Esempio di configurazione dell'abilitazione di SAML SSO per i client Jabber

Sommario

Introduzione

In questo documento viene descritto come configurare i client Cisco Jabber e i server di infrastruttura per l'SSO (Single Sign-On) SAML (Security Assertion Markup Language).

Prerequisiti

È necessario eseguire il provisioning di server di infrastruttura quali Cisco Unified Communications Manager (CUCM) IM e Presence, Cisco Unity Connection (UCXN) e CUCM per gli utenti Jabber e la configurazione client Jabber di base.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CUCM IM e Presence versione 10.5(1) o successiva
- UCXN versione 10.5(1) o successive
- CUCM 10.5(1) o versioni successive
- Cisco Jabber Client versione 10.5

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

1. Distribuire i certificati in tutti i server in modo che il certificato possa essere convalidato da un browser Web. In caso contrario, gli utenti riceveranno messaggi di avviso sui certificati non validi. Per ulteriori informazioni sulla convalida dei certificati, vedere Convalida dei certificati.

2. Verificare l'individuazione del servizio dell'SSO SAML nel client. Il client utilizza l'individuazione dei servizi standard per abilitare l'SSO SAML nel client. Abilitare l'individuazione dei servizi con i seguenti parametri di configurazione: ServicesDomain, VoiceServicesDomain e ServiceDiscoveryExcludedServices.

   Per ulteriori informazioni su come abilitare l'individuazione dei servizi, vedere Modalità di individuazione dei servizi da parte del client.

3. Per abilitare l'uso di SSO per i servizi telefonici da parte di Jabber, consultare l'esempio di configurazione di SAML SSO di Unified Communications Manager versione 10.5.

4. Per abilitare l'uso di SSO per le funzionalità IM da parte di Jabber, consultare l'esempio di configurazione di SAML SSO di Unified Communications Manager versione 10.5.

5. Per abilitare l'uso di SSO per Voicemail da parte di Jabber, fare riferimento all'esempio di configurazione di SSO SAML Unity Connection versione 10.5.

6. Per configurare il computer client per l'accesso automatico (solo Jabber per Windows), fare riferimento all'esempio di configurazione dell'autenticazione Kerberos nel programma di installazione di SAML SSO

7. Dopo l'abilitazione di SSO su CUCM e IMP, per impostazione predefinita tutti gli utenti Jabber accedono con SSO. Gli amministratori possono modificare questa impostazione in base all'utente, in modo che alcuni utenti non utilizzino l'SSO e accedano con i nomi utente e le password Jabber. Per disabilitare l'SSO per un utente Jabber, impostare il valore del parametro SSO_Enabled su FALSE.

   Se Jabber è stato configurato in modo da non richiedere agli utenti i propri indirizzi e-mail, il primo accesso a Jabber potrebbe essere non SSO. In alcune distribuzioni, il parametro ServicesDomainSsoEmailPrompt deve essere impostato su ON. In questo modo Jabber dispone delle informazioni necessarie per eseguire il primo accesso SSO. Se gli utenti hanno eseguito l'accesso a Jabber in precedenza, questa richiesta non è necessaria perché le informazioni richieste sono disponibili.

Verifica

Quando Jabber per Windows viene avviato, deve eseguire automaticamente l'accesso senza

richiedere credenziali o input. Per gli altri client Jabber, le credenziali verranno richieste solo una volta.

Risoluzione dei problemi

Se si verifica un problema, raccogliere una segnalazione del problema Jabber e contattare il Technical Assistance Center (TAC) di Cisco.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).