Management and Governance Lens

AWS Well-Architected Framework

Management and Governance Lens: AWS Well-Architected Framework

Table of Contents

Management and Governance Lens — Coming Soon

Publication date: **December 4, 2020**

The Management and Governance Lens for AWS Well-Architected, now under development, will make it easier for customers to develop management and governance solutions to support the design, implementation, and operation of applications in AWS and on-premises. The Management and Governance Lens provides prescriptive guidance on key concepts, design principles, and best practices for optimizing management and governance—including recommended combinations of AWS services, integration points with AWS Partner Network (APN) Partner solutions, and vetted reference implementations. The Management and Governance Lens incorporates best practices learned from customers migrating thousands of applications to AWS, and includes guidance on satisfying regulatory expectations for different industries.

Customers of every size across all industries are moving to the cloud to become more agile, reduce costs, instantly scale, and deploy globally in minutes. When making this transition, customers need the visibility into their AWS and on-premises environments to give confidence that applications adhere both to their internal control and operational requirements, and the proven AWS Well-Architected Framework pillars.

The AWS Well-Architected Management and Governance Lens helps customers successfully leverage familiar processes and tools from AWS Technology Partners, and offers guidance on how to use them, and integrate across AWS for effective management and governance solutions.

This document describes a few management and governance scenarios that our customers encounter, the AWS services that support these scenarios, and links to published solutions and AWS Competency Partners that enable these scenarios. This document also describes the AWS services that support these scenarios, including AWS Config, AWS Control Tower, AWS Organizations, AWS Security Hub, AWS Service Catalog, and AWS SSO.

Identity management

Running workloads in the cloud requires controlling access to environments, enabling a set of permissions, and leveraging existing corporate directories for user lifecycle management of passwords and credentials. These scenarios must also provide a way to ensure compliance with security and risk policy.

Identity management starts with a single sign-on solution to simplify and centralize credentials, enforce multi-factor authentication methods to meet security requirements, use of privileges to gain access, and detection of insecure policies and unauthorized access.

For information about the services, solutions, and APN Partners for managing identity and access, see Identity management (p. 4).

Network management

To set up and maintain cloud environments effectively, customers need a way to connect cloud workloads to enterprise networks users and applications. Customers might also need to publish applications to the internet or to manage connections from cloud to the internet.

Network management must scale for enterprise-wide environments in order to configure, manage, and coordinate AWS resources. The network connections must be monitored to ensure they are deployed correctly while providing visibility to operations and traffic flow. Access from the internet and the edge must be monitored for threats while providing the ability to do forensics and analysis while protecting data and applications. Network resources must be managed and allocated to preserve capacity and control bandwidth costs.

For information about the services, solutions, and APN Partners in network management, see Network management (p. 6).

Security information and event management (SIEM)

Customers require in-depth visibility into the security of their infrastructure and applications. Achieving this level of visibility requires the collection of logs and audit trails, the preservation of these logs for analysis and reporting, supported by the capability of real-time reporting with correlation of events, and analysis of those events.

Security information and events must be retained in an immutable form to support forensic analysis, meet service agreements for issue resolution, and satisfy business requirements of minimizing downtime and provide automated analysis and notification of common patterns.

For information about the services, solutions, and APN Partners for security information and event management, see Security information and event management (SIEM) (p. 10).

Monitoring and observability

In a cloud environment, customers need in-depth visibility into every resource across their entire global environment. Similar to SIEM, monitoring and observability also supports the ability to know if the technology environment is operationally healthy and available.

A key objective for this scenario includes the ability to deploy a consistent solution for all application teams to standardize an operational view, and to quickly onboard new applications. Meet target service level requirements for the business, including notification to the right teams of when an application or resource is not meeting control, operational, or financial targets. Customers desire consistent tools across all applications and resources to provide a consistent view, streamline communications and monitoring tasks, while simplifying monitoring processes.

For information about the services, solutions, and APN Partners in monitoring and observability, see Monitoring and observability (p. 8).

Cost management and governance

Customers allocate a budget and financial resources to capture a return on investment on cloud projects, to drive down technology costs, or to acquire new business capabilities and new product features.

To do this effectively, customers must track and monitor the cost of cloud technology, including additional costs including staffing and licenses in order to validate the return on investment. As customers grow their cloud footprint, they require visibility into resource consumption and the ability to manage costs across their enterprise-wide environments.

For information about the services, solutions, and APN Partners in cost management and governance, see Cost management and governance (p. 12).

Service management

Customers provide cloud resources and infrastructure to internal teams and application developers. Internal teams should have a way to request resources, while also notifying and being notified about incidents and problems. Customers must be able to know about provisioned assets and report on their application portfolio including infrastructure, resources, and licenses.

Service management helps organize manage service requests, changes, incidents, problems, and overall asset management. Enterprise customers need a consistent set of service management processes across their hybrid technology landscape to meet management and governance requirements. Customers must ensure that resources being provisioned are compliant.

For information about the services, solutions, and APN Partners in service management, see Service management (p. 14).

Identity management

Effective identity management is enabled by AWS services, solutions, and APN Partners that provide single sign-on solutions, credential management integration with corporate directories, and multi-factor authentication methods, with enforcement for the use of permissions to gain access.

Here we highlight APN Partners and published solutions that integrate with AWS services, such as AWS Identity and Access Management (IAM) and AWS Single Sign-On. These we will be combined into a complete view when the Management and Governance Lens is published.

AWS service solutions

- AWS Control Tower
- AWS Identity and Access Management (IAM)
- AWS Marketplace
- AWS Single Sign-On
- AWS Organizations

Many independent software vendors (ISVs) have developed integrations with these AWS services, allowing customers to enable their solution for multi-account AWS environments, available to be entitled in AWS Marketplace.

Existing APN Partners and solutions

Customers can now connect their **Okta Identity Cloud** to AWS Single Sign-On (AWS SSO) once, manage access to AWS centrally in AWS SSO, and enable end users to sign in using Okta to access all their assigned AWS accounts through AWS Organizations. The integration helps customers simplify AWS access management across multiple accounts while maintaining familiar Okta experiences for administrators who manage identities, and for end users as they sign in. AWS SSO and Okta Identity Cloud use standards-based automation to provision users and groups into AWS SSO, saving administration time and increasing security. For more information, click here.

OneLogin cloud-based Identity and Access Management (IAM) enables IT teams to centrally manage and provision access to AWS resources. Whether you're newly migrating to AWS or an Enterprise user, integrating Control Tower with OneLogin ensures you can easily and securely scale your enterprise-wide environments and IAM permissions. For more information, click here.

Ping's Workforce360 solution provides central authentication services to connect employees across any application, directory, and situation. By providing authentication for all end users and identities in customer environments, Ping can eliminate authentication silos, and help your business increase agility. The result is a centrally managed authentication hub that provides a highly configurable, secure, and consistent experience for your workforce. For more information, click here.

This blog post shows how to configure attribute-based access control (ABAC) permissions to federate users into **AWS Systems Manager Session Manager**. We demonstrate how you can use attributes defined in external identity systems as part of the ABAC decisions within AWS, with SAML session tags. For example, you can grant access to specific managed instances based on the department that your AWS Identity and Access Management (IAM) user belongs to.

Delivery partners

Choose from our global list of APN Technology and Consulting Partners with the AWS Security Competency Identity and Access Control category which helps to define and manage user identity, access policies, and entitlements. Helps enforce business governance including, user authentication, authorization, and single sign-on.

The AWS Professional Services Security, Risk, and Compliance practice helps customers develop the confidence and technical ability to migrate the most sensitive workloads to the cloud.

Network management

To set up and maintain cloud environments effectively, organizations need network management solutions that scale in an enterprise-wide environment to configure, manage, and coordinate AWS resources automatically.

Here we highlight APN Partners and published solutions that are integrated with AWS services, such as AWS Transit Gateway and AWS Network Firewall, that will be integrated into a complete view when the Management and Governance Lens is published.

AWS service solutions

- AWS Transit Gateway
- AWS Network Firewall
- AWS Control Tower
- AWS Marketplace
- AWS Organizations

Many ISVs have developed integrations with these AWS services, allowing customers to enable their solution for multi-account AWS environments, available to be entitled in AWS Marketplace.

Existing APN Partners and solutions

This pattern describes the simplest configuration in which **AWS Transit Gateway** can be used to connect an on-premises network to virtual private clouds (VPCs) in multiple AWS accounts within an AWS Region. Using this setup, you can establish a hybrid network that connects multiple VPC networks in a Region and an on-premises network. This is accomplished by using a transit gateway and a virtual private network (VPN) connection to the on-premises network. For more information, click here.

Amazon Virtual Private Cloud (Amazon VPC) provides customers with the ability to create as many virtual networks as they need, as well as different options for connecting those networks to each other and to non-AWS infrastructure. One common strategy for connecting multiple VPCs with remote networks is to implement a hub-and-spoke network topology in each Region that routes all traffic through a network transit center using AWS Transit Gateway or a transit VPC. Another common strategy is to create a meshed network that uses individual connections between all networks. Both approaches can create an efficient and available transit network, each offering specific benefits and tradeoffs for different business needs. For more information, click here.

Automate and centralize **Amazon VPC Flow Logs** for monitoring, troubleshooting, anomaly detection, or archival in a multi-account environment using AWS Control Tower for multi-account governance and built-in centralized logging with AWS CloudTrail and AWS Config. Using this solution, you can manage VPC Flow Logs across multiple accounts with self-service automation and periodic consistency checking. For more information, click here.

Automate your network setup in AWS Control Tower using **Aviatrix**. This solution uses the Aviatrix Platform to provide networking functionality and serve as a network factory for newly provisioned accounts through Account Factory in AWS Control Tower. It also can enroll existing ones as managed accounts using the Enroll Existing Account Functionality. For more information click here.

This Quick Start automatically deploys an **Aviatrix Controller** for enabling Aviatrix Orchestrator for AWS Transit Gateway in a new or existing virtual private cloud (VPC) in the AWS Cloud. For more information, click here.

This Quick Start builds a highly available, secure Fully Qualified Domain Name (FQDN) Egress Filtering service in the AWS Cloud in about 10 minutes. It automatically deploys an **Aviatrix Controller** for enabling Egress Filtering in a new or existing virtual private cloud (VPC). One important network security measure is to effectively control inbound (ingress) and outbound (egress) VPC network traffic, in order to distinguish between legitimate and illegitimate requests. With this Quick Start, you can connect to VPCs in the AWS Cloud with enhanced security, and access your Amazon Elastic Compute Cloud (Amazon EC2) instances, applications, and services. The Aviatrix Controller deploys Aviatrix gateways in your VPCs, and configures egress security policies across all gateways. For more information, click here.

This Quick Start deploys an **F5 BIG-IP Virtual Edition (VE)** cluster in the AWS Cloud in about 30 minutes. For more information, click here.

This Quick Start automatically deploys an outbound web filtering proxy in the AWS Cloud, using the **Sophos Unified Threat Management (UTM)** virtual appliance. The Quick Start also uses Sophos Outbound Gateway to extend security to multiple virtual private clouds (VPCs). For more information, click here.

This Quick Start automatically deploys **Citrix Web App Firewall (WAF)** for high availability (HA) in the AWS Cloud. Citrix WAF is a firewall that protects web applications and sites from both known and unknown attacks, including application-layer and zero-day threats. Citrix WAF is positioned in front of a web server, monitoring web traffic before it reaches the web application. For more information, click here.

Delivery partners

Choose from our global list of APN Technology and Consulting Partners with the AWS Security Competency Network and Infrastructure Security including network inspection designed to detect and protect your workloads from malicious or unauthorized traffic.

The AWS Professional Services Management and Governance Practice helps deploy automated, robust, agile, IT operations and governance capabilities for the cloud.

Monitoring and observability

In a cloud environment, customers need in-depth visibility into every resource across multiple accounts and Regions. To set up and maintain cloud environments effectively, companies need monitoring and observability solutions that scale in an enterprise-wide environments in order to have complete visibility and insights in real time.

Here we highlight APN Partners and published solutions that are integrated with AWS services, such as AWS Control Tower, AWS Config, Amazon CloudWatch, and AWS Organizations, that will be integrated into a complete view when the Management and Governance Lens is published.

AWS service solutions

- AWS Control Tower
- AWS Config
- Amazon CloudWatch
- AWS Marketplace
- AWS Organizations

Many ISVs have developed integrations with these AWS services, allowing customers to enable their solution for multi-account AWS environments, available to be entitled in AWS Marketplace.

Existing APN Partners and solutions

Check Point CloudGuard is a comprehensive cloud native security platform for visibility, workload protection, and posture management of cloud workloads and services. For more information, click here.

Datadog Pro is a unified monitoring platform with infrastructure monitoring, application performance monitoring, log management, user experience (UX) monitoring, and more. By bringing together data from distributed sources, it provides a consolidated view across AWS environments to enhance your cloud health, work, and performance. For more information, click here.

Dynatrace provides software intelligence to simplify cloud complexity. With automatic and intelligent observability at scale, it delivers precise answers about the performance of cloud platform environments. It seamlessly integrates with AWS Control Tower and securely governs AWS accounts as soon as they are created. A smart baselining capability adapts dynamically and monitors the performance of your environments in real time. For more information, click here.

New Relic One includes: Telemetry Data Platform to ingest, analyze, and alert on all your metrics, events, logs, and traces, full-stack observability to quickly visualize and troubleshoot your entire software stack in one connected experience, applied intelligence to automatically detect anomalies, correlate issues and reduce alert noise. For more information, click here.

Delivery partners

APN Partners in the AWS Cloud Management Tools (CMT) Competency Cloud Governance category aim to simplify the management of AWS resources. They provide policy driven guardrails to track, report, alert, and act on configuration changes and non-compliant resources or actions. They easily integrate with AWS management tools and external third-party solutions to drive governance of a customer's cloud resources.

APN Partners in the AWS Devops Competency Monitoring, Logging, and Performance category analyze logs and monitor your application and infrastructure performance to ensure real-time visibility, insights, and operational health.

The AWS Professional Services Management and Governance Practice helps deploy automated, robust, agile, IT operations and governance capabilities for the cloud.

Security information and event management (SIEM)

Customers require in-depth visibility into the security of their infrastructure and applications. Achieving this level of visibility requires the collection of logs and audit trails, the preservation of these logs for analysis and reporting, supported by the capability of real-time reporting with correlation of events, and analysis of those events. Security information and events must be retained in an immutable form to support forensic analysis, meet service agreements for issue resolution, and satisfy business requirements of minimizing downtime and provide automated analysis and notification of common patterns.

Here we have highlight APN Partners and published solutions that are integrated with AWS services, such as AWS Control Tower, AWS Config, AWS CloudTrail and AWS Security Hub, that will be integrated into a complete view when the Management and Governance Lens is published.

AWS service solutions

- AWS Control Tower
- AWS Config
- AWS CloudTrail
- AWS Security Hub
- Amazon GuardDuty
- AWS Marketplace

Many ISVs have developed integrations with these AWS services, allowing customers to enable their solution for multi-account AWS environments, available to be entitled in AWS Marketplace.

Existing APN Partners and solutions

New Relic One includes: Telemetry Data Platform to ingest, analyze, and alert on all your metrics, events, logs, and traces, full-stack observability to quickly visualize and troubleshoot your entire software stack in one connected experience, applied intelligence to automatically detect anomalies, correlate issues and reduce alert noise. For more information, click here.

Splunk's Grand Central interfaces with the AWS Organizations API to gather all the member accounts within your organization. It uses AWS CloudFormation to deploy StackSets on OUs. The StackSets enable the member accounts to send logs back to Splunk for centralized logging and analysis using AWS services. For more information, click here.

Sumo Logic Security Integration on AWS. This Quick Start automatically deploys Sumo Logic Security Integrations in the AWS Cloud. Sumo Logic is focused on continuous intelligence, a new category of software that addresses data challenges presented by digital transformations, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform automates the collection, ingestion, and analysis of applications, infrastructure, security, and Internet of Things (IoT) data to derive actionable insights. Similar to security information and event management (SIEM) software, Sumo Logic uses apps to collect security events generated by AWS and other security services to provide an aggregate view of overall security and compliance posture. This Quick Start deployment is for users who want to set up and configure the Sumo Logic console for 12 AWS services that provide security analytics. For more information, click here.

Reduce complexity and risk, enhance your security posture while saving time and reducing operational burden by automating **AWS Security Hub** enablement and configuration in an **AWS Control Tower** multi-account managed environment using **AWS Control Tower lifecycle events**. This solution also enables and configures AWS Security Hub on any new account provisioned or updated from the Account Factory and runs a scheduled task to ensure that all accounts stay enabled. For more information, click here.

AWS Security Hub Automated Response and Remediation is an add-on solution that works with AWS Security Hub to provide a ready-to-deploy architecture and a library of automated playbooks. The solution makes it easier for AWS Security Hub customers to resolve common security findings and to improve their security posture in AWS. For more information, click here.

Delivery partners

Choose from our global list of APN Technology and Consulting Partners with the AWS Security Competency Logging, Monitoring SIEM, Threat Detection, and Analytics category that helps customers enable and configure centralized logging, reporting, and analysis of logs to provide visibility and security insights.

AWS Professional Services Security, Risk, and Compliance practice helps customers develop the confidence and technical ability to migrate the most sensitive workloads to the cloud.

Cost management and governance

Customers allocate a budget and financial resources to capture a return on investment on cloud projects, to drive down technology costs, or to acquire new business capabilities and new product features.

To do this effectively, customers must track and monitor the cost of cloud technology, including additional costs including staffing and licenses in order to validate the return on investment. As customers grow their cloud footprint, they require visibility into resource consumption and the ability to manage cost across their environments.

Here we highlight published AWS services, APN Partners, and solutions that run on AWS, such as AWS Cost and Usage Report, AWS Cost Explorer, and AWS Trusted Advisor, that will be integrated into a complete view when the Management and Governance Lens is published.

AWS service solutions

- AWS Budgets
- AWS Cost Explorer
- AWS Cost & Usage report
- AWS Cost Categories
- AWS Marketplace
- AWS Service Catalog
- AWS Trusted Advisor
- Cost Allocation Tags

Many ISVs have developed integrations with these AWS services, allowing customers to enable their solution for multi-account AWS environments, available to be entitled in AWS Marketplace.

Existing APN Partners and solutions

Apptio is a leading provider of cloud-based Technology Business Management (TBM) software that helps CIOs manage the business of IT. Apptio's suite of applications use business analytics to provide facts and insights about technology cost, value, and quality, so IT leaders can make faster, data-driven decisions. The purpose-built applications help companies align technology spend to the business. For more information, click here.

CloudHealth by VMware gives customers complete visibility into cloud and container costs, usage, and performance, so that you can deliver higher quality products faster, while keeping costs under control across thousands of resource deployments. For more information, click here.

CloudCheckr unifies disparate data sources to provide immediate and actionable insights. These insights allow end users to achieve significant cost savings, while ensuring the highest level of AWS security and compliance with AWS Organizations. When integrated with AWS Control Tower, end users can quickly create new AWS accounts and seamlessly apply a multi-functional toolkit of cloud governance solutions. For more information, click here.

Spot by NetApp's solution allows end users to fully leverage Amazon EC2 Spot Instances and reserved capacity without operational overhead and complexity. Spot by NetApp automates and optimizes your AWS infrastructure delivering SLA-backed availability and performance at the lowest possible cost. Machine learning and application-driven scaling enables you to run any workload, providing an optimal blend of Savings Plans, Reserved Instances, Spot Instances, and On-Demand Instances. For more information, click here.

Extend a self-managed Active Directory to AWS Control Tower. One common use case for customers during their early cloud journey is to use existing identity service such as Microsoft Active Directory. This blog post shows you how to set up AWS Control Tower to delegate user authentication to a self-managed Microsoft Active Directory using AWS Managed Microsoft AD. For more information, click here.

Delivery partners

APN Partners in the AWS Cloud Management Tools (CMT) Competency Resource & Cost Optimization category help customers gain visibility into their AWS accounts and see exact workload costs, resource utilization, chargebacks, and more. Once cost visibility is achieved, APN Partner solutions provide resource and cost optimization recommendations to help customers maximize their AWS investment.

The AWS Professional Services Advisory practice helps customers achieve organizational change and tangible business outcomes from adopting the AWS Cloud.

Service management

Service management helps organize manage service requests, changes, incidents, problems, and overall asset management. Customers need a consistent set of service management processes across their hybrid technology landscape to meet management and governance requirements. Customers must ensure that resources being provisioned are compliant. To optimize automation, they must have a Configuration Management Database (CMDB) that acts as a single source of truth for all business services and supporting technology resources.

Here we highlight APN Partners and published solutions that are integrated with AWS services, such as AWS Service Catalog and the AWS Service Management Connector, that will be integrated into a complete view when the Management and Governance Lens is published.

AWS service solutions

- AWS Config
- AWS Service Catalog
- AWS Service Management Connector
- AWS Systems Manager
- AWS Organizations

Many ISVs have developed integrations with these AWS services, allowing customers to enable their solution for multi-account AWS environments, available to be entitled in AWS Marketplace.

Existing APN Partners and solutions

To help customers integrate provisioning secure, compliant, and pre-approved AWS products into their **ServiceNow** portal, AWS created the AWS Service Management Connector for ServiceNow (formerly the AWS Service Catalog Connector). The AWS Service Management Connector for ServiceNow enables ServiceNow end users to provision, manage, and operate AWS resources natively through ServiceNow. For more information, click here.

The AWS Service Management Connector for **Jira Service Management** allows Jira Service Management end-users to provision, manage, and operate AWS resources natively through Atlassian's Jira Service Management. Jira Service Management administrators can provide pre-approved, secured and governed AWS resources to end-users through AWS Service Catalog, create and manage operational items through AWS Systems Manager OpsCenter, execute automation playbooks through AWS Systems Manager Automation and track resources in a configuration item view powered by AWS Config seamlessly on the Jira Service Management with the AWS Service Management Connector. For more information, click here.

Delivery partners

APN Partners in the AWS Cloud Management Tools (CMT) Competency Cloud Governance category aim to simplify the management of AWS resources. They provide policy driven guardrails to track, report, alert, and act on configuration changes and non-compliant resources or actions. They easily integrate with AWS management tools and external third-party solutions to drive governance of a customer's cloud resources.

The AWS Professional Services Management and Governance Practice helps deploy automated, robust, agile, IT operations and governance capabilities for the cloud.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.