Pięć najlepszych sposobów radzenia sobie z zarządzaniem hybrydowym w środowisku AD i AAD

ACTIVE ROLES

One Identity

ONE IDENTITY™

greeneris
creating innovation

Spis treści

ONE IDENTITY

greeneris
creating innovation

AAD nie jest kopią lokalnej instancji AD.

Active Directory jest wszędzie, a jego kuzyn Azure Active Directory (AAD), oparty na chmurze, szybko zyskuje na popularności. Obecnie prawie 90% organizacji na całym świecie korzysta z usługi Active Directory (AD) dla zasobów lokalnych (tzw. on-prem). Odpowiada to 500 milionom organizacji i około 10 miliardom codziennych uwierzytelnień. W rzeczywistości w świecie zarządzania tożsamością i dostępem (IAM) AD stało się nieuniknione i absolutnie niezbędne do lokalnego uwierzytelniania i autoryzacji użytkowników. Każdy musi przejść przez AD, po prostu tak się to robi. Dokładając połączenia z Azure AD – złożoność zarządzania po prostu gwałtownie wzrosła – może to powodować wiele wyzwań, jeśli środowiska tożsamości lokalnej i w chmurze nie są prawidłowo zarządzane i synchronizowane. Obecnie jest ponad 10 milionów subskrybentów AAD reprezentujących około 700 milionów kont i około 13 miliardów logowań dziennie. Większość tych operacji dotyczy dostępu do niezwykle popularnych aplikacji biurowych dostępnych za pośrednictwem platformy chmurowej Microsoft, takich jak Office 365, Exchange Online, SharePoint itp. Jednak zaufanie do platformy Azure rośnie dla tradycyjnych działań IAM, takich jak uwierzytelnianie wieloskładnikowe (MFA), federacja i logowanie jednokrotne oraz zarządzanie hasłami. Należy zauważyć, że większość z tych rozszerzonych możliwości jest dostępna tylko za pośrednictwem usługi Azure Active Directory Premium, która jest znacznie droższa niż funkcja AAD niezbędna do korzystania z usługi Office 365.

We wszystkich, z wyjątkiem najrzadszych przypadków, organizacje, które stosują AAD skoncentrowane na chmurze, robią to, nadal mocno zakorzenione w lokalnym świecie AD. Stanowi to ogromny i nieoczekiwany problem — usługa AAD nie jest po prostu opartą na chmurze kopią lokalnej usługi AD. Jest to całkowicie odrębne środowisko. Innymi słowy, w organizacjach, w których lokalna AD i Azure AD współistnieją i są równie ważne dla sukcesu, organizacja – oraz zespół IT – musi zarządzać dwuczęściowym, hybrydowym środowiskiem AD.

Migracja do chmury jest obarczona złożonością, ryzykiem, niewydolnością i pułapkami. Jeśli nie zostanie odpowiednio wdrożona i zarządzana, może powodować wielkie problemy dla Administratorów AD i użytkowników. Ta ulotka dotyczy pięciu potencjalnie uciążliwych wyzwań, które większość organizacji musi pokonać, próbując przebrnąć przez potencjalnie burzliwe przejście na hybrydową implementacje AD.

greeneris creating innovation

ONE IDENTITY

Wyzwanie #1: Dwa narzędzia to za dużo

Nie jest tajemnicą, że natywne narzędzia AD, które mają pomagać w zarządzaniu tożsamościami i dostępem, mają co najwyżej ograniczone możliwości. Mimo poważnych wysiłków na rzecz ulepszenia natywnego narzędzia Active Directory Users and Computers (ADUC) większość organizacji decyduje się na zastosowanie narzędzia innych firm w celu usprawnienia, automatyzacji i zapewnienia spójności zadań związanych z zarządzaniem usługami AD. Sytuacja tylko się pogarsza, gdy organizacje wdrażają Azure Active Directory (AAD). AAD nie używa ADUC i wymaga własnego narzędzia do podstawowych zadań administracyjnych.

Wykonanie tej samej czynności, takiej jak dodanie użytkownika, w AD i AAD wymaga użycia oddzielnych narzędzi z całkowicie niepowiązanymi interfejsami, odmienną funkcjonalnością i rozbieżnymi metodologiami szkolenia. W związku z tym i tak uciążliwe zadanie dla lokalnej usługi AD musi zostać wykonane również dla usługi AAD. Ponownie, AAD nie jest wersją AD w chmurze. Tak więc domowe skrypty, automatyzacja PowerShell i manualne procesy nie mogą być łatwo zastosowane do AAD.

Rozwiązanie 1: Jedno narzędzie do wszystkiego

Idealnym rozwiązaniem problemu dwóch narzędzi byłoby jedno narzędzie, które przezwycięży wady administracji ADUC i AAD. To narzędzie istnieje w rozwiązaniu One Identity - Active Roles. Active Roles zapewniają warstwę automatyzacji, spójności i prostoty użycia, dzięki czemu każde zadanie administracyjne dla usług AD i AAD jest szybkie, łatwe i dokładne. Tysiące organizacji codziennie polega na Active Roles, aby zapewnić wydajność i bezpieczeństwo administrowania swoimi lokalnymi wymaganiami AD, a dodatkowo teraz organizacje te mogą stosować tą samą metodologię do AAD.

Active Roles jest zoptymalizowane zarówno dla AD, jak i AAD, dzięki czemu zapewniają wykonywanie zadań za jednym zamachem, które rozwiązuje problemy hybrydowego zarządzania środowiskiem AD. Administratorzy zgłaszają znaczne oszczędności czasu (często ponad 80%) dzięki wykorzystaniu Active Roles. Zgłaszają również dramatyczny wzrost bezpieczeństwa (tj. mniej okazji dla błędów użytkowników). Active Roles udostępnia szablony procesów roboczych, które zapewniają, że zadania administracyjne w hybrydowym środowisku AD są wykonywane poprawnie za każdym razem.

Natywne narzędzia AD, które mają pomagać w zarządzaniu tożsamościami i dostępem, mają ograniczone możliwości.

greeneris creating innovation

ONE IDENTITY

Niespójne procesy — zwykle nazywane procesami roboczymi w świecie IAM — są często przyczyną błędów synchronizacji lub prowizorycznej aprowizacji.

greeneris

Wyzwanie #2: Niespójność

Zmuszone do polegania na manualnych procesach, nadmiernie obciążone organizacje IT zmagające się z zarządzaniem zawiłościami hybrydowego środowiska AD często robią wszystko, co w ich mocy a przez to popadają w złe nawyki typu „po prostu załatwić sprawę" - bez namysłu jak to powinno być zrobione poprawnie. To zrozumiałe: mamy niecierpliwych użytkowników domagających się natychmiastowych rezultatów; narzędzia, które utrudniają wykonywanie zadań w sposób spójny w jednym środowisku, a tym bardziej w dwóch; oddzielne i niepowiązane natywne narzędzia o ograniczonych możliwościach; i zbytnie poleganie na wiedzy plemiennej czyli „zawsze tak się to robiło".

Te niespójne procesy — zwykle nazywane procesami roboczymi (workflows) w świecie IAM — są często przyczyną błędów synchronizacji lub prowizorycznej aprowizacji użytkowników. Typowe obszary niespójności w hybrydowym środowisku AD obejmują:

- Dostosowanie przynależności do grupy z rolą zarówno w AD jak i AAD
- Uzyskiwanie odpowiednich zgód biznesowych na działania związane z uprawnieniami do zasobów
- Przypisywanie odpowiednich uprawnień poszczególnym administratorom (model jak najmniejszych uprawnień)
- Projektowanie łatwo powtarzalnych procesów dla poszczególnych zadań

Ponieważ usługa AAD nie jest po prostu kopią usługi AD w chmurze, spójność nie oznacza wycinania i wklejania lokalnych procesów pracy usługi AD do chmury (takiego jak proces roboczy skryptu PowerShell). Oznacza to jednak, że procesy robocze muszą odpowiadać unikalnym potrzebom zarówno AD jak i AAD.

Rozwiązanie 2: Szablony

Active Roles obejmuje wstępnie zdefiniowane szablony procesów roboczych (ang. workflow templates) dla AD i AAD (indywidualnie i dla środowisk hybrydowych), które są oparte na doświadczeniu i innowacjach tysięcy organizacji, które korzystają z Active Roles do usprawnienia automatyzacji i aby zabezpieczyć administrowanie ich hybrydowymi środowiskami AD.

Szablony te obejmują wszystko, od działań aprowizacji w katalogach, uzyskiwania zatwierdzenia od odpowiednich menedżerów linii biznesowej (LOB), dodawania do grup, przypisywania członkostwa DL (lista dystrybucyjna) w programie Exchange/Exchange Online i praktycznie każdego możliwego scenariusza. W rzeczywistości, Active Roles obejmują gotowe szablony dostępu do pakietu Office 365 i Exchange Online.

Ponadto, Active Roles zawiera konfigurowalne szablony i procesy robocze, aby sprostać unikalnym potrzebom każdej organizacji. Podczas gdy wiele organizacji może rozpocząć ścieżkę automatyzacji od skryptów, większość z nich dowiaduje się, że łatwość użycia i intuicyjność Active Roles sprawia, że jest to preferowane narzędzie w ich strategii zarządzania usługami AD. Jego zasięg — w tym hybrydowe środowisko AD — i ukierunkowanie na pomoc organizacjom w przezwyciężaniu najtrudniejszych wyzwań związanych z AD/AAD sprawia, że Active Roles jest wiodącą w branży platformą automatyzacji.

greeneris creating innovation

ONE IDENTITY

Narzędzia natywne nie radzą sobie z provisioningiem

Wyzwanie #3: Wszystko zaczyna się od provisioningu

Duża część obciążenia związanego z zarządzaniem AD/AAD wynika z aprowizacji użytkowników (ang. provisioning). Obejmuje to konfigurowanie kont w katalogu, umieszczanie osób w odpowiednich grupach i upewnianie się, że mają dostęp do właściwych kont i dostępu do wszystkich niezbędnych aplikacji – takich jak Exchange, Exchange Online, SharePoint, SharePoint Online, Office 365 – i niezliczonych innych aplikacji opartych na chmurze, które są dostępne za pośrednictwem AAD. Ale założenie kont to jedno, a ich wyłączenie (lub wyksięgowanie) to drugie i być może ważniejsze. W końcu ryzyko związane z zachowaniem dostępów przez pracownika, który został zwolniony, jest niezwykle wysokie – ale można go łatwo uniknąć przy użyciu odpowiednich narzędzi.

Jak wspomniano wcześniej, natywne narzędzia po prostu nie wystarczają, kiedy chodzi o provisioning. Konfiguracja dostępu lokalnego wymaga użycia ADUC dla AD, innego interfejsu i procesu dla Exchange, innego dla Skype dla firm, a lista jest długa.

To nawet nie uwzględnia dodatkowych narzędzi wymaganych do konfiguracji tego sama użytkownika w AAD i wszystkich powiązanych usługach w chmurze.

Istnieje wiele wyzwań związanych z udostępnianiem/ponownym udostępnianiem/wycofywaniem zasobów w hybrydowym środowisku AD, a mianowicie:

- Korzystanie z wielu narzędzi natywnych stwarza duże pole do popełnienia błędu ludzkiego i niespójności.
- Czas potrzebny na „pełne” udostępnienie użytkownikowi środowiska hybrydowego oznacza, że użytkownicy mogą doświadczać długich okresów bezczynności i braku produktywności w oczekiwaniu na przyznanie dostępów.
- Opóźnienia w wycofywaniu (lub ponownym udostępnianiu) zasobów wprowadzają ryzyko ponieważ niepożądany dostęp może zostać zachowany na długo po tym, kiedy powinien zostać wycofany.
- Wiarygodne źródło danych (zazwyczaj system HR) jest trudne do udostępnienia dla AD, nie wspominając o AAD, co skutkuje dużą ilością interwencji ludzkiej wymaganej do wykonania najbardziej podstawowych działań związanych z zaopatrzeniem/ponownym zaopatrzeniem/wycofaniem zasobów.
- Nie można polegać na synchronizacji między usługami AD i AAD, jeśli oryginalne dane AD są wadliwe – bezpośredni skutek błędów aprowizacji.

Najważniejsze jest to, że jeśli nie możesz prawidłowo zapewnić provisioningu, nie możesz mieć pewności co do bezpieczeństwa ani skuteczności swojego hybrydowego środowiska AD.

greeneris creating innovation

ONE IDENTITY

greeneris
creating innovation

ONE IDENTITY

Rozwiązanie 3: Provisioning zrobiony raz a dobrze

Jak więc zapewnić prawidłową aprowizację? Na początek kluczowe jest wyeliminowanie jak największej liczby błędów natury ludzkiej. Odbywa się to za pomocą jednego narzędzia, które zapewnia dokładną aprowizację (i wycofywanie aprowizacji) zarówno dla usług AD, jak i AAD. Active Roles jest właśnie takim narzędziem. Dzięki wykorzystaniu szablonów dla procesów roboczych i automatyzacji, Active Roles usprawnia proces aprowizacji hybrydowych usług AD do pojedynczego działania — w tym AD, AAD, Exchange, Exchange Online, SharePoint, SharePoint Online, Skype dla firm i tak dalej.

Ale to nie koniec. Active Roles czerpie również z wiarygodnych źródeł danych, takich jak system HR, w celu inicjowania i wykonywania kompleksowej aprowizacji i deaprowizacji w całym hybrydowym środowisku AD.
Kiedy coś dzieje się automatycznie i zgodnie z ustalonymi przez Ciebie zasadami, przypadki błędu spowodowanego czynnikiem ludzkim, niedopatrzenia lub pomyłki są praktycznie eliminowane.

Wyzwanie #4: Synchronizacja

Usługa Azure AD zawiera funkcję o nazwie Azure AD Connect, która synchronizuje użytkowników, grupy, atrybuty i hasła z lokalnej usługi AD z usługą AAD. Ta pojedyncza funkcja doprowadziła do powszechnego zaadoptowania usługi Office 365 — płynnej migracji użytkowników pakietu Office do wersji w chmurze, często bez świadomości użytkownika.
Umożliwia to użytkownikom logowanie jednokrotne, dzięki czemu szybko i bezproblemowo mogą uzyskać dostęp do zasobów lokalnych i w chmurze.

Oczywiście jeżeli chodzi o płynną migrację to o wiele łatwiej jest powiedzieć niż zrobić. Zazwyczaj zabezpieczenia dostępu w chmurze opierają się na uprawnieniach i członkostwie ustanowionym w lokalnym AD.
Tak więc wszelkie błędy, czynniki ryzyka lub luki w zabezpieczeniach, które istnieją w lokalnym AD – być może spowodowane ograniczeniami narzędzi natywnych – zostaną zreplikowane do środowiska Azure AD.

Podam przykład: Załóżmy, że masz grupę w AD o nazwie Finanse i Użytkownik X został dodany do grupy, ponieważ Użytkownik A był na urlopie i potrzebował pokrycia. Jednak gdy Użytkownik A wrócił z urlopu, Użytkownik X nigdy nie został usunięty z grupy. Może się to zdarzyć z wielu powodów, takich jak: personel administracyjny AD był zbyt zajęty – lub zapomniał – aby odebrać dostęp, gdy nie był już potrzebny; być może kierownik działu finansów nie zdawał sobie sprawy z ryzyka związanego z nadmierną aprowizacją; lub natywne narzędzia sprawiły, że było to zbyt trudne lub czasochłonne. Jakikolwiek nie byłby to powód, gdy AD jest zsynchronizowane z AAD, wówczas te same niepożądane prawa/dostępy skojarzone z tym użytkownikiem są teraz obecne również w AAD. Jeśli w usłudze SharePoint Online, OneDrive lub dowolnej z setek aplikacji, które potencjalnie można włączyć za pośrednictwem usługi AAD, dostępne są zasoby finansowe, to użytkownik ten ma uprawnienia (lub przynajmniej prawa) do dostępu do tych poufnych danych i manipulowanie nimi.

To duże ryzyko. Rozważ konsekwencje nieumyślnych błędów w lokalnej usłudze AD, które są replikowane do usługi AAD i wszystkich zasobów, z którymi usługa AAD łączy użytkowników.

Rozwiązanie 4: Automatyzacja

Rozwiązanie jest proste – jeśli w AD nie ma błędów, nie replikują się one do AAD. Jak więc zapewnić, że twoje środowisko AD jest schludne i dobrze zorganizowane?
Skoro źródłem większości błędów jest czynnik ludzki, to zminimalizowanie sposobności do ich występowania jest kluczem do czystego i bezpiecznego środowiska AD – a tym samym czystego i bezpiecznego AAD.

greeneris creating innovation
ONE IDENTITY

Active Roles zapewnia automatyzację i wbudowane procesy robocze niezbędne aby upewnić się, że użytkownicy otrzymują odpowiednie prawa i są umieszczani w odpowiednich grupach, wraz ze wszelkimi zgodami, śledzeniem aktywności czy kontrolą wymaganą do zmniejszenia ryzyka. Jeśli łatwo (lub automatycznie) można przyznać ludziom odpowiednie prawa, a następnie w razie potrzeby je cofnąć, to łatwo jest utrzymać AD w ładzie. Active Roles mogą nawet komunikować się z wiarygodnym źródłem danych (takim jak system HR), aby automatycznie inicjować działania na kontach AD i AAD. Tak więc w naszym przykładzie, gdy Użytkownik A wróciłby z urlopu, Active Roles automatycznie przywróciłyby te prawa i unieważniły prawa Użytkownika X.

Dzięki korzystaniu z Active Roles, jako kluczowych dla Twojej strategii zarządzania usługami AD, potencjalne błędy – i ich replikacja do AAD – jest znacznie ograniczona.

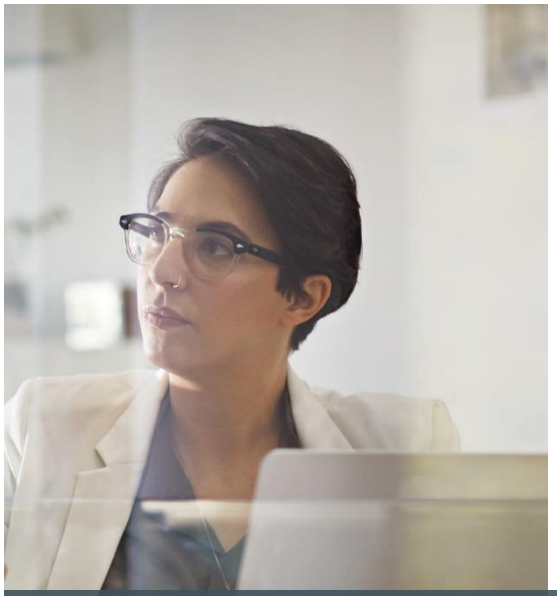
Wyzwanie #5:Kto daje ci prawa?

Rażącą luką w zabezpieczeniach natywnych narzędzi do zarządzania AD/AAD jest brak zarządzania kontami uprzywilejowanymi (PAM). Za pomocą tych narzędzi konto administratora jest wymagane do wykonania dowolnej czynności — takiej jak aprowizacja użytkownika, umieszczenie osób w grupach, zresetowanie hasła, instalowanie aktualizacji, tworzenie kopii zapasowych, wdrażanie nowego kontrolera domeny lub inne niezbędne czynności administracyjne. Problem polega na tym, że to konto jest powiązane z katalogiem, a nie z osobą. Oznacza to, że wiele osób dzieli dane uwierzytelniające i wszyscy używają tych samych danych logowania administratora. Dodatkowo ten jeden login ma dostęp do wszystkiego.

Nie ma więc znaczenia, czy akcja polega na zresetowaniu hasła użytkownika, czy na wdrożeniu nowego kontrolera domeny – każdy z tym loginem ma takie same prawa.
Ta sytuacja jest obarczona ryzykiem z powodu całkowitego braku jednostki odpowiedzialnej za konto administratora. Co więcej, lokalne konto administratora AD nie ma zastosowania do usługi AAD (i na odwrót), a uprawnienia nadal są typu „wszystko albo nic”, co naraża środowisko chmury na ryzyko.

Rozwiąźnie 5: Odpowiednie prawa

Właściwym sposobem nadawania praw administratora w hybrydowym środowisku AD jest przyznanie uprzywilejowanym użytkownikom uprawnień wystarczających do wykonywania ich pracy — nie większych, nie mniejszych. Jest to koncepcja nazywana dostępem z jak najmniejszymi uprawnieniami (least-privilege access).



Ta sytuacja jest obarczona ryzykiem ze względu na całkowity brak odpowiedzialności indywidualnej za konto administratora.

greeneris creating innovation

ONE IDENTITY

W myśl tej zasady Active Roles zapewniają dodatkową warstwę zabezpieczeń dla AD i AAD, dzięki której możesz zarządzać tym, co poszczególni administratorzy mogą robić, a czego nie mogą robić. Eliminuje to możliwość nieumyślnego lub złośliwego podejmowania działań wykraczających poza ich rolę i odpowiedzialność.

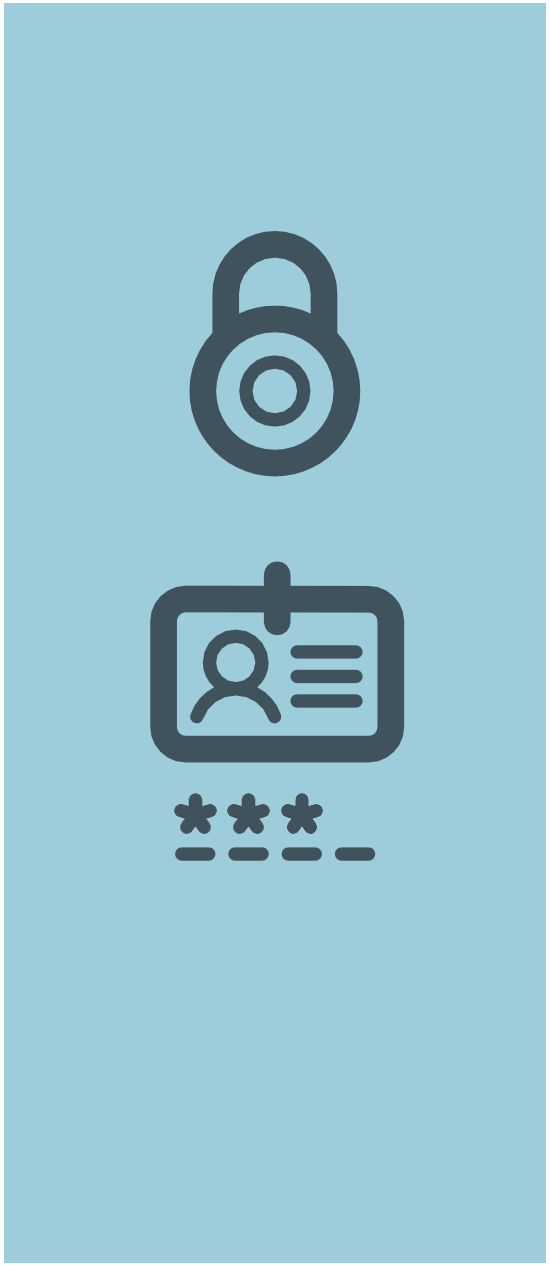
Dzięki Active Roles mamy jedno narzędzie, które umożliwia definiowanie ról administracyjnych w usługach AD, AAD, Office 365, Exchange i tak dalej.

Administrator, którego zadaniem jest resetowanie haseł, może resetować tylko hasła (może chcesz, aby obsługiwał zarówno środowiska AD, jak i AAD); administratorzy zajmujący się provisioningiem nie mogą uzyskać dostępu do dzienników ani manipulować nimi; a osoba instalująca oprogramowanie jest odizolowana od wykonywania codziennych zadań administracyjnych. Active Roles działa jako dodatkowa warstwa kontroli i bezpieczeństwa wokół hybrydowych środowisk AD.

Ale to nie wszystko… Możliwości AR nie kończą się na chmurze

Oprócz rozwiązania pięciu wspomnianych powyżej wyzwań, Active Roles zapewnia również:

- Audyt z historią zmian i raportowaniem aktywności użytkowników zarówno dla AD, jak i AAD
- Zarządzanie licencjami aplikacji w celu optymalizacji kontroli wydatków SaaS
- Integracja z wiodącymi narzędziami do zarządzania usługami AD do audytu, migracji, zarządzania zasadami grupy i kontroli zmian
- Rozbudowane możliwości tworzenia skryptów i ich dostosowywania
- Integracja z funkcjonalnością IAM obejmuje:
  - Aprowizację i zarządzanie przedsiębiorstwem
  - Mostkowanie domen AD
  - Przechowywanie haseł
  - Samoobsługa użytkownika i LOB (line of business)
  - Uwierzytelnianie wieloskładnikowe
  - Bezpieczny dostęp zdalny
  - Bezpieczeństwo adaptacyjne oparte na ryzyku



greeneris creating innovation

ONE IDENTITY

Podsumowanie

Wraz z szybkim rozwojem usługi Azure Active Directory zdecydowana większość organizacji będzie nadal korzystać z lokalnej usługi AD, jednocześnie coraz bardziej polegając na chmurze. To hybrydowe środowisko AD stwarza wyjątkowe wyzwania, które mogą być niezwykle problematyczne w zarządzaniu za pomocą natywnych narzędzi lub procesów ręcznych. Active Roles firmy One Identity to idealne rozwiązanie pozwalające uniknąć lub złagodzić uciążliwości związane z opisanymi powyżej wyzwaniami hybrydowymi, a także wyeliminować luki w zabezpieczeniach, zmniejszyć ryzyko, a przede wszystkim zapewnić spójność i wydajność w dowolnym hybrydowym środowisku AD.

greeneris

About One Identity

The One Identity family of identity and access management (IAM) solutions offers IAM for the real world, including business-centric, modular and integrated, and future-ready solutions for identity governance, access management and privileged management.

© 2016 Quest Software Inc. ALL RIGHTS RESERVED. This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

ONE IDENTITY

greeneris creating innovation