SECURING WINDOWS EC2 INSTANCES

“How do I secure my EC2 Windows instances?”

Overview

Amazon Elastic Compute Cloud (Amazon EC2) provides AWS customers with the ability to launch and fully manage virtual machines in the cloud. Amazon EC2 offers different instance types that support a variety of operating systems with individual security-related capabilities and requirements. This document provides recommendations and best practices for securing EC2 instances running Microsoft Windows Server.

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

General Best Practices

When securing Windows instances, there are some universal design principles to consider. For example, it’s best to implement Active Directory Domain Services to enable a scalable, secure, and manageable infrastructure for distributed locations. Additionally, after launching instances through the AWS Console or using an EC2 provisioning tool such as AWS CloudFormation, it is good practice to utilize native OS features such as Microsoft Windows PowerShell DSC to maintain configuration state in the event that configuration drift occurs. Keeping general best practices in mind, Windows instances in AWS should adhere to the following high-level best practices:

- **Least Access:** Grant access only to systems and locations that are trusted and expected. This applies to all Microsoft products such as Active Directory, Microsoft business productivity servers, and infrastructure services such as Remote Desktop Services, reverse proxy servers, IIS web servers, etc. Use AWS capabilities such as Amazon EC2 instance security groups, network access control lists (ACLs), and Amazon VPC public/private subnets to layer security across multiple locations in an architecture. Within a Windows instance, customers can use Windows Firewall to further layer a defense-in-depth strategy within their deployment.

  Install only the OS components and applications that are necessary for the system to function as designed. Configure infrastructure services such as IIS to run under service accounts or to use features such as application pool identities to access resources locally and remotely across your infrastructure.

- **Least Privilege:** Determine the minimum set of privileges that instances and accounts need in order to perform their functions. Restrict these servers and users to only allow these defined permissions. Use techniques such as Role Based Access Controls to reduce the surface area of administrative accounts and create the most limited roles to accomplish a task.

  Use OS features such as Encrypting File System (EFS) within NTFS to encrypt sensitive data at rest and control application and user access to it.

- **Configuration Management:** Create a baseline server configuration incorporating up-to-date security patches and host-based protection suites that include anti-virus, anti-malware, intrusion detection/prevention, and file integrity monitoring. 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 and work toward fully automated change processes. Also leverage Just Enough Administration (JEA) with Windows PowerShell DSC to limit administrative access to the minimum required functions.
- **Audit Logs:** Audit access and all changes to EC2 instances to verify server integrity and ensure only authorized changes are made. Leverage features such as Enhanced Logging for IIS to enhance default logging capabilities. AWS capabilities such as VPC Flow Logs and AWS CloudTrail are also available to audit network access, including allowed/denied requests and API calls respectively.

Application on the AWS Platform

The following sections offer prescriptive advice and guidelines for Windows instances and infrastructure to help maintain a compliant, monitored, and controlled Windows Server environment.

Network Access

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

- Configure Amazon EC2 instance security groups to permit the minimum required network traffic for the EC2 instance and to allow access only from defined, expected, and approved locations. For example, if an EC2 instance is an IIS web server, configure its security groups to permit only inbound HTTP/HTTPS, Windows 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. Also, because network ACLs apply to an entire subnet, they can be used as defense-in-depth in case an instance is ever launched unintentionally without a correct security group.
- Centrally manage Windows Firewall settings with Group Policy Objects (GPO) to further enhance network controls. Customers often use the Windows Firewall for further visibility into network traffic and to complement security group filters, creating advanced rules to block specific applications from accessing the network or to filter traffic from a subset IP addresses. For example, the Windows Firewall can limit access to the EC2 metadata service IP address to specific whitelisted users or applications. Alternatively, a public-facing service might use security groups to restrict traffic to specific ports and the Windows Firewall to maintain a blacklist of explicitly blocked IP addresses.
- 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 customers to implement special IAM policies for change control, making it easier to audit changes to security group rules or automated rule-verification scripts. Multiple ENIs also provide additional options for controlling network traffic including the ability to create host-based routing policies or leverage different VPC subnet routing rules based on an ENI's assigned subnet.
- Many of the Windows OS roles and Microsoft business applications also provide enhanced functionality such as IP Address Range restrictions within IIS, TCP/IP filtering policies in Microsoft SQL Server, and connection filter policies in Microsoft Exchange. Network restriction functionality within the application layer can provide additional layers of defense for critical business application servers.

In addition to restricting network access to each Amazon EC2 instance, Amazon VPC supports implementing additional network security controls like in-line gateways, proxy servers, and various network monitoring options. See the *Resources* section for security-related Solution Briefs.

User Access to EC2 Instances

When managing Windows instances, limit access to a few well-defined centralized management servers or bastion hosts to reduce the environment's attack surface. Also, use secure administration protocols like RDP encapsulation over SSL/TLS. The Remote Desktop Gateway Quick Start[1] provides best practices for deploying remote desktop gateway, including configuring RDP to use SSL/TLS.

Use Active Directory or AWS Directory Service to tightly and centrally control and monitor interactive user and group access to Windows instances, and avoid local user permissions. Also avoid using Domain Administrators and instead create more granular, application-specific role-based accounts. Just Enough Administration (JEA) allows changes to Windows instances to be managed without interactive or administrator access. In addition, JEA enables organizations to lock down administrative access to the subset of Windows PowerShell commands required for instance administration. For additional information, see the Controlling EC2 OS Access Solution Brief.

Systems Administrators should use Windows accounts with limited access to perform daily activities, and only elevate access when necessary to perform specific configuration changes. Additionally, only access Windows instances directly when absolutely necessary. Instead, leverage central configuration management systems such as EC2 Run Command, Systems Center Configuration Manager (SCCM), Windows PowerShell DSC, or Amazon EC2 Simple Systems Manager (SSM) to push changes to Windows servers.

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[2] 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. For Windows-to-Windows communication, use well-defined and well-documented Windows groups and roles to grant application-level access between Windows instances. Groups and roles allow customers to define least privilege application and NTFS folder-level permissions to limit access to application-specific requirements.

Data Encryption

Always encrypt sensitive data that is transmitted or stored.[3] AWS provides encrypted Elastic Block Storage (EBS) volumes to protect data at rest. Customers can also use Microsoft EFS and NTFS permissions for folder- and file-level encryption. Encrypt sensitive data in transit using 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 or Windows Firewall rules.

Configuration Management

Amazon Machine Images (AMIs) provide an initial configuration for an EC2 instance, which includes the Windows OS and optional customer-specific customizations, such as applications and security controls. Create an AMI catalog containing customized security configuration baselines to ensure all Windows 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.

Each EC2 instance should[4] adhere to organizational security standards. Do not install any Windows roles and features that are not required, and do install software to protect against malicious code (antivirus, antimalware, exploit mitigation), monitor host-integrity, and perform intrusion detection. Configure security software to monitor and maintain OS security settings, protect the integrity of critical OS files, and alert on deviations from the security

[1] http://docs.aws.amazon.com/quickstart/latest/rd-gateway/welcome.html

[2] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

[3] 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

[4] See the *Resources* section for documentation regarding configuration and centralized log management systems on AWS.

baseline. Consider implementing recommended security configuration benchmarks published by Microsoft, the Center for Internet Security (CIS), or the National Institute of Standards and Technology (NIST). Consider using other Microsoft tools for particular application servers, such as the Best Practice Analyzer for SQL Server.[5]

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.

Change Management

After initial security baselines are applied to EC2 instances at launch, control ongoing EC2 changes 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 Windows or application patching, software upgrades, or configuration file updates).

AWS provides several tools to help manage changes to AWS resources including AWS CloudTrail, AWS Config, AWS CloudFormation, and AWS Elastic Beanstalk (Elastic Beanstalk), AWS OpsWorks,[6] and management packs for Systems Center Operations Manager and System Center Virtual Machine Manager. Note that Microsoft releases Windows patches every Tuesday (sometimes even daily) and AWS updates all AWS managed Windows AMIs within five days after Microsoft releases a patch. Therefore it is important to continually patch all baseline AMIs, update AWS CloudFormation templates and Auto Scaling group configuration with the latest AMI IDs, and implement tools to automate running instance patch management.

Microsoft provides several options for managing Windows OS and application changes. SCCM, for example, provides full lifecycle coverage of environment modifications. Select tools that address business requirements and control how changes will affect application SLAs, capacity, security, and disaster recovery procedures. Avoid manual changes and instead leverage automated configuration management software or command line tools such as the EC2 Run Command or Windows PowerShell to implement scripted, repeatable change processes. To assist with this requirement, use bastion hosts with enhanced logging for all interactions with your Windows instances to ensure that all events and tasks are automatically recorded.

Audit and Accountability

AWS CloudTrail, AWS Config, and AWS Config Rules provide audit and change tracking features for auditing AWS resource changes. Configure Windows event logs to send local log files to a centralized log management system to preserve log data for security and operational behavior analysis. Microsoft System Center Operations Manager (SCOM) aggregates information about Microsoft applications deployed to Windows instances and applies preconfigured and custom rulesets based on application roles and services. System Center Management Packs build on SCOM to provide application-specific monitoring and configuration guidance. System Center Management Packs[7] support Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014, and many more servers and technologies. The AWS Management Pack for Microsoft System Center Operations Manager (SCOM) and the AWS Systems Manager for Microsoft System Center Virtual Machine Manager (SCVMM) integrate with Microsoft Systems Center to help you monitor and manage your on-premises and AWS environments together.

In addition to Microsoft systems management tools, customers can use Amazon CloudWatch to monitor instance CPU utilization, disk performance, network I/O, and perform host and instance status checks. The EC2Config service provides access to additional, advanced features for Windows instances. For example, it can export Windows system, security, application, and Internet Information Services (IIS) logs to CloudWatch Logs, which can then be integrated with Amazon CloudWatch metrics and alarms. Customers can also create scripts that export Windows performance counters to Amazon CloudWatch custom metrics.

[5] https://www.microsoft.com/en-us/download/details.aspx?id=29302
[6] See the Infrastructure Configuration Management Solution Brief for more information
[7] http://social.technet.microsoft.com/wiki/contents/articles/16174.microsoft-management-packs.aspx

Resources

CIS Microsoft Windows Server 2012 R2	https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v1.1.0.pdf Center for Internet Security - Microsoft Windows Server 2012 Benchmark v1.1.0 (published 11/4/2014)
CIS Microsoft IIS 8 Benchmark	https://benchmarks.cisecurity.org/tools2/iis/CIS_Microsoft_IIS_8_Benchmark_v1.0.0.pdf Center for Internet Security - CIS Microsoft IIS 8 Benchmark v1.0.0 (published 1/6/2014)
Microsoft Security Baselines for Windows OS and Internet Explorer 11	http://blogs.technet.com/cfs-filesystemfile.ashx/__key/telligent-evolution-components-attachments/01-4062-00-00-03-63-59-73/Win81_2D00_WS2012R2_2D00_IE11_2D00_Baselines_2D00_FINAL.zip
NIST Checklist for Windows Server 2012 R2 Version 2, Release 3	https://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=560
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/