POWERCON2020

Azure AD Privileged Identity Management

Luca Cavana
CavanaSystems
luca.cavana@cavanasystems.com

@CavanaLuca

Speaker

Consulente IT
MCSA Windows Server
Hurricane Electric IPv6 Sage

10 anni di esperienza su:
Windows Server
Exchange Server
Azure AD
Office 365

Agenda

- Cos'è Azure AD Privileged Identity Management
- PIM per Azure AD
- PIM per Azure Resources
- Access Reviews

Azure AD Privileged Identity Management

Cos'è Azure AD PIM

- Servizio che ci permette di gestire, controllare e monitorare l'accesso alle risorse più importanti

Azure AD PIM permettere di gestire l'appartenenza ai *roles* tramite dei workflow di autorizzazione (eligible) e delle attivazioni a tempo (active)

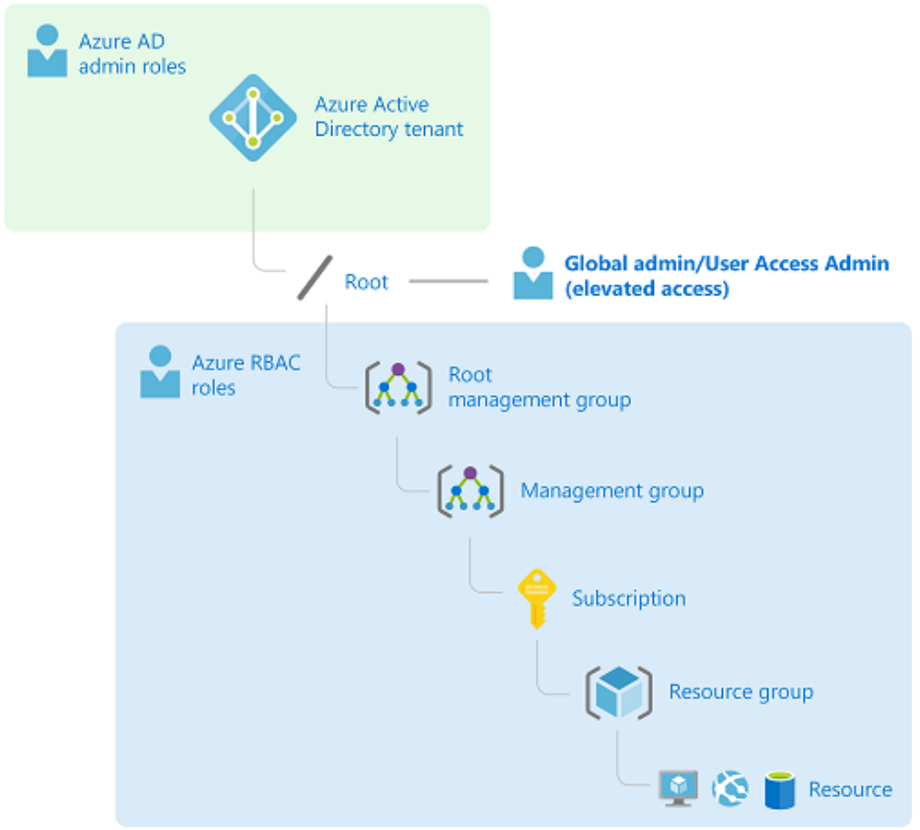
Perché Azure AD PIM

- Gli utenti privilegiati sono quelli più a rischio
- Per la compliance alle normative

Prerequisiti

- Azure AD Premium P2

Azure AD Roles vs Azure Roles



Ruoli Azure AD: Global Admin, Cloud Device Administrator, Password Administrator

Ruoli Office 365: Exchange Administrator, SharePoint Administrator

Ruoli Azure RBAC: Owner, Contributor, Virtual Machine Contributor, Storage Account Reader

Azure AD Roles

Il *Global Admin* che attiva PIM diventa *Security Administrator* e *Privileged Role Administrator*

I Roles di Azure AD hanno privilegi su tutto il Tenant

Sono disponibili in Preview le Administrative Units ma non sono supportate in Azure AD PIM

Possono essere Permanently Eligible, Eligible, Permanently Assigned, Assigned

Non tutti i ruoli Office 365 sono disponibili in Azure AD

Demo

Azure Resources

È analogo a come vengono gestiti i *Roles* di Azure AD, con alcune eccezioni:

- È possibile invitare utenti Guest
- Si applica sia alla Management Plane che alla Service Plane
- È valido solo per ARM

Le risorse vanno aggiunte tramite un processo di Discovery:

- Management Group
- Subscription
- Resource Group
- Resource

Una volta aggiunte PIM diventa lo *User Access Administrator* per la risorsa

Demo

Access Reviews

Permettono di automatizzare il processo di validazione degli accessi ad intervalli regolari

Consente di tenere traccia del motivo per cui un privilegio viene rinnovato oppure revocato

Può essere assegnato in self-service oppure ad un revisore formale

Il servizio può esprimere delle raccomandazioni

- Basate sul pattern di utilizzo delle utenze
- Possono essere utilizzate come suggerimenti o applicate direttamente

Demo

Grazie

Luca Cavana
CavanaSystems
luca.cavana@cavanasystems.com

@CavanaLuca