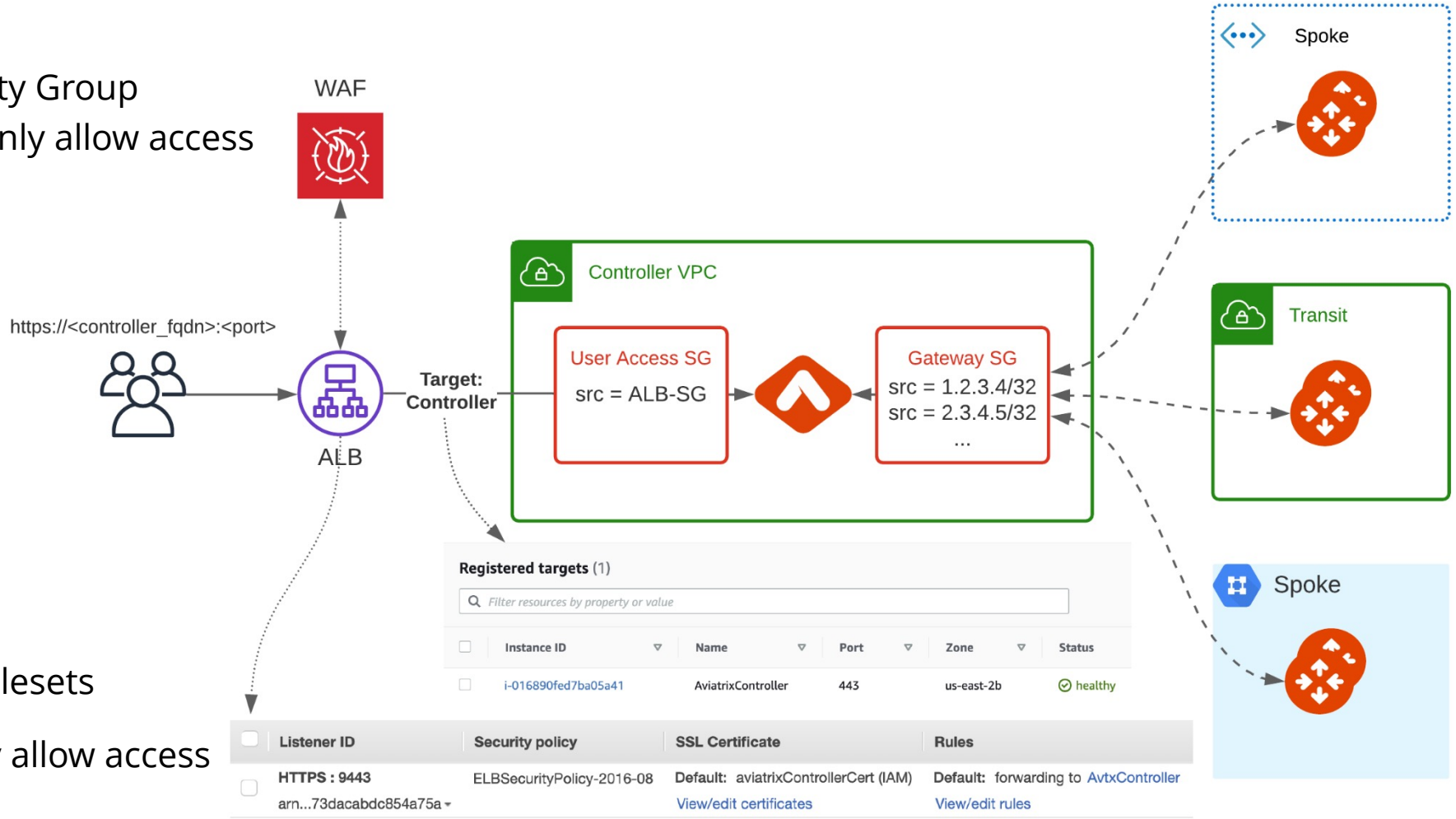


Securing Aviatrix Controller with Application Load Balancer

aviatrix

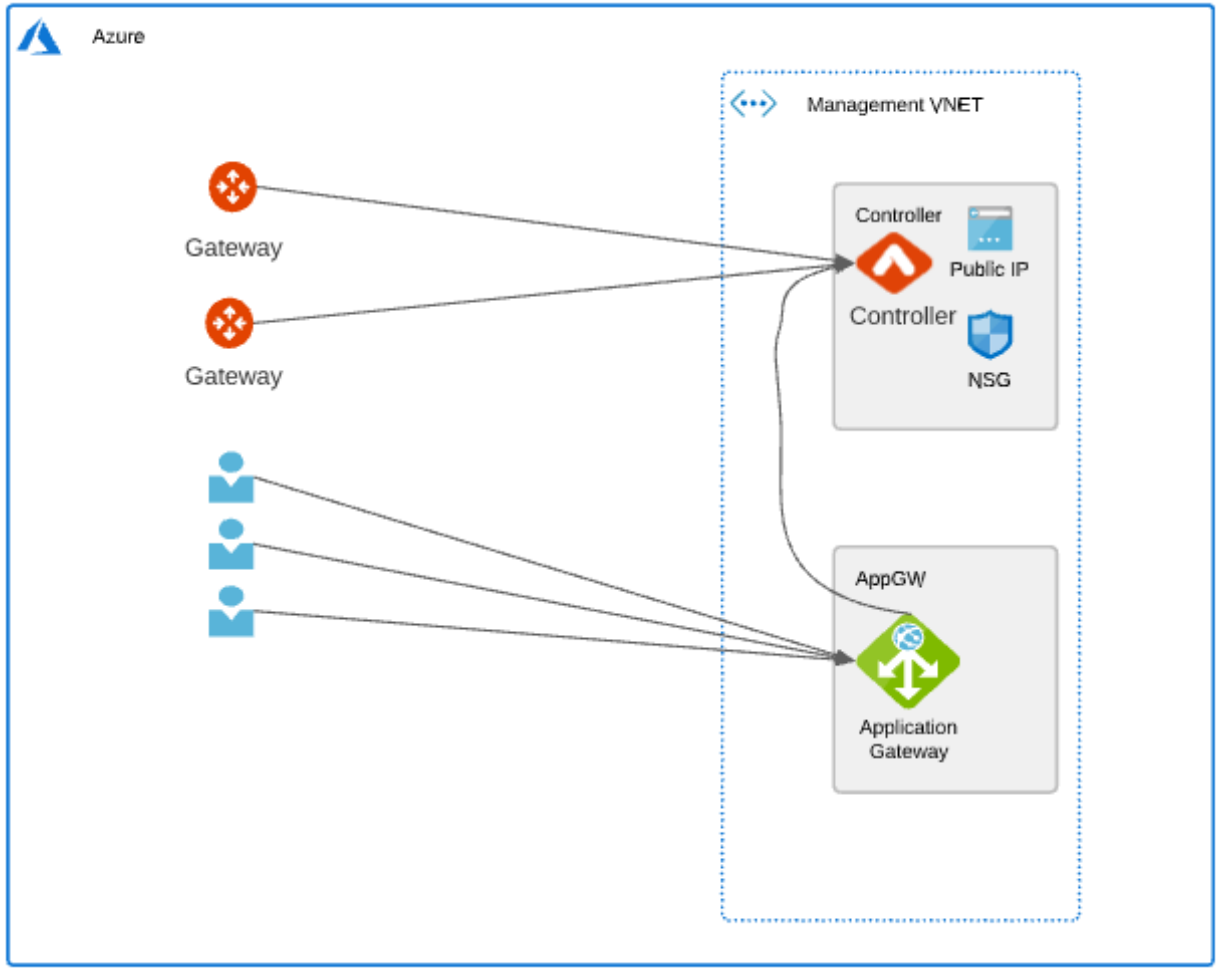
Applies to any cloud

- 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

aviatrix

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
- Benchmarks posted at https://community.aviatrix.com/t/35hpa6g
- Secure Egress
  - In many customer environments, the t3.small / B2s / n1-standard-2 is adequate
  - 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 Sizing

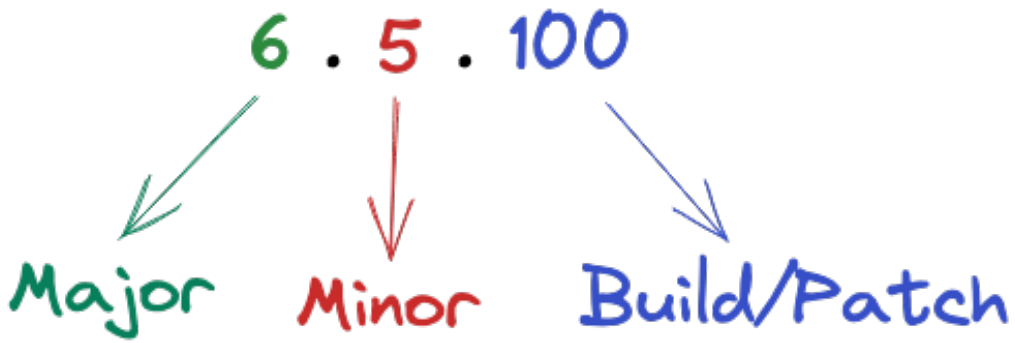
aviatrix

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

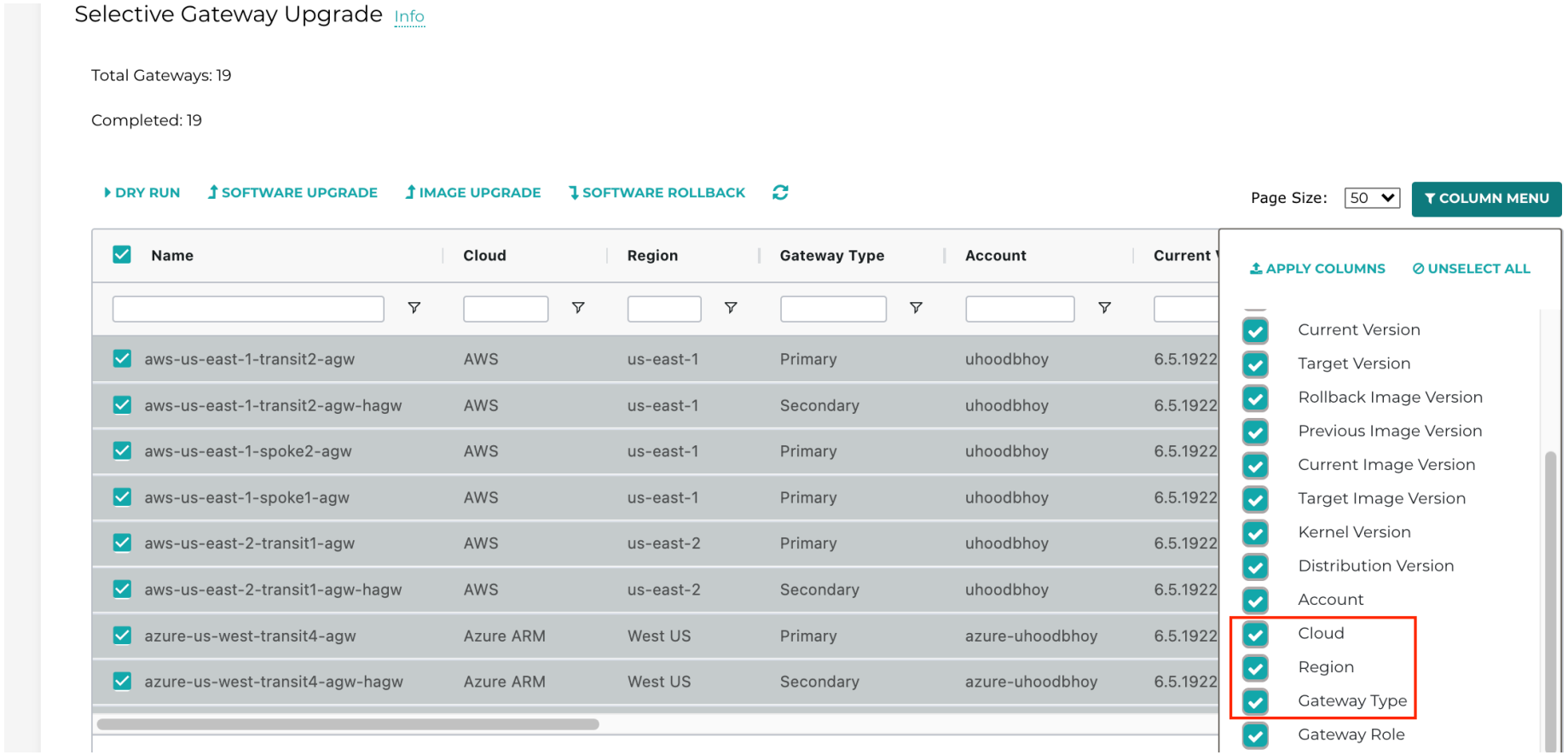
- At any point in time, the Controller supports 2 unique Gateway software versions :
  - **Target Version:** same version as the Controller
  - **Previous:** previous version of the Controller
- Example of supported scenario
  - Upgrade the Controller from 6.5 to 6.5.100
  - Upgrade a group of Gateways 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

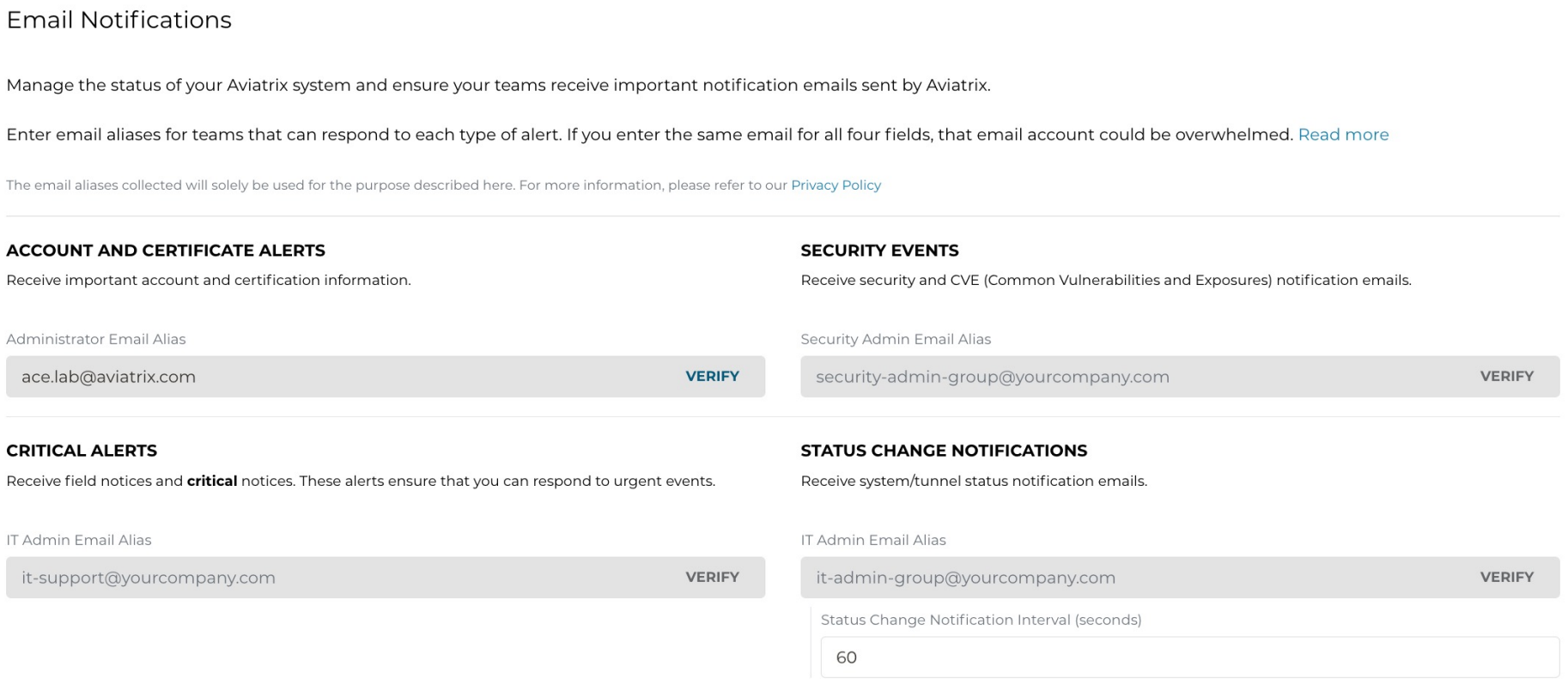


Support Resources

aviatrix

Support Portal

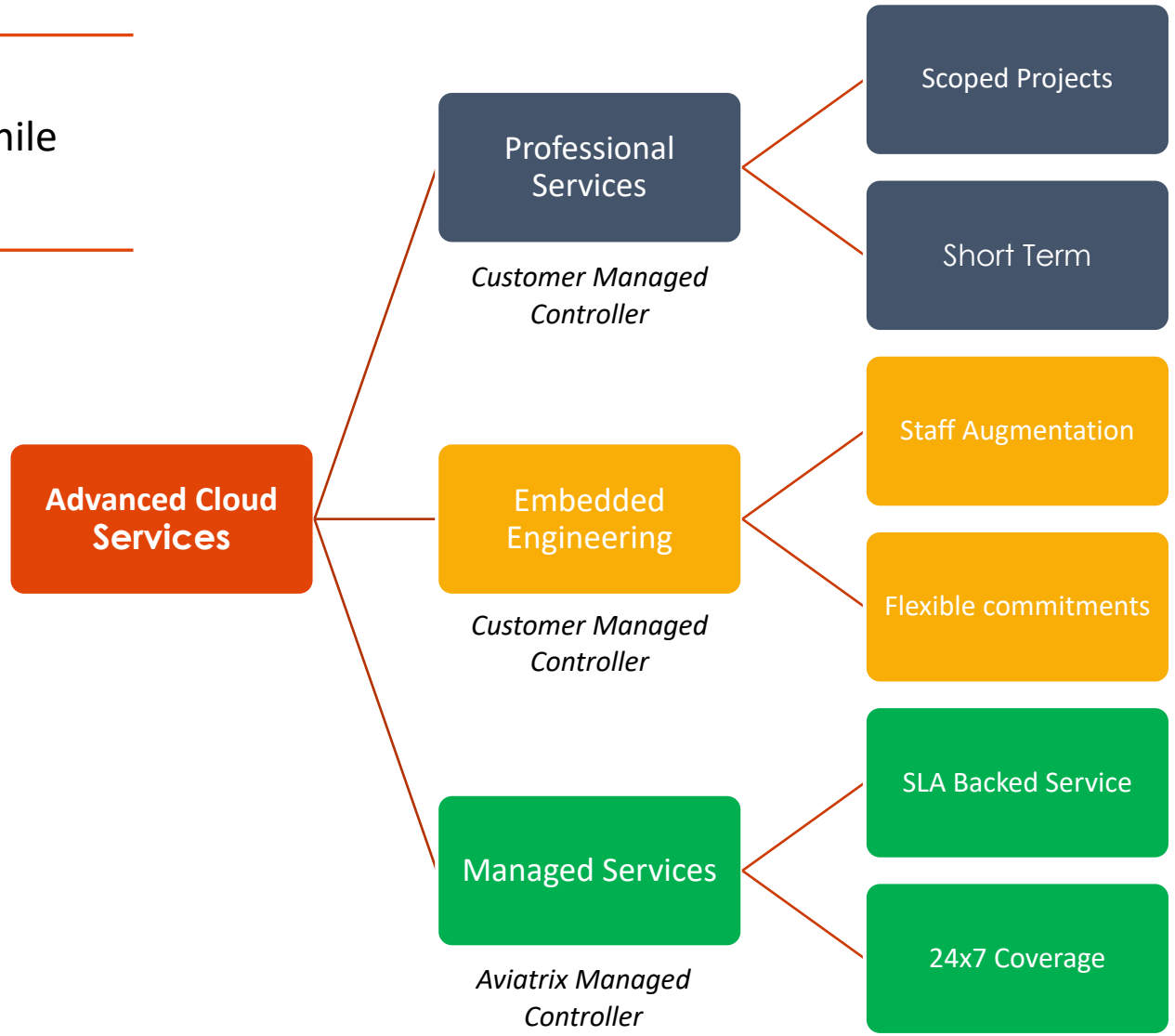
- Aviatrix customers may visit Support portal – https://support.aviatrix.com to access:
  - Knowledge Base with videos
  - Documentation
  - Community
  - History of tickets
  - CSP outage tracker
- Sign up for Email Notifications from Controller



ACS Offering

Advanced Cloud Services is a portfolio of offerings enabling Aviatrix to support your cloud network while you focus on your business

- Customization of all offerings
- Expertise across all major CSPs
- Global 24x7 coverage



aviatrix

Next:

Distributed Cloud Firewall