SECURITY SUMMIT

14-15-16 marzo 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

Sessione

Active Directory: scopri le strategie per migliorarne sicurezza ed operatività

Elia Mariani, Sales Account Manager, One Identity

Maurizio Ostinet, Solutions Architect, One Identity

14 marzo 2023 orario 14.00-14.40

Elia Mariani

SALES ACCOUNT MANAGER, ONE IDENTITY

Maurizio Ostinet

SOLUTIONS ARCHITECT , ONE IDENTITY

Active Directory è la Chiave di volta

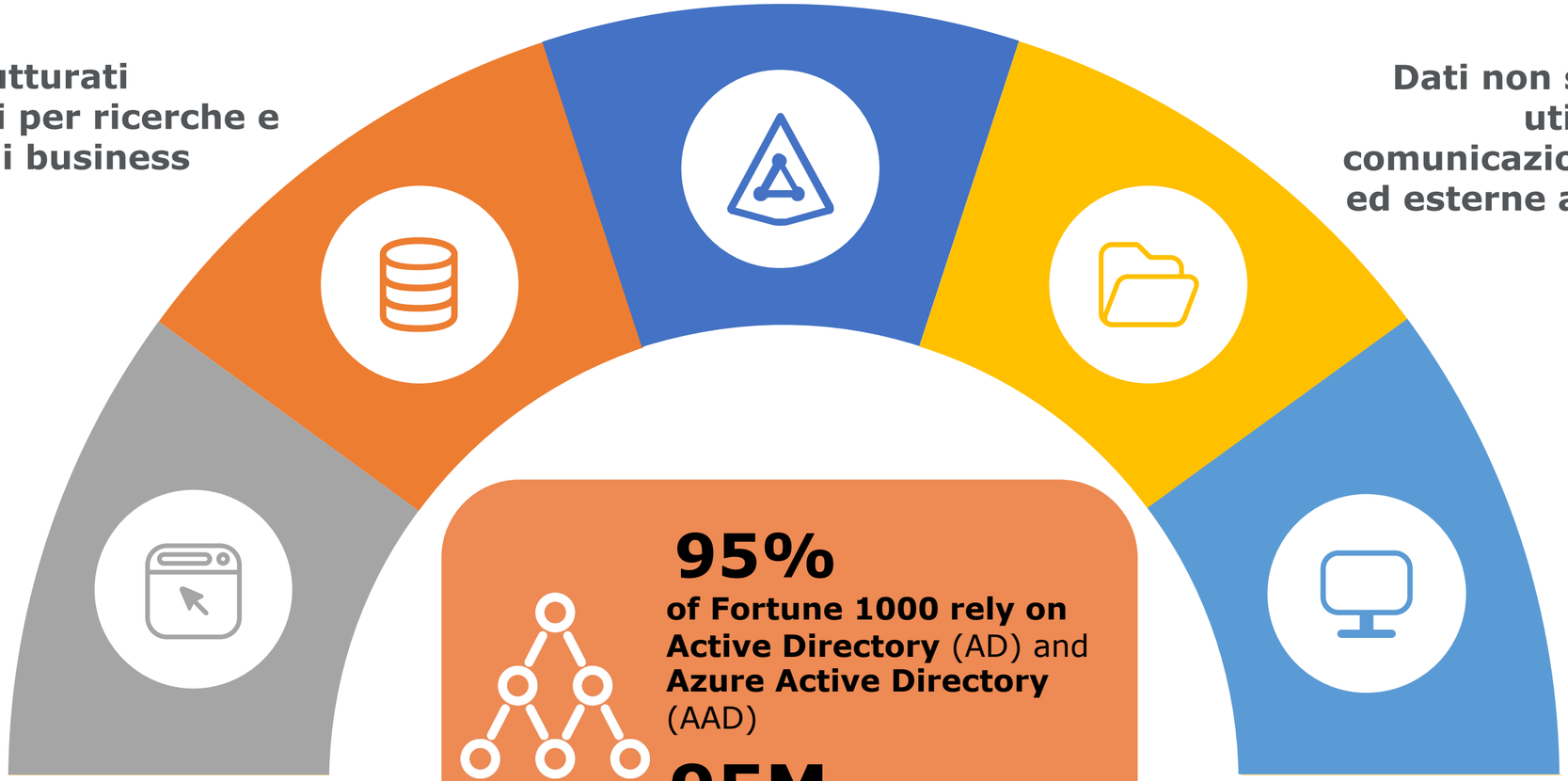
Active Directory
Provider primario di autenticazione e accesso

Dati strutturati utilizzati per ricerche e analisi di business

Dati non strutturati utilizzati per comunicazioni interne ed esterne all'azienda

Applicazioni

Computer, tablet, smartphone utilizzati per consumare le risorse di business



95%
of Fortune 1000 rely on Active Directory (AD) and **Azure Active Directory** (AAD)

95M AD accounts are attacked daily

Senza Active Directory …

… Tutto il resto cade a pezzi

Active Directory / Azure Active Directory – Quali strategie di protezione mettere in campo?

Gestione ciclo di vita User-Account

Account privilegiati

Accesso Role-based

Delega amministrativa granulare

Auditing

Mettere in Sicurezza e Gestire Active Directory / Azure Active Directory con One Identity Active Roles

Analizzare regolarmente gli Account

1. Generare una lista di user accounts – si tratta semplicemente di eseguire qualche comando in PowerShell, un esempio è reperibile qui: https://www.ultimatewindowssecurity.com/tools/Output-ADUsersAsCSV/

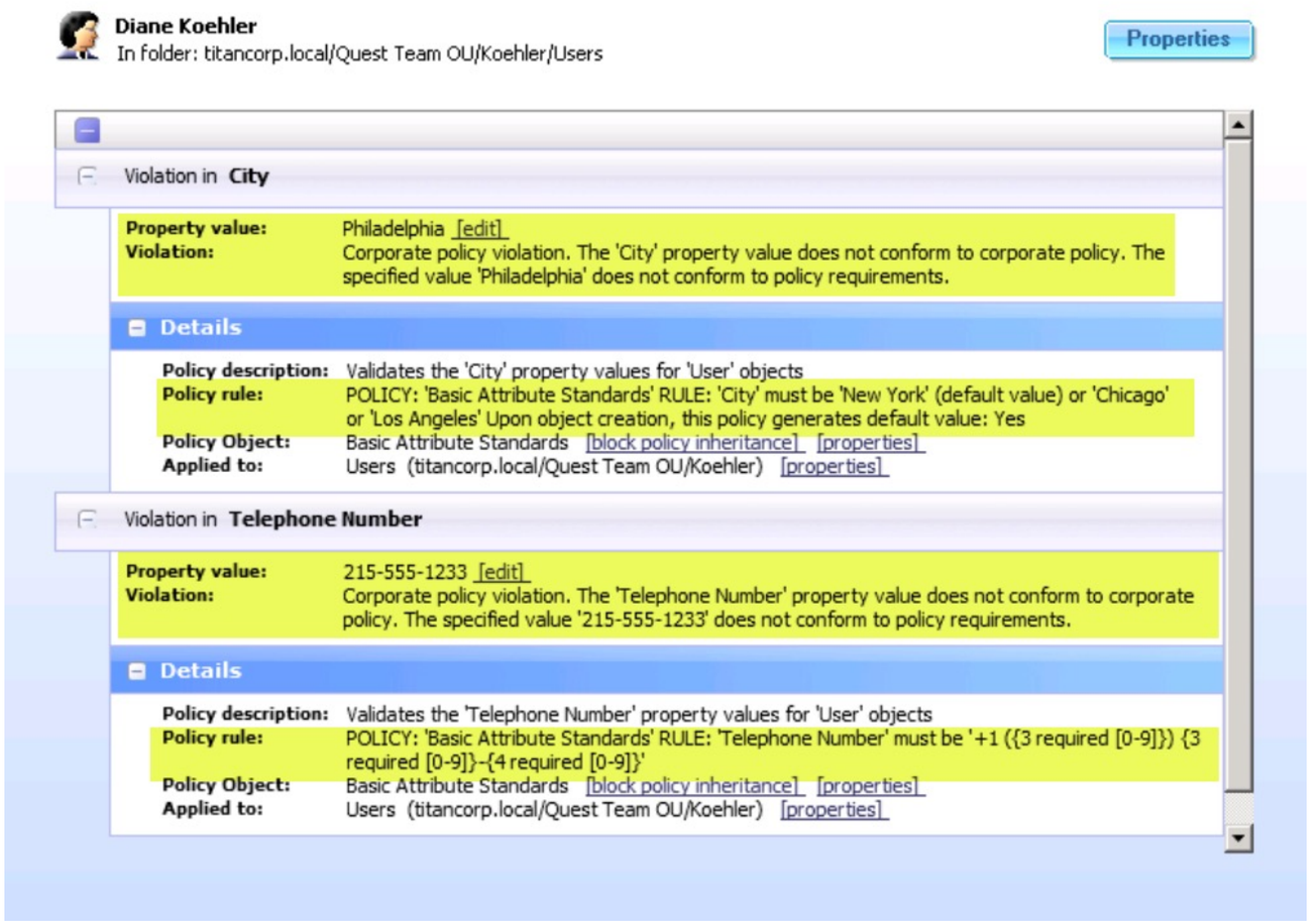
	A	B	C	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Distinguished Name	Display Name	SAM ID	Description	Office	Phone	E-mail Address	Job Title	Dept	Org	Company	Manager	Can user change password ?	Does password expire?	Is account disabled?	Account Expiration Date	Last Log-on Date	Has user ever logged on?
2	CN=Administrator,CN=Users,DC=mt	Administrat	Built-in account for administering the computer/domain										Yes	Yes	No		10/13/12	Yes
3	CN=Guest,CN=Users,DC=mtg,DC=lo	Guest	Built-in account for guest access to the computer/domain										Yes	No	Yes			No
4	CN=krbtgt,CN=Users,DC=mtg,DC=lo	krbtgt	Key Distribution Center Service Account										Yes	Yes	Yes			No

2. Filtrare i risultati per trovare account che non sono conformi alle security policy
   - password senza scadenza
   - includere criteri di filtro per eliminare eccezioni (es. service accounts)
3. Analizzare la lista risultante ed effettuare le opportune azioni di bonifica

Analizzare regolarmente gli Account con Active Roles

Active Roles consente di comparare la configurazione e lo stato degli oggetti di AD con un modello, che fa riferimento alle policy aziendali.

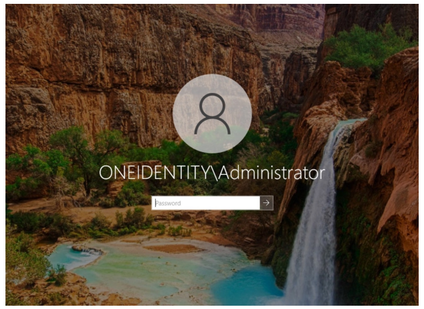
I risultati di questo confronto possono essere visualizzati on-demand sulla console o tramite report schedulati e inviati via email.

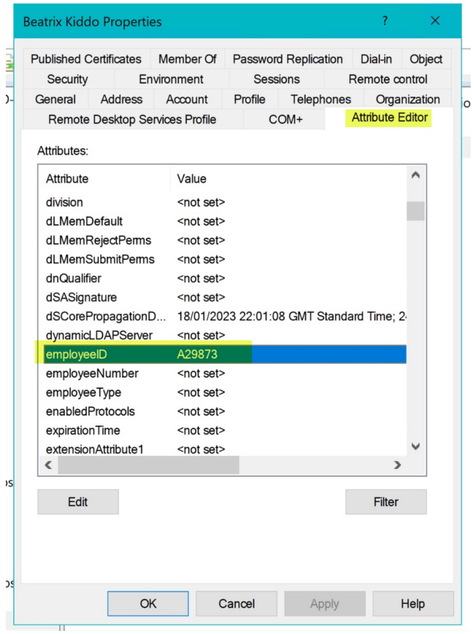


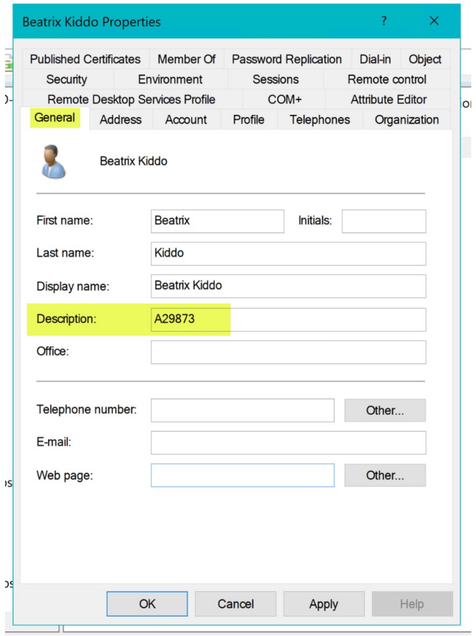
Associare gli Account alle Identità

Esistono varie opzioni per creare un link tra gli Account ed il database HR

- utilizzare l'attributo ***Employee ID***
- utilizzare il campo ***Description***
- inserire la matricola nel ***logon name***

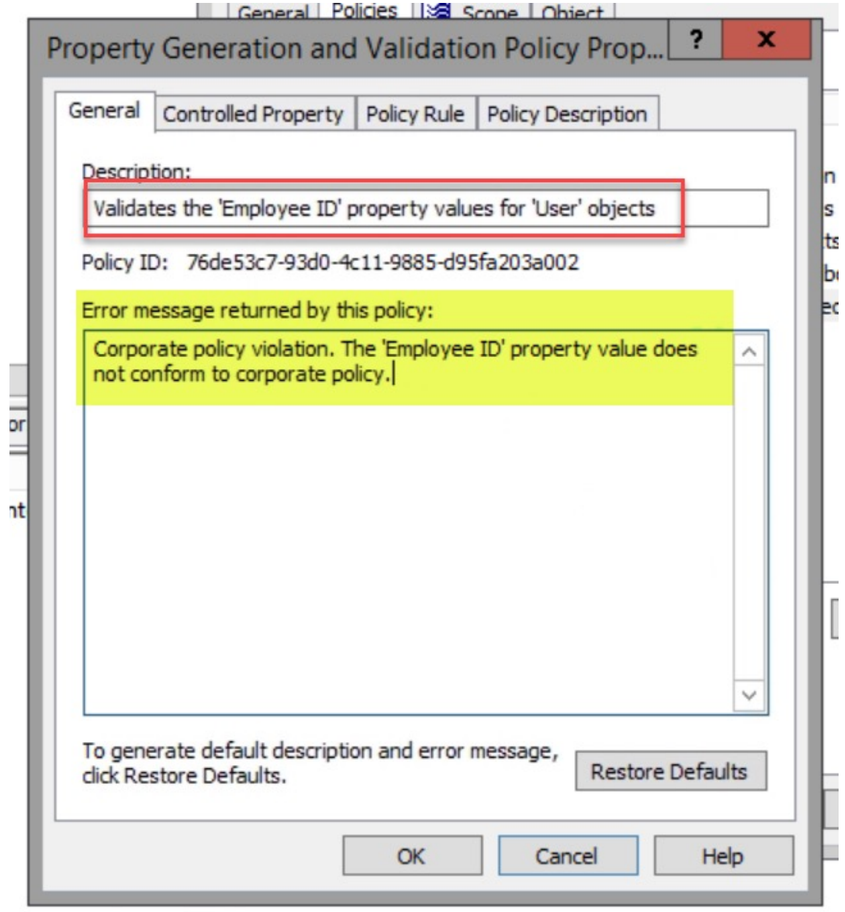






Associare gli Account alle Identità (persone fisiche) con Active Roles

Attraverso le Policy di Active Roles è possibile imporre che TUTTI gli Account abbiano l'attributo **Employee ID valorizzato** secondo un determinato formato



Rilevare la presenza di nuovi Account

- Gli attaccanti tipicamente creano **account da usare come backdoor**
- **Tracciare** la presenza di **nuovi account** è fondamentale ma è spesso **un'attività onerosa**
- L'ideale sarebbe riuscire a tracciare un account al momento della sua creazione, identificando ad esempio: **Chi ha effettuato la creazione?** Perchè?

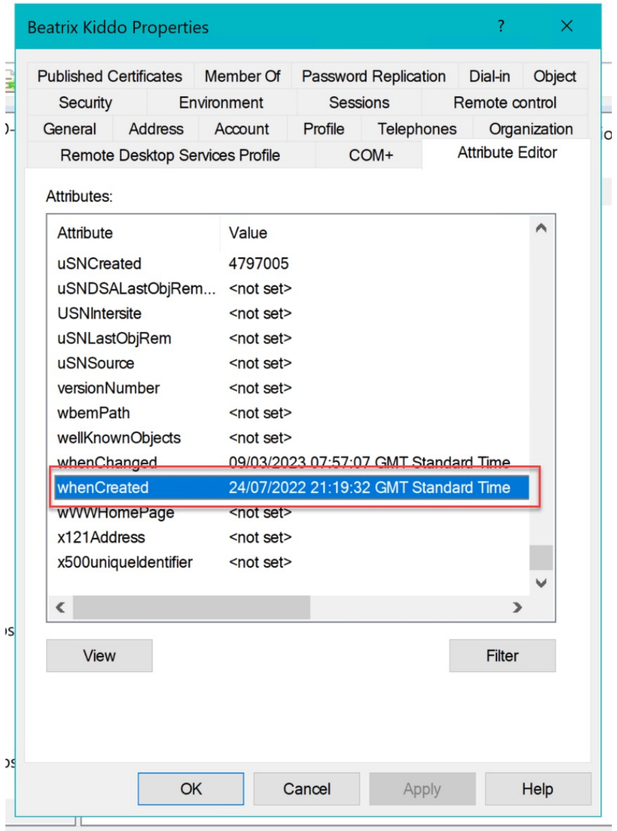
Rilevare la presenza di nuovi Account

- Cercare nei security logs del domain controller l'**evento 4720**
- Analizzare l'attributo ***WhenCreated***

Controllare:

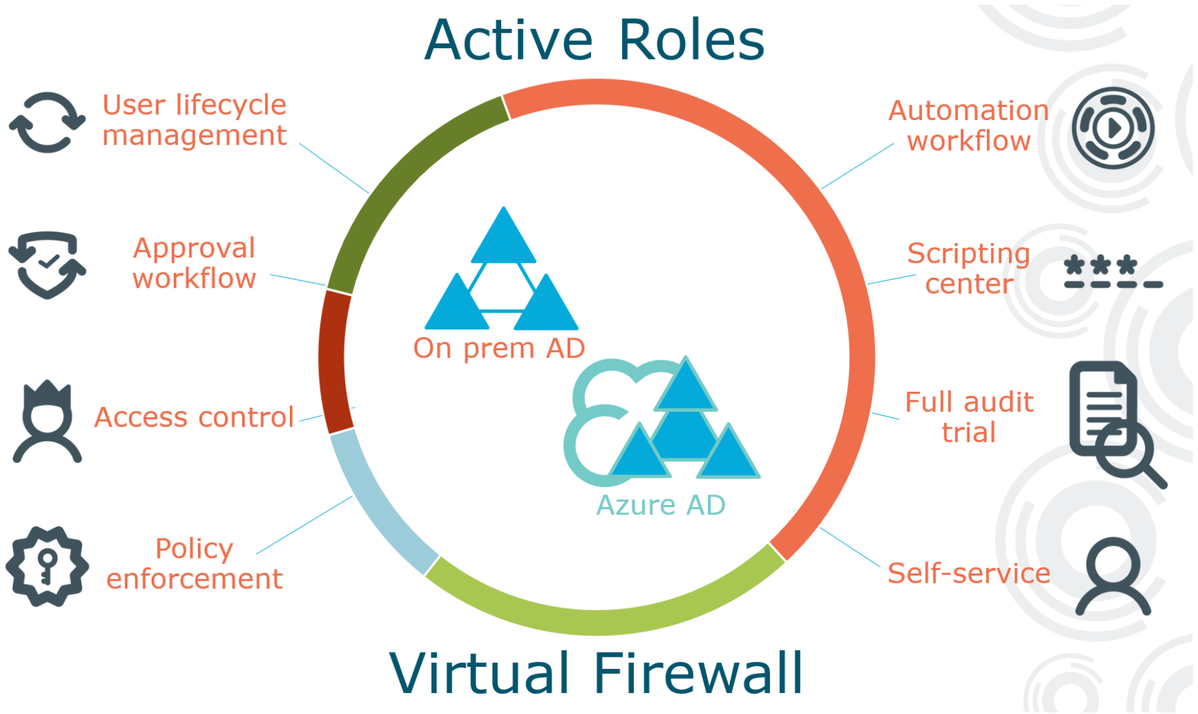
- Esistenza di un ticket o di documentazione in grado di **validare la creazione**
- Corrispondenza degli attributi rispetto alla **naming convention** definita
- Conformità con standard e **policy di creazione degli account**

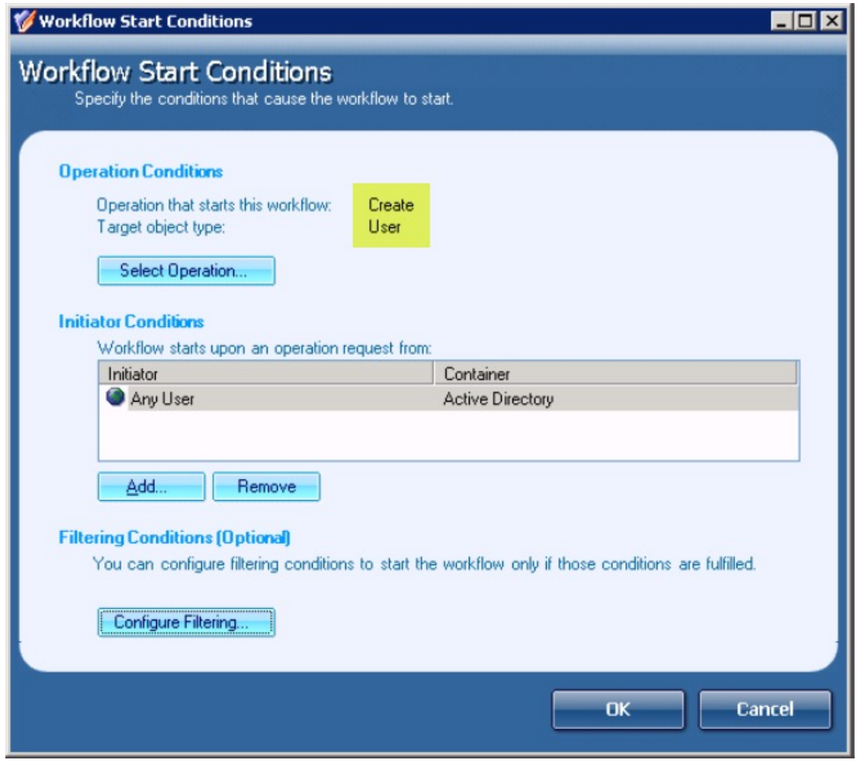
```
Event ID 4720 - A user account was created
Subject:
      Security ID: ACME-FR\administrator
      Account Name: administrator
      Account Domain: ACME-FR
         Logon ID:
0x20f9d New Account:
      Security ID: ACME-FR\John.Locke
      Account Name: John.Locke
      Account Domain: ACME-FR
Attributes:
      SAM Account Name: John.Locke
      Display Name: John Locke
      User Principal Name: John.Locke@acme-fr.local
```



Rilevare la presenza di nuovi Account con Active Roles

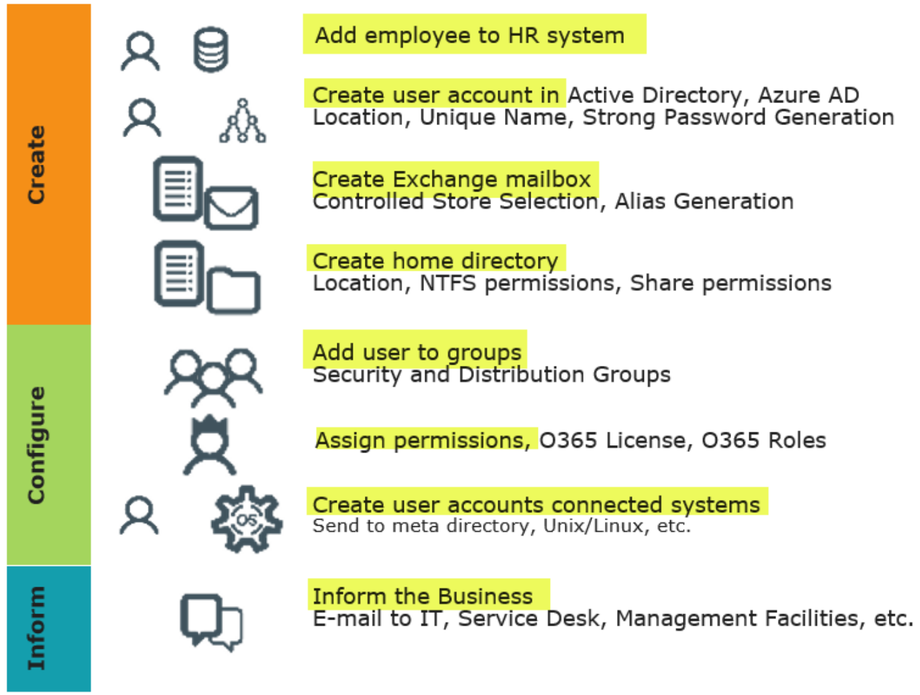
Active Roles agisce come un firewall virtuale
a protezione di Active Directory / Azure AD





Automatizzare i processi relativi al Ciclo di vita degli Account

E’ necessario automatizzare il più possibile i processi coinvolti nella creazione degli account allo scopo di ridurre la probabilità di errori umani.




```
New-ADUser -Name ‘randyjones’
-SamAccountName randyjones – AccountExpirationDate 01/01/2030
-GivenName ‘Randy’ -Surname ‘Jones’
-DisplayName ‘RandyJones’
-Path ‘CN=Users,DC=acme,DC=local’
– EmployeeID ‘93299’
-OfficePhone‘27884’
-Title ‘CEO’

Enable-Mailbox -Identity acme\ randyjones -Database Database01

Add-ADGroupMember Group1 acme\randyjones
Add-ADGroupMember Group2 acme\randyjones
```

Automatizzare i processi relativi al ciclo di vita degli Account con Active Roles

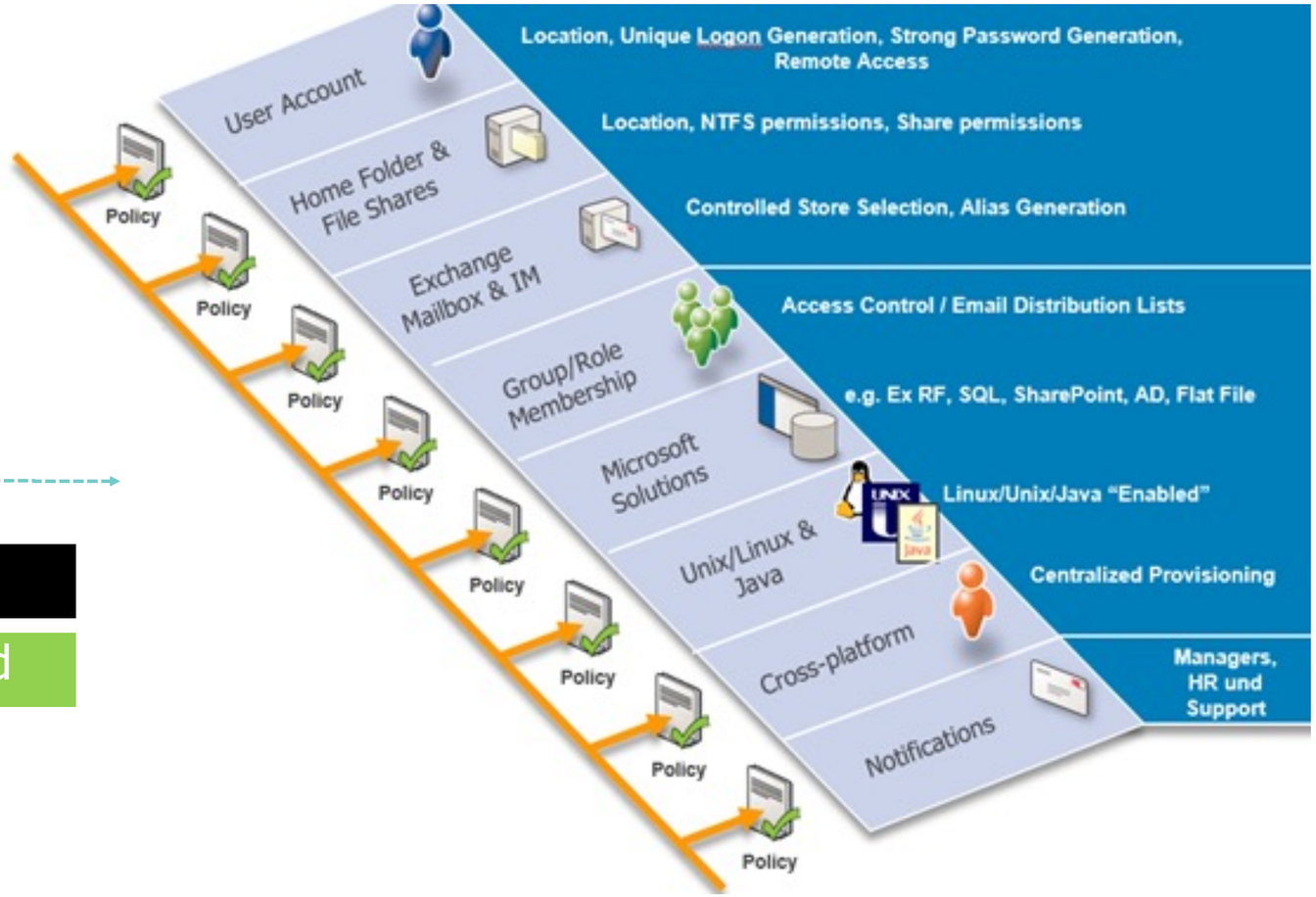
HR System

- **Joiner**
- **Mover**
- **Leaver**

Active Roles

Automated

Policy-based



Gestire gli Account "dormienti"

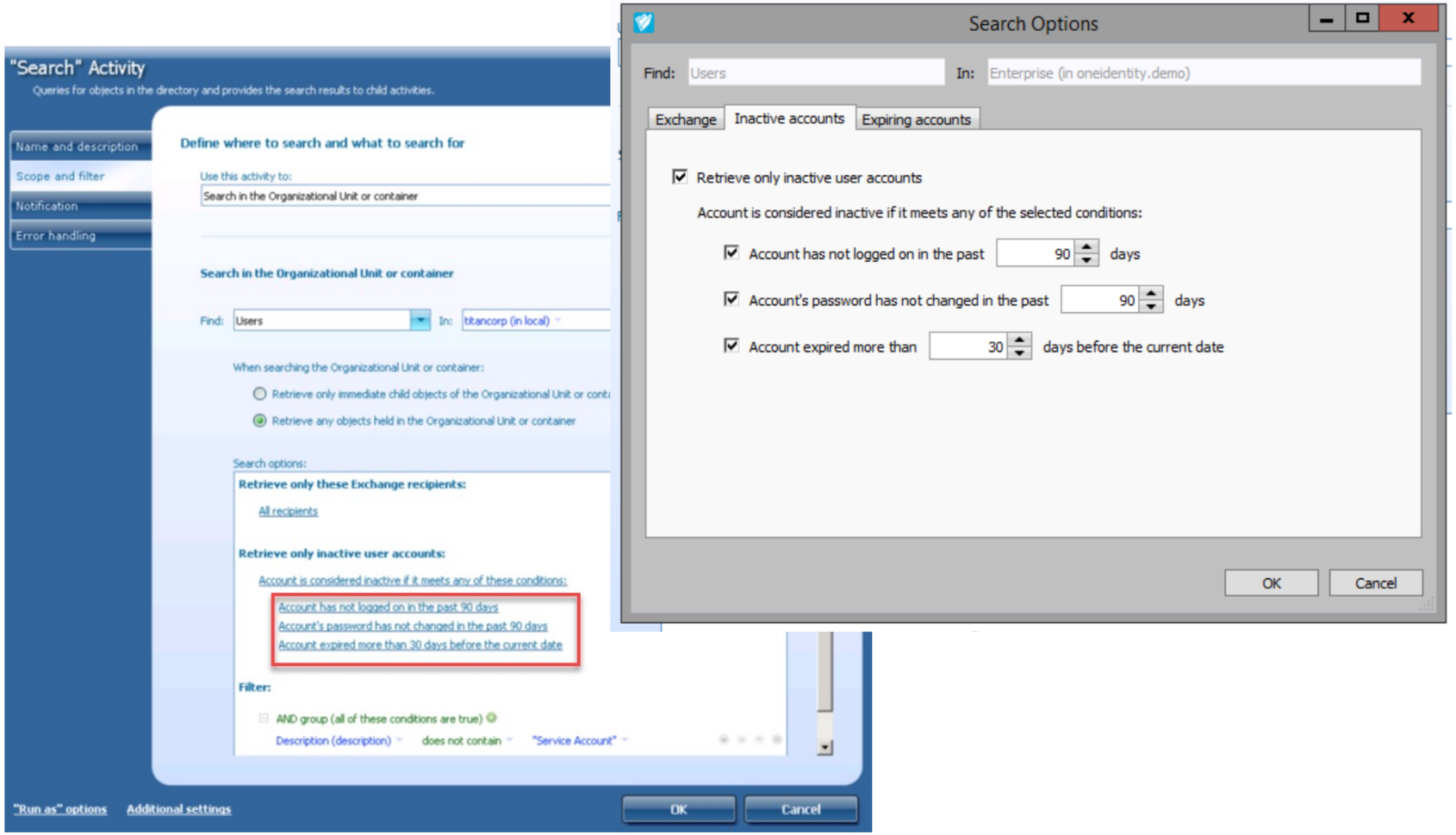
L'attributo *lastLogonTimestamp* può essere utilizzato per interrogare i domain controller e rilevare la data dell'ultimo logon, che aiuta nell'identificazione degli account "dormienti". ***lastLogonTimestamp*** è esposto dalla commandlet **Get-ADUser** con la property ***LastLogonDate***

```
28  $list = Get-ADUser `
29      -Filter * `
30      -SearchBase $args[1]   `
31      -server $args[2]   `
32      -Properties DistinguishedName,DisplayName,SamAccountName,EmployeeID,Description,Office,
        OfficePhone,EmailAddress,Title,Department,Organization,Company,Manager,
        CannotChangePassword,PasswordNeverExpires,Enabled,AccountExpirationDate,LastLogonDate,
        logonCount
```

1	Distinguished Name	Display Name	SAM ID	Last Log-on Date	Has user ever logged on?
2	CN=Eric Parietti,CN=Users,DC=1ID,DC=Lab	Eric Parietti	eric.parietti		No
3	CN=Patrick Hunter,OU=ACME,OU=1ID,DC=1ID,DC=Lab	Patrick Hunter	patrick.hunter	14/10/2019 16:49:33	Yes
4	CN=SG_TempDomAdmin5,OU=Safeguard Managed Priv Users,OU	SG_TempDomAdmin5	SG_TempDomAdmin5	14/09/2020 16:27:56	Yes
5	CN=Tony Brown,OU=Password Manager,OU=1ID,DC=1ID,DC=Lab	Tony Brown	tony.brown	15/01/2021 14:02:49	Yes
6	CN=Maurizio Ostinet,CN=Users,DC=1ID,DC=Lab	Maurizio Ostinet	mostinet_ADM	15/01/2021 18:38:32	Yes
7	CN=Domain Admin 3,OU=SafeGuard Accounts,DC=1ID,DC=Lab	Domain Admin 3	domain_adm_3	19/03/2022 22:07:32	Yes
8	CN=Domain Admin 2,OU=SafeGuard Accounts,DC=1ID,DC=Lab	Domain Admin 2	domain_adm_2	28/11/2022 19:30:09	Yes
9	CN=Elia Mariani,CN=Users,DC=1ID,DC=Lab	Elia Mariani	emariani	16/02/2023 07:18:44	Yes
10	CN=Samin Bolouri,CN=Users,DC=1ID,DC=Lab	Samin Bolouri	sbolouri	28/02/2023 18:06:23	Yes

Gestire gli Account "dormienti" con Active Roles

Active Roles automatizza le procedure che identificano e gestiscono gli account "dormienti", incluse ***classificazione***, ***discovery*** e ***remediation***.



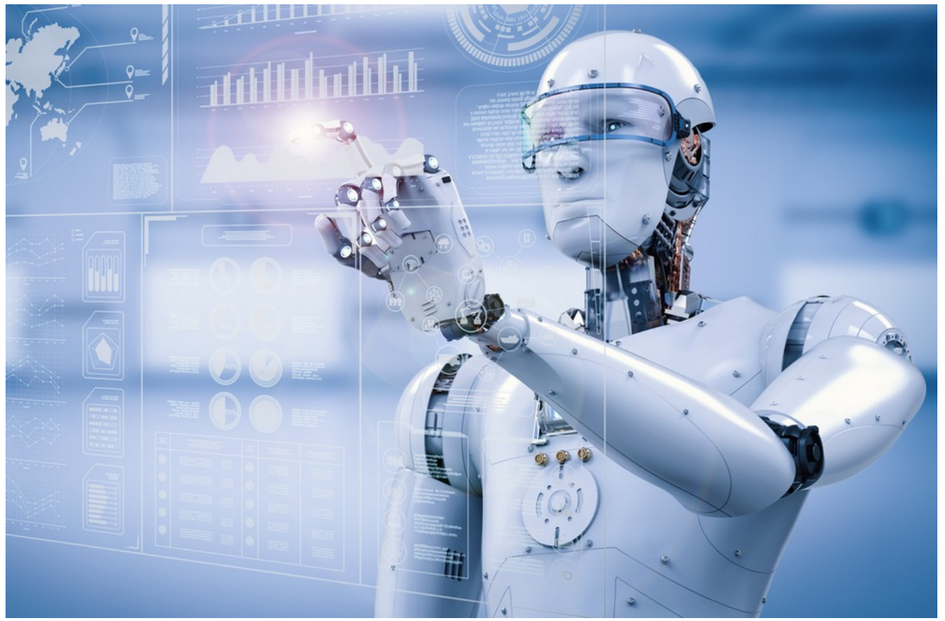
Account NON umani

Le applicazioni fanno uso di account di servizio, I cosiddetti ***service account***, che spesso sono in grado di accedere con **privilegi elevati** ai sistemi e **costituiscono una fonte di rischio elevatissimo** per varie ragioni:

- Lo **scopo dell'account spesso è sconosciuto**

- La **password dell'account tipicamente non viene mai aggiornata**, spesso per paura di creare impatti sull'operatività dell'applicazione

- L'account ha la possibilità di effettuare **logon interattivi**



Gestire Account NON umani

Da dove iniziare?

- **Identificare l'account** (prefisso nel logon name, inserimento in OU ad-hoc, tagging attraverso attributo in AD)

- **Documentare lo scopo** (a cosa serve) dell'account utilizzando i campi Description o Notes del profile

- **Designare un owner**: account umano o Gruppo AD che corrisponde al team responsabile della tecnologia che fa uso dell'account

Come proteggerli?

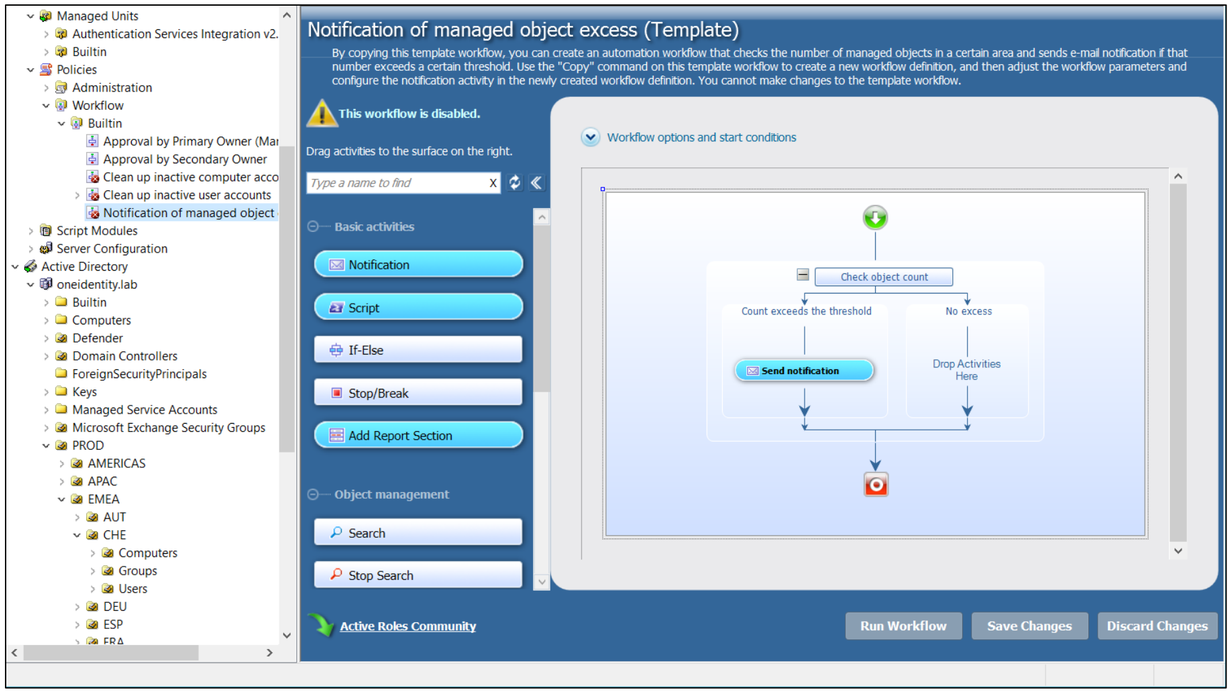
- Determinare i sistemi sui quali l'account è stato utilizzato attraverso l'**analisi dei security logs di windows**

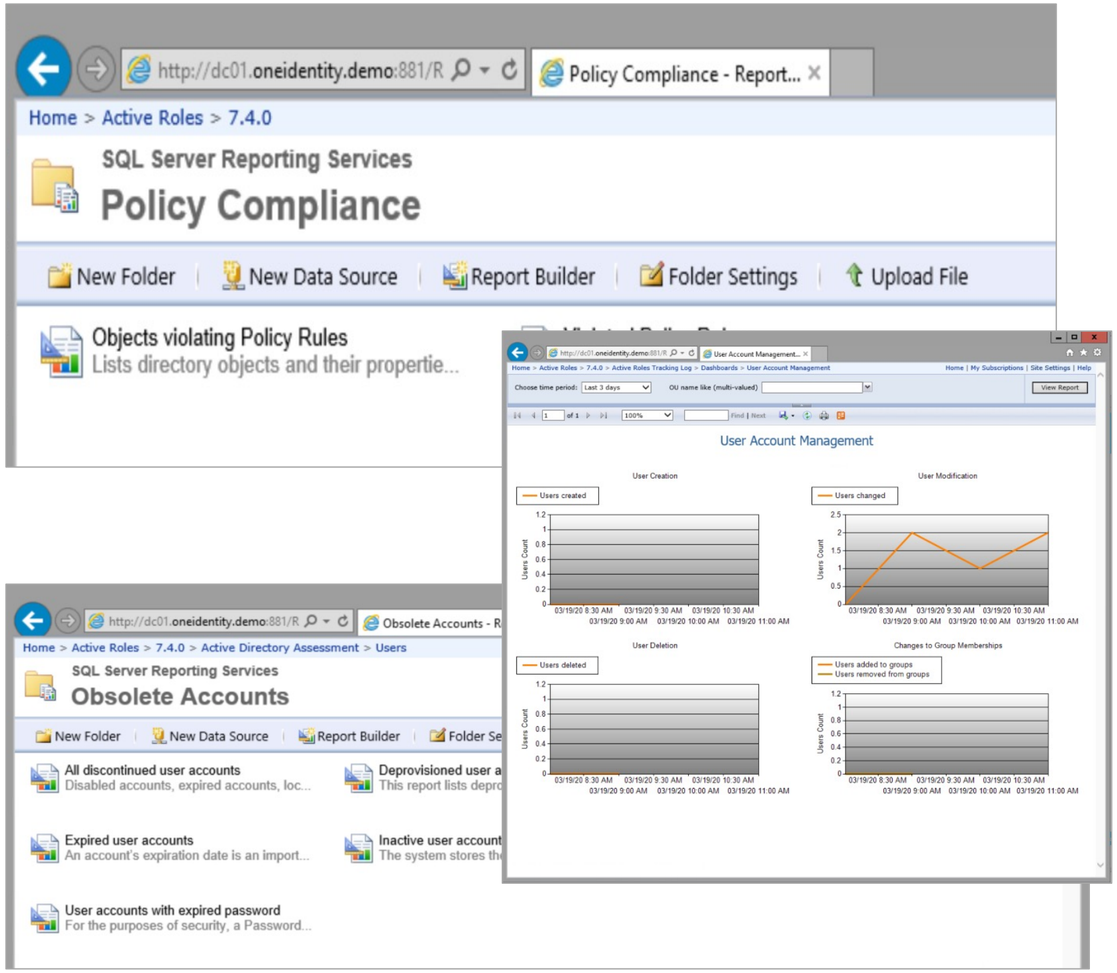
- **Limitare i permessi di logon interattivo** degli account non-umani attraverso le GPO in modo da impedire abusi perpetrati da un attaccante utilizzando accessi via console o RDP

- Utilizzare le funzionalità legate agli oggetti Managed Service Accounts (MSA) e group Managed Service Accounts (gMSA) in grado di **operare la rotazione automatica della password**

Gestire Account NON umani con Active Roles

Active Roles, attraverso workflow e report comparativi, è in grado di **imporre e validare che tutti gli account non-umani siano configurati in modo conforme con policy e standard aziendali**





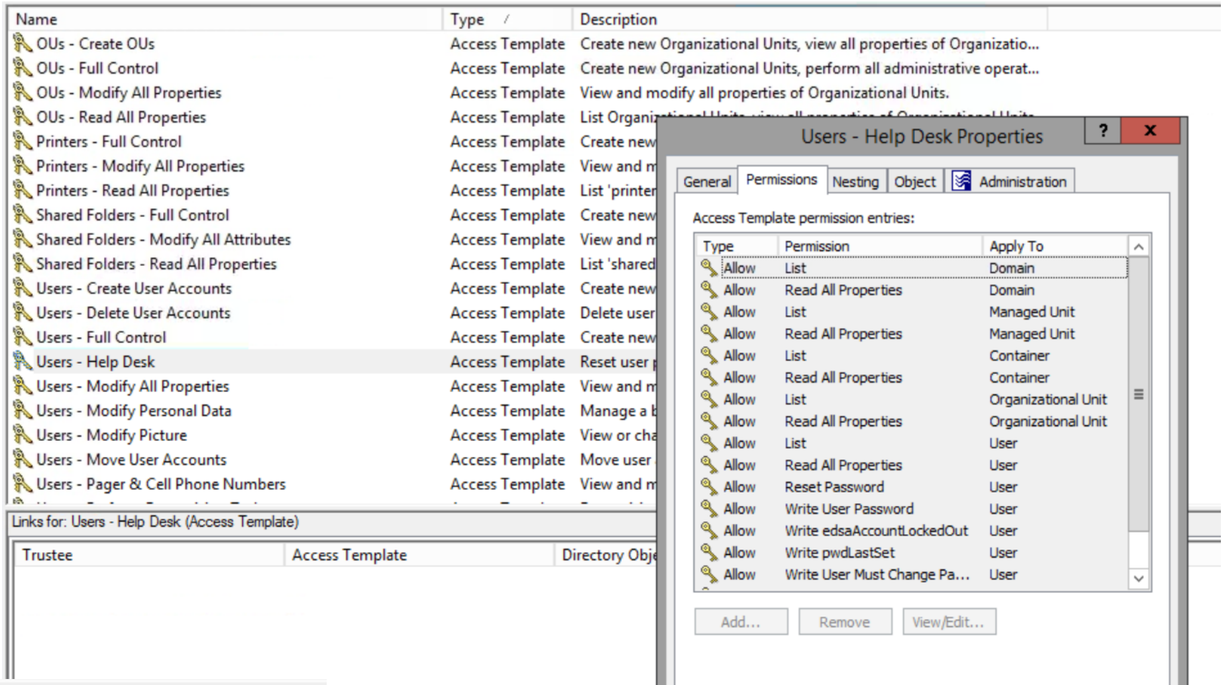
Adottare un approccio “least-privilege” per l’accesso degli amministratori ad Active Directory

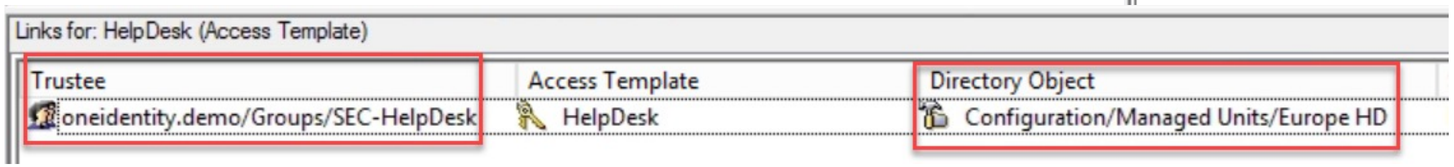
Active Directory consente all’account di domain admin di delegare privilegi di amministrazione su specifiche OU. Tuttavia questo modello amministrativo presenta importanti limiti:

- Attività di amministrazione banali e di routine (es. password reset, creazioni di nuovi utenti / sblocco di utenti) richiedono tipicamente un **eccesso di privilegi**
- Probabilità elevata di presenza di **errori e situazioni di inconsistenza**
- I tentativi di assegnare privilegi in modo granulare portano ad una **perdita di visibilità** in merito a CHI ha accesso a QUALE risorsa

Adottare un approccio “least-privilege” per l’accesso degli amministratori ad Active Directory con Active Roles

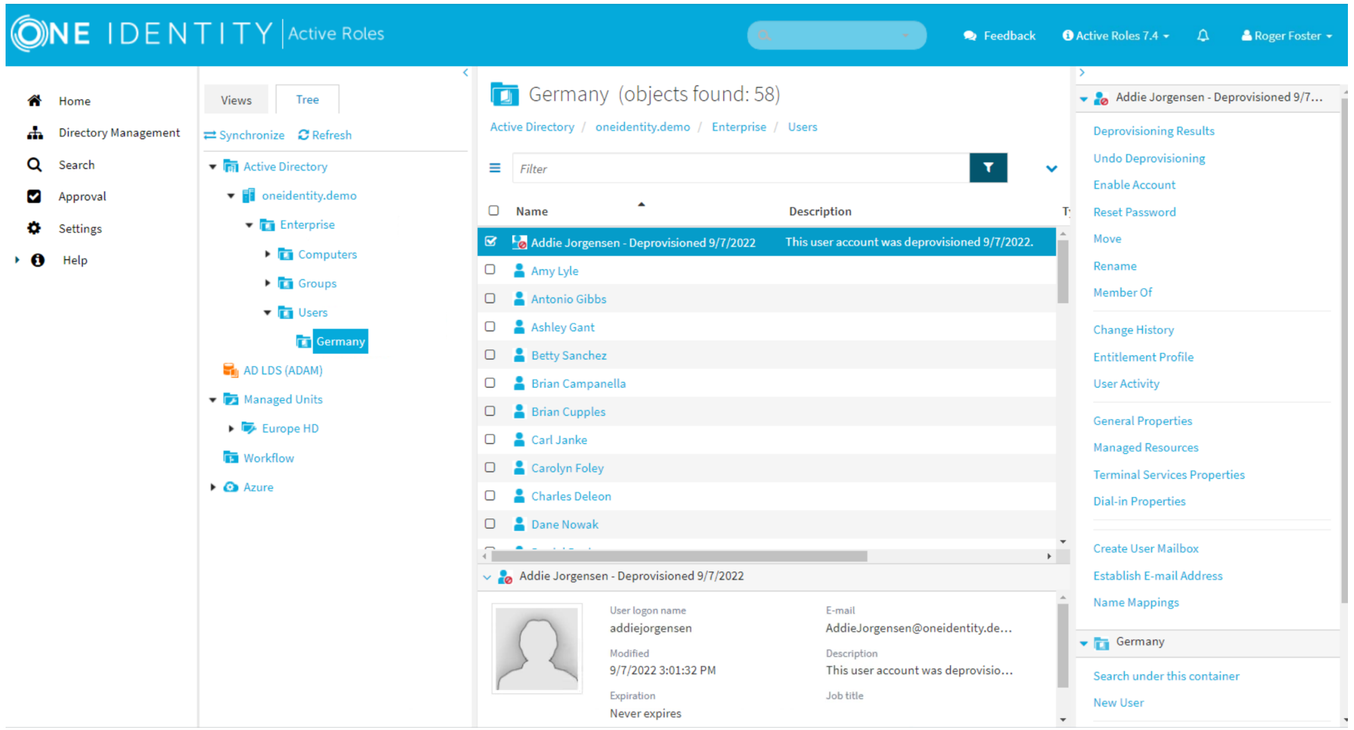
I “ruoli” in Active Roles sono abilitati con gli ***Access Template*** che rappresentano una collezione di privilegi caratterizzati da un livello di granularità molto elevato ed applicabili a qualsiasi porzione dell’infrastruttura AD. La delega dei privilegi consiste nell’associare Access Template a ***Trustee*** (Gruppi o Account delegati) e ***Directory Object*** (lo Scope, es. OU)





Adottare un approccio “least-privilege” per l’accesso degli amministratori ad Active Directory con Active Roles – Interfacce Web

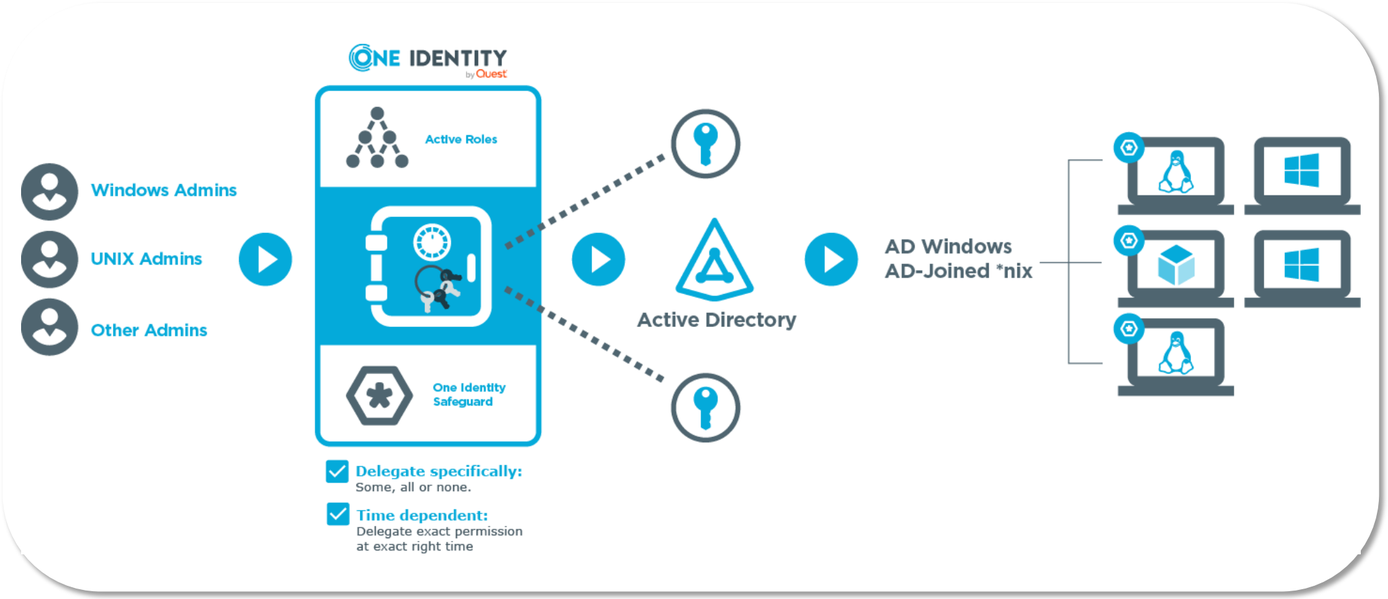
Active Roles mette a disposizione delle **interface Web**, in alternativa alla classica console MMC, **di semplice utilizzo**, particolarmente adatte per tipologie di utenti quali operatori di Help Desk o HR.



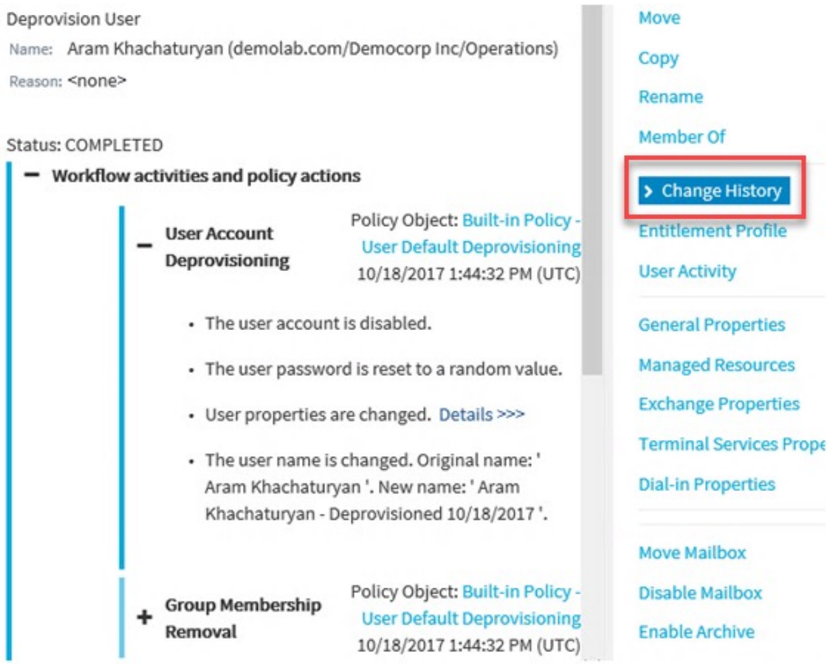
Just in Time Privilege

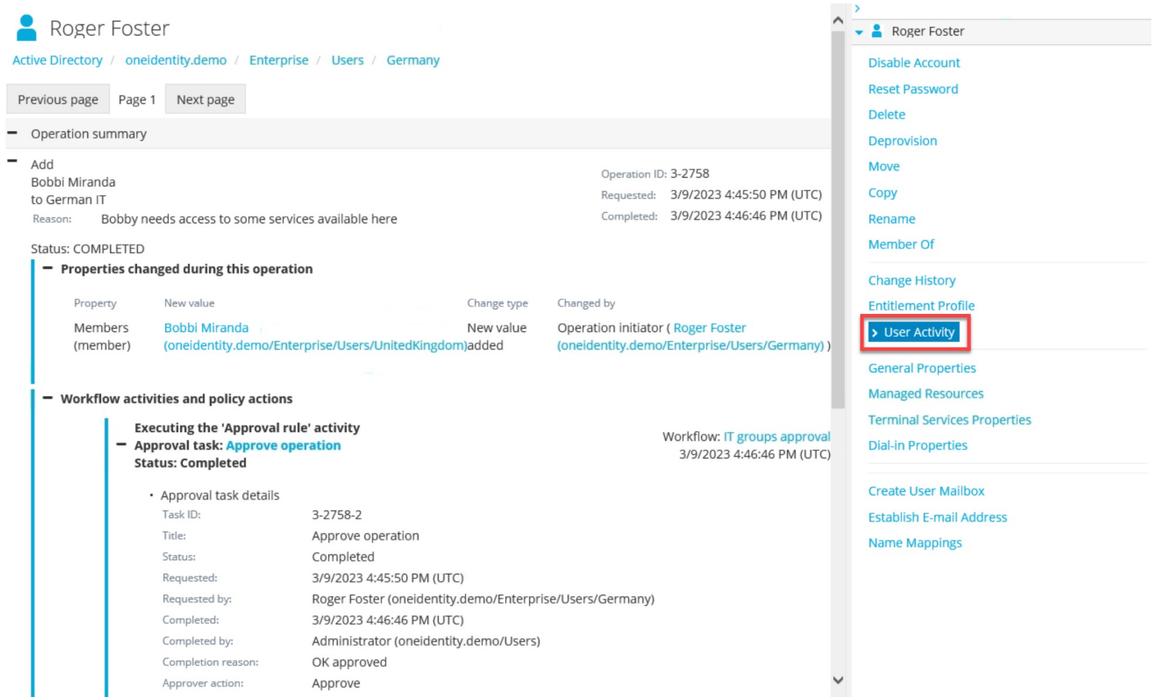
Attraverso l'integrazione nativa tra Active Roles e la soluzione PAM di One Identity è possibile:

- Applicare la **logica Zero Trust** agli **Account Privilegiati di AD**
- Garantire che i **Privilegi** siano **assegnati esclusivamente al momento della richiesta**
- **Revocare i Privilegi** quando non sono più necessari
- **Disabilitare gli Account** quando non sono utilizzati
- **Ruotare automaticamente la password** degli Account al termine del loro utilizzo



Rispondere alle esigenze di Auditing e Compliance con Active Roles





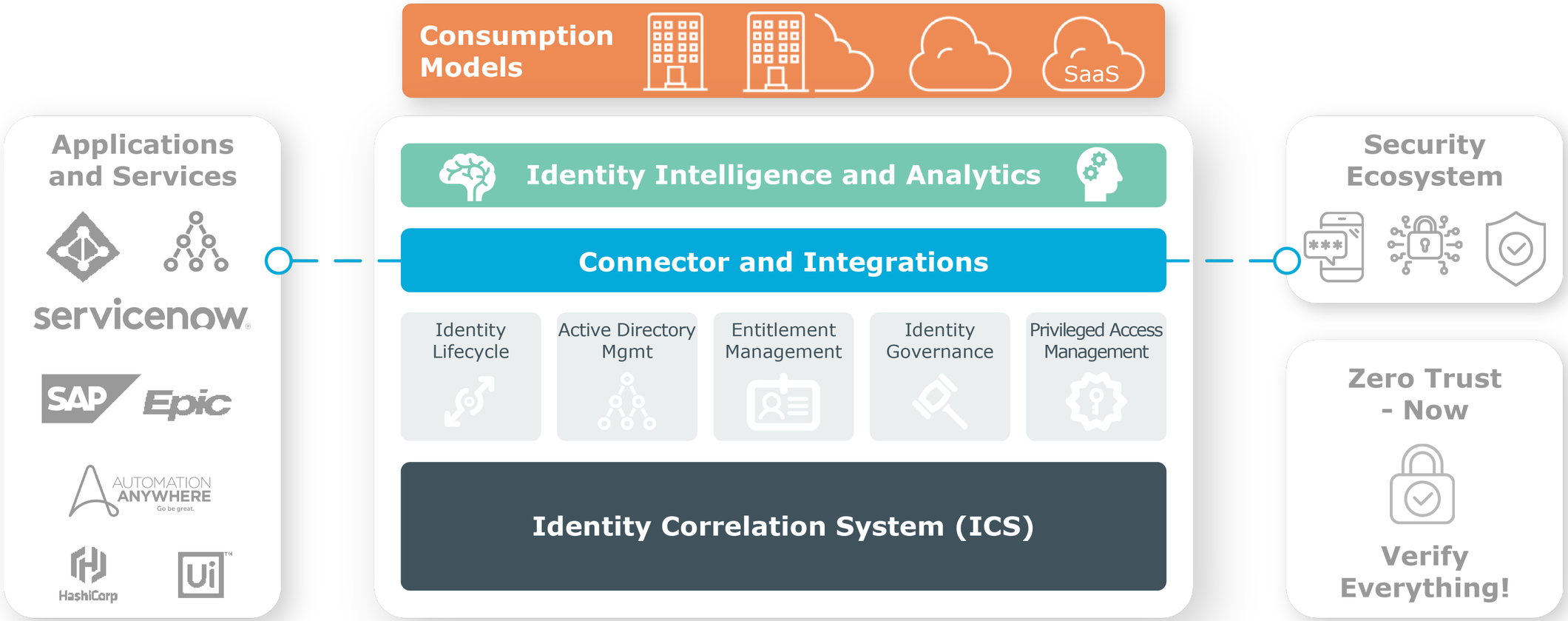
Change History - visibilità su tutte le change operate su un oggetto

User Activity - visibilità su tutta l'attività svolta da parte di un utente


ONE IDENTITY
by Quest

Piattaforma unificata per la sicurezza delle identità

Persone | Applicazioni | Dati



Conosciuta e affidabile

80 out of the **Fortune** **100** as customers

1,000 partners around the globe

11,000+ enterprise customers

Common Criteria certified*

* Identity Manager and Safeguard product lines

500M+ identities actively managed

97% customer satisfaction worldwide

20+ years in identity security

ISO 27001 CERTIFIED by schellman

Unica leader in 3 Magic Quadrants

IGA

AS OF FEB 2018

PAM

AS OF JULY 2021

IAM

AS OF OCT 2021

Q&A

Elia Mariani, Sales Account Manager, One Identity

elia.mariani@oneidentity.com

366 1179924

Maurizio Ostinet, Solutions Architect, One Identity

maurizio.ostinet@oneidentity.com

335 7199293