Documentation

Network Resiliency Best Practices Guide

Overview

The Network Resiliency Best Practices Guide describes existing Aviatrix features that help you improve the reliability and resiliency of your Aviatrix network. These best practices mean that you will be able to absorb the impact of any issues that occur, while continuing to provide service.

- Controller Best Practices
- CoPilot Best Practices
- IAM Best Practices
- Gateway Best Practices
- Multicloud Transit Best Practices
- AWS Transit Gateway Orchestrator Best Practices
- Transit FireNet Best Practices
- External Connections (S2C) Best Practices
- UserVPN Best Practices

NOTE

This guide will be updated on an ongoing basis. Please contact your Aviatrix account representative if you have any questions pertaining to this document.

Glossary

You can access the following glossary links for more information on Aviatrix terminology and general cloud networking terminology.

- Aviatrix Glossary
- General Glossary
- Multicloud Rosetta Stone

Controller Best Practices

IMPORTANT

IMPORTANT

The Aviatrix Controller and CoPilot can both be offline for a period of time without impacting the data plane. While the Controller is offline, traffic will continue to flow, but routing changes will not be processed. Understanding the impact of the Controller being offline will help in successful operation of the Aviatrix platform.

1. The Aviatrix Controller is shipped with a self-signed certificate. Establish a DNS hostname and install a TLS certificate issued by your organization or a recognized certificate authority.
2. Deploy the Aviatrix Controller and CoPilot in the same dedicated VPC.
3. Select and secure a suitable set of public IP addresses for both the Controller and CoPilot.

   WARNING

   Modifying these addresses will prevent communication between the Controller and gateways. Contact Support in the event of any accidental modification.

4. Controller High Availability (AWS): Configure the Aviatrix Controller to automatically restore itself in the event of a system issue.
5. Controller Security Group Management: Configure the Aviatrix Controller to manage security groups to restrict connectivity between Controller and Gateways as well as Aviatrix CoPilot. This prevents potential downtime or loss of visibility caused by user induced errors when managing Access Control Lists.
6. Controller Backup and Restore: The Controller orchestrates the configuration of your cloud network environment and should be periodically backed up to the appropriate AWS/Azure/Google account. If a replacement Controller is launched, you can restore the configuration data from your backup. Configure cloud storage accounts to replicate across regions in the event of a cloud provider outage.
7. Controller Disk/CPU/Memory Sizing Recommendations

   IMPORTANT

   Since these recommendations may change over time, please review and ensure your environment matches current Aviatrix sizing guidelines.

8. SAML Authentication: Enable SAML-based authentication and role-based access controls to the Aviatrix platform.
9. Build a development environment: Follow the DevOPS lifecycle and establish a development environment comprised of a Controller and CoPilot which includes a subset of features and test applications.
10. Restrict access to the Aviatrix Controller and CoPilot: Access can be restricted by means of a Web Application Firewall (WAF) and Web ACLs, which allows your UserVPN clients to authenticate to the SAML endpoint without allowing access to the Controller. Access to the Controller from WAF can be limited with access controls.

    As an alternative, access can be restricted via configuration in the Controller and CoPilot.

11. Logging: Export logs to one of our supported integrations.

CoPilot Best Practices

1. Aviatrix CoPilot is shipped with a self-signed certificate. Establish a DNS hostname and install a TLS certificate issued by your organization or a recognized certificate authority.
2. Deploy CoPilot: CoPilot provides important visibility into your environment. Choose the deployment method that best suits your needs. Deploy the Aviatrix Controller and CoPilot in the same dedicated VPC.
3. Notification and Alerting: By configuring proactive alerting of gateways, VPN tunnels, and other network components, you can receive alerts in case of any failures or performance degradation. When creating alerts, establish severity levels for your environment to ensure prompt response based on the issue detected.

   Use the CoPilot webhook feature to integrate Aviatrix with your organizations' Incident Management tools for faster detection and incident repair.

   Ensure that you enter at least one email address on the Monitor > Notification > Recipients tab so that you are notified when the alert conditions are met.

   Recommended metrics to use in alerts:

Controller/CoPilot System Metrics	**Value**
CPU Idle	<20%
CPU Used (%)	>= 89%
Memory Available (%)	< 30%
Disk Free (%)	< 6%
Memory Used (%)	more than 89 (%)
Gateway Health Metrics	
Gateway Status	Any change Available conditions are Down, Keep Alive Fail, Config Fail, and Upgrade Fail.
Underlay Connection Status	Any change
Connection Status	Any change
BGP Peering Status	Any change
Gateway Network Metrics	

Controller/CoPilot System Metrics	Value
Limit Exceeded Rate (PPS)	> 40 pkt/s
Bandwidth Ingress Limit Exceeded Rate	> 40 pkt/s
Bandwidth Egress Limit Exceeded Rate	> 40 pkt/s
Conntrack Limit Exceeded Rate	> 40 pkt/s
Packet Drop (%)	more than 1(%)
PPS Limit Exceeded Drop (%)	more than 1 (%)
Packets Dropped while Receiving	> 40 pkt/s
Packets Dropped During Transmission	> 40 pkt/s
Errored Packets Received Rate	> 40 pkt/s
Errored Packets Transmitted Rate	> 40 pkt/s

NOTE

Aviatrix CoPilot includes default alerts that should be used in all environments to ensure the healthy operation of the network. Ensure that you assign the appropriate recipients to these alerts, and that alerts are reviewed and acted upon in a timely manner.

The following are default alerts and cannot be deleted:

- Global Control Plane Health
- Global Memory Swap Surge
- Global Network Health

4. CoPilot Security Group Management: In addition to Controller and Gateway Security Group management, also enable CoPilot Security Group Management to restrict access to the CoPilot instance.
5. Customize Backup Schedules and Counts: Retain up to 60 days of Controller backups, to ensure quick recovery in the event of any issues. Determine a reasonable number of backups for your environment. Prior to network change windows, review backups and/or create a manual backup. Aviatrix recommends retaining an offline copy of your backup during upgrades. In addition to Controller backups, enable CoPilot backups to the Controller.
6. CoPilot Disk/CPU/Memory Sizing Recommendations

IMPORTANT

Since these recommendations may change over time, please review and ensure your environment matches current Aviatrix sizing guidelines.

7. RBAC (Role Based Access Control): Limit access for non-administrators to read-only accounts. When assigning access, always follow the principle of least privilege.
8. SAML: Only configure if not already configured in Controller.

IAM Best Practices

Aviatrix Account Audits: Use the Account Audit feature to be informed about when your policies deviate from Aviatrix standards. Audit failures are displayed in the CoPilot (Administration > Audit) and Controller dashboards.

Gateway Best Practices

1. Configure High Availability for Gateways and Tunnels: Aviatrix recommends deploying multiple HA gateways in different Availability Zones (AZs) to ensure redundancy. This helps distribute network traffic and provides automatic failover in case of a gateway failure.
2. Enable Single AZ HA: In non-production or non-critical environments which do not employ multiple gateways, Aviatrix recommends that gateways be deployed with single AZ HA enabled. This helps ensure uptime in the event of any issues. This is enabled by default if launched from the Controller or CoPilot. If using Terraform, you must enable the appropriate flag.
3. Auto Right-Sizing: Easily increase or decrease gateway size for gateway instances based on provided recommendations.

   NOTE

   If you want to schedule gateway scaling, or add new gateway instances when scaling up, you can continue to use the Gateway Scaling feature. The tabs for the Gateway Scaling feature only display if you configured the Gateway Scaling feature prior to CoPilot 4.15.

4. Adjusting Aviatrix Controller Gateway Keepalive Timers: Recovery times depend on the selected HA strategy. Align your objectives for each environment with the Aviatrix guidelines for recovery.
5. Gateway sizing recommendations: While each environment is different, Aviatrix provides recommendations on typical instance sizes for gateway deployments by cloud provider. Ensure that your environmental needs match the deployed instance sizes. Consider factors such as the number of VPCs, anticipated bandwidth requirements, and any specific performance needs of your applications.
6. Other gateway settings you can configure for resiliency are:
   - Modifying TCP MSS Sizes: The recommended maximum for AWS, Azure, and OCI is 1370 bytes. The recommended maximum for GCP is 1330 bytes. The default is usually sufficient.
   - IPsec Anti-Replay Window: The default size (1) is usually sufficient.

Multicloud Transit Best Practices

1. Multi-Region Design Patterns: Aviatrix recommends implementing a transit network architecture to centralize and simplify network connectivity. By using a hub-and-spoke model, you can connect multiple VPC or VNet environments to a central transit hub, which provides redundancy and centralized control. Also see Overview of Aviatrix Multicloud Transit Network.

   Transit architectures should span a minimum of two cloud provider regions. Ensure applications are designed to operate in the event of a single regional outage.

2. Multicloud Deployments: Connect different cloud providers using MultiCloud Transit Peering.
3. Multi-Tier Transit: Use in larger deployments. You can add transit layers to simplify peerings.

AWS Transit Gateway Orchestrator Best Practices

Only do the following if using the Aviatrix AWS TGW Orchestrator feature.

1. Enable TGW nightly audit of routes: This ensures routing consistency when working in TGW Orchestrator environments.
2. Enable TGW route approval: This ensures the predictability of your network routing. Confirm and advertise approved routes learned over Direct Connect or VPN connections.
3. Use Transit Gateway Peering: Connect Transit Gateways in multiple accounts and regions together with Transit Gateway Peering for redundancy.

Transit FireNet Best Practices

1. Simplify the insertion of Next Generation Firewalls with Transit FireNet: With Transit FireNet, Aviatrix simplifies the insertion and health-check of firewalls in a topology. Transit FireNet can filter traffic in both East/West and North/South directions and you can select inspected traffic. Health monitors ensure continuity of service in the event of a firewall outage.
2. Deploy Across Availability Zones: Transit FireNet is designed to provide high availability and fault tolerance. Deploy multiple Transit FireNet gateways across different availability zones and regions to ensure redundancy and resiliency. Deploy firewalls and Transit FireNets in matching availability zones to optimize latency.
3. Firenet Vendor Integrations: To simplify deployment of Next Generation Firewalls (NGFW), use existing Aviatrix vendor integrations to rapidly deploy and prepare Palo Alto, Check Point, and Fortinet FortiGate firewalls in the cloud.

Transit FireNet allows for the use of almost every NGFW (Next Generation Firewall) appliance. However, existing firewall integrations can help improve the speed of deployment by pre-configuring routes on the firewalls.

4. Firewall instances should be deployed in HA pairs and designed to meet the throughput needs of your environment.

External Connections (S2C) Best Practices

1. Deploy Across Regions: Deploy Site2Cloud connections across provider regions for redundancy.
2. Active-Active HA: To achieve redundancy for VPN connections, Aviatrix supports an active-active HA architecture. By establishing multiple tunnels between your on-premises data center and the cloud, you can ensure continuous connectivity even if one tunnel or gateway fails.
3. Use BGP AS Path Prepend: When establishing a Site2Cloud connection, review your traffic engineering requirements. Utilize AS Path Prepend when needed to influence traffic flows.
4. BGP route approval: Ensure the predictable flow of traffic by enabling BGP route approval. This prevents accidental injection of routes.
5. Handling IP-Overlap: In the event of IP overlap between Cloud and On-Premise environments, or between overlapping cloud environments, build Site2Cloud connectivity with Mapped NAT enabled. Mapped NAT simplifies IP address translation between existing environments.
6. Keeping IPSEC Tunnels Active: In environments that may not have regular traffic, avoid security association timeouts by enabling Periodic Ping as a keep-alive mechanism.
7. Reduce Convergence Time: Event Triggered HA reduces convergence time.
8. Fine-tune detection timers when networks overlap: When on-premise and cloud networks overlap, follow Aviatrix recommendations for improving failover timers.
9. The following settings are also available for resiliency:
    a. Dead Peer Connection
    b. Site2Cloud RX Balancing
    c. BGP timers and settings

UserVPN Best Practices

1. Establish User VPN Profiles to Restrict Access: Establish VPN profiles for each environment requiring remote access.
2. Follow the principle of "least privilege": Create a base Deny-All ruleset and add additional access as required. Assign multiple profiles to a user in a layered approach via SAML to simplify access management.

3. Geographic redundancy: Deploy UserVPN gateways in geographically redundant locations, and use VPN User Accelerator when applicable to ensure uptime and low latency connectivity to your cloud environments.
4. Scale-out: Determine the approach that best suits your needs when deploying VPN gateways. Select from either load balancer, round-robin DNS, or geographically-based DNS response to address user VPN demands.
5. Increase the maximum number of user connections per gateway: Establish thresholds for usage of each VPN gateway to better distribute load.
6. Client certificate sharing: Do this to reduce provisioning requirements and use your chosen Identity Management system to provide role-based controls over access.
7. Integrate with SAML: Integrate VPN deployments with your identity management systems to provide uniform controls over authentication, authorization, and accounting.
