Configurez le soutien HTTPS de l'intégration ISE SCEP

Contenu

Introduction

Ce document décrit l'étape nécessaire pour configurer le soutien sécurisé de Transfer Protocol d'hypertexte (HTTPS) de l'intégration de Protocol d'inscription de certificat Secure (SCEP) avec le Cisco Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base du web server de l'Internet Information Services de Microsoft (IIS)
- Expérience de la configuration de SCEP et de Certificats sur ISE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Release 1.1.x ISE

- Entreprise R2 des Windows Server 2008 avec des correctifs pour KB2483564 et KB2633200 installés

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Le relatif à l'information aux services de certificat de Microsoft est donné comme guide spécifiquement pour Cisco Bring Your Own Device (BYOD). Référez-vous au TechNet de Microsoft comme source définitive de vérité pour l'autorité de certification de Microsoft, le service d'inscription de périphérique de réseau (NDES), et les configurations du serveur associées par SCEP.

Informations générales

Dans un déploiement BYOD, un des principaux composants est un serveur de l'entreprise R2 de Microsoft 2008 qui fait installer le rôle NDES. Ce serveur est un membre de la forêt de Répertoire actif (AD). Pendant l'installation initiale de NDES, le web server IIS de Microsoft est automatiquement installé et configuré pour prendre en charge l'arrêt de HTTP de SCEP. Dans des déploiements certain BYOD, les clients pourraient vouloir sécuriser plus loin les transmissions entre ISE et NDES utilisant HTTPS. Cette procédure détaille l'étape nécessaire pour demander et installer un certificat de Protocole SSL (Secure Socket Layer) pour le site Web SCEP.

Configurez

Configuration de certificat de serveur NDES

> Remarque: Vous devez configurer un nouveau certificat pour IIS (seulement requis quand IIS est intégré avec un PKI de tiers tel que Verisign ou quand l'autorité de certification (CA) et des rôles de serveur NDES sont séparés sur les serveurs distincts). Dans l'installer, si le rôle NDES est sur un serveur en cours de Microsoft CA, IIS utilise le certificat d'identité de serveur créé pendant l'installation CA. Pour des configurations autonomes de ce type, ignorez directement à la section de **configuration obligatoire du serveur IIS NDES** dans ce document.

1. Connectez au serveur NDES par l'intermédiaire de la console ou de la RDP.
2. **Début de** clic **- > outils d'administration - > gestionnaire de l'Internet Information Services (IIS)**.
3. Mettez en valeur le nom du serveur IIS et cliquez sur l'icône de **Certificats de serveur**.
4. Cliquez sur en fonction la **demande de certificat Create**, et terminez-vous les champs.
5. Ouvrez le fichier créé de .cer dans l'étape précédente avec un éditeur de texte et copiez le contenu sur le presse-papier.
6. Accédez au site Web d'inscription de Web de Microsoft CA et cliquez sur la **demande un certificat**.URL d'exemple : http://yourCAIP/certsrv

7. Cliquez sur Submit une **demande de certificat à l'aide de….** La pâte dans le contenu de certificat du presse-papier, et choisissent le modèle de **serveur Web**.
8. Cliquez sur Submit et puis sauvegardez le fichier du certificat à l'appareil de bureau.
9. Revenez au serveur NDES et ouvrez le gestionnaire IIS utilty. Cliquez sur en fonction le nom du serveur et cliquez sur alors la **demande complète de certificat** afin d'importer le certificat de serveur de création récente.

Configuration obligatoire du serveur IIS NDES

1. Développez le **nom du serveur**, développez les **sites**, **site Web par défaut de** clic.
2. **Attaches de** clic dans le coin supérieur droit.
3. Cliquez sur Add, changez le **Typeto** HTTPS, et choisissez le certificat de la liste déroulante.
4. Cliquez sur **OK**.

Configuration du serveur ISE

1. Connectez à l'interface d'inscription de Web du serveur CA et téléchargez la chaîne de certificat de CA.
2. Du GUI ISE, naviguez vers la **gestion - > des Certificats - > mémoire de certificat** et importez la chaîne de certificat de CA dans la mémoire ISE.
3. Naviguez vers la **gestion - > des Certificats - > des profils SCEP CA** et configurez l'URL pour HTTPS. **La Connectivité de test de** clic et cliquent sur alors la **sauvegarde**.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- Naviguez vers la **gestion - > des Certificats - > certificat Storeand** vérifient que la chaîne de certificat de CA et le certificat d'autorité d'enregistrement de serveur NDES (RA) sont présents.
- Employez Wireshark ou vidage mémoire de TCP pour surveiller l'échange SSL d'initiale entre le noeud d'admin ISE et le serveur NDES.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Décomposez la topologie du réseau BYOD en buts logiques afin d'aider à l'identifier mettent au point et capturent des points le long du chemin entre ces points finaux - ISE, NDES, et CA.
- Assurez-vous qu'on permet bidirectionnel le TCP 443 entre l'ISE et le serveur NDES.

- Des logs surveillez CA et NDES serveur d'application pour des erreurs d'enregistrement et employez Google ou le TechNet pour rechercher ces erreurs.
- Utilisez l'utilitaire de vidage mémoire de TCP sur le RPC ISE et surveillez le trafic à et du serveur NDES. Ceci se trouve sous des **exécutions** > des **outils de diagnostic** > les **outils généraux**.
- Installez Wireshark sur le serveur NDES ou l'ENVERGURE d'utilisation sur les Commutateurs intermédiaires afin de capturer le trafic SCEP à et du RPC ISE.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

> Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Informations connexes

- Configurez le soutien SCEP de BYOD
- Support et documentation techniques - Cisco Systems