BALASYS

One Identity Active Roles

Hibrid Active Directory, egyszerűen és biztonságosan

ELŐNYÖK

- Megvédi az Active Directory és az Azure Active Directory kritikus adatait
- A legkisebb jogosultság elve alapján szabályozza az adminisztrátorok hozzáférését
- Automatizálja az egyéni és csoportos felhasználói fiókok létrehozását és megszüntetését
- Kezeli az Exchange Online, Lync, SharePoint Online, Office 365, és számos más szoftverhez tartozó identitásokat
- Kiküszöböli a natív eszközök hiányosságait
- Egyetlen, intuitív eszközt biztosít a hibrid környezethez
- Auditkész jelentéseket készít
- Megmutatja, hogy ki, mikor, mit változtatott
- Gyorsan üzembe helyezhető, így befektetése gyorsan megtérül

ÁTTEKINTÉS

A Microsoft® Active Directory® (AD) és Azure Active Directory (AAD) adminisztrátorok felelősek a kritikus adatok biztonságos kezeléséért, a törvényi és belső szabályzóknak való megfelelésért, valamint azért, hogy a felhasználók csak a számukra engedélyezett erőforrásokhoz férjenek hozzá.

Azonban a mai feszített tempójú üzletvitel mellett, az adminisztrátorok nem tudnak lépést tartani a hibrid AD környezethez való hozzáférési igényekkel – túl sok a kérés hozzáférések létrehozására, változtatására, és törlésére. Ennek következményeként az adminisztrátorok biztonsági problémákkal is szembesülnek. Ilyen például, amikor egy volt alkalmazott továbbra is hozzáfér kritikus adatokhoz. De sokszor előfordul az is, hogy hosszú napokat (és éjszakákat) kell üzleti igények kiszolgálásával vagy audit riportok készítésével tölteni. Mindehhez adjuk még hozzá azt az igényt, hogy az Active Directory és Azure Active Directory kezelést delegálni kell különböző adminisztratív csoportok között, és persze az üzleti vezetők igényét se felejtsük el, hiszen ők hagynak jóvá minden változtatást. Könnyen belátható, hogy a mai AD és AAD adminisztrátoroknak segítségre van szüksége!

Szerencsére a segítség megérkezett! A One Identity Active Roles segítségével Ön megoldhatja biztonsági problémáit, és eleget tehet soha véget nem érő törvényi kötelezettségeinek is, mindezt az Active Directory és az Azure Active Directory egyszerű és hatékony védelmével.

Az Active Roles automatizált eszközöket biztosít a felhasználói fiókok kezeléséhez, kiküszöbölve ezzel az Active Directory és az Azure Active Directory natív hiányosságait, és felgyorsítva ezzel az Ön napi munkáját. Moduláris architektúrája lehetővé teszi, hogy szervezete ne csak a ma, de a holnap üzleti kihívásaival is könnyedén szembenézhessen.

JELLEMZŐK

Biztonságos hozzáférés

Az Active Roles átfogó kiemelt felhasználó-kezelést biztosít az Active Directory-hoz, és az Azure Active Directory-hoz, így lehetővé teszi, hogy a legkisebb jogosultság elve alapján szabályozhassa az adminisztrátorok hozzáférését. Előre definiált házirendek és engedélyek alapján hozza létre és kényszeríti ki a hozzáférési szabályokat, így megszünteti a hibrid AD natív kezelésére jellemző hibákat és anomáliákat. Ezen felül a robosztus és személyre szabott jóváhagyási rendszer egy olyan IT folyamatot biztosít, amely egybevág az üzleti igényekkel: az automatikus címtárkezelést kiegészíti a felelősségi láncolatokkal.

Napi címtár-kezelés

Az Active Roles segítségével Ön hatékonyan kezelheti az alábbiakat mind a helyben telepített, mind az Azure AD környezetben egyaránt:

- Exchange felhasználók, beleértve a mailbox/OCS hozzárendelést, létrehozást, mozgatást, törlést, valamint a jogosultságok és levelezési listák kezelését
- Felhasználói csoportok
- Számítógépek, megosztott könyvtárak, nyomtatók, helyi felhasználók és csoportok
- Active Directory és Azure Active Directory

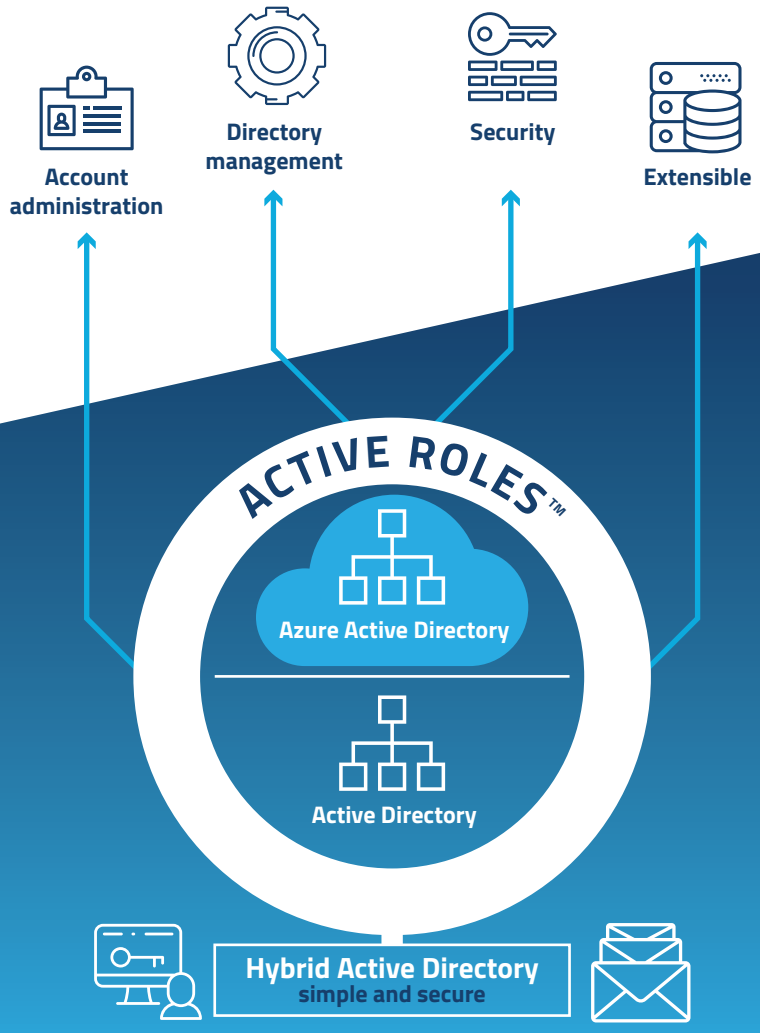
Az Active Roles intuitív kezelőfelülettel rendelkezik, amely megkönnyíti a mindennapi adminisztrációt és a helpdesk működését hibrid AD/AAD környezetben. Az MMC „snap-in"-t és a webes kezelőfelületet egyaránt támogatja.

Automatizált fiók létrehozás

Az Active Roles számos feladatot automatizál, mint például

- Az egyéni és csoportos felhasználói fiókok létrehozását az AD-ban és az AAD-ban
- Az email fiókok létrehozását az Exchange-ben és az Exchange Online-ban
- A csoporttagságok kezelését az AD-ben és AAD-ben
- Az erőforrások allokálását a Windows-ban

Az Active Roles ezen felül automatizálja a felhasználók hozzáférési jogosultságainak visszavonását és visszaállítását az AD-ben és az AAD-ben egyaránt, sőt, az Active Directory-hoz kapcsolt más rendszerekben is. Így a felhasználók és felhasználói csoportok teljes életciklusuk alatt hatékonyan és biztonságosan kezelhetők. Ha egy felhasználó hozzáférését meg kell változtatni, vagy vissza kell vonni, a szükséges frissítések automatikusan megtörténnek minden releváns rendszerben: a hibrid AD/AAD környezetben ugyanúgy, mint, az AD-hez kapcsolódó más rendszerekben is, mint például a Unix, a Linux vagy a Mac OS X.



Hibrid AD-re optimalizált

Az Active Roles egyetlen telepítéssel képes kiszolgálni a helyileg telepített AD és az Azure AD igényeket egyaránt. Egyetlen kezelőfelületet, egységes munkafolyamatokat, és konzisztens felhasználói élményt biztosít a teljes hibrid környezetben. Szükségtelenné teszi a nehézkes, korlátozott és gyakori hibákat eredményező, különálló eszközök használatát és a manuális folyamatokat.

Identity Analytics

Kezelje a kockázatokat, mielőtt még problémát okoznának! Kapjon átfogó képet a felhasználói jogosultságokról a hibrid AD környezetben is! A Starling Identity Analytics & Risk Intelligence (egy Active Roles-hoz vásárolható kiegészítő) elemzést készít a felhasználói jogosultságokról az Active Directory-ban, az Azure Active Directory-ban és magában az Active Roles-ban is, és megjelöli a szerepkörükhöz, kollégákhoz, vagy a biztonsági szabályokhoz képest elfogadhatatlanul magas jogosultságú felhasználókat.

One Identity Hybrid előfizetés

Terjessze ki az Active Roles funkcionalitását a One Identity Hybrid előfizetéssel, amely azonnali hozzáférést nyújt számos további felhő-alapú funkciókhoz és szolgáltatáshoz. Ezek közé tartozik a Starling Two-Factor Authentication, amely biztonságos adminisztrátori hozzáférést tesz lehetővé, és a Starling Identity Analytics & Risk Intelligence, amely előre jelzi a kockázatokat, valamint elemzi az Active Roles-hoz való hozzáféréseket is. Ez a szolgáltatás további célrendszerekre és alkalmazási területekre is kiterjeszthető, így egyetlen One Identity előfizetéssel minden megoldásunkhoz hozzáférhet.

„Ha egy felhasználó hozzáférését meg kell változtatni, vagy vissza kell vonni, a szükséges frissítések automatikusan megtörténnek a releváns rendszerekben: a hibrid AD/AAD környezetben ugyanúgy, mint az AD-hez kapcsolódó más rendszerekben is, mint például a Unix, a Linux vagy a Mac OS X.”

Integrálja a kezelési pontokat

Az Active Roles remekül kiegészíti az ön jogosultság- és hozzáférés-kezelési stratégiáját. Egyszerűbbé és ésszerűbbé teszi a felhasználók kezelését. Zökkenőmentesen integrálható más One Identity termékekkel, mint például az Identity Manager, a Privileged Password Manager, az Authentication Services, a Defender, a Password Manager, a Cloud Access Manager és a ChangeAuditor termékekkel. Az Active Roles ezen felül automatizálja és kiterjeszti a Power Shell, az ADSI, az SPML és a testre szabható webes kezelőfelületek képességeit is.

Az Active Roles támogat minden olyan szinkronizálási technológiát, amely az alábbiak biztonságos kezeléséhez szükséges:

- Lync
- Exchange
- SharePoint
- AD LDS
- Office 365
- Azure AD
- Microsoft SQL Server
- OLE DB (MS Access)
- Flat file

Kezelje csoportjait és felhasználóit hosztolt környezetben

Szinkronizálja az AD domain klienseket a hoszt AD domain-nel hosztolt környezetekben is! Az Active Roles lehetővé teszi a felhasználói és csoport fiókok kezelését a kliens domain-ból a hoszt domain-ba, úgy, hogy közben a jelszavakat és az attribútumokat is szinkronizálja. Használja ki az ”out-of-the-box” konnektorokat, és szinkronizálja helyi AD fiókjait a Microsoft Office 365-tel, a Lync Online-nal és a SharePoint Online-nal.

A One Identity-ről

A One Identity segít a cégeknek a jogosultság és hozzáférés-kezelést (Identity and Access Management, IAM) jól csinálni. Jogosultság szabályozást (identity governance), hozzáférés-kezelést, kiemelt-felhasználó kezelést és jogosultságot, mint szolgáltatást (identity as a service) tartalmazó egyedi termékportfóliója támogatja a szervezeteket üzleti lehetőségeik teljes kihasználásában, mindezt biztonsági béklyók nélkül, mégis védelmet nyújtva a fenyegetések ellen.

ONE IDENTITY by Quest

Tudjon meg többet a **balasys.hu** weboldalon.