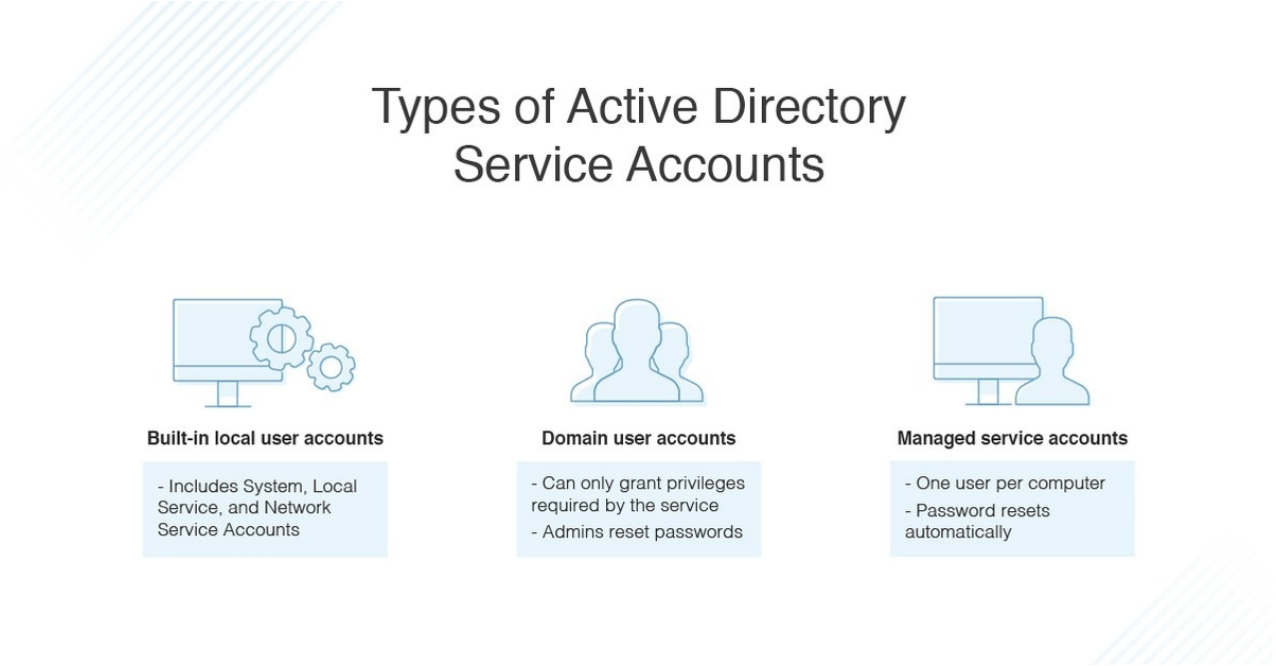
10 nejlepších osvědčených postupů pro účty služby Active Directory

dnsstuff.com/active-directory-service-accounts

November 4, 2019

S Windows Active Directory lze nastavit řadu různých typů účtů s nezbytnými oprávněními, přístupy a rolemi. Patří sem servisní účty, které jsou určeny pro použití při instalaci aplikací nebo služeb do operačního systému. Mezi běžné typy účtů služeb Active Directory patří vestavěné místní uživatelské účty, uživatelské účty domény, účty spravovaných služeb a virtuální účty. Tyto účty mají širší oprávnění a lepší přístup k infrastruktuře než jiné účty, což je činí zranitelnými vůči zneužití zabezpečení.



V tomto článku uvedu osvědčené postupy pro zabezpečení vašich servisních účtů a vysvětlím, proč posledním a nejdůležitějším osvědčeným postupem servisních účtů je zajistit, abyste měli řešení, jako je Access Rights Manager, které vám poskytne kritické informace o vašich oprávněních AD. .

Skočit dopředu:

10. Implementujte software pro správu přístupových práv

Jak fungují účty služby Active Directory

Každý typ servisního účtu má své vlastní provozní účely.

- **Mezi vestavěné místní uživatelské účty** patří systémový účet (pro správu místního systému), účet místní služby, který přistupuje k síťovým službám bez přihlašovacích údajů, a účet síťové služby, který přistupuje k síťovým zdrojům pomocí přihlašovacích údajů počítače.
- **Uživatelské účty domény** jsou určeny pro použití službami a jsou centrálně spravovány službou Active Directory . Je možné vytvořit uživatelský účet pro jednu službu nebo jej sdílet mezi více službami. S uživatelskými účty domény však můžete udělit pouze oprávnění požadovaná službou a hesla je třeba pravidelně obnovovat.
- **Účty spravovaných služeb** Active Directory jsou podobné uživatelským účtům domény, ale heslo se pravidelně a automaticky obnovuje. Každému počítači můžete přiřadit pouze jeden uživatelský účet a každý účet lze použít s více službami v počítači. Alternativně můžete pro každou službu vytvořit samostatné účty.

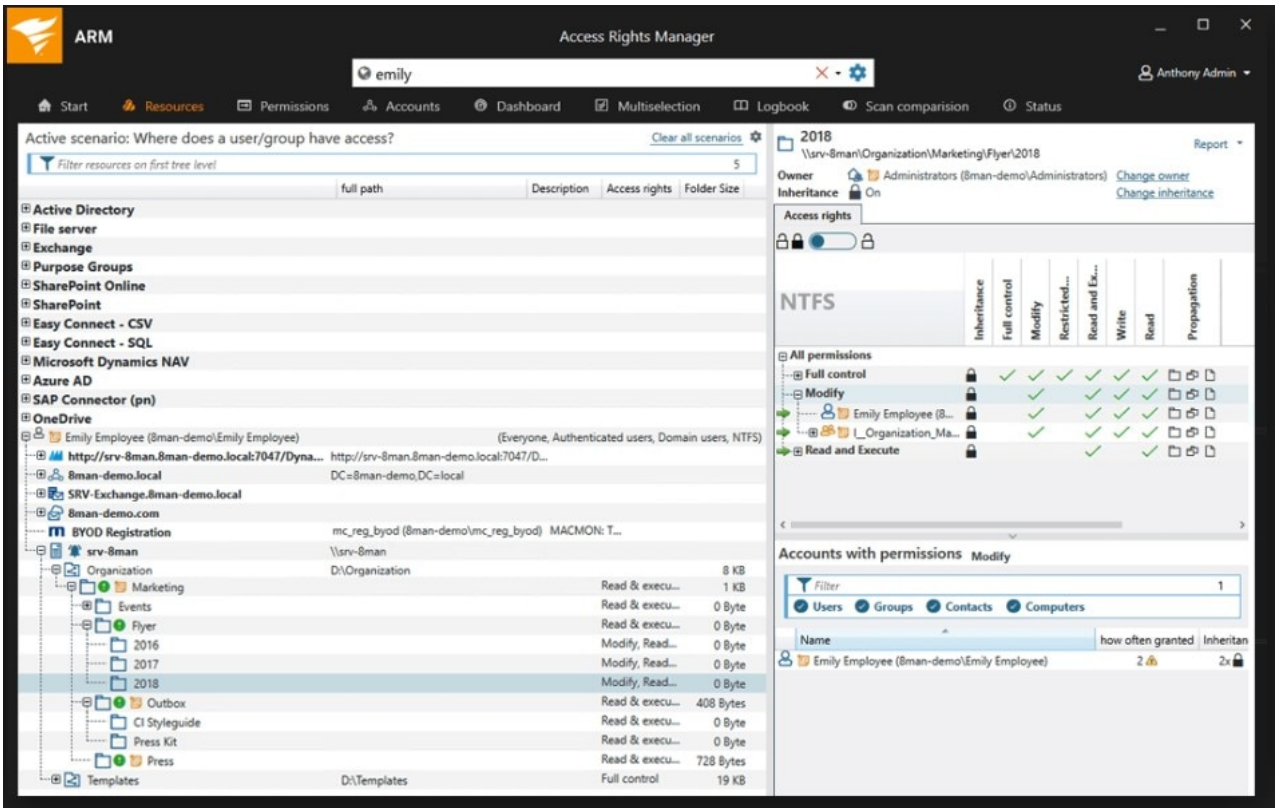
Mezi výhody účtu řízených služeb patří zvýšená bezpečnost a snadná údržba. Tyto účty navíc mohou provozovat služby na počítači s možností připojení k síťovým službám jako konkrétní uživatelský principál. Je však důležité tyto účty pravidelně kontrolovat a znát některé osvědčené postupy pro zajištění bezpečnosti.

Doporučené postupy pro účty služby Active Directory

1. **Mějte omezený přístup.** Ujistěte se, že přidělujete účtům služeb AD pouze minimální oprávnění, která vyžadují pro úkoly, které potřebují k provedení, a neposkytujte jim více přístupu, než je nutné. V mnoha případech můžete odebrat funkce pro vzdálený přístup, přihlášení k terminálové službě, přístup k internetu a práva vzdáleného ovládání.
2. **Vytvořte servisní účty od začátku.** Nevytvářejte účty služeb v Active Directory kopírováním starých, protože byste mohli omylem kopírovat z účtu služby s mnohem vyššími oprávněními, než potřebujete. To by mohlo vést k bezpečnostním problémům a zneužití účtu, pokud někomu poskytnete účet s přístupem ke zdrojům nebo informacím, se kterými by neměl být zasvěcen.
3. **Nevkládejte servisní účty do vestavěných privilegovaných skupin.** Vkládání účtů služeb do skupin s vestavěnými oprávněními může být riskantní, protože každá osoba ve skupině bude mít přístup k přihlašovacím údajům účtu služby. Pokud dojde ke zneužití účtu, může být těžké zjistit, kdo je pachatelem. Pokud potřebujete účet služby pro privilegovanou skupinu, vytvořte novou skupinu se stejnými oprávněními a povolte přístup *pouze* k účtu služby.

4. **Zakázat přístup servisního účtu k důležitým objektům.** Použijte seznam řízení přístupu k ochraně citlivých souborů, složek, skupin nebo objektů registru před zneužitím účty služby AD. Chcete-li přístup zakázat, přejděte do objektu a otevřete okno „Vlastnosti“ pro přístup k bezpečnostním oprávněním, přidejte účet do seznamu „Položka oprávnění“ a nastavte stav na „Odmítnout“. To zabrání účtu služby v přístupu k objektu. Pokud potřebujete udělit někomu konkrétní přístup k objektu, můžete jej přidat a později, až dokončí svůj úkol, přepnout zpět na „Odmítnout“.
5. **Odstraňte nepotřebná práva.** Odepření nepodstatných uživatelských práv je užitečné pro udržení silných bezpečnostních opatření. To zahrnuje „zakázat přístup k tomuto počítači ze sítě“, „zakázat místní přihlášení“ a „zakázat přihlášení jako dávkovou úlohu“.
6. **Nastavte přístup pomocí funkce „Přihlásit se do“.** Když vytvoříte servisní účet, můžete mu povolit přihlášení pouze k určitým počítačům, abyste chránili citlivá data. Otevřete Uživatelé a počítače služby Active Directory a poté „Vlastnosti“. Na záložce „Účet“ klikněte na tlačítko „Přihlásit se k“ a přidejte počítače do seznamu povolených zařízení, ke kterým se servisní účet může přihlásit.
7. **Omezte časové rámce.** Další zabezpečení můžete přidat tak, že nakonfigurujete účty služeb AD tak, aby se mohly přihlásit pouze v určitou denní dobu.
8. **Kontrola konfigurace hesla.** Můžete nastavit servisní účet, aby uživatel nemohl změnit své vlastní heslo . Můžete to také nastavit tak, aby účet nemohl být delegován na někoho jiného. Tím je zajištěno, že administrátor kontroluje heslo a nikdo jiný než oprávnění uživatelé nemá přístup k účtu.
9. **Povolit auditování.** Nezapomeňte povolit auditování pro všechny účty služeb a související objekty. Jakmile je auditování povoleno, pravidelně kontrolujte protokoly, abyste viděli, kdo, kdy a pro jaké účely účty používá. Audit je jedním z nejdůležitějších osvědčených postupů: pomáhá zajistit bezpečnost, ověřuje dodržování interních procesů a opatření pro dodržování předpisů a dokáže odhalit jakékoli problémy nebo porušení dříve, než uplyne příliš mnoho času.
10. **Implementujte software pro správu přístupových práv.** Být opatrný je zásadní, aby se zabránilo zneužití širokého přístupu a oprávnění. Nástroj pro správu přístupových práv může být přínosem pro zajištění toho, že uživatelské účty jsou nastaveny a spravovány s příslušnými oprávněními a přístupem.

Doporučuji SolarWinds ® Access Rights Manager (ARM), který je navržen tak, aby automatizoval proces správy účtu a zkrátil čas, který musíte věnovat poskytování. Software také obsahuje podrobné nástroje pro audit a sledování shody, které vám pomohou splnit přísné požadavky na dodržování bezpečnosti, včetně předpisů pro dodržování zásad a odvětví, jako jsou GDPR, PCI DSS a HIPAA .



Nástroje auditu v ARM jsou jednoduché a snadno použitelné a umožňují vám rychle vytvářet zprávy o používání účtu a chování, které jsou připraveny pro auditora a správu, a také o chování, které prokáže dodržování důležitých bezpečnostních procesů.

Dalším řešením, které stojí za to vyzkoušet, je Passportal. Toto je řešení správy hesel pro MSP a další poskytovatele IT služeb, stejně jako velké korporace a podniky všech typů.

S Passportal získáte přístup k centralizované cloudové platformě pro správu hesel. Můžete si uložit tolik hesel, kolik potřebujete, vyhledávat a libovolně je měnit a konfigurovat nastavení tak, aby vyhovovalo vašim potřebám.

Pokud tedy potřebujete způsob, jak spravovat přihlašovací údaje služby Active Directory – nebo přihlašovací údaje vašich klientů – Passportal je komplexní řešení. Je navržen tak, aby byl také zabezpečený, takže se nemusíte bát, že by se vaše hesla a další klíčová data dostala do nesprávných rukou.