CONTROLLING EC2 OS ACCESS

Overview
Access control at the operating system (OS) level is a security practice that can be challenging to implement successfully. Well-executed OS-level controls securely and efficiently grant business units access to necessary resources without hindering productivity. AWS lets customers build and tear down complex environments with a dynamic and agile platform that requires equally dynamic access controls. This document provides AWS customers with best practices and high-level architectural guidance for controlling OS-level access to Amazon Elastic Compute Cloud (Amazon EC2) instances.

The following sections assume a basic understanding of Amazon EC2 and Windows/Linux authentication.

General Best Practices
A universal principle for implementing OS-level access control is that the access controls should align with existing business processes and requirements. This ensures that the correct users have secure access to the resources they need to do their jobs. It is also universally essential that administrators always know what access is granted and to whom. From these two concepts, we can derive a few important practices:

- Ensure the access control system is granular enough to align with an organization’s structure and job roles so that permissions can be narrowed down to appropriate levels for resources, users, and groups of users.
- Create processes to verify access control changes (e.g., adding or removing users or resources) and automate them, if possible.
- Audit access controls and permissions on a regular basis (e.g., monthly reports) and randomly (e.g., impromptu audits).
- Monitor access to quickly identify and address any misalignment between access rights and reality.
- Ensure auditing and monitoring logs can be analyzed independently of an EC2 instance’s running status, including after instance termination.

Application on the AWS Platform
The following sections offer two prescriptive approaches for EC2 access management: one that grants emergency-only access and a second that leverages a centralized directory service to control OS-level access. When selecting the best approach for an organization, consider whether its AWS infrastructure changes are automated or if its systems or applications require manual configuration or local access. If its infrastructure is automated, then OS-level access for users or administrators might not be necessary at all.

Emergency-Only Access to EC2 Instances
Emergency-only, break-glass access control is typically appropriate for customers who have mature capabilities for centralized monitoring, log management, and configuration management, and who automate their AWS infrastructure and application deployments.

AWS customers have the ability to elastically grow and shrink their compute infrastructure by dynamically launching and terminating ephemeral compute nodes. Centralized monitoring and configuration management systems monitor and manage these instances without local user access; blue-green deployment models automatically deploy infrastructure upgrades or new application versions in parallel to existing EC2 instances. When embracing an automated configuration and deployment model, many AWS customers realize that they no longer need developers or systems administrators to routinely and interactively log in to the operating system. Instead of provisioning or managing individual access to their EC2 instances, they grant emergency-only access through emergency-only access control mechanisms; for example, whenever anyone needs to log directly into an EC2 instance, they must first obtain access from a credential escrow system and logging in triggers aggressive alarming.

Considerations
Provisioning effective emergency-only access and the associated monitoring requires significant automation expertise and maturity. One method to automatically provision emergency access is to specify an escrowed EC2 key pair when EC2 instances are launched, and then either build user monitoring and alerting into the instance AMI or bootstrap these capabilities during instance initialization. An alternative method is to use a configuration management tool to create a special user account during an emergency scenario, providing temporary emergency-only access as needed. These approaches to OS-level access must be tightly controlled and should alert the appropriate personnel whenever this emergency-only access is used.

Centralized Directory Service

A centralized directory service enables administrators to control user or group access to EC2 instance operating systems in alignment with their organization’s security requirements. This approach is more appropriate for customers whose users or applications regularly require OS-level interactive logins during deployment and configuration, or for day-to-day support and management.

A centralized directory service acts as a source of truth for users, groups, and privileges. Administrators can leverage the directory service’s user and group constructs to implement partial lights-out access on a per-user or per-group basis, and/or for specific groups of machines (e.g., allow only the production team to log in to production machines). This section describes AWS-managed and self-managed options for leveraging centralized user directories to manage access to EC2 instances.

AWS Managed Directories

**AWS Directory Service** is a managed service that makes it easy for a customer to deploy directory services into their AWS environment. It creates a central repository for managing user accounts and group memberships, and supports domain-joining Amazon EC2 instances running Linux and Microsoft Windows, Kerberos-based single sign-on (SSO), and group policies. In addition to automatically provisioning directory servers, AWS Directory Service automatically handles time-consuming tasks such as managing the deployment of directory servers across Availability Zones, replication monitoring, patch management, host monitoring and recovery, snapshot backups, and point-in-time recovery.

This option is appropriate for customers who have not yet implemented a central directory service or who are looking to deploy a separate directory service for AWS.

**AWS OpsWorks** is an application management service that makes it easy to deploy and operate applications on AWS. In addition to its application, OS, and application-stack configuration management capabilities, AWS OpsWorks allows administrators to control IAM user-level SSH or RDP access to Amazon EC2 instances. AWS OpsWorks leverages AWS IAM as a central user repository and automatically orchestrates the provisioning of local user access when a user is authorized for OS-level access to an EC2 instance.

For organizations that already leverage AWS OpsWorks for configuration management and application deployment, AWS OpsWorks OS access control features are a great way to manage access to their EC2 instances.

Self-Managed Directories

**AD Connector** enables AWS customers to easily connect existing Microsoft Active Directory (AD) servers to their AWS environment without complex directory synchronization technologies or costly federation infrastructure. It allows organizations to use their existing corporate credentials to log on to EC2 instances, provides federated access to the AWS console, and enables user access to AWS applications such as Amazon WorkSpaces, Amazon WorkDocs, and Amazon WorkMail. AD Connector provides a streamlined experience for existing end users and IT administrators, and enforces existing security policies such as password expiration, password history, and account lockouts for both on-premises and AWS resources.

This option is appropriate for customers looking to integrate an existing Active Directory infrastructure with their AWS resources without deploying additional infrastructure in AWS.

**Amazon EC2** allows AWS customers to deploy and manage Microsoft Active Directory or other directory service software on EC2 instances in their AWS environment. AWS customers can refer to the Active Directory Quick Start reference guide for architectural considerations and configuration steps for automatically deploying highly available Active Directory Domain Services (AD DS). This Quick Start includes best practices for launching and configuring the necessary AWS services for deploying a new AD environment or for extending an on-premises AD environment to AWS.

Self-managed directories on EC2 instances are an excellent option for customers looking to leverage their existing directory service expertise in their AWS environment.

---

## Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
</table>