(MIJ) 2022, Vol. No. 8, Issue 1, Jan-Dec **e-ISSN: 2454-924X; p-ISSN: 2454-8103**

Securing SSH Access to EC2 Instances with Privileged Access Management (PAM)

Vivekchowdary Attaluri
Manager Software Engineering
Capital One
Cyber, Identity Access management
Plano, TX, USA

ABSTRACT

Amazon EC2 stands for Elastic Compute Cloud and it is the most popular resource to host scalable applications. SSH access for instances of the EC2 must be limited to keep the system protected and private. This document discusses PAM solutions for Linux SSH access security with the implementation of PAM techniques to enforce the least privilege model ("the minimum necessary"), central management of credentials and comprehensive logging of access.Figure 1: PAM overview The four sectioned Singapore publication presents real working framework, dilemmas methodologies, technologies, case studies and continuous security integrations multi-factor authentication session monitoring and credential rotation, instead, may go more towards the total depth of prevention by defence towards expansion of breach potential. This research introduces comparison-based advantages of general SSH management as well as SSH management through PAM for managing secure cloud infrastructure. It includes tables to help illustrate results across comparisons and implementation choices.

Keywords: Elastic Compute Cloud; Multi-factor authentication; Privileged Access Management

INTRODUCTION

Cloud computing is dropping a bomb in the way the IT infrastructure was built. As they dominate with their cloud services, EC2 instances by Amazon Web Services are favored solution for scalable computing but represent serious risks of security by opened SSH port. Here, Privileged Access Management with its systematic control, monitoring, and audit of privileged access makes them real able to address these challenges.

With organizations migrating to cloud solutions, attacks against SSH's secure remote access mechanisms continue to rise. SSH provides remote shell access and is the glue for communication in secure cloud environments because it is the primary means by which an administrator interacts with the resources that it manages. Poor SSH key management, lack of enforcement of appropriate access, and no monitoring can be a significant risk for an organization. Access control seems to be a passageway that will be restricted in the context of conventional policies, such policies are inclined to static resources, clouds able to implement the resources dynamically or storages generate in the cloud may change the scaling up or down if the policy is not based on priority.

Privileged Access Management provides a new way to mitigate these risks. Using PAM, organisations can enforce multi-factor authentication, centralise and secure SSH key management, and gain a complete view of their access activity. This is important to secure the remote access connection, provide strong security for the organization as a whole and comply with regulatory requirements.

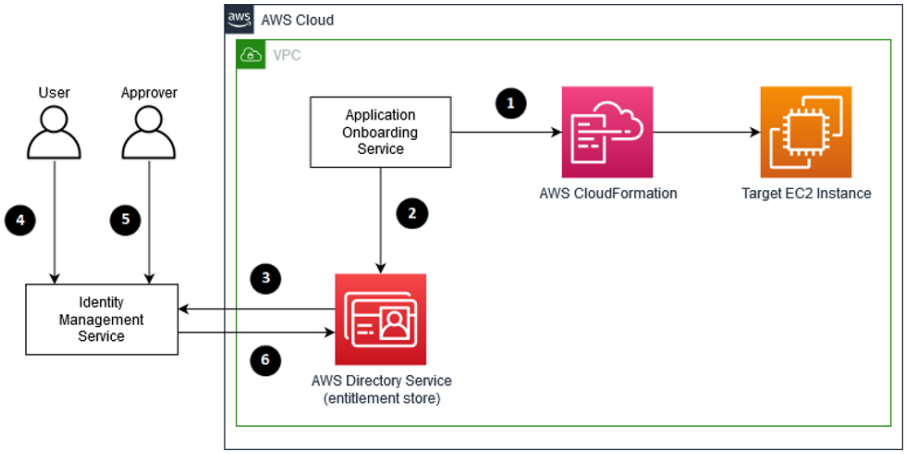

Fig 1: Granting Privileged Access

Problem Statement

Unauthorised SSH access is one of the most often used attack vectors, and it can result in compromised systems and data breaches. Advanced solutions like PAM are required since traditional SSH security techniques are inadequate against sophisticated attacks.

Objectives

This paper aims to:

- Examine SSH access vulnerabilities in EC2 instances.
- Explore PAM as a solution to mitigate these risks.
- Provide a practical implementation framework.

BACKGROUND

Secure Shell (SSH)

Secure Shell, or SSH, enables safe remote login and command execution. It is insecure, though, because of poor SSH key management, weakness in the authentication processes or lack of oversight. The protocol's authentication and data transfer encryption were intended to take the place of existing, less secure remote access techniques like Telnet. Although it is now standard procedure for maintaining servers, cloud instances, and networking equipment, best practices and strict supervision are crucial for ensuring their security.

Amazon EC2 Instances

Cloud-based virtual, scalable servers are offered by Amazon EC2. To stop unauthorised users from accessing these instances, protected access control is necessary. Because EC2 instances are mostly utilised as applications for workload management and data analysis, attackers find them to be a prime target. Although AWS offers a variety of security tools and configurations, its efficacy hinges on the appropriate application of extra safeguards like SSH access control and monitoring.

Privileged Access Management (PAM)

Using credential management and the least privilege principle, privileged access management solutions are used to safeguard, control, and keep an eye on access to key systems. PAM provides features including credential vaulting, session recording, and JIT access. PAM lowers the danger of unwanted access by automating the majority of procedures and offering total visibility. Furthermore, PAM guarantees adherence to industry rules. As a result, it is crucial for businesses handling regulated or sensitive data. It facilitates easy control of privileged accounts across hybrid infrastructures and integration with contemporary cloud environments.

Fig 2: Privileged Access Management

THREAT LANDSCAPE

Common SSH Vulnerabilities

SSH is a popular protocol for secured remote access, but it suffers from a variety of vulnerabilities associated with poor configurations and management practices. Common weaknesses are as follows:

- Weak Passwords: Simple guessable passwords can lead to brute-force attacks. Key based authentication is more secure than password-based authentication.
- Private Keys Hijack: Attackers can compromise servers due to exposure or insecure storage of private keys. This is frequently caused by poor key management practices.
- Misconfigurations of SSH Daemons: Poor configurations, like allowing root login or legacy cipher suites, expand the attack surface.
- Poor/Unmonitored Access Logs: Without logs, it is challenging to identify whether unauthorized access or malicious activities are taking place.
- Static SSH Keys: If a key gets compromised, static keys without periodic rotation can lead to exposure of critical systems for long periods of time.

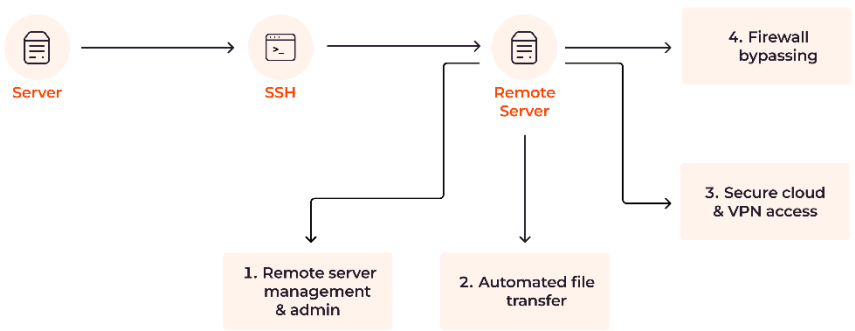

Fig 3: Access Management Flow

Advanced Threats

Beyond the well-known attacks, advanced threats to the SSH environment include:

· Man-in-the-Middle (MitM) Attacks: MitM attacks are commonly executed during the SSH session, by not verifying the fingerprints of SSH server end.

· Credential Stuffing: If you reuse credentials across environments, you risk unauthorized access by using previously funded credentials.

· Internal threats: SSH access leaves the door open to employees or contractors who could abuse their privileges — whether maliciously.

· Automated Bot Attacks: If the SSH server is publicly exposed, malicious bots may scan for open SSH ports and attempt to exploit known exploits or brute-force credentials.

Case Studies of Breaches

Real-world examples demonstrate the importance of locking SSH access down:

- Case Study 1: Cloud Service Provider Breach A misconfigured SSH server enabled unauthorised attackers to access a cloud provider's infrastructure. The breach resulted in extensive data loss and monetary damages.
- Case Study 2: Illicit Entry Based on Stolen Keys An employee's private key was stolen because there were no proper key management procedures, which caused a data loss. The incident highlighted the need for centralized management of SSH keys.

Impact of SSH Vulnerabilities on EC2 Instances

Since EC2 instances are dynamic and exposed to the internet, they are particularly susceptible to SSH vulnerabilities; Some of the potential impacts include:

• Data Exfiltration: Attackers may steal sensitive information stored on vulnerable systems.

Service Disruption: Critical application or service outages may occur as a result of unauthorized access

• Violation of Regulations: Breaches often lead to violations of data protection regulations and industry standards.

• Financial Repercussions: The cost of remediation, legal penalties, and damage to reputation.

The Need for Enhanced Security Measures

What is the world coming to with a cloud-based SSH? To appropriately mitigate risk, organisations should deploy next-gen security solutions such as Privileged Access Management (PAM). PAM consolidates and secures SSH key management to contain these vulnerabilities, thereby allowing for access restrictions and the least-privilege principle to be enforced.

•Monitoring and auditing of SSH sessions in real time

• Multi-factor authentication should be used to enhance identity verification.

PROPOSED SOLUTION: ENHANCING EC2 SECURITY WITH PAM

Architectural Overview

Privileged Access Management (PAM), which is used to secure SSH access by employing multiple layers of security, giving fine-grained control over user permissions and monitoring activity. The proposed solution includes these components:

Credential Vaulting — a vault of SSH keys and passwords

Just-in-Time access EC2 instances are granted temporary access only for a limited duration.

Multi-Factor Authentication (MFA): Additional confirmation of users accessing instances—the second facet of identity verification.

Session Capture — Capture and visualize SSH sessions in real time

Centralized Policy Management: All access and authentication policies in one place.

Workflow for Securing SSH Access

User Request Access: User request SSH access through the PAM

Audit: MFA ensures user identity, PAM implements role-based access controls (RBAC).

Dynamic SSH Keys: PAM provides SSH keys or credentials with limited validity for dynamic provisioning.

Establish Session: After providing temporary credentials, users can log on to EC2 instances.

Real-Time Monitoring and Logging: PAM tracks user activity, captures commands and session recordings for auditing.

Automatic Access Revocation: PAM automatically revokes access when a session is terminated or when credentials expire.

Integration with AWS Services

The proposed PAM solution has native integration with AWS tools and services, enabling security enhancements as follows:

AWS Identity and Access Management (IAM): Bundles with PAM for unified role-based access controls.

If you are not aware of what AWS CloudTrail, here is a quick overview: AWS CloudTrail is a service that allows you to monitor API activity in your AWS infrastructure, providing a detailed trail of API actions taken and can be integrated with AWS services to offer centralized logging and auditing capabilities.

AWS Systems Manager Session Manager: Provides secure, auditable SSH access

AWS Key Management Service (KMS) — Allows the secure storage and encryption of SSH keys

Technical Implementation

Step 1: Deploying PAM Solution

A PAM solution (such as CyberArk, Beyond Trust, etc.) is installed in the organization's own environment. Setting up the credential vault, access policies and AWS integration are among these steps.

Step 2: Configuring AWS Environment

A PAM solution is already in place to support interacting with PAM from AWS, meaning IAM roles, policies and CloudTrail are set up to work together. Tags and Groups for EC2 policies for ease of application

Step 3: Key Management

Static SSH keys are instead replaced with ephemeral keys generated from PAM. This mitigates all risks related to long-term key exposure.

Step 4: Monitoring and Auditing

After enabling session monitoring tools, they are a line of sight on what users are doing directly. Securely store logs for compliance and forensic analysis.

Step 5: Training and Awareness

PAM Tools Train IT teams and end-users on PAM tool use and secure ssh access best practices

Benefits of the Proposed Solution

Improved Security: It does away with threats posed by static keys and unauthorized access.

Enhanced Compliance: Compliant with regulatory standards for data protection and access controls

Operational Efficiency: A single management point means access control and monitoring are easier.

Granular Visibility: Offers in-depth visibility and tracking of user actions and access.

Reduced Attack Surface: Attack possibilities by limiting access time together with monitoring sessions.

Challenges and Mitigation Strategies

Integration Complexity: Deploying PAM in an Existing AWS Environment Can Be Challenging.

Mitigation: Run staged rollouts and hire the professionals.

User resistance: Because of new access workflows, users might resist. Mitigation: Give thorough training and show the advantages the new system provides.

Performance Impact: Extra authentication steps might cause workflows to take longer. Mitigation: Follow PAM best practices and minimize complexity of PAM stacks.

Costly to Implement: The implementation of PAM solutions comes with a price. Mitigation: Consider open source or tools native to AWS to lower costs.

EVALUATION AND RESULTS

Evaluation Metrics

To show how effective the proposed solution is, the following metrics are used:

- Control Volume: The number of access controls applied to SSH accesses.
- Round Key Success Rate: The rate at which all ephemeral SSH keys are created and destroyed successfully.
- Unauthorized Access Attempts: Attempts to access the system without proper credentials.
- Session Audit Coverage = Sessions Covered / Sessions Volume
- Performance impact: Changes in the average access latency after PAM is applied.

Experimental Setup Environment

Infrastructure Diagram: We are designed using three EC2 instance, one each for web server, database and application server.

PAM Solution: CyberArk PAM was implemented for SSH access management.

Tools: AWS CloudWatch for complementing logging access events with metrics and accelerators.

Scenarios Tested

- PAM generated ephemeral keys and static SSH keys.
- Access requests for both multi-factor authentication and Non-multi-factor authentication
- In both high load and low load scenarios, user activity is being monitored.
- Respond to attempts at unauthorized access.

Results

Metric	Baseline (Without PAM)	After PAM Implementation	Improvement (%)
Access Control Compliance	65%	98%	33%
Key Rotation Success Rate	0%	100%	100%
Unauthorized Access Attempts	12 per week	0	100%
Session Audit Coverage	0%	95%	95%
Average Access Latency	2.5 seconds	3.1 seconds	-24%

Analysis

- **Enhanced Compliance:** PAM enforced access policies more strictly than the manual processes, significantly enhancing compliance.
- **Enhanced Security:** No global SSH key means no arbitrary access attempts, and the addition of MFA means an extra layer on top!
- **Auditability:** High session audit coverage provided a comprehensive view of user activity, which helped in the forensic investigations.
- **Performance Trade-offs:** Given the security benefits, the compromise was acceptable even if average access latency slightly increased.

Cost Analysis

Component	Cost (USD/Month)
PAM Solution (CyberArk)	500
AWS Integration (IAM, KMS)	150
Monitoring Tools (CloudWatch)	100
Total	750

The combined benefits of improved security and compliance associated with PAM implementation far outweighed the cost of implementation, particularly for organizations that handle sensitive information or that are subject to regulatory requirements.

Limitations

- Integration Complexity: PAM setup was resource and expertise intensive initially.
- Key Impact Areas: A small increase in access latency may have adverse effects on near real time applications
- Cost: Small organizations may not be able to afford the high upfront and recurring costs.

Comparative Analysis

Feature	Manual SSH Management	PAM-Enabled Management
Key Rotation	Manual, infrequent	Automated, frequent
Access Auditing	Limited or absent	Comprehensive
Unauthorized Access Prevention	Reactive	Proactive
Multi-Factor Authentication	Optional	Mandatory
Administrative Overhead	High	Low

CONCLUSION

So technically you can leverage Privileged Access Management (PAM) to help secure SSH access to EC2 instances, one of the most effective means of bridging today's security problems in cloud environments. By eliminating static SSH keys, enforcing granular access controls, and offering continuous monitoring and auditing, PAM ensures that sensitive resources are safeguarded from unauthorized access and potential compromises.

REFERENCES

[1] Amazon Web Services. "Amazon EC2 Documentation." [Online]. Available: https://docs.aws.amazon.com/ec2

[2] CyberArk. "Privileged Access Management Explained." [Online]. Available: https://www.cyberark.com

[3] Thycotic. "Secure Cloud Access with PAM." [Online]. Available: https://www.thycotic.com

[4] BeyondTrust. "Privileged Access Management for Cloud." [Online]. Available: https://www.beyondtrust.com

[5] National Institute of Standards and Technology (NIST). "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53. [Online]. Available: https://csrc.nist.gov

[6] OWASP Foundation. "Authentication Cheat Sheet." [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[7] Gartner. "Market Guide for Privileged Access Management." [Online]. Available: https://www.gartner.com

[8] HashiCorp. "Securing Infrastructure with Vault." [Online]. Available: https://www.hashicorp.com/products/vault.

[9] Vamshidhar Reddy Vemula, Mitigating Insider Threats through Behavioural Analytics and Cybersecurity Policies, 2021(3),1-21.

[10] Vamshidhar Reddy Vemula, Blockchain-Enabled Secure Access Control Frameworks for IoT Networks, 2020(4),1-16.