WHITE PAPER

Una sinergia ottimale: 10 modi per sfruttare al massimo Active Directory con One Identity Active Roles

Informazioni su questo documento

Il presente documento illustra 10 passaggi per rimediare ai problemi degli account utente in AD e prevenirli. Questi passaggi sfruttano le funzioni native di AD e la tecnologia dei flussi di lavoro comuni, come Microsoft SharePoint, in questo modo l'implementazione dei suggerimenti forniti nel presente documento presenta una curva di apprendimento molto ridotta.

Tuttavia, anche seguendo tutti i suggerimenti del presente documento, senza strumenti aggiuntivi a supporto della gestione e automatizzazione dei processi, gran parte degli oneri amministrativi e di conferma manuale rimarrà a carico di responsabili aziendali, rappresentanti HR e personale IT.

È possibile eliminare quasi tutti questi problemi con One Identity Active Roles di Quest. Active Roles fornisce svariate funzioni per eliminare gli interventi di utenti finali, responsabili e personale HR. Prosegui nella lettura per scoprire come Active Roles semplifica ciascuno dei 10 passaggi.

Panoramica

Microsoft Active Directory (AD) e Azure AD (AAD) offrono strumenti organizzativi e standard per la gestione e archiviazione dei dati di identità e account. One Identity Active Roles garantisce agilità, sicurezza, velocità e uniformità nella gestione di AD/Azure AD. Grazie alla sinergia fra Active Roles e AD/AAD, i dirigenti dell'amministrazione IT possono sfruttare una soluzione in grado di ottimizzare in modo significativo sicurezza ed efficienza degli ambienti AD, riducendo le vulnerabilità. Per usare un'analogia, è come aggiungere a una potente auto sportiva sospensioni da corsa, turbocompressore, strumentazione collegata al cloud e un sistema di monitoraggio delle prestazioni notevolmente migliorato, proteggendo il tutto con un portachiavi programmabile ad accesso remoto estremamente sicuro.

Nonostante il veicolo di serie sia di per sé ottimo, la versione aftermarket potenziata consente di affrontare tutte le sfide su strada, fra cui minacce e modifiche imponenti. È un'auto più veloce, più sicura, scorre bene in curva, richiede meno manutenzione ed è più efficiente nel consumo di carburante. L'investimento aggiuntivo viene recuperato subito e consente di effettuare in sicurezza viaggi impensabili finora. Si tratta in poche parole di un'auto migliore.

Lo stesso vale per la sinergia fra Active Roles e One Identity Active Roles.

Come il 95% delle aziende Fortune 1000, starai già usando la soluzione di serie, ovvero Microsoft Active Directory, come strumento quotidiano per il provisioning/deprovisioning delle autorizzazioni utente. Tuttavia, il mondo si evolve rapidamente e le risorse gestite da AD, Azure AD e LDS continuano a diversificarsi. Inoltre, sussistono ulteriori tendenze che aumentano le complessità relative ad AD/AAD, tra cui sicurezza delle identità, migrazione al cloud e il ruolo critico di AD/AAD nella gestione degli accessi privilegiati (PAM). Di recente, l'implementazione di architetture di sicurezza Zero Trust (o Zero Standing Privilege) per prevenire e limitare i danni delle violazioni impone l'espansione e l'ottimizzazione delle funzionalità native di AD/AAD. È qui che One Identity Active Roles automatizza e migliora i servizi AD/AAD.

Questo documento presenta 10 passaggi per eliminare i dati indesiderati degli account utente di Microsoft AD/AAD. Si tratta di un processo fondamentale in termini di efficienza e sicurezza. Nell'analisi individuale dei dieci passaggi, offriremo indicazioni specifiche, dimostrando l'importanza e il contributo offerto da One Identity Active Roles. Molti passaggi sono ascrivibili al buon senso, come l'eliminazione degli account inutilizzati e la revoca dell'accesso ad applicazioni e altre risorse. Tuttavia, nella bagarre delle attività quotidiane, è difficile assegnare la priorità alle attività manuali di manutenzione degli account rispetto ai problemi più gravi relativi a dati e tecnologie. Scopri come One Identity Active Roles automatizza e rende sicure queste attività, garantendo, in sinergia con One Identity CertAccess, il tracciamento e la registrazione dei processi di autorizzazione, approvazione e certificazione.

I 10 passaggi sfruttano le funzioni native di AD e la tecnologia dei flussi di lavoro comuni, come Microsoft SharePoint, garantendo una curva di apprendimento molto ridotta per l'implementazione dei suggerimenti forniti nel presente documento.

Active Roles fornisce svariate funzioni per eliminare gli interventi di utenti finali, responsabili e personale HR.

Tuttavia, anche seguendo tutti i suggerimenti del presente documento, senza strumenti aggiuntivi a supporto della gestione e automatizzazione dei processi, gran parte degli oneri amministrativi e di conferma manuale rimarrà a carico di responsabili aziendali, rappresentanti HR e personale IT.

È possibile eliminare quasi tutti questi problemi con One Identity Active Roles di Quest. Active Roles fornisce svariate funzioni per eliminare gli interventi di utenti finali, responsabili e personale HR.

Prosegui nella lettura per scoprire la sinergia ottimale fra Active Directory e One Identity Active Roles.

Il ruolo centrale di Active Directory nel controllare i rischi e garantire la conformità

Active Directory (AD) svolge una funzione fondamentale nella gestione di identità e accessi (IAM) nella maggior parte delle organizzazioni, pertanto è una della tecnologia di rete più importanti. Sempre più sistemi e applicazioni sfruttano AD e Azure Active Directory (AAD) per autenticazione, criteri, diritti e gestione delle configurazioni. Una falla di sicurezza in AD mette a repentaglio ogni attività.

Importanza degli account utenti e difficoltà nella manutenzione

Proteggere Active Directory/Azure AD è fondamentale per controllare i rischi e garantire la conformità. Tuttavia, eliminare i dati indesiderati e mantenere AD in uno stato organizzato e sicuro rappresenta una sfida, specie riguardo gli account utente.

Gli account utente sono la base per l'autenticazione e l'accesso a reti, sistemi e applicazioni. Si tratta di risorse difficili da mantenere senza adeguati strumenti a supporto del monitoraggio di tutte le autorizzazioni degli utenti sulle varie piattaforme. All'assunzione di un dipendente segue la creazione di un account utente. L'evoluzione di responsabilità e mansioni dell'utente comporta l'aggiornamento del suo account AD (es. titolo professionale, dipartimento e numero di telefono), anche quando entra ed esce dai gruppi. Infine, quando l'utente lascia definitivamente l'organizzazione, i diritti di accesso dell'account dovrebbero essere correttamente eliminati.

Questo processo sembra semplice e diretto. Tuttavia, molte organizzazioni operano con un numero significativo di account utente con autorizzazioni inadeguate o obsolete e non conformi ai criteri di sicurezza dell'organizzazione. Tutti questi account utente espongono l'organizzazione a rischi di sicurezza.

La causa principale di questi problemi è da ricercare nell'inadeguatezza delle pratiche relative al ciclo di vita degli account utente. Di solito, le organizzazioni fanno affidamento su utenti finali, responsabili e personale HR per riconoscere gli eventi riguardanti gli account AD degli utenti. Queste figure devono quindi informare i team IT, già oberati di lavoro, che andranno ad apportare le modifiche necessarie in AD per mantenere gli account utente aggiornati. L'eccessivo affidamento sui processi manuali spesso comporta la mancata applicazione di tali modifiche, con conseguenti autorizzazioni inadeguate e account fantasma, facili prede di criminali intenti a seminare il caos nelle organizzazioni.

10 passaggi per migliorare agilità, sicurezza e prestazioni di Active Directory

Passaggio 1. Eseguire un'analisi regolare degli account

La soluzione più efficace per eliminare gli account indesiderati e garantire la sicurezza in AD/AAD è rivedere regolarmente gli account utente. Esaminando le proprietà degli account prima di un audit, è possibile individuare e risolvere rapidamente molti problemi riscontrati dagli auditor.

Un'operazione semplice: ottenere un elenco degli account utenti

In passato, non era semplice ottenere un elenco degli account utente. Oggi, è sufficiente eseguire uno script Windows PowerShell e importare i risultati in Microsoft Excel. Scopri questo script (Output-ADUsersAsCSV) disponibile all'indirizzo http://www.ultimatewindowssecurity.com/tools/Output-ADUsersAsCSV.Il risultato sarà un foglio di calcolo, simile a quello mostrato qui sotto.

Individuazione degli account non conformi grazie ai filtri

Una volta eseguito lo script, è possibile filtrare il foglio di calcolo risultante in base a varie proprietà degli utenti per trovare gli account non conformi. Inizia concentrandoti sugli account con problemi di facile individuazione, come una password che non scade mai. Quindi, inserisci criteri di filtraggio su altre colonne, come l'ID SAM o la descrizione, per eliminare servizi, applicazioni e altri account che rappresentano eccezioni note.

	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

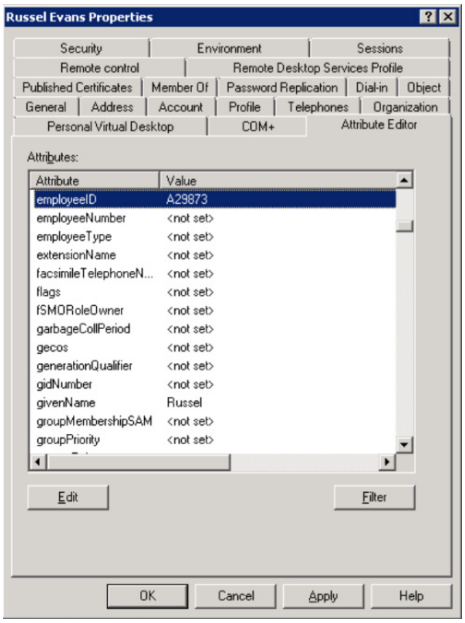
Questi sono problemi facili da risolvere prima dell'audit e ridurranno il numero di rischi rilevati in tale procedura. Un altro problema ovvio da ricercare sono gli account inattivi (a questo argomento è dedicato un intero passaggio più avanti nel documento).

Fra gli altri problemi da attenzionare, citiamo gli account che non andavano creati in primo luogo o il cui provisioning è contrario agli standard di denominazione o ad altri controlli in materia di creazione di account.

Ad esempio: lo standard di denominazione della Acme Corp. impone che tutti gli account degli utenti finali inizino con "u-", gli account di amministrazione con "p-" (a indicare i privilegi) e gli account di servizio con "s-". Come prima cosa, filtra tutti gli account con tali prefissi per trovare quelli non conformi. In alcuni casi, potrebbe trattarsi di eccezioni legittime, che verranno esaminate in un passaggio successivo. Molti di questi account si riveleranno sospetti e andranno tracciati per determinarne scopo e stato.

Si tratta di un passaggio da eseguire prima di un audit e, idealmente, ogni mese per mantenere AD sempre sotto controllo. Dopotutto, la tua mansione operativa non riguarda il solo superamento degli audit, ma la garanzia della sicurezza e organizzazione di AD in ogni momento.

Questo passaggio prevede un controllo investigativo o reattivo, non preventivo o proattivo. L'obiettivo è evitare i problemi prima che si verifichino. Il passaggio 2 è la prima soluzione per conseguire questo obiettivo.



Esistono molti modi per collegare gli account AD ai record dei dipendenti: (1) Usare l'attributo ID dipendente o Numero dipendente di AD (2) Attraverso la scheda Editor attributi, come mostrato nella figura qui sopra (3) Inserendo l'ID del dipendente nel campo Descrizione o Note (4) Incorporando il numero del dipendente nel nome di accesso

Il contributo di Active Roles

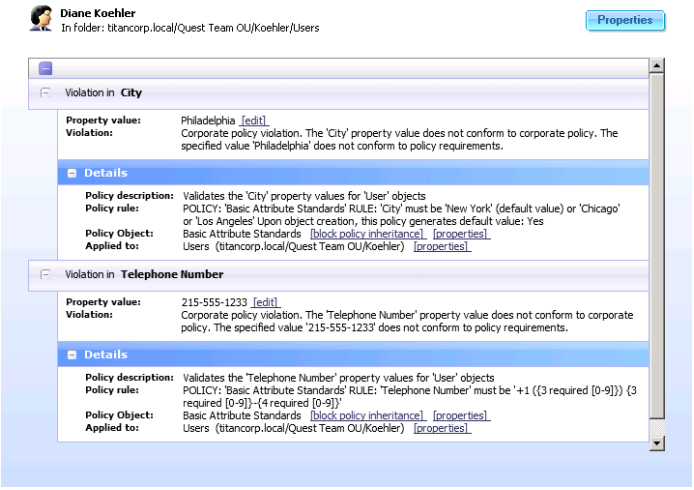
Active Roles consente di confrontare gli standard degli oggetti AD previsti (chiamati criteri) con quelli attuali. I risultati di questo confronto (definito richiesta di verifica dei criteri) vengono forniti su richiesta, con due clic su una schermata o tramite report programmati regolarmente. Questa funzionalità consente alle organizzazioni di eliminare i dati indesiderati.

Un investimento amministrativo relativamente ridotto nella creazione dei criteri è il primo passo per riassumere il controllo.

Passaggio 2. Collegare gli account ai record dei dipendenti

La soluzione più basilare per eliminare i dati indesiderati e garantire la sicurezza negli account AD è collegare tutti gli account a utenti effettivi. Ciò comprende gli account non umani, come quelli creati per servizi e applicazioni, che saranno illustrati nel passaggio 7. In primo luogo, concentrati sugli account creati per le persone, compresi utenti finali, appaltatori, amministratori e altri.

Tutti gli account dei dipendenti vanno ricollegati ai record principali dei dipendenti nel sistema HR.



Active Roles consente di confrontare gli standard degli oggetti AD previsti (chiamati criteri) con quelli attuali.

Questo collegamento è cruciale poiché l'accesso dei dipendenti alla rete deve essere legato al relativo stato e ruolo all'interno dell'organizzazione. Il documento ufficiale da sfruttare è il record principale delle HR, che sarà quasi sicuramente aggiornato.

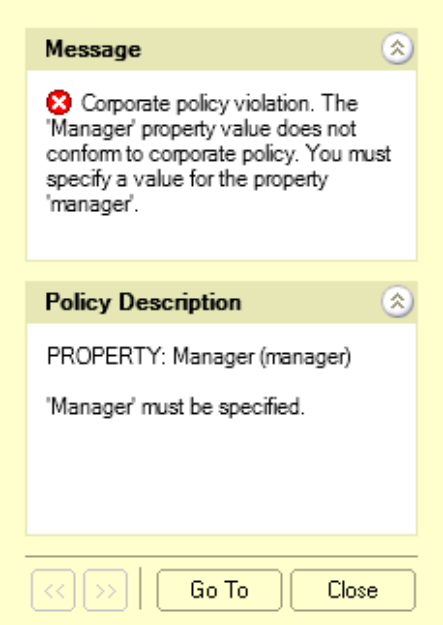
In caso di modifiche a stato o ruolo dei dipendenti, devi poter trovare i relativi account e modificarne stato o diritti di conseguenza. Documentare l'ID dei dipendenti negli account AD è fondamentale. Ovviamente, dovrai anche implementare procedure per semplificare la risposta a questi eventi. Si tratta di un argomento che approfondiremo in un passaggio successivo.

Il contributo di Active Roles

Sfruttando i criteri di creazione degli account, Active Roles può imporre la creazione di account non umani con un valore Manager o EmployeeID. Infatti, Active Roles può gestire il provisioning degli account e il formato di qualsiasi attributo.

Passaggio 3. Monitorare i nuovi account

Negli audit IT di AD, è comune individuare account inutili e non standard, compresi quelli non conformi alle convenzioni di denominazione aziendale. Ciò accade quando troppi dipendenti del dipartimento IT hanno l'autorità di creare account. Questo problema verrà esaminato in un passaggio successivo.



Le intrusioni portate assegno, sia umane che automatizzate, spesso prevedono la creazione di account backdoor per ottenere un accesso continuo e mascherare le attività.

Intrusioni mediante account backdoor

Le intrusioni portate assegno, sia umane che automatizzate, spesso prevedono la creazione di account backdoor per ottenere un accesso continuo e mascherare le attività. Nello specifico, Flame, un recente malware "weaponized", creava account simili ogni volta che rilevava la sua esecuzione sotto l'autorità di un amministratore di dominio.

Fermare le intrusioni alla creazione degli account

Tracciare i nuovi account è dunque fondamentale, ma è anche dispendioso in termini di tempo e spesso inutile. Il momento migliore per rintracciare gli account non conformi è la loro creazione:

- Identificare chi ha creato l'account
- Lavora ancora presso l'azienda?
- Per quale motivo è stato creato l'account?

Come monitorare e rivedere i nuovi account

Esistono due soluzioni per rivedere e reagire ai nuovi account:

- Monitorare i log di sicurezza del controller di dominio AD per l'ID evento 4720 (devi abilitare la sottocategoria di audit Gestione account utenti).
- Eseguire lo script Output-ADUsersAsCSV e ordinare in base alla colonna della data di creazione.

Nell'esame di ciascun account, dovrai rispondere ai seguenti interrogativi:

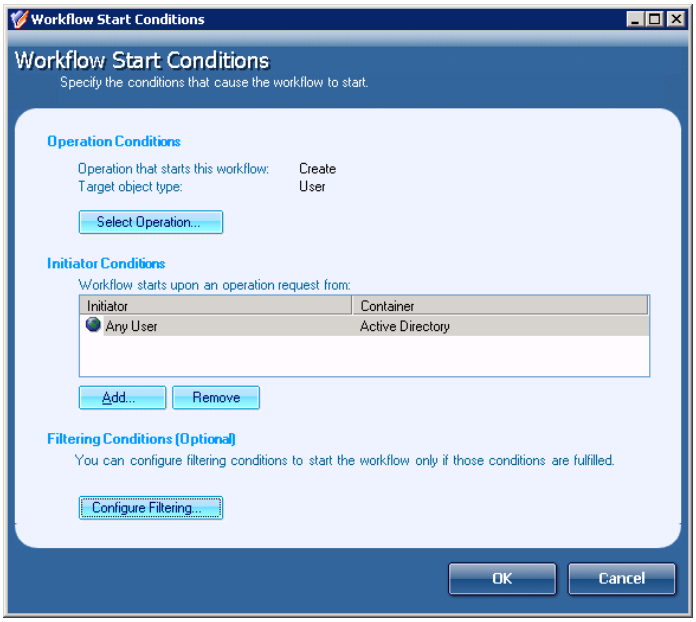
- Esiste un ticket di lavoro o altri documenti a conferma di questo account?
- L'account rispetta le convenzioni di denominazione stabilite?
- L'account è conforme agli altri standard e criteri di creazione degli account dell'organizzazione?

```
ID evento 4720: è stato creato un account utente

Oggetto

     ID di sicurezza: ACME-FR\administrator

     Nome dell'account: amministratore

     Dominio dell'account: ACME-FR

        ID di accesso:

0x20f9d Nuovo account:

     ID di sicurezza: ACME-FR\John.Locke

     Nome dell'account: John.Locke

     Dominio dell'account: ACME-FR

Attributi:

     Nome account SAM: John.Locke

     Nome visualizzato: John Locke

     Nome utente principale: John.Locke@acme-fr.local
```

Se l'account non è autorizzato o conforme, dovrai rivolgerti a chi lo ha creato. Il vantaggio del primo metodo è che l'evento 4720 del registro di sicurezza indica chi ha creato l'account.

Il contributo di Active Roles

Active Roles agisce come un firewall virtuale intorno ad Active Directory, assicurando l'applicazione di accessi basati sul modello dei privilegi minimi. La possibilità di utilizzare i flussi di lavoro per qualsiasi operazione (es. creazione, modifica o eliminazione di account nel dominio) garantisce l'automatizzazione di tutti i processi in genere eseguiti manualmente. Ciò implica che tutte le azioni importanti vengono effettivamente svolte, in modo immediato, completo e con un controllo totale.



Passaggio 4. Automatizzare la manutenzione dell'account

Passaggi per la creazione di un nuovo account

Per garantire la creazione di nuovi account conformi ai tuoi standard, automatizza il più possibile tale processo per ridurre i potenziali errori umani. La creazione dell'account prevede i seguenti passaggi:

1. Creazione dell'account in AD
2. Impostazione degli attributi di identità (titolo professionale, numeri di telefono e così via)
3. Creazione della casella di posta dell'account in Microsoft Exchange/O365
4. Aggiunta dell'account ai gruppi pertinenti al ruolo dell'utente
5. Registrazione dell'account AD in altre applicazioni, se necessario

Automatizzazione con script PowerShell

Gli script PowerShell consentono di automatizzare molti di questi passaggi. Il seguente script esegue i passaggi da 1 a 4.

```
New-ADUser –Name ‘randyjones’

–SamAccountName randyjones – AccountExpirationDate
01/01/2014

–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
```

Puoi creare una versione personalizzata di questo script per i ruoli a elevata rotazione della tua organizzazione. Inoltre, puoi migliorare lo script in modo che accetti input e crei gli account secondo le scelte effettuate al momento dell'esecuzione.

Il contributo di Active Roles

Active Roles offre numerose interfacce, tra cui PowerShell, script ADSI, SPML, SCIM, MMC e Web. Ciò garantisce la possibilità di imporre standard (chiamati criteri) a qualsiasi operazione CRUD degli oggetti AD, indipendentemente dall'interfaccia. Grazie a questo livello di gestione, potrai controllare tutte le attività all'interno dell'ambiente AD in base ai tuoi standard. Spetta a te decidere se il mancato rispetto degli standard risulterà in una violazione consentita (segnalabile) o in una risposta di errore.

Passaggio 5. Gestire gli utenti in uscita e le modifiche ai ruoli

Gli account utente fantasma o orfani mettono a repentaglio la sicurezza delle organizzazioni che usano gli strumenti di gestione AD tradizionali. Senza automazione e/o un'unica fonte affidabile di identità e autorizzazioni, è probabile che i dati delle identità facciano riferimento a persone non più al servizio o sotto contratto con la tua organizzazione. È cruciale informare i responsabili degli aggiornamenti di stato, operanti nelle un HR o nelle IT, in caso di eventuali fuoriuscite dall'organizzazione o passaggi di ruolo.

La ricerca di account inattivi non è la soluzione del problema

Per quanto semplice possa sembrare, le organizzazioni spesso non riescono a disabilitare gli account utente o a modificare i diritti in seguito alla modifica di stato degli utenti. In base alle risposte fornite negli audit, le organizzazioni di solito gestiscono la disabilitazione degli utenti in uscita cercando gli account inattivi, ovvero gli account che non si sono collegati di recente. Si tratta di un approccio fallace poiché se una persona che non fa più parte dell'organizzazione continua ad accedere alla rete, il suo account non verrà classificato come inattivo, non rientrando così nel relativo report.

Cercare gli account inattivi è come curare i sintomi piuttosto che la causa. Questo problema può essere risolto con un approccio che copre l'intero ciclo di vita degli account AD, dall'assunzione alla fuoriuscita e tutte le fasi intermedie.

Quanto affermato vale anche per i dati ridondanti. Si tratta di un aspetto importante quanto la creazione oculata di nuove elementi. Senza eliminare i dati ridondanti e indesiderati, AD si riempirà di dati inutili.

Soluzioni efficaci per la gestione di utenti in uscitae modifiche di ruolo

Di seguito sono indicate, in ordine di preferenza, tre soluzioni per gestire in modo ottimale le modifiche di stato:

- Inserire la disabilitazione degli account AD nei processi chiaramente definiti e rigorosamente eseguiti dalla maggior parte delle organizzazioni per rimuovere l'accesso fisico di un utente all'edificio.
- Automatizzare gli eventuali flussi di lavoro delle applicazioni HR in modo da inviare un'e-mail agli amministratori in caso di cessazione del rapporto di impiego di un dipendente, trasferimento a un nuovo ruolo o a un responsabile diverso.
- Programmare report giornalieri circa cessazioni dei rapporti di impego e modifica delle mansioni da comunicare agli amministratori dell'account, considerando che la maggior parte delle applicazioni HR permette di programmare l'invio automatico dei report.

La disabilitazione degli account e gli aggiornamenti di stato delle autorizzazioni sono necessari per rispettare i requisiti istituzionali e di settore. Indipendentemente dal processo, la dirigenza deve riconoscere l'importanza di tali aspetti, definendo in modo chiaro le responsabilità.

Il contributo di Active Roles

Le funzionalità relative ai flussi di lavoro di Active Roles comprendono attività e interi processi attivati da modifiche alla directory. Ciò include criteri di eliminazione degli account che permettono alla tua organizzazione di definire in modo preciso il destino di un account utente una volta cessato il rapporto di impiego con una persona.

Tra le opzioni disponibili citiamo disabilitazione dell'account, trasferimento della posizione OU, crittografia della password e alterazione del nome di accesso, ridenominazione con variabili di funzionamento, assegnazione di delegati per le directory home e di posta e così via.

In particolare, Active Roles può rimuovere l'utente da tutti i gruppi di sicurezza, concedere nuovamente l'autorizzazione alla directory home dell'utente, liberare le licenze O365 assegnate e molto altro ancora. È importante sottolineare che tali criteri possono essere attivati in modo manuale, programmatico o automatico.

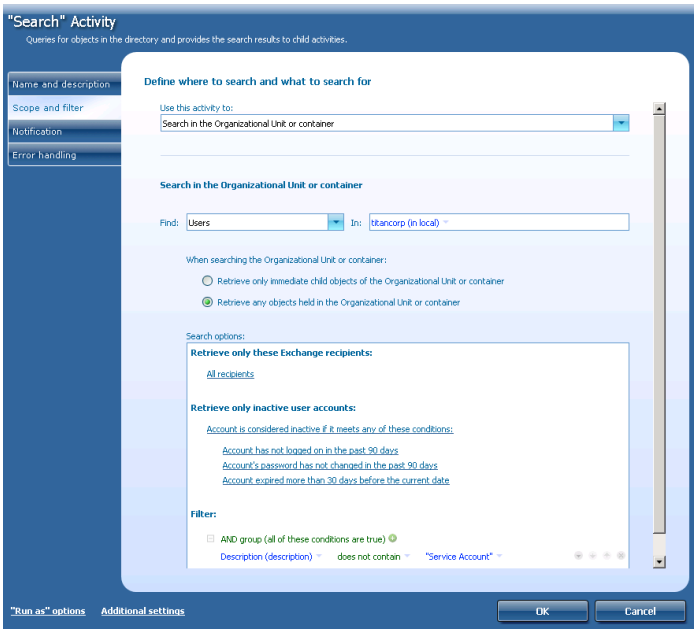
Passaggio 6. Gestire gli account inattivi

Il passaggio successivo prevede la verifica regolare degli account inattivi (gli account utente non collegati di recente). Anche in questo caso, questo passaggio non sostituisce il passaggio 5.

Trovare gli account inattivi è semplice

Prima di Windows 2003, era difficile trovare gli account inattivi, ma l'attributo lastLogonTimestamp ha semplificato questa operazione. Tale replica (ogni sette giorni) consente di inviare query ai controller di dominio e vedere le ore degli ultimi accessi, in modo da identificare gli utenti inattivi.

LastLogonTimestamp è esposto da Get-ADUser con la proprietà LastLogonDate, come mostrato nello script OutputADUsersAsCSV nel passaggio 1. Con lo script in questione, è sufficiente ordinare la colonna relativa all'ultimo accesso in ordine decrescente per identificare subito gli account che non hanno effettuato l'accesso di recente.



È opportuno anche verificare la presenza di account utente che non hanno mai effettuato l'accesso. Nei fogli di calcolo creati con Output-ADUsersAsCSV, questi account sono indicati da righe in cui la colonna relativa all'ultimo accesso è vuota.

Il contributo di Active Roles

Active Roles automatizza i processi di identificazione e gestione degli account inattivi, compresa la classificazione, individuazione e correzione. Questo semplifica il processo di eliminazione degli account indesiderati e, insieme a criteri adeguati sulla gestione del ciclo di vita degli account (come il deprovisioning), risolve i problemi legacy ed evita quelli futuri.

Passaggio 7. Gestire gli account non umani

Non tutti gli account corrispondono direttamente a una persona. Ad esempio, molte applicazioni richiedono uno o più account per l'accesso dei servizi. Questi account spesso sono dotati di un accesso privilegiato a server e dati, pertanto devono essere protetti.

Perché gli account con privilegi elevati sono a rischio

Tuttavia, non è semplice tenere traccia di applicazioni e altri account non umani. Negli audit IT, non è raro individuare account con privilegi a rischio per i seguenti motivi:

- Non si conosce scopo o motivo dell'esistenza dell'account.
- Nonostante l'uscita di molti amministratori, la password di un account non è stata aggiornata, per timore di causare errori in un'applicazione in rete.
- L'account dispone dell'autorità di accedere in modo interattivo.
    - Agli account non umani dovrebbe essere proibito l'accesso interattivo, mediante console o desktop remoto, per impedire agli amministratori (che conoscono la password dell'account) di accedere in modo anonimo mediante tale account, senza responsabilità individuale

Identificazione degli account non umani

Il primo passaggio nella gestione degli account non umani prevede la loro identificazione. Per farlo, puoi usare un prefisso nella convenzione di denominazione del nome di accesso, inserendo gli account in una specifica unità organizzativa (OU) Account non umani o applicando un'etichetta che li identifichi come tali tramite altri attributi in AD.

Documentazione di scopo e proprietario di ciascun account

In seguito, occorre documentare scopo degli account e sistemi su cui vengono usati nei campi Descrizione o Note dell'account.

Active Roles automatizza i processi di identificazione e gestione degli account inattivi, compresa la classificazione, individuazione e correzione.

Definisci un proprietario per ciascuno account non umano e documentalo in AD. Il proprietario può essere un account utente umano individuale, ma di solito è opportuno selezionare un gruppo corrispondente al team responsabile per l'applicazione o le altre soluzioni tecnologiche che utilizzano l'account. Il proprietario può anche essere documentato nel campo Descrizione o Note.

L'uso degli account del servizio gestito (MSA) è stato introdotto in Windows Server 2008 R2 (in seguito, account del servizio gestiti del gruppo, gMSA) per gestire in automatico (modificare) le password degli account di servizio. Utilizzando MSA/gMSA, si può ridurre in modo drastico il rischio di compromissione degli account di sistema.

Manutenzione della password

Una delle maggiori sfide riguardanti gli account non umani è la manutenzione delle password. La password di un account non umano va modificata ogni volta che un amministratore (che conosce la password) lascia l'organizzazione. Se gli account non sono documentati correttamente, è difficile determinare a quali account non umani avesse accesso un amministratore. Tuttavia, modificare la password di un account comporta rischi poiché occorre aggiornare servizi o attività pianificate eseguiti tramite tale account o applicazioni che memorizzano la password dell'account in questione per evitare errori agli avvii o ai successivi tentativi di accesso.

Definizione dei sistemi su cui viene usato un account

Durante l'eliminazione di un gruppo indesiderato di account non umani esistenti, è possibile determinare i sistemi su cui vengono usati gli account consultando il registro di sicurezza di Windows. Supponendo che la sottocategoria di audit Operazioni ticket di servizio Kerberos sia abilitata in Default Domain Controller Policy Group Policy Object (GPO), i controller di dominio registreranno l'evento ID 4769. Cercando nei log di sicurezza dei controller di dominio tutte le occorrenze di 4769 in cui il nome account corrisponde all'account di servizio, è possibile recuperare un elenco di tutti i computer su cui viene usato l'account in questione. Consulta il campo relativo al nome del servizio in questi eventi. Il campo relativo al nome del servizio nell'evento ID 4769 identifica il computer per il quale l'account utente sta richiedendo l'autenticazione.

Limitazione dei diritti di accesso degli account non umani

Un ultimo passaggio per rendere sicuri gli account non umani consiste nel limitarne i diritti di accesso ai computer in tutto il dominio. In questo modo, si evita l'uso improprio degli account non umani da parte di utenti che si collegano in modo interattivo con gli account alla console di un computer o tramite desktop remoto. Questo passaggio rappresenta una misura di difesa profonda in caso di mancata modifica delle password quando un amministratore abbandona l'organizzazione. Cinque tipi di accesso in Windows presentano entrambi gli elementi e consentono di autorizzare e negare i diritti:

Per accedere in un determinato modo, occorre il corrispondente diritto di consentire accesso. Anche in questo caso, se ti è stato assegnato anche il diritto di negare l'accesso, non sarai autorizzato a effettuare l'accesso (il diritto di negare l'accesso prevale sul diritto di consentirlo). Puoi trovare questi diritti in un GPO in Impostazioni del computer\Impostazioni di Windows\

Impostazioni di sicurezza\Criteri locali\Assegnazioni diritti utente.

Di solito, gli account non umani dovrebbero disporre solo del diritto "Accedi come servizio". È consigliabile negare esplicitamente i diritti di accesso Interattivo e Desktop remoto per evitare usi impropri degli account. Se aggiungi tutti gli account non umani a un gruppo specifico per questo scopo, puoi assegnare a quel gruppo i diritti "Nega accesso locale" e "Nega accesso tramite Servizi Desktop remoto" in un GPO, come criterio di dominio predefinito, applicato a tutti i computer del dominio.

Presta attenzione nel negare il diritto di accesso alla rete: l'applicazione che utilizza l'account potrebbe dover accedere a risorse su altre reti.

Il contributo di Active Roles

Active Roles può imporre a tutti gli account non umani configurazioni basate su convenzioni di denominazione, impostazioni degli attributi, posizione degli oggetti e appartenenza ai gruppi (legata al GPO) in linea con gli standard della tua azienda e convalidare il tutto mediante report di confronto. Inoltre, è possibile abilitare i flussi di lavoro if-then per imporre l'approvazione (a livelli) per tutti gli account (di servizio) creati in una certa posizione OU e/o per gli account con un particolare prefisso di denominazione e così via. Tutte queste azioni saranno completamente controllate e legate all'effettivo individuo responsabile.

Passaggio 8. Controllo delle eccezioni

Documentare le eccezioni legittime e approvate

Un antico proverbio recita: "Le regole sono fatte per essere infrante". Esistono sicuramente eccezioni legittime agli standard per gli account utente. Ad esempio, un'applicazione potrebbe necessitare di un account utente con un nome specifico, contrario alla normale convenzione di denominazione. Per situazioni del genere, occorre una soluzione per documentare le eccezioni legittime e approvate. L'approccio ideale prevede una OU denominata Eccezioni o la segnalazione degli account con eccezione nei campi Descrizioni o Note.

Tuttavia, non è sufficiente indicare un account come un'eccezione, occorre documentare anche scopo e proprietario dell'account, come illustrato nel passaggio 7.

Tipo di accesso	Diritti di accesso
Interattivo	Consenti accesso locale Nega accesso locale
Desktop remoto	Consenti accesso tramite Servizi Desktop remoto Nega accesso tramite Servizi Desktop remoto
Servizio	Accedi come servizio Nega accesso come servizio
Attività pianificata	Accedi come servizio Nega accesso come servizio
Rete (es., accesso a cartelle condivise)	Accesso come processo batch Nega accesso come processo batch
Crittografia del trasporto RDP FIPS 140-2	Accedi al computer dalla rete Nega accesso tramite Servizi Desktop remoto

Un antico proverbio recita: "Le regole sono fatte per essere infrante". Esistono sicuramente eccezioni legittime agli standard per gli account utente.

Evitare che le eccezioni diventino la regola

Nelle implementazioni AD con elevate percentuali di account con eccezioni, i dipendenti sono soliti segnalare gli account come eccezione ogniqualvolta è poco pratico rispettare standard e procedure di manutenzione degli account. La previsione di eccezioni non va usata in modo improprio.

Il contributo di Active Roles

Active Roles può ospitare e controllare le eccezioni attraverso criteri che assicurano la creazione degli account con eccezioni solo in determinate posizioni. Se viene creata un'eccezione nella relativa posizione, Active Roles garantisce che tutti gli standard di configurazione necessari, gli attributi o altri vincoli di criterio siano soddisfatti e applicati.

Inoltre, è possibile utilizzare flussi di lavoro di approvazione in caso di escalation a seguito di una richiesta di creazione (in modo manuale o programmatico) di una nuova eccezione, in modo da evitare che le eccezioni diventino la regola.

Passaggio 9. Controllare l'autorità amministrativa

Limitare chi può creare account

AD presenta spesso molti account inutili o sospetti poiché troppe persone dispongono dell'autorità per la creazione di account utente.

Per applicare i controlli sulla creazione di nuovi account, cruciali per la sicurezza e la conformità, è opportuno lasciare la creazione degli account a pochi dipendenti qualificati.

Utilizzare Delega guidata del controllo

AD supporta i privilegi minimi consentendo agli amministratori di dominio di delegare autorizzazioni selezionate a specifiche OU. Se implementata correttamente, la funzione di delega del controllo di AD permette di assegnare ai dipendenti solo l'autorità necessaria allo svolgimento delle loro mansioni. Ad esempio, anziché rendere l'help desk membro di Domain Admins, puoi concedere al gruppo Help Desk l'autorizzazione Reimposta password sulla OU contenente gli account degli utenti finali.

Grazie ai suoi oltre 300 modelli di accesso di comune utilizzo collaudati e testati, Active Roles è uno degli strumenti più rapidi da implementare.

Per avviare Delega guidata del controllo, basta fare clic con il pulsante destro del mouse sulla OU desiderata e selezionare "Delega il controllo". La figura seguente mostra la delega dell'autorità di reimpostazione della password al gruppo Help Desk.

Il contributo di Active Roles

I "ruoli" in Active Roles sono denominati modelli di accesso e rappresentano gruppi di autorizzazioni a elevati livelli di granularità, applicabili a qualsiasi posizione nelle infrastrutture Active Directory. È possibile applicarli anche a posizioni virtuali che è possibile personalizzare e mantenere in modo dinamico all'interno dello strumento.

I modelli di accesso sono un gruppo di autorizzazioni AD, suddivise in categorie per oggetto di destinazione, che permettono di delegare in modo intuitivo i permessi di amministrazione in base a un modello di privilegi minimi. Può trattarsi di gruppi di autorizzazioni semplici, come "Reimposta password", o più complessi, come autorizzazioni di lettura/scrittura/elenco di tutti gli attributi di un oggetto AD. Grazie ai suoi oltre 300 modelli di accesso di comune utilizzo collaudati e testati, Active Roles è uno degli strumenti più rapidi da implementare, garantendo un ROI immediato. La creazione di nuovi modelli è semplice e veloce.

Passaggio 10. Sfruttare la tecnologia dei flussi di lavoro

SharePoint come soluzione ottimale per la gestione degli account rispetto alla semplice posta elettronica

Molte organizzazioni cercano di gestire richieste di nuovi account, cessazioni di rapporti di impiego, cambiamenti di mansioni e varie approvazioni esclusivamente mediante la posta elettronica. Questo approccio rende difficile rispettare gli standard di gestione degli account o dimostrare la conformità. La tecnologia dei flussi di lavoro, come gli elenchi in SharePoint, non è sicuramente un'opzione di automazione completa per la gestione degli account, ma è un netto passo avanti rispetto all'uso della sola posta elettronica. SharePoint, come tecnologia dei flussi di lavoro esemplificativa, permette di inserire indirizzi e-mail negli elenchi di annunci, in modo da trasformare le e-mail in arrivo in nuovi voci dell'elenco e trasferire i documenti allegati negli allegati delle voci dell'elenco. Puoi personalizzare l'elenco con i campi Stato per tracciare le fasi di elaborazione delle voci dell'elenco.

Esempio: usare SharePoint per gestire le modifiche degli account legate alle cessazioni dei rapporti di impiego

Ad esempio, puoi usare un elenco SharePoint abilitato per la posta elettronica per organizzare le notifiche di cessazione di impiego e documentare la conformità con le procedure relative agli utenti in uscita. Se usi l'opzione 2 o 3 nel passaggio 5, configura l'applicazione HR in modo che invii le e-mail al tuo elenco SharePoint e aggiunga le colonne Stato e Note all'elenco. In caso di trasmissione all'elenco di report o notifiche di cessazione del rapporto di impiego, puoi disabilitare gli account associati in AD e modificare la voce dell'elenco per documentarne l'elaborazione e la conseguente disabilitazione degli account. Puoi anche registrarti agli avvisi dell'elenco in modo da essere informato non appena viene creata una voce. Elenchi simili possono essere creati per le richieste di nuovi account e le notifiche relative ai cambi di mansione. Devi sfruttare la tecnologia dei flussi di lavoro per ridurre gli oneri cartacei degli amministratori, migliorando al contempo la conformità.

Il contributo di Active Roles

L'architettura di Active Roles permette di applicare funzionalità di reporting e auditing a tutte le operazioni CRUD. Ciò garantisce report per tutte le modifiche o le creazioni di nuovi account, tutte le creazioni di gruppi, le modifiche e il deprovisioning degli account In effetti, tutto ciò che accade attraverso Active Roles è sottoposto ad audit.

I report includono le cinque W (who, what, when, where e why, chi, cosa, quando, dove e perché) e possono essere inviati in automatico ai responsabili degli audit. Inoltre, i report sono accessibili online, tramite un portale Web.

L'elevato livello degli audit consente inoltre di annullare le azioni in modo sicuro. Un'azione errata di deprovisioning, ad esempio, può essere annullata in pochi clic, senza pregiudicare la continuità operativa.

Garantire la sicurezza di AD ed eliminare gli account indesiderati in modo automatico

Estendere e automatizzare le funzioni degli strumenti nativi per ridurre i rischi

I 10 suggerimenti contenuti in questo documento ti aiuteranno a eliminare gli account indesiderati in AD, oltre a evitare che i problemi si ripetano. Tuttavia, se ci si limita a seguire i suggerimenti senza investire in strumenti aggiuntivi, gran parte degli oneri di conferma manuale e amministrativa gravanti sul personale IT resteranno invariati, così come gli interventi necessari di utenti finali, responsabili e personale HR per la notifica e le informazioni su importanti eventi del ciclo di vita degli utenti.

L'IT della maggior parte delle organizzazioni dedica molto tempo alla creazione ed eliminazione degli account in AD. Gli strumenti nativi sono inefficienti e dispendiosi in termini di tempo, con processi manuali che introducono la possibilità di errori umani pericolosi per la sicurezza e stabilità dell'ambiente Windows. Inoltre, molte organizzazioni utilizzano processi altrettanto inefficienti ma completamente separati per la creazione di account nei sistemi non Windows, aumentando così gli oneri amministrativi e introducendo ancora più rischi per la sicurezza.

Manutenzione automatizzata degli account, riduzione delle attività e ottimizzazione della sicurezza con Active Roles

Come visto nella sezione "Il contributo di Active Roles" in ciascun passaggio, Active Roles automatizza la maggior parte della manutenzione di AD e offre una pletora di funzioni per eliminare gli interventi di utenti finali, responsabili e personale HR. Active Roles consente di portare a termine tutti i passaggi di questo documento.

Garantisce la sincronizzazione fra AD, database e directory esterne, compresi SharePoint Server, applicazioni aziendali e molto altro ancora. Ogni sistema su quasi tutti i sistemi operativi moderni oggi può sfruttare una sincronizzazione bidirezionale dell'identità in locale o nel cloud. Soprattutto, grazie all'integrazione con le applicazioni HR, la creazione di account di identità può essere utilizzata per agevolare la gestione automatica degli accessi.

Active Roles automatizza la creazione e l'amministrazione di account basati su AD. Gli utenti vengono assegnati a mansioni corrispondenti alle loro responsabilità, in modo da concedere la autorizzazioni opportune alle risorse giuste. In questo modo, gli utenti sono più soddisfatti poiché in grado di recuperare le risorse necessarie per il loro lavoro, così come gli amministratori, grazie all'automatizzazione di tutte le attività che riduce le attività ripetitive che richiedono continui clic.

Active Roles fornisce gestione immediata degli account di utenti e gruppo, sicurezza avanzata basata su ruoli, amministrazione quotidiana delle identità e reporting e controllo integrato per gli ambienti basati su Windows.

Active Roles include queste funzioni:

- **Accesso sicuro**: Active Roles agisce come un firewall virtuale intorno ad Active Directory, consentendoti di controllare gli accessi tramite deleghe utilizzando un modello dei privilegi minimi. Basato su policy amministrative definite e relative autorizzazioni, genera e applica rigorosamente le regole per gli accessi, eliminando gli errori e le incoerenze comuni negli approcci nativi alla gestione AD. Inoltre, procedure di approvazione affidabili e personalizzate creano processi e controlli IT coerenti con i requisiti aziendali, con catene di responsabilità che vanno a completare la gestione automatizzata dei dati delle directory.
- **Creazione automatizzata degli account**. Automatizzazione di un'ampia gamma di attività, tra cui:
- Creazione di account di utenti e gruppi in AD e AAD
- Creazione di caselle di posta elettronica in Exchange/Exchange Online
- Popolamento dei gruppi
- Assegnazione delle risorse in Windows

Active Roles automatizza inoltre il processo di riassegnazione e rimozione dei diritti di accesso degli utenti nei sistemi AD/AAD e nei sistemi collegati ad AD (compresa l'eliminazione di utenti e gruppi) per garantire un processo amministrativo efficiente e sicuro per la durata di utenti e gruppi. In caso di aggiornamento o rimozione di un accesso utente, gli aggiornamenti avvengono in automatico in AD, Exchange, SharePoint, OCS, Lync e Windows e qualsiasi sistema collegato ad AD come Unix, Linux e Mac OS X.

- **Gestione quotidiana delle directory.** Gestione immediata garantita di tutti gli elementi seguenti:
- Destinatari di Exchange/Exchange Online, compresa assegnazione di caselle di posta/OCS, creazione, spostamento, eliminazione, autorizzazioni e gestione degli elenchi di distribuzione
- Gruppi
- Computer, fra cui condivisioni, stampanti, utenti e gruppi locali
- Active Directory, compreso AD LDS
- Include anche interfacce intuitive per migliorare l'amministrazione quotidiana e le operazioni di help desk tramite uno snap-in MMC e un'interfaccia Web
- **Gestione di gruppi e utenti in un ambiente in host:** Active Roles funziona in un ambiente in host in cui gli account provenienti dal dominio AD client vengono sincronizzati con un dominio AD host. Ciò permette la gestione di account di utenti e gruppi dal dominio client al dominio in host, sincronizzando anche attributi e password. Utilizza i connettori predefiniti per sincronizzare i tuoi account AD in locale con altre piattaforme e applicazioni. Sfrutta una gamma in continua espansione di oltre 30 connettori (https://www.cloud.oneidentity.com/products/connect/connectors) per vari servizi e applicazioni basati sul cloud come Salesforce, G-Suite e ServiceNow tramite One Identity Starling Connect.
- **Consolida i punti di gestione attraverso l'integrazione:** Active Roles si integra con tecnologie e strategie IAM esistenti, estende tutte le funzionalità, semplifica e consolida i punti di gestione garantendo un'integrazione immediata con molti prodotti One Identity, tra cui Identity Manager, Privilege Password Manager, Desktop Virtualization, Authentication Services, Defender, Password Manager e Quest Change Auditor. Inoltre, Active Roles automatizza ed espande le funzionalità di PowerShell, ADSI, SPML e le interfacce Web personalizzabili.

10 passaggi per ottenere prestazioni, agilità e sicurezza

Passaggio 1. Eseguire un'analisi regolare degli account

Passaggio 2. Collegare gli account ai record dei dipendenti

Passaggio 3. Monitorare i nuovi account

Passaggio 4. Automatizzare la manutenzione dell'account

Passaggio 5. Gestire gli utenti in uscita e le modifiche ai ruoli

Passaggio 6. Gestire gli account inattivi

Passaggio 7. Gestire gli account non umani

Passaggio 8. Controllare le eccezioni

Passaggio 9. Controllare l'autorità amministrativa

Passaggio 10. Sfruttare la tecnologia dei flussi di lavoro

Questi 10 passaggi possono eliminare gli account indesiderati in AD/Azure AD, ottimizzando prestazioni e sicurezza. One Identity Active Roles consente di eseguire questi passaggi ed eliminare i dati indesiderati. Quindi, riprendendo la metafora iniziale, parti con il modello di serie della tua auto, elimina gli account indesiderati e goditi prestazioni, velocità e gestione offerte da Active Roles nella tua strategia AD/AAD.

Microsoft Active Directory e One Identity Active Roles: una sinergia ottimale

Informazioni su One Identity

One Identity di Quest permette alle organizzazioni di implementare una strategia di sicurezza incentrata sulle identità, con base locale, cloud o in un ambiente ibrido. Grazie alla nostra offerta esclusiva, ampia e con forti capacità di integrazione, che include gestione degli accessi account, governance e amministrazione delle identità e gestione degli accessi privilegiati, le organizzazioni possono davvero raggiungere il massimo potenziale e la massima sicurezza, ponendo le identità come base dei propri programmi e concedendo l'accesso corretto a tutti i tipi di utente, sistemi e dati. Per ulteriori informazioni, visita la pagina OneIdentity.com

Whitepaper_2021_MicrosoftBetterTogetherwithOIDActiveRoles_PG_IT-WL-67415