Estensione Single Sign-On Kerberos

Guida per l'utente

Dicembre 2019

Indice

Introduzione

L'estensione Single Sign-On (SSO) Kerberos semplifica il Single Sign-On con Kerberos sui dispositivi Apple della tua organizzazione.

Autenticazione Kerberos semplificata

L'estensione SSO Kerberos semplifica il processo di acquisizione di un Ticket Granting Ticket (TGT) di Kerberos da parte del dominio Active Directory dell'organizzazione, consentendo agli utenti di autenticarsi con facilità per accedere a risorse come siti web, app e file server. Su macOS, l'estensione SSO Kerberos acquisisce in modo proattivo un TGT di Kerberos a ogni cambiamento dello stato delle rete, così che l'utente sia subito pronto ad autenticarsi quando serve.

Gestione degli account Active Directory

L'estensione SSO Kerberos aiuta inoltre gli utenti a gestire i propri account Active Directory. Su macOS, consente agli utenti di modificare la password di Active Directory e li avvisa quando sta per scadere. Gli utenti possono anche modificare la password del loro account locale in modo che corrisponda a quella di Active Directory.

Supporto per Active Directory

L'estensione SSO Kerberos dovrebbe essere usata con un dominio Active Directory locale. Azure Active Directory non è supportato. Per usare l'estensione SSO Kerberos, non è necessario associare i dispositivi a un dominio Active Directory. Inoltre gli utenti non hanno bisogno di accedere ai propri computer Mac con Active Directory o con gli account mobili; al contrario, Apple consiglia l'utilizzo di account locali.

Requisiti

- iOS 13, iPadOS o macOS Catalina.
- Un dominio Active Directory con Windows Server 2008 o successivo. L'estensione SSO Kerberos non è pensata per essere utilizzata con Azure Active Directory; richiede un tradizionale dominio Active Directory locale.
- Accesso alla rete su cui è ospitato il dominio Active Directory. L'accesso alla rete può essere effettuato tramite Wi-Fi, Ethernet o VPN.
- I dispositivi devono essere gestiti con una soluzione di gestione dei dispositivi mobili (Mobile Device Management, MDM) che supporta il payload del profilo di configurazione Extensible Single Sign-On (SSO). Contatta il fornitore della soluzione MDM per chiedere se questo payload del profilo di configurazione è supportato.

Enterprise Connect

L'estensione SSO Kerberos è pensata per sostituire Enterprise Connect. Se al momento la tua organizzazione usa Enterprise Connect e vuole passare all'estensione SSO Kerberos, fai riferimento alla sezione "Transizione da Enterprise Connect" di questo documento per maggiori informazioni.

Per cominciare

Sviluppare e distribuire un profilo di configurazione

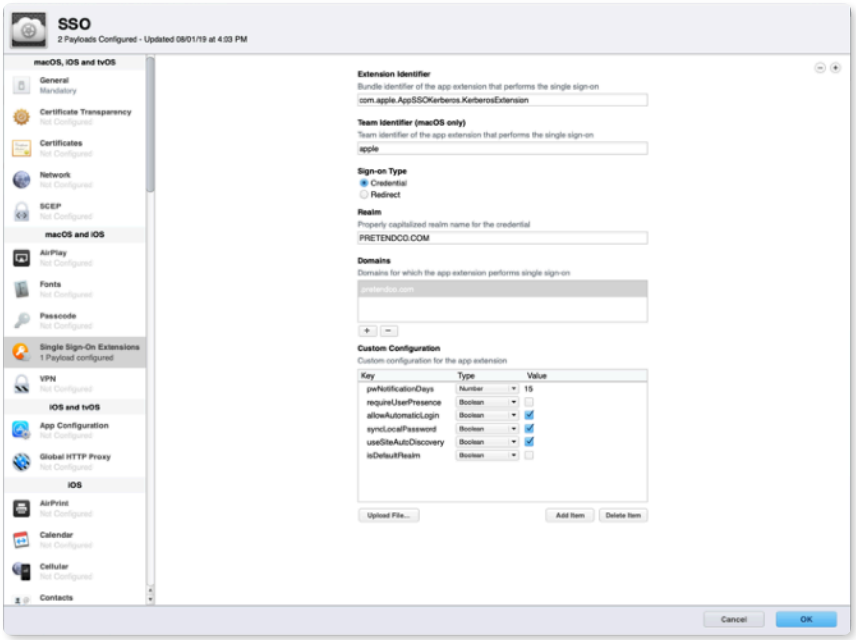
Per utilizzare l'estensione SSO Kerberos, occorre prima configurarla usando un profilo di configurazione, inviato al dispositivo tramite una soluzione MDM.

Nota: il profilo di configurazione deve essere inviato al dispositivo tramite una soluzione MDM. Su macOS, deve trattarsi di una registrazione MDM approvata dall'utente e installata nel sistema. Non è possibile aggiungere manualmente il profilo.

Per la configurazione mediante profilo di configurazione, devi usare il payload Extensible Single Sign-On introdotto in iOS 13, iPadOS e macOS 10.15. Profile Manager, che fa parte di macOS Server, include il supporto per il payload Extensible Single Sign-On. Se la soluzione MDM non supporta ancora questo payload, dovresti poter creare il profilo necessario in Profile Manager e poi importarlo nella tua soluzione MDM per la distribuzione. Per maggiori informazioni, contatta il fornitore MDM.

Per creare un profilo di configurazione usando Profile Manager, segui questi passaggi:

1. Accedi a Profile Manager.
2. Crea un profilo per un gruppo di dispositivi o un dispositivo specifico.
3. Seleziona le estensioni Single Sign-On nell'elenco dei payload, quindi fai clic sul pulsante di aggiunta (+) per aggiungere un nuovo payload.
4. Nel campo Extension Identifier, inserisci "com.apple.AppSSOKerberos.KerberosExtension".
5. Nel campo Team Identifier, inserisci "apple".



6. In Sign-on Type, seleziona Credential.
7. Nel campo Realm, inserisci il nome del dominio Active Directory in cui risiedono gli account utente dell'organizzazione, tutto in maiuscolo. Non usare il nome della foresta di Active Directory, a meno che gli account utente non si trovino a quel livello.

8. In Domains, fai clic sul pulsante con il segno + e aggiungi i domini di tutte le risorse che utilizzano Kerberos. Per esempio, se usi l'autenticazione Kerberos con le risorse in us.pretendco.com, aggiungi ".us.pretendco.com" (non dimenticare il punto iniziale).
9. In Custom Configuration, aggiungi i seguenti valori:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Non verificato
allowAutomaticLogin	Boolean	Verificato
syncLocalPassword	Boolean	Verificato
useSiteAutoDiscovery	Boolean	Verificato
isDefaultRealm	Boolean	Non verificato

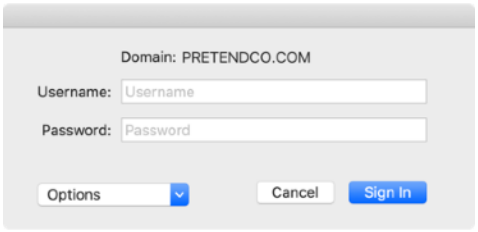
10. Fai clic su OK per salvare il nuovo profilo di configurazione. Verrà automaticamente installato sul dispositivo o sul gruppo di dispositivi selezionato.

Configurazione utente – iOS e iPadOS

1. Collega il tuo dispositivo a una rete in cui è disponibile il dominio Active Directory dell'organizzazione.
2. Scegli come procedere.
   - Usa Safari per accedere a un sito web che supporta l'autenticazione Kerberos.
   - Apri un'app che supporta l'autenticazione Kerberos.
3. Inserisci il nome utente e la password di Kerberos o di Active Directory.
4. Ti verrà chiesto se effettuare sempre l'accesso in automatico. La maggior parte degli utenti sceglie Yes.
5. Tocca Sign In. Dopo una breve pausa, verrà caricato il tuo sito web o la tua app. Se scegli di accedere automaticamente all'estensione SSO Kerberos, non ti verranno più chieste le credenziali fino a quando non modifichi la password. In caso contrario, dovrai immettere le credenziali Kerberos solo quando scadono (in genere dopo 10 ore).

Configurazione dell'utente - macOS

1. Devi autenticarti nell'estensione SSO Kerberos. Puoi iniziare la procedura in diversi modi:
   - Se il tuo Mac è connesso alla rete in cui è disponibile il dominio Active Directory, ti verrà chiesto di autenticarti subito dopo che è stato installato il profilo di configurazione Extensible SSO.
   - Se usi Safari per accedere a un sito web che accetta l'autenticazione Kerberos oppure usi un'app che la richiede, ti verrà chiesto di autenticarti.
   - Ti verrà immediatamente chiesto di autenticarti ogni volta che connetti il Mac a una rete in cui è disponibile Active Directory.
   - Puoi selezionare il menu extra dell'estensione SSO Kerberos e poi cliccare Sign In.
2. Ti verranno chieste le credenziali Kerberos. Inserisci il nome utente e la password di Kerberos o di Active Directory.



3. Ti verrà chiesto se vuoi accedere in automatico. La maggior parte degli utenti seleziona Yes.
4. Fai clic su Sign In. Dopo una breve pausa, verrà caricato il tuo sito web o la tua app. Se scegli di accedere automaticamente all'estensione SSO Kerberos, non ti verranno più chieste le credenziali fino a quando non modifichi la password. In caso contrario, ti verrà chiesto di immettere le credenziali Kerberos solo quando scadono, in genere dopo 10 ore.
5. Se la tua password sta per scadere, riceverai una notifica che ti informa dei giorni che mancano alla scadenza. Puoi fare clic sulla notifica per cambiare la password.
6. Se hai attivato la funzione di sincronizzazione delle password, ti verranno chieste la password Active Directory e la password locale attuale. Inseriscile entrambe e poi fai clic su OK per sincronizzarle. Vedrai questa richiesta al momento dell'accesso iniziale, anche se le tue password sono già sincronizzate.

Modifica della password - macOS

Puoi anche cambiare la password Active Directory con l'estensione SSO Kerberos:

1. Verifica di aver effettuato l'accesso all'estensione SSO Kerberos.
2. Seleziona il menu extra dell'estensione SSO Kerberos e scegli Change Password. Potresti inoltre ricevere una notifica che ti avvisa che la password sta per scadere.
3. Inserisci prima la tua password attuale e poi quella nuova. Assicurati di usare una nuova password che soddisfi i requisiti della tua organizzazione. Fai clic su OK.
4. Dopo una breve pausa, vedrai una finestra che ti avvisa che la password è stata cambiata. Se la funzione di sincronizzazione delle password è attiva, la password del tuo account locale verrà aggiornata in modo da corrispondere alla nuova password Active Directory.

Usare il menu extra dell’estensione SSO Kerberos – macOS

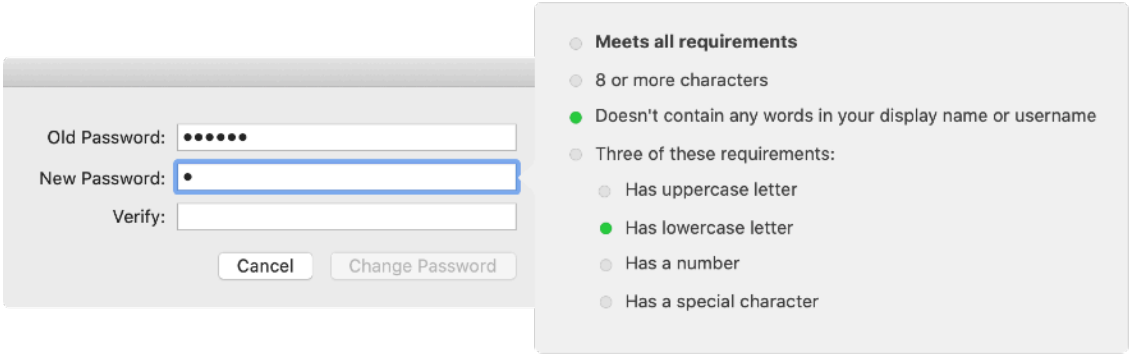
Il menu extra dell’estensione SSO Kerberos permette di accedere facilmente a informazioni utili sul tuo account e sulle funzioni dell’estensione. Viene visualizzato come una chiave grigia o nera nella barra dei menu in alto a destra.

Per ottenere informazioni di stato sul tuo account, inizia controllando il colore dell’icona del menu extra dell’estensione SSO Kerberos. Se è grigia, non hai effettuato l’accesso all’estensione. Se è nera, hai effettuato l’accesso. Dopo aver selezionato la chiave, vedrai l’account con cui hai effettuato l’accesso, nonché quanti giorni ti restano prima che la password scada. Da questo menu puoi anche di connetterti e disconnetterti dall’account e cambiare la password.

Funzioni avanzate

Testing delle password in tempo reale

In molte configurazioni Active Directory, l'estensione SSO Kerberos può testare la validità delle nuove password mentre gli utenti le inseriscono, indicando i requisiti da rispettare. Dopo aver configurato il testing, l'utente visualizzerà questa schermata:



Per usare questa funzione, il tuo dominio Active Directory deve usare solo i criteri per le password standard di Active Directory. Per impostazione predefinita, Active Directory consente agli amministratori di richiedere che una password sia complessa e abbia una determinata lunghezza. Per sapere cosa si intende per "password complessa", vedi technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Nota: potresti non essere in grado di usare questa funzione se il tuo dominio utilizza strumenti di terze parti o file Dynamic Link Library (DLL) per estendere i criteri per la password standard di Active Directory. Per esempio, se non puoi utilizzare determinate parole diverse dal nome utente nella password, o devi usare un numero specifico di caratteri speciali, probabilmente stai usando estensioni per i criteri delle password di terze parti. Se hai dubbi, chiedi delucidazioni all'amministratore di Active Directory.

Se il dominio Active Directory della tua organizzazione soddisfa i requisiti, puoi attivare il testing delle password in tempo reale. Nel profilo di configurazione della tua estensione SSO Kerberos, imposta i seguenti parametri:

Parametro	Key	Type	Value	Facoltativo
Richiedere password complesse	pwReqComplexity	Boolean	SÌ	No
Richiedere lunghezza password	pwReqLength	Integer	Numero	Sì
Riutilizzare limite di password precedente	pwReqHistory	Integer	Numero	Sì
Richiedere età minima per la password	pwReqMinAge	Integer	Numero	Sì

Il testing delle password in tempo reale presenta alcune limitazioni. Per esempio, non è in grado di verificare se una password è già stata usata o se contiene il nome visualizzato in Active Directory nel caso tu non abbia un TGT di Kerberos. Questa situazione può presentarsi quando imposti la password per la prima volta o se la password è scaduta. Tutti gli altri test funzioneranno normalmente.

Visualizzazione dei requisiti per la password

Se non puoi usare il testing delle password in tempo reale, puoi configurare l'estensione SSO in modo da mostrare una stringa di testo con i requisiti mentre gli utenti inseriscono una nuova password. Nel profilo di configurazione dell'estensione SSO Kerberos, imposta come "pwReqText" una stringa contenente il testo che vuoi mostrare all'utente mentre cambia la password.

Modificare o disattivare le funzionalità relative alle password

Alcune organizzazioni potrebbero non essere in grado di usare la funzionalità standard di modifica della password fornita dall'estensione SSO Kerberos, in quanto non consentono di cambiare la password di Active Directory. Nel tuo profilo di configurazione dell'estensione SSO Kerberos, imposta "allowPasswordChanges" su FALSE per disattivare questa funzionalità.

Supporto delle pagine web per la modifica della password – macOS

L'estensione SSO Kerberos può essere configurata in modo da aprire pagine web per la modifica della password nel browser predefinito quando l'utente seleziona "Cambia password" o conferma un messaggio sulla scadenza della password. Apple consiglia di utilizzare questa funzione solo quando si usa un account locale, in quanto gli account mobili non sono supportati.

Nel profilo di configurazione dell'estensione SSO Kerberos, imposta come "pwChangeURL" l'URL del sito web di modifica della password. Una volta che gli utenti hanno modificato la password, devono disconnettersi dall'estensione Kerberos e accedere nuovamente con la password aggiornata. Se la sincronizzazione delle password locali è attiva, gli utenti ricevono istruzioni per sincronizzare nuovamente le password.

Sincronizzazione delle password – macOS

L'estensione SSO Kerberos può impostare la password dell'account locale in modo che corrisponda alla password Active Directory dell'utente. Attiva questa funzione impostando "syncLocalPassword" su TRUE nella sezione Custom Configuration del profilo di configurazione dell'estensione SSO Kerberos.

La sincronizzazione delle password svolge due funzioni di base. Prima di tutto, quando l'utente usa l'estensione SSO Kerberos per cambiare le password, questa funzione imposta la password locale in modo che corrisponda a quella di Active Directory. Se la password dell'account locale e quella di Active Directory non dovessero più essere sincronizzate, l'estensione SSO Kerberos ripristina la sincronizzazione nel seguente modo:

- Al momento dell'attivazione della sincronizzazione delle password e a ogni successivo tentativo di connessione all'estensione SSO Kerberos, le date dell'ultima modifica delle password dell'account locale e di Active Directory vengono confrontate ai valori nella cache. Se i valori corrispondono, le password vengono sincronizzate e non è richiesta alcuna azione. Se non corrispondono, l'estensione SSO Kerberos chiederà all'utente di inserire le password dell'account locale e di Active Directory. Una volta che l'utente ha fornito la password locale, l'estensione SSO Kerberos la imposta in modo che corrisponda a quella di Active Directory.
- La modifica della password funziona in un modo simile. Quando l'utente cambia la password con l'estensione SSO Kerberos, la vecchia password di Active Directory verrà confrontata con quella dell'account locale. Se la nuova password locale corrisponde a una vecchia password di Active Directory, l'estensione SSO Kerberos le cambia entrambe. Se non corrispondono, viene cambiata solo la password di Active Directory. All'utente viene poi chiesto di inserire la password locale durante il successivo tentativo di connessione.

Questa funzione presenta i seguenti requisiti:

- Se gli utenti hanno effettuato l'accesso ai loro computer Mac con l'account Active Directory e non con quello locale, la sincronizzazione delle password viene disattivata. Questa funzione è pensata per essere utilizzata solo con gli account locali; se gli utenti hanno effettuato l'accesso ai loro computer Mac con gli account Active Directory, la funzione non è necessaria.
- Se negli account locali viene applicato un criterio per la password, per esempio usando un profilo di configurazione o il comando pwpolicy, assicurati che il criterio per la password locale corrisponda a quello di Active Directory o sia meno rigido di quest'ultimo. Se il criterio per la password locale è più rigido rispetto a quello di Active Directory, l'estensione SSO Kerberos può accettare una password che soddisfi i requisiti di Active Directory, ma non riesce a impostare la password locale, poiché non rispetta i requisiti per le password locali. È sconsigliato usare questa funzione se il criterio per la password locale deve essere più rigido rispetto a quello di Active Directory.
- Il nome utente locale è diverso da quello di Active Directory; solo le password sono impostate in modo da corrispondere.

Supporto per smart card – macOS

L'estensione SSO Kerberos supporta l'uso di identità basate su smart card per l'autenticazione. Le smart card devono avere un driver CryptoTokenKit disponibile; non sono supportati i driver basati su tokenD. macOS 10.15 include il supporto per lo standard Personal Identity Verification (PIV), ampiamente utilizzato dal governo statunitense.

Prima di iniziare, assicurati che il tuo dominio Active Directory sia configurato in modo da supportare l'autenticazione tramite smart card. La procedura per attivare l'autenticazione ad Active Directory tramite smart card esula dallo scopo di questo documento. Per maggiori informazioni, fai riferimento alla documentazione Microsoft.

Per accedere all'estensione SSO Kerberos con una smart card, segui questi passaggi:

1. Fai clic sul menu Options, quindi seleziona "Use a smart card".
2. Quando vedi il pulsante Identity, inserisci la smart card e fai clic sul pulsante.
3. Scegli l'identità con cui vuoi autenticarti, fai clic su OK e poi su Sign In.
4. Inserisci il PIN quando ti viene chiesto.

Se l'estensione SSO Kerberos ha bisogno di acquisire un TGT di Kerberos, ti verrà chiesto di inserire la tua smart card e il tuo PIN. Sono disponibili maggiori informazioni sulla compatibilità della smart card in macOS eseguendo "man SmartCardServices" in Terminale.

Notifiche distribuite – macOS

L'estensione SSO Kerberos pubblica notifiche distribuite quando si verificano diversi eventi. In macOS, le app e i servizi usano le notifiche distribuite per comunicare ad altri servizi e app che si è verificato un evento. In questo modo, un'app o un servizio in ascolto di questo evento può intraprendere delle azioni quando si verifica.

Un amministratore può usare questa funzionalità per eseguire alcune azioni quando si verificano determinati eventi. Per esempio, un amministratore potrebbe voler eseguire uno script ogni volta che l'estensione SSO Kerberos acquisisce una nuova credenziale di Kerberos.

L'estensione SSO Kerberos si limita semplicemente a pubblicare notifiche distribuite quando si verificano degli eventi specifici, ma non esegue alcuna azione. L'amministratore deve fornire uno strumento per restare in ascolto di queste notifiche ed eseguire azioni quanto si verificano gli eventi.

L'appendice contiene un esempio di uno script e una property list launchD (.plist) che possono restare in ascolto di notifiche ed eseguire azioni. Modifica questo esempio come necessario in base alla tua distribuzione.

Qui sotto trovi le notifiche distribuite pubblicate dall'estensione SSO Kerberos.

Nome	Quando viene pubblicata
com.apple.KerberosPlugin.ConnectionCompleted	L'estensione SSO Kerberos ha eseguito la sua procedura di connessione.
com.apple.KerberosPlugin.ADPasswordChanged	L'utente ha cambiato la password di Active Directory con l'estensione.
com.apple.KerberosPlugin.LocalPasswordSynced	L'utente ha sincronizzato le password di Active Directory e dell'account locale.
com.apple.KerberosPlugin.InternalNetworkAvailable	L'utente si è collegato a una rete su cui è disponibile il dominio Active Directory configurato.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	L'utente si è collegato a una rete su cui non è disponibile il dominio Active Directory configurato.
com.apple.KerberosExtension.gotNewCredential	L'utente ha acquisito un nuovo TGT di Kerberos.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	L'utente ha cambiato la password Active Directory e la password locale è stata aggiornata in modo da corrispondere alla nuova password di Active Directory.

Supporto della riga di comando – macOS

Gli amministratori possono usare uno strumento a riga di comando chiamato *app-sso* per controllare l'estensione SSO Kerberos e accedere a informazioni utili. Per esempio, possono usare lo strumento per avviare login, modifiche di password e logout. Lo strumento può anche stampare informazioni utili, come l'utente attualmente connesso, il sito Active Directory attuale del computer, la condivisione principale della rete dell'utente, quando scade la password dell'utente, e una tante altre informazioni utili nel formato property list o JSON. Questa informazione può essere analizzata e caricata su una soluzione di gestione del Mac per scopi di inventario, ma non solo.

Per maggiori informazioni sull'utilizzo di app-sso, esegui "app-sso -h" nell'app Terminale.

Account mobili – macOS

L'estensione SSO Kerberos non richiede che il Mac sia vincolato ad Active Directory o che l'utente abbia effettuato l'accesso al Mac con un account mobile. Apple consiglia di usare l'estensione SSO Kerberos con un account locale. Gli account locali funzionano meglio con il modello di distribuzione consigliato per macOS, e sono la scelta migliore per gli utenti Mac odierni, che potrebbero connettersi in modo intermittente alla rete dell'organizzazione. L'estensione SSO Kerberos è stata specificatamente creata per migliorare l'integrazione di Active Directory da un account locale.

Tuttavia, anche se dovessi scegliere di continuare a usare gli account mobili, puoi comunque utilizzare l'estensione SSO Kerberos. Questa funzione presenta i seguenti requisiti:

- La sincronizzazione delle password non funziona con gli account mobili. Se usi l'estensione SSO Kerberos per cambiare la password dell'account Active Directory e hai effettuato l'accesso al Mac con lo stesso account utente che stai usando con tale estensione, la modifica della password funziona allo in modo analogo a quella del pannello delle preferenze Users & Groups. Tuttavia, se modifichi una password esterna, ovvero se cambi la password su un sito web o se la modifica viene apportata dall'help desk, l'estensione SSO Kerberos non può ripristinare la sincronizzazione tra la password dell'account mobile e quella di Active Directory.
- Non è possibile usare un URL di modifica della password con l'estensione di Kerberos e un account mobile.

Mappatura dominio/realm

Un amministratore potrebbe dover definire una mappatura dominio/realm per Kerberos. Per esempio, un'organizzazione potrebbe avere un realm Kerberos chiamato "ad.pretendco.com", ma potrebbe dover utilizzare l'autenticazione Kerberos per le risorse nel dominio "fakecompany.com".

Nota: l'implementazione di Kerberos sui sistemi operativi Apple può determinare automaticamente la mappatura dominio/realm in quasi tutte le situazioni. È molto raro che un amministratore personalizzi queste impostazioni.

La mappatura dominio/realm può essere configurata per l'estensione SSO Kerberos seguendo questi passaggi:

1. Nella sezione Custom Configuration del profilo Extensible SSO, aggiungi un oggetto chiamato domainRealmMapping. Il tipo di oggetto dovrebbe essere Dictionary.
2. Imposta il nome in maiuscole del tuo realm come chiave di questo dizionario.
3. Imposta Array come tipo di valore di questo dizionario. Il primo valore dovrebbe corrispondere al nome del tuo realm Kerberos (in minuscolo, preceduto da un punto). Il secondo valore dovrebbe corrispondere al nome del dominio che deve essere autenticato rispetto a questo realm (anche in questo caso con un punto all'inizio). Aggiungi array in base alla necessità.

Per maggiori informazioni, fai riferimento alla documentazione Kerberos.

Transizione da Enterprise Connect

Panoramica

L'estensione SSO Kerberos è pensata per sostituire Enterprise Connect, uno strumento simile già utilizzato da molte organizzazioni. La maggior parte delle organizzazioni che passa da Enterprise Connect all'estensione SSO Kerberos svolgerà questa procedura:

1. Creare un profilo di configurazione per l'estensione SSO Kerberos che fornisca una funzionalità simile a quella dell'attuale profilo Enterprise Connect.
2. Disinstallare Enterprise Connect.
3. Distribuire il nuovo profilo di configurazione dell'estensione SSO Kerberos.
4. Chiedere agli utenti di accedere all'estensione SSO Kerberos.

Per passare all'estensione SSO Kerberos non è necessario aggiornare i computer Mac dell'organizzazione a macOS 10.15. Enterprise Connect funziona correttamente con macOS 10.15, ma le organizzazioni dovrebbero comunque pianificare un'eventuale transizione da Enterprise Connect.

Chi non dovrebbe effettuare la transizione

L'estensione SSO Kerberos soddisferà le esigenze della maggior parte delle organizzazioni che usano Enterprise Connect. Tuttavia, le organizzazioni con i seguenti scenari potrebbero non essere in grado di effettuare la transizione da Enterprise Connect o riuscire a effettuare solo una transizione parziale:

- Le organizzazioni che dispongono di Mac con macOS 10.14 o versioni precedenti dovrebbero continuare a usare Enterprise Connect su questi sistemi ed effettuare la transizione all'estensione SSO Kerberos solo sui Mac con macOS 10.15. L'estensione SSO Kerberos e il profilo di configurazione associato funzioneranno solo sui computer Mac con macOS 10.15. Aggiorna questi sistemi a macOS 10.15 per utilizzare l'estensione SSO Kerberos.
- Le organizzazioni che utilizzano uno strumento di gestione del Mac che non supporta la registrazione MDM approvata dall'utente.
- Le organizzazioni che non usano uno strumento di gestione.
- Le organizzazioni che usano un livello di funzionalità di Active Directory di Windows Server 2003 o versioni precedenti.

Creare un profilo di configurazione dell'estensione SSO Kerberos

Dovrai creare un profilo di configurazione per l'estensione SSO Kerberos che sia simile al profilo di configurazione di Enterprise Connect. Molte preference key del tuo attuale profilo Enterpise Connect hanno degli equivalenti nel profilo dell'estensione SSO Kerberos. Per prima cosa, consulta la tabella qui sotto, che contiene una mappa delle preference key dell'estensione SSO Kerberos equivalenti a quelle di Enterprise Connect:

Enterprise Connect	Estensione SSO Kerberos	Note
adRealm	Realm	Il realm deve essere scritto completamente in maiuscolo.
Automatic login (enabled by default)	allowAutomaticLogin	Aggiungilo alla sezione Custom Configuration. Deve essere impostato su True affinché il login automatico funzioni.
disablePasswordFunctions	allowPasswordChange	Aggiungilo alla sezione Custom Configuration. Imposta su False per disattivare le modifiche alla password.
passwordChangeURL	pwChangeURL	Aggiungilo alla sezione Custom Configuration.
passwordExpireOverride	pwExpireOverride	Aggiungilo alla sezione Custom Configuration.
passwordNotificationDays	pwNotificationDays	Aggiungilo alla sezione Custom Configuration.
prepopulatedUsername	principalName	Aggiungilo alla sezione Custom Configuration.
pwReqComplexity	pwReqComplexity	Aggiungilo alla sezione Custom Configuration.
pwReqHistory	pwReqHistory	Aggiungilo alla sezione Custom Configuration.
pwReqLength	pwReqLength	Aggiungilo alla sezione Custom Configuration.
pwReqMinimumPasswordAge	pwReqMinAge	Aggiungilo alla sezione Custom Configuration.
pwReqText	pwReqText	Aggiungilo alla sezione Custom Configuration. Fornisci una stringa di testo da visualizzare invece di un percorso a un file RTF.
syncLocalPassword	syncLocalPassword	Aggiungilo alla sezione Custom Configuration.

Nota: alcune preference key del tuo profilo di configurazione Enterprise Connect potrebbero non essere elencate qui perché fanno riferimento a funzionalità che non sono più necessarie nell'estensione SSO Kerberos o che non sono più supportate.

Disinstallare Enterprise Connect

Non è possibile eseguire contemporaneamente l'estensione SSO Kerberos e Enterprise Connect sullo stesso computer. Dopo aver effettuato la transizione all'estensione SSO Kerberos, disinstalla Enterprise Connect. Ti serviranno i diritti amministrativi per effettuare la disinstallazione. Per disinstallare Enteprise Connect, segui i passaggi di seguito:

Enterprise Connect 2.0 e versioni successive

1. Per scaricare l'agent Enterprise Connect, apri l'app Terminale ed esegui "launchctl unload /Library/LaunchAgents/com.apple.ecAgent" come utente attualmente connesso.
2. Per uscire dal menu extra di Enterprise Connect, apri l'app Terminale e inserisci "killall Enterprise\ Connect\ Menu" nell'app Terminale.
3. Cancella l'app Enterprise Connect dalla cartella Applications.
4. Cancella il file .pilst launchd di Enterprise Connect in /Library/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 e versioni precedenti

1. Esci da Enterprise Connect inserendo "killall Enterprise\ Connect" nell'app Terminale.
2. Cancella l'app Enterprise Connect dalla cartella Applications.

L'appendice fornisce uno script di esempio che rimuove qualsiasi versione di Enterprise Connect.

Attivatori dello script di Enterprise Connect

Enterprise Connect può eseguire script quando si verificano determinati eventi. Per esempio, può eseguire uno script quando completa la procedura di connessione o quando un utente cambia la password. L'estensione SSO Kerberos gestisce gli script in modo diverso da Enterprise Connect. Infatti, non esegue direttamente gli script, ma pubblica una notifica distribuita quando si verifica un evento; in questo modo, un altro processo può restare in ascolto ed eseguire lo script. Per maggiori dettagli, vedi la sezione "Funzioni avanzate" di questo documento.

Qui sotto trovi riferimenti sugli attivatori di script di Enterprise Connect e sulle notifiche distribuite equivalenti nell'estensione SSO Kerberos.

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

Condivisioni di rete

L'estensione SSO Kerberos non supporta la gestione delle condivisioni di rete, come la directory home della rete dell'utente. Puoi sostituire gran parte di questa funzionalità con gli script.

Appendice

Profilo di gestione dei dispositivi: ExtensibleSingleSignOnKerberos

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

Guida di riferimento per il protocollo di gestione dei dispositivi mobili

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

Profilo di gestione dei dispositivi: ExtensibleSingleSignOnKerberos.ExtensionData

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

Script di esempio - Elaborare le notifiche distribuite

L'estensione SSO Kerberos pubblica varie notifiche distribuite quando si verificano diversi eventi, per esempio quando un utente cambia una password o la rete aziendale passa online. Come amministratore, puoi usare uno script o un'app per restare in ascolto di queste notifiche e intraprendere delle azioni quando vengono pubblicate, per esempio eseguendo uno script o un comando della shell.

Qui sotto trovi uno script di esempio che può eseguire script o comandi quando vengono pubblicate notifiche. Dovrebbe essere implementato come LaunchAgent per eseguirlo come utente connesso o come LaunchDaemon per eseguirlo come radice. Lo script richiede due parametri:

- **-notification** è il nome della notifica distribuita di cui vuoi restare in ascolto. Vedi pagina 11 per gli esempi.
- **-action** è l'azione che vuoi eseguire quando viene pubblicata la notifica distribuita. Un esempio è "sh /path/to/script.sh".

Per eseguire lo script, devi installare gli strumenti da riga di comando per sviluppatori. Sul sito Apple Developer è disponibile un pacchetto per l'installazione di questi strumenti.

```
#!/usr/bin/swift

import Foundation

class NotifyHandler {

    // Action we want to run, like a shell command or a script
    public var action = String()

    // Runs every time we receive the specified distributed
    // notification
    @objc func gotNotification(notification: NSNotification){
        let task = Process()
        task.launchPath = "/bin/zsh"
        task.arguments = ["-c", action]
        task.launch()
    }
}

// MAIN

let scriptPath: String = CommandLine.arguments.first!

// -notification is the name of the notification you are listening for
guard let notification = UserDefaults.standard.string(forKey: "notification") else {
    print("\(scriptPath): No notification passed, exiting…")
    exit(1)
}
```

```
// -action is the action you want to run. This can be a shell

// command, script, etc.
guard let action = UserDefaults.standard.string(forKey: "action") else {
    print("\(scriptPath): No action passed, exiting…")
    exit(1)
}

let nh = NotifyHandler()
nh.action = action

print("Action is \(nh.action) and notification is \(notification)")

// Listen for the specified notification
DistributedNotificationCenter.default().addObserver(
    nh,
    selector: #selector(nh.gotNotification),
    name: NSNotification.Name(rawValue: notification),
    object: action)

RunLoop.main.run()
```

Script di esempio - Disinstallare Enterprise Connect

Questo semplice script rimuove qualsiasi versione di Enterprise Connect. Eseguilo da una soluzione di gestione del Mac o manualmente. Lo script deve essere eseguito con privilegi di radice

```
#!/bin/zsh

# Unload the Kerberos helper from versions of EC prior to 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

# Remove the privileged helper from versions of EC prior to 1.6
if [[ -e /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper ]]; then
  rm /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper
fi

# Remove the authorization db entry from versions of EC prior to 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
  # Enterprise Connect 2.0 or greater is installed
  # Unload ecAgent for logged in user and remove from 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

  # Quit the menu extra
  killall "Enterprise Connect Menu"
fi

# Finally, remove the Enterprise Connect app bundle
rm -rf /Applications/Enterprise\ Connect.app
```