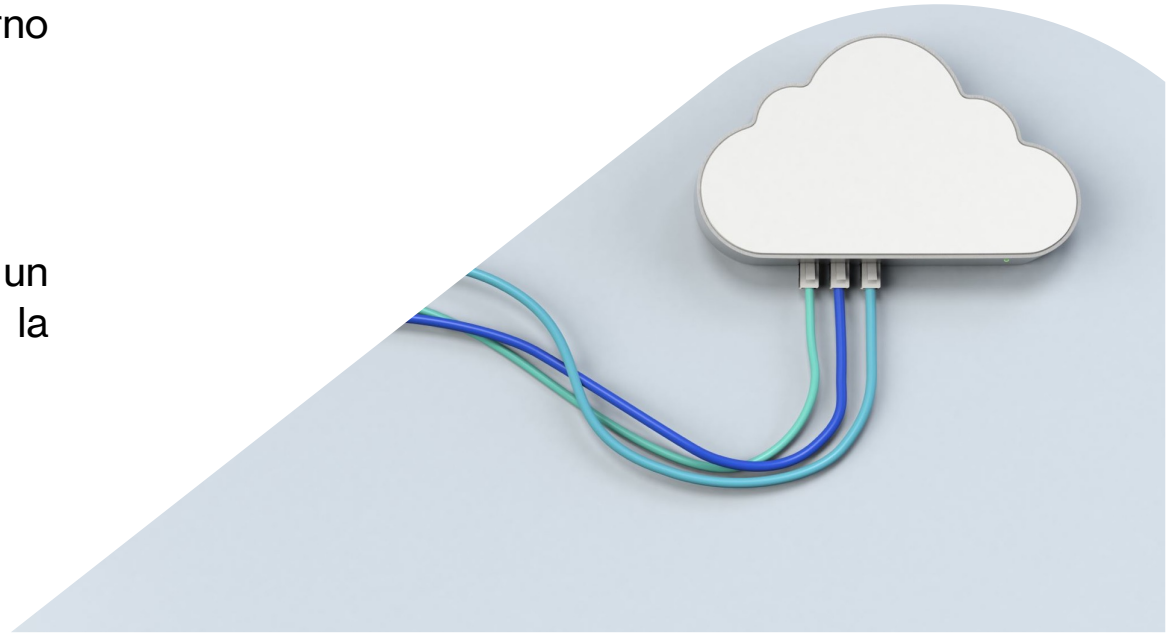

Identity and Access Management (IAM) On-Premise
Luisa Mele

Introduzione all'IAM On-Premise

L'Identity and Access Management (IAM) On-Premise è un sistema di gestione delle identità e degli accessi che opera all'interno dell'infrastruttura IT aziendale.

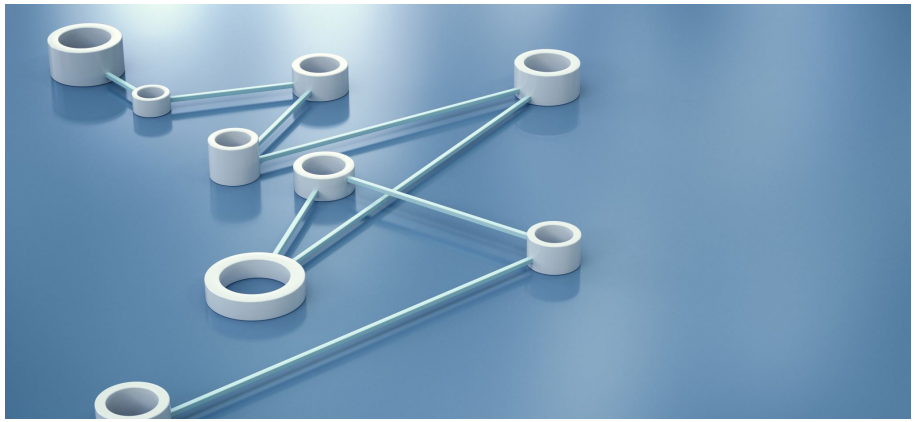
Vantaggi:

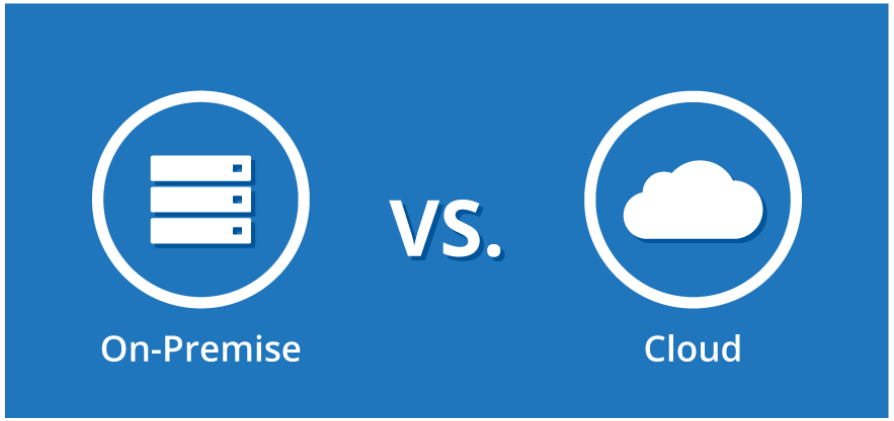
A differenza delle soluzioni cloud, garantisce un maggiore controllo sulla sicurezza e la conformità ai regolamenti.



Componenti Chiave di un IAM On-Premise

Un sistema IAM on-premise include directory service (es. Active Directory), autenticazione, gestione delle identità e degli accessi, oltre a strumenti per l'audit e la conformità. Questi componenti lavorano insieme per garantire accessi sicuri e controllati.



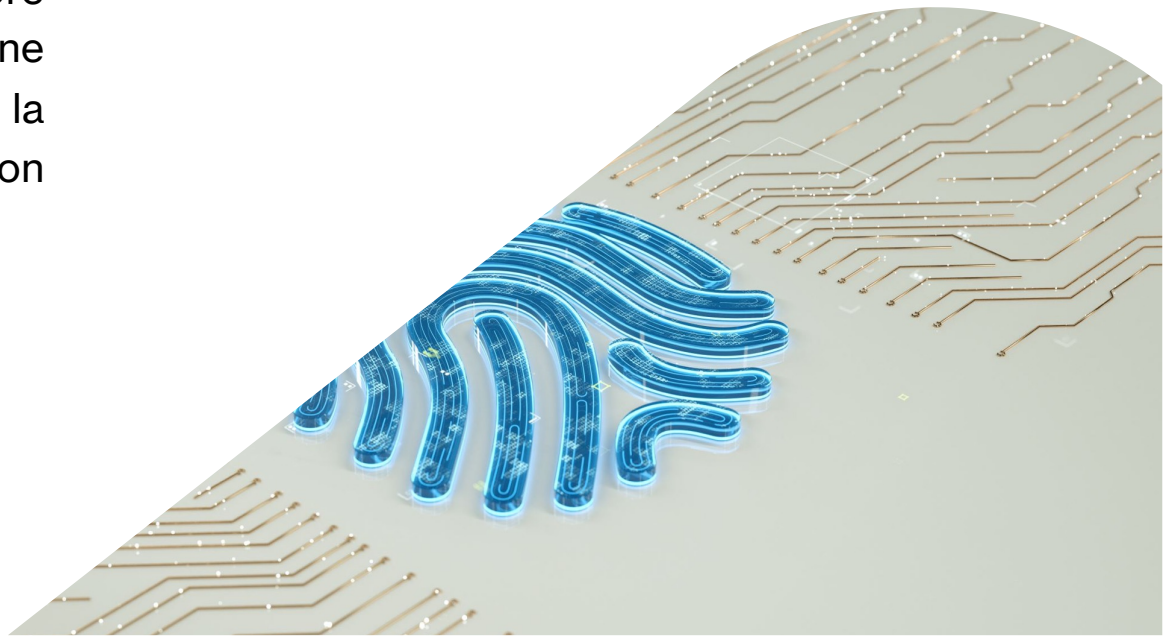


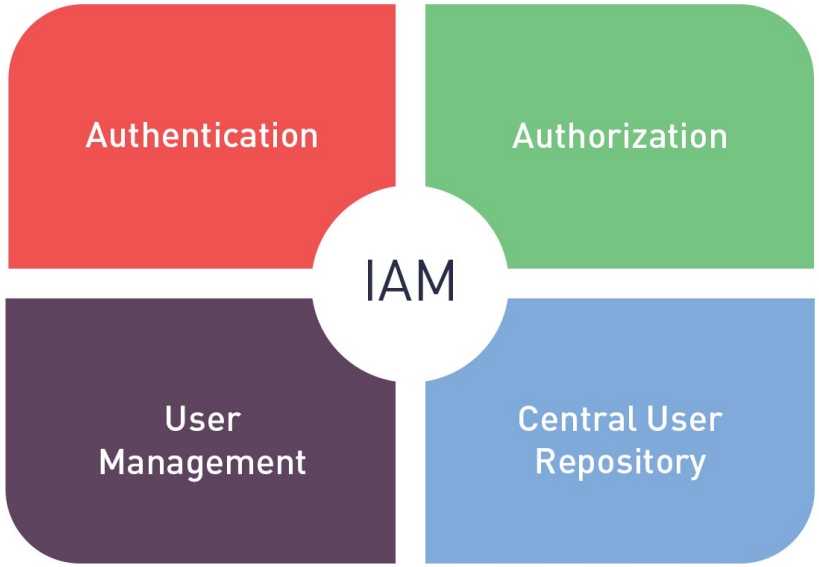
Differenze tra IAM On-Premise e Cloud IAM

IAM On-Premise offre maggiore sicurezza e controllo ma richiede più risorse per la gestione. Le soluzioni cloud, invece, sono più scalabili e flessibili. Sempre più aziende adottano un approccio ibrido per combinare i vantaggi di entrambi.

Tipologie di Autenticazione in IAM On-Premise

L'autenticazione può avvenire tramite Single Sign-On (SSO), autenticazione multi-fattore (MFA), certificati digitali e autenticazione federata. Queste tecnologie migliorano la sicurezza riducendo il rischio di accessi non autorizzati.





Modelli di Autorizzazione in IAM

IAM utilizza modelli di controllo degli accessi come RBAC (Role-Based Access Control) e ABAC (Attribute-Based Access Control) per limitare l'accesso alle risorse aziendali in base a ruoli, attributi e regole definite.

Tecnologie e Strumenti per IAM On-Premise

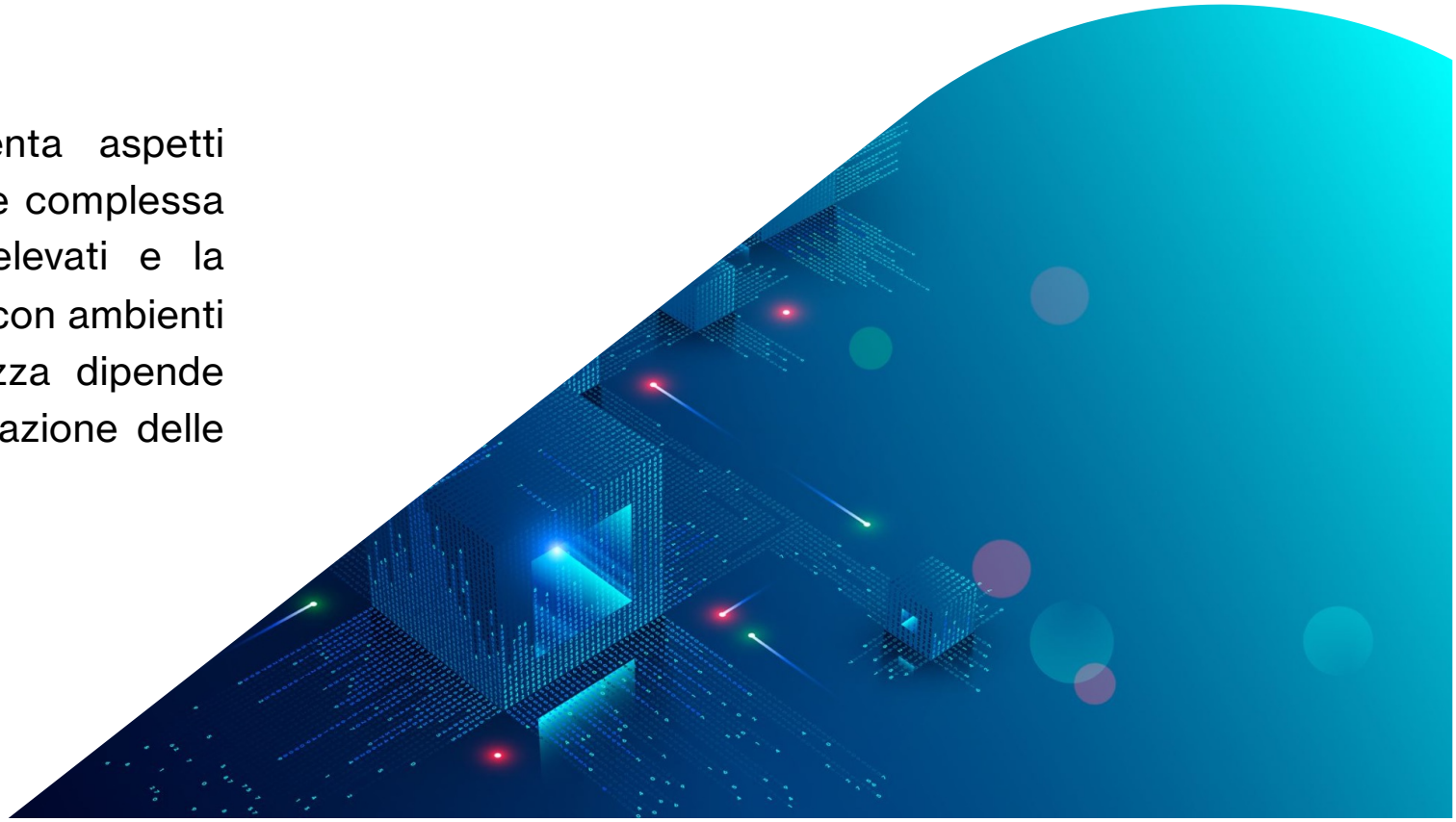
Le aziende possono implementare IAM On-Premise con strumenti come Microsoft Active Directory, OpenLDAP, FreeIPA e IBM Security Identity. Questi sistemi garantiscono un'identità centralizzata e sicura per gli utenti.

Sicurezza e Best Practices nell'IAM On-Premise

Adottare un approccio Zero Trust, implementare il principio del Least Privilege Access e utilizzare MFA sono fondamentali per ridurre il rischio di accessi non autorizzati e attacchi informatici.

Problemi Comuni dell'IAM On-Premise

IAM On-Premise presenta aspetti intricati come la gestione complessa delle identità, i costi elevati e la difficoltà di integrazione con ambienti cloud. Inoltre, la sicurezza dipende dalla corretta implementazione delle policy di accesso.



Installazione

- installazione:
  Server Manager > Ruoli > Active Directory Domain Services
  Creazione dominio: azienda.local
  Strutturazione con OU (Organizational Units)

OpenLDAP (Linux):

- Installazione:

Bash: sudo apt install slapd ldap-utils

Creazione utenti e gruppi con ldapadd

- **FreeIPA (Linux IAM)**

Configurazione su CentOS/RHEL:

Bash: sudo ipa-server-install

Integrazione con Kerberos

Grazie!