Certificats numériques

Ce chapitre décrit comment configurer les certificats numériques.

À propos des certificats numériques

Les certificats numériques fournissent une identification numérique aux fins d'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Les autorités de certification sont chargées de gérer les demandes de certificat et d'émettre des certificats numériques. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur.

Un certificat numérique inclut également une copie de la clé publique de l'utilisateur ou du périphérique. Une autorité de certification peut être un tiers de confiance, comme VeriSign, ou une autorité de certification privée (interne) que vous établissez au sein de votre organisation. Les autorités de certification émettent des certificats numériques dans le contexte d'une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité.

Pour l'authentification à l'aide de certificats numériques, au moins un certificat d'identité et son certificat CA d'émission doivent exister sur un ASA. Cette configuration autorise plusieurs identités, racines et hiérarchies de certificat. L'ASA évalue les certificats tiers par rapport aux CRL, également appelées listes de révocation d'autorité, depuis le certificat d'identité jusqu'à la chaîne des autorités de certification subordonnées.

Voici une description de plusieurs types de certificats numériques disponibles :

- Un certificat d'autorité de certification est utilisé pour signer les autres certificats. Il est autosigné et appelé certificat racine. Un certificat émis par un autre certificat CA s'appelle un certificat subordonné.
- Les autorités de certification délivrent également des certificats d'identité, qui sont des certificats pour des systèmes ou des hôtes spécifiques.

- Les certificats de signataire de code sont des certificats spéciaux utilisés pour créer des signatures numériques pour signer le code, le code signé révélant lui-même l'origine du certificat.

Dans une hiérarchie avec une racine et deux certificats CA intermédiaires, une validation de CRL pour l'accès à distance échoue sur la tête de réseau exécutant la version 9.13 ou une version ultérieure lorsque le certificat d'ID est signé par une CA intermédiaire, mais que la CRL est signée par une autre CA intermédiaire. La défaillance se produit même si la tête de réseau fait confiance aux deux intermédiaires lorsque ceux-ci sont signés par la même racine.

Par conséquent, chaque signataire doit conserver sa propre CRL. Chaque signataire précisera ensuite l'emplacement de la CRL dans la liste d'URL de chaque certificat qu'il signe. Sinon, vous pouvez configurer un remplacement d'URL dans le point de confiance de chaque signataire pointant vers le bon emplacement de CRL.

La CA locale intègre une fonctionnalité d'autorité de certificat indépendante sur l'ASA, déploie les certificats et assure une vérification sécurisée de la révocation des certificats émis. La CA locale fournit une autorité interne sécurisée et configurable pour l'authentification des certificats avec inscription des utilisateurs via une page de connexion au site Web.

Remarque Les certificats CA et les certificats d'identité s'appliquent à la fois aux connexions VPN de site à site et aux connexions VPN d'accès à distance. Les procédures dans ce document font référence à l'utilisation du VPN d'accès à distance dans l'interface graphique utilisateur du gestionnaire ASDM.

Astuces Pour un exemple de scénario comprenant la configuration des certificats et l'équilibrage de charges, consultez l'URL suivante : https://supportforums.cisco.com/docs/DOC-5964.

Cryptographie à clé publique

Les signatures numériques, activées par le chiffrement à clé publique, fournissent un moyen d'authentifier les appareils et les utilisateurs. Dans le chiffrement à clé publique, comme le système de chiffrement RSA, chaque utilisateur dispose d'une paire de clés contenant une clé publique et une clé privée. Les clés agissent comme des compléments, et tout ce qui est chiffré avec l'une des clés peut être déchiffré avec l'autre.

En termes simples, une signature se forme lorsque les données sont chiffrées avec une clé privée. La signature est jointe aux données et envoyée au récepteur. Le récepteur applique la clé publique de l'expéditeur aux données. Si la signature envoyée avec les données correspond au résultat de l'application de la clé publique aux données, la validité du message est établie.

Ce processus repose sur le récepteur ayant une copie de la clé publique de l'expéditeur et sur un degré élevé de confiance que cette clé appartient à l'expéditeur, et non à une personne se faisant passer pour l'expéditeur.

L'obtention de la clé publique d'un expéditeur est normalement gérée en externe ou par le biais d'une opération effectuée lors de l'installation. Par exemple, la plupart des navigateurs Web sont configurés avec les certificats racine de plusieurs autorités de certification par défaut. Pour le VPN, le protocole IKE, un composant IPsec, peut utiliser des signatures numériques pour authentifier les périphériques homologues avant de configurer des associations de sécurité.

Évolutivité des certificats

Sans certificats numériques, vous devez configurer manuellement chaque homologue IPsec pour chaque homologue avec lequel il communique; par conséquent, chaque nouvel homologue que vous ajoutez à un réseau nécessite une modification de configuration sur chaque homologue avec lequel il doit communiquer de manière sécurisée.

Lorsque vous utilisez des certificats numériques, chaque homologue est inscrit auprès d'une CA. Lorsque deux homologues tentent de communiquer, ils échangent des certificats et signent numériquement les données pour s'authentifier. Lorsqu'un nouvel homologue est ajouté au réseau, vous inscrivez cet homologue auprès d'une CA et aucun des autres homologues ne nécessite de modification. Lorsque le nouvel homologue tente une connexion IPsec, les certificats sont automatiquement échangés et l'homologue peut être authentifié.

Avec une CA, un homologue s'authentifie auprès de l'homologue distant en lui envoyant un certificat et en effectuant une cryptographie à clé publique. Chaque homologue envoie son certificat unique, qui a été émis par la CA. Ce processus fonctionne, car chaque certificat encapsule la clé publique de l'homologue associé, chaque certificat est authentifié par la CA et tous les homologues participants reconnaissent la CA comme une autorité d'authentification. Le processus s'appelle IKE avec une signature RSA.

L'homologue peut continuer à envoyer son certificat pour plusieurs sessions IPsec et à plusieurs homologues IPsec jusqu'à l'expiration du certificat. Lorsque son certificat expire, l'administrateur homologue doit en obtenir un nouveau auprès de la CA.

Les CA peuvent également révoquer les certificats d'homologues qui ne participent plus à IPsec. Les certificats révoqués ne sont pas reconnus comme valides par les autres homologues. Les certificats révoqués sont répertoriés dans une CRL, que chaque homologue peut vérifier avant d'accepter un certificat d'un autre homologue.

Certaines CA disposent d'une autorité d'enregistrement dans le cadre de leur mise en œuvre. Une autorité d'enregistrement est un serveur qui agit en tant que mandataire pour la CA, de sorte que les fonctions CA puissent continuer à fonctionner lorsque la CA n'est pas disponible.

Paires de clés

Les paires de clés sont des clés d'algorithme de signature numérique à courbe elliptique (ECDSA), qui ont les caractéristiques suivantes :

- Les clés RSA peuvent être utilisées pour SSH ou SSL.
- L'inscription SCEP prend en charge la certification des clés RSA.
- La taille de clé RSA maximum est de 4 096 et la valeur par défaut est de 2 048.
- La longueur maximum de la clé ECDSA est de 521, et la valeur par défaut est de 384.
- Vous pouvez générer une paire de clés RSA à usage général, utilisée à la fois pour la signature et le chiffrement, ou vous pouvez générer des paires de clés RSA distinctes pour chaque objectif. Des clés de signature et de chiffrement distinctes aident à réduire l'exposition des clés, car SSL utilise une clé pour le chiffrement, mais pas pour la signature. Cependant, IKE utilise une clé pour la signature, mais pas pour le chiffrement. En utilisant des clés distinctes pour chacune, l'exposition des clés est réduite au minimum.

Point de confiance

Les points de confiance vous permettent de gérer et de suivre les autorités de certification et les certificats. Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de configuration spécifiques à l'autorité de certification et une association avec un certificat d'identité inscrit.

Après avoir défini un point de confiance, vous pouvez le référencer par son nom dans les commandes nécessitant de spécifier une CA. Vous pouvez configurer de nombreux points de confiance.

Remarque Si l'ASA a plusieurs points de confiance qui partagent la même CA, un seul de ces points de confiance partageant la CA peut être utilisé pour valider les certificats d'utilisateur. Pour contrôler le partage du point de confiance qu'une CA utilise pour la validation des certificats d'utilisateur émis par cette CA, utilisez la commande **support-user-cert-validation**.

Pour l'inscription automatique, un point de confiance doit être configuré avec une URL d'inscription, et la CA que représente le point de confiance doit être disponible sur le réseau et doit prendre en charge SCEP.

Vous pouvez exporter et importer la paire de clés et les certificats émis associés à un point de confiance au format PKCS12. Ce format est utile pour dupliquer manuellement une configuration de point de confiance sur un autre ASA.

Inscription de certificat

L'ASA a besoin d'un certificat CA pour chaque point de confiance et d'un ou deux certificats pour lui-même, selon la configuration des clés utilisées par le point de confiance. Si le point de confiance utilise des clés RSA distinctes pour la signature et le chiffrement, l'ASA a besoin de deux certificats, un pour chaque fonction. Dans les autres configurations de clés, un seul certificat est nécessaire.

L'ASA prend en charge l'inscription automatique avec SCEP et l'inscription manuelle, ce qui vous permet de coller un certificat codé en base 64 directement dans le terminal. Pour les VPN de site à site, vous devez inscrire chaque ASA. Pour les VPN d'accès à distance, vous devez inscrire chaque ASA et chaque client VPN d'accès à distance.

Serveur mandataire pour les demandes SCEP

L'ASA peut servir de mandataire pour les demandes SCEP entre Secure Client (services client sécurisés) et une CA tierce. La CA ne doit être accessible à l'ASA que si celui-ci agit en tant que mandataire. Pour que l'ASA fournisse ce service, l'utilisateur doit s'authentifier à l'aide de l'une des méthodes prises en charge par AAA avant que l'ASA envoie une demande d'inscription. Vous pouvez également utiliser l'analyse de l'hôte et des politiques d'accès dynamique pour appliquer des règles d'admissibilité à l'inscription.

L'ASA prend en charge cette fonctionnalité uniquement avec une session VPN Secure Client (services client sécurisés) SSL ou IKEv2. Il prend en charge toutes les autorités de certification conformes à SCEP, y compris Cisco IOS CS, Windows Server 2003 CA et Windows Server 2008 CA

L'accès sans client (par navigateur) ne prend pas en charge le mandataire SCEP, bien que WebLaunch (Secure Client (services client sécurisés) initié sans client) le prenne en charge.

L'ASA ne prend pas en charge l'interrogation des certificats.

L'ASA prend en charge l'équilibrage de charges pour cette fonctionnalité.

Vérification de la révocation

Lorsqu'un certificat est émis, il est valide pour une période fixe. Parfois, une CA révoque un certificat avant l'expiration de cette période; par exemple, en raison de problèmes de sécurité ou d'un changement de nom ou d'association. Les CA publient périodiquement une liste signée des certificats révoqués. L'activation de la vérification de la révocation force l'ASA à vérifier que la CA n'a pas révoqué un certificat chaque fois qu'il l'utilise pour l'authentification.

Lorsque vous activez la vérification de la révocation, l'ASA vérifie l'état de révocation du certificat pendant le processus de validation du certificat PKI, qui peut utiliser la vérification des CRL, OCSP ou les deux. Le protocole OCSP est uniquement utilisé lorsque la première méthode renvoie une erreur (par exemple, indiquant que le serveur n'est pas disponible).

Lors de la vérification des CRL, l'ASA récupère, analyse et met en mémoire cache les CRL, qui fournissent une liste complète des certificats révoqués (et non révoqués) avec leurs numéros de série. L'ASA évalue les certificats en fonction des CRL, également appelées listes de révocation d'autorité, à partir du certificat d'identité jusqu'à la chaîne des autorités de certification subordonnées.

Le protocole OCSP offre une méthode plus évolutive de vérification de l'état de révocation dans la mesure où il localise l'état du certificat auprès d'une autorité de validation, à laquelle il demande l'état d'un certificat spécifique.

Serveurs CA pris en charge

L'ASA prend en charge les serveurs CA suivants :

CS Cisco IOS, CA local ASA et les prestataires CA tiers conformes à X.509, y compris, sans s'y limiter :

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

Les CRL fournissent à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration des CRL fait partie de la configuration d'un point de confiance.

Vous pouvez configurer l'ASA pour rendre les vérifications de CRL obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check crl**. Vous pouvez également rendre la vérification

de la CRL facultative en utilisant la commande **revocation-check crl none**, qui permet de réussir l'authentification par certificat lorsque la CA n'est pas disponible pour fournir des données CRL mises à jour.

Remarque La commande **revocation-check crl none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'ASA peut récupérer les CRL des autorités de certification à l'aide de HTTP, SCEP ou LDAP. Les CRL extraites pour chaque point de confiance sont mises en cache pour une durée configurable pour chaque point de confiance.

Remarque Même si le serveur CRL répond par l'indicateur HTTP « Connection: Keep-alive » (Connexion : Keepalive) pour indiquer une connexion persistante, l'ASA ne demande pas la prise en charge de la connexion persistante. Modifiez les paramètres sur le serveur CRL pour répondre par « Connection: Close » (Connexion : Fermer) lorsque la liste est envoyée.

Lorsque l'ASA a mis en cache une CRL plus longtemps que la configuration de la mise en cache des CRL, l'ASA considère la CRL comme trop ancienne pour être fiable ou « obsolète ». L'ASA tente de récupérer une version plus récente de la CRL la prochaine fois qu'une authentification par certificat nécessite une vérification de la CRL obsolète.

Vous pourriez recevoir un échec de *vérification de la révocation* pour une connexion ou un certificat utilisateur si vous dépassez la limite de taille de 16 Mo pour la CRL.

L'ASA met les CRL en cache pendant une durée déterminée par les deux facteurs suivants :

- Le nombre de minutes spécifié avec la commande **cache-time**. La valeur par défaut est de 60 minutes.
- Le champ NextUpdate dans les CRL extraites, qui peut être absent des CRL. Vous contrôlez si l'ASA requiert et utilise le champ NextUpdate avec la commande **enforcenextupdate**.

L'ASA utilise ces deux facteurs de la manière suivante :

- Si le champ NextUpdate n'est pas obligatoire, l'ASA marque les CRL comme obsolètes après la durée définie par la commande **cache-time**.
- Si le champ NextUpdate est obligatoire, l'ASA marque les CRL comme obsolètes à la première des deux fois spécifiées par la commande **cache-time** et le champ NextUpdate. Par exemple, si la commande **cache-time** est définie à 100 minutes et que le champ NextUpdate indique que la prochaine mise à jour est à 70 minutes, l'ASA marque les CRL comme obsolètes en 70 minutes.

Si l'ASA a une mémoire insuffisante pour stocker toutes les CRL mises en cache pour un point de confiance donné, il supprime la CRL la moins récemment utilisée pour faire de la place pour une CRL nouvellement récupérée. Les grandes CRL nécessitent un surdébit de calcul important pour les analyser. Par conséquent, pour de meilleures performances, utilisez de nombreuses CRL de plus petite taille plutôt que quelques grandes CRL, ou de préférence, utilisez OCSP.

Consultez les tailles de cache suivantes :

- Mode de contexte unique : 128 Mo
- Mode de contexte multiple : 16 Mo par contexte

OCSP

L'OCSP fournit à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration de l'OCSP fait partie de la configuration du point de confiance.

L'OCSP localise l'état du certificat sur une autorité de validation (un serveur OCSP, également appelé *répondeur*) que l'ASA interroge pour connaître l'état d'un certificat en particulier. Cette méthode offre une meilleure évolutivité et un état de révocation plus à jour que la vérification des CRL, et aide les entreprises avec de grandes installations PKI à déployer et à étendre des réseaux sécurisés.

Remarque L'ASA autorise un décalage de cinq secondes pour les réponses OCSP.

Vous pouvez configurer l'ASA pour rendre les vérifications OCSP obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check ocsp**. Vous pouvez également rendre la vérification OCSP facultative en utilisant la commande **revocation-check ocsp none**, qui permet de réussir l'authentification par certificat lorsque l'autorité de validation n'est pas disponible pour fournir des données OCSP mises à jour.

Remarque La commande **revocation-check ocsp none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'OCSP fournit trois façons de définir l'URL du serveur OCSP. L'ASA utilise ces serveurs dans l'ordre suivant :

1. L'URL OCSP définie dans une règle de remplacement de certificat de correspondance à l'aide de la commande **match certificate**).
2. L'URL OCSP configurée à l'aide de la commande **ocsp url**.
3. Le champ AIA du certificat client.

Remarque Pour configurer un point de confiance pour valider un certificat de répondeur OCSP autosigné, vous devez importer le certificat de répondeur autosigné dans son propre point de confiance en tant que certificat CA de confiance. Ensuite, vous devez configurer la commande **match certificate** dans le point de confiance de validation du certificat client pour utiliser le point de confiance qui comprend le certificat de répondeur OCSP autosigné pour valider le certificat de répondeur. Utilisez la même procédure pour configurer la validation des certificats de répondeur externes au chemin de validation du certificat client.

Le certificat du serveur OCSP (répondeur) signe généralement la réponse OCSP. Après avoir reçu la réponse, l'ASA tente de vérifier le certificat du répondeur. La CA définit normalement la durée de vie du certificat de répondeur OCSP sur une période relativement courte pour réduire au minimum les risques de compromission. La CA comprend généralement une extension ocsp-no-check dans le certificat du répondeur, qui indique que ce certificat n'a pas besoin de vérification de l'état de révocation. Cependant, si cette extension est absente, l'ASA tente de vérifier l'état de révocation en utilisant la même méthode que spécifiée dans le point de confiance. Si le certificat du répondeur n'est pas vérifiable, les vérifications de révocation échouent. Pour éviter cette possibilité, utilisez la commande **revocation-check none** pour configurer le point de confiance de validation du certificat du répondeur et utilisez la commande **revocation-check ocsp** pour configurer le certificat client.

Certificats et coordonnées de connexion de l'utilisateur

La section suivante décrit les différentes méthodes d'utilisation des certificats et des coordonnées de connexion de l'utilisateur (nom d'utilisateur et mot de passe) pour l'authentification et l'autorisation. Ces méthodes s'appliquent à IPsec, Secure Client (services client sécurisés) et au SSL VPN sans client.

Dans tous les cas, l'autorisation LDAP n'utilise pas le mot de passe comme identifiant. L'autorisation RADIUS utilise un mot de passe commun pour tous les utilisateurs ou le nom d'utilisateur comme mot de passe.

Informations d'authentification de l'utilisateur

La méthode par défaut pour l'authentification et l'autorisation utilise les coordonnées de connexion de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur comme identifiant

Certificats

Si des certificats numériques d'utilisateur sont configurés, l'ASA valide d'abord le certificat. Cependant, il n'utilise aucun des DN des certificats comme nom d'utilisateur pour l'authentification.

Si l'authentification et l'autorisation sont toutes deux activées, l'ASA utilise les coordonnées de connexion de l'utilisateur pour l'authentification et l'autorisation de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise le nom d'utilisateur comme identifiant

Si l'authentification est désactivée et que l'autorisation est activée, l'ASA utilise le champ DN principal pour l'autorisation.

- Authentification
  - DÉSACTIVÉ (défini sur Aucun) par le paramètre du groupe de serveurs d'authentification
  - Aucun identifiant utilisé

- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise la valeur du nom d'utilisateur du champ DN principal du certificat comme identifiant

Remarque Si le champ de DN principal n'est pas présent dans le certificat, l'ASA utilise la valeur du champ DN secondaire comme nom d'utilisateur pour la demande d'autorisation.

Prenons par exemple un certificat d'utilisateur qui comprend les champs et les valeurs de DN du sujet suivants :

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

Si le DN principal = EA (adresse courriel) et le DN secondaire = CN (nom commun), le nom d'utilisateur utilisé dans la demande d'autorisation serait anyuser@example.com.

Lignes directrices pour les certificats numériques

Cette section comprend des lignes directrices et des limites que vous devez vérifier avant de configurer les certificats numériques.

Directives relatives au mode contextuel

- Pris en charge en mode de contexte unique seulement pour les autorités de certification tierces.

Directives en matière de basculement

- Ne prend pas en charge la réplication des sessions dans le basculement dynamique.
- Ne prend pas en charge le basculement pour les autorités de certification locales.
- Les certificats sont automatiquement copiés sur l'unité de secours si vous configurez le basculement dynamique. Si vous constatez qu'un certificat est manquant, utilisez la commande **write standby** sur l'unité active.

Directives IPv6

Ne prend pas en charge IPv6.

Certificats de CA locale

- Assurez-vous que l'ASA est configuré correctement pour prendre en charge les certificats. Un ASA mal configuré peut entraîner l'échec de l'inscription ou demander un certificat contenant des renseignements inexacts.
- Assurez-vous que le nom d'hôte et le nom de domaine de l'ASA sont configurés correctement. Pour afficher le nom d'hôte et le nom de domaine actuellement configurés, saisissez la commande **show running-config**.

- Assurez-vous que l'horloge ASA est réglée avec précision avant de configurer la CA. Les certificats ont une date et une heure de validité et d'expiration. Lorsque l'ASA s'inscrit auprès d'une CA et obtient un certificat, l'ASA vérifie que l'heure actuelle se situe dans la plage de validité du certificat. Si ce n'est pas le cas, l'inscription échoue.
- Trois jours avant l'expiration du certificat de CA locale, un certificat de renouvellement de remplacement est généré et un message de journal système informe l'administrateur qu'il est temps de procéder au renouvellement du certificat de CA locale. Le nouveau certificat de CA locale doit être importé sur tous les périphériques nécessaires avant l'expiration du certificat actuel. Si l'administrateur ne répond pas en installant le certificat de renouvellement comme nouveau certificat de CA locale, les validations peuvent échouer.
- Le certificat de CA locale est renouvelé automatiquement après son expiration en utilisant la même paire de clés. Le certificat de renouvellement peut être exporté au format base 64.

  L'exemple suivant montre un certificat de CA locale codé en base 64 :

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

Prise en charge du mandataire SCEP

- Assurez-vous que l'ASA et les nœuds de service de politique Cisco ISE sont synchronisés à l'aide du même serveur NTP.
- Secure Client (services client sécurisés) 3.0 ou une version ultérieure doit être en cours d'exécution sur le terminal.
- La méthode d'authentification, configurée dans le profil de connexion pour votre stratégie de groupe, doit être définie pour utiliser à la fois AAA et l'authentification par certificat.
- Un port SSL doit être ouvert pour les connexions VPN IKEv2.
- La CA doit être en mode d'octroi automatique.

Directives supplémentaires

- Le type de certificat que vous pouvez utiliser est limité par les types de certificats pris en charge par les applications qui utiliseront le certificat. Les certificats RSA sont généralement pris en charge par toutes les applications qui utilisent des certificats. Cependant, les certificats EDDSA peuvent ne pas être pris en charge par les systèmes d'exploitation des ordinateurs, les navigateurs, ASDM ou Secure Client (services client sécurisés). Par exemple, vous devez utiliser un certificat RSA pour l'identité et l'authentification VPN d'accès à distance. Pour le VPN de site à site, où l'ASA est l'application qui utilise le certificat, EDDSA est pris en charge.
- Pour les ASA configurés en tant que serveurs ou clients CA, limitez la période de validité du certificat à une date antérieure à la date de fin recommandée, soit le 19 janvier 2038 à 03:14:08 UTC. Ces lignes directrices s'appliquent également aux certificats importés de fournisseurs tiers.

- L'ASA établit une connexion LDAP/SSL uniquement si l'un des critères de certification suivants est satisfait :
  - Le certificat du serveur LDAP est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA) et est valide.
  - Un certificat d'autorité de certification des serveurs émettant la chaîne est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA), et tous les certificats d'autorité de certification subordonnés de la chaîne sont complets et valides.
- Lorsqu'une inscription de certificat est terminée, l'ASA stocke un fichier PKCS12 contenant la paire de clés et la chaîne de certificat de l'utilisateur, ce qui nécessite environ 2 Ko de mémoire flash ou d'espace disque par inscription. La quantité réelle d'espace disque dépend de la configuration de la clé RSA et des champs de certificat. Gardez ces lignes directrices à l'esprit lors de l'ajout d'un grand nombre d'inscriptions de certificat en attente sur un ASA avec une quantité limitée de mémoire flash disponible, car ces fichiers PKCS12 sont stockés dans la mémoire flash pendant toute la durée du délai d'expiration de récupération de l'inscription configuré. Nous vous conseillons d'utiliser une taille de clé d'au moins 2048.
- Vous devez configurer l'ASA pour utiliser un certificat d'identité afin de protéger le trafic ASDM et le trafic HTTPS vers l'interface de gestion. Les certificats d'identité qui sont automatiquement générés avec SCEP sont régénérés après chaque redémarrage, alors assurez-vous d'installer manuellement vos propres certificats d'identité. Pour obtenir un exemple de cette procédure qui s'applique uniquement à SSL, consultez l'URL suivante : http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
- L'ASA et le Secure Client (services client sécurisés) ne peuvent valider que les certificats dans lesquels le champ X520Serialnumber (numéro de série dans le nom d'objet) est au format PrintableString. Si le format du numéro de série utilise un encodage tel que UTF8, l'autorisation de certificat échouera.
- Utilisez uniquement des caractères et des valeurs valides pour les paramètres de certificat lorsque vous les importez sur l'ASA. Dans l'ASA, ces certificats sont décodés afin d'être intégrés dans des structures de données internes. Les certificats comportant des champs vides sont interprétés comme non conformes aux normes de décodage et, par conséquent, la validation de l'installation échoue. Cependant, à partir de la version 9.16, les valeurs vides des champs facultatifs n'ont aucune incidence sur les critères de décodage et de validation d'installation.
- Pour utiliser un caractère générique (*), assurez-vous d'utiliser l'encodage sur le serveur CA qui autorise ce caractère dans la valeur de chaîne. Bien que la RFC 5280 recommande d'utiliser un UTF8String ou PrintableString, vous devez utiliser UTF8String, car PrintableString ne reconnaît pas le caractère générique comme un caractère valide. L'ASA rejette le certificat importé si un caractère ou une valeur non valide est détecté pendant l'importation. Par exemple :

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕv°3é¼p0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

- Configurez le serveur DNS sur le périphérique pour une inscription ACME réussie. Pour en savoir plus sur la procédure de configuration du serveur DNS, consultez Configurer des serveurs DNS.

Configurer les certificats numériques

Les rubriques suivantes expliquent comment configurer les certificats numériques.

Configurer les paires de clés

Pour créer ou supprimer des paires de clés, procédez comme suit.

Procédure

Étape 1 Générez une paire de clés RSA par défaut à usage général.

crypto key generate rsa modulus 2048

Exemple :

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

Le module de clé par défaut est 2048, mais vous devez spécifier explicitement le module pour vous assurer d'obtenir la taille dont vous avez besoin. La clé s'appelle Default-RSA-Key.

Pour les clés RSA, le module peut être l'un des éléments suivants (en bits) : 2 048 ou.

Si vous souhaitez également une clé d'algorithme de signature à courbe elliptique (ECDSA), vous pouvez générer la clé Default-ECDSA-Key. La longueur par défaut est de 384, mais vous pouvez également utiliser 256 ou 521.

crypto key generate ecdsa elliptic-curve 384

Si vous souhaitez également une clé d'algorithme de signature à courbe d'Edwards (EdDSA), vous pouvez générer la clé Default-EdDSA-Key. La longueur par défaut est de 256 bits.

Remarque
Les inscriptions EST sur l'ASA à l'aide de paires de clés de type EdDSA (Ed25519) ne sont pas prises en charge. Les inscriptions EST ne peuvent utiliser que des clés RSA ou ECDSA.

crypto key generate eddsa edward-curve Ed25519

Étape 2 (Facultatif) Créez des clés supplémentaires avec des noms uniques.

crypto key generate rsa label *key-pair-label* **modulus** *size*

crypto key generate ecdsa label *key-pair-label* **elliptic-curve** *size*

Exemple :

```
ciscoasa(config)# crypto key generate rsa label exchange modulus 2048
```

L'étiquette est référencée par le point de confiance qui utilise la paire de clés.

Étape 3 Vérifiez les paires de clés que vous avez générées.

show crypto key mypubkey {**rsa** | **ecdsa**}

Exemple :

```
ciscoasa/contexta(config)# show crypto mypubkey key rsa
```

Étape 4 Enregistrez la paire de clés que vous avez générée.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 5 Si nécessaire, supprimez les paires de clés existantes afin de pouvoir en générer de nouvelles.

crypto key zeroize {**rsa** | **ecdsa**}

Exemple :

```
ciscoasa(config)# crypto key zeroize rsa
```

Étape 6 (Facultatif) Archivez le certificat et la paire de clés du serveur CA local.

copy

Exemple :

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

Cette commande copie le certificat et la paire de clés du serveur CA local ainsi que tous les fichiers de l'ASA à l'aide de FTP ou de TFTP.

Remarque
Assurez-vous de sauvegarder tous les fichiers du serveur CA local aussi souvent que possible.

Étape 7 Pour les méthodes d'inscription qui prennent en charge l'inscription automatique, des paires de clés sont automatiquement générées et stockées dans la mémoire flash au moment de l'inscription. Pour activer cette prise en charge, les paramètres clés suivants sont spécifiés dans le point de confiance :

L'exemple suivant montre la configuration de la paire de clés ECDSA :

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

crypto-ca-trustpoint mode commands/options:
  256  256 bits
  384  384 bits
  521  521 bits
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve 521
ciscoasa(config-ca-trustpoint)#
```

L'exemple suivant montre la configuration de la paire de clés RSA :

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

ciscoasa(config-ca-trustpoint)# keypair rsa modulus ?

crypto-ca-trustpoint mode commands/options:
  2048  2048 bits
  3072  3072 bits
  4096  4096 bits
ciscoasa(config-ca-trustpoint)# keypair rsa modulus 2048
ciscoasa(config-ca-trustpoint)#
```

Étape 8 Vous pouvez supprimer les paires de clés en exécutant la commande suivante :

crypto key zeroize rsa

L'exemple suivant montre comment supprimer des paires de clés :

Exemple :

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
```

Configurer les points de confiance

Pour configurer un point de confiance, procédez comme suit :

Procédure

Étape 1 Créez un point de confiance qui correspond à la CA à partir de laquelle l'ASA doit recevoir un certificat.

crypto ca trustpoint *trustpoint-name*

Exemple :

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

Vous entrez en mode de configuration du point de confiance de la CA de chiffrement, qui contrôle les paramètres de point de confiance spécifiques à la CA que vous pouvez configurer à partir de l'étape 3.

Étape 2 Précisez l'interface source pour la certification CA :

enrollment interface *interface-name*

```
ciscoasa(config-ca-trustpoint)#  enrollment interface mgmt
```

Étape 3 Choisissez une des options suivantes :

- Demandez l'inscription automatique à l'aide de SCEP avec le point de confiance spécifié et configurez l'URL d'inscription en exécutant la commande suivante :

  enrollment protocol scep *url*

  Exemple :

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment protocol scep url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

- Demandez l'inscription automatique à l'aide de CMP avec le point de confiance spécifié et configurez l'URL d'inscription en exécutant la commande suivante :

  enrollment protocol cmp *url*

  Exemple

  ```
  ciscoasa/ contexta(config-ca-trustpoint)# enrollment protocol cmp url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

  Remarque
  La licence de l'opérateur doit être incluse pour permettre l'inscription au CMP.

- Demandez l'inscription manuelle avec le point de confiance spécifié en collez le certificat reçu de la CA au terminal en exécutant la commande suivante :

  enrollment terminal

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
  ```

- Demandez un certificat autosigné en exécutant la commande suivante :

  enrollment self

- Demandez l'inscription automatique à l'aide d'EST avec le point de confiance spécifié et configurez l'URL d'inscription en exécutant la commande suivante :

  enrollment protocol est *url*

  Exemple

  ```
  asa(config-ca-trustpoint)# enrollment protocol est ?

  crypto-ca-trustpoint mode commands/options:
    url CA server enrollment URL
  asa(config-ca-trustpoint)# enrollment protocol est url ?
   crypto-ca-trustpoint mode commands/options:
    LINE < 477 char  URL
  asa(config-ca-trustpoint)# enrollment protocol est url https://xyz.com/est
  ```

Étape 4 Si le point de confiance a été configuré pour utiliser CMP à l'étape ci-dessus, vous pouvez éventuellement activer la fonctionnalité qui demande automatiquement des certificats. Saisissez un pourcentage de la durée de vie absolue du certificat, après quoi l'inscription automatique sera nécessaire et précisez si vous souhaitez générer une nouvelle clé lors du renouvellement du certificat.

```
[no] auto-enroll [<percent>] [regenerate]
```

Étape 5 Spécifiez les options de configuration CRL disponibles.

revocation-check crl none

Remarque
La commande **revocation-check crl none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
ciscoasa/contexta(config-ca-trustpoint)# revocation-check none
```

Remarque
Pour activer la vérification CRL requise ou facultative, assurez-vous de configurer le point de confiance pour la gestion des CRL après l'obtention des certificats.

Étape 6 Activez ou désactivez l'extension des contraintes de base et l'indicateur CA.

[**no**]**ca-check**

L'extension des contraintes de base détermine si le sujet du certificat est une autorité de certification (CA), auquel cas le certificat peut être utilisé pour signer d'autres certificats. L'indicateur de d'autorité de certification fait partie de cette extension. La présence de ces éléments dans un certificat indique que la clé publique du certificat peut être utilisée pour valider les signatures de certificat.

La commande **ca-check** est activée par défaut. Vous ne devez donc saisir cette commande que si vous souhaitez désactiver les contraintes de base et l'indicateur CA.

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# no ca-check
```

Étape 7 Lors de l'inscription, demandez à la CA d'inclure l'adresse courriel spécifiée dans l'extension de nom alternatif du sujet du certificat.

email *address*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

Étape 8 (Facultatif) Spécifiez une période de nouvelle tentative en minutes, applicable uniquement à l'inscription SCEP.

enrollment retry period

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

Étape 9 (Facultatif) Spécifiez un nombre maximum de nouvelles tentatives autorisées, applicable uniquement à l'inscription SCEP.

enrollment retry count

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

Étape 10 Lors de l'inscription, demandez à la CA d'inclure le nom de domaine complet spécifié dans l'extension de nom alternatif du sujet du certificat.

fqdn *fqdn*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

Étape 11 Lors de l'inscription, demandez à la CA d'inclure l'adresse IP de l'ASA dans le certificat.

ip-address *ip-address*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

Étape 12 Spécifiez la paire de clés dont la clé publique doit être certifiée.

keypair *name*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

Étape 13 Si vous avez des points de confiance configurés pour CMP, déterminez si vous souhaitez générer des clés EDDSA, des clés EDCSA ou des clés RSA pour des inscriptions manuelles et automatiques.

```
no keypair name | [rsa modulus 2048|4096] | [edcsa elliptic-curve 256|384|521] | [ eddsa
edwards-curve Ed25519 ]
```

Remarque
Les inscriptions EST sur l'ASA à l'aide de paires de clés de type EDDSA (Ed25519) ne sont pas prises en charge. Les inscriptions EST ne peuvent utiliser que des clés RSA et ECDSA. L'inscription à ACME avec le type de paire de clés EDDSA n'est pas prise en charge.

Remarque
Lorsque le groupe de chiffrement ECDHE_ECDSA est utilisé, configurez le point de confiance avec un certificat contenant une clé compatible avec ECDSA. Les certificats avec une clé RSA ne sont pas compatibles avec les chiffrements ECDSA.

Étape 14 Configurez les remplacements d'URL OCSP et les points de confiance à utiliser pour la validation des certificats de répondeur OCSP.

match certificate map-name override ocsp

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

Étape 15 Configurez l'interface source pour que l'ASA atteigne le protocole OCSP :

interface *nameif*

Exemple :

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
```

Étape 16 Désactivez l'extension de nonce sur une requête OCSP. L'extension de nonce lie cryptographiquement les requêtes aux réponses pour éviter les attaques par relecture.

ocsp disable-nonce

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

Étape 17 Configurez un serveur OCSP que l'ASA utilisera pour vérifier tous les certificats associés à un point de confiance plutôt que le serveur spécifié dans l'extension AIA du certificat client.

ocsp url

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

Étape 18 Spécifiez une phrase de défi enregistrée auprès de la CA lors de l'inscription. La CA utilise généralement cette phrase pour authentifier une demande de révocation ultérieure.

password *string*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

Étape 19 Définissez une ou plusieurs méthodes pour la vérification de la révocation : CRL, OCSP et Aucune.

Remarque
Lorsque vous affectez une URL OCSP pour la vérification de la révocation, vous pouvez spéficier l'interface (y compris l'interface de gestion) à partir de laquelle l'OCSP est accessible. Cette valeur d'interface détermine la décision de routage.

revocation check

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

Étape 20 Lors de l'inscription, demandez à la CA d'inclure le DN du sujet spécifié dans le certificat. Si une chaîne de nom distinctif comprend une virgule, incluez la chaîne de valeur entre guillemets doubles (par exemple, O= « Société, Inc. »).

subject-name *X.500 name*

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

Étape 21 Lors de l'inscription, demandez à la CA d'inclure le numéro de série de l'ASA dans le certificat.

serial-number

Exemple :

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

Étape 22 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa/contexta(config)# write memory
```

Configurer les CRL pour un point de confiance

Pour utiliser la vérification des CRL obligatoires ou facultatives lors de l'authentification par certificat, vous devez configurer les CRL pour chaque point de confiance. Pour configurer les CRL pour un point de confiance, procédez comme suit :

Procédure

Étape 1 Entrez dans le mode de configuration du point de confiance CA cryptographique pour accéder au point de confiance dont vous souhaitez modifier la configuration des CRL.

crypto ca trustpoint *trustpoint-name*

Exemple :

```
ciscoasa (config)# crypto ca trustpoint Main
```

Remarque

Assurez-vous d'avoir activé les CRL avant de saisir cette commande. En outre, la CRL doit être disponible pour que l'authentification réussisse.

Étape 2 Entrez dans le mode de configuration de CRL pour le point de confiance actuel.

crl configure

Exemple :

```
ciscoasa(config-ca-trustpoint)# crl configure
```

Astuces
Pour définir tous les paramètres de configuration de CRL aux valeurs par défaut, utilisez la commande **default**. À tout moment pendant la configuration de la CRL, saisissez à nouveau cette commande pour redémarrer la procédure.

Étape 3 Choisissez l'une des options suivantes pour configurer la politique de récupération :

- Les CRL sont extraites uniquement des URL des points de distribution de CRL (CDP) spécifiées dans les certificats authentifiés.

  policy cdp

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

  Remarque
  La récupération SCEP n'est pas prise en charge par les points de distribution spécifiés dans les certificats.

- Les CRL sont extraites uniquement de la règle de correspondance de la carte de certificat que vous configurez.

  policy static

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

- Les CRL sont extraites des points de distribution de CRL spécifiés dans les certificats authentifiés et de la règle de correspondance de la carte de certificat que vous configurez.

  policy both

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

Étape 4 Si vous avez utilisé les mots clés **static** ou **both** lors de la configuration de la politique de CRL, vous devez configurer la règle de correspondance de la carte de certificat pour la récupération des CRL. Vous pouvez désormais configurer plusieurs CDP statiques sur une seule carte.

enrollment terminal

Pour supprimer une instance en particulier, sous la forme **no** de la commande, incluez le numéro de séquence ou l'URL. Assurez-vous que les valeurs spécifiées correspondent aux valeurs configurées. Pour supprimer toutes les entrées de la carte, utilisez simplement la commande **no**.

Exemple :

```
ciscoasa(crypto ca trustpoint)#enrollment terminal

ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  10 url http://192.0.2.10
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  20 url http://192.0.2.12
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  30 url http://192.0.2.13
```

Étape 5 Précisez HTTP, LDAP ou SCEP comme méthode de récupération des CRL.

protocol http | **ldap** | **scep**

Exemple :

```
ciscoasa(config-ca-crl)# protocol http
```

Étape 6 Configurez la durée pendant laquelle l'ASA met en cache les CRL pour le point de confiance actuel. L'argument *refresh-time* est le nombre de minutes que l'ASA attend avant de prendre en compte une CRL obsolète.

cache-time *refresh-time*

Exemple :

```
ciscoasa(config-ca-crl)# cache-time 420
```

Étape 7 Effectuez l'une des opérations suivantes :

- Exigez la présence du champ NextUpdate dans les CRL. Il s'agit du paramètre par défaut.

  enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- Permettez au champ NextUpdate d'être absent des CRL.

  no enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# no enforcenextupdate
  ```

Étape 8 Identifiez le serveur LDAP à l'ASA si LDAP est spécifié comme protocole de récupération. Vous pouvez spécifier le serveur par nom de domaine DNS ou par adresse IP. Vous pouvez également fournir un numéro de port si le serveur écoute les requêtes LDAP sur un port autre que la valeur par défaut de 389.

ldap-defaults *server*

Exemple :

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

Remarque
Si vous utilisez un nom de domaine au lieu d'une adresse IP pour spécifier le serveur LDAP, assurez-vous d'avoir configuré l'ASA pour utiliser DNS.

Étape 9 Autorisez la récupération de la CRL si le serveur LDAP requiert des informations d'authentification.

ldap-dn *admin-DN password*

Exemple :

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c001RunZ
```

Étape 10 Récupérez la CRL actuelle de la CA représentée par le point de confiance spécifié et testez la configuration de la CRL pour le point de confiance actuel.

crypto ca crl request *trustpoint*

Exemple :

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

Étape 11 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa (config)# write memory
```

Exporter ou importer une configuration de point de confiance

Pour exporter et importer une configuration de point de confiance, procédez comme suit :

Procédure

Étape 1 Exportez une configuration de point de confiance avec toutes les clés et tous les certificats associés au format PKCS12.

crypto ca export *trustpoint*

Exemple :

```
ciscoasa(config)# crypto ca export Main
```

L'ASA affiche les données PKCS12 dans le terminal. Vous pouvez copier les données. Les données du point de confiance sont protégées par un mot de passe. Toutefois, si vous enregistrez les données du point de confiance dans un fichier, assurez-vous que celui-ci se trouve dans un emplacement sécurisé.

Étape 2 Importez les paires de clés et les certificats émis qui sont associés à une configuration de point de confiance.

crypto ca import *trustpoint* **pkcs12***passphrase*

Exemple :

```
ciscoasa(config)# crypto ca import Main pkcs12 ?
```

L'ASA vous invite à coller le texte dans le terminal au format base 64. Une étiquette correspondant au nom du point de confiance que vous créez est attribuée à la paire de clés importée avec le point de confiance.

Remarque
Si un ASA dispose de points de confiance qui partagent la même CA, vous ne pouvez utiliser qu'un seul des points de confiance qui partagent la CA pour valider les certificats d'utilisateur. Pour contrôler le partage du point de confiance qu'une CA utilise pour la validation des certificats d'utilisateur émis par cette CA, utilisez le mot clé **support-user-cert-validation**.

Exemples

L'exemple suivant exporte les données PKCS12 pour le point de confiance principal avec la phrase secrète Wh0zits :

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

L'exemple suivant importe manuellement les données PKCS12 dans le point de confiance principal avec la phrase secrète Wh0zits :

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

Dans l'exemple suivant, un certificat est importé manuellement pour le point de confiance principal :

```
ciscoasa (config)# crypto ca import Main certificate
% The fully qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

Configurer les règles de mappage des certificats CA

Vous pouvez configurer des règles en fonction des champs Issuer (Émetteur) et Subject (Sujet) d'un certificat. En utilisant les règles que vous créez, vous pouvez mapper les certificats d'homologues IPsec aux groupes de tunnels à l'aide de la commande **tunnel-group-map**.

Pour configurer une règle de mappage de certificat CA, procédez comme suit :

Procédure

Étape 1 Entrez dans le mode de configuration de la carte de certificat CA pour la règle que vous souhaitez configurer et précisez le numéro de séquence de la règle.

crypto ca certificate map [*map_name*]*sequence-number*

Exemple :

```
ciscoasa(config)# crypto ca certificate map test-map 10
```

Si vous ne spécifiez pas le nom de la carte, la règle est ajoutée à la carte par défaut : DefaultCertificateMap. Pour chaque numéro de règle, vous pouvez spécifier un ou plusieurs champs à faire correspondre.

Étape 2 Spécifiez le nom de l'émetteur ou le nom du sujet :

{**issuer-name** | **subject-name**} [**attr** *attribute*] *operator string*

Exemple :

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr uid eq jcrichton
```

Vous pouvez faire correspondre la valeur complète ou spécifier les attributs que vous souhaitez faire correspondre. Les attributs suivants sont valides :

- c : pays
- cn : nom commun
- dc : composant de domaine
- dnq : qualificateur de nom distinctif
- emailAddress : adresse courriel
- genq : qualificatif générationnel
- gn : prénom
- i : initiales
- ip : adresse IP
- l : localité
- n : nom
- o : nom de l'organisation
- ou : unité organisationnelle
- ser : numéro de série

Remarque

Assurez-vous de spécifier l'attribut de numéro de série dans le nom d'objet. Le mappage de certificat correspond uniquement à un attribut de numéro de série spécifié dans le nom d'objet.

- sn : nom de famille
- sp : État/province
- t : titre
- uid : ID d'utilisateur
- uname : nom non structuré

Voici des opérateurs valides :

- eq : le champ ou l'attribut doit être identique à la valeur donnée.
- ne : le champ ou l'attribut ne peut pas être identique à la valeur attribuée.
- co : une partie ou la totalité du champ ou de l'attribut doit correspondre à la valeur donnée.
- nc : aucune partie du champ ou de l'attribut ne peut correspondre à la valeur donnée.

Étape 3 Spécifiez l'autre nom d'objet :

alt-subject-name *operator string*

Exemple :

```
ciscoasa(config-ca-cert-map)# alt-subject-name eq happydays
```

Voici des opérateurs valides :

- eq : le champ doit être identique à la valeur donnée.
- ne : le champ ne peut pas être identique à la valeur donnée.
- co : une partie ou la totalité du champ doit correspondre à la valeur donnée.
- nc : aucune partie du champ ne peut correspondre à la valeur donnée.

Étape 4 Spécifiez l'utilisation de la clé étendue :

extended-key-usage *operator OID_string*

Exemple :

```
ciscoasa(config-ca-cert-map)# extended-key-usage nc clientauth
```

Voici des opérateurs valides :

- co : une partie ou la totalité du champ doit correspondre à la valeur donnée.
- nc : aucune partie du champ ne peut correspondre à la valeur donnée.

Voici des chaînes OID valides :

- *string* : chaîne définie par l'utilisateur.

- clientauth : authentification du client (1.3.6.1.5.5.7.3.2)
- codesigning : signature de code (1.3.6.1.5.5.7.3.3)
- emailprotection – Secure Email Protection (1.3.6.1.5.5.7.3.4)
- ocspsigning : signature OCSP (1.3.6.1.5.5.7.3.9)
- serverauth : authentification du serveur (1.3.6.1.5.5.7.3.1)
- timestamping : horodatage (1.3.6.1.5.5.7.3.8)

Configurer les identités de référence

Lorsque l'ASA agit en tant que client TLS, il prend en charge les règles de vérification de l'identité d'un serveur d'applications, comme défini dans la RFC 6125. Cette RFC spécifie les procédures pour représenter les identités de référence (configurées sur l'ASA) et les vérifier par rapport aux identités présentées (envoyées par le serveur d'applications). Si l'identité présentée ne peut pas être comparée à l'identité de référence configurée, la connexion n'est pas établie et une erreur est enregistrée.

Le serveur présente son identité en incluant un ou plusieurs identifiants dans le certificat de serveur présenté à l'ASA lors de l'établissement de la connexion. Les identités de référence sont configurées sur l'ASA pour être comparées à l'identité présentée dans un certificat de serveur lors de l'établissement de la connexion. Ces identifiants sont des instances spécifiques des quatre types d'identifiants spécifiés dans la RFC 6125. Les quatre types d'identifiants sont les suivants :

- CN_ID : nom distinctif relatif (RDN) dans un champ d'objet de certificat qui ne contient qu'une seule paire d'attributs types et de valeurs de type de nom commun (CN), dans lequel la valeur correspond à la forme globale d'un nom de domaine. La valeur CN ne peut pas être en texte libre. Un identifiant de référence CN-ID n'identifie pas un service d'application.
- DNS-ID : une entrée subjectAltName de type dNSName. Il s'agit d'un nom de domaine DNS. Un identifiant de référence DNS-ID n'identifie pas un service d'application.
- SRV-ID : une entrée subjectAltName de type otherName dont le format de nom est SRVName comme défini dans la RFC 4985. Un identifiant SRV-ID peut contenir à la fois un nom de domaine et un type de service d'application. Par exemple, un SRV-ID de « _imaps.example.net » serait divisé en une partie de nom de domaine DNS de « example.net » et une partie de type de service d'application de « imaps ».
- URI-ID : Une entrée subjectAltName de type uniformResourceIdentifier dont la valeur comprend à la fois (i) un schéma et (ii) un composant « hôte » (ou son équivalent) qui correspond à la règle « reg-name » spécifiée dans la RFC 3986. Un identifiant URI-ID doit contenir le nom de domaine DNS, pas l'adresse IP et pas seulement le nom d'hôte. Par exemple, un URI-ID de « sip:voice.example.edu » serait divisé en une partie de nom de domaine DNS de « voice.example.edu » et un type de service d'application de « sip ».

Une identité de référence est créée lors de la configuration d'une identité avec un nom précédemment inutilisé. Une fois qu'une identité de référence a été créée, les quatre types d'identifiants et leurs valeurs associées peuvent être ajoutés ou supprimés de l'identité de référence. Les identifiants de référence PEUVENT contenir des renseignements identifiant le service d'application et doivent contenir des renseignements identifiant le nom de domaine DNS.

Avant de commencer

- Les identités de référence sont utilisées lors de la connexion au serveur de journal système et au serveur de licences Smart uniquement. Aucune autre connexion en mode client SSL ASA ne prend actuellement en charge la configuration ou l'utilisation des identités de référence.
- L'ASA met en œuvre toutes les règles de correspondance des identifiants décrites dans la RFC 6125, à l'exception des certificats épinglés et du système de secours pour les clients interactifs.
- La possibilité d'épingler des certificats n'est pas mise en œuvre. Par conséquent, `aucune correspondance n'a été trouvée, le certificat épinglé` ne se produira pas. De plus, un utilisateur n'aura pas la possibilité d'épingler un certificat si aucune correspondance n'est trouvée, car notre mise en œuvre n'est pas un client interactif.

Procédure

Étape 1 Saisissez la commande **[no] crypto ca reference-identity** dans le mode de configuration globale pour placer l'ASA en mode ca-reference-identity.

[no] crypto ca reference-identity *reference-identity-name*

Si aucune identité de référence avec ce *reference-identity-name* n'est trouvée, une nouvelle identité de référence est créée. Si la forme **no** de la commande est exécutée pour une identité de référence toujours utilisée, un avertissement s'affiche et l'identité de référence n'est pas supprimée.

Étape 2 Saisissez les ID de référence en mode ca-reference-identity. Plusieurs identifiants de référence de tout type peuvent être ajoutés à l'identité de référence.

- **[no] cn-id** *value*
- **[no] dns-id** *value*
- **[no] srv-id** *value*
- **[no] uri-id** *value*

Pour supprimer une identité de référence, utilisez la forme no de la commande.

Exemple

Configurez une identité de référence pour la validation du certificat de serveur RFC 6125 pour un serveur de journal système :

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Prochaine étape

Utilisez l'identité de référence lors de la configuration des connexions du journal système et du serveur Smart Call Home.

Obtenir des certificats manuellement

Pour obtenir des certificats manuellement, procédez comme suit :

Avant de commencer

Vous devez déjà avoir obtenu un certificat CA codé en base-64 auprès de la CA représentée par le point de confiance.

Procédure

Étape 1 Importez le certificat CA pour le point de confiance configuré.

crypto ca authenticate *trustpoint*

Exemple :

```
ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:     24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

L'utilisation de la commande **enrollment terminal** lors de la configuration du point de confiance requiert que vous obteniez manuellement des certificats.

Étape 2 Inscrivez l'ASA auprès du point de confiance.

crypto ca enroll *trustpoint*

Exemple :

```
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---
```

```
Redisplay enrollment request? [yes/no]: n
```

Cette commande génère un certificat pour la signature des données et, en fonction du type de clés que vous avez configuré, pour le chiffrement des données. Si vous utilisez des clés RSA distinctes pour la signature et le chiffrement, la commande **crypto ca enroll** affiche deux demandes de certificat, une pour chaque clé. Si vous utilisez des clés RSA à usage général pour la signature et le chiffrement, la commande **crypto ca enroll** affiche une demande de certificat.

Pour terminer l'inscription, procurez-vous un certificat pour toutes les demandes de certificat générées par la commande **crypto ca enroll** auprès de la CA représentée par le point de confiance applicable. Assurez-vous que le certificat est au format base-64.

Étape 3 Lorsqu'un point de confiance est configuré pour CMP, il est possible de spécifier une valeur secrète partagée (ir) ou le nom du point de confiance qui contient le certificat qui signera la demande (cr), mais pas les deux. Fournissez une valeur hors bande par la CA qui est utilisée pour confirmer l'authentification et l'intégrité des messages échangés avec l'ASA ou fournissez le nom du point de confiance avec un certificat d'appareil précédemment émis et utilisé pour signer la demande d'inscription CMP. Les mots clés de secrets partagés ou de certificats de signature ne sont disponibles que lorsque le protocole d'inscription du point de confiance est défini sur CMP.

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

Étape 4 Déterminez si une nouvelle paire de clés doit être générée ou non avant de créer la demande d'inscription.

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

Étape 5 Importez chaque certificat que vous recevez de la CA et assurez-vous de coller le certificat dans le terminal au format base-64.

crypto ca import *trustpoint* **certificate**

Exemple :

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

Étape 6 Vérifiez que le processus d'inscription a réussi en affichant les détails du certificat émis pour l'ASA et le certificat CA pour le point de confiance.

show crypto ca certificate

Exemple :

```
ciscoasa(config)# show crypto ca  certificate Main
```

Étape 7 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 8 Répétez ces étapes pour chaque point de confiance que vous configurez pour l'inscription manuelle.

Obtenir des certificats automatiquement avec SCEP

Cette section décrit comment obtenir automatiquement des certificats en utilisant SCEP.

Avant de commencer

Vous devez déjà avoir obtenu un certificat CA codé en base-64 auprès de la CA représentée par le point de confiance.

Procédure

Étape 1 Obtenez le certificat CA pour le point de confiance configuré.

crypto ca authenticate *trustpoint*

Exemple :

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

Lorsque vous configurez le point de confiance, l'utilisation de la commande **enrollment url** détermine si vous devez obtenir les certificats automatiquement ou non par SCEP.

Étape 2 Inscrivez l'ASA auprès du point de confiance. Cette commande récupère un certificat pour la signature des données et, en fonction du type de clés que vous avez configuré, pour le chiffrement des données. Avant d'entrer cette commande, communiquez avec l'administrateur CA, qui devra peut-être authentifier la demande d'inscription manuellement avant que la CA n'accorde les certificats.

crypto ca enroll *trustpoint*

Exemple :

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

Si l'ASA ne reçoit pas de certificat de la CA dans un délai d'une minute (par défaut) après l'envoi d'une demande de certificat, il renvoie la demande de certificat. L'ASA continue d'envoyer une demande de certificat chaque minute jusqu'à ce qu'un certificat soit reçu.

Si le nom de domaine complet configuré pour le point de confiance n'est pas identique au nom de domaine complet de l'ASA, y compris la casse des caractères, un avertissement s'affiche. Pour résoudre ce problème, quittez le processus d'inscription, apportez les corrections nécessaires et saisissez à nouveau la commande **crypto ca enroll**.

Remarque
Si l'ASA redémarre après que vous ayez lancé la commande **crypto ca enroll**, mais avant que vous ayez reçu le certificat, saisissez la commande **crypto ca enroll** et avisez l'administrateur CA.

Étape 3 Vérifiez que le processus d'inscription a réussi en affichant les détails du certificat émis pour l'ASA et le certificat CA pour le point de confiance.

show crypto ca certificate

Exemple :

```
ciscoasa/contexta(config)# show crypto ca certificate Main
```

Étape 4 Enregistrez la configuration en cours d'exécution.

write memory

Exemple :

```
ciscoasa/contexta(config)# write memory
```

Configurer la prise en charge du serveur mandataire pour les demandes SCEP

Pour configurer l'ASA afin d'authentifier les points terminaux d'accès à distance à l'aide d'autorités de certification tierces, procédez comme suit :

Procédure

Étape 1 Entrez le mode de configuration tunnel-group ipsec-attributes.

tunnel-group *nom* **ipsec-attributes**

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

Étape 2 Activez les services clients.

crypto ikev2 enable outside client-services port *portnumber*

Exemple :

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

Le numéro de port par défaut est 443.

Remarque
Cette commande est nécessaire uniquement si vous prenez en charge IKEv2.

Étape 3 Entrez dans le mode de configuration tunnel-group general-attributes.

tunnel-group *nom* **general-attributes**

Exemple :

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

Étape 4 Activez l'inscription SCEP pour le groupe de tunnels.

scep-enrollment enable

Exemple :

```
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this option.
```

Étape 5 Entrez dans le mode de configuration des attributs group-policy.

group-policy *nom* **attributes**

Exemple :

```
ciscoasa(config)# group-policy FirstGroup attributes
```

Étape 6 Inscrivez la CA SCEP pour la stratégie de groupe. Entrez cette commande une fois par stratégie de groupe pour prendre en charge un certificat numérique tiers.

scep-forwarding-url value *URL*

Exemple :

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

URL est l'URL SCEP sur la CA.

Étape 7 Fournissez un mot de passe secondaire commun lorsqu'aucun certificat n'est disponible pour la prise en charge WebLaunch du mandataire SCEP.

secondary-pre-fill-username clientless hide use-common-password *password*

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
use-common-password secret
```

Vous devez utiliser le mot clé **hide** pour prendre en charge le mandataire SCEP.

Par exemple, un certificat n'est pas disponible pour un terminal qui en demande un. Une fois que le terminal a le certificat, l'Secure Client (services client sécurisés) se déconnecte, puis se reconnecte à l'ASA pour bénéficier d'une politique DAP qui fournit un accès aux ressources de réseau interne.

Étape 8 Masquez le nom d'utilisateur prérempli secondaire pour les sessions VPN Secure Client (services client sécurisés).

secondary-pre-fill-username ssl-client hide use-common-password *password*

Exemple :

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
```

```
use-common-password secret
```

Malgré le mot clé **ssl-client** hérité des versions précédentes, utilisez cette commande pour prendre en charge les sessions Secure Client (services client sécurisés) qui utilisent IKEv2 ou SSL.

Vous devez utiliser le mot clé **hide** pour prendre en charge le mandataire SCEP.

Étape 9 Fournissez le nom d'utilisateur lorsqu'aucun certificat n'est disponible.

secondary-username-from-certificate {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]

Exemple :

```
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback
 cisco-secure-desktop machine-unique-id
```

Comment configurer des types de certificats spécifiques

Après avoir établi des certificats de confiance, vous pouvez commencer d'autres tâches fondamentales telles que l'établissement de certificats d'identité ou des configurations plus avancées telles que l'établissement de certificats CA local ou de signature de code.

Avant de commencer

Lisez les renseignements sur les certificats numériques et établissez des certificats de confiance. Les certificats CA sans clé privée sont utilisés par tous les protocoles VPN et webvpn, et sont configurés dans des points de confiance pour valider les certificats clients entrants. De même, un groupe de confiance est une liste de certificats de confiance utilisés par les fonctionnalités de webvpn pour valider les connexions mandataires aux serveurs https et pour valider le certificat smart-call-home.

Procédure

Une CA locale permet aux clients VPN d'inscrire des certificats directement auprès de l'ASA. Cette configuration avancée convertit l'ASA en une CA. Pour configurer les CA, consultez Certificats de l'autorité de certification (CA), à la page 34.

Prochaine étape

Configurez une alerte d'expiration de certificat ou surveillez les certificats numériques et l'historique de gestion des certificats.

Certificats de l'autorité de certification (CA)

Cette page vous permet de gérer les certificats CA. Les rubriques suivantes expliquent ce que vous pouvez faire.

Gestion du serveur CA

Configurer l'importation automatique des certificats de groupe de confiance

La licence Smart utilise l'infrastructure Smart Call Home. Lorsque l'ASA configure les rapports anonymes de Smart Call Home en arrière-plan, l'ASA crée automatiquement un point de confiance contenant le certificat de la CA qui a émis le certificat de serveur Call Home. L'ASA prend désormais en charge la validation du certificat si la hiérarchie d'émission du certificat de serveur change, sans avoir besoin de l'intervention du client pour ajuster les modifications à la hiérarchie des certificats. Vous pouvez automatiser la mise à jour de l'ensemble de groupes de confiance à des intervalles périodiques afin que Smart Call Home puisse rester actif si le certificat autosigné du serveur CA change. Cette fonctionnalité n'est pas prise en charge dans le cadre des déploiements à contextes multiples.

L'importation automatique des ensembles de certificat de confiance vous oblige à spécifier l'URL utilisée par l'ASA pour télécharger et importer le groupe. Utilisez la commande suivante pour que l'importation ait lieu quotidiennement à des intervalles réguliers avec l'URL Cisco par défaut et l'heure par défaut de 22 heures :

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

Vous pouvez également activer l'importation automatique avec une URL personnalisée à l'aide de la commande suivante :

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

Pour vous offrir plus de flexibilité pour définir les téléchargements en dehors des heures de pointe ou à d'autres moments pratiques, saisissez la commande suivante qui active l'importation avec une heure personnalisée :

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

La définition de l'importation automatique avec une URL personnalisée et une heure personnalisée nécessite la commande suivante :

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

Afficher l'état de la politique de groupe de confiance

Utilisez la commande suivante pour voir l'état actuel de la politique de groupe de confiance :

```
show crypto ca trustpool policy
```

Cette commande renvoie les renseignements suivants :

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
```

```
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

Effacer le groupe de confiance CA

Pour réinitialiser la politique de groupe de confiance à son état par défaut, utilisez la commande suivante :

```
clear configure crypto ca trustpool
```

Étant donné que l'importation automatique des certificats de point de confiance est désactivée par défaut, l'utilisation de cette commande désactive la fonctionnalité.

Définir une alerte d'expiration de certificat (pour les certificats d'identité ou CA)

L'ASA vérifie tous les certificats CA et d'ID des points de confiance pour déterminer leur expiration une fois toutes les 24 heures. Si un certificat est sur le point d'expirer, un journal système sera émis en tant qu'alerte.

Une interface de ligne de commande est fournie pour configurer les intervalles de rappel et de récurrence. Par défaut, les rappels commencent à 60 jours avant l'expiration et se répèteront tous les 7 jours. Vous pouvez configurer l'intervalle auquel les rappels sont envoyés et le nombre de jours avant l'expiration à laquelle la première alerte est envoyée en utilisant la commande suivante :

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

Quelle que soit la configuration des alertes, un rappel est envoyé chaque jour pendant la dernière semaine d'expiration. Les commandes **show** et **clear** suivantes ont également été ajoutées :

```
clear conf crypto ca alerts
show run crypto ca alerts
```

En plus du rappel de réabonnement, si un certificat déjà expiré est détecté dans la configuration, un journal système est généré une fois par jour pour rectifier la configuration en renouvelant le certificat ou en supprimant le certificat expiré.

Par exemple, supposons que les alertes d'expiration sont configurées pour commencer à 60 jours et se répètent ensuite tous les 6 jours. Si l'ASA est redémarré au bout de 40 jours, une alerte est envoyée ce jour-là et l'alerte suivante est envoyée le 36e jour.

Remarque La vérification de l'expiration n'est pas effectuée sur les certificats de groupe de confiance. Le point de confiance CA local est également traité comme un point de confiance normal pour la vérification de l'expiration.

Supervision des certificats numériques

Consultez les commandes suivantes pour superviser l'état du certificat numérique :

- **show crypto ca server**

  Cette commande affiche la configuration et l'état de la CA locale.

- **show crypto ca server cert-db**

  Cette commande affiche les certificats d'utilisateur émis par la CA locale.

- **show crypto ca server certificate**

  Cette commande affiche les certificats de la CA locale sur la console au format base 64 et le certificat de renouvellement, lorsqu'ils sont disponibles, y compris l'empreinte numérique du certificat de renouvellement pour la vérification du nouveau certificat lors de l'importation sur d'autres périphériques.

- **show crypto ca server crl**

  Cette commande affiche les CRL.

- **show crypto ca server user-db**

  Cette commande affiche les utilisateurs et leur état. Elle peut être utilisée avec les qualificateurs suivants pour réduire le nombre d'enregistrements affichés :

  - allowed. Affiche uniquement les utilisateurs actuellement autorisés à s'inscrire.
  - enrolled. Affiche uniquement les utilisateurs inscrits et titulaires d'un certificat valide.
  - expired. Affiche uniquement les utilisateurs titulaires de certificats expirés.
  - on-hold. Répertorie uniquement les utilisateurs sans certificat et qui ne sont actuellement pas autorisés à s'inscrire.

- **show crypto ca server user-db allowed**

  Cette commande affiche les utilisateurs admissibles à l'inscription.

- **show crypto ca server user-db enrolled**

  Cette commande affiche les utilisateurs inscrits disposant de certificats valides.

- **show crypto ca server user-db expired**

  Cette commande affiche les utilisateurs disposant de certificats expirés.

- **show crypto ca server user-db on-hold**

  Cette commande affiche les utilisateurs sans certificat qui ne sont pas autorisés à s'inscrire.

- **show crypto key** *name of key*

  Cette commande affiche les paires de clés que vous avez générées.

- **show running-config**

  Cette commande affiche les règles de mappage des certificats émis par la CA locale.

Exemples

L'exemple suivant montre une clé RSA à usage général :

```
ciscoasa/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  00ea2c38 df9c606e ddb7b08a e8b0a1a8 65592d85 0711cac5 fceddee1 fa494297
  525fffc0 90da8a4c e696e44e 0646c661 48b3602a 960d7a3a 52dae14a 5f983603
  e1f33e40 a6ce04f5 9a812894 b0fe0403 f8d7e05e aea79603 2dcd56cc 01261b3e
  93bff98f df422fb1 2066bfa4 2ff5d2a4 36b3b1db edaebf16 973b2bd7 248e4dd2
  071a978c 6e81f073 0c4cd57b db6d9f40 69dc2149 e755fb0f 590f2da8 b620efe6
  da6e8fa5 411a841f e72bb8ea cf4bdb79 f4e57ff3 a940ce3b 4a2c7052 56c1d17b
  af8fe2e2 e58718c6 ed1da0f0 1c6f36eb 79eb1aeb f098b5c4 79e07658 a52d8c7a
  51ceabfb f8ade096 7217cf2d 3728077e 89441d89 9bf5f875 c8d2db39 c858bb7a
  7d020301 0001
```

L'exemple suivant montre la liste CRL de la CA locale :

```
ciscoasa(config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

L'exemple suivant montre un utilisateur en attente :

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

L'exemple suivant montre la sortie de commande **show running-config**, dans laquelle s'affichent les règles de mappage des certificats émis par la CA locale :

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

Historique de gestion des certificats

Tableau 1 : Historique de gestion des certificats

Nom de la caractéristique	Versions de plateforme	Description
Certificate Management	7.0(1)	Les certificats numériques (y compris les certificats CA, les certificats d'identité et les certificats de signataire de code) fournissent une identification numérique pour l'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur. Les autorités de certification émettent des certificats numériques dans le contexte d'une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité.
Certificate Management	7.2(1)	Nous avons introduit les commandes suivantes : **issuer-name** *DN-string*, **revocation-check crl none**, **revocation-check crl**, **revocation-check none**. Nous avons rendu obsolètes les commandes suivantes : **crl** {**required** | **optional** | **nocheck**}.
Certificate Management	8.0(2)	Nous avons introduit les commandes suivantes : **cdp-url**, **crypto ca server**, **crypto ca server crl issue**, **crypto ca server revoke** *cert-serial-no*, **crypto ca server unrevoke** *cert-serial-no*, **crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*], **crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**], **crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}, **crypto ca server user-db remove** *username*, **crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}, **crypto ca server user-db write**, [**no**] **database path** *mount-name directory-path*, **debug crypto ca server** [*level*], **lifetime** {**ca-certificate** | **certificate** | **crl**} *time*, **no shutdown**, **otp expiration** *timeout*, **renewal-reminder** *time*, **show crypto ca server**, **show crypto ca server cert-db** [**user** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*], **show crypto ca server certificate**, **show crypto ca server crl**, **show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**], **show crypto key** *name of key*, **show running-config**, **shutdown**.

Nom de la caractéristique	Versions de plateforme	Description
Mandataire SCEP	v 8.4(1)	Nous avons introduit cette fonctionnalité, qui permet un déploiement sécurisé des certificats de périphérique à partir d'autorités de certification tierces. Nous avons introduit les commandes suivantes : **crypto ikev2 enable outside client-services port** *portnumber*, **scep-enrollment enable**, **scep-forwarding-url value** *URL*, **secondary-pre-fill-username clientless hide use-common-password** *password*, **secondary-pre-fill-username ssl-client hide use-common-password** *password*, **secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**].
Identités de référence	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée pendant la validation PKI pour les connexions TLS au serveur de journal système et au serveur de licences Smart uniquement. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons ajouté ou modifié les commandes suivantes : **crypto ca reference-identity**, **logging host**, **call home profile destination address**
Serveur CA local	9.12(1)	Pour que le FQDN de l'URL d'inscription soit configurable au lieu d'utiliser le FQDN configuré de l'ASA, une nouvelle option d'interface de ligne de commande est introduite. Cette nouvelle option est ajoutée au mode smpt du serveur CA de chiffrement. Nous avons rendu obsolète le serveur CA local et le supprimerons dans une version ultérieure : lorsque l'ASA est configuré en tant que serveur CA local, il est en mesure d'émettre des certificats numériques, de publier des listes de révocation de certificats (CRL) et de révoquer en toute sécurité les certificats émis. Cette fonctionnalité a été abandonnée et, par conséquent, la commande du serveur CA de chiffrement l'a été aussi.
Serveur CA local	9.13(1)	Nous avons supprimé la prise en charge du serveur CA local. Ainsi, la commande **crypto ca server** et ses sous-commandes sont supprimées. Nous avons supprimé les commandes suivantes : **crypto ca server** et toutes ses sous-commandes.

Nom de la caractéristique	Versions de plateforme	Description
Modifications des commandes du point de distribution de la CRL	9.13(1)	Les commandes de configuration d'URL de CDP statiques sont supprimées et déplacées vers la commande de certificat correspondante. Commandes nouvelles ou modifiées : **crypto-ca-trustpoint crl** et **crl url** ont été supprimées avec d'autres logiques connexes. **match-certificate override-cdp** a été introduite.
Taille du cache de la CRL augmentée	9.13(1)	Pour éviter l'échec de téléchargements de CRL volumineux, la taille du cache a été augmentée et la limite du nombre d'entrées dans une CRL individuelle a été supprimée. • Augmentation de la taille totale du cache de la CRL à 16 Mo par contexte pour le mode de contexte multiple. • Augmentation de la taille totale du cache de la CRL à 128 Mo pour le mode de contexte unique.
Option de restauration des contrôles de validité du certificat de contournement	9.15(1)	L'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP, qui avait été supprimée dans la version 9.13(1), a été rétablie. Commandes nouvelles ou modifiées : **revocation-check crl none**, **revocation-check ocsp none**, **revocation-check crl ocsp none** et **revocation-check ocsp crl none** ont été restaurées.
Modifications apportées aux commandes de certificat correspondantes pour prendre en charge l'URL du point de distribution de la CRL statique	9.15(1)	La commande de configuration d'URL de CDP statiques a permis aux CDP statiques d'être mappés de façon unique à chaque certificat d'une chaîne validée. Cependant, un seul de ces mappages était pris en charge pour chaque certificat. Cette modification permet aux CDP configurés de manière statique d'être mappés à une chaîne de certificats pour l'authentification. Commandes nouvelles ou modifiées : **match certificate** *map* **override cdp** *seq* **url** *url* and **no match certificate** *map* **override cdp** *seq* **url** *url*
Les modifications apportées à la paire de clés du point de confiance et à la clé de chiffrement génèrent des commandes	9.16(1)	La prise en charge des certificats avec des tailles de clé inférieures à 2 048 a été supprimée. Toute configuration utilisant des options de 512, 768 ou 1 024 bits est transférée vers la version 2 048 avec notification dûe. La prise en charge de l'utilisation de l'algorithme de hachage SHA1 pour la certification a été supprimée. **Remarque** La commande **crypto ca permit-weak-crypto** a été introduite pour remplacer ces restrictions. La nouvelle option de clé EDDSA a été ajoutée aux options RSA et ECDSA existantes.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.