DATENBLATT

Active Roles

Verwaltung und Schutz für hybrides Active Directory und darüber hinaus

Vorteile

- Schutz geschäftskritischer Active Directory und Azure Active Directory Daten
- Regulierung von Verwaltungszugriff über Least-Privilege-Modell
- Überwindung der Einschränkungen nativer Tools
- Automatisierte Erstellung und Löschung von Benutzer-/Gruppenkonten
- Verwaltung von Konten für Exchange Online, Lync, SharePoint Online, Office 365 und viele weitere Lösungen
- Bereitstellung eines einzigen, intuitiven Tools für Hybridumgebungen
- Erstellung von auditfähigen Berichten
- Rasche Bereitstellung für eine schnelle Amortisation
- Identifizierung der Urheber von Änderungen und des Änderungszeitpunkts
- Modulare Architektur für die Erfüllung heutiger und zukünftiger Geschäftsanforderungen
- Auf viele nicht von Windows stammende und SaaS-Systeme erweiterte AD-zentrische Identitätsverwaltung

Überblick

Die Herausforderungen bei der Kontoverwaltung in Active Directory (AD) und Azure AD sind zahlreich und vielfältig. Zudem ist der Schutz dieser wichtigen Systeme oft mit großen Schwierigkeiten verbunden. Mit nativen Tools sind die Verwaltung und der Schutz eines hybriden AD ineffizient, unzusammenhängend und anfällig für Fehler.

Bei dem rasenden Tempo heutiger Unternehmen können Organisationen nur schwer mit den Anfragen Schritt halten, Zugriff auf die hybride AD-Umgebung zu erstellen, zu ändern oder zu entfernen. Dazu sind sie mit Sicherheitsproblemen konfrontiert wie beispielsweise ehemaligen Mitarbeitern, die weiterhin Zugriff auf kostbares geistiges Eigentum haben. Das ist vor allem in Bezug auf die Erfüllung der Geschäftsanforderungen sowie der Anforderung von Berichten durch Prüfer heikel. Hinzu kommt noch die Notwendigkeit, den administrativen Zugriff auf Active Directory und Azure Active Directory streng zu kontrollieren und bei der explosionsartig steigenden Anzahl von nicht von Windows stammenden und SaaS-Anwendungen, die ebenfalls verwaltet werden müssen, auf dem Laufenden zu bleiben.

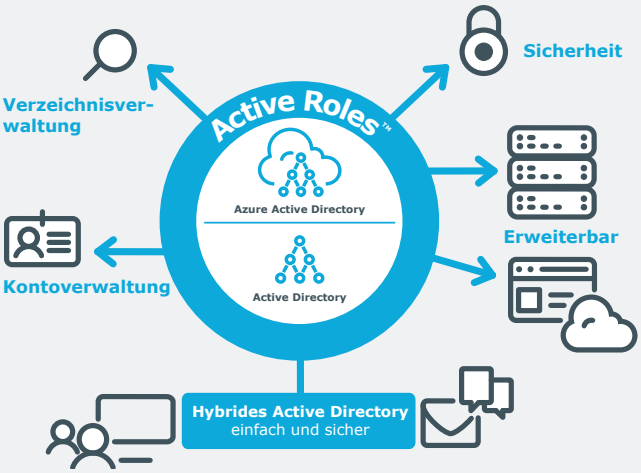
Glücklicherweise gibt es jetzt eine Lösung für dieses Problem. Mit One Identity Active Roles können Sie diese mühsamen und für Fehler anfälligen Verwaltungsaufgaben automatisieren und Ihre Sicherheitsprobleme lösen. Active Roles automatisiert und vereinheitlicht die Verwaltung von Konten und Gruppen, während es den sehr wichtigen administrativen Zugriff sichert und schützt.

Active Roles liefert automatisierte Tools für die Verwaltung von Benutzer- und Gruppenkonten, um die Unzulänglichkeiten der nativen Tools bei Active Directory und Azure Active Directory zu beseitigen. So erhalten Sie die Möglichkeit, Ihre Aufgaben effizienter, genauer und mit weniger manuellem Eingreifen zu erledigen. Die Lösung basiert auf einer modularen Architektur, die Ihrer Organisation eine einfache Möglichkeit an die Hand gibt, allen Geschäftsanforderungen zuverlässig gerecht zu werden – jetzt und in Zukunft.

Funktionen und Merkmale

Für hybride AD Umgebungen geeignet

Active Roles ist für die Erfüllung der Anforderungen des lokalen AD sowie von Azure AD in einer Hybridbereitstellung optimiert. Die Lösung bietet eine zentrale Konsole, vereinheitlichte Workflows sowie konsistente Administrationsfunktionen für Ihre ganze Hybridumgebung. Mit ihr entfallen die mit der Verwendung separater Tools und manueller Prozesse verbundene Mühseligkeit, Fehleranfälligkeit und Beschränkung.



Sicherer Zugriff

Active Roles bietet umfassende Funktionen für die Verwaltung privilegierten Konten in Active Directory und Azure Active Directory, sodass Sie den Zugriff durch Delegierung auf Basis des Least-Privilege-Prinzips (Prinzip der minimalen Rechte) kontrollieren können. Die Lösung erstellt und erzwingt Zugriffsregeln auf Basis definierter Verwaltungsrichtlinien und entsprechender Berechtigungen und eliminiert so die Fehler und Inkonsistenzen, die bei Verwendung der nativen Funktionen für die Verwaltung hybrider AD Bereitstellungen so häufig auftreten. Robuste und personalisierte Genehmigungsverfahren gewährleisten, dass IT-Betrieb und IT-Überwachung gemäß den Geschäftsanforderungen ablaufen. Zuständigkeitsketten ergänzen die automatisierte Verwaltung der Verzeichnisdaten.

Automatisierte Kontoverwaltung

Active Roles automatisiert eine Reihe von Aufgaben, unter anderem:

- Erstellung von Benutzer- und Gruppenkonten in AD und AAD
- Einfache Erweiterung administrativer Vorgänge an nicht von Windows stammenden Systemen und SaaS-Anwendungen bei AD-/AAD-basierten Konten
- Erstellung von Postfächern in Exchange und Exchange Online
- Auffüllung von Gruppen in AD und AAD
- Zuweisung von Ressourcen unter Windows

Die Lösung automatisiert außerdem die Neuzuteilung und Aufhebung von Benutzerzugriffsrechten in AD, AAD und mit AD verbundenen Systemen, einschließlich der Deprovisionierung von Benutzern und Gruppen, und gewährleistet effiziente und sichere administrative Abläufe für Benutzer und Gruppen während des gesamten Lebenszyklus. Wenn die Zugriffsrechte eines Benutzers geändert oder zurückgenommen werden müssen, werden die nötigen Aktualisierungen automatisch für alle relevanten Systeme und Anwendungen in der hybriden AD-/AAD-Umgebung und allen anderen mit dem AD verbundenen Systemen vorgenommen, beispielsweise UNIX, Linux und Mac OS X Systeme sowie eine umfangreiche und wachsende Sammlung vieler beliebter SaaS-Anwendungen über die Lösung One Identity Starling Connect.

Alltägliche Verzeichnisverwaltung

Active Roles ermöglicht die problemlose Verwaltung von Folgendem in lokalen sowie Azure AD Umgebungen:

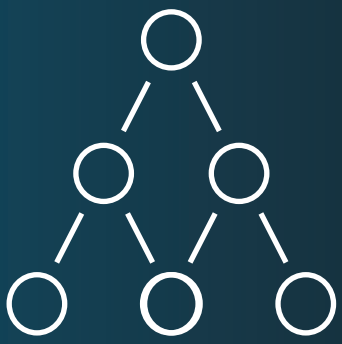
- Exchange Empfängern, inklusive Postfachzuweisung und OCS Zuweisung sowie Erstellung, Verschiebung, Löschung, Berechtigungen und Verteilerlistenverwaltung
- Gruppen
- Computern, einschließlich Freigaben, Druckern sowie lokalen Benutzern und Gruppen
- Active Directory und Azure Active Directory

Active Roles bringt intuitive Oberflächen zur Optimierung alltäglicher Administrations- und Helpdesk-Aufgaben in der hybriden AD-/AAD-Umgebung mit – zur Wahl stehen ein MMC Snap-in und eine Weboberfläche.

Außerdem unterstützt Active Roles die beliebtesten und relevantesten Personalisierungsoptionen wie beispielsweise PowerShell, um maximale Flexibilität sowie die Möglichkeit zu liefern, Active Roles so zu nutzen, dass für Ihr Unternehmen größtmöglicher Nutzen entsteht.

Erweiterung des Verwaltungsumfangs

Active Roles unterstützt den SCIM-Standard, der es ermöglicht, dass jede SCIM-fähige SaaS-Anwendung (über One Identity Starling Connect) in die AD-basierten Funktionen zur Konto- und Gruppenverwaltung von Active Roles eingebunden werden kann.



Wenn der Zugriff eines Benutzers geändert oder entfernt werden muss, werden automatisch Aktualisierungen bei AD, AAD, Exchange Online, SharePoint Online, OCS, Skype for Business und Windows sowie allen an AD angebundenen Systemen wie Unix, Linux, Mac OS X und SaaS-Anwendungen vorgenommen.

Verwaltung von Gruppen und Benutzern in einer gehosteten Umgebung

Mit unserer Lösung können Sie in gehosteten Umgebungen AD Domänen-Clients mit einer AD Hostdomäne synchronisieren. So ermöglicht Active Roles eine einheitliche Verwaltung von Benutzer- und Gruppenkonten in Client- und Host-Domänen bei gleichzeitiger Synchronisierung von Attributen und Kennwörtern. Zusätzlich können Sie über sofort einsatzbereite Connectors lokale AD-Konten mit Microsoft Office 365, Lync Online/Skype for Business und SharePoint Online synchronisieren.

Konsolidierung von Verwaltungspunkten mittels Integration

Active Roles ergänzt Ihre vorhandene Technologieinfrastruktur und Ihre Strategie für Identitäts- und Zugriffsverwaltung nahtlos. Die Lösung vereinfacht und konsolidiert Verwaltungspunkte, indem sie eine unkomplizierte Integration mit vielen One Identity Produkten gewährleistet, so beispielsweise Identity Manager, Safeguard, Authentication Services, Password Manager und Change Auditor. Active Roles automatisiert und erweitert außerdem die Funktionen von PowerShell, ADSI, SPML und anpassbaren Webschnittstellen.

Dabei bringt Active Roles sämtliche Synchronisierungstechnologien mit, die Sie für die Verwaltung und Sicherung von Folgendem benötigen:

- Lync/Skype for Business
- Exchange
- One Drive
- SharePoint
- AD LDS
- Office 365 (einschließlich Rollen und Gruppen)
- Azure AD
- Microsoft SQL Server
- OLE DB (MS Access)
- Flatfiles

Über One Identity

One Identity ist ein Quest-Software-Unternehmen, das Organisationen dabei hilft, eine identitätsorientierte Sicherheitsstrategie zu entwickeln. Mit einem einzigartig breiten Portfolio von Angeboten für Identitäts- und Zugriffsverwaltung einschließlich Identitätsgovernance, Verwaltung privilegierten Zugriffs und Kontoverwaltung, die alle um eine hybride Cloud-Bereitstellungsstrategie erweitert sind, hilft One Identity Organisationen, durch Sicherheitsvorkehrungen ungehindert und doch gegen Bedrohungen geschützt ihr volles Potential auszuschöpfen. Dieses Engagement für den langfristigen Erfolg der Kunden ist nur bei One Identity zu finden. Über 7.500 Organisationen auf der ganzen Welt verlassen sich bei der Verwaltung von über 125 Millionen Identitäten auf Lösungen von One Identity, wodurch sie mehr Flexibilität erhalten und ihre Effizienz erhöhen und gleichzeitig den Zugriff auf ihre Systeme und Daten sichern – lokal, in der Cloud oder hybrid. Weitere Informationen finden Sie auf www.oneidentity.com.

Datasheet_2019_ActiveRoles74_US_RS_42104