National Security Agency

Cybersecurity & Infrastructure Security Agency

| Cybersecurity Information

Use Secure Cloud Identity and Access Management Practices

Executive summary

Users seeking alternatives to traditional on-premises (on-prem) infrastructure and services have turned to cloud technology increasingly over the years. These on-demand services allow for remote storage, compute resources, and sharing of data between authorized users that enables a wider range of collaboration and mission flexibility. However, cloud environments pose unique security challenges. Proper identity protection practices and access control policies are necessary to help provide integrity and confidentiality of data in the cloud. Malicious cyber actors (MCAs) frequently target cloud environments due, in part, to their remote nature and shared security models.

The purpose of this cybersecurity information sheet (CSI) is to explain some of the common threats to cloud identity management, and to recommend best practices organizations should employ to mitigate these threats when operating in the cloud.

Threat model

Increases in both telework and off-premises storage and services have rapidly expanded cloud reliance. Cloud environments are valuable targets for adversaries. As organizations continue to move data and services into these environments, MCAs can take advantage of the ubiquitous access clouds often provide. Identity and access management (IAM) is critical to securing cloud resources from MCAs. However, users can easily misconfigure access controls to accidentally allow open access to resources. Such misconfigurations are common and have resulted in massive data leaks.

For example, according to Website Planet, whose security researchers discovered and reported a data leak in October 2021 where a marketing research and conferencing company left an Amazon S3 bucket accessible to the public. The storage bucket reportedly contained over 8TB of customer data including business meeting recordings, audio transcripts, and more. [1] More recently, in May 2023 a corporation reported an incident in which a misconfiguration in their cloud environment made customer data (including names, phone numbers, emails, vehicle identification numbers (VINs), and more) publicly accessible potentially from October 2016 until May 2023. [2]

Initial malicious access attempts on cloud resources frequently target user credentials. For example, social engineering often targets users in an attempt to harvest credentials or get users to accept multifactor authentication (MFA) push requests. MCAs may also attempt to exploit external accounts that have been granted access to the organization's tenant.

ATT&CK® Tactic	Technique
Initial Access	Phishing [T1566]
Initial Access	Trusted Relationship [T1199]
Credential Access	Multi-Factor Authentication Request Generation [T1621]

Once an MCA compromises the targeted cloud environment, they may try to grant themselves roles or keys, or provision new accounts to escalate privilege, persist, or move laterally, targeting cloud services they have interest in or attempting to leverage federated identities to access the victim's on-prem environment.

ATT&CK Tactic	Technique
Persistence	Account Manipulation [T1098]
Persistence, Defense Evasion	Modify Authentication Process [T1556]
Persistence	Create Account: Cloud Account [T1136.003]
Lateral Movement	Remote Services: Cloud Services [T1021.007]

Security considerations

While many of the standard recommendations for securing identities on-prem still apply, there are additional considerations to factor in when managing identities for a cloud environment.

Identity management

Multifactor authentication

Single-factor authentication (e.g., password or PIN only) based account access is susceptible to credential theft, forgery, and reuse across multiple systems. Cloud accounts are generally globally accessible; thus they are more susceptible to certain types of single-factor authentication weaknesses. Multifactor authentication (MFA) boosts account security, better resisting compromise by enhancing user verification methods. MFA requires two or more factors for login: something the user knows, has, or is. Typically this is implemented using a password and a second factor usually based on a randomly seeded numeric token, a biometric option (such as a fingerprint or facial recognition), or a physical token (unique hardware-based identifier: smartcard, Common Access Card, etc.).

Many types of MFA are susceptible to phishing techniques[1]. Where possible, organizations should use phishing-resistant MFA methods such as public key (PK)-based Fast Identity Online (FIDO)/WebAuthn Authentication or public key infrastructure (PKI)-based MFA (e.g., CAC/PIV cards). Phishing-resistant MFA commonly leverages a hardware bound private key. If the device/token allows the private key to be exported that impacts the trustworthiness of the authentication factor, as the user may export the private key which may then be shared or otherwise compromised if improperly handled. Organizations using third-party MFA tooling options should maintain awareness of security relevant changes to the chosen MFA tooling, especially changes that may allow keys to be exportable. For further guidance on phishing-resistant MFA implementations, see CISA's fact sheet, Implementing Phishing-Resistant MFA. [4]

Managing PKI certificates

Certificates can be used in cloud environments in many ways. Two common types of PKI certificates used in cloud environments are client certificates and server-side transport layer security (TLS) certificates. Client certificates can be used for authenticating users to a cloud service (either solely or as part of an MFA solution) or to authenticate non-person entities (aka "workload identities" or "service identities") to other systems. As organizations increasingly deploy workloads in the cloud, TLS certificates for these applications must be properly managed. Proper management includes secure key storage and periodic key rotation, as well as implementation of key revocation.

Organizations using PKI certificates for user authentication should maintain a list of trusted certificate authorities, only allow trusted certificates, document revoked certificates, and remove users and block access associated with revoked certificates. For guidance on managing personal identity verification (PIV) cards for federal government use refer to FIPS 201-3. [5]

[1] For more details on phishing techniques refer to Phishing Guidance: Stopping the Attack Cycle at Phase One. [3]

When hosting workloads in the cloud, it is important to securely manage the TLS server certificates used for securing web communications and any client certificates used for inter-workload authentication. Some cloud services will manage the certificates for the customer automatically, but some deployments use customer-managed certificates.

Organizations using customer-managed application servers should refrain from storing private keys in plain text on the virtual instance hosting the server. Certificates should instead be managed with a key management system (KMS), which functions to store the encrypted keys, and control and monitor access to the keys. Key management systems can decrypt stored keys into memory for use in granting access as needed. Keys should also be regularly rotated through automated mechanisms. Misusing certificates weakens security and diminishes the integrity of the system. For more information on threats to TLS server certificates refer to National Institute of Standards and Technology (NIST) SP 1800-16. [6] For additional guidance on TLS implementations refer to NIST SP 800-52. [7] For more information on cloud key management, see the NSA and CISA CSI: Use Secure Cloud Key Management Practices.

Credential best practices

Misconfiguration and improper handling can expose user credentials to adversarial exploit. Cloud credentials should never be stored in plain text. If needed, users can leverage secrets management tools (preferably ones that use hardware security module (HSM) capabilities to protect secret keys) to manage cloud credentials (e.g., password managers for human secrets or secret stores for workload credentials). To further mitigate risk, users should disable features that allow web sites or programs to remember passwords. MFA, such as one-time PIN tokens, PKI tokens, or smartcards, for users and non-person PKI-based authentication (for workloads) should be implemented where possible.

In situations where PKI-based authentication is not technically feasible, secret keys can be generated to allow applications to manage cloud resources programmatically. When issuing keys for applications that need to interact with the cloud, it is vital that these be handled properly as MCAs see them as valuable targets. Each cloud service provider (CSP) offers different options for obtaining and managing these credentials so it is best to periodically review their guidance. Overall, it is best to avoid creating keys with root or administrative privileges. These keys should be generated for short-term use only, and accounts should be granted the least required privileges needed to accomplish operational tasks. These credentials should never be included in plain text in application source code or embedded into binaries. Instead, they should be handled securely by a secrets manager and stored encrypted. If using secure shell (SSH) key pairs to connect to cloud hosted virtual machines, the private key should be stored in a secrets manager and should not be shared.

Organizations should consider requiring administrators to connect to cloud resources using privileged access workstations (PAWs), which should be hardened according to established best practices, require MFA, and perform thorough logging. Administrators often require access to cloud resources through protocols such as SSH that do not always support these controls. PAWs are easier for organizations to control, properly harden, and monitor. PAWs can enforce MFA for all administrator actions, even when the protocol does not support it, and simplify auditing of administrator actions. This makes hardening and logging on the workstations simpler than on unmanaged devices. Some CSPs offer PAWs as a service to ease adoption of this security feature.

Identity federation

Organizations operating in cloud environments customarily federate identities to simplify managing identities across environments. Systems that federate identities from on-prem to cloud environments are frequently targeted by MCAs to allow movement between environments.

ATT&CK Tactic	Technique
Initial Access	Valid Accounts: Cloud Accounts [T1078.004]

The protection and monitoring of identity federation servers is crucial to overall security. Endpoint detection and response systems should be used on identity federation servers to identify exploitation attempts and changes should be routinely audited to identify potential compromise. Protect certificates and keys used for identity federation with a hardware security module (HSM). Organizations should also implement network segmentation principles to isolate these sensitive servers as much as possible. For more information on identity federation system architectures and security see CISA's report on Secure Cloud Business Applications Hybrid Identity Solutions Architecture. [9]

Access management

Managing conditional context-based access

While secure passwords, login tokens, and MFA are useful for protecting user accounts, MCAs may still be able to compromise a user's credentials. One way to limit the impact of such compromises is by implementing policies to enforce conditional access based on additional context. This context is expressed in policies, which can often be set for cloud tenants to restrict a user's ability to log in to a system if a predefined set of conditions are not met. For example, denying attempted logins made from outside permitted geographical locations based on their internet protocol (IP) addresses.

These controls can be especially useful for protecting privileged accounts—or accounts with broad/sensitive access—by requiring administrators to log into these accounts from the organization's on-prem facility. Organizations should thoroughly review and test their conditional access configurations and enforcement to prevent advanced cyber adversaries from exploiting gaps in these policies.

Encrypted channels for accessing resources

Controlling access is important when storing cloud data. Unauthorized access can degrade the overall security posture and negatively impact operations.

- Assign permissions appropriate for the needs of the authorized user to access the level of data required for a task.
- Continuously verify access and administrative privilege assignments to validate they align with the principle of least privilege.
- Enable monitoring and logging of access requests and policy changes.
- Investigate abnormal activity and requests.
- Encrypt data at rest and in transit, securely storing and managing cryptographic keys[2].
- Use secure protocols such as TLS1.2 or higher, using algorithms from the Commercial National Security Algorithm (CNSA) Suite 2.0 when possible and CNSA Suite 1.0 at a minimum for client connections to cloud resources[3].

[2] For more details, see NSA & CISA CSI: Use Secure Cloud Key Management Practices.

[3] For more details, see NSA & CISA CSI: Implement Network Segmentation and Encryption in Cloud Environments.

Separation of duties

Separation of duties is a critical concept when it comes to securing cloud resources. NIST defines separation of duties as “the principle that no user should be given enough privileges to misuse the system on their own.” [8] One way this can be accomplished is by requiring two-person controls for performing particularly sensitive operations.

Another method is by separating administrator roles to control how resources are accessed and managed. For example, access control administrators of the KMS with the necessary privileges to grant access to keys protecting sensitive data or capabilities should not be able to grant themselves access to use those issued keys. While there are cases where users should have the ability to create, manage, and use their own encryption keys, this is an important method of increasing the security of sensitive organizational data.

Additionally, write access to backups should be restricted to help counteract ransomware tactics, techniques, and procedures (TTPs) used by MCAs to target data backups. One way to reduce the risk of cloud environment data backup breaches is by provisioning separate backup management accounts for administrators who require access to the backups. These precautions limit the impact that an insider threat actor or MCA who has access credentials can do in a compromised cloud environment.

User data protections

User devices are a common attack vector for MCAs to gain access to an organization’s cloud environment. It is important for cloud users to practice good cyber hygiene where the devices they use to access cloud resources are concerned. Users should:

- Keep OS and applications updated and patched.
- Refrain from opening emails and web links from unknown parties to minimize phishing and malware infection opportunities.
- Change and remove defaults (e.g., default passwords and default user accounts).
- Monitor accounts for unexplained activities.
- Verify URLs to check for modified URLs designed to redirect users to spoofed websites.
- Consider the risks and benefits of allowing users to access cloud resources from unmanaged devices, such as bring your own device or personal computers.

Privilege controls

Improperly constrained user and application accesses can lead to excessive disclosure of sensitive data and promote malicious movement through the cloud. Follow the principle of least privilege and restrict accounts to only the resources needed to perform mission functions. When granting privileges, keep in mind that many cloud vendors use hierarchical permission schemes, so granting a user or group privileged access to a resource will grant them the same level of access to nested resources—that is, granting access to a “folder” or “organizational unit” grants access to all resources within that unit.

Different cloud vendors and services may offer different access control methods. The most common methods are:

- Role-based access controls (RBAC), and
- Attribute-based access controls (ABAC).

Most CSPs offer a hybrid of the two approaches, augmenting roles with attribute-based conditions to enforce conditional access. When using RBAC, organizations can assign privileges to roles and then assign users to a role, or roles, granting them the relevant privileges. When the privilege assignments to a role are altered, the update affects everyone assigned that role. ABAC is a key element for Zero Trust (ZT) maturity in the identity/user pillar. This method is used to control access to data by assigning attributes to resources and to users, providing more fine-grained policy protection to resources than using RBAC policies alone. For more information on IAM ZT maturity, see Advancing Zero Trust Maturity Throughout the User Pillar.

One way to manage enterprise permission controls and detect drift is by codifying permissions. Known as policy as code, this approach is beneficial for enterprise permission management as it can be used to create a known good state for permission settings, can be audited and version controlled, and can be used to detect drift. For more details on using policy as code in cloud environments, see the NSA CSI: Enforce Secure Automated Deployment Practices through Infrastructure as Code. In addition to policy as code, identity governance systems may be used to automate workflows to assign roles to individuals based on business needs.

Consider implementing the Just-in-Time (JIT) security practice where increased privileged access to applications or a system is limited to predetermined periods for specified activities. Privilege elevation with JIT should be logged and can require justification statements, if desired, for better tracking and verification of privilege requests.

Finally, avoid using privileged accounts for everyday activities, instead only use the privileged account for maintenance, updates, account management operations, threat-hunting operations, etc., that require privileged access. Periodically audit IAM configurations to confirm only necessary privileges are granted to users. Many CSPs offer services that will track unused privileges to help admins tailor accounts to the least privileges users need to accomplish their day-to-day responsibilities. However, it is important to consider occasional or emergency ("break glass") access when removing seemingly unused permissions.

Securing the cloud instance metadata service

The cloud instance metadata service (IMDS) can be queried from virtual instances in the cloud for general information about the tenant. However, this service can also be used to retrieve a variety of information, including IAM credentials that malicious actors can use to gain additional access to the cloud tenant.

ATT&CK Tactic	Technique
Credential Access	Unsecured Credentials: Cloud Instance Metadata API [T1552.005]

The exact implementation of the cloud IMDS will vary by CSP. Typically, MCAs query the IMDS by exploiting a server-side request forgery (SSRF) vulnerability in an application that customer organizations are serving publicly from an instance running in the cloud that has access to the IMDS. [10]

Use established best practices for protecting applications, such as sanitizing user input and deploying web application firewalls. These practices may prevent SSRF techniques that could use the application to query the IMDS and return credentials to the malicious actor. Use the most up-to-date version of IMDS available, as it may implement additional security measures. Restrict access to the IMDS for instances or accounts that do not require it. Each CSP's IMDS may work slightly differently; therefore, it is important to review the vendor's best practice guidance regarding their IMDS to take all possible precautions to prevent misuse of the service.

Best practices

It is important for organizations operating in the cloud to ensure employees understand the risks that arise from improper identity and access management. To reduce the risk of a cybersecurity incident, organizations should follow these best practices:

Identity management:

- Require the use of phishing-resistant MFA for user accounts.
- Do not store server TLS certificates in plain text on the virtual instance hosting a web server; instead, use a secrets manager.
- Handle user PKI certificates carefully to prevent unauthorized collection, and promptly revoke compromised or unnecessary certificates.
- Only use secret keys when required and provision them for short-term access with the least privileges necessary.
- Secure identity federation servers and audit identity federation to detect attempts by MCAs to abuse trust relationships.

Access management:

- Use context-based access control policies and review policies prior to deployment and periodically after deployment to identify potential gaps.
- Consider requiring administrators access cloud resources using PAWs.
- Limit use of administrative accounts and use JIT to limit privileged access and improve tracking of privileged actions in the tenant.
- Connect to cloud resources over an encrypted channel using secure protocols such as TLS 1.2 or higher and CNSA approved cipher suites (preferably CNSA Suite 2.0).
- Assign privileges according to best practices for access control by carefully applying the separation of duties and least privilege principles, and audit privilege assignments and access requests.
- Consider using policy as code to allow for improved tracking and review of access control policies, and frequently check for drift.
- Secure the cloud IMDS by restricting users/services with the privilege to query the IMDS, using the most up to date version, implementing vendor specific best practices, and implementing best practices to secure cloud-hosted applications and prevent SSRF vulnerabilities.

Further guidance

Supplementary NSA cybersecurity guidance is available at NSA Cybersecurity Advisories & Guidance. See below for a list of documents that are particularly relevant:

- Enduring Security Framework (ESF) Recommended Best Practices for Administrators: Identity and Access Management
- NSA's Top Ten Cloud Security Mitigation Strategies
  - Manage Cloud Logs for Effective Threat Hunting
  - Implement Network Segmentation and Encryption in Cloud Environments
  - Use Secure Cloud Key Management Practices
  - Enforce Secure Automated Deployment Practices through Infrastructure as Code
- Advancing Zero Trust Maturity Throughout the User Pillar
- CNSA Suite 2.0 Algorithms
- Top Ten Cybersecurity Mitigations
  - Top 10 Mitigation Strategies
  - Update and Upgrade Software Immediately
  - Transition to Multi-Factor Authentication
  - Defend Privileges and Accounts
  - Actively Manage Systems and Configurations

Additional CISA guidance includes:

- Implementing Phishing-Resistant MFA
- Phishing Guidance: Stopping the Attack Cycle at Phase One
- Secure Cloud Business Applications Hybrid Identity Solutions Architecture

Relevant NIST guidance includes:

- Securing Web Transactions: TLS Server Certificate Management
- Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- Digital Identity Guidelines

Works cited

[1] Website Planet. Report: Conferencing Service Exposes Private Customers' Meetings. 2022. https://www.websiteplanet.com/blog/civicom-leak-report/

[2] Toyota Motor Corporation. Apology and Notice Concerning Newly Discovered Potential Data Leakage of Customer Information due to Cloud Settings. 2023. https://global.toyota/en/newsroom/corporate/39241625.html

[3] Cybersecurity and Infrastructure Security Agency et al. Phishing Guidance: Stopping the Attack Cycle at Phase One. 2023. https://media.defense.gov/2023/Oct/18/2003322402/-1/-1/0/CSI-PHISHING-GUIDANCE.PDF

[4] Cybersecurity and Infrastructure Security Agency. Implementing Phishing-Resistant MFA. 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[5] National Institute of Standards and Technology. NIST FIPS PUB 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors. 2022. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf

[6] National Institute of Standards and Technology. NIST SP 1800-16: Securing Web Transactions: TLS Server Certificate Management. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf

[7] National Institute of Standards and Technology. NIST SP 800-52 Rev. 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

[8] National Institute of Standards and Technology. Separation of Duty (SOD). 2017. https://csrc.nist.gov/glossary/term/separation_of_duty

[9] Cybersecurity and Infrastructure Security Agency. Secure Cloud Business Applications Hybrid Identity Solutions Architecture. 2023. https://www.cisa.gov/sites/default/files/2023-03/csso-scuba-guidance_document-hybrid_identity_solutions_architecture-2023.03.14-final.pdf

[10] SANS Institute. Cloud Instance Metadata Services (IMDS). 2023. https://sans.org/blog/cloud-instance-metadata-services-imds-/

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademarks

ATT&CK and MITRE and are registered trademarks of The MITRE Corporation.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk:
NSA: 443-634-0721, MediaRelations@nsa.gov
CISA: 703-235-2010, CISAMedia@cisa.dhs.gov