23.3. Identity Management and Access Control

Objective

23.3.1. Identities used for public cloud services are managed, protected, and consistently used to form a secure basis for controlling access to resources.

Context

Scope

23.3.2. This section is primarily concerned with the management of identities used to access or administer public cloud services.

23.3.3. Identities that interact with cloud platform management portals and application programming interfaces (APIs) to create, view, modify, or delete resources are considered privileged users in the context of public cloud.

23.3.4. Concepts used in this section related to identification management include:

a. Identity providers
b. Relying parties
c. Credentials, and identity information used in authentication
d. Policy decision points and policy enforcement points

These concepts are described in ISO/IEC IT Security and Privacy framework for identity management (ISO/IEC 24760-1:2019) and framework for access management (ISO/IEC 29146:2016).

23.3.5. Reference to other chapters and sections in this document is essential. In particular:

- Section 2.3 – Using cloud services
- Chapter 16 – Access control and passwords
- Section 16.2 – System access and passwords
- Section 16.3 – Privileged user access
- Section 16.4 – Privileged access management
- Section 16.7 – Multi-factor authentication

Overview

23.3.6. Public cloud services introduce new areas of risk associated with the management of identity and access, including:

a. Separation between identity providers and relying parties, with differing standards and capabilities for authentication, assignment of privileges, and access provisioning/deprovisioning.
b. Ubiquitous access to public cloud services, and in particular cloud administration services, from the internet.
c. The decoupling of the authentication and authorisation steps as part of access control (i.e., separation of the identity provider and the policy decision point/policy enforcement point).

23.3.7. This section highlights controls agencies can use to manage these cloud identity and access management risks and move towards a Zero Trust approach to information security.

Public cloud identity providers

23.3.8. There are three models of identity management commonly used with public cloud services:

1. Cloud accounts based on identities and authentication from other services or systems using identity federation (such as SAML V2.0 or OpenID Connect).
2. Cloud identities synchronised from an existing identity system.
3. Cloud identities directly provisioned in local cloud service identity stores, either manually or through automation following a standard specification such as the System for Cross-domain Identity Management (SCIM).

23.3.9. Due to the differing standards and capabilities offered by both identity providers and relying parties a combination of identity management models may be required to support the use of public cloud services.

23.3.10. Cloud-based identities may be issued and authenticated by different identity providers, each offering their own levels of assurance and receiving their own levels of trust from the identity consumer.

23.3.11. Identity providers are privileged entities that must prove a chain of trust, for example by strong cryptographic signing of authentication responses, to prevent a malicious actor tampering with authentication traffic as it passes between the provider and the relying party.

Public cloud access policy enforcement

23.3.12. Once an entity is authenticated, access control mechanisms determine what authorised actions are able to be performed and what resources can be interacted with.

23.3.13. Many cloud based system follow Zero Trust principles for access control, with access control determined by a combination of the cloud service's policy decision points and policy enforcement points.

23.3.14. The separation between the authentication and authorisation steps introduces the opportunity for unauthorised access to occur, through:

a. Misconfigured mapping between attributes asserted by the authentication provider and their use by the authorisation system.
b. Impersonation of authorised users through mimicking the authentication service assertions to the authorisation system.
c. Delays between a user being removed from the authentication system and re-authentication occurring.

23.3.15. The use of cloud services provides the opportunity to move from purely role-based access control (RBAC) to incorporating more attributes (than just role definitions) as part of attribute-based access control decisions (ABAC).

References

23.3.16. Further references can be found at:

Reference	Title	Publisher	Source
	Identification management	GCDO	Identification management | NZ Digital government
NIST SP-800-210 (2020)	General access control guidance for cloud systems	NIST	General Access Control Guidance for Cloud Systems | NIST
OpenID Connect	Welcome to OpenID Connect	OpenID	OpenID Connect | OpenID
SAML V2.0	SAML Wiki	OASIS Open	FrontPage - SAML Wiki (oasis-open.org)
RFC 7642	System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements	IETF	RFC 7642 - System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements (ietf.org)

PSR References

23.3.17. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR mandatory requirements	GOV2 - Take a risk-based approach GOV5 - Manage risks when working with others GOV6 - Manage security incidents INFOSEC1 - Understand what you need to protect INFOSEC2 - Design your information security INFOSEC3 - Validate your security measures INFOSEC4 - Keep your security up to date	Mandatory requirements | Protective Security Requirements
PSR protocol for information security	Management protocol for information security	Management protocol for information security | Protective Security Requirements

Rationale & Controls

Privileged account separation

23.3.18.R.01. **Rationale**

Separating administrative accounts between environments (for example cloud and on-premise) reduces the risk of a compromise in one laterally spreading to the other.

23.3.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7433]

Accounts used to perform privileged actions SHOULD NOT be synchronised between environments.

Username and passwords

23.3.19.R.01. **Rationale**

Credentials used to access public cloud services can be reused across cloud service providers, and are at risk of discovery or being easily guessed. Due to these services being directly accessible from the internet, authentication should not rely on a single factor for standard users, and must not for privileged users. Refer to section 16.4 Privileged Access Management (PAM).

23.3.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7436]

Where administration interfaces or portals are accessible from the internet, privileged accounts MUST be configured to use multiple factors of authentication.

23.3.19.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7437]

Where cloud service interfaces or portals are accessible from the internet, user accounts SHOULD be configured to use multiple factors of authentication.

Offboarding

23.3.20.R.01. **Rationale**

Public cloud services often rely on a Zero Trust approach to security where policy decision and policy enforcement points are used to control access based on authentication and privilege assignments. Timely removal of user access is essential to ensure unauthorised access to cloud services does not occur from former staff.

23.3.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7440]

Staff offboarding processes MUST be updated to include removing all access to public cloud based services, prior to implementation or adoption of public cloud services.

Authentication

23.3.21.R.01. **Rationale**

Identity providers are privileged entities that must prove a chain of trust to prevent a malicious actor tampering with authentication traffic as it passes between the provider and the relying party.

23.3.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7443]

Agencies MUST ensure that relying parties continually verify the authenticity of their identity provider's responses, through for example, cryptographic signing of authentication requests and responses.

Relying parties

23.3.22.R.01. **Rationale**

Cloud provider authentication services often provide additional information attributes to relying parties to inform authentication and access control decisions. These attributes may include information such as the individual's local time of day, the status of their device (including if it has been successfully used before), or their location.

23.3.22.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7446]

Agencies SHOULD ensure that relying parties use all available information from the identity provider to inform access control decisions.