IDENTITY MANAGEMENT IN HYBRID CLOUD IT INFRASTRUCTURES

Marius Toderici[1] and Aurel Mihail Titu[2,3]
[1]National University of Science and Technology POLITEHNICA Bucharest, Romania, ORCID 0009-0007-6065-6502, marius@toderici.ro
[2]Lucian Blaga University of Sibiu, Sibiu, Romania, Corresponding author, ORCID 0000-0002-0054-6535, mihail.titu@ulbsibiu.ro
[3]Academy of Romanian Scientists, 3 Ilfov Street, Bucharest, Romania

ABSTRACT: Identity management in hybrid cloud infrastructures must handle user access in both the organization's on-premises infrastructure and the cloud. The primary function of identity management is to grant users access to resources for which they have the appropriate rights, when needed, in a secure and transparent manner. To achieve this, a solution is required that provides an IAM authentication authority, enforces multi-factor authentication (MFA), and utilizes single sign-on (SSO) to simplify access and enhance productivity. Ensuring data security is a key priority for any IT team, as data is one of an organization's most valuable assets. A hybrid cloud infrastructure includes both on-premises data centers and local physical infrastructure, as well as cloud-hosted resources. Security is crucial for any organization, making the use of an SSO system highly recommended. SSO simplifies user access by eliminating the need to remember multiple complex passwords. Additionally, it is advisable to minimize password usage and promote "zero-trust" technologies, which enhance security while reducing the burden of complex password management imposed by security policies.

KEYWORDS: User management, hybrid cloud, privileged account management, IAM systems.

DOI 10.56082/annalsarscieco.2024.1.4

1. INTRODUCTION

Ensuring an organization's data security is a top priority for any IT team, as data is one of its most valuable assets. A hybrid cloud infrastructure encompasses both on-premises data centers and physical infrastructure, as well as cloud-hosted resources. Due to the distributed nature of equipment, different hosted systems, and disparate network architectures, ensuring security is a complex challenge.

To address these challenges, security assurance solutions should include:

- Interconnection with major cloud service providers (Amazon, Google, or Microsoft Azure) to enable secure connections, scanning, and management of cloud services. Without direct integration with these providers, maintaining data security becomes significantly more difficult.
- Artificial intelligence (AI) and machine learning (ML) components to assist IT teams in monitoring the vast number of devices and users. Many user behaviors follow identifiable patterns, and AI-driven behavioral analytics can detect vulnerabilities and threats in real-time more effectively than manual assessment.
- A centralized security analytics solution that collects data and presents it through dashboards, offering a comprehensive view of the hybrid infrastructure. With tools that provide centralized visibility, security teams can better correlate events and threats, enforce policies more efficiently, and enhance overall protection.
- Support for containerized environments, which has become essential. As organizations increasingly adopt virtual machines and containerized applications, many data transfers occur within containers rather than across networks. Traditional network segmentation is ineffective in these cases, making micro-segmentation and security enforcement at the container level crucial for maintaining data integrity.
- Log analysis and security information and event management (SIEM) to handle the large volume of security events generated by infrastructure components. Manual tracking and interpretation are infeasible for IT teams, necessitating SIEM solutions that automate log collection, security event correlation, and alert generation. Some SIEM systems also incorporate AI to enhance automation and improve threat detection.

Hybrid cloud security best practices employ a multi-layered approach to protection, leveraging log and event information managed by a security information and event management (SIEM) application within the service network (Figure 1). Modular hybrid cloud security systems operate at multiple levels, including the hypervisor, operating system, web server, database, and application layers, as well as network traffic analysis.

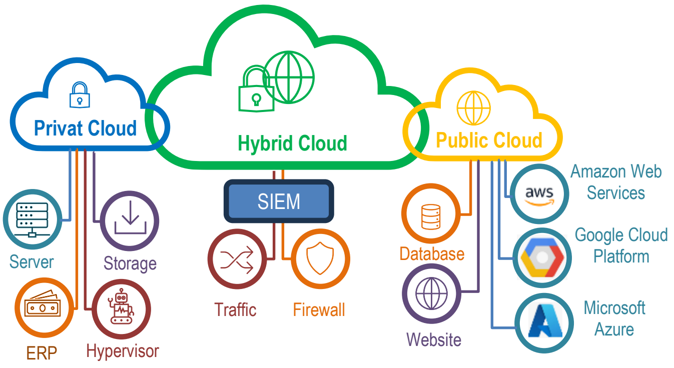

Figure 1. Ensuring security in hybrid cloud systems (Source cisco.com)

Network traffic—including both web traffic and other I/O transfer requests—is continuously scanned, monitored, and analyzed in real-time. Security solutions for hybrid cloud ecosystems must integrate with hypervisor-based software platforms that orchestrate virtual machines and containerized environments, ensuring comprehensive protection across the infrastructure.

2. IDENTITY MANAGEMENT IN HYBRID INFRASTRUCTURES

Identity management in hybrid infrastructures must handle user access across the organization's on-premises infrastructure as well as in the cloud. The primary function of identity management is to grant users access to the resources they are authorized to use, when needed, in a secure and transparent manner.

This requires a solution that provides an identity and access management (IAM) authentication authority, enforces multi-factor authentication (MFA) for enhanced security, and implements single sign-on (SSO) to simplify access and improve productivity.

Currently, there is no single solution for identity management in hybrid cloud infrastructures (Figure 3).

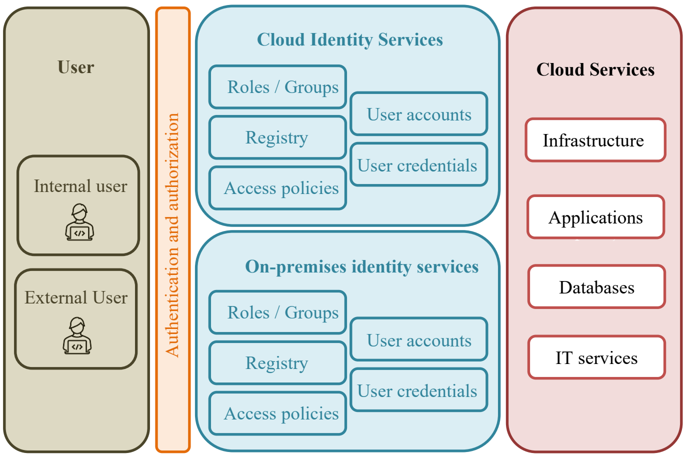

Figure 2 Identity management in hybrid cloud architecture (Source: cisa.gov)

In the following sections, we will present four of the most representative identity management models:

- Federated Authentication;
- Password-Through Authentication;
- Credential Synchronization;
- Cloud Primary Authentication.

2.1 Federated authentication

The federated authentication model allows users to authenticate both on-premises and in the cloud. In this model, a trust connection is established between the on-premises domain and the cloud, enabling users to authenticate locally and then access both on-premises and cloud resources. After local authentication via single sign-on (SSO), users are automatically authenticated when accessing cloud services.

In a federated setup, authentication is managed locally within the on-premises infrastructure. This approach is recommended for organizations that want to retain full control over authentication and avoid transmitting authentication policies outside the organization. Managing all authentication operations in a centralized system ensures that each user has a single record, allowing for unified policy enforcement and centralized tracking of authentication attempts.

Large organizations with multiple locations must also consider authentication latency. To ensure smooth operations, local authentication authorities should be deployed at remote sites and synchronized with the central authority.

From a security perspective, the on-premises environment serves as the source of user identity. If this service is compromised, an unauthorized user could exploit the trust connection between the two environments to gain access to cloud identity services. To mitigate this risk, organizations must implement robust security measures for their local Identity and Access Management environment and adopt Privileged Access Management (PAM) solutions. PAM helps reduce the risk of compromising local identity management services by enforcing stricter access controls for privileged accounts. [1]

2.2 Password through authentication

An alternative to the federated authentication model is password authentication. In this approach, authentication is performed locally by the organization's identity management service, with an additional agent-based service deployed on-premises to validate users directly with the cloud identity service. This setup allows the organization to maintain control over the authentication process and enforce security policies according to internal procedures. This architecture is implemented through a software agent installed either on the identity management solution itself or on an alternative component with access to the IAM system for user validation. The agent connects to the cloud identity service and operates in two modes:

- Request receiving mode – The agent directly handles authentication requests;
- Authentication request forwarding mode – If a user attempts to authenticate in the cloud, the agent forwards the authorization credentials to the local IAM system for validation. The authentication request is processed, and the response is sent back to the cloud identity service.

To reduce the risk of credential compromise, it is strongly recommended to implement multi-factor authentication (MFA) as an additional security layer. Similar to the federated authentication model, password authentication relies on the local identity management service, which must be highly secured to prevent unauthorized access. [4] Additionally, to ensure high availability, organizations should:

- Deploy redundant agents or connectors in case of failures.
- Implement local security controls at multiple endpoints to ensure continued access to the identity management system, even if the central node becomes unavailable.

2.3 Credential synchronization

Credential synchronization is another way of authentication in hybrid infrastructure. This modality is based on having the same account on both local and cloud infrastructure and the interconnected system ensures password synchronization. The user authenticates to the nearest cloud or local location using his credentials based on username and password. Using a single password simplifies users' lives. When they change their password the system will synchronize and transmit the new password to the entities responsible for authentication.

In this approach the organization has to regularly maintain the users' passwords, the frequency of synchronization is at the discretion of the organization. The source of user identity remains the local IAM service. In order to limit password guessing attempts for cloud authentication on the cloud side it is good to implement authentication protections by blocking access if the wrong password has been entered 5 or 10 times.[5]

2.4 Primary authentication in the cloud

Cloud Primary Authentication refers to a hybrid identity architecture that allows users to authenticate to the hybrid infrastructure through a cloud-based identity service. The authenticated user will have access to local applications as well as the cloud. User authentication is based solely on the identity service provided by the cloud. Integrating a cloud-based identity service into organizations requires more effort than other methods. [11]

The advantages of this method are the possibility to use different authentication methods in addition to multi-factor authentication. By using modern authenticators and open standards for authentication, organizations can more easily benefit from security, monitoring and other capabilities built into their cloud identity services.

A comparison of these types of identity management in hybrid cloud systems is shown in **Table 1**.

Table 1. Table comparing authentication types

How to authenticate	Location of the identity management authority	Advantages	Disadvantages
Federated authentication	Authority location is on-premises	Supports older methods of authorization and authentication. Supports password less authentication between on-premises and cloud infrastructure.	Higher authentication times for remote users if local authentication authorities are not put in place. Architecture complexity. Higher costs if deploying local authorities that interconnect with the central node.
Password through authentication	Authority location is on-premises	The user experience is good. Allows integration of SSO single sign-on.	Longer authentication times for remote users if local authentication authorities are not put in place. An agent must be installed on the identity management authority. Security is password based.
Credential synchronization	Authority location is on-premises and/or authentication service in the cloud	The user experience is good. Allows integration of SSO single sign-on.	Security is password-based. Brute force may be used in the attack. May need to install an agent on identity management authority.
Primary authentication in the cloud	The authentication service is in the cloud	The user experience is better. Benefit from all the advantages of cloud services. Can also be deployed in a federated model.	It relies exclusively on the cloud if it is unavailable users cannot log in. Lack of standards makes collaboration between different cloud systems difficult.

3. PASSWORD MANAGEMENT

The hybrid cloud infrastructure is complex, with the two systems interconnected: on-premises infrastructure and the cloud hosting a multitude of systems. Security is very important for any organization so the use of SSO [7] single sign-on is recommended to simplify the life of users who do not need to memorize different complex passwords. It is therefore recommended to use as few passwords as possible and the use of zero-trust technologies is encouraged to simplify the life of users and reduce the risk of using complex passwords imposed by security policies.

However, in many cases there are applications or systems that cannot integrate with new zero-trust technologies. For these situations it is beneficial to use password management applications. These password management applications allow the use of complex and strong passwords eliminating the need for users to remember these passwords. The use of these applications has several advantages such as the storage of complex passwords, the possibility to comply with password management policies, the possibility to store keys or certificates needed for various applications or services.

On the other hand, storing passwords in a single location also presents a risk, as this can be seen as a possible point of failure. If the password manager is compromised the stored passwords could be found by a malicious user and if the password manager is hosted outside the organization the availability could be affected which may prevent users from getting to the passwords and performing their work. The first risk can be mitigated by encrypting passwords and the second by using cache-based solutions that also reduce the availability risk. Modern password management solutions use encrypted transmission of passwords and they can only be decrypted by the user which reduces the risk of passwords being intercepted by a potential attacker. The stored passwords are also encrypted so that the password manager provider does not have access to the stored information and the encryption key is with the user, which is in line with the zero-trust policy.

There are several password management solutions on the market:

- Solutions for enterprise organizations - using PAM applications for hybrid environments that manage both user accounts and roles as well as passwords. There are several solutions on the market such as CyberArk and Delinea. These have connectors to most applications and services located on on-premises infrastructure or in the cloud.
- Cloud-based solutions - in this case users can access the account from multiple devices. Passwords are stored encrypted and can be accessed using locally installed apps, on mobile phones or via the browser. If an internet connection is not available to access the password manager applications use cache-based "vault copies".[11]
- On-premises solutions - the password manager is installed on the organization's local infrastructure. The user once authenticated to the local network can access the passwords in the vault without the need for an internet connection. This solution is good if the user will authenticate to the local network.
- Mobile solutions - modern mobile phones contain a built-in feature provided by operating system manufacturers that stores credentials both locally and, in the cloud, (Apple iCloud Keychain or Google Password Manager). This feature allows the user to log in via an account and access the saved credentials. In addition, the devices are protected by modern security methods. These password managers complement the organization's password storage and management solutions.
- Browser-based password management solutions - there are several browser applications that offer credential storage functionality (Firefox, Chrome, Safari, Edge). These store credentials locally and require authentication on a computer to access them. Once authenticated the user has access to this facility.
- Modern password management solutions are great for organizations because they add security, simplify users' lives and have many useful extra features.[8]

4. MANAGEMENT OF PRIVILEGED ACCOUNTS

Privileged accounts must be very well protected in any infrastructure because these accounts have full access to various resources that if they get into the hands of malicious people can cause great damage and loss to the organization. For these reasons these accounts must be very well secured and managed through clear and strict security policies. Using a privileged account management solution is very important in hybrid infrastructure (Figure 3).

A PAM solution for the hybrid environment will allow centralized management of privileged accounts in the two infrastructures the on-premises and the cloud allowing centralized and unified control of the entire hybrid environment.

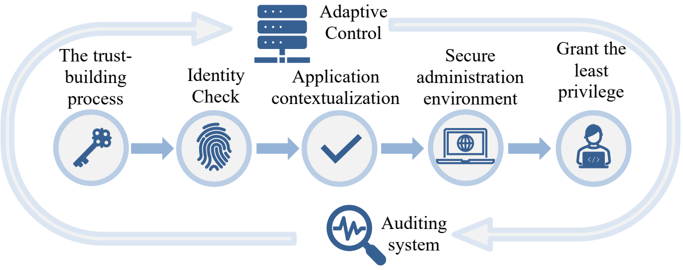
Adaptive Control
The trust-building process
Identity Check
Application contextualization
Secure administration environment
Grant the least privilege
Auditing system

Figure 3. Management of privileged accounts

A Privileged Access Management (PAM) solution for a hybrid cloud infrastructure should include at least the following key features:

- Integrate local infrastructure and local identity management as well as cloud infrastructure and cloud identity management providing a centralized and simplified view of privileged account management.
- Provide session logging and logging for all accounts used in the hybrid environment.
- Provide just-in-time (JIT) access for privileged accounts with the ability to segment the network and systems. The principle of granting the least privilege necessary being one of the basic security policies. Time-based access control provides balance between utility and security.
- Adopt zero-trust architectures as the basis of identity management security policy because hybrid infrastructure is outside the traditional perimeter providing remote, cloud, or intra-organizational access to resources. Identity management is key to implementing zero-trust policy.
- The use of protocols for MFA authentication is mandatory in this infrastructure which can be extended by using various additional user controls such as geolocation, device from which access is requested, network, risk-based assessment etc.
- Continuous monitoring of accounts to be able to detect abnormal behavior. Any action that is outside of security policies should be flagged to the security team so that appropriate action can be taken as soon as possible.

Last but not least, continuous user education is a crucial component of the security process. People are more likely to follow security protocols when they understand them, recognize their benefits, and are aware of their measurable consequences. User acceptance plays a key role in the successful implementation of security policies, making ongoing education and awareness essential for maintaining a secure environment.

5. CONCLUSIONS

Identity and Access Management (IAM) systems are essential for any organization, serving as a critical tool for IT teams to control and manage user access to sensitive information. These systems provide role-based access control (RBAC), enabling system administrators to regulate access to systems and networks based on user roles within the organization. IAM solutions can be deployed on-premises, in the cloud, or within hybrid IT infrastructures.

IAM systems play a crucial role in protecting access to an organization's resources. Given the multitude of processes, large user base, and complex IT ecosystems, IT administrators can no longer rely on manual, error-prone processes to assign and track user privileges effectively.

Accounts with elevated privileges (such as administrators and database administrators) have the highest level of permissions, making them prime targets for cyber threats. To mitigate security risks, it is strongly recommended to implement additional protection measures for these accounts. A compromise of privileged accounts can result in significant losses for an organization, regardless of whether the infrastructure is cloud-based, hybrid, or on-premises.

To enhance security, organizations should adopt Privileged Access Management (PAM) solutions, which provide additional layers of protection for privileged accounts. These solutions, as described in this article, help prevent unauthorized access, minimize the risk of credential theft, and ensure compliance with security policies.

6. REFERENCES

1. Jose Diaz Rivera, J., A. M.-C., *Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication,* IEEE Open Journal of the Communications Society, vol. 5, (2024).
2. Gooley, J., D. Y., *Cisco Software-Defined,* Cisco Press, (2021).
3. Leng, T., *SD-WAN Solution,* Huawei Technologies Co, (2024).
4. Thakur, M. A., R. G., *User identity & lifecycle management using LDAP directory server on distributed network.* International Conference on Pervasive Computing (ICPC), pp. 1-3. Pune, India, (2015).
5. Thakur, M. A., R. G., *User identity and Access Management trends in IT infrastructure- an overview.* International Conference on Pervasive Computing (ICPC), pg. 1-4, Pune, India, (2015).
6. Sarwar, M. I., Q. A., *Digital transformation of public sector governance with IT service management–A Pilot Study.* IEEE Access, vol. 11, 6490-6512, (2023).

7. Kihara, M., S. I., *Security and Performance of Single Sign-on Based on One-Time Pad Algorithm,* Cryptography, (2020).
8. Banciu, D., *Infrastructură de tip Cloud pentru Instituţiile Publice din România – ICIPRO. Big Data, The Cloud, Analztics – Triunghiul Profitabilităţii*, Bucureşti, (2016).
9. Mohammadinodoushan, M., B. C., *Resilient Password Manager Using Physical Unclonable Functions,* IEEE Access, vol. 9, 17060-17070, (2021).
10. Uddin, M., S. I.-N., *A dynamic access control model using authorising workflow and task-role-based access control,* IEEE Access, vol. 7,, 166676-166689, (2019).
11. Banciu, D., *Cercetare – Dezvoltare – Inovare prin soluţii cloud*, Mobile Innovation 2015, Bucharest, (2015).
12. TITU, M.A., Deac-Suteu. D., Toderici, M.I., *Catalogul de servicii informatice - Instrument pentru îmbunătățirea calității și securității suportului informatic într-o companie,* Acta Technica Napocensis, (2021).
13. Majumdar, S., Madi, T., Wang, Y., Jarraya, Y., Pourzandi, M., Wang, L., Debbabi, M., *Security Compliance Auditing of Identity and Access Management in the Cloud: Application to OpenStack,* International Conference on Cloud Computing Technology and Science (CloudCom) (pg. 58-65), Vancouver, Canada, (2015).