WHITEPAPER

Zusammen einfach besser: 10 Schritte für ein optimiertes Active Directory mit One Identity Active Roles

Über dieses Dokument

In diesem Dokument finden Sie 10 Schritte zum Beheben und Vermeiden von Problemen in Zusammenhang mit Benutzerkonten in AD. Bei diesen Schritten kommen native AD-Funktionen und gängige Workflow-Technologie wie Microsoft SharePoint zum Einsatz, weshalb auch der Einarbeitungsaufwand zum Implementieren der Empfehlungen aus diesem Dokument sehr gering ausfällt.

Doch auch bei Berücksichtigung all dieser Empfehlungen bleibt ohne zusätzliche Tools zum Verwalten und Automatisieren von Prozessen der Großteil des Verwaltungs- und manuellen Prüfungsaufwands an Ihren Geschäftsbereichsmanagern, HR-Mitarbeitern und IT-Teams hängen.

Die gute Nachricht ist, dass One Identity Active Roles von Quest bei praktisch all diesen Herausforderungen Abhilfe schaffen kann. Active Roles bietet zahlreiche Funktionen, mit denen die Abhängigkeit von Endbenutzern, Managern und HR-Personal eliminiert wird. In diesem Dokument erfahren Sie, wie Active Roles jeden einzelnen der 10 Schritte erleichtert.

Überblick

Microsoft Active Directory (AD) und Azure AD (AAD) ermöglichen die Organisation und Standardisierung der Verwaltung und Speicherung von Identitäts- und Kontodaten. One Identity Active Roles sorgt für Agilität, Sicherheit, Geschwindigkeit und Einheitlichkeit bei der Verwaltung von AD/Azure AD. Durch die Kombination von Active Roles und AD/AAD verfügen IT-Administratoren über eine Lösung, die die Sicherheit und Effizienz in ihrer AD-Umgebung deutlich steigert und Schwachstellen reduziert. Wären wir jetzt im Automobilbereich, wäre dies damit vergleichbar, einen leistungsstarken Sportwagen um ein Rennsportfahrwerk, einen Turbolader und ein deutlich besseres Dahsboard- und Leistungsüberwachungssystem mit Cloud-Anbindung zu ergänzen, wobei all das mit einem programmierbaren und überaus sicheren Funkschlüsselanhänger geschützt wird.

Das Fahrzeug aus dem Showroom ist zwar großartig, doch mit der nachgerüsteten Version sind Sie auf der Straße allem gewachsen, auch massiven Veränderungen und Gefahren. Das erweiterte Modell ist nicht nur schneller und sicherer, es hat auch eine unglaublich gute Kurvenlage, erfordert weniger laufende Wartungsmaßnahmen und ist kraftstoffsparender. Ihre Zusatzinvestitionen amortisieren sich schnell und Sie sind damit für Routen gerüstet, die vorher nie infrage kamen. Alles in allem ist der Wagen einfach besser.

Genauso ist es auch bei Active Directory und One Identity Active Roles. Zusammen sind sie besser.

Wenn es bei Ihnen so ist wie bei 95 % der Fortune 1000-Unternehmen, haben Sie bereits das Fahrzeug aus dem Showroom: Sie verwenden Microsoft Active Directory als Grundlage für die alltägliche Provisionierung/Deprovisionierung von Benutzerberechtigungen. Doch die Welt entwickelt sich immer schneller und die mit AD und Azure AD – sowie AD LDS – verwalteten Ressourcen werden zunehmend vielfältiger. Zudem steigt aufgrund anderer Trends die Komplexität rund um AD/AAD. Dies gilt beispielsweise für die Identitätssicherheit, die Migration zur Cloud und die kritische Rolle von AD/AAD für die Verwaltung des privilegierten Zugriffs (Privileged Access Management, PAM). Die Implementierung einer Zero Trust-Sicherheitsarchitektur – oder von Zero Standing Privileges (keinerlei beständige Berechtigungen) – zum Vermeiden von Sicherheitsverletzungen und Begrenzen des gegebenenfalls entstehenden Schadens erhöht ebenfalls die Notwendigkeit der Erweiterung und Verbesserung der nativen Funktionen von AD/AAD. One Identity Active Roles kann AD/AAD-Services automatisieren und optimieren.

In diesem Dokument erläutern wir 10 Schritte zum Bereinigen Ihrer Microsoft AD/AAD-Benutzerkontodaten. Dieser Prozess ist für die Effizienz und Sicherheit unerlässlich. Bei der Erläuterung der zehn Schritte führen wir Sie durch jeden einzelnen Schritt und zeigen Ihnen, warum er wichtig ist und wie One Identity Active Roles den Schritt unterstützt oder beschleunigt. Viele Schritte liegen eigentlich auf der Hand, zum Beispiel das Löschen ungenutzter Konten und das Entziehen des Zugriffs auf Anwendungen und andere Ressourcen. Doch wie wir alle wissen, ist es im Eifer des täglichen Gefechts schwierig, manuelle Aufgaben zur Kontowartung zu priorisieren, wenn es akute technische oder datenbezogene Probleme gibt. Entdecken Sie, wie One Identity Active Roles diese Aufgaben automatisieren und absichern kann. In Kombination mit One Identity CertAccess können Sie zudem sicherstellen, dass Autorisierungs-, Genehmigungs- und Zertifizierungsprozesse befolgt und protokolliert werden.

Active Roles bietet zahlreiche Funktionen, mit denen die Abhängigkeit von Endbenutzern, Managern und HR-Personal eliminiert wird.

Bei diesen 10 Schritten kommen native AD-Funktionen und gängige Workflow-Technologie wie Microsoft SharePoint zum Einsatz, weshalb der Einarbeitungsaufwand zum Implementieren der Empfehlungen aus diesem Dokument sehr gering ausfällt.

Doch auch bei Berücksichtigung all dieser Empfehlungen bleibt ohne zusätzliche Tools zum Verwalten und Automatisieren von Prozessen der Großteil des Verwaltungs- und manuellen Prüfungsaufwands an Ihren Geschäftsbereichsmanagern, HR-Mitarbeitern und IT-Teams hängen.

Die gute Nachricht ist, dass One Identity Active Roles von Quest bei praktisch all diesen Herausforderungen Abhilfe schaffen kann. Active Roles bietet zahlreiche Funktionen, mit denen die Abhängigkeit von Endbenutzern, Managern und HR-Personal eliminiert wird.

Lesen Sie weiter und informieren Sie sich darüber, inwiefern und warum Active Directory und One Identity Active Roles zusammen einfach besser sind.

Active Directory ist für das Risikomanagement und die Gewährleistung der Compliance unerlässlich

Active Directory (AD) bildet in den meisten Unternehmen die Grundlage für das Identitäts- und Zugriffsmanagement (IAM) und ist demnach auch die wahrscheinlich wichtigste Technologie im Netzwerk. Immer mehr Systeme und Anwendungen stützen sich für die Authentifizierung, Richtlinien, Berechtigungen und die Konfigurationsverwaltung auf AD und Azure Active Directory. Unzureichende AD-Sicherheit beeinträchtigt die Sicherheit insgesamt.

Benutzerkonten sind wichtig für die Sicherheit, aber schwer zu pflegen

Für das Risikomanagement und zuverlässige Compliance ist es unbedingt erforderlich, Active Directory/Azure AD abzusichern. Allerdings ist es durchaus eine Herausforderung, dafür zu sorgen, dass AD in einem einwandfreien, gut organisierten und sicheren Zustand bleibt – insbesondere, wenn es um die Benutzerkonten geht.

Benutzerkonten sind die Basis für die Authentifizierung und den Zugriff auf Netzwerke, Systeme und Anwendungen.

Ohne angemessene Tools für die Nachverfolgung sämtlicher Benutzerberechtigungen über verschiedene Plattformen hinweg sind diese Konten schwer zu pflegen. Bei Einstellung eines neuen Mitarbeiters wird ein Benutzerkonto erstellt. Wenn sich die Arbeit und Aufgaben dieses Benutzers ändern, wird sein AD-Konto aktualisiert (beispielsweise die Position, Abteilung und Telefonnummer). Das gilt auch, wenn der Benutzer Gruppen beitritt oder Gruppen verlässt. Sollte der Benutzer das Unternehmen schlussendlich komplett verlassen, sollten die Zugriffsrechte des Kontos ordnungsgemäß gelöscht werden.

Dieser Prozess klingt einfach und unkompliziert. Viele Unternehmen arbeiten jedoch mit einer beträchtlichen Anzahl an Benutzerkonten, die über unangemessene oder veraltete Berechtigungen verfügen und gegen die Sicherheitsrichtlinien des Unternehmens verstoßen. Das größte Problem ist, dass solche Konten Sicherheitsrisiken für das Unternehmen bedeuten.

Die Ursache dieser Probleme ist eine unzureichende Lebenszyklusverwaltung mit Blick auf Benutzerkonten. In der Regel vertrauen Unternehmen darauf, dass Endbenutzer, Manager und HR-Mitarbeiter Ereignisse mit Auswirkungen auf das AD-Konto von Benutzern erkennen. Diese viel beschäftigten Personen sollen dann das überarbeitete IT-Team informieren, damit es die nötigen Änderungen in AD vornimmt und die Benutzerkonten auf dem aktuellen Stand bleiben. Wenn ausschließlich manuelle Prozesse zum Einsatz kommen, werden diese Änderungen allzu oft nicht ausgeführt, was zu Geisterkonten und unangemessenen Berechtigungen führt, die von bösartigen Akteuren ausgenutzt werden können, um ein Unternehmen ins Chaos zu stürzen.

10 Schritte zum Steigern der Agilität, Sicherheit und Leistung von Active Directory

Schritt 1: Konten regelmäßig analysieren

Die effektivste Vorgehensweise zum Gewährleisten eines einwandfreien und sicheren AD/AAD besteht in der regelmäßigen Überprüfung der Benutzerkonten. Beim Durchgehen der Kontoeigenschaften vor einem Audit können Sie viele Punkte, die für Auditoren problematisch sind, schnell finden und ausräumen.

Das Generieren einer Liste der Benutzerkonten ist einfach

Es gab eine Zeit, in der das Erstellen einer Liste mit Benutzerkonten keine einfache Aufgabe war. Heute muss einfach nur ein Windows PowerShell Skript ausgeführt werden und dann importieren Sie die Ergebnisse in Microsoft Excel. Das unter http://www.ultimatewindowssecurity.com/tools/Output-ADUsersAsCSV verfügbare Skript (Output-ADUsersAsCSV) gibt die Ergebnisse als Tabelle aus, ähnlich wie unten.

	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

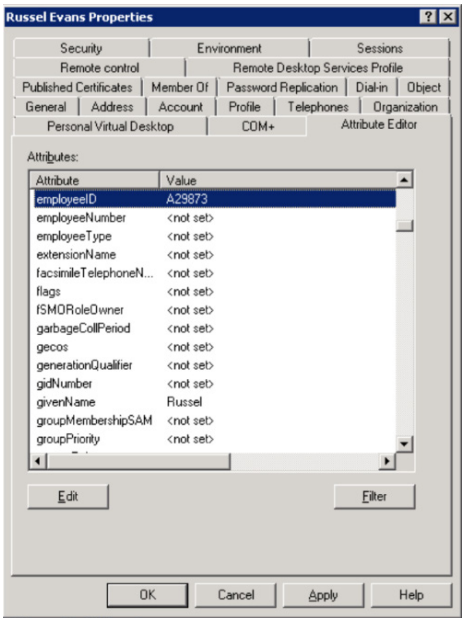
Nicht konforme Konten lassen sich durch Filtern der Tabelle aufdecken

Mit einem Skript und der damit erstellten Tabelle können Sie nach verschiedenen Benutzereigenschaften filtern, um nicht konforme Konten ausfindig zu machen. Suchen Sie zuerst nach Konten mit Problemen, die leicht identifizierbar sind, beispielsweise ein nie ablaufendes Kennwort. Beziehen Sie dann Filterkriterien in anderen Spalten ein, z. B. „SAM-ID“ oder „Description“ (Beschreibung), um Service-, Anwendungs- und sonstige Konten auszuschließen, die Ausnahmen darstellen.

Das sind Probleme, die sich vor Eintreffen der Auditoren schnell beheben lassen, sodass Sie den Risikobefund Ihres Audits verbessern können. Ein offensichtliches Problem, nach dem Sie Ausschau halten sollten, sind inaktive Konten. Diesem Thema ist hier ein ganzer Schritt gewidmet.

Es gibt aber noch viele weitere Probleme, beispielsweise Konten, die eigentlich nie hätten erstellt werden sollen oder bei deren Provisionierung gegen Namensstandards oder andere Kontrollen für die Kontoerstellung verstoßen wurde.

Hier ein Beispiel: Die Namensstandards von Acme Corp schreiben vor, dass alle Endbenutzerkonten mit „u-“, Administratorkonten mit „p-“ (für privilegiert) und Servicekonten mit „s-“ beginnen müssen. Filtern Sie zuerst alle Konten heraus, die mit diesen Präfixen beginnen, um die übrigen fragwürdigen Konten ausfindig zu machen. Einige dieser Konten können legitime Ausnahmen darstellen, die Sie in einem späteren Schritt angehen können. Viele werden sich als rätselhafte Konten herausstellen, denen Sie nachgehen müssen, um ihren Zweck und Status zu bestimmen.



AD-Konten können auf verschiedene Weisen mit Mitarbeiterdatensätzen verknüpft werden: (1) Mit dem Attribut „Mitarbeiter-ID“ oder „Mitarbeiternummer“ in AD (2) Über die Registerkarte „Attribut-Editor“, wie oben abgebildet

(3) Durch Eingabe der Mitarbeiter-ID im Beschreibungs- oder Anmerkungsfeld (4) Durch Einbindung der Mitarbeiternummer in den Anmeldenamen

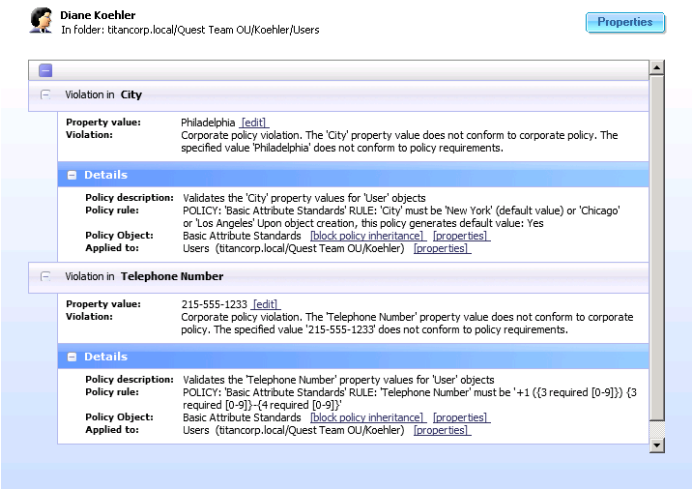
Diesen Schritt sollten Sie vor einem Audit definitiv ausführen. Um die Kontrolle über Ihr AD zu behalten, empfiehlt es sich allerdings, das monatlich zu tun. Immerhin wurden Sie wahrscheinlich nicht nur eingestellt, damit das Unternehmen seine Audits besteht. Das Ziel sollte sein, ein durchweg sicheres und gut organisiertes AD zu erreichen.

Beachten Sie, dass es sich bei diesem Schritt um eine Kontrolle zum Aufdecken oder Reagieren handelt und nicht um eine präventive oder proaktive Kontrolle. Ihr Ziel sollte sein, das Auftreten dieser Probleme zu vermeiden. Schritt 2 ist die erste Möglichkeit, dieses Ziel zu erreichen.

Wie Active Roles helfen kann

Active Roles bietet die Möglichkeit, Ihre angestrebten AD-Objektstandards (als Richtlinien bezeichnet) mit Ihren AD-Objekten zu vergleichen. Die Ergebnisse dieses Vergleichs (also der Anfrage zum Ausführen der Richtlinienprüfung) werden ad hoc auf dem Bildschirm bereitgestellt, mit zwei Klicks oder durch regelmäßig geplante Berichte. Diese Funktionalität kann einem Unternehmen helfen, für Ordnung zu sorgen.

Das Erstellen der Richtlinien ist mit einem relativ geringen administrativen Aufwand verbunden und dann können Sie damit beginnen, Ihr AD wieder unter Kontrolle zu bringen.



Active Roles bietet die Möglichkeit, Ihre angestrebten AD-Objektstandards (als Richtlinien bezeichnet) mit Ihren AD-Objekten zu vergleichen.

Schritt 2: Konten mit Personalakten verbinden

Die fundamentalste Möglichkeit, AD-Konten in einwandfreiem und sicherem Zustand zu halten, besteht in der Verknüpfung der Konten mit tatsächlichen Benutzern. Das umfasst auch Konten, die nicht für Personen erstellt werden, also beispielsweise Konten für Services und Anwendungen. Das wird später in Schritt 7 erläutert. Konzentrieren Sie sich zunächst auf Konten, die für Personen erstellt wurden, einschließlich Endbenutzern, Auftragnehmern, Administratoren und anderer Personen.

Vor allem sollte jedes Mitarbeiterkonto mit dem Masterdatensatz des jeweiligen Mitarbeiters in Ihrem Personalsystem verknüpft werden.

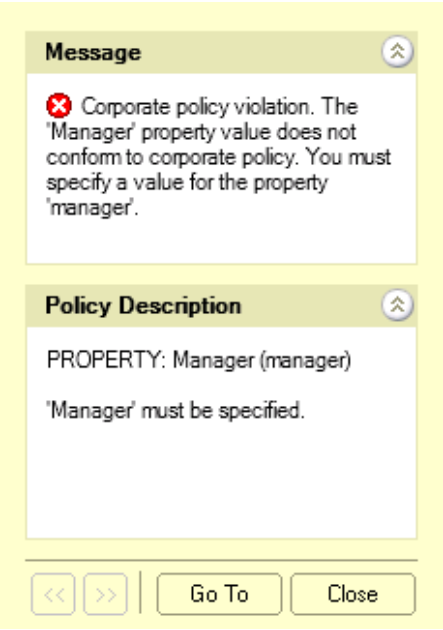
Diese Verknüpfung ist wichtig, weil der Zugriff eines Mitarbeiters auf das Netzwerk an seinen Status und seine Rolle innerhalb des Unternehmens gebunden sein sollte. Der offizielle Datensatz, der dafür verwendet werden sollte, ist der Masterdatensatz im Personalsystem, der auch am wahrscheinlichsten auf dem neuesten Stand ist.

Wenn sich der Status oder die Rolle eines Mitarbeiters ändert, müssen Sie imstande sein, seine Konten zu finden und den Status oder die Berechtigungen entsprechend zu ändern. Der Schlüssel ist das Dokumentieren der Mitarbeiter-ID in AD-Konten. Natürlich müssen Sie auch Verfahren implementieren, um die Reaktion auf solche Ereignisse zu erleichtern. Das besprechen wir in einem späteren Schritt.

Wenn sich der Status oder die Rolle eines Mitarbeiters ändert, müssen Sie imstande sein, seine Konten zu finden und den Status oder die Berechtigungen entsprechend zu ändern. Der Schlüssel ist das Dokumentieren der Mitarbeiter-ID in AD-Konten. Natürlich müssen Sie auch Verfahren implementieren, um die Reaktion auf solche Ereignisse zu erleichtern. Das besprechen wir in einem späteren Schritt.

Wie Active Roles helfen kann

Mithilfe von Erstellungsrichtlinien kann Active Roles vorschreiben, dass alle nicht für Personen erstellten Konten mit einem Wert für die Manager- oder Mitarbeiter-ID erstellt werden. Eigentlich kann Active Roles die Kontoprovisionierung und das Format jeglicher Attribute verwalten.



Erfolgreiche Eindringlinge, ob menschlich oder automatisiert, erstellen oft Backdoor-Konten, um fortlaufenden Zugriff sicherzustellen und ihre Aktivitäten zu verschleiern.

Schritt 3: Neue Konten überwachen

Bei IT-Audits von AD ist es nicht ungewöhnlich, unnütze und nicht standardkonforme Konten zu finden – darunter auch diejenigen, die von den Namenskonventionen des Unternehmens abweichen. Das passiert, wenn zu viele Mitarbeiter in der IT-Abteilung Konten erstellen dürfen. Darauf gehen wir in einem späteren Schritt ein.

Eindringlinge erstellen oft Backdoor-Konten

Erfolgreiche Eindringlinge, ob menschlich oder automatisiert, erstellen oft Backdoor-Konten, um fortlaufenden Zugriff sicherzustellen und ihre Aktivitäten zu verschleiern. Flame, eine moderne, als Waffe eingesetzte Malware, zielte speziell darauf ab, ein solches Konto zu erstellen, wenn sie feststellte, dass ein Domänenadministrator angemeldet war.

Halten Sie sie direkt bei der Kontoerstellung auf

Das Aufspüren neuer Konten ist also unerlässlich – aber auch zeitaufwendig und oftmals nicht schlüssig. Der beste Zeitpunkt zum Aufspüren eines nicht konformen Kontos ist der Zeitpunkt der Erstellung:

- Ermitteln Sie, wer das Konto erstellt hat.
- Arbeitet die Person noch in Ihrem Unternehmen?
- Warum wurde das Konto erstellt?

Wie Sie neue Konten überwachen und prüfen

Es gibt zwei Möglichkeiten, um neue Konten zu überprüfen und darauf zu reagieren:

- Sie können die Sicherheitsprotokolle von AD-Domänencontrollern auf das Ereignis mit der ID 4720 überprüfen (dafür müssen Sie die Audit-Unterkategorie „Benutzerkontenverwaltung“ aktivieren).
- Sie können das Skript Output-ADUsersAsCSV ausführen und dann anhand des Erstellungszeitpunkts sortieren.

Bei der Überprüfung der einzelnen Konten sollten Sie versuchen, die folgenden Fragen zu beantworten:

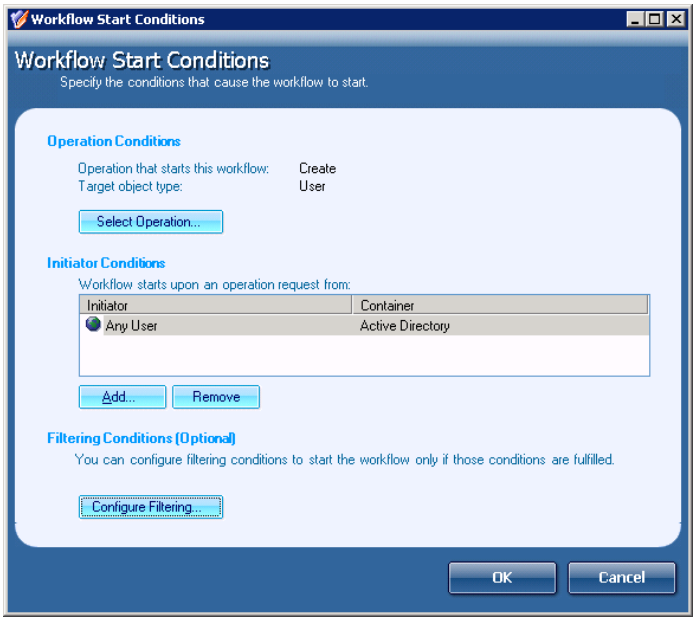
- Gibt es ein arbeitsbezogenes Ticket oder sonstige bekräftigende Dokumentation für dieses Konto?
- Stimmt das Konto mit festgelegten Namenskonventionen überein?
- Entspricht das Konto den anderen Kontoerstellungsstandards und -richtlinien Ihres Unternehmens?

```
Ereignis-ID 4720 – Ein Benutzerkonto wurde erstellt.
Antragsteller:
      Sicherheits-ID: ACME-FR\administrator
      Kontoname: administrator
      Kontodomäne: ACME-FR
         Anmelde-ID:
0x20f9d Neues Konto:
      Sicherheits-ID: ACME-FR\John.Locke
      Kontoname: John.Locke
      Kontodomäne: ACME-FR
Attribute:
      SAM-Kontoname: John.Locke
      Anzeigename: John Locke
      Benutzerprinzipalname: John.Locke@acme-fr.local
```

Wenn Sie feststellen, dass das Konto unzulässig oder nicht konform ist, müssen Sie dem nachgehen und mit dem Kontoersteller sprechen. Der Vorteil bei Verwendung der ersten Methode ist, dass Ereignis 4720 im Sicherheitsprotokoll Ihnen mitteilt, wer das Konto erstellt hat.

Wie Active Roles helfen kann

Active Roles fungiert als virtuelle Firewall um Active Directory und sorgt dafür, dass der Zugriff basierend auf dem Least-Privilege-Prinzip erzwungen wird. Da Workflows für sämtliche Vorgänge – wie das Erstellen, Ändern oder Löschen eines Kontos in der Domäne – genutzt werden können, sind Sie in der Lage, normalerweise manuelle Prozesse zu automatisieren. Dadurch ist sichergestellt, dass diese überaus wichtigen Aktionen auch tatsächlich ausgeführt werden, und zwar unmittelbar, vollständig und mit umfassender Prüfung.



Schritt 4: Kontowartung automatisieren

Schritte zum Erstellen eines neuen Kontos

Um sicherzustellen, dass neue Konten entsprechend Ihren Standards erstellt werden, sollten Sie den Kontoerstellungsprozess weitestgehend automatisieren, sodass das Risiko menschlicher Fehler reduziert wird. Die Kontoerstellung umfasst die folgenden Schritte:

1. Erstellen des Kontos in AD
2. Festlegen von Identitätsattributen (Position, Telefonnummern usw.)
3. Erstellen des Postfachs für das Konto in Microsoft Exchange/Office 365
4. Hinzufügen des Kontos zu Gruppen, die zur Rolle des Benutzers passen
5. Registrierung des AD-Kontos in anderen Anwendungen (nach Bedarf)

Automatisierung mit PowerShell Skripts

Viele dieser Schritte können mit PowerShell Skripts automatisiert werden. Das folgende Skript kümmert sich um die Schritte 1 bis 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
```

Für Rollen mit hoher Fluktuation in Ihrem Unternehmen können Sie eine individuell angepasste Version dieses Skripts erstellen. Sie können das Skript auch erweitern, damit Eingabewerte berücksichtigt werden und das Konto entsprechend den zum Ausführungszeitpunkt gewählten Optionen erstellt wird.

Wie Active Roles helfen kann

Active Roles bietet zahlreiche Schnittstellen, beispielsweise für PowerShell, ADSI Skripts, SPML, SCIM, MMC und das Web. Das Wichtige ist, dass Sie Standards (als Richtlinien bezeichnet) unabhängig von der Schnittstelle bei allen CRUD-Operationen für AD-Objekte erzwingen können. Durch diese Verwaltungsmöglichkeiten können Sie sicherstellen, dass sämtliche Aktivitäten in Ihrer AD-Umgebung komplett von Ihren Standards gesteuert werden. Bei Nichteinhaltung Ihrer Standards können Sie auswählen, ob die Folge ein erlaubter Verstoß (meldepflichtig) oder die Ausgabe eines Fehlers sein soll.

Schritt 5: Umgang mit ausgeschiedenen Benutzern und Rollenänderungen

Für Unternehmen mit klassischen Tools zur AD-Verwaltung stellen Geisterkonten oder verwaiste Benutzerkonten eine beständige Gefahrenquelle dar. Ohne Automatisierung und/oder Single Source of Truth für Identitäten und Berechtigungen werden Ihre Identitätsdaten wahrscheinlich auch Personen umfassen, die nicht mehr bei Ihnen angestellt oder im Auftrag Ihres Unternehmens tätig sind. Es ist unerlässlich, dass die jeweils für Statusaktualisierungen zuständigen Stellen – ob Personalabteilung oder IT – benachrichtigt werden, wenn jemand das Unternehmen verlässt oder eine neue Rolle übernimmt.

Das Aufspüren inaktiver Konten löst dieses Problem nicht

Es scheint zwar nichts Kompliziertes zu sein, doch Unternehmen versäumen es oft, Benutzerkonten zu deaktivieren oder Berechtigungen zu ändern, wenn ein Benutzer nicht mehr den gleichen Status hat. Wenn im Rahmen von Audits Fragen dazu gestellt werden, wie ein Unternehmen die Deaktivierung ausgeschiedener Benutzer handhabt, lautet eine häufige Antwort:
In der Regel wird Ausschau nach inaktiven Konten gehalten, indem nach Konten gesucht wird, bei denen sich in letzter Zeit niemand angemeldet hat. Dieser Ansatz ist insofern mängelbehaftet, als dass das Konto eines ehemaligen Mitarbeiters nicht als inaktiv identifiziert und in den Bericht über inaktive Konten aufgenommen wird, wenn die Person noch auf das Netzwerk zugreift.

Bei der Suche nach inaktiven Konten werden die Symptome anstelle der Ursache behandelt. Dieses Problem kann mit einem Ansatz ausgeräumt werden, der den gesamten Lebenszyklus von AD-Konten berücksichtigt – von der Einstellung bis hin zum Ausscheiden.

Das gleiche Prinzip könnte auf redundante Daten angewendet werden. Dies ist genauso wichtig wie die ordnungsgemäße Erstellung neuer Einträge. Ohne Bereinigung redundanter und unerwünschter Daten wird Ihr AD mit Daten überhäuft.

Effektive Möglichkeiten für den Umgang mit ausgeschiedenen Benutzern und Rollenänderungen

Im Folgenden finden Sie drei Möglichkeiten für den effektiven Umgang mit Statusänderungen, in absteigender Reihenfolge gemessen am Vorrang:

- Die meisten Unternehmen verfügen über einen klar definierten und strikt ausgeführten Prozess zum Entziehen des physischen Zugangs eines Benutzers zum Gebäude. Machen Sie die Deaktivierung des AD-Kontos zu einem Teil dieses Prozesses.
- Wenn es in Ihrer HR-Anwendung einen Workflow gibt, sollten Sie ihn so einrichten, dass automatisch eine E-Mail an Administratoren gesendet wird, wenn ein Benutzer das Unternehmen verlässt, eine neue Rolle übernimmt oder einem anderen Manager unterstellt wird.
- Bei den meisten HR-Anwendungen können automatische Berichte geplant werden. Richten Sie einen täglichen Bericht über Kündigungen und berufliche Veränderungen ein, der Kontoadministratoren bereitgestellt wird.

Unterm Strich sind Kontodeaktivierungen und Aktualisierungen des Berechtigungsstatus erforderlich, um Compliance mit Branchen- und Regierungsauflagen sicherzustellen. Ganz gleich, wie Ihr Prozess aussieht – das Management sollte sich seiner Bedeutung bewusst sein und die Zuständigkeiten sollten klar definiert werden.

Wie Active Roles helfen kann

Die Workflow-Optionen von Active Roles umfassen Aufgaben und ganze Prozesse, die durch Änderungen am Verzeichnis angestoßen werden. Dazu gehören auch Richtlinien für die Kontobeendigung, mit denen Ihr Unternehmen genau festlegen kann, was mit einem Benutzerkonto geschieht, wenn eine Person das Unternehmen verlässt.

Die Optionen umfassen das Deaktivieren des Kontos, das Verschieben der Organisationseinheit, das Verschlüsseln des Kennworts und Ändern des Anmeldenamens, das Umbenennen mit Operationsvariablen, das Einrichten von Delegierungen für E-Mails und Basisordnern usw.

Vor allem kann Active Roles den Benutzer aus sämtlichen Sicherheitsgruppen entfernen, neue Berechtigungen für das Basisverzeichnis des Benutzers vergeben, zugewiesene Office 365-Lizenzen freigeben und mehr. Ein wichtiger Hinweis an dieser Stelle ist, dass die Richtlinien manuell, programmgesteuert oder automatisch ausgelöst werden können.

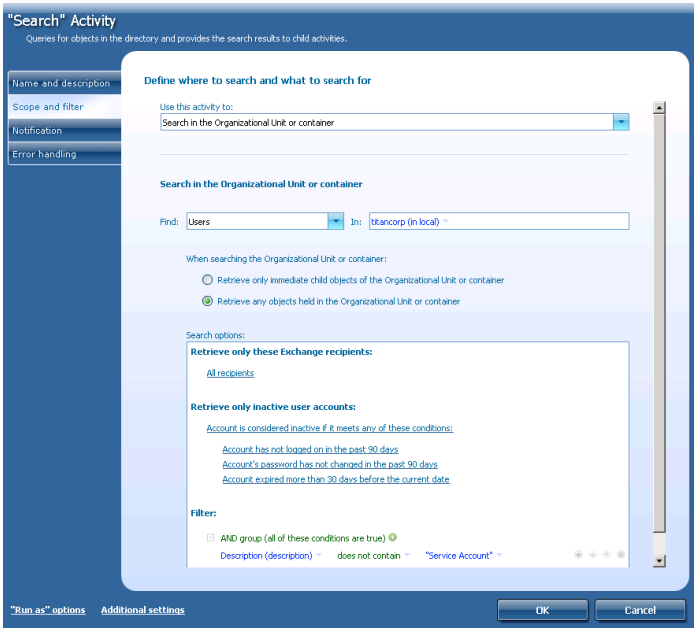
Schritt 6: Inaktive Konten angehen

Im nächsten Schritt geht es darum, regelmäßig nach inaktiven Konten Ausschau zu halten (also Benutzerkonten, bei denen sich in letzter Zeit niemand angemeldet hat). Dieser Schritt ist aber keinesfalls als Ersatz für Schritt 5 zu werten.

Inaktive Konten lassen sich leicht ausfindig machen

Vor Windows 2003 war das Aufspüren inaktiver Konten eine Herausforderung. Mit dem Attribut lastLogonTimestamp ist dies jetzt aber relativ einfach. Für diesen Abgleich (alle sieben Tage) können Sie Domänencontroller abfragen und sich die letzten Anmeldezeiten ansehen, um inaktive Konten zu identifizieren.

LastLogonTimestamp wird mit Get-ADUser über die Eigenschaft LastLogonDate verfügbar gemacht, wie im Skript OutputADUsersAsCSV in Schritt 1 veranschaulicht. Mit diesem Skript müssen Sie einfach nur anhand des letzten Anmeldezeitpunkt in absteigender Reihenfolge sortieren, um Konten ohne kürzlich erfolgte Anmeldung ganz einfach zu identifizieren.



Sie sollten auch auf Benutzerkonten achten, die sich nie angemeldet haben. In den mit Output-ADUsersAsCSV erstellten Tabellen erkennen Sie solche Konten daran, dass die Spalte zum letzten Anmeldezeitpunkt in der jeweiligen Zeile leer ist.

Wie Active Roles helfen kann

Active Roles automatisiert die Prozesse zum Identifizieren und Verwalten inaktiver Konten, einschließlich Klassifizierung, Erkennung und Korrektur. Dadurch wird der Kontobereinigungsprozess vereinfacht. Bei Verwendung in Kombination mit den richtigen Richtlinien für die Kontolebenszyklusverwaltung (z. B. die Deprovisionierung) können nicht nur bestehende Probleme gelöst, sondern auch künftige vermieden werden.

Active Roles automatisiert die Prozesse zum Identifizieren und Verwalten inaktiver Konten, einschließlich Klassifizierung, Erkennung und Korrektur.

Schritt 7: Nicht für Personen erstellte Konten verwalten

Nicht alle Konten sind direkt einer Person zugeordnet. Viele Anwendungen benötigen beispielsweise ein oder mehrere Konten für Services, um sich anzumelden. Diese Konten haben oft privilegierten Zugriff auf Server und Daten. Deshalb müssen sie abgesichert werden.

Warum hochgradig privilegierte Konten gefährdet sind

Anwendungskonten und andere nicht für Personen erstellte Konten sind schwer nachzuverfolgen. Bei IT-Audits ist es nicht ungewöhnlich, privilegierte Konten aufzudecken, die aus folgenden Gründen gefährdet sind:

- Niemand weiß genau, welchen Zweck das Konto hat oder warum es existiert.
- Trotz des Ausscheidens vieler Administratoren wurde ein Kontokennwort aus Angst, eine Anwendung irgendwo im Netzwerk zu beeinträchtigen, nicht aktualisiert.
- Das Konto ist befugt, sich interaktiv anzumelden.
    - Nicht für Personen erstellten Konten sollte es nicht erlaubt sein, sich interaktiv anzumelden – an der Konsole oder über Remotedesktops –, damit Administratoren (die das Kontokennwort kennen) sich nicht anonym mit diesem Konto und ohne individuelle Zurechenbarkeit anmelden können.

Nicht für Personen erstellte Konten identifizieren

Der erste Schritt für die Verwaltung von nicht für Personen erstellten Konten ist die Identifizierung ebendieser Konten. Dafür können Sie ein Präfix in der Namenskonvention für den Anmeldenamen verwenden, die Konten einer speziellen Organisationseinheit „Nicht für Personen erstelle Konten“ zuordnen oder sie mit einem anderen Attribut in AD als solche Konten kennzeichnen.

Den Zweck und Inhaber der einzelnen Konten dokumentieren

Als Nächstes sollten der Zweck des Kontos und die Systeme, auf denen es genutzt wird, in den Beschreibungs- oder Anmerkungsfeldern des Kontos dokumentiert werden.

Bestimmen Sie einen Inhaber für jedes nicht für Personen erstellte Konto und dokumentieren Sie dies in AD. Der Inhaber kann ein individuelles, für eine Person erstelltes Benutzerkonto sein, in der Regel ist es aber besser, eine Gruppe auszuwählen, die dem Team entspricht, welches für die Anwendung oder sonstige Technologie zuständig ist, die das Konto nutzt. Der Inhaber kann ebenfalls im Beschreibungs- oder Anmerkungsfeld dokumentiert werden.

Die Verwendung verwalteter Dienstkonten wurde in Windows Server 2008 R2 (und später auch gruppenverwaltete Dienstkonten) eingeführt, um die Kennwörter von Servicekonten automatisch zu verwalten (zu ändern). Mit verwalteten Dienstkonten/gruppenverwalteten Dienstkonten können Sie das Risiko einer Kompromittierung von Systemkonten beträchtlich senken.

Kennwortverwaltung

Die Kennwortverwaltung ist eine der größten Herausforderungen bei Konten, die nicht für Personen erstellt sind. Das Kennwort eines nicht für Personen erstellten Kontos muss jedes Mal geändert werden, wenn ein Administrator (der das Kennwort kennt) das Unternehmen verlässt. Ohne ordnungsgemäße Kontodokumentation lässt sich nur schwer bestimmen, zu welchen nicht für Personen erstellten Konten die einzelnen Administratoren Zugriff hatten. Das Ändern eines Kontokennworts birgt jedoch Risiken, da alle Services oder geplanten Aufgaben, die mit diesem Konto ausgeführt werden, und sämtliche Anwendungen, in denen das Kennwort dieses Kontos gespeichert ist, aktualisiert werden müssen, damit sie beim nächsten Start oder Anmeldeversuch nicht versagen.

Ermitteln, auf welchen Systemen ein Konto verwendet wird

Wenn Sie eine Reihe bestehender Konten bereinigen möchten, die nicht für Personen erstellt wurden, können Sie mithilfe des Windows-Sicherheitsprotokolls bestimmen, auf welchen Systemen die Konten verwendet werden. Sofern Sie die Audit-Unterkategorie „Ticketvorgänge des Kerberos-Services“ in Ihrem Gruppenrichtlinienobjekt „Standarddomänencontrollerrichtlinie“ aktiviert haben, protokollieren Ihre Domänencontroller das Ereignis mit der ID 4769. Durch das Durchsuchen der Domänencontroller-Sicherheitsprotokolle nach allen Vorkommen von 4769 (wobei als Kontoname das betreffende Servicekonto angegeben ist) können Sie eine Liste aller Computer erstellen, auf denen das Konto verwendet wird. Sehen Sie sich in diesen Ereignissen das Feld zum Servicenamen an. Bei Ereignissen mit der ID 4769 sind im Servicenamensfeld die Computer angegeben, für die das Benutzerkonto eine Authentifizierung anfordert.

Anmelderechte von nicht für Personen erstellten Konten beschränken

Ein letzter Schritt zum Absichern von Konten, die nicht für Personen erstellt wurden, besteht im Beschränken ihrer Anmelderechte auf Computern in der gesamten Domäne. Dadurch verhindern Sie, dass nicht für Personen erstellte Konten von jemandem missbraucht werden, der sich an der Konsole eines Computers oder über einen Remotedesktop interaktiv mit dem Konto anmeldet. Dieser Schritt dient als Defense-in-Depth-Maßnahme, falls Kennwortänderungen beim Ausscheiden von Administratoren versäumt werden. Fünf Anmeldetypen in Windows bieten beide Möglichkeiten und können Rechte zulassen und ablehnen:

Um sich auf eine bestimmte Weise anzumelden, müssen Sie über das entsprechende Recht zum Zulassen der Anmeldung verfügen. Wenn Ihnen aber auch das Recht zum Ablehnen der Anmeldung zugewiesen wurde, können Sie sich selbst dann nicht anmelden. Der Grund dafür ist, dass das Recht zum Ablehnen der Anmeldung Vorrang vor dem Zulassungsrecht hat. Sie finden diese Rechte in einem Gruppenrichtlinienobjekt unter Computereinstellungen\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten.

Generell sollten nicht für Personen erstellte Konten nur über das Recht „Anmelden als Service“ verfügen. Es empfiehlt sich, die Anmelderechte „Interaktiv“ und „Remotedesktop“ explizit zu verweigern, um zu verhindern, dass das Konto missbräuchlich verwendet wird. Wenn Sie alle nicht für Personen erstellten Konten zu einer speziellen Gruppe für diesen Zweck hinzufügen, können Sie dieser Gruppe die Rechte „Lokal anmelden verweigern“ und „Anmelden über Remotedesktopdienste verweigern“ in einem Gruppenrichtlinienobjekt wie „Standarddomänenrichtlinie“ zuweisen, das auf alle Domänencomputer angewendet wird.

Seien Sie beim Verweigern des Netzwerkanmelderechts achtsam. Die Anwendung, die das Konto nutzt, muss möglicherweise auf Ressourcen in anderen Netzwerken zugreifen.

Wie Active Roles helfen kann

Active Roles kann vorschreiben und (durch Vergleichsberichte) bestätigen, dass alle nicht für Personen erstellten Konten so konfiguriert werden bzw. sind, dass sie mit Blick auf die Namenskonvention, Attributeinstellungen, Objektspeicherorte und Gruppenmitgliedschaften (an Gruppenrichtlinienobjekt gebunden) den Standards Ihres Unternehmens entsprechen. Außerdem können Wenn/dann-Workflows genutzt werden, um eine (stufenweise) Genehmigung für alle Konten bzw. Servicekonten zu erzwingen, die an einem bestimmten Speicherort in Organsiationseinheiten erstellt werden, und/oder für Konten mit einem bestimmten Namenspräfix usw. Dabei werden alle diese Aktionen umfassend geprüft und sind an die jeweils zuständige Person gebunden.

Schritt 8: Ausnahmen verwalten

Legitime, genehmigte Ausnahmen dokumentieren

Das Sprichwort „Regeln sind dazu da, gebrochen zu werden“ gibt es schon seit Langem. Und auch bei den Standards für Benutzerkonten gibt es definitiv legitime Ausnahmen. Es kann beispielsweise sein, dass eine Ihrer Anwendungen ein Benutzerkonto mit einem spezifischen Namen erfordert, der gegen Ihre reguläre Namenskonvention verstößt. Für Situationen wie diese benötigen Sie eine Möglichkeit zum Dokumentieren legitimer, genehmigter Ausnahmen. Die beste Option hierfür ist eine Organisationseinheit namens „Ausnahmen“ oder das Kennzeichnen von Ausnahmekonten in den Beschreibungs- oder Anmerkungsfeldern.

Das einfache Kennzeichnen eines Kontos als Ausnahme reicht aber nicht aus. Wie in Schritt 7 beschrieben sollten auch der Zweck und Inhaber des Kontos dokumentiert werden.

Anmeldetyp	Anmelderechte
Interaktiv	Lokal anmelden zulassen Lokal anmelden verweigern
Remotedesktop	Anmelden über Remotedesktopdienste zulassen Anmelden über Remotedesktopdienste verweigern
Service	Anmelden als Service Anmelden als Service verweigern
Geplante Aufgabe	Anmelden als Service Anmelden als Service verweigern
Netzwerk (z. B. Zugriff auf freigegebene Ordner)	Anmelden als Stapelverarbeitungsauftrag Anmelden als Batchauftrag verweigern
FIPS 140-2-RDP-Transportverschlüsselung	Auf diesen Computer vom Netzwerk aus zugreifen Anmelden über Remotedesktopdienste verweigern

Das Sprichwort „Regeln sind dazu da, gebrochen zu werden“ gibt es schon seit Langem. Und auch bei den Standards für Benutzerkonten gibt es definitiv legitime Ausnahmen.

Lassen Sie Ausnahmen nicht zur Regel werden

Vorsicht: Es gibt AD-Implementierungen mit einem großen Anteil an Ausnahmekonten. Bei solchen Implementierungen haben die Mitarbeiter es sich zur Gewohnheit gemacht, Konten als Ausnahmen zu kennzeichnen, wenn das Befolgen von Standards und Verfahren für die Kontowartung sich als lästig erweist. Die Regelung für Ausnahmen sollte nicht übermäßig genutzt werden.

Wie Active Roles helfen kann

Active Roles kann Ausnahmen berücksichtigen und mithilfe von Richtlinien kontrollieren, sodass Ausnahmekonten nur an bestimmten Speicherorten zulässig sind. Wenn eine Ausnahme am Ort für Ausnahmen erstellt wird, stellt Active Roles sicher, dass allen erforderlichen Konfigurationsstandards, Attributen oder Richtlinienbeschränkungen Rechnung getragen wurde und dass sie erzwungen werden.

Außerdem können Genehmigungs-Workflows verwendet werden, sodass bei (manuellen oder programmgesteuerten) Erstellungsanfragen für eine neue Ausnahme eine Eskalation stattfindet. So können Sie verhindern, dass Ausnahmen zur Regel werden.

Schritt 9: Administratorbefugnisse verwalten

Begrenzen Sie die Personen, die Konten erstellen dürfen

AD ist oft mit unnützen oder rätselhaften Konten übersät, weil zu viele Personen zum Erstellen von Benutzerkonten befugt sind.

Zum Erzwingen von Kontrollen für die Erstellung neuer Konten, die für Sicherheit und Compliance unerlässlich sind, muss die Anzahl der Personen, die Konten erstellen können, auf einige wenige geschulte Mitarbeiter beschränkt werden.

Assistent zum Zuweisen der Objektverwaltung verwenden

AD unterstützt das Least-Privilege-Prinzip durch die Möglichkeit für Administratoren, ausgewählte Berechtigungen über spezifische Organisationseinheiten zu delegieren. Bei ordnungsgemäßer Implementierung ermöglicht die Option zum Zuweisen der Objektverwaltung von AD es Mitarbeitern,

> *Active Roles umfasst mehr als 300 häufig verwendete, bewährte Zugriffsvorlagen, die Active Roles zu einem der Tools machen, mit dem Sie am schnellsten einsatzbereit sind.*

ihre Arbeit zu erledigen, ohne dass sie mehr Befugnisse als nötig erhalten. Statt den Helpdesk zu einem Mitglied der Domänenadministratoren zu machen, können Sie der Helpdesk-Gruppe beispielsweise die Berechtigung zum Zurücksetzen von Kennwörtern in der Organisationseinheit gewähren, die Ihre Endbenutzerkonten enthält.

Klicken Sie zum Starten des Assistenten zum Zuweisen der Objektverwaltung einfach mit der rechten Maustaste auf die gewünschte Organisationseinheit und wählen Sie „Objektverwaltung zuweisen“ aus. Die folgende Abbildung zeigt die Befugnis zum Zurücksetzen von Kennwörtern, die an die Helpdesk-Gruppe delegiert wurde.

Wie Active Roles helfen kann

Die „Rollen“ in Active Roles werden als Zugriffsvorlagen bezeichnet. Sie sind Sammlungen von Berechtigungen mit einem sehr hohen Detaillierungsgrad, die an jedem Ort in Ihrer Active Directory Infrastruktur angewendet werden können. Es ist sogar möglich, sie an virtuellen Orten anzuwenden, die innerhalb des Tools angepasst und dynamisch verwaltet werden können.

Zugriffsvorlagen sind eine Sammlung von AD-Berechtigungen, die nach Zielobjekt kategorisiert sind. Mit ihnen können Sie Administratorberechtigungen mühelos basierend auf dem Least-Privilege-Prinzip delegieren. Diese Berechtigungssätze können so einfach sein wie „Kennwort zurücksetzen“ oder so detailliert wie Berechtigungen zum Lesen/Schreiben/Auflisten für alle Attribute eines AD-Objekts. Active Roles umfasst mehr als 300 häufig verwendete, bewährte Zugriffsvorlagen, die Active Roles zu einem der Tools machen, mit dem Sie am schnellsten einsatzbereit sind und Investitionsrenditen generieren. Zudem lassen sich neue Vorlagen schnell und einfach erstellen.

Schritt 10: Workflow-Technologie nutzen

Für die Kontoverwaltung ist SharePoint besser als nur E-Mails

Viele Unternehmen versuchen, Anfragen für neue Konten, Kündigungen, berufliche Veränderungen und verschiedene Genehmigungen nur mit E-Mails zu bewältigen. Mit diesem Ansatz ist es schwierig, Kontoverwaltungsstandards zu befolgen und Compliance nachzuweisen. Workflow-Technologien wie Listen in SharePoint werden zwar niemals eine Option für die vollständige Automatisierung der

Kontoverwaltung sein, sie sind aber definitiv besser als nur E-Mails. SharePoint – als Beispiel für Workflow-Technologie – ermöglicht es Ihnen, Ankündigungslisten eine E-Mail-Adresse zuzuweisen, mit der eingehende E-Mails in neue Listenelemente umgewandelt und angefügte Dokumente in Listenelement-Anhängen übernommen werden. Sie können die Liste mit Statusfeldern anpassen, um die Bearbeitungsschritte des Listenelements zu verfolgen.

Beispiel: Verwendung von SharePoint zum Verwalten kündigungsbedingter Kontoänderungen

Sie können beispielsweise eine SharePoint Liste mit E-Mail-Unterstützung verwenden, um Kündigungsbenachrichtigungen zu organisieren und die Compliance mit Ihrem Verfahren für ausgeschiedene Benutzer zu dokumentieren. Wenn Sie Option 2 oder 3 in Schritt 5 nutzen, konfigurieren Sie Ihre HR-Anwendung so, dass sie ihre E-Mails an Ihre SharePoint Liste sendet, und fügen Sie der Liste Status- und Anmerkungsspalten hinzu. Wenn neue Kündigungsbenachrichtigungen oder -meldungen in die Liste eingetragen werden, können Sie die zugehörigen Konten in AD deaktivieren und das Listenelement bearbeiten, um zu dokumentieren, dass es bearbeitet wurde und welche Konten als Reaktion darauf deaktiviert wurden. Sie können in der Liste sogar Alarme abonnieren, damit Sie benachrichtigt werden, sobald ein Element erstellt wird. Für Anfragen für neue Konten und Benachrichtigungen wegen beruflicher Veränderungen können ähnliche Listen erstellt werden. Der springende Punkt ist, dass Sie Workflow-Technologie nutzen müssen, um Administratoren zu entlasten und gleichzeitig die Compliance zu verbessern.

Wie Active Roles helfen kann

Mit der Active Roles Architektur stehen Berichterstellungs- und Prüfungsfunktionen zur Verfügung, die auf alle CRUD-Operationen angewendet werden können. Das bedeutet, dass Berichte für sämtliche Erstellungen neuer Konten oder Änderungen daran sowie alle Gruppenerstellungen, -änderungen und Kontodeprovisionierungen verfügbar sind. Tatsächlich wird alles, was über Active Roles geschieht, geprüft.

Die Berichte umfassen Angaben zu den fünf Ws (wer, was, wann, wo und warum) und können automatisch an Auditoren gesendet werden. Außerdem kann online über ein Webportal auf Berichte zugegriffen werden.

Eine willkommene Begleiterscheinung dieser umfangreichen Prüfungen ist die Möglichkeit, Aktionen auf sichere Weise rückgängig zu machen. Eine irrtümliche Deprovisionierungsaktion kann beispielsweise mit wenigen Klicks mittels Rollback korrigiert werden, ohne dass die Geschäftskontinuität beeinträchtigt wird.

Ein immer einwandfreies und sicheres AD – auf automatische Weise

Erweiterung und Automatisierung der Funktionen nativer Tools zum Reduzieren der Risiken

Die 10 Empfehlungen in diesem Dokument helfen Ihnen, die Benutzerkonten in Ihrem AD zu bereinigen und zu verhindern, dass Probleme erneut auftreten. Wenn Sie jedoch diesen Empfehlungen einfach nur folgen, ohne in zusätzliche Tools zu investieren, bleibt ein Großteil des Verwaltungs- und manuellen Prüfungsaufwands für Ihr IT-Team bestehen – genau wie die Abhängigkeit von Endbenutzern, Managern und HR-Mitarbeitern, die das IT-Team über wichtige Ereignisse im Benutzerlebenszyklus benachrichtigen und informieren sollen.

Innerhalb der IT verbringen die meisten Unternehmen deutlich zu viel Zeit mit dem Erstellen und Löschen von Benutzerkonten in AD. Native Tools sind ineffizient und zeitaufwendig. Die manuellen Prozesse, die sie erfordern, bergen das Risiko menschlicher Fehler, die die Sicherheit und Stabilität Ihrer Windows-Umgebung beeinträchtigen können. Zudem haben viele Unternehmen gleichermaßen ineffiziente, aber komplett separate Prozesse zum Erstellen von Konten für ihre nicht Windows-basierten Systeme, was den Verwaltungsaufwand erhöht und noch mehr Sicherheitsrisiken mit sich bringt.

Active Roles automatisiert die Wartung von Benutzerkonten, reduziert den Aufwand und verbessert die Sicherheit

Wie in den Abschnitten „Wie Active Roles helfen kann“ in jedem Schritt angegeben, automatisiert Active Roles den Großteil der AD-Wartung. Zudem bietet das Tool zahlreiche Funktionen, mit denen die Abhängigkeit von Endbenutzern, Managern und HR-Mitarbeitern eliminiert wird. Active Roles hilft Ihnen bei der Umsetzung sämtlicher Schritte aus diesem Dokument.

Active Roles ermöglicht die AD-Synchronisierung mit externen Datenbanken und Verzeichnissen, einschließlich SharePoint Server, spezieller Anwendungen von Geschäftsbereichen und mehr. Für alle Systeme mit praktisch jedem modernen Betriebssystem ist jetzt eine bidirektionale Identitätssynchronisierung verfügbar, ob lokal oder in der Cloud. Und das Beste ist, dass die Identitätskontenerstellung bei Integration mit Ihrer HR-Anwendung zur Unterstützung der automatisierten Zugriffsverwaltung verwendet werden kann.

Active Roles automatisiert die AD-basierte Kontoerstellung und -verwaltung. Benutzern werden die zu ihren Zuständigkeiten passenden Jobrollen zugewiesen, sodass sie genau die richtigen Berechtigungen für die richtigen Ressourcen erhalten – nicht mehr und nicht weniger. Benutzer sind zufrieden, weil sie Zugriff auf die für ihre Arbeit erforderlichen Ressourcen haben; Administratoren sind zufrieden, weil alles automatisiert ist und der Zeitaufwand für unliebsame, klicklastige Aufgaben minimiert wird.

Mit Active Roles erhalten Sie ein gebrauchsfertiges Tool für die Verwaltung von Benutzer- und Gruppenkonten, strikt durchgesetzte rollenbasierte Sicherheit und die tagtägliche Identitätsverwaltung, das integrierte Prüfungs- und Berichterstellungsfunktionen für Windows-zentrierte Umgebungen bietet.

Die Vorteile von Active Roles umfassen:

- **Sicherer Zugriff**: Active Roles agiert als virtuelle Firewall um das Active Directory und ermöglicht Ihnen die Zugriffssteuerung durch Delegierung nach dem Least-Privilege-Prinzip. Die Lösung erstellt und erzwingt Zugriffsregeln auf Basis definierter Verwaltungsrichtlinien und entsprechender Berechtigungen und eliminiert die Fehler und Inkonsistenzen, die bei Verwendung der nativen Verwaltungsfunktionen von AD so häufig auftreten. Mit zuverlässigen und personalisierten Genehmigungsverfahren wird sichergestellt, dass die IT- und Überwachungsprozesse den Geschäftsanforderungen entsprechen. Diese Prozesse beinhalten auch Zuständigkeitsketten, die die automatisierte Verwaltung von Verzeichnisdaten ergänzen.
- **Automatisierte Kontoerstellung:** Die Lösung automatisiert zahlreiche Aufgaben, so unter anderem:
- Erstellung von Benutzer- und Gruppenkonten in AD/AAD

- Erstellung von Postfächern in Exchange/Exchange Online
- Füllen von Gruppen
- Zuweisung von Ressourcen unter Windows

Außerdem automatisiert Active Roles die Neuzuteilung und Aufhebung von Benutzerzugriffsrechten in AD/AAD und mit AD verbundenen Systemen, einschließlich der Löschung von Benutzern und Gruppen, und gewährleistet effiziente und sichere administrative Abläufe für Benutzer und Gruppen während ihrer gesamten Lebensdauer. Wenn die Zugriffsrechte eines Benutzers geändert oder zurückgenommen werden müssen, werden die nötigen Aktualisierungen automatisch in AD, Exchange, SharePoint, OCS, Lync, Windows und allen anderen mit dem AD verbundenen Systemen vorgenommen, beispielsweise in UNIX, Linux und Mac OS X.

- **Tagtägliche Verzeichnisverwaltung:** Sie können Folgendes problemlos verwalten:
- Exchange/Exchange Online Empfänger, inklusive Postfachzuweisung und OCS Zuweisung sowie Erstellung, Verschiebung, Löschung, Berechtigungen und Verteilerlistenverwaltung
- Gruppen
- Computern, einschließlich Freigaben, Druckern sowie lokalen Benutzern und Gruppen
- Active Directory, einschließlich AD LDS
- Active Roles bringt auch intuitive Oberflächen zur Vereinfachung alltäglicher Administrations- und Helpdesk-Aufgaben mit – zur Wahl stehen ein MMC Snap-in und eine Weboberfläche
- **Verwaltung von Gruppen und Benutzern in einer gehosteten Umgebung:** Active Roles arbeitet in einer gehosteten Umgebung, in der Konten einer AD-Client-Domäne mit einer AD-Host-Domäne synchronisiert werden. Active Roles ermöglicht die Verwaltung von Benutzer- und Gruppenkonten in Client- und Host-Domänen bei gleichzeitiger Synchronisierung von Attributen und Kennwörtern. Sie können gebrauchsfertige Connectors nutzen, um Ihre lokalen AD-Konten mit anderen Plattformen und Anwendungen zu synchronisieren. Mit One Identity Starling Connect steht eine schnell wachsende Palette aus mehr als 30 Connectors (https://www.cloud.oneidentity.com/products/connect/connectors) für verschiedene Cloud-basierte Services und Anwendungen zur Verfügung, darunter Salesforce, G-Suite und ServiceNow.
- **Konsolidierung von Verwaltungspunkten mittels Integration:** Active Roles ergänzt Ihre vorhandene Technologie und bestehende IAM-Strategie. Die Lösung ergänzt alle Funktionen und vereinfacht und konsolidiert Verwaltungspunkte, indem sie eine unkomplizierte Integration mit vielen One Identity Produkten gewährleistet, beispielsweise Identity Manager, Privilege Password Manager, Desktop Virtualization, Authentication Services, Defender, Password Manager und Quest Change Auditor. Active Roles automatisiert und ergänzt außerdem die Funktionen von PowerShell, ADSI, SPML und anpassbaren Webschnittstellen.

10 Schritte für starke Leistung, Agilität und Sicherheit

Schritt 1: Konten regelmäßig analysieren

Schritt 2: Konten mit Personalakten verbinden

Schritt 3: Neue Konten überwachen

Schritt 4: Kontowartung automatisieren

Schritt 5: Umgang mit ausgeschiedenen Benutzern und Rollenänderungen

Schritt 6: Inaktive Konten angehen

Schritt 7: Nicht für Personen erstellte Konten verwalten

Schritt 8: Ausnahmen verwalten

Schritt 9: Administratorbefugnisse verwalten

Schritt 10: Workflow-Technologie nutzen

Mit diesen 10 Schritten können Sie Ihre AD/Azure AD-Daten bereinigen, was für hohe Leistung und Sicherheit unerlässlich ist. One Identity Active Roles hilft Ihnen bei der Umsetzung dieser Schritte und Wahrung eines einwandfreien Datenzustands für die Zukunft. Nehmen Sie also Ihre Grundlage, werten Sie sie mit bereinigten Daten auf und profitieren Sie von der Leistung, Geschwindigkeit und den Möglichkeiten, die Active Roles für Ihre AD/AAD-Strategie bietet.

Microsoft Active Directory und One Identity Active Roles: zusammen einfach besser

Über One Identity

One Identity von Quest ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Dank unseres einzigartig breit gefächerten und integrierten Portfolios mit Angeboten zum Identitätsmanagement, einschließlich Kontoverwaltung, Identity Governance und Administration sowie Verwaltung des privilegierten Zugriffs, sind Unternehmen in der Lage, ihr volles Potenzial auszuschöpfen und Sicherheit dadurch zu erreichen, dass Identitäten in den Mittelpunkt des Programms gestellt werden und der ordnungsgemäße Zugriff für alle Benutzertypen, Systeme und Daten ermöglicht wird. Weitere Informationen finden Sie unter OneIdentity.com.

Whitepaper_2021_MicrosoftBetterTogetherwithOIDActiveRoles_PG-DE-WL-67415