SECURING AMAZON EC2 INSTANCES

"How do I secure my EC2 instances?"

Overview

Amazon Elastic Compute Cloud (Amazon EC2) provides AWS customers with the ability to launch and fully manage virtual machines in the cloud. This document covers high-level guidance and best practices for securing Amazon EC2 instances. These best practices span operating systems and offer a framework for more specific recommendations, such as those offered in the Securing Windows Instances Solution Brief.

This document assumes a basic understanding of the AWS platform and operating system (OS) security.

General Best Practices

The process for securing Amazon EC2 instances involves principles that are applicable to any OS, whether running in a virtual machine or on premises:

- **Least Access:** Restrict server access from both the network and on the instance, install only the required OS components and applications, and leverage host-based protection software.
- **Least Privilege:** Define the minimum set of privileges each server needs in order to perform its function.
- **Configuration Management:** Create a baseline server configuration and track each server as a configuration item. Assess each server against the current recorded baseline to identify and flag any deviations. Ensure each server is configured to generate and securely store appropriate log and audit data.
- **Change Management:** Create processes to control changes to server configuration baselines.
- **Audit Logs:** Audit access and all changes to EC2 instances to verify server integrity to ensure only authorized changes are made.

Application on the AWS Platform

The following sections offer prescriptive advice for applying server-level security controls to Amazon EC2 instances in the AWS cloud.

Network Access

Each EC2 instance has one or more Elastic Network Interfaces (ENIs) that provide network connectivity to an Amazon Virtual Private Cloud (Amazon VPC) subnet. Each ENI is protected by one or more security groups that act as stateful virtual firewalls, a stateless network access control list (ACL), and subnet route table rules. The following best practices implement the principle of least access for EC2 network connections:

- Configure security groups to permit the minimum required network traffic for the EC2 instance. For example, if an EC2 instance is a web server, configure its security groups to permit only inbound HTTP/HTTPS, management traffic, and minimal outbound connections.
- Leverage security groups as the primary mechanism for controlling network access to EC2 instances. When necessary, use network ACLs sparingly to provide stateless, coarse-grain network control. Security groups are more versatile than network ACLs due to their ability to perform stateful packet filtering and create rules that reference other security groups. However, network ACLs can be effective as a secondary control for denying a specific subset of traffic or providing high-level subnet guard rails.
- Configure VPC subnet route tables with the minimal required network routes. For example, place only EC2 instances that need direct Internet access into subnets with routes to an Internet Gateway, and place only EC2 instances that need direct access to internal networks into subnets with routes to a virtual private gateway.
- Consider using additional security groups or ENIs to control and audit EC2 instance management traffic separately from regular application traffic. This approach allows specific IAM policies to control changes to specific security groups or automated rule-verification scripts to more easily audit security group rules. Separate ENIs allow customers to combine host-based routing policies with VPC subnet routing rules to control network traffic.

See the *Resources* section for additional Solution Briefs related to network access control.

User Access to EC2 Instances

Tightly control and monitor interactive access to EC2 instances. Interactive access is typically either provided through emergency-only, *break-glass* scenarios, or managed through a central directory service. For users and apps that require regular access to instances, make sure to configure them with least privileges. For more information, see the Controlling EC2 OS Access Solution Brief.

AWS API Access from EC2 Instances

Applications running on EC2 instances frequently access additional AWS services and must be granted permissions to make API calls. The recommended approach for granting EC2-based applications AWS permissions is with an IAM role for EC2[1] because this eliminates the need to distribute and rotate long-term credentials on EC2 instances. When creating IAM roles, associate least-privilege IAM policies that restrict access to the specific API calls the application requires.

Data Encryption

Always encrypt sensitive data that is transmitted or stored.[2] AWS provides encrypted Elastic Block Storage (EBS) volumes to protect data at rest. Customers can use instance-level encrypted file systems, such as EncFS or EFS/NTFS, and also the AWS Key Management Service (AWS KMS) to create encryption keys for encrypting data at the file level. To encrypt sensitive data in transit, use an encryption protocol such as Transport Layer Security (TLS) or IPsec. Make sure to allow only encrypted connections between EC2 instances and the AWS API endpoints or other sensitive remote network services. This can be enforced through the use of outbound security group rules.

Configuration Management

Amazon Machine Images (AMIs) provide an initial configuration for an EC2 instance, which includes the OS and optional customer-specific customizations, such as applications and security controls. Create an AMI catalog containing customized security configuration baselines to ensure all instances are launched with standard security controls. Security baselines can be baked into an AMI, bootstrapped dynamically when an EC2 instance is launched, or packaged as a product for uniform distribution through AWS Service Catalog portfolios. For more information on AMI configuration options, see the AWS AMI Design Solution Brief.

EC2 instance OS configuration[3] should adhere to organizational security standards and contain host-integrity management software. Configure security software to monitor and maintain OS security settings, protect the integrity of critical OS files, and alert on deviations from the security baseline. AWS customers can also run Amazon Inspector assessments to improve the security and compliance of applications deployed on EC2 instances. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices and includes a knowledge base of hundreds of rules mapped to common security compliance standards (e.g., PCI DSS) and vulnerability definitions. Examples of built-in rules include checking if remote root login is enabled, or if vulnerable software versions are installed. These rules are regularly updated by AWS security researchers.

Configure OS, audit, and application logging to send local log files to a centralized log management system[3] to preserve log data for security and operational behavior analysis. For example, consider including a log management agent such as the CloudWatch Logs agent or another third-party agent as part of an EC2 instance security baseline. For OS-specific configuration management advice, please see the Securing EC2 Windows Instances Solution Brief.

Change Management

After initial security baselines are applied to EC2 instances at launch, control ongoing EC2 changes in order to maintain the security of your virtual machines. Establish a change management process to authorize and incorporate changes to AWS resources (such as security groups, route tables, and network ACLs) as well as to OS and application configurations (such as OS or application patching, software upgrades, or configuration file updates). To implement changes, customers can either replace EC2 instances in blue-green deployments or use a configuration management tool to run in-place updates.

---

[1] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html
[2] For more information, see the AWS whitepaper *Securing Data at Rest with Encryption*: https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf
[3] See the *Resources* section for documentation regarding configuration management systems and logging on AWS.

Audit and Accountability

AWS CloudTrail, AWS Config, and AWS Config Rules provide audit and change tracking features for auditing AWS resource changes. In addition to AWS-provided audit logs, it is important to identify all system and application logs as well as the software components that generate EC2 instance logs. Configure instances to send important local log files to a centralized log management system for analysis. To effectively analyze the logs of a significant number of distributed servers, aggregate them into a common repository that includes features for searching and reporting.

Resources

AWS AMI Design	https://d0.awsstatic.com/aws-answers/AWS_AMI_Design.pdf AWS Solution Brief on common AMI design strategies
Controlling EC2 OS Access	https://d0.awsstatic.com/aws-answers/AWS_Controlling_OS_Access_to_EC2.pdf AWS Solution Brief on different methods for controlling OS-level access to EC2 instances
VPC Security Capabilities	https://d0.awsstatic.com/aws-answers/VPC_Security_Capabilities.pdf AWS Solution Brief on features and considerations for secure VPC design
Infrastructure Configuration Management	https://d0.awsstatic.com/aws-answers/AWS_Infrastructure_Configuration_Management.pdf AWS Solution Brief on services and third-party products for configuration management
Native AWS Security-Logging Capabilities	https://d0.awsstatic.com/aws-answers/AWS_Native_Security_Logging_Capabilities.pdf AWS Solution Brief on platform-supported logging features
AWS Secure Initial Account Setup	https://d0.awsstatic.com/aws-answers/AWS_Secure_Account_Setup.pdf AWS Solutions Brief that gives baseline security guidance for AWS accounts
Tips for Securing Your EC2 Instance	http://aws.amazon.com/articles/1233/ AWS article on best practices for securing EC2 instances
Amazon Inspector Website	https://aws.amazon.com/inspector/