Rozšíření Kerberos pro jednotné přihlašování

Uživatelská příručka

Prosinec 2019

Obsah

Úvod **3**

Začátky **4**

Pokročilé funkce **8**

Přechod z Enterprise Connectu **13**

Příloha **16**

Úvod

Rozšíření Kerberos pro jednotné přihlašování (SSO) pomůže vaší organizaci používat na zařízeních Apple jednotné přihlašování přes Kerberos.

Zjednodušené ověřování přes Kerberos

Rozšíření Kerberos pro SSO zjednodušuje proces, kterým se z vaší domény Active Directory obstarává tiket na přidělování tiketů (ticket-granting ticket, TGT) Kerberu. Tím uživatelům usnadňuje přihlašování ke zdrojům, jako jsou webové stránky, aplikace nebo servery. V macOS si rozšíření Kerberos pro SSO aktivně vyžádá TGT, kdykoli se změní stav sítě, aby byl uživatel v případě potřeby připravený na ověření.

Správa účtů Active Directory

Rozšíření Kerberos pro SSO taky uživatelům usnadňuje správu jejich účtu Active Directory. V macOS umožňuje uživatelům měnit si hesla k Apple Directory a upozorňuje je, když heslu brzy vyprší platnost. Uživatelé si taky můžou změnit hesla ke svým místním účtům tak, aby odpovídala heslům z Active Directory.

Podpora Active Directory

Rozšíření Kerberos pro SSO by se mělo používat s lokální doménou Active Directory. Služba Azure Active Directory není podporována. K používání rozšíření Kerberos pro SSO není potřeba, aby zařízení bylo propojené s doménou Active Directory. Navíc se uživatelé nemusí k Macu přihlašovat svými účty Active Directory ani mobilními účty. Apple naopak doporučuje používat místní účty.

Požadavky

- iOS 13, iPadOS nebo macOS Catalina.
- Doména Active Directory s Windows Serverem 2008 nebo novějším. Rozšíření Kerberos pro SSO není určené k používání s Azure Active Directory. Vyžaduje tradiční lokální doménu Active Directory.
- Přístup k síti, ve které je doména Active Directory hostovaná. Může se jednat o přístup přes Wi-Fi, Ethernet nebo VPN.
- Zařízení je nutné spravovat pomocí řešení správy mobilních zařízení (MDM), které podporuje datovou část pro konfigurační profil rozšiřitelného jednotného přihlašování (SSO). Kontaktujte svého dodavatele MDM a zeptejte se, jestli tuto datovou část konfiguračních profilů podporuje.

Enterprise Connect

Rozšíření Kerberos pro SSO je zamýšlené jako náhrada Enterprise Connectu. Pokud momentálně používáte Enterprise Connect a chcete přejít na rozšíření Kerberos pro SSO, přečtěte si v tomto dokumentu část Přechod z Enterprise Connectu, která uvádí další informace.

Začátky

Sestavení a nasazení konfiguračního profilu

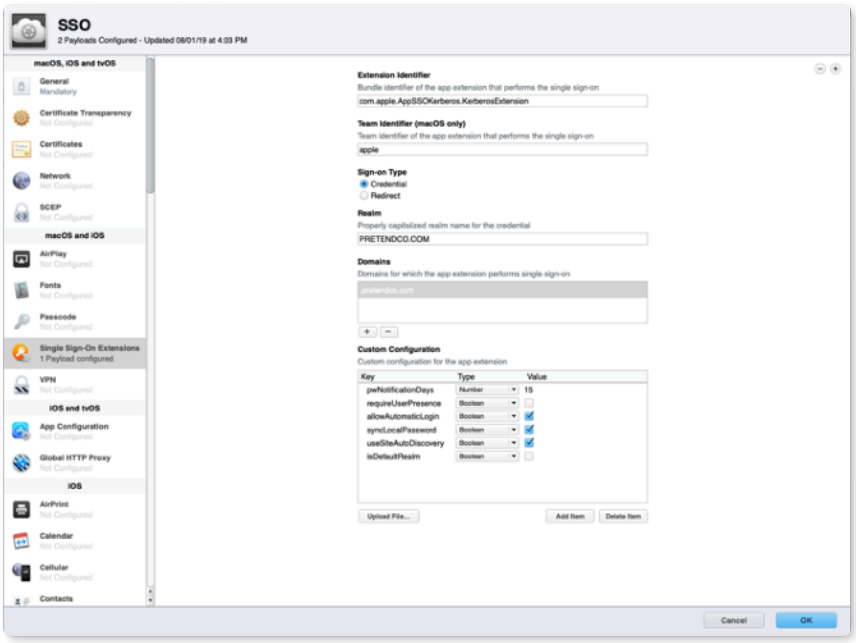
Abyste mohli používat rozšíření Kerberos pro SSO, musíte ho nakonfigurovat pomocí konfiguračního profilu, distribuovaného do zařízení pomocí řešení MDM.

Poznámka: Je nutné, aby byl konfigurační profil do zařízení distribuován přes MDM. V macOS musí jít o registraci do MDM, kterou schvaluje uživatel a která se instaluje do prostoru Systém. Ruční přidávání profilů není podporováno.

Při konfiguraci pomocí konfiguračního profilu použijte datovou část pro rozšiřitelné jednotné přihlašování, kterou jsme uvedli v iOS 13, iPadOS a macOS 10.15. Profile Manager (součást macOS Serveru) obsahuje podporu datové části pro rozšiřitelné jednotné přihlašování. Pokud vaše řešení MDM tuto datovou část ještě nepodporuje, možná můžete potřebný profil sestavit v Profile Manageru, potom ho naimportovat do MDM a rozdistribuovat ho. Další informace vám sdělí váš dodavatel MDM.

Konfigurační profil v Profile Manageru sestavíte tímhle způsobem:

1. Přihlaste se do Profile Manageru.
2. Vytvořte profil pro skupinu zařízení nebo konkrétní zařízení.
3. V seznamu datových částí vyberte Single Sign-On Extensions (Rozšíření pro jednotné přihlašování), klikněte na tlačítko Přidat (+) a přidejte novou datovou část.
4. Do pole Extension Identifier (Identifikátor rozšíření) zadejte „com.apple.AppSSOKerberos.KerberosExtension“.
5. Do pole Team Identifier (Identifikátor týmu) zadejte „apple“.



6. V části Sign-on Type (Typ přihlášení) vyberte typ přihlašovacích údajů.
7. Do pole Realm zadejte název domény Active Directory, ve které se nacházejí vaše uživatelské účty, a to velkými písmeny. Nepoužívejte název vašeho lesa Active Directory, pokud se vaše uživatelské účty nenacházejí na úrovni lesa.

8. V části Domains (Domény) klikněte na tlačítko Přidat (+) a přidejte domény všech zdrojů, které používají Kerberos. Například pokud ověřování Kerberos používáte se zdroji z my.vymyslenafirma.cz, přidejte „.my.vymyslenafirma.cz“. (Nezapomeňte na tečku na začátku.)
9. V části Custom Configuration (Vlastní konfigurace) přidejte následující hodnoty:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Nezaškrtnuto
allowAutomaticLogin	Boolean	Zaškrtnuto
syncLocalPassword	Boolean	Zaškrtnuto
useSiteAutoDiscovery	Boolean	Zaškrtnuto
isDefaultRealm	Boolean	Nezaškrtnuto

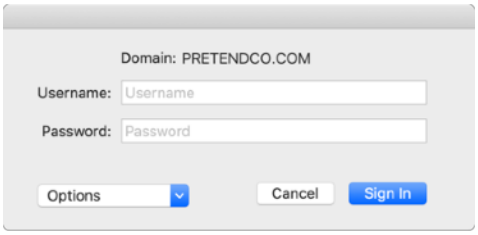
10. Kliknutím na OK nový konfigurační profil uložte. Automaticky se nainstaluje do vybraného zařízení nebo skupiny zařízení.

Nastavení na straně uživatele – iOS a iPadOS

1. Připojte zařízení k síti, ve které je dostupná doména Active Directory vaší organizace.
2. Proveďte jedu z těchto možností:
   - V Safari přejděte na web, který podporuje ověřování přes Kerberos.
   - Spusťte aplikaci, která podporuje ověřování přes Kerberos.
3. Zadejte své uživatelské jméno a heslo ke Kerberu nebo Active Directory.
4. Zobrazí se dotaz, jestli se chcete automaticky přihlásit natrvalo. Většina uživatelů by měla klepnout na Ano.
5. Klepněte na Přihlásit se. Po krátké pauze se webová stránka nebo aplikace načte. Když zvolíte, že se chcete k rozšíření Kerberos pro SSO přihlašovat automaticky, už se vám nebudou zobrazovat výzvy k zadání přihlašovacích údajů, dokud si nezměníte heslo. Pokud automatické přihlašování odmítnete, budete muset zadat přihlašovací údaje, teprve až vaše přihlášení ke Kerberu vyprší – obvykle za 10 hodin.

Nastavení na straně uživatele – macOS

1. Musíte se přihlásit k rozšíření Kerberos pro SSO. Tento proces se dá zahájit několika způsoby:
   - Pokud je váš Mac připojený k síti, ve které je dostupná vaše doména Active Directory, zobrazí se vám výzva k přihlášení okamžitě po nainstalování konfiguračního profilu pro rozšiřitelné SSO.
   - Výzva k ověření se zobrazí, když v Safari otevřete web, který přijímá ověřování přes Kerberos, nebo použijete aplikaci vyžadující ověřování přes Kerberos.
   - Okamžitá výzva k ověření se zobrazí, kdykoli svůj Mac připojíte k síti, ve které je dostupná služba Active Directory.
   - Můžete vybrat ikonu nabídky pro Kerberos SSO a kliknout na Přihlásit se.
2. Zobrazí se výzva k zadání přihlašovacích údajů pro Kerberos. Zadejte své uživatelské jméno a heslo ke Kerberosu nebo Active Directory.



3. Zobrazí se dotaz, jestli se chcete přihlašovat automaticky. Většina uživatelů by měla kliknout na Ano.
4. Klikněte na Přihlásit se. Po krátké pauze se webová stránka nebo aplikace načte. Když zvolíte, že se chcete k rozšíření Kerberos pro SSO přihlašovat automaticky, už se vám nebudou zobrazovat výzvy k zadání přihlašovacích údajů, dokud si nezměníte heslo. Pokud automatické přihlašování odmítnete, budete muset zadat přihlašovací údaje, teprve až vaše přihlášení ke Kerberu vyprší – obvykle za 10 hodin.
5. Jakmile se přiblíží vypršení hesla, přijde vám oznámení s informací, kolik dní vám do vypršení zbývá. Na oznámení můžete kliknout a heslo si změnit.
6. Jestli máte zapnutou synchronizaci hesel, budete požádáni o své aktuální heslo k Active Directory a o místní heslo. Zadejte obě a kliknutím na OK je synchronizujte. Tato výzva se zobrazí při prvním přihlášení, i když už hesla jsou synchronizovaná.

Změny hesel – macOS

Pomocí rozšíření Kerberos pro SSO si můžete taky změnit heslo k Active Directory:

1. Ujistěte se, že jste k rozšíření Kerberos pro SSO přihlášení.
2. Vyberte ikonu nabídky pro Kerberos SSO a zvolte Změnit heslo. Může vám taky přijít oznámení, že se blíží vypršení hesla.
3. Zadejte své stávající heslo a potom nové heslo. Ujistěte se, že nové heslo splňuje požadavky vaší organizace na hesla. Klikněte na OK.
4. Po krátké pauze se zobrazí dialogové okno s informací, že změna hesla proběhla úspěšně. Pokud máte zapnutou synchronizaci hesel, aktualizuje se i heslo k vašemu místnímu účtu, aby odpovídalo novému heslu k Active Directory.

Požívání ikony nabídky pro Kerberos SSO – macOS

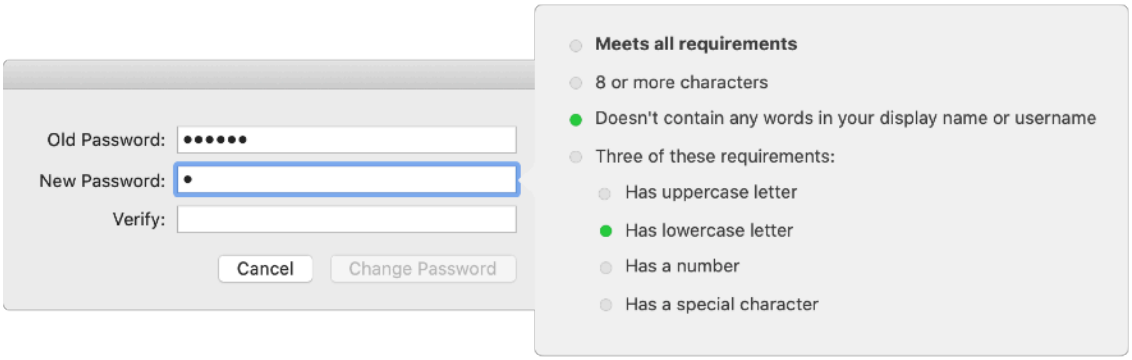
Ikona nabídky pro Kerberos SSO umožňuje snadný přístup k užitečným informacím o vašem účtu a o funkcích rozšíření. Zobrazuje se jako šedivý nebo černý klíč na řádku nabídek vpravo nahoře.

Informace o stavu vašeho účtu zjistíte podle barvy ikony Kerberos SSO v nabídce. Když je klíč šedivý, nejste k rozšíření přihlášení. Když je klíč černý, jste přihlášení. Když klíč vyberete, zobrazí se vám účty, ke kterým jste přihlášení, spolu s informací o tom, za kolik dní vaše heslo vyprší. Pomocí nabídky se taky můžete přihlásit, odhlásit nebo si změnit heslo.

Pokročilé funkce

Testování hesel při zadávání

V mnoha konfiguracích Active Directory můžete pomocí rozšíření pro Kerberos SSO testovat nová uživatelská hesla už během zadávání a informovat uživatele o tom, jaké požadavky musí při změně hesla dodržovat. Po nakonfigurování této funkce uvidí uživatelé při zadávání nového hesla tohle:



K používání této funkce je zapotřebí, aby doména Active Directory používala jenom standardní zásady hesel Active Directory. Ve výchozím nastavení Active Directory umožňuje správci vyžadovat, aby hesla byla složitá a měla určitou délku. Charakteristiky složitého hesla popisuje článek technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Poznámka: Tuto funkci možná nebudete moct používat, pokud vaše doména používá nástroje nebo DLL knihovny od jiných dodavatelů, kterými rozšiřuje standardní zásady hesel v Active Directory. Například pokud vaši uživatelé nesmí v hesle používat zakázaná slova (jiná než své uživatelské jméno) nebo musí v heslu použít konkrétní počet zvláštních znaků, pravděpodobně používáte rozšíření zásad hesel od jiného dodavatele. Pokud si nejste jistí, zeptejte se na bližší informace svého správce Active Directory.

Pokud vaše doména Active Directory splňuje požadavky, můžete si testování hesel při zadávání zapnout. V konfiguračním profilu rozšíření Kerberos pro SSO nastavte následující parametry:

Parameter	Key	Type	Value	Volitelné
Vyžadovat složitá hesla	pwReqComplexity	Boolean	ANO	Ne
Požadovaná délka hesla	pwReqLength	Integer	Číslo	Ano
Znovu použít předchozí limit hesel	pwReqHistory	Integer	Číslo	Ano
Minimální stáří hesla	pwReqMinAge	Integer	Číslo	Ano

Testování hesel při zadávání má určitá omezení. Nedokáže ověřit, jestli už heslo bylo dřív použito. Taky nedokáže ověřit, jestli heslo neobsahuje uživatelské jméno z Active Directory nebo jestli už uživatel nemá TGT Kerberu. To se stává, například když nastavujete heslo poprvé nebo když vaše heslo vypršelo. Všechny ostatní kontroly fungují normálně.

Zobrazení požadavků hesel

Pokud nemůžete používat testování hesel při zadávání, můžete v rozšíření Kerberos pro SSO nastavit, aby se při zadávání nového hesla zobrazoval textový řetězec, který uživatele informuje o požadavcích vaší organizace na hesla. V konfiguračním profilu rozšíření Kerberos pro SSO nastavte proměnnou „pwReqText“ na textový řetězec, který se má uživatelům zobrazovat při změnách hesla.

Změny hesel a vypnutí této funkce

Některé organizace možná nechtějí používat standardní funkce Kerberos SSO pro změny hesel, protože uživatelům neumožňují provádět změny hesel Active Directory. Jestli chcete tuto funkci vypnout, v konfiguračním profilu rozšíření Kerberos pro SSO nastavte proměnnou „allowPasswordChanges“ na FALSE.

Podpora webu pro změnu hesel – macOS

Rozšíření Kerberos pro SSO se dá nastavit tak, aby se, když uživatel zvolí „Změnit heslo“ nebo zareaguje na upozornění o konci platnosti hesla, otevřel ve výchozím prohlížeči web na změnu hesla. Tuto funkci doporučuje Apple používat jen s lokálními účty, protože mobilní účty v ní nejsou podporované.

V konfiguračním profilu rozšíření Kerberos pro SSO nastavte proměnnou „pwChangeURL“ na webovou adresu vašeho webu pro změnu hesla. Jakmile si uživatel změní heslo, musí se od rozšíření pro Kerberos odhlásit a potom se znova přihlásit pomocí nového hesla. Pokud je zapnutá místní synchronizace hesel, systém uživatele provede procesem, který mu pomůže hesla opět synchronizovat.

Synchronizace hesel – macOS

Rozšíření Kerberos pro SSO může nastavit heslo k místnímu účtu tak, aby se shodovalo s uživatelovým heslem k Active Directory. Tuto funkci zapnete tak, že v části Custom Configuration (Vlastní konfigurace) v konfiguračním profilu rozšíření Kerberos pro SSO nastavíte proměnnou „syncLocalPassword“ na TRUE.

Synchronizace hesel se skládá ze dvou základních funkcí. Zaprvé, když si uživatel pomocí rozšíření Kerberos pro SSO změní heslo, tato funkce mu změní lokální heslo tak, aby odpovídalo heslu k Active Directory. Pokud přestanou být lokální heslo a heslo k Active Directory synchronizované, rozšíření Kerberos pro SSO je opět synchronizuje následujícím způsobem:

- Po zapnutí synchronizace hesel a při každém dalším pokusu o přihlášení přes rozšíření Kerberos pro SSO se porovná datum, kdy si uživatel naposledy změnil místní heslo a kdy heslo k Active Directory, s daty uloženými v mezipaměti. Když se hodnoty budou shodovat, jsou hesla synchronizovaná a není potřeba dělat nic dalšího. Když se nebudou shodovat, rozšíření Kerberos pro SSO se uživatele zeptá na jeho místní heslo a heslo k Active Directory. Až uživatel zadá místní heslo, rozšíření Kerberos pro SSO přenastaví jeho místní heslo tak, aby odpovídalo heslu k Active Directory.
- Změna hesla funguje podobně. Když si uživatel pomocí rozšíření Kerberos pro SSO změní heslo, jeho staré heslo k Active Directory se porovná s místním účtem. Pokud se staré heslo k Active Directory shoduje s místním heslem, rozšíření Kerberos pro SSO změní obě hesla. Pokud se neshodují, změní se jenom heslo k Active Directory. Uživateli se potom při dalším pokusu o připojení zobrazí výzva k zadání místního hesla.

Tato funkce má následující požadavky:

- Když je uživatel přihlášený k Macu pomocí Active Directory – nikoli pomocí místního účtu –, je synchronizace hesel vypnutá. Funkce je určená výhradně pro místní účty, takže pokud je uživatel přihlášený k Macu pomocí účtu Active Directory, není tato funkce potřeba.
- Pokud u místních účtů vynucujete určité zásady hesel (například pomocí konfiguračního profilu nebo příkazu pwpolicy), pohlídejte si, aby zásady místních hesel byly stejné nebo mírnější než zásady hesel v Active Directory. Pokud jsou zásady místních hesel přísnější než zásady hesel v Active Directory, může se stát, že rozšíření Kerberos pro SSO přijme heslo, které vyhovuje požadavkům Active Directory, ale už se mu nepodaří změnit místní heslo, protože nové heslo nebude vyhovovat místním požadavkům. Jestli nutně potřebujete, aby byly zásady místních hesel přísnější než zásady hesel v Active Directory, pak tuto funkci nepoužívejte.
- Pokud je místní uživatelské jméno jiné než uživatelské jméno v Active Directory, budou se synchronizovat jenom hesla.

Podpora chytrých karet – macOS

Rozšíření Kerberos pro SSO umožňuje používat ověřování identity založené na chytrých kartách. Chytré karty musí používat ovladač CryptoTokenKit – ovladače založené na tokend nejsou podporovány. macOS 10.15 obsahuje podporu standardu PIV, který hojně využívá americká administrativa.

Než začnete, ujistěte se, že vaše doména Active Directory je nakonfigurovaná na podporu ověřování pomocí chytrých karet. Proces zapnutí ověřování pomocí chytrých karet je nad rámec tohoto dokumentu. Podrobnosti si přečtěte v dokumentaci Microsoftu.

Jestli se chcete k rozšíření Kerberos pro SSO přihlásit pomocí chytré karty, proveďte tento postup:

1. Klikněte na nabídku Options (Volby) a zvolte Use a smart card (Použít chytrou kartu).
2. Až uvidíte tlačítko Identity (Identita), vložte chytrou kartu a klikněte na něj.
3. Zvolte identitu, ke které se chcete přihlásit, klikněte na OK a potom na Přihlásit se.
4. Až k tomu budete vyzváni, zadejte PIN.

Pokud si rozšíření Kerberos pro SSO musí obstarat TGT Kerberu, budete požádáni o vložení chytré karty a zadání PIN. Další informace o podpoře chytrých karet v macOS zobrazíte tak, že v Terminálu spustíte příkaz „man SmartCardServices“.

Distribuovaná oznámení – macOS

Rozšíření Kerberos pro SSO posílá při různých událostech distribuovaná oznámení. Aplikace a služby v macOS můžou pomocí distribuovaných oznámení říkat jiným aplikacím a službám, že došlo k nějaké události. Aplikace nebo služba, která na takovou událost čeká, pak může provést další akci.

Pomocí této funkce může správce nastavit, aby se při určité události spustila určitá akce. Správce například může nastavit, aby se spustil určitý skript pokaždé, když rozšíření Kerberos pro SSO získá přes Kerberos nové přihlašovací údaje.

Ve chvíli, kdy dojde k určené události, rozšíření Kerberos pro SSO jenom pošle distribuované oznámení. Samo žádnou další akci neprovádí. Správce musí nastavit nástroj, který bude čekat na oznámení a podle potřeby provádět potřebné akce.

V příloze najdete příklad skriptu a seznam vlastností launchd (.plist), který dokáže čekat na oznámení a spouštět akce. Příklad si upravte podle potřeb svého nasazení.

Tady jsou popsaná distribuovaná oznámení, která umí rozšíření Kerberos pro SSO posílat:

Název	Kdy se posílá
com.apple.KerberosPlugin.ConnectionCompleted	Rozšíření Kerberos pro SSO dokončilo proces připojování.
com.apple.KerberosPlugin.ADPasswordChanged	Uživatel si pomocí rozšíření změnit heslo k Active Directory.
com.apple.KerberosPlugin.LocalPasswordSynced	Uživatel synchronizoval své místní heslo s heslem Active Directory.
com.apple.KerberosPlugin.InternalNetworkAvailable	Uživatel se připojil k síti, ve které je dostupná nakonfigurovaná doména Active Directory.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	Uživatel se připojil k síti, ve které není dostupná nakonfigurovaná doména Active Directory.
com.apple.KerberosExtension.gotNewCredential	Uživatel získal nový TGT Kerberu.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	Uživatel si změnil heslo k Active Directory a místní heslo bylo taky změněno, aby se shodovalo s novým heslem k Active Directory.

Podpora příkazového řádku – macOS

Pomocí nástroje příkazového řádku zvaného *app-sso* můžou správci rozšíření Kerberos pro SSO ovládat a zobrazovat si užitečné informace. Můžou pomocí něj například vyvolat přihlášení, změnu hesla nebo odhlášení. Nástroj taky umí zobrazovat užitečné informace jako aktuálně přihlášeného uživatele, aktuální web Active Directory používaný daným počítačem, sdílené zdroje v uživatelově domácí síti, datum vypršení uživatelova hesla a spoustu dalších informací ve formě seznamu vlastností nebo ve formátu JSON. Pro potřeby správy inventáře nebo jiné účely můžete informace zpracovat a nahrát je do svého řešení pro správu Macu.

Další informace o používání součásti app-sso zobrazíte tak, že v Terminálu spustíte příkaz „app-sso -h“.

Mobilní účty – macOS

Rozšíření Kerberos pro SSO nevyžaduje, aby byl Mac provázaný s Active Directory ani aby byl uživatel přihlášený k Macu pomocí mobilního účtu. Apple doporučuje používat rozšíření Kerberos pro SSO s místními účty. Místní účty fungují s doporučeným modelem nasazení macOS nejlépe a jsou nejlepší volbou pro dnešní uživatele Macu, kteří se můžou k síti vaší organizace přihlašovat jen příležitostně. Rozšíření Kerberos pro SSO bylo vytvořené konkrétně za tím účelem, aby vylepšilo integraci místních účtů s Active Directory.

Ale rozšíření Kerberos pro SSO můžete používat, i pokud se rozhodnete nadále používat mobilní účty. Tato funkce má následující požadavky:

- Synchronizace hesel nefunguje s mobilními účty. Když si pomocí rozšíření Kerberos pro SSO změníte heslo k Active Directory a zrovna jste k Macu přihlášení tím uživatelským účtem, který používáte s rozšířením Kerberos pro SSO, bude změna hesel fungovat stejně jako na panelu předvoleb Uživatelé a účty. Ale když provedete externí změnu hesla (jinými slovy, když si změníte heslo na webu nebo vám ho změní technická podpora), nemůže rozšíření Kerberos pro SSO synchronizovat heslo k vašemu mobilnímu účtu s heslem k Active Directory.
- Používání webové adresy pro změnu hesla s rozšířením pro Kerberos a mobilním účtem není podporováno.

Mapování realmu domény

Správce možná bude potřebovat nadefinovat pro Kerberos vlastní mapování realmu domény. Například se může stát, že organizace bude mít v Kerberu realm s názvem „ad.vymyslenafirma.cz“, ale bude potřebovat ověřovat pomocí Kerberu zdroje v doméně „falesnaspolecnost.cz“.

Poznámka: Implementace Kerberu v operačních systémech Apple umí ve většině situací určit mapování realmu domény automaticky. Správce musí tato nastavení upravovat jen ve vzácných případech.

Následujícím postupem můžete u rozšíření Kerberos pro SSO nakonfigurovat mapování realmu domény:

1. V profilu rozšíření Kerberos pro SSO v části Custom Configuration (Vlastní konfigurace) přidejte objekt zvaný domainRealmMapping. Objekt by měl mít typ Dictionary (Slovník).
2. Nastavte proměnnou slovníku na název vašeho realmu psaný velkými písmeny.
3. Nastavte hodnotu slovníku, aby měla typ Array (Pole). První hodnota by měla být název vašeho realmu Kerberu malými písmeny, na začátku s tečkou. Druhá hodnota by měla být název domény, kterou oproti tomuto realmu potřebujete ověřovat, a opět musí začínat tečkou. Podle potřeby přidávejte pole.

Další informace najdete v dokumentaci ke Kerberu.

Přechod z Enterprise Connectu

Přehled

Rozšíření Kerberos pro SSO je zamýšlené jako náhrada Enterprise Connectu, což je podobný nástroj používaný v mnoha organizacích. Většina organizací přecházejících z Enterprise Connectu na rozšíření Kerberos pro SSO se bude řídit následujícím postupem:

1. Sestavte konfigurační profil rozšíření Kerberos pro SSO, který bude zajišťovat podobné funkce jako váš stávající profil Enterprise Connectu.
2. Odinstalujte Enterprise Connect.
3. Nasaďte nový konfigurační profil rozšíření Kerberos pro SSO.
4. Požádejte uživatele, aby se přihlásili k rozšíření Kerberos pro SSO.

Pokud v rámci organizace aktualizujete své Macy na macOS 10.15, není přechod na rozšíření Kerberos pro SSO povinný. Enterprise Connect funguje v macOS 10.15 i nadále. Přesto by organizace měly přechod na Enterprise Connect začít plánovat.

Kdo by přecházet neměl

Rozšíření Kerberos pro SSO splňuje potřeby drtivé většiny organizací, které teď používají Enterprise Connect. Ovšem organizace splňující následující kritéria možná z Enterprise Connectu přejít nemůžou anebo můžou uskutečnit jenom částečný přechod:

- Organizace, které v tuto chvíli používají Macy s macOS 10.14 nebo starším, by měly na těchto systémech nechat běžet Enterprise Connect a na rozšíření Kerberos pro SSO přejít jenom s těmi Macy, které aktualizují na macOS 10.15. Rozšíření Kerberos pro SSO a s ním související konfigurační soubory totiž fungují jenom na Macích s macOS 10.15. Aktualizujte své systémy na macOS 10.15, ať můžete využívat výhody rozšíření Kerberos pro SSO.
- Organizace používající nástroj na správu Macu, který nepodporuje uživatelem schválenou registraci do MDM.
- Organizace, které žádný nástroj na správu nepoužívají.
- Organizace, které používají funkční úroveň Active Directory z Windows Serveru 2003 nebo staršího.

Sestavení konfiguračního profilu rozšíření Kerberos pro SSO

Budete si muset sestavit konfigurační profil rozšíření Kerberos pro SSO, který bude podobný vašemu konfiguračnímu profilu Enterprise Connectu. Spousta proměnných, kterými určujete předvolby (tzv. preference keys) v konfiguračním profilu Enterprise Connectu, má odpovídající ekvivalenty i v konfiguračním profilu rozšíření Kerberos pro SSO. Začněte tím, že si projdete následující tabulku, která popisuje, které proměnné předvoleb v Enterprise Connectu odpovídají kterým proměnným v Kerberos SSO:

Enterprise Connect	Rozšíření Kerberos pro SSO	Poznámky
adRealm	Realm	Název realmu by měl být velkými písmeny.
Automatic login (enabled by default)	allowAutomaticLogin	Přidejte do části Custom Configuration (Vlastní konfigurace). Musí být nastaveno na True, aby automatické přihlašování fungovalo.
disablePasswordFunctions	allowPasswordChange	Přidejte do části Custom Configuration (Vlastní konfigurace). Nastavením na False znemožníte změny hesel.
passwordChangeURL	pwChangeURL	Přidejte do části Custom Configuration (Vlastní konfigurace).
passwordExpireOverride	pwExpireOverride	Přidejte do části Custom Configuration (Vlastní konfigurace).
passwordNotificationDays	pwNotificationDays	Přidejte do části Custom Configuration (Vlastní konfigurace).
prepopulatedUsername	principalName	Přidejte do části Custom Configuration (Vlastní konfigurace).
pwReqComplexity	pwReqComplexity	Přidejte do části Custom Configuration (Vlastní konfigurace).
pwReqHistory	pwReqHistory	Přidejte do části Custom Configuration (Vlastní konfigurace).
pwReqLength	pwReqLength	Přidejte do části Custom Configuration (Vlastní konfigurace).
pwReqMinimumPasswordAge	pwReqMinAge	Přidejte do části Custom Configuration (Vlastní konfigurace).
pwReqText	pwReqText	Přidejte do části Custom Configuration (Vlastní konfigurace). Zadejte textový řetězec, který se má zobrazit místo cesty k RTF souboru.
syncLocalPassword	syncLocalPassword	Přidejte do části Custom Configuration (Vlastní konfigurace).

Poznámka: Některé proměnné předvoleb, které používáte v konfiguraci Enterprise Connectu, tu nemusí být uvedené. Třeba odkazují na funkce, které v rozšíření Kerberos pro SSO nejsou potřeba nebo které už nejsou podporovány.

Odinstalování Enterprise Connectu

Používání rozšíření Kerberos pro SSO souběžně s Enterprise Connectem na stejném počítači není podporováno. Až přejdete na rozšíření Kerberos pro SSO, odinstalujte Enterprise Connect. K odinstalování budete potřebovat správcovská oprávnění. Enterprise Connect můžete odinstalovat tímto postupem:

Enterprise Connect 2.0 a novější

1. Odnačtěte agent Enterprise Connectu tím, že otevřete aplikaci Terminál a jako aktuálně přihlášený uživatel spustíte příkaz „launchctl unload /Library/LaunchAgents/com.apple.ecAgent".
2. Zavřete ikonu nabídky Enterprise Connect tím, že v Terminálu spustíte příkaz „killall Enterprise\ Connect\ Menu".
3. Smažte aplikaci Enterprise Connect ze složky Aplikace.
4. Smažte spouštěcí soubor .plist Enterprise Connectu, uložený v umístění /Knihovna/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 a starší

1. Ukončete Enterprise Connect tím, že v Terminálu spustíte příkaz „killall Enterprise\ Connect".
2. Smažte aplikaci Enterprise Connect ze složky Aplikace.

V příloze najdete ukázku skriptu, který odstraní jakoukoli verzi Enterprise Connectu.

Spouštěče skriptů Enterprise Connectu

Enterprise Connect umí spouštět skripty, když dojde k určitým událostem. Například může Enterprise Connect spustit skript pokaždé, když dokončí proces připojování nebo když si uživatel změní heslo. Rozšíření Kerberos pro SSO pracuje se skripty jinak než Enterprise Connect. Samo rozšíření žádné skripty nespouští. Když dojde k určené události, pošle místo toho distribuované oznámení, na které může čekat jiný proces – a ten potom spustí skript. Podrobnosti se dočtete v tomto dokumentu v části Pokročilé funkce.

V následující tabulce jsou uvedené spouštěče skriptů Enterprise Connectu a jejich ekvivalentní distribuovaná oznámení v rozšíření Kerberos pro SSO:

Enterprise Connect	Rozšíření Kerberos pro SSO
auditScriptPath	com.apple.KerberosPlugin.InternalNetworkAvailable
connectionCompletedScriptPath	com.apple.KerberosPlugin.ConnectionCompleted
passwordChangeScriptPath	com.apple.KerberosPlugin.ADPasswordChanged

Sdílené síťové zdroje

Rozšíření Kerberos pro SSO nepodporuje práci se sdílenými síťovými zdroji, jako je například uživatelova síťová domovská složka. Většinu těchto funkcí můžete nahradit skripty.

Příloha

Profil správy zařízení: ExtensibleSingleSignOnKerberos

developer.apple.com/documentation/devicemanagement/extensiblesinglesignonkerberos?language=objc

Referenční materiály k protokolu MDM

developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf

Profil správy zařízení: ExtensibleSingleSignOnKerberos.ExtensionData

developer.apple.com/documentation/devicemanagement/extensiblesinglesignonkerberos/extensiondata?language=objc

Ukázkový skript – Vyhodnocování distribuovaných oznámení

Rozšíření Kerberos pro SSO rozesílá distribuovaná oznámení při různých událostech, například když si uživatel změní heslo nebo když se zařízení připojí k firemní síti. Jako správce můžete pomocí skriptu nebo aplikace těmto oznámením naslouchat, a jakmile budou přijata, provést určenou akci – třeba spustit skript nebo příkaz shellu.

Dole je uvedený ukázkový skript, který umí při příjmu oznámení spouštět skripty nebo příkazy. Měli byste ho spouštět jako LaunchAgent, pokud se má spustit s oprávněními přihlášeného uživatele, nebo jako LaunchDaemon, pokud se má spustit s kořenovými oprávněními. Skript vyžaduje dva parametry:

- **-notification** je název distribuovaného oznámení, na které má čekat. Příklady najdete na straně 11.
- **-action** je akce, kterou má při příjmu distribuovaného oznámení provést. Příkladem je třeba „sh /path/to/script.sh.“

Abyste mohli skript spouštět, musíte si nainstalovat vývojářské nástroje příkazového řádku. Jejich instalátor najdete na webu Apple Developer.

```
#!/usr/bin/swift

import Foundation

class NotifyHandler {

    // Akce, kterou chceme spustit, třeba shellový příkaz nebo skript
    public var action = String()

    // Spustí se pokaždé, když přijme určené distribuované
    // oznámení
    @objc func gotNotification(notification: NSNotification){
        let task = Process()
        task.launchPath = "/bin/zsh"
        task.arguments = ["-c", action]
        task.launch()
    }
}

// HLAVNÍ ČÁST

let scriptPath: String = CommandLine.arguments.first!

// -notification je název oznámení, na které čekáme
guard let notification = UserDefaults.standard.string(forKey: "notification") else {
    print("\(scriptPath): Neurčeno žádné oznámení. Skript se ukončí…")
    exit(1)
}

// -action je akce, kterou chceme spustit. Může jít o shellový

// příkaz, skript atd.
```

```
guard let action = UserDefaults.standard.string(forKey: "action") else {
    print("\(scriptPath): Neurčena žádná akce. Skript se ukončí…")
    exit(1)
}

let nh = NotifyHandler()
nh.action = action

print("Akce je \(nh.action) a oznámení je \(notification)")

// Čeká na určené oznámení
DistributedNotificationCenter.default().addObserver(
    nh,
    selector: #selector(nh.gotNotification),
    name: NSNotification.Name(rawValue: notification),
    object: action)

RunLoop.main.run()
```

Ukázkový skript – Odinstalování Enterprise Connectu

Tento ukázkový skript odstraní jakoukoli verzi Enterprise Connectu. Spusťte ho z nástroje na správu Macu nebo ručně. Skript musíte spustit s kořenovými oprávněními.

```
#!/bin/zsh

# Odnačte pomocný nástroj Kerberu z verzí EC před 1.6
if [[ -e /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist ]]; then
  launchctl bootout system /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist
  rm /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist
fi

# Odstraní privilegovaný pomocný nástroj z verzí EC před 1.6
if [[ -e /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper ]]; then
  rm /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper
fi

# Odstraní z databáze záznam o autorizaci z verzí EC před 1.6
/usr/bin/security authorizationdb read com.apple.Enterprise-Connect.writeKDCs > /dev/null

if [[ $? -eq 0 ]]; then
  security authorizationdb remove com.apple.Enterprise-Connect.writeKDCs
fi

if [[ -e /Library/LaunchAgents/com.apple.ecAgent.plist ]]; then
  # Je nainstalovaný Enterprise Connect 2.0 nebo novější
  # Odnačteme přihlášenému uživateli agenta ecAgent a odstraníme ho z launchd

  loggedInUser=$(scutil <<< "show State:/Users/ConsoleUser" | awk '/Name :/ && ! /loginwindow/ { print $3 }')
  loggedInUID=$(id -u $loggedInUser)

  launchctl bootout gui/$loggedInUID /Library/LaunchAgents/com.apple.ecAgent.plist
  rm /Library/LaunchAgents/com.apple.ecAgent.plist

  # Vyhodíme ikonu z nabídky
  killall "Enterprise Connect Menu"
fi

# Nakonec odstraníme balíček aplikací Enterprise Connect
rm -rf /Applications/Enterprise\ Connect.app
```