Vue générale des Certificats et des autorités dans CUCM

Contenu

Introduction

Le but de ce document est de comprendre les fondements des Certificats et des autorités de certification. Ce document complimente d'autres documents Cisco qui se rapportent à tout le cryptage ou fonctions d'authentification dans Cisco Unified Communications Manager (CUCM).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

But des Certificats

Des Certificats sont utilisés entre les points d'extrémité pour établir une confiance/authentification et un cryptage des données. Ceci confirme que les points finaux communiquent avec le périphérique destiné et ont l'option de chiffrer les données entre les deux points finaux.

Définissez la confiance du point de vue d'un certificat

La plupart de partie importante de Certificats est la définition dont les points d'extrémité mettent en boîte sont de confiance par votre point final. Ce document vous aide à savoir et définir vos données sont chiffrées et partagées avec le site Web destiné, téléphone, ftp server, et ainsi de suite.

Quand votre système fait confiance à un certificat, ceci signifie qu'il y a des certificats préinstallés sur votre système qui énonce qu'il est de 100 pour cent de sûr qu'il partage les informations avec le point final correct. Autrement, il termine la transmission entre ces points d'extrémité.

Un exemple non technique de ceci est votre permis de conduire. Vous utilisez ce permis (serveur/certificat de service) de montrer que vous êtes qui vous dites que vous êtes ; vous avez obtenu votre permis de votre Division locale du branchement de véhicules à moteur (certificat intermédiaire) qui a été donné l'autorisation par la Division des véhicules à moteur (DMV) de votre état (autorité de certification). Quand vous devez afficher votre permis (serveur/certificat de service) à un dirigeant, le dirigeant sait qu'ils peuvent faire confiance au branchement DMV (certificat intermédiaire) et à la Division des véhicules à moteur (autorité de certification), et ils peuvent vérifier que ce permis a été émis par eux (autorité de certification). Votre identité est vérifiée au dirigeant et maintenant ils espèrent que vous êtes qui vous dites que vous êtes. Autrement, si vous donnez un permis faux (serveur/certificat de service) qui n'a pas été signé par le DMV (certificat intermédiaire), puis ils ne feront pas confiance qu'à qui vous dites vous êtes. Le reste de ce document fournit une explication en profondeur et technique de hiérarchie de certificat.

Comment les navigateurs utilisent des Certificats

1. Quand vous visitez un site Web, écrivez l'URL, tel que http://www.cisco.com.
2. Les DN trouve l'adresse IP du serveur qui héberge ce site.
3. Le navigateur navigue vers ce site.

Sans Certificats, il est impossible de savoir si un serveur DNS escroc était utilisé, ou si vous étiez conduit à un autre serveur. Les Certificats s'assurent que vous correctement et sécurisé êtes conduit au site Web destiné, tel que votre site Web de banque, où le personnel ou les informations confidentielles que vous écrivez est sécurisée.

Tous les navigateurs ont différentes icônes qu'ils les utilisent, mais normalement, vous voyez un cadenas dans la barre d'adresses comme ceci :

1. Cliquez sur en fonction les affichages de cadenas et d'une fenêtre :**Figure 1 : Identification de site Web**
2. Cliquez sur en fonction les **Certificats de vue** pour voir le certificat du site suivant les indications de cet exemple :**Figure 2 : Les informations de certificat, onglet Général** Les informations mises en valeur sont importantes.**Émise par** est la société ou l'Autorité de certification (CA) confiances de ce vos système déjà.**Valide de/à** est la plage de dates que ce certificat est utilisable. (Parfois vous voyez un certificat où vous connaissez vous confiance le CA, mais vous voyez que le certificat est non valide. Vérifiez toujours la date ainsi vous savez s'il a expiré.)**TIP :** Une pratique recommandée est de créer un rappel dans votre calendrier pour renouveler le certificat avant qu'elle expire. Ceci empêche de futures questions.

Les différences entre le PEM contre des Certificats DER

Le PEM est ASCII ; DER est binaire. La figure 3 affiche le format de certificat PEM.

Figure 3 : Exemple de certificat PEM
La figure 4 affiche le certificat DER.

Figure 4 : Exemple de certificat DER
La plupart des sociétés CA format PEM comme de Verisign ou de Thawt utilisation pour envoyer les Certificats aux clients, parce qu'il est qui respecte les emails. Le client devrait copier la chaîne entière et l'inclure **-----COMMENCEZ LE CERTIFICAT-----** et **-----CERTIFICAT D'EXTRÉMITÉ-----**, collez-le dans un fichier texte, et sauvegardez-le avec l'extension .PEM ou .CER.

Windows peut lire DER et CER formate avec son propre applet de Gestion de certificat et affiche le certificat suivant les indications de la figure 5.

Figure 5 : Les informations de certificat
Dans certains cas, un périphérique exige un format spécifique (ASCII ou binaire). Afin de changer ceci, téléchargez le certificat du CA dans le format nécessaire ou utilisez un outil de convertisseur SSL, tel que https://www.sslshopper.com/ssl-converter.html.

Hiérarchie de certificat

Afin de faire confiance à un certificat d'un point final, il doit y a une confiance déjà établie avec un tiers CA par exemple, des expositions de figure 6 il y a une hiérarchie de trois Certificats.

Figure 6 : Hiérarchie de certificat
- **Verisign** est un CA.
- **SSL étendu CA de validation de la classe 3 de Verisign** est une intermédiaire ou un certificat de serveur de signature (un serveur autorisé par CA à délivrer des Certificats dans son nom).
- **www.website.com** est un serveur ou un certificat de service.

Votre point final doit savoir qu'il peut faire confiance aux Certificats CA et d'intermédiaire d'abord avant qu'il sache qu'il peut faire confiance au certificat de serveur présenté par la prise de contact SSL (détails ci-dessous). Pour comprendre mieux comment cette confiance fonctionne, référez-

vous à la section dans ce document : **Définissez la « confiance » du point de vue d'un certificat**.

Certificats Auto-signés contre de tiers Certificats

Les principales différences entre les Certificats auto-signés et tiers sont qui signés le certificat, si vous leur faites confiance.

Un certificat auto-signé est un certificat signé par le serveur qui le présente ; donc, le serveur/certificat de service et le certificat de CA sont le même.

Une tierce partie CA est un service fourni par ou un public CA (comme Verisign, confient, Digicert) ou un serveur (comme Windows 2003, Linux, Unix, IOS) ce contrôle la validité du serveur/du certificat de service.

Chacun peut être un CA si votre système fait confiance à ce CA, est ce qui importe plus.

Noms de terrain communal et noms alternatifs soumis

Les noms de terrain communal (NC) et les noms alternatifs soumis (SAN) sont des références à l'adresse IP ou au nom de domaine complet (FQDN) de l'adresse qui est demandée. Par exemple, si vous entrez dans https://www.cisco.com, puis la NC ou le SAN doit avoir www.cisco.com dans l'en-tête.

Dans l'exemple présenté dans la figure 7, le certificat a la NC comme www.cisco.com. La demande URL de www.cisco.com du navigateur vérifie le FQDN URL contre les informations que le certificat présente. Dans ce cas, ils s'assortissent, et il affiche que la prise de contact SSL est réussie. Ce site Web a été vérifié pour être le site Web correct et des transmissions sont maintenant chiffrées entre l'appareil de bureau et le site Web.

Figure 7 : Vérification de site Web

Dans le même certificat, il y a une en-tête SAN pour trois adresses FQDN/DNS :

Figure 8 : En-tête SAN

Ce certificat peut authentifier/vérifie www.cisco.com (également défini dans la NC), cisco.com, et cisco-images.cisco.com. Ceci signifie que vous pouvez également taper cisco.com, et ce même certificat peut être utilisé pour authentifier et chiffrer ce site Web.

CUCM peut créer des en-têtes SAN. Référez-vous au document de la brûlure de Jason, CUCM téléchargeant des Certificats GUI de Web de CCMAdmin sur la Communauté de support pour plus d'informations sur des en-têtes SAN.

Certificats de caractère générique

Les Certificats de masque sont des Certificats qui emploient un astérisque (*) pour représenter n'importe quelle chaîne dans une section d'un URL. Par exemple, afin d'avoir un certificat pour www.cisco.com, ftp.cisco.com, ssh.cisco.com, et ainsi de suite, un administrateur devrait seulement créer un certificat pour *.cisco.com. Afin d'épargner l'argent, les besoins d'administrateur seulement d'acheter un certificat simple et n'a pas besoin d'acheter de plusieurs Certificats.

Cette caractéristique n'est pas actuellement prise en charge par Cisco Unified Communications

Manager (CUCM). Cependant, vous pouvez maintenir cette amélioration : CSCta14114 : Demande de support de certificat de masque dans CUCM et importation de clé privée.

Identifiez les Certificats

Quand les Certificats ont les mêmes informations dans eux, vous pouvez voir si c'est le même certificat. Tous les Certificats ont un seul numéro de série. Vous pouvez employer ceci pour comparer si les Certificats sont les mêmes Certificats, régénéré, ou contrefaçon. La figure 9 fournit un exemple :

Figure 9 : Numéro de série de certificat

CSRs et leur but

Le CSR signifie la demande de signature de certificat. Si vous voulez créer un tiers certificat pour un serveur CUCM, vous avez besoin d'un CSR pour se présenter au CA. Ce CSR semble beaucoup comme un certificat PEM (ASCII).

Remarque: Ce n'est pas un certificat et ne peut pas être utilisé en tant qu'un.

CUCM crée CSRs automatiquement par l'intermédiaire du GUI de Web : **La gestion de Cisco Unified >** la **Gestion du système d'exploitation de Sécurité >** de **certificat > se produisent CSR >** choisissent le service que vous voulez créer le certificat **> générez** alors le **CSR**. Chaque fois que cette option est utilisée, une nouveaux clé privée et CSR est générée.

Remarque: Une clé privée est un fichier qui est seul à ces serveur et service. Ceci devrait ne jamais être donné à n'importe qui ! Si vous fournissez une clé privée à quelqu'un, elle compromet la Sécurité que le certificat fournit. En outre, ne régénérez pas un nouveau CSR pour le même service si vous employez le vieux CSR pour créer un certificat. CUCM supprime le vieux CSR et la clé privée et remplace chacun d'eux, qui rend le vieux CSR inutile.

Référez-vous à la documentation de la brûlure de Jason sur la Communauté de support : CUCM téléchargeant des Certificats GUI de Web de CCMAdmin pour les informations sur la façon dont créer CSRs.

Utilisation des Certificats entre le processus de point final et de prise de contact SSL/TLS

Le protocole handshake est une gamme de messages ordonnancés qui négocient les paramètres de Sécurité d'une session de transfert des données. Référez-vous au SSL/TLS en détail , qui documente l'ordre de message dans le protocole handshake. Ceux-ci peuvent être vus dans une capture de paquet (PCAP). Les détails incluent l'initiale, ultérieur, et des messages finaux envoyés et reçus entre le client et serveur.

Comment CUCM utilise des Certificats

La différence entre le chat et la Tomcat-confiance

Quand des Certificats sont téléchargés à CUCM, il y a deux options pour chaque service par l'intermédiaire de **gestion de Cisco Unified >** de **Sécurité >** de **Gestion >** de **découverte de**

certificat du système d'exploitation.

Les cinq services qui te permettent **pour gérer des** Certificats dans CUCM sont :

- chat
- ipsec
- callmanager
- capf
- TV (dans la version 8.0 et ultérieures CUCM)

Voici les services qui te permettent **pour télécharger des** Certificats à CUCM :

- chat
- Tomcat-confiance
- ipsec
- ipsec-confiance
- callmanager
- CallManager-confiance
- capf
- capf-confiance

Ce sont les services disponibles dans la version 8.0 et ultérieures CUCM :

- TV
- TV-confiance
- téléphone-confiance
- téléphone-VPN-confiance
- téléphone-SAST-confiance
- téléphone-ctl-confiance

Référez-vous aux guides de Sécurité CUCM par la release pour plus de détails sur ces types de Certificats. Cette section explique seulement la différence entre un certificat de service et un certificat de confiance.

Par exemple, avec le **chat**, les Tomcat-**confiances** téléchargent le CA et les Certificats intermédiaires de sorte que ce noeud CUCM le connaisse peuvent faire confiance à n'importe quel certificat signé par le CA et le serveur intermédiaire. Le certificat de chat est le certificat qui est présenté par le service de chat sur ce serveur, si un point final fait une demande de HTTP à ce serveur. Afin de permettre la présentation de tiers Certificats par le chat, le noeud CUCM doit savoir qu'il peut faire confiance au CA et au serveur intermédiaire. Par conséquent, c'est une condition requise de télécharger le CA et les Certificats intermédiaires avant que le certificat de chat (service) soit téléchargé.

Référez-vous au CUCM de la brûlure de Jason téléchargeant des Certificats GUI de Web de CCMAdmin sur la Communauté de support pour information qui vous aidera à comprendre comment télécharger des Certificats à CUCM.

Chaque service a son propres certificat de service et Certificats de confiance. Ils ne fonctionnent pas outre de l'un l'autre. En d'autres termes, un CA et un certificat intermédiaire téléchargés comme service de Tomcat-confiance ne peuvent pas être utilisés par le service de callmanager.

Remarque: Les Certificats dans CUCM sont a par base de noeud. Par conséquent, si vous avez besoin de Certificats téléchargés à l'éditeur, et vous ayez besoin des abonnés pour avoir les

mêmes Certificats, vous devez les télécharger à chaque serveur et noeud individuels avant la version 8.5 CUCM. Dans la version 8.5 et ultérieures CUCM, il y a un service qui réplique les Certificats téléchargés vers le reste des Noeuds dans la batterie.

Remarque: Chaque noeud a une NC différente. Par conséquent, un CSR doit être créé par chaque noeud pour que le service présente leurs propres Certificats.

Si vous avez des questions spécifiques supplémentaires sur les fonctionnalités de sécurité l'unes des CUCM, référez-vous à la documentation de Sécurité.

Conclusion

Ce document aide et établit un haut niveau de la connaissance sur des Certificats. Ce sujet peut importer peut devenir plus en profondeur, mais ce document vous familiarise assez pour fonctionner avec des Certificats. Si vous avez des questions sur n'importe quelles fonctionnalités de sécurité CUCM, référez-vous aux guides de Sécurité CUCM par pour en savoir plus de release.

Informations connexes

- Guides de maintenance et de Sécurité de Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Cisco prennent en charge la Communauté : CUCM téléchargeant des Certificats GUI de Web de CCMAdmin
- Bogue CSCta14114 : Demande de support de certificat de masque dans CUCM et importation de clé privée
- Cisco Emergency Responder (CER) expliqué
- Support et documentation techniques - Cisco Systems