Introduction to AWS GoldBase

A Solution to Automate Security, Compliance, and Governance in AWS

October 2015
Notice

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. 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.
Abstract

The AWS GoldBase solution is designed to enable customers create secure and compliant workloads in AWS, as well as reduce the complexity of maintaining secure baselines at scale as customer environments transform over time. This solution provides many benefits, including the ability to securely deploy recommended, reliable, and secure resources in AWS. AWS GoldBase is an automated reference architecture, following security-leading practices and supporting multiple customer compliance requirements (e.g. FISMA, PCI, CJIS, FFIEC, HIPAA, etc.). This solution allows for a repeatable process that you can use to ensure compliant configuration of AWS resources in the cloud, while reducing the time needed to approve applications for production use.
Architecting for Compliance in AWS

Compliance in the Cloud

Compliance is a broad term used within technology and business. The simplest definition of *comply* is to “meet specified standards.” Ensuring compliance in the cloud includes adhering to the following standards:

- Third-party Security Frameworks
- Established policies within the customer organization
- Security-leading practices across industry verticals

AWS GoldBase provides you with validated, automated and recommended reference architecture, which has been validated against specific security and compliance requirements in mind (examples of which are listed in the next section). Within the context of deploying applications on AWS, AWS GoldBase incorporates advanced, leading practices for ensuring integrity, availability, confidentiality, and security at scale through predictable, repeatable and verifiable security configurations.

Compliance Standards

The [AWS Shared Responsibility](https://aws.amazon.com/sharedresponsibility) model outlines the responsibilities for security and compliance in customer environments. When deploying systems in the AWS Cloud, AWS shares security responsibilities with you. AWS manages the underlying infrastructure, and you are responsible for securing anything you deploy in AWS. AWS is highly accredited, which means that an auditor has verified that specific security controls are in place and operating as intended.

To help you meet specific government, industry, and company security standards and regulations, AWS provides certification reports that describe how the AWS Cloud infrastructure meets the requirements of an extensive list of global security standards, including: [ISO 27001](https://www.iso.org/iso-27001-information-security.html), [SOC](https://cybersecurity.google.com/soc), the [PCI Data Security Standard](https://www.pcisecuritystandards.org/), [FedRAMP](https://fedramp.gov), the [Australian Signals Directorate (ASD) Information Security Manual](https://csrc.nist.gov/CS/ divs/sp/800-53#asdm), and the [Singapore Multi-Tier Cloud Security Standard](https://www.mctasg.gov.sg/mtcs/mtcs-ss-584-standard) (MTCS SS 584).

Examples of security standards which AWS GoldBase can support:

- [FedRAMP](https://fedramp.gov) (SM) - AWS has achieved two Agency Authority to Operate (ATOs) under the Federal Risk and Authorization Management Program
FedRAMP at the Moderate impact level. All U.S. government agencies can leverage the AWS Agency ATO packages stored in the FedRAMP repository to evaluate AWS for their applications and workloads, provide authorizations to use AWS, and transition workloads into the AWS environment.

- **The Department of Defense (DoD) Cloud Security Model (CSM)** - Provides a formalized assessment and authorization process for cloud service providers (CSPs) to gain a DoD Provisional Authorization, which can subsequently be leveraged by DoD customers.

- **HIPAA** - AWS enables covered entities and their business associates subject to the [U.S. Health Insurance Portability and Accountability Act](https://healthcare.gov/hipaa/) (HIPAA) to leverage the AWS environment to process, maintain, and store protected health information. Additionally, AWS, as of July 2013, is able to sign business associate agreements (BAA) with such customers.

- **ISO 27001** - AWS is [ISO 27001 certified](https://aws.amazon.com/about-aws/compliance/iso27001/) under the International Organization for Standardization (ISO) 27001 standard. ISO 27001 is a widely adopted global security standard that outlines the requirements for information security management systems.

- **CJIS Security Policy** – AWS’s cloud infrastructure has been architected to be one of the most flexible and secure cloud computing environments available for storing criminal justice information. Our architecture provides an extremely scalable, highly-reliable platform enabling customers to deploy applications to include Criminal Justice Information Services (CJIS) workloads according to the [CJIS Security Policy](https://abi.cms.gov/PP/501a553f-6c66-4827-961a-90114d150a36).

- **PCI DSS** - AWS is Level 1 compliant under the [Payment Card Industry (PCI) Data Security Standard (DSS)](https://aws.amazon.com/about-aws/compliance/security/pci-dss/index.html). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud.

- **EU Data Protection Directive** - The Article 29 Working Party has approved the [AWS Data Processing Agreement](https://aws.amazon.com/about-aws/compliance/data-protection-agreement/), which includes the Model Clauses. The Article 29 Working Party has found that the AWS Data Processing Agreement meets the requirements of the Directive with respect to Model Clauses.
AWS GoldBase

AWS GoldBase is a solution to enable customers to streamline, automate, and implement secure baselines in AWS, from initial design to operational secure readiness. AWS GoldBase incorporates the expertise of AWS solutions architects, as well as security and compliance personnel, to build a secure and reliable architecture in an easy-to-implement package through automation.

AWS GoldBase Solution

The AWS GoldBase solution includes the following items for customer use:

- Security Control Responsibility Matrix (CRM)
- Architecture diagrams
- AWS CloudFormation templates
- User Guides and deployment instructions

Benefits

- Reduced cost and time for secure deployment
- Reliable security controls adherence
- Transparency, compliance and auditability
- Real time risk management (e.g. continuous monitoring)
- Constrained standardization for multiple security frameworks

Security Controls Responsibility Matrix (CRM)

The AWS GoldBase solution includes a security CRM, which maps features and resources to specific security controls requirements. Security, compliance and audit personnel can leverage these documents as a reference for making certification and accrediting of systems in AWS easier. The matrix outlines control implementation reference architecture and evidence examples, which meets the security control “risk mitigation” for the AWS customer environment.
Figure 1: NIST SP 800-53 rev. 4 control security control matrix

Architectural Diagrams
Architectural diagrams are included with the AWS GoldBase solution. These diagrams illustrate and document the design. They provide a visual reference that demonstrates the components deployed by the AWS CloudFormation templates. These diagrams accompany the description of security features implemented by the AWS GoldBase templates.

Figure 2: Architectural diagrams for AWS GoldBase

AWS CloudFormation Templates
The AWS GoldBase offering includes AWS CloudFormation templates, which enable recommended automated deployments of a secure and compliant baseline architectures. The default AWS GoldBase solution consists of four JSON (JavaScript Object Notation) template files, which can be launched as stacks using the AWS CloudFormation service.

What is an AWS CloudFormation Stack?
When you use AWS CloudFormation, you manage related resources as a single unit called a stack. In other words, you create, update, and delete a collection of resources by creating, updating, and deleting stacks. All the resources in a stack are defined by the stack’s AWS CloudFormation template.
To update resources, you first modify the stack templates and then update your stack by submitting the modified template. You can work with stacks by using the AWS CloudFormation console, API, or AWS CLI.

<table>
<thead>
<tr>
<th>Server/Data Stack</th>
<th>Operating System Deployment</th>
<th>Fault Tolerance Deployment</th>
<th>Data Container Deployment</th>
<th>Application Services Deployment</th>
<th>EC2 Instances, Availability Zones, RDS Databases and Autoscaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Stack</td>
<td>Management Network</td>
<td>Development Network</td>
<td>Production Network</td>
<td></td>
<td>VPCs, Subnets, Gateways, Route Tables, NACLs</td>
</tr>
<tr>
<td>Access Stack</td>
<td>Access Management and Resource constraints</td>
<td></td>
<td></td>
<td></td>
<td>Users, Groups &amp; Roles, CloudFormation access and Service Catalog constraints</td>
</tr>
</tbody>
</table>

**Figure 3:** AWS CloudFormation stacks

This solution provides modularity capabilities, which enables you to deploy a subset of resources as needed. The design facilitates reusability of templates for multiple use cases. Additionally, for greater control and security, AWS CloudFormation templates can be imported into AWS Service Catalog as portfolios and/or products to enable centralized management of resources to support consistent governance, security and compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

**User Guide with Deployment Instructions**

The AWS GoldBase solution includes a user guides, which provide step-by-step instructions on how to deploy services using the AWS CloudFormation templates, as well as instructions for creating AWS Service Catalogs products and portfolios and for enabling versioning to support automatic distribution to all users who have access to the product and portfolios. Additionally, AWS Service Catalog customers can apply AWS Identity and Access Management (IAM) permissions to control who can view and modify your products and portfolios as, well as apply constraints to restrict specific AWS resources.
AWS GoldBase Delivery

AWS GoldBase packages can be customized to meet multiple regulated, security and compliance frameworks. To get started or to get more information on the AWS GoldBase solution email: aws-goldbase@amazon.com.

Conclusion

The AWS GoldBase solution was designed to create a recommended, secure baseline for customer environments across multiple security and compliance frameworks, standards and regulatory authorities. The result enables an automated, secure and auditable baseline. The benefits reduce costs, time, and effort to deploy secure and compliant capabilities in AWS using leading practices in security by design architecture.

The AWS GoldBase solution is available for public sector, enterprise and other regulated customer workloads. It can be customized by customers directly or through our experienced architects, engineers, and IT transformation leads, who work alongside your staff and/or via trusted partners to focus on high-quality delivery and sustainable knowledge transfer.

The AWS GoldBase solution is the evolution of a secure customer baseline of resources in AWS. It supports multiple leading security-practices and directly implements several customer compliance requirements (e.g. Access Control, Firewall rules, Audit & logging, etc.) which can relied upon, verified and reported on within a “real-time” risk management approach.
Further Reading

- AWS Compliance Center: http://aws.amazon.com/compliance
- AWS Sales and Business Development: http://aws.amazon.com/compliance/contact/
- Government and Education on AWS: http://aws.amazon.com/government-education/
- AWS Professional Services: http://aws.amazon.com/professional-services/