Cloud Architecture Pattern

Cloud SAW

# Introduction

Cloud SAW (Secure Access/Administrative Workstation) is a cloud-hosted computing device, or a group of devices designed to provide secure access to sensitive data and systems. It is configured with security measures such as isolation, hardening, access restrictions, regular patching, logging, monitoring, and auditing. It helps to minimize the risk of compromise and ensure a secure operational environment.

# Context

* Controlled and audited access to any secure cloud environment that handles sensitive data and bound to compliance such as HIPAA and GDPR.
* A centralized access point for managing multiple and diverse cloud infrastructures.
* Secure remote administration of cloud resources.

# Architecture

A diagram of a software company

AI-generated content may be incorrect.

# Design Considerations

1. SAW should be hosted in a secure, isolated, and hardened network.
2. SAW must be protected with multi-factor authentication (MFA) and role-based access control (RBAC), following the principle of least privilege.
3. SAW should support and undergo regular, automated audits to ensure compliance with security policies and standards.
4. SAW should be provisioned automatically to eliminate manual errors and enforce consistency.
5. All activities performed on SAW must be continuously logged and monitored.
6. Clear governance policies should define usage restrictions, access rights, data handling, and incident response procedures.
7. Automated patch management and regular maintenance are essential to address known vulnerabilities proactively.

# Alternative Patterns

* Privileged Access Workstations (PAW)
* Jump Servers