# AWS Architecture and Security Recommendations for FedRAMP[SM] Compliance

***Accelerate time to compliance***

*Brett Miller*

*Andrew McDermott*

*Hart Rossman*

*December 2014*

# Contents

# Purpose:

Moving from traditional datacenters to the AWS cloud presents a real opportunity for workload owners to select from over 200 different security features (Figure 1 - AWS Enterprise Security Reference ) that AWS provides. "What do I need to implement in order to build a secure and compliant system that can attain an ATO from my DAA?" is a common question that government customers ask. In many cases, organizations do not possess a workforce with the necessary real-world experience required to make decision makers feel comfortable with their move to the AWS cloud. This can make it seem challenging for customers to quickly transition to the cloud and start realizing the cost benefits, increased scalability, and improved availability that the AWS cloud can provide.

# AWS Security Architecture

Amazon's shared security model clearly delineates the security responsibility that falls under the customer's purview, but does not provide detailed guidance on building secure systems in accordance with FedRAMP guidelines. This document is designed to provide an additional layer of guidance that can help organizations "right-size" the security approach so they can migrate faster while reducing compliance related security gaps in their system. This document is not meant to be prescriptive or comprehensive, but instead discusses best practices and illustrates how customers can configure and implement AWS services to make security and compliance easier. Regardless of the initial size or scope of the workload, this document will provide foundational guidance and direction so that organizations can design their AWS infrastructures to be scalable, secure, manageable, and compliant.

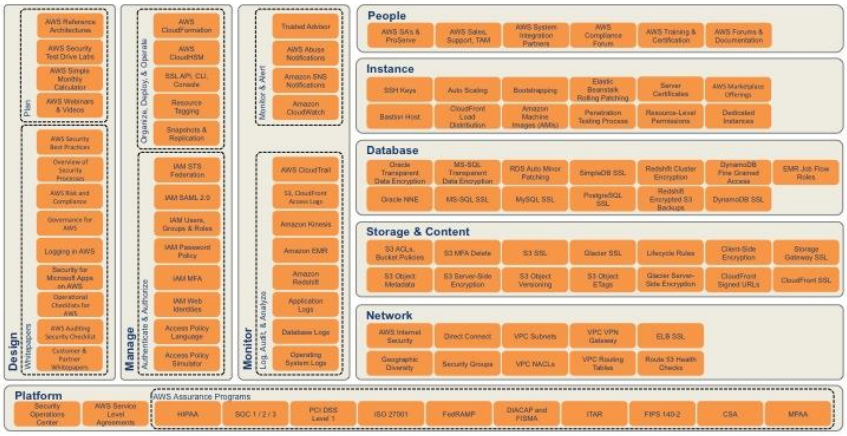



**Figure 1 - AWS Enterprise Security Reference Architecture**

This document only covers an introduction to the security controls and mechanisms AWS can provide. If additional and specific guidance is required, AWS's Security Assurance, Solutions Architects, and Professional Services teams have service offerings that can dive deeply into an organization's security and compliance challenges to help accelerate the ATO process.

- Cloud Governance Consultation

- Enterprise Compliance Readiness Assessment
- Security and Compliance Workshops
- Security Architecture Assessments

This guide is designed to augment the library of AWS best practice guides and provide additional guidance/justification as to why a certain design consideration should be made. This document will not cover all aspects of operating a fault-tolerant, secure, and documented system. It will address the foundational building blocks and design considerations with running a workload on AWS while achieving an ATO. Additionally, even though this document will address a broad range of AWS services, the current services within AWS' FedRAMP Agency ATOs are limited to Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), and Amazon Redshift within the AWS GovCloud (US) Region and AWS US East/West Regions. More services are being added to the FedRAMP authorization over time, please see the AWS FedRAMP FAQ for current information regarding the AWS FedRAMP authorization: http://aws.amazon.com/compliance/fedramp-faqs/.

Since a three-tier web based application is the most common design pattern we observe today, we will assume the following requirements throughout this document:

- Users are on the public Internet and access resources via web browser.
- Web portal and tiers must be highly available.
- Compliance to FedRAMP 800-53v3 Moderate security controls
- Site must be designed to be scalable and redundant.
- Strong isolation and visibility/control between functional tiers
- Dedicated development and production environments
- Centralized and controlled administrative interfaces

For illustrative purposes, AWS has designed a basic sample architecture (Figure 2 - Sample Reference ) that meets the requirements above and will be referenced throughout this document. **NOTE: This is only sample architecture and does not reflect any particular customer or set of requirements.**

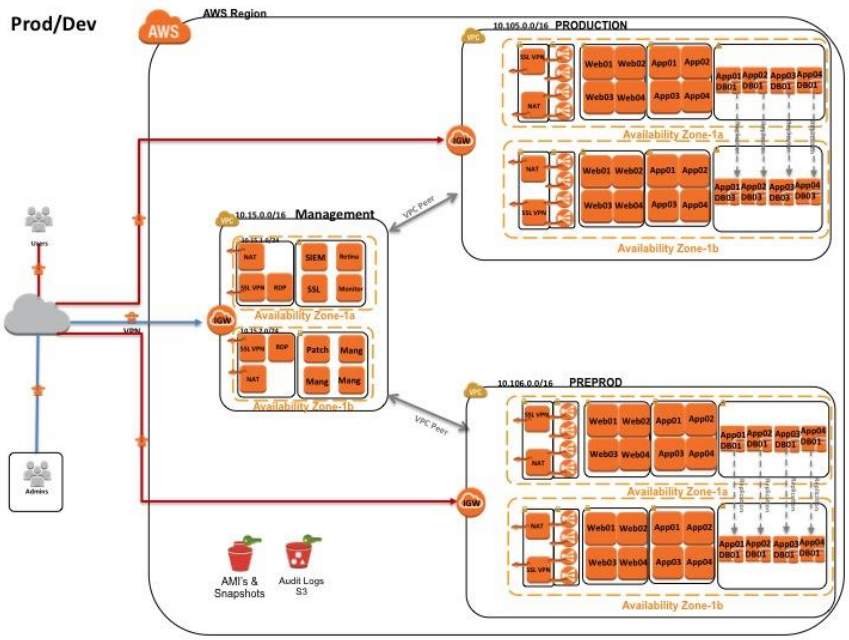



**Figure 2 - Sample Reference Architecture**

Throughout this document, AWS includes the applicable 800-53v3 security controls that can be partially or completely satisfied by architecting the solution using the proposed design and incorporating the recommended AWS security mechanisms. **It is essential to understand that the controls documented below can help satisfy the security requirements at the guest OS level, which is the responsibility of the customer.**

# Architecture Designed for Scalability, Process Isolation, and Governance:

The sample reference architecture (Figure 2 - Sample Reference ) takes into consideration growth, scalability, and governance and is typical in many web portal use cases where customers require dedicated development and production environments. The sample design does not incorporate all necessary or available security services; its sole purpose is to help illustrate how AWS services can enhance the application's security posture while fulfilling 800-53v3 security controls. The core tenant of the reference design ensures security function isolation between production and development areas by implementing VPCs that have administrative rights and roles that differ from the production enclaves. This level of process isolation ensures if a problem, misconfiguration, or exploit negatively impacts the development environment, it does not impact production workloads. The dedicated management VPC isolates security and configuration management functions yet allows visibility and control of all other VPCs. Let's discuss each component separately.

# Management/Security VPC

The purpose of the security/management VPC is to isolate the security processes from the development and production environment but allow centralization of monitoring, logging, and configuration management functions. There are three major security functions provided by the management VPC: (1) remote access, (2) security monitoring, and (3) patching.

## Remote Access

The Management VPC is the area where all privileged access to all environments must pass before traversing to other areas. This centralized access will ensure all privileged access is tracked, monitored, and authorized. In this design, a bastion host is used to access all resources. A bastion host is a hardened instance used for administrative access to the customer's AWS environment. On the bastion host, two-factor authentication is configured for all access and the bastion host is hardened to the DISA STIG standards and configured to log security related access to an external service contained with the management subnet. Within the security groups that govern access to the bastion host, only authorized IP addresses are allowed to access the RDP port.

## Security Monitoring

Security monitoring is critical and required for ATO. Additionally, it provides the data to detect and respond to incidents, outages, and exploits. This design centralizes all monitoring capabilities, security management, logs, and patching. This becomes an important piece of the OPSEC process and reduces the administrative burden by duplicating security functions in other VPCs. There are three distinct functions contained within the management VPC:

- Patch Servers - Windows SUS, Red Hat Satellite, etc.
- Security information and event management servers -SIEM Monitors OS and applications centrally
- Security Scanning tools – Automated security scanning of OS, Application, and Databases

# Amazon Machine Images

An Amazon Machine Image (AMI) contains all information necessary to boot an Amazon EC2 instance with your software. An AMI is like a template of a computer's root volume. For example, an AMI might contain the software to act as a web server (Linux, Apache, and your web site) or it might contain the software to act as a Hadoop node (Linux, Hadoop, and a custom application). You launch one or more instances from an AMI. An instance might be one web server within a web server cluster or one Hadoop node. AMIs are available from a variety of sources, including:

- Official AMIs published by the organization's cloud services team
- Amazon-maintained AMIs
- Public AMIs from other organizations, available through the AWS Marketplace and Amazon EC2

- AMIs generated from imported virtual machines

# Passing User Data to the Instance

When an instance is launched, the administrator can specify user data, which is used to configure the instance. Additionally, user data can be added to the Amazon EBS-backed instances when they're stopped. Scripts placed in user data will be executed via Cloud-init. Cloud-init is an open source application built by Canonical that is used to bootstrap Linux images in a cloud computing environment such as Amazon EC2. User data is leveraged to configure an instance during launch or even run a configuration script.

# Instance Metadata

Amazon EC2 instances can access instance-specific metadata as well as data supplied when launching the instances. The data will assist in creating generic AMIs that that will be modified by configuration files supplied at launch time. For example, if you run web servers for various government organizations, they can use the same AMI and retrieve their content from the Amazon S3 bucket specified at launch. To add a new customer, create a bucket for the customer, add their content, and launch your AMI.

# CloudFormation Helper Applications

AWS CloudFormation includes a set of helper applications (cfn-init, cfn-signal, cfn-get-metadata, and cfn-hup) that are based on cloud-init. The helper applications not only provide functionality similar to cloud-init, but also allow the instance to update your metadata after the instance and applications are operational. They will update the metadata after deployment because AWS CloudFormation stores the metadata. The added flexibility does require additional setup—the administrator will create security credentials for the instance so that the instance can call the AWS CloudFormation API to retrieve the updated metadata.

Using the tools listed above along with a defined and documented CM process, administrators can deploy, patch, and scale their Amazon EC2 fleet while maintaining up-to-date and patched instances. There are two distinct methods for maintaining patched systems in AWS, baking AMIs and Bootstrapping.

# Baking AMIs

Baking AMIs is a process of preloading AMIs with the necessary patches, configuration, and software so they are completely preconfigured and ready to deploy. This practice yields results similar to building a "Golden Image," wherein the approved hardening and system configuration is contained in the AMI. In practice, bootstrapping is also used with this method in order to ensure the newly available patches are applied after the AMI was built. This process can vary, but steps to implement typically look like the following:

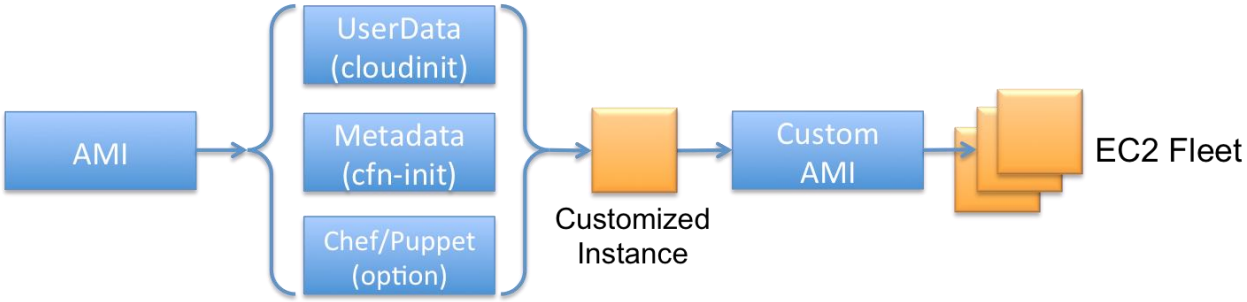



**Figure 3 Baking AMIs**

| Step | Notes |
|---|---|
| **1) Choose a base AMI** | Select your base AMI from an approved source |
| **2) Bake the base AMI** | Use any combination of approved methods and tools to customize the configuration of the instance (install packages, set configurations, copy files, etc.) |
| **3) Create a new AMI from your custom instance** | In the console, right click on the instance and choose “Create image (EBS AMI)" |
| **4) Boot new EC2 instances specifying your baked AMI** | Your instances boot quickly, and include all required configurations and software. |

# Bootstrapping

Bootstrapping is a process that allows administrators to reduce the overall amount of AMIs you maintain, by customizing each instance as it launches leveraging automation abilities provided by Amazon EC2. This process can vary, but steps to implement typically look like the following:

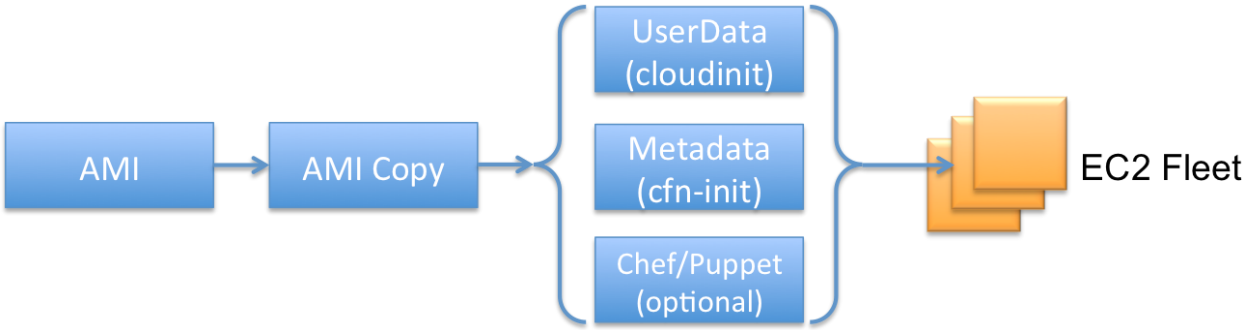


**Figure 4 - Bootstrapping AMIs**

| Step | Notes |
|---|---|
| **1) Choose a base AMI** | Select the base AMI from an approved source |
| **2) Make a copy of the base AMI** | AMIs maintained by other organizations may be disabled, rendering your instances unbootable. Create a copy first. |
| **3) Bootstrap the AMI copy** | Use any combination of approved methods and tools to automate the configuration of the instance as it boots (install packages, set configurations, copy files, etc.) |
| **4) Wait for bootstrapping to finish** | After the instances complete bootstrapping, they are ready for use. The time required for this step depends greatly on your configuration. |

Which Method is Best?

For best results and flexibility, use a combination of both methods. This provides a continuum, allowing administrators to choose between faster boot times or more change agility.

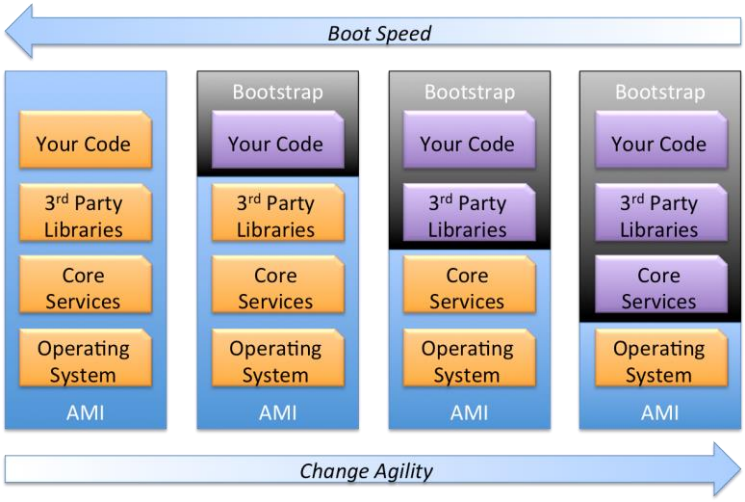



**Figure 5 - Which process is best?**

For the most flexibility, administrators could choose either option for a portion of a specific layer. For example, baking the code into the AMI that historically doesn't change very often, and bootstrap code that requires frequent upgrades or iterations.

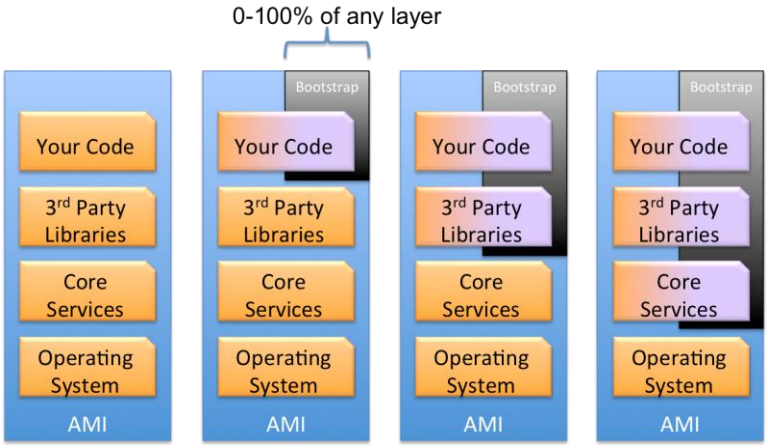



**Figure 6 - AMI baking options**

# Copying AMIs between AWS Regions

Because AMIs are region-specific, they must be copied to every region that launch instances. The AWS CLI contains a command called `aws ec2 copy-image`. It is designed to help migrate AMIs to a new Region. Run `aws ec2 copy-image help` for more details.

# Maintaining Environments

This section describes methods to upgrade and/or patch entire stacks of systems.

## The "Patch in Place" Method

In data center environments with physical systems, system administrators and operational stewards often perform patch management by applying patches to the existing systems. While often successful, this process can cause significant service disruption and can be accompanied by difficult, time consuming back-out procedures. This patch management method is still possible within AWS, in accordance with a government agency's existing procedures.

## The "Replace and Retire" Method

Cloud computing and virtualization provide new abilities enabling a patch management method sometimes referred to as "replace and retire". This process has significant advantages including the ability to:

- Build a new discrete environment in parallel with the legacy environment
- Test the patched systems in a live environment with minimal disruption
- Gradually provision load to the new environment
- Roll back to the legacy environment if required
- Maintain the older instances indefinitely as a back-out plan

# Cutting Over by Trickle Testing

The replace and retire methodology enables cloud-ready application owners to perform a large-scale, gradual cutover from legacy environments to new environments. *Trickle Testing* provides a continuum for workload distribution between the legacy and new environments, which can be much less disruptive to the user population than the older "A/B Testing" method involving a binary cut between environments (usually via a DNS record change). This process is highly automated for environments using Amazon Route 53, Amazon CloudWatch (Cloudwatch), Elastic Load Balancing, and Auto Scaling, but can also be accomplished without those features. A conceptual diagram is included below, showing an Internet-facing workload gradually moving from the legacy environment to a new environment.

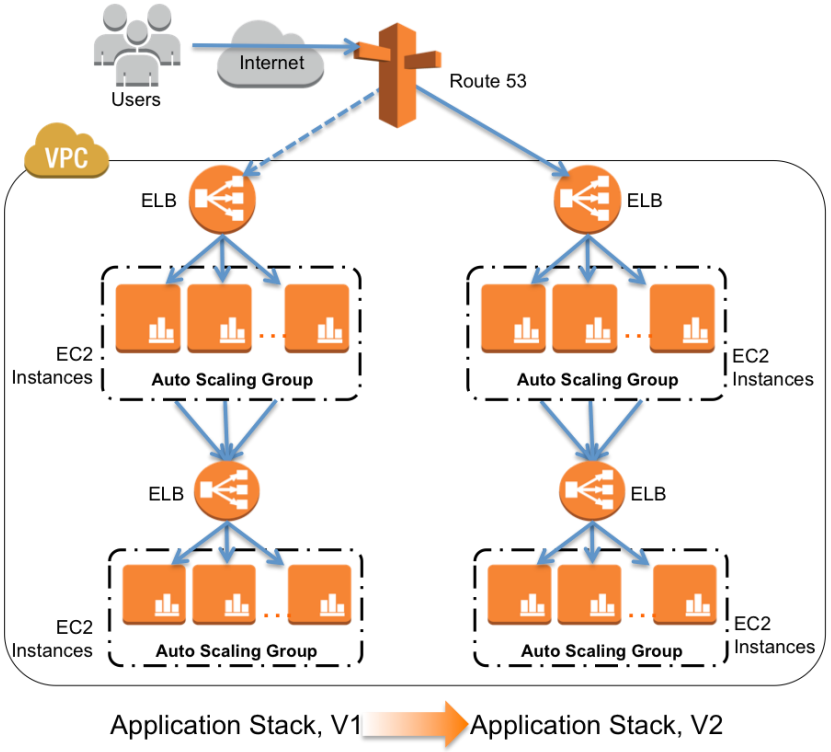
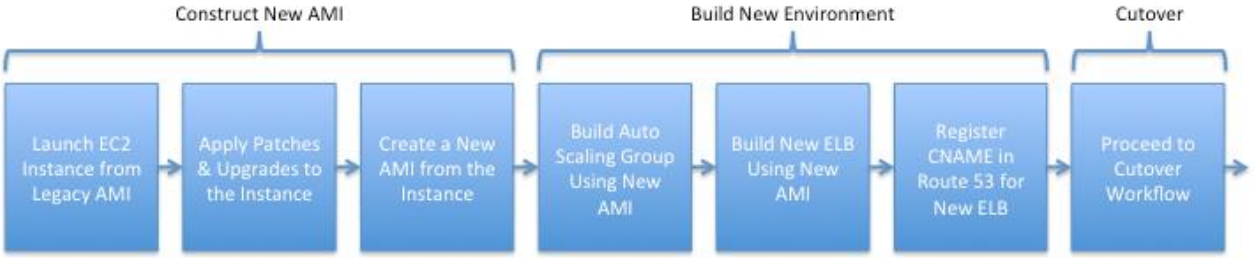


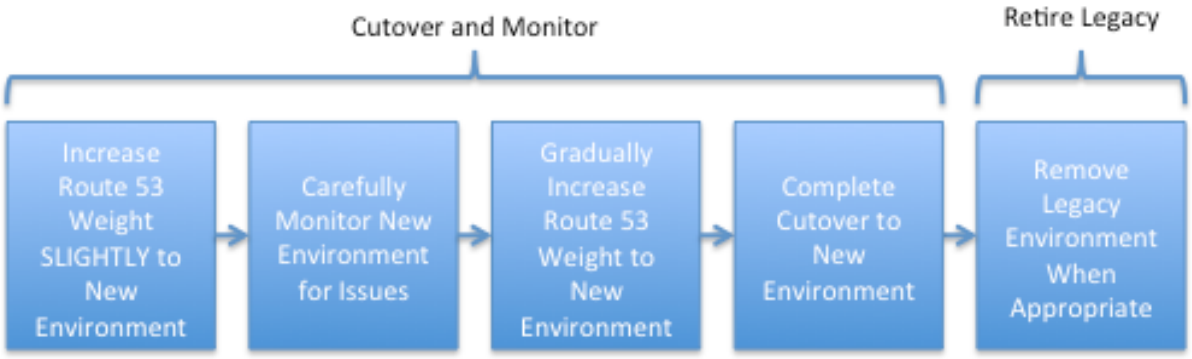

**Figure 7 - Trickle and Replace**

## Setup



The high level steps for setting up the new environment consist of constructing a new AMI, building out a new parallel environment, and preparing for the cutover.

### Cutting Over




Create or modify an Amazon Route 53 weighted resource record set to send a small portion of your workload to the new environment. Weighted resource record sets let you associate multiple answers with a single DNS name. Monitor the new environment closely for any errors or issues. If unrecoverable issues occur, simply readjust the record weighting to zero to initiate a cut back to the legacy environment. Otherwise, adjust the weighting gradually over time, sending more and more of the user population to the new environment.

CloudWatch, Elastic Load Balancing and Auto Scaling will automatically decrease the capacity of the old environment while increasing capacity in the new environment. After Route 53 is sending 100% of the load to the new environment, the legacy environment can be maintained as long as necessary as a back-out option. After it is no longer required, all resources in the legacy environment can be terminated.

For detailed information about Amazon Route 53 weighted record sets, including calculations for workload distribution probability, see the Amazon Route 53 Developer Guide (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html).

# AWS Patch Management

The shared responsibility model can relieve operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

Emergency, non-routine, and other configuration changes to existing AWS infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms for similar systems. Updates to AWS' infrastructure are done to minimize any impact on the customer and their use of the services. AWS will communicate with customers, either via email, or through the AWS Service Health Dashboard (http://status.aws.amazon.com/) when service use is likely to be adversely affected.

For more information, see Whitepaper: Overview of Security Processes (PDF) (http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

# Centralized Security and Vulnerability Scanners

Regular and automated scanning for vulnerabilities is a critical aspect for continuous monitoring strategies and is required to maintain a FedRAMP ATO. In our reference design, the security scanners such as Retina or Nessus are centrally located within a controlled subnet within the Management VPC. The scanners require unfettered access to the production subnet so they can adequately ascertain the security posture of the applications. To do this, security groups need to be written to allow only the specific IPs from the scanner to all IPs within the production subnets. This ensures regular and accurate results of all components operating within the virtual infrastructure.

**800-53 Controls satisfied by a dedicated Management/Security VPC**

| Control | Brief Description | Rationale |
|---|---|---|
| **AC-5** | The organization:<br><br>Separates duties of individuals as necessary, to prevent malevolent activity without collusion; Documents separation of duties; and Implements separation of duties through assigned information system access authorizations. | By isolating the production and development/test environments, customers can separate all duties and processes across separate VPC environments. |
| **IR-4 (1)** | The organization employs automated mechanisms to support the incident handling process. | The proposed design implements a VPC that houses several security functions including SIEM and log management. The isolated subnets support the incident response process. |
| **SC-7 (1) (2) (3)(5) (13)** | (a)Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and<br><br>(b) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.<br><br>- The organization physically allocates publicly accessible information system components to | The proposed design centralizes and authorizes access based on role and monitors all activity of users. |

| Control | Brief Description | Rationale |
|---|---|---|
| | separate sub-networks with separate physical network interfaces.<br><br>- The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.<br><br>- The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. | |

# Production VPC

As the name suggests, the production VPC incorporates all components to fully operationalize the system. Security is implemented in all layers of the networking, operating systems, applications, and databases. Security Groups and NACLS provide isolation and a "defense-in-depth" strategy to establish a combination of stateful and stateless filtering at the instance and subnet levels of the VPC. To centrally monitor privileged users from the management VPC, a peering relationship is setup so ISSOs can monitor all activities from a central location without having to write permissions on the VPC. To maximize the availability of the applications, elastic load balancers are used to distribute load and dynamically grow or shrink each tier of the system. Instances are distributed across availability zones to ensure high availability of resources. The only component within the reference architecture that does not have an ELB is the database tier. Redundancy and availability must be engineered at the database level and data replicated across AWS Availability Zones (AWS AZs). In future iterations of the design, Amazon Relational Database Service (Amazon RDS) can be introduced but currently the service is not part of AWS's FedRAMP list of approved services (https://aws.amazon.com/compliance/fedramp-faqs )

**800-53 Controls satisfied by a Dedicated Production VPC**

| Control | Brief Description | Rationale |
|---|---|---|
| **AC-5** | The organization:<br><br>Separates duties of individuals as necessary, to prevent malevolent activity without collusion.<br><br>Documents separation of duties.<br><br>Implements separation of duties through assigned information system access | By isolating the production and development/test environments, all duties and processes are distinct and controlled across two separate VPC environments. |

| Control | Brief Description | Rationale |
|---|---|---|
| | authorizations. | |
| **CM-4, CM 5 (5)** | The organization:<br>- Analyzes changes to the information system to determine potential security impacts prior to change implementation<br>- Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment. | The proposed design isolates the Production VPC from developers and other staff so configurations can be strictly enforced and maintained. |
| **CM-7** | The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services. | The proposed design only explicitly permits ports/protocol that are defined and necessary to meet operational requirements. |
| **SC-4** | The information system prevents unauthorized and unintended information transfer via shared system resources. | The design provides process isolation and controls access to all tiers of the application. |
| **SC-7 (1) (2) (3)(5) (13)** | (a)Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and(b) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.<br><br>The organization physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces.<br><br>The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. | All access to production resources are monitored and controlled via managed interfaces. All privileged access to production VPC is regulated and authorized from the management VPC. |

| Control | Brief Description | Rationale |
|---|---|---|
| | The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. | |
| **SC-32** | The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. | Security groups will provide logical separation between web tiers, data, and application components. |

# Development VPC

The development VPC is self-contained and designed to simulate the production environment. However, the development team has the flexibility to innovate quickly without the overhead of security processes that are mandatory in the production environment. The security roles are not as delineated as in the production area allowing developers to dynamically change and alter the infrastructure to meet the evolving requirements of their customer. For operational security concerns, ISSOs and other security personnel may have read-only access to the environment so they can monitor for operational issues that could negatively affect the overall security posture.

**800-53 Controls satisfied by a Dedicated Development VPC**

| Control | Brief Description | Rationale |
|---|---|---|
| **AC-5** | The organization:<br><br>Separates duties of individuals as necessary, to prevent malevolent activity without collusion.<br><br>Documents separation of duties.<br><br>Implements separation of duties through assigned information system access authorizations. | By isolating the production and development/test environments, all duties and processes are distinct and controlled across two separate VPC environments. |
| **CM-4, CM 5 (5)** | The organization:<br><br>Analyzes changes to the information system to determine potential security impacts prior to change implementation. | The proposed design isolates the Production VPC from developers and other staff in order to strictly enforce and maintain the approved production baseline. |

| Control | Brief Description | Rationale |
|---|---|---|
| | Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment. | |
| **SC-7 (1) (2) (3)(5) (13)** | (a)Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and<br><br>(b) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.<br><br>The organization physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces.<br><br>The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.<br><br>The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. | All access to development resources are monitored and controlled via managed interfaces. All privileged access to development VPC is regulated and authorized from the management VPC. |
| **SC-32** | The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. | Security groups, NACLs and subnets will provide logical separation between web tiers, data, and application components. |

# Other Considerations:

If necessary, an additional VPC could be added to isolate a pre-production environment. This environment would closely resemble the production environment but be primarily used for testing code and new security

mechanisms in a controlled and managed environment. This type of environment would be under strict configuration management control.

Architecting a secure virtual infrastructure is critical to ensure a robust security posture and is foundational to achieving an ATO. A scalable and secure VPC design will ensure the infrastructure can accommodate future growth while maintaining the organizations confidence in the security posture. If additional assistance and/or guidance is needed, contact your AWS sales rep team to setup a Professional Services Security Architecture Assessment engagement.

# Identity and Access Control

AWS Identity and Access Management (IAM) is the most important aspect of running a secure AWS environment. A solid IAM policy will enforce a "Policy of Least Privilege" while providing ISSOs the control and visibility they require to securely monitor their systems. A common and dangerous practice AWS routinely observes is customers using the master AWS account for API calls, access to the management console, etc. Best practices and experience suggests not using your master account for anything but "break glass" emergency situations. The high level activities that should be completed and documented in your SSP are outlined below: (See http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html for details):

High level IAM best practices:

1) Create individual accounts for anyone that requires access to the AWS infrastructure or APIs or use IAM federation from enterprise identity management system

2) Use groups or roles to assign permissions to IAM users

3) Enable multi factor authentication for all IAM users

4) Use roles for applications that run on EC2 instances

5) Delegate by using roles instead of sharing credentials

6) Rotate credentials regularly.

Below are the 800-53 controls that can be partially or completely satisfied when customers configure IAM to meet AWS security best practices. **NOTE:** The controls listed below cover the security requirements within the AWS account's environment, not within the guest OS or any applications deployed on it (unless explicitly stated)

**800-53 controls satisfied by IAM best practices**

| Control | Brief Description | Rationale |
|---|---|---|
| **AC-2** | The organization employs automated mechanisms to support the management of | Using the IAM best practices listed above, customers can control all |

| | | |
|---|---|---|
| **(1)(3)(7)** | information system accounts. | aspects of AWS account management. |
| **AC-3(3), AC-6(1) (2)** | - The information system automatically disables inactive accounts<br><br>- The organization:<br><br>Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and<br><br>(b) Tracks and monitors privileged role assignments.<br><br>- The organization explicitly authorizes access to [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware and security-relevant information]. | Security functions within the AWS infrastructure can explicitly be defined within IAM to include read-only permissions for ISSO functions. |
| **AC-5** | The organization:<br><br>Separates duties of individuals as necessary, to prevent malevolent activity without collusion;<br><br>Documents separation of duties; and<br><br>Implements separation of duties through assigned information system access authorizations. | By isolating the production and development/test environments, customers can separate all duties and processes across two separate VPC environments. |
| **AC-17 (4)** | The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. | With IAM, administrators can define the API calls and GUI functions every privileged user can perform within the AWS infrastructure. |
| **IA-2(1) (2)** | The information system uses multifactor authentication for network access to privileged accounts. | MFA can be configured for every privileged user that accesses or modifies the AWS infrastructure. |

| | | |
|---|---|---|
| **IA-3** | The information system uniquely identifies and authenticates before establishing a connection. [*Assignment*: o*rganization-defined list of specific and/or types of devices*] | The underlying AWS infrastructure does not permit unauthenticated privileged user access for console or API access. |
| **IA-4, IA-5** | The organization manages information system identifiers for users and devices by:<br><br>Receiving authorization from a designated organizational official to assign a user or device identifier.<br><br>Selecting an identifier that uniquely identifies an individual or device.<br><br>Assigning the user identifier to the intended party or the device identifier to the intended device;<br><br>Preventing reuse of user or device identifiers for [Assignment: organization-defined time period]; and<br><br>- The organization manages information system authenticators for users and devices by:<br><br>Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator.<br><br>Establishing initial authenticator content for authenticators defined by the organization<br><br>Ensuring that authenticators have sufficient strength of mechanism for their intended use<br><br>Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators<br><br>Changing default content of authenticators upon information system installation<br><br>Establishing minimum and maximum lifetime | Within IAM, customers can dictate the frequency of rotation/replacement of identifiers and authenticators to the AWS infrastructure. |

| | | |
|---|---|---|
| | restrictions and reuse conditions for authenticators (if appropriate).<br><br>Changing/refreshing authenticators at least every [Assignment: organization-defined time period by authenticator type]. | |
| **SC-4** | The information system prevents unauthorized and unintended information transfer via shared system resources. | Using IAM best practices, customers can design a robust AWS identity management policy that can restrict access to different roles and groups of users. |

# Security Groups and Network ACLs:

Security groups provide stateful filtering at the instance level and can meet the network security needs of many AWS customers. However, VPC users can choose to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide.

A network access control list (ACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You can set up network ACLs with rules similar to your security groups in order to add a layer of stateless filtering to your VPC.

Customers should implement network ACLs as an additional layer of defense and a mitigation technique to reduce the impact of future misconfigurations, intrusions, vulnerabilities, etc. Due to their stateless nature, network ACLs are best implemented as a blacklist because their large rule sets can become unwieldy and difficult to manage. Network ACLs are applied at the subnet level and should block traffic that should not enter the subnets such as FTP, Database ports in your public subnet, etc.

Below are the 800-53 controls that can be partially or completely satisfied if security groups and NACLS configured properly across their virtual infrastructure.

**NOTE:** The controls listed below cover the security requirements within the AWS account's environment, not within the guest OS or any applications deployed on it (unless explicitly stated).

**800-53 Controls satisfied by Security Groups and Network ACLS**

| Control | Brief Description | Rationale |
|---|---|---|
| **AC-4** | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. | Security groups along with NACLs will ensure data flows are explicitly permitted or denied according the approved security policy. |

| | | |
|---|---|---|
| **AC-17, AC-17 (3), AC-4, SC-7 (3)(4) (7)** | The organization:<br><br>Documents allowed methods of remote access to the information system.<br><br>Establishes usage restrictions and implementation guidance for each allowed remote access method.<br><br>Monitors for unauthorized remote access to the information system.<br><br>Authorizes remote access to the information system prior to connection.<br><br>Enforces requirements for remote connections to the information system.<br><br>The information system routes all remote accesses through a limited number of managed access control points.<br><br>The information system:<br><br>Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.<br><br>Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture. | Security Groups along with NACLs will allow administrators to only permit and enforce specific IP and protocols to remote access bastion hosts and therefore limit the remote access through a limited number of managed access control points. Customers can configure end-to-end network isolation by using an IP address range and routing all of network traffic between BMC's virtual private cloud (VPC) and another network designated by the customer via an encrypted Internet Protocol security (IPsec) VPN. |
| **SC-7 (5)** | The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception) | By Default, security groups explicitly deny all protocol and IP traffic |
| **SC-32** | The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. | Security groups will provide logical separation between web tiers, data, and application components. |

# Harden Operating Systems and Applications:

Hardening the Windows Operating system while keeping your application functioning properly can be a challenge. AWS has found that installing applications on hardened OS's can be problematic. When the registry is locked down, it can be very difficult to install applications without a lot of errors. If this becomes an issue, our suggestion is to install applications on a clean version of windows, snapshot the OS and use GPOs (either locally or from the AD server) to lock down the OS. When applying the GPOs and backing off security settings, reboot constantly because many of the registry changes only take effect upon reboot. If DISA STIGS are employed as a security baseline, expect to back off the auditing policy. By default, many security policies can audit all access (read, write, modify) to system objects that will fill up your disks immediately. Once the machine is locked down to an acceptable state and the application is running normally, AWS suggests running a security scanner, validating the security posture, and repeating the process until all findings are mitigated or documented. Once the instance has been sufficiently configured, secured, the approved by the security team, the "gold image" should be converted into an organizationally consumed AMI image. If the process takes too much time/resources to complete, a third-party vendor have products on the AWS marketplace (https://aws.amazon.com/marketplace/search/results/ref=srh_navgno_search_box?page=1&searchTerms=hardened+images) They are pre-configured and hardened but there is an associated cost with their product.

Below are the 800-53 controls that can be partially or completely satisfied if customers harden all components/OS/Applications to be compliant with the DISA STIGS.

**800-53 Controls satisfied by Hardening OS's and Applications**

| Control | Brief Description | Rationale |
|---|---|---|
| **AC-17 (8)** | The organization disables [*Assignment: organization-defined networking protocols within the information system deemed to be non-secure*] except for explicitly identified components in support of specific operational requirements. | The hardening process will remove all unnecessary networking protocols. |
| **AU-2 (4), AU-3 (1), AU-5, AU-12** | The organization includes execution of privileged functions in the list of events to be audited by the information system.<br><br>The information system includes [Assignment: organization-defined additional, more detailed information] in the audit records for audit events identified by type, location, or subject | The hardening process will produce a list of auditable events that can be configured and implemented within the windows security policy. The security policy can dictate who and how an administrator is notified about audit events. The policy will be configured to use internal system clocks for time stamps of audit records. |

| | | |
|---|---|---|
| **AU-8 (1)** | The information system uses internal system clocks to generate time stamps for audit records. | The policy will use NIST clocks for time stamps of audit records. |
| **AU-4 (4)** | The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. | Administrators can define the amount of storage dedicated to audit record storage on their instances. Using S3 bucket will ensure storage of audit events will never be exceeded. |
| **AU-9 (1) (2)** | The information system protects audit information and audit tools from unauthorized access, modification, and deletion.<br><br>- The information system backs up audit records at [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited. | The audit records will be exported to S3 as read-only and explicitly accessible to ISSO and other security personnel |
| **SC-32** | The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. | Security groups will provide logical separation between web tiers, data, and application components |
| **CM-6** | Establishes and documents mandatory configuration settings for information technology products employed within the information system [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with the sensitivity level; | Administrators maintain AMI images that contain all necessary security hardening, auditing, and logging necessary the system. The hardened images will be the only images accessible to system administrators. |
| **CM-6 (1)** | The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. | MS Active Directory can manage all aspects of configuration and settings with a MS domain. Linux based systems can use puppet, chef or other industry standard CM software. |
| **SI-3 (1)(2)(3)** | The organization:<br><br>Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to | The organization will centrally manage anti-virus and malicious code mechanisms to all instances and resources. All signatures will be updated and pushed out on a regular basis. |

| | | |
|---|---|---|
| | detect and eradicate malicious code:<br><br>Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or<br><br>Inserted through the exploitation of information system vulnerabilities; | |
| **CM-7** | The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services | The hardening of the OS and applications along with Windows Group Policy objects will ensure port and protocols are not used without ISSO approval. |

# Encrypting Data at Rest:

Encrypting Data at Rest is a requirement for many government organizations that host sensitive data in a multi-tenant environment. Best practices suggest that whenever technically and financially feasible, customers should encrypt all data in their system. The recommendations below address some of the data at rest concerns.

**Database:** Ensure the database is using TDE (transparent data encryption) and scan the system using a database security scanner. There are several products in this domain that can be found on Google (https://www.google.com/ - q=database+scanners+security)

. Once you have a security report, use the iterative approach depicted in the hardening section to mitigate findings. If you need assistance choosing a product that meets your specific requirements, contact your sales rep to setup an AWS Professional Services engagement. They can help you find the most appropriate third-party partner that can meet your specific needs.

**File Systems/Amazon EBS:** Customers should configure their compute instances and block stores to protect the confidentiality and integrity of their information at rest. Amazon EBS encryption can be enabled for any non-boot volumes. In addition, there are many third-party in the marketplace (https://aws.amazon.com/marketplace/search/results/ref=srh_navgno_search_box?page=1&searchTerms=encryption+key+management) or open source tools (ex Linux LUKS) could be used to meet the file system encryption requirement.

**Amazon S3 buckets:** Amazon S3 allows customers to encrypt objects one-click client-side encryption with their own keys or they can AWS can manage the keys.

Below are the 800-53 controls that can be partially or completely satisfied if customers employ data at rest encryption throughout their application. **NOTE:** The controls listed below cover the security requirements at OS and DB layers.

**800-53 Controls satisfied by Encrypted Data at Rest**

| Control | Brief Description | Rationale |
|---|---|---|
| **SC-28** | The information system protects the confidentiality and integrity of information at rest. | Admins configure encryption at rest for all EBS volumes using third-party products or use the built-in tools within the operating system. Data containing within DB tables will be encrypted using TDE. |

# Patch Management:

An automated patch management is critical in operating a large cloud based system. It is suggested that customers use a tool that can manage patches for both the operating system and applications. Microsoft SCM can meet this requirement along with other patch management systems available in the marketplace.

Below are the 800-53 controls that can be partially or completely satisfied if customers implement a patch management system throughout their application. **NOTE:** The controls listed below cover the security requirements at the infrastructure layer, not the application layer (unless explicitly stated).

**800-53 Controls Satisfied by a Centralized Patch Management System**

| Control | Brief Description | Rationale |
|---|---|---|
| **CM-6, CM-02** | Establishes and documents mandatory configuration settings for information technology products employed within the information system [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with the sensitivity level | Since AWS is responsible for patching the infrastructure, customers must implement an automated patch management process for the OS and applications and maintain the configurations within a CM process. |

# Auditing and Logging:

When hardening and configuring the OS and applications, ensure all logs are sent to a SIEM. This ensures that the system will meet FedRAMP's requirement to centrally monitor your application logs but falls short of monitoring the AWS infrastructure since it was not designed to consume AWS CloudTrail logs. To meet the requirement, users should configure their AWS services to turn on logging capabilities (Table 1 - AWS Logging Options) and implement a tool to consume AWS logs and provide an interface for ISSOs to monitor security relevant changes. A custom application could be written to condense the logs or you could use a third-party product. Implementing a third-party product takes hours, not days to configure unlike large SIEM products. The AWS Marketplace hosts many third-party partners that can be used to consolidate your audit logs

(https://aws.amazon.com/marketplace/search/results/ref=srh_navgno_search_box?page=1&searchTerms=log+management). **NOTE: Many of the SAAS service providers do not have a FedRAMP ATO, so using their services will have to be discussed with the authorizing official at the sponsoring agency.**

| Service | Data | Method | Format | Default | Frequency |
|---|---|---|---|---|---|
| AWS CloudTrail | IAM, AWS STS, VPC, EC2, Amazon EBS, Amazon RDS, Amazon Redshift, CloudTrail | Amazon S3 via:<br>• Console<br>• CLI | • JSON<br>• SNS | Off | < 15 minutes |
| AWS Elastic Load Balancing | Access Logs | Amazon S3 | Text | Off | 5 or 60 minutes |
| Auto Scaling | Service events | • CLI<br>• API | • CLI: XML, Text<br>• API: XML | On | Immediate |
| Amazon RDS | • Service events<br>• MySQL logs<br>• Oracle logs<br>• SQL Server logs | Amazon RDS via:<br>• CLI<br>• Console<br>• API<br>• SNS<br>DB logs via:<br>• Console<br>• CLI | • Events: text<br>• Logs: varies by engine<br>• SNS: JSON, text | • Events: On<br>• SNS: Off | Immediate |
| AWS OpsWorks | Chef logs | CLI | Text | On | Immediate |
| AWS CloudFormation | • Stack events<br>• Historical events | • Console<br>• CLI<br>• API | • CLI, Console: Text<br>• API: XML | On | Immediate |
| AWS Elastic Beanstalk | • Environment launch events, EC2 instance logs | • Console, CLI, API<br>• Amazon S3 | • CLI, Console: Text<br>• API: XML | • Events: On<br>• Amazon S3: Off | Immediate |
| Amazon Redshift | • Connections<br>• User changes<br>• STL system tables, including queries | Amazon S3 via:<br>• Console<br>• CLI | • Logs: text<br>• Tables: SQL output | • Amazon S3: Off<br>• Tables: On | Amazon S3: < 1 hour<br>Tables: |

| | | | | | |
|---|---|---|---|---|---|
| | | Tables via:<br>• CLI | | | Immediate |
| AWS CloudHSM | Appliance logs | Syslog | Text | • Local: On<br>• Remote: Off | Immediate |
| Amazon Glacier | Vault notifications | Amazon SNS | Amazon SNS formats | Off | Immediate |
| Amazon ElastiCache | Service events | Amazon SNS | Amazon SNS formats | Selectable | Immediate |
| Amazon Simple Workflow | Workflow history | • CLI<br>• API | JSON | On | Immediate |
| Amazon Simple Email Service (Amazon SES) | Feedback notifications | • Amazon SES<br>• Amazon SNS | JSON | Off | Immediate |
| Amazon Simple Notification Service (Amazon SNS) | Messages | Amazon SNS | Amazon SNS formats | Off | Immediate |
| AWS Data Pipeline | • Pipeline events<br>• Task Runner logs | • Console<br>• Amazon SNS<br>• Local (Task Runner)<br>• Amazon S3 | Various | • Console: On<br>• SNS: Off<br>• Task Runner: Optional<br>• Amazon S3: Recommended | • Console, Local: Immediate<br>• Amazon S3: hourly |
| Amazon EMR | Hadoop logs | • Console<br>• Master Node<br>• Amazon S3 | Various | • Console: Off<br>• Master Node: On<br>• Amazon S3: Off | 5 minutes |
| Amazon S3 | Server access logs | Amazon S3 via:<br>• Console<br>• API | Text | Off | < 2 hours |
| Amazon | • Access logs<br>• Cookies | Amazon S3 | • Text<br>• W3C | • Requests: Off | < 24 hours |

| | | | | | |
|---|---|---|---|---|---|
| CloudFront | | via:<br>• Console<br>• API | extended | • Cookies: Off | |

**Table 1 - AWS Logging Options**

Below are the 800-53 controls that can be partially or completely satisfied audit and logging are configured to be consistent with industry best practices and the DISA STIGs . **NOTE:** The controls listed below cover the security requirements at the infrastructure layer, not the application layer (unless explicitly stated).

**800-53 Controls Satisfied by configuring AWS infrastructure auditing and logging**

| Control | Brief Description | Rationale |
|---|---|---|
| **AC-2 (4)(7)** | Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and<br><br>-Tracks and monitors privileged role assignments. | Customers should implement a centralized auditing and logging solution that can track all aspects of user and role management. Cloudtrail can be used to monitor IAM role activity and Cloudwatch logs can be configured to monitor security related events within OS and application layers |
| **AC-17 (1) (5) (7)** | Monitors for unauthorized remote access to the information system | Customers should implement a centralized auditing and logging solution that can track all aspects of user and role management. Cloudtrail can be used to monitor IAM role activity but cannot monitor user activity within the OS and application layers. |
| **AU-6 (1) (3) (7)** | Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity and reports findings to designated organizational officials. | Same as above |
| **AU-7(1)** | The information system provides the capability to automatically process audit records for events of interest based on selectable event | The centralized audit reduction system should allow the ISSO to search on multiple criteria. |

| | | |
|---|---|---|
| | criteria. | |
| **AU-9(1) (2), AU (11), CM-3(3),CM-5 (1)**<br><br>**d** | The information system backs up audit records at [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.<br><br>-The organization retains audit records online for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.<br><br>- Audits activities associated with configuration-controlled changes to the system; and…<br><br>- The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. | Backing up logs to a protected S3 bucket that is limited to access by security staff will ensure the logs cannot be modified without proper authorization. |
| **CM-6 (3), CM-8 (3), IR-6 (1), SI-4 (2), (4) (5)** | The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.<br><br>- The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.<br><br>- The information system provides near real-time alerts when the following indications of compromise or potential compromise occurs [*Assignment: organization-defined list of compromise indicators*] | The audit reduction and monitoring system would complement and enhance a system wide monitoring tool such as Dome9 or other third-party product. |

# Security Scanning:

Use scanners such as Retina or Tenable's Nessus (www.tenable.com) to scan your environment on a regular basis. Run the scanner from two perspectives, one from the Internet (unauthenticated) to simulate the attack surface a hacker or intruder can see; and then run an authenticated scan from an inside subnet that has unfettered access to all subnets. AWS suggests writing a security group that allows all ports/protocols from the scanner IP to all hosts within the environment. Remember to notify AWS when you plan to security scan your environment so the internal AWS IPS doesn't flag your scan as malicious (https://portal.aws.amazon.com/gp/aws/html-forms controller/contactus/AWSSecurityPenTestRequest).

Below are the 800-53 controls that can be partially or completely satisfied if customers institute a security scanning process and vulnerability management program. **NOTE:** The controls listed below cover the security requirements at the infrastructure layer, not the application layer (unless explicitly stated).

**800-53 Controls satisfied by a comprehensive security scanning program**

| **800-53 Controls satisfied by a comprehensive security scanning program** | | |
|---|---|---|
| **Control** | Brief Description | Rationale |
| **RA-5(5) (6), SI-2 (2)** | -Scans for vulnerabilities in the information system and hosted applications<br><br>- Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:<br><br>- The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. | Customers should leverage their already existing vulnerability scanning process. ISSO should start scanning the OS's and applications immediately to demonstrate how the security process handles vulnerability mitigation. |

# CloudFormation Templates:

AWS CloudFormation gives developers and systems administrators an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion. The templates could also satisfy several configuration and security functionality verification security controls.

Below are the 800-53 controls that can be partially satisfied if customers use AWS CloudFormation templates to augment their configuration management processes. However, AWS CloudFormation templates cannot manage all components of the application such as the operating system and installed

applications. A comprehensive configuration management process will use other tools such puppet or chef
**NOTE:** The controls listed below cover the security requirements at the infrastructure layer, not the application layer (unless explicitly stated).

**800-53 Controls satisfied by using Cloud Formation Templates**

| Control | Brief Description | Rationale |
|---|---|---|
| **CM-2 (1) (3), CM-3** | - The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.<br><br>The organization:<br><br>Determines the types of changes to the information system that are configuration controlled.<br><br>Approves configuration-controlled changes to the system with explicit consideration for security impact analyses.<br><br>Documents approved configuration-controlled changes to the system.<br><br>Retains and reviews records of configuration-controlled changes to the system.<br><br>Audits activities associated with configuration-controlled changes to the system; | AWS CloudFormation templates will help customers maintain a strict configuration management scheme of the cloud infrastructure. If an error or misconfiguration of the infrastructure or associated security mechanism (security groups, NACLs) is detected, the administrators can analyze the current infrastructure templates; compare with previous versions, and redeploy the configurations to a known and approved state. |
| **CM-4** | The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. | Once AWS CloudFormation templates are entered into the CM process, deltas of changes to the templates can be analyzed, risk assessed, and implemented in a consistent manner. |
| **CM-8 (1) (3)** | The organization develops, documents, and maintains an inventory of information system components that:<br><br>Accurately reflects the current information | AWS CloudFormation templates are the approved baseline for all changes to the infrastructure. They provide an automated method to assess the status of an operational infrastructure against an approved base line. |

| | | |
|---|---|---|
| | system;<br><br>Is consistent with the authorization boundary of the information system;<br><br>Is at the level of granularity deemed necessary for tracking and reporting.<br><br>- The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.<br><br>- Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system;<br><br>- The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system**.** | Customers should run the CloudFormer tool quarterly to assessment the current baseline against the approved and accredited configuration. |
| **SI-6** | The information system verifies the correct operation of security functions… | AWS CloudFormation scripts will be foundation to ensure the essential security mechanisms (security groups, network acls) are deployed as designed and authorized. |

# Monitoring:

Maintaining operational awareness of applications, infrastructure, and networking components is critical to satisfy the necessary 800-53 security controls. There are two aspects of monitoring that need to be assessed: the application and infrastructure components. The application can be monitored with the traditional technologies that are used today such as IBM's qradar, Dell's Intrust, or Splunk. The SIEM software runs on standard operating systems so it can be installed on Amazon EC2 instances and operate in the same manner as they did within a traditional data center. Since the AWS infrastructure is accessed through APIs and standard interfaces, security monitoring tools often require modification to provide the same level of transparency offered in the traditional computing environment. In most cases, application owners can provide complete computing stack monitoring by augmenting their SIEM tools with third- party products that use the AWS APIs to monitor, log, and control all aspects of the customers AWS infrastructure. There are several third-party AWS partner products that satisfy the requirements to monitor AWS infrastructure changes to include Dome9, CloudCheckr, and Sumo Logic. **NOTE: Many of the SAAS**

**service providers do not have a FedRAMP ATO, so using their services will have to be discussed with the authorizing official at the sponsoring agency.**

**800-53 Controls satisfied by a comprehensive monitoring strategy**

| Control | Brief Description | Rationale |
|---|---|---|
| **CM-6 (3)** | The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. | Implementing a SIEM solution is critical to maintain security awareness of the application and infrastructure. Customers should use SIEM solution but will need to incorporate a third-party product or develop a solution to monitor the customers AWS infrastructure. |
| **CM-8 (1) (3)** | The organization develops, documents, and maintains an inventory of information system components that:<br><br>Accurately reflects the current information system;<br><br>Is consistent with the authorization boundary of the information system;<br><br>Is at the level of granularity deemed necessary for tracking and reporting<br><br>- The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.<br><br>- Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and….<br><br>- The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another | AWS CloudFormation templates will be an approved baseline for all changes to the infrastructure. They could provide an automated method to assess the status of an operational infrastructure against an approved base line. Customers can run the CloudFormer tool quarterly to assess the current baseline against the approved and accreditation configuration. |

| | | |
|---|---|---|
| | system as a component within that system**.** | |
| **Si-4 (1) (2) (4) (5)** | The organization:<br><br>Monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives]<br><br>- The organization employs automated tools to support near real-time analysis of events and detects information system attacks;<br><br>-The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.<br><br>- The information system provides near real-time alerts when the following indications of compromise or potential compromise occurs | Monitoring the application and infrastructure using traditional and cloud SIEM products ensure all security functions and process are operating normally. |

# Governance in AWS:

At this point, governance in AWS may not be a priority but it is a good practice to tag resources to make it easier to manage those resources, track billing, and provide additional visibility.
See http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html for details.

# AMI Library:

Managing an image library where the images are routinely patched, hardened, scanned and documented will ensure deployed AMI's are consistent with the predefined security policies. Customers should restrict new instances to use the approved and validated images.

**800-53 Controls satisfied by managing an Image Library**

| Control | Brief Description | Rationale |
|---|---|---|
| **CM-6** | Establishes and documents mandatory configuration settings for information technology products employed within the information system [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with | Maintaining an image repository that is centrally managed, hardened and configured with monitoring software will ensure all mandatory configuration settings are enforced |

| | | |
|---|---|---|
| | the sensitivity level | throughout the virtual infrastructure. |
| **CM-7** | The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*] | Managing a predefined list of Operating Systems, applications and their approved configurations to include employing a policy of least privilege will ensure all instances are conformant to customer and the sponsoring agency security policies. |

# Final Thoughts

If implemented, these recommendations will serve as the building blocks to ensure the virtual cloud infrastructure scales with customer demand; decreases administrative costs by centrally managing all resources; and meets or exceeds the necessary FedRAMP security requirements. If organizations require additional information or need guidance on how to properly secure their cloud infrastructure, ask your AWS Sales Representative about an AWS professional service security engagement.