DATENBLATT

Active Roles On Demand

SaaS-Bereitstellungen zur Verringerung des Risikos bei der Verwaltung und Sicherung von Active Directory und Azure AD

Vorteile

- Umfassendes IAM- und AD-Kontolebenszyklusmanagement mit On-Demand-Bereitstellung
- Verwaltung von Berechtigungen und Schutz kritischer AD- und Azure AD-Daten
- Konfiguration von Zero Trust-Sicherheit
- Regulierung des privilegierten Zugriffs über Least-Privilege-Modelle
- Vereinfachte Verwaltung komplexer Umgebungen mit einem einfachen, intuitiven Tool
- Überwindung von Einschränkungen nativer AD-Tools
- Automatisierte Erstellung und Löschung von Benutzer-/Gruppenkonten
- Verwaltung von Konten für Exchange Online, Lync, SharePoint Online, Office 365 und viele weitere Lösungen
- Identifizierung des Urhebers und Zeitpunkts von Änderungen
- Erweiterung der modularen Architektur und der Identitätsverwaltung und -Governance

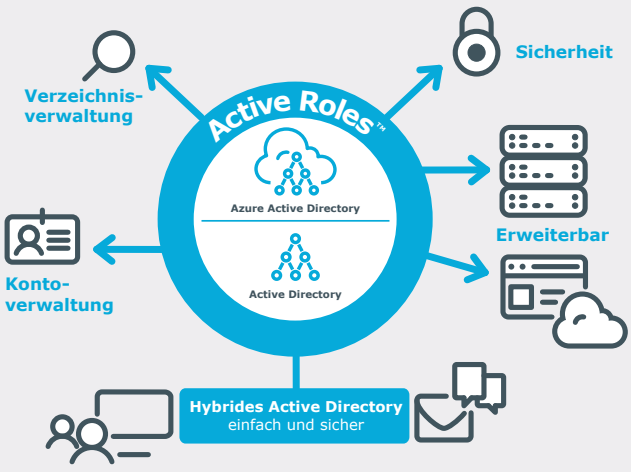
Cloud ohne Kompromisse

Bei der Verwaltung und Absicherung von Konten in Active Directory (AD) und Azure AD gibt es diverse Herausforderungen zu meistern, darunter das Risiko von Sicherheitsverletzungen, Ineffizienzen bei der Bereitstellung und Complianceprobleme. AD und Azure AD sind zuverlässige, leistungsstarke Tools, die von 95 Prozent der Fortune 1000-Unternehmen genutzt werden. Allerdings sind native AD-Tools ineffizient und nicht auf die Unterstützung von modernen, hybriden Umgebungen ausgelegt. Werden für hybride ADs nur native AD-Tools eingesetzt, wird deren Verwaltung und Schutz unwirksam, unzusammenhängend und fehleranfällig. Glücklicherweise gibt es Abhilfe. Active Roles On Demand ist die SaaS-Lösung, mit der solche Herausforderungen gemeistert werden können. Sie ergänzt die Fähigkeiten von nativen AD-Tools und verbessert die Effizienz, Automatisierung, Sicherheit und Compliance ihrer Umgebungen erheblich. Sämtliche Merkmale und Funktionen von Active Roles On Demand sind in der SaaS-Bereitstellung – der Cloud ohne Kompromisse – verfügbar.

Herausforderungen

Die schnell voranschreitende digitale Transformation und das rasante Tempo heutiger Geschäftsentwicklungen erschweren es Unternehmen, mit den Anfragen Schritt zu halten, Zugriffe auf die hybride AD-Umgebung zu erstellen, zu ändern oder zu entfernen. Darüber hinaus haben sie mit Sicherheitsproblemen zu kämpfen, wie ehemaligen Mitarbeitern, die immer noch Zugriff auf wertvolles geistiges Eigentum haben, mit anspruchsvollen Geschäftsanforderungen sowie der Pflicht, Prüfern Berichte zur Verfügung zu stellen. Dazu kommt die Notwendigkeit, den administrativen Zugriff auf Active Directory und Azure Active Directory streng zu kontrollieren und den Überblick zu behalten bei der explosionsartig steigenden Anzahl von nicht von Windows stammenden SaaS-Anwendungen, die ebenfalls verwaltet werden müssen.

Wenn der Zugriff eines Benutzers geändert wird, werden Aktualisierungen nicht nur automatisch in AD, AAD, Exchange Online, SharePoint Online, OCS, Teams und Windows vorgenommen, sondern auch in Systemen, die in AD eingebunden sind.



Funktionen und Merkmale

Sicherer Zugriff

Active Roles On Demand ermöglicht eine umfassende Verwaltung von privilegierten Konten für Active Directory und Azure Active Directory, sodass Sie den Zugriff mittels Delegierung nach dem Least-Privilege-Prinzip kontrollieren können. Die Lösung erstellt und erzwingt Zugriffsregeln auf Basis definierter Verwaltungsrichtlinien und entsprechender Berechtigungen und eliminiert so die Fehler und Inkonsistenzen, die bei einem nativen Ansatz für die Verwaltung der hybriden AD so häufig auftreten.

Mit moderner Authentifizierung über OAUTH verfügt Active Roles On Demand über robuste, personalisierte Genehmigungsverfahren. Diese richten einen IT- und Überwachungsprozess ein, die mit den Geschäftsanforderungen übereinstimmen und Verantwortungsketten beinhalten, welche die automatisierte Verwaltung von Verzeichnisdaten ergänzen.

Für hybride AD-Umgebungen geeignet

Active Roles On Demand ist auf die Anforderungen von lokalen ADs sowie von Azure ADs in hybriden oder reinen Azure-Umgebungen ausgelegt. Die Lösung bietet eine einzelne Konsole, einheitliche Workflows sowie eine konsistente Verwaltung in Ihrer gesamten hybriden Umgebung. Da Active Roles On Demand mehrere Instanzen unterstützt, kann auf die Verwendung von separaten Tools und manuellen Prozessen verzichtet werden, die mühselig, fehleranfällig und hinderlich sind.

Automatisierte Kontoverwaltung

Active Roles On Demand automatisiert unter anderem folgende Aufgaben:

- Änderungen, die an in AD eingebundenen Systemen vorgenommen werden, zum Beispiel UNIX/Linux und Mac OSx
- Erstellung von Benutzer- und Gruppenkonten in AD und AAD
- Erweiterung administrativer Vorgänge bei AD/AAD-basierten Konten auf nicht von Windows stammende Systeme und SaaS-Anwendungen
- Erstellung von Postfächern in Exchange und Exchange Online
- Auffüllung von Gruppen in AD und AAD
- Zuweisung von Ressourcen in Windows

Nach ISO 27001 zertifiziert

One Identity ist ein Unternehmen von Quest und ein führender globaler Anbieter von identitätsbasierten Sicherheitslösungen. Seine Cloud-Infrastruktur und -Prozesse sind gemäß der internationalen Norm ISO/IEC 27001 zertifiziert, die Best Practices für Systeme zum Informationssicherheitsmanagement vorgibt.

Tagtägliche Verzeichnisverwaltung

Mit Active Roles On Demand können Sie die folgenden Ressourcen in lokalen Umgebungen und Azure AD-Umgebungen problemlos verwalten:

- Exchange 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 und Azure Active Directory

Active Roles On Demand unterstützt zudem die beliebtesten und relevantesten Personalisierungsoptionen wie PowerShell, um eine maximale Flexibilität und die Möglichkeit zu bieten, Active Roles On Demand auf eine Art und Weise zu verwenden, die Ihrem Unternehmen den größten Nutzen bringt.

Erweiterung des Verwaltungsumfangs

Active Roles On Demand unterstützt den SCIM-Standard, der die Einbindung (über One Identity Starling Connect) jeder SCIM-fähigen SaaS-Anwendung in die AD-basierten Funktionen zur Konto- und Gruppenverwaltung von Active Roles On Demand erlaubt.

Verwaltung von Gruppen und Benutzern in einer gehosteten Umgebung

Synchronisieren Sie AD-Domänen-Clients in gehosteten Umgebungen mit einer AD-Hostdomäne. Active Roles On Demand ermöglicht Benutzer- und Gruppenkonten.

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_ActiveRolesSaaS_US_PG-DE-WL-65340