Rapports anonymes et Smart Call Home

Ce chapitre décrit comment configurer les services de création de rapports anonymes et les services Smart Call Home.

À propos des rapports anonymes

Vous pouvez contribuer à l'amélioration de la plateforme ASA en activant les rapports anonymes, qui permettent à Cisco de recevoir en toute sécurité un minimum de renseignements sur les erreurs et l'intégrité de l'appareil. Si vous activez la fonctionnalité, votre identité de client restera anonyme et aucune information d'identification ne sera envoyée.

L'activation de la création de rapports anonymes crée un point de confiance et installe un certificat. Un certificat CA est requis pour que votre ASA valide le certificat de serveur présent sur le serveur Web Smart Call Home et pour former la session HTTPS afin que votre ASA puisse envoyer des messages en toute sécurité. Cisco importe un certificat prédéfini dans le logiciel. Si vous décidez d'activer les rapports anonymes, un certificat est installé sur l'ASA avec un nom de point de confiance codé en dur : _SmartCallHome_ServerCA. Lorsque vous activez la création de rapports anonymes, ce point de confiance est créé, le certificat approprié est installé et vous recevez un message au sujet de cette action. Le certificat apparaît ensuite dans votre configuration.

Si le certificat approprié existe déjà dans votre configuration lorsque vous activez les rapports anonymes, aucun point de confiance n'est créé et aucun certificat n'est installé.

Remarque Lorsque vous activez les rapports anonymes, vous acceptez de transférer les données spécifiées à Cisco ou aux fournisseurs agissant pour le compte de Cisco (y compris dans des pays en dehors des États-Unis). Cisco protège la confidentialité de tous ses clients. Pour en savoir plus sur le traitement des renseignements personnels par Cisco, consultez la Déclaration de confidentialité de Cisco à l'adresse suivante : http://www.cisco.com/web/siteassets/legal/privacy.html

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 émet 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 apporter des modifications à la hiérarchie des certificats. Vous pouvez également importer automatiquement les certificats du groupe de confiance afin que l'ASA renouvelle la hiérarchie des certificats sans intervention manuelle.

Lorsque vous mettez à niveau ASA 9.14(2.14), la configuration du point de confiance passe automatiquement de CallHome_ServerCA à CallHome_ServerCA2.

Exigence DNS

Un serveur DNS doit être configuré correctement pour que l'ASA atteigne le serveur Cisco Smart Call Home et envoie des messages à Cisco. Comme il est possible que l'ASA réside dans un réseau privé et n'ait pas accès au réseau public, Cisco vérifie votre configuration DNS puis la configure pour vous, au besoin, en procédant comme suit :

1. Effectuer une recherche DNS pour tous les serveurs DNS configurés.
2. Obtenir le serveur DNS à partir du serveur DHCP en envoyant des messages DHCPINFORM sur l'interface du niveau de sécurité le plus élevé.
3. Utiliser les serveurs DNS de Cisco pour la recherche.
4. Utiliser des adresses IP statiques de façon aléatoire pour tools.cisco.com.

Ces tâches sont effectuées sans modifier la configuration actuelle. (Par exemple, le serveur DNS appris à partir du DHCP ne sera pas ajouté à la configuration.)

Si aucun serveur DNS n'est configuré et que l'ASA ne peut pas atteindre le serveur Cisco Smart Call Home, Cisco génère un message de journal système avec le niveau de gravité d'avertissement pour chaque message Smart Call Home envoyé pour vous rappeler de configurer le DNS correctement.

Consultez le guide des messages de journal système pour obtenir des renseignements sur les messages de journal système.

À propos de Smart Call Home

Une fois entièrement configuré, Smart Call Home détecte les problèmes sur votre site et les signale à Cisco ou par l'intermédiaire d'autres canaux définis par l'utilisateur (comme la messagerie électronique ou directement), souvent avant même que vous ne soyez conscient de l'existence de ces problèmes. Selon la gravité de ces problèmes, Cisco répond à vos problèmes de configuration système, à vos annonces de fin de vie de produit, à vos problèmes d'avis de sécurité, etc. en fournissant les services suivants :

- Identification rapide des problèmes grâce à une surveillance continue, des alertes proactives en temps réel et des diagnostics détaillés.
- Signalement des problèmes potentiels grâce aux notifications Smart Call Home, dans lesquelles une demande de service a été ouverte, avec toutes les données de diagnostic jointes.
- Résolution plus rapide des problèmes critiques grâce à un accès direct et automatique aux experts du TAC de Cisco.
- Utilisation plus efficace des ressources en personnel grâce à une résolution de problèmes plus rapide.
- Génération automatique des demandes de service auprès du TAC de Cisco (si vous disposez d'un contrat de service), acheminées vers l'équipe d'assistance appropriée, qui fournit des renseignements détaillés à propos du diagnostic permettant d'accélérer la résolution des problèmes.

Le portail Smart Call Home offre un accès rapide aux renseignements requis qui vous permettent d'effectuer les opérations suivantes :

- Passer en revue tous les messages, les diagnostics et les recommandations de Smart Call Home en un seul endroit.
- Vérifier l'état des demandes de service.
- Consulter les renseignements les plus récents sur l'inventaire et la configuration de tous les appareils compatibles avec Smart Call Home.

S'abonner aux groupes d'alertes

Un groupe d'alertes est un sous-ensemble prédéfini des alertes Smart Call Home prises en charge par l'ASA. Les différents types d'alertes Smart Call Home sont regroupés dans différents groupes d'alertes, selon leur type. Chaque groupe d'alertes signale la sortie de certaines interfaces de ligne de commande. Les groupes d'alertes Smart Call Home pris en charge sont les suivants :

- syslog
- diagnostic
- environnement
- stocks
- configuration
- menace
- snapshot
- télémétrie
- test

Attributs des groupes d'alertes

Les groupes d'alertes ont les attributs suivants :

- Les événements s'enregistrent d'abord auprès d'un groupe d'alertes.

- Un groupe peut s'associer à plusieurs événements.
- Vous pouvez vous abonner à des groupes d'alertes spécifiques.
- Vous pouvez activer et désactiver des groupes d'alertes spécifiques. Le paramètre par défaut est activé pour tous les groupes d'alertes.
- Les groupes d'alertes de diagnostic et d'environnement prennent en charge l'abonnement aux messages périodiques.
- Le groupe d'alertes de journal système prend en charge l'abonnement basé sur l'ID de message.
- Vous pouvez configurer un seuil pour l'utilisation du CPU et de la mémoire pour le groupe d'alertes d'environnement. Lorsqu'un paramètre donné a dépassé un seuil prédéfini, un message est envoyé. La plupart des valeurs de seuil dépendent de la plateforme et ne peuvent pas être modifiées.
- Vous configurez le groupe d'alertes d'instantané pour envoyer la sortie des interfaces de ligne de commande que vous spécifiez.

Messages envoyés à Cisco par des groupes d'alertes

Les messages sont envoyés à Cisco périodiquement et chaque fois que l'ASA se recharge. Ces messages sont classés par groupes d'alertes.

Les alertes d'inventaire comprennent la sortie des commandes suivantes :

- **show version** : affiche la version du logiciel ASA, la configuration matérielle, la clé de licence et les données de disponibilité associées pour le périphérique.
- **show inventory—**Récupère et affiche les renseignements d'inventaire sur chaque produit Cisco installé dans l'appareil réseau. Chaque produit est identifié par des renseignements d'appareil uniques, appelés UDI, qui est une combinaison de trois éléments de données distincts : l'identifiant de produit (PID), l'identifiant de version (VID) et le numéro de série (SN).
- **show failover state** : affiche l'état de basculement des deux unités d'une paire de basculement. Les renseignements affichés comprennent l'état principal ou secondaire de l'unité, l'état actif/veille de l'unité et le dernier motif signalé pour le basculement.
- **show environment** : affiche des renseignements sur l'environnement système pour les composants du système ASA, tels que l'état opérationnel du matériel pour le châssis, les pilotes, les ventilateurs et les alimentations, ainsi que l'état de la température, la tension et l'utilisation du processeur.

Les alertes de configuration comprennent la sortie des commandes suivantes :

- **show context** : affiche les interfaces allouées et l'URL du fichier de configuration, le nombre de contextes configurés, ou si vous activez la création de rapports anonymes dans l'espace d'exécution du système, à partir d'une liste de tous les contextes.
- **show call-home registered-module status** : affiche l'état du module enregistré. Si vous utilisez le mode de configuration système, la commande affiche l'état du module de système en fonction de l'ensemble du périphérique, et non en fonction du contexte.
- **show running-config** : affiche la configuration en cours d'exécution sur l'ASA.
- **show startup-config** : affiche la configuration de démarrage.

- **show access-list | include elements** : affiche les compteurs d'accès et une valeur d'horodatage pour une liste d'accès.

Les alertes de diagnostic comprennent la sortie des commandes suivantes :

- **show failover** : affiche des renseignements sur l'état de basculement de l'unité.
- **show interface : affiche des statistiques sur l'interface.**
- **show cluster info : affiche des renseignements sur la grappe.**
- **show cluster history : affiche l'historique de la grappe.**
- **show crashinfo** (tronqué) : après un rechargement inattendu du logiciel, le périphérique envoie un fichier d'information sur les plantages modifié qui ne contient que la section de recherche de la source du fichier. Ainsi, seuls les appels de fonction, les valeurs de registre et les vidages de pile sont signalés à Cisco.
- **show tech-support no-config : affiche les renseignements utilisés pour le diagnostic par les analystes de l'assistance technique.**

Les alertes d'environnement comprennent la sortie des commandes suivantes :

- **show environment** : affiche des renseignements sur l'environnement système pour les composants du système ASA, tels que l'état opérationnel du matériel pour le châssis, les pilotes, les ventilateurs et les alimentations, ainsi que l'état de la température, la tension et l'utilisation du processeur.
- **show cpu usage** : affiche les renseignements sur l'utilisation du processeur.
- **show memory detail** : affiche les détails de la mémoire système libre et allouée.

Les alertes de menace comprennent la sortie des commandes suivantes :

- **show threat-detection rate** : affiche les statistiques de détection des menaces.
- **show threat-detection shun** : affiche les hôtes actuellement banis.
- **show shun** : affiche les renseignements sur le bannissement.
- **show dynamic-filter reports top** : génère des rapports sur les 10 principaux sites malveillants, ports et hôtes infectés classés par le filtre de réseau de zombies.

Les alertes d'instantané peuvent comprendre la sortie des commandes suivantes :

- **show conn count** : affiche le nombre de connexions actives.
- **show asp drop** : affiche le chemin de sécurité accéléré des paquets ou des connexions abandonnés.

Les alertes de télémétrie comprennent la sortie des commandes suivantes :

- **show perfmon detail : affiche** les détails de performance de l'ASA.
- **show traffic – affiche l'activité de transmission et de réception de l'interface.**
- **show conn count** : affiche le nombre de connexions actives.
- **show vpn-sessiondb summary : affiche les renseignements sur le résumé de la session VPN.**
- **show vpn load-balancing : affiche les statistiques de durée d'exécution pour la configuration de la grappe virtuelle d'équilibrage de charges VPN.**

- **show local-host | include interface : affiche les états du réseau des hôtes locaux.**
- **show memory : affiche un résumé de la mémoire physique maximum et de la mémoire libre actuelle disponible pour le système d'exploitation.**
- **show context** : affiche les interfaces allouées et l'URL du fichier de configuration, le nombre de contextes configurés, ou si vous activez la création de rapports anonymes dans l'espace d'exécution du système, à partir d'une liste de tous les contextes.
- **show access-list | include elements** : affiche les compteurs d'accès et une valeur d'horodatage pour une liste d'accès.
- **show interface : affiche des statistiques sur l'interface.**
- **show threat-detection statistics protocol : affiche les statistiques du protocole IP.**
- **show phone-proxy media-sessions count : affiche le nombre de sessions multimédias correspondantes stockées par le mandataire téléphonique.**
- **show phone-proxy secure-phones count : affiche le nombre de téléphones capables de fonctionner en mode sécurisé stockés dans la base de données.**
- **show route : affiche la table de routage.**
- **show xlate count : affiche le nombre de sessions NAT (xlates).**

Seuil de gravité des messages

Lorsque vous abonnez un profil de destination à certains groupes d'alertes, vous pouvez définir un seuil pour l'envoi des messages de groupe d'alertes en fonction du niveau de gravité des messages. Tout message dont la valeur est inférieure au seuil spécifié du profil de destination n'est pas envoyé à la destination.

Le tableau suivant affiche le mappage entre les niveaux de gravité des messages et les niveaux de gravité du journal système.

Tableau 1 : Mappage des niveaux de gravité des messages et des niveaux du journal système

Niveau	Niveau de gravité des messages	Niveau de gravité du journal système	Description
9	Catastrophique	S. O.	Défaillance catastrophique à l'échelle du réseau.
8	Sinistre	S. O.	Incidence importante sur le réseau.
7	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	0	Urgence. Système inutilisable.

Niveau	Niveau de gravité des messages	Niveau de gravité du journal système	Description
6	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	Alerte. Conditions critiques; une attention immédiate est requise.
5	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	Critique. Conditions majeures.
4	Déterminé par le mot clé de l'interface de ligne de commande spécifié : **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	Erreur. Conditions mineures.
3	Avertissement	4	Conditions de mise en garde.
2	Notification	5	Notification de base et messages d'information. Peuvent être sans importance pris isolément.
1	Normal	6	de l'autre partie. Événement normal, indiquant un retour à l'état normal.
0	Débogage	7	Messages de débogage (paramètre par défaut).

Profils d'abonnement

Un profil d'abonnement vous permet d'associer les destinataires cibles aux groupes concernés. Lorsqu'un événement enregistré auprès d'un groupe abonné dans un profil se déclenche, le message associé à l'événement est envoyé aux destinataires configurés. Les profils d'abonnement possèdent les attributs suivants :

- Vous pouvez créer et configurer plusieurs profils.
- Un profil peut configurer plusieurs destinataires de courriel ou HTTPS.
- Un profil peut abonner plusieurs groupes à un niveau de gravité spécifié.
- Un profil prend en charge trois formats de message : texte court, texte long et XML.
- Vous pouvez activer et désactiver un profil spécifique. Les profils sont désactivés par défaut.
- Vous pouvez préciser la taille maximum des messages. La valeur par défaut est de 3 Mo.

Un profil par défaut, « Cisco TAC », a été fourni. Le profil par défaut comporte un ensemble prédéfini de groupes (de diagnostic, d'environnement, d'inventaire, de configuration et de télémétrie) pour superviser et prédéfinir les courriels de destination et les URL HTTPS. Le profil par défaut est créé automatiquement lorsque vous configurez Smart Call Home pour la première fois. L'adresse courriel de destination est callhome@cisco.com et l'URL de destination est https://tools.cisco.com/its/service/oddce/services/DDCEService.

Remarque Vous ne pouvez pas modifier l'adresse courriel de destination ni l'URL de destination du profil par défaut.

Lorsque vous abonnez un profil de destination aux groupes d'alertes de configuration, d'inventaire, de télémétrie ou d'instantané, vous pouvez choisir de recevoir les messages du groupe d'alertes de manière asynchrone ou périodique à une heure spécifiée.

Le tableau suivant mappe le groupe d'alertes par défaut à son abonnement au niveau de gravité et à sa période (le cas échéant) :

Tableau 2 : Mappage d'abonnement entre le groupe d'alertes et le niveau de gravité

Groupe d'alertes	Niveau de gravité	Période
Configuration	Information	Mensuelle
Diagnostic	Informatif et supérieur	S. O.
Environnement	Notification et supérieur	S. O.
Inventaire	Information	Mensuelle
Snapshot	Information	s.o.
Syslog	Journal système équivalent	S. O.
Télémétrie	Information	Tous les jours
Tester	s.o.	s.o.
La chasse aux menaces	Notification	s.o.

Lignes directrices relatives aux rapports anonymes et à Smart Call Home

Cette section comprend des lignes directrices et des limites que vous devez consulter avant de configurer les rapports anonymes et Smart Call Home.

Lignes directrices relatives aux rapports anonymes

- Le DNS doit être configuré.
- Si un message de rapport anonyme ne peut pas être envoyé lors du premier essai, l'ASA réessaie deux fois avant d'abandonner le message.

- Les rapports anonymes peuvent coexister avec d'autres configurations de Smart Call Home sans modifier la configuration existante. Par exemple, si Smart Call Home est désactivé avant d'activer la création de rapports anonymes, il reste désactivé, même après l'activation des rapports anonymes.
- Si les rapports anonymes sont activés, vous ne pouvez pas supprimer le point de confiance, et lorsque les rapports anonymes sont désactivés, le point de confiance reste. Si les rapports anonymes sont désactivés, vous pouvez supprimer le point de confiance, mais la désactivation des rapports anonymes n'entraînera pas la suppression du point de confiance.
- Si vous utilisez une configuration en mode de contexte multiple, les commandes **dns**, **interface** et **trustpoint** sont dans le contexte d'administration et les commandes **call-home** sont dans le contexte système.
- 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 de renouvellement automatique des groupes de confiance n'est pas prise en charge dans le cadre des déploiements à contextes multiples.

Lignes directrices relatives à Smart Call Home

- En mode de contexte multiple, la commande subscribe-to-alert-group snapshot periodic est divisée en deux commandes : l'une pour obtenir des renseignements de la configuration système et l'autre pour obtenir des renseignements du contexte utilisateur.
- Le serveur dorsal Smart Call Home n'accepte que les messages au format XML.
- Un message Smart Call Home est envoyé à Cisco pour signaler des événements de grappe importants si vous avez activé la mise en grappe et configuré Smart Call Home pour vous abonner au groupe d'alertes de diagnostic avec un niveau de gravité critique. Un message de mise en grappe Smart Call Home est envoyé uniquement pour les événements suivants :
  - Lorsqu'une unité rejoint la grappe
  - Lorsqu'une unité quitte la grappe
  - Lorsqu'une unité de grappe devient l'unité de contrôle de grappe
  - Lorsqu'une unité secondaire tombe en panne dans la grappe

  Chaque message envoyé comprend les renseignements suivants :
  - Le nombre de membres actifs dans la grappe
  - La sortie de la commande **show cluster info** et de la commande **show cluster history** sur l'unité de contrôle de grappe

Configurer les rapports anonymes et Smart Call Home

Les rapports anonymes font partie du service Smart Call Home et permettent à Cisco de recevoir de manière anonyme un minimum de renseignements sur les erreurs et l'intégrité de votre appareil, mais le service Smart Call Home offre une assistance personnalisée sur l'intégrité de votre système, ce qui permet au TAC de Cisco de superviser vos appareils et d'ouvrir un dossier lorsqu'il y a un problème, souvent avant même que vous sachiez que le problème est survenu.

Vous pouvez avoir les deux services configurés sur votre système en même temps, bien que la configuration du service Smart Call Home offre les mêmes fonctionnalités que les rapports anonymes, ainsi que des services personnalisés.

Lorsque vous passez en mode de configuration, vous recevez une invite qui vous demande d'activer les services de création de rapports anonymes et de Smart Call Home en fonction des lignes directrices suivantes :

- À l'invite, vous pouvez choisir [Y]es (Oui), [N]o (Non) ou [A]sk later (Demander plus tard). Si vous choisissez [A]sk later (Demander plus tard), vous recevrez un rappel à nouveau dans sept jours ou lors du rechargement de l'ASA. Si vous continuez à choisir [A]sk later (Demander plus tard), l'ASA répond deux fois de plus à des intervalles de sept jours avant de prendre en charge une réponse [N]o (Non) et ne demande plus de réponse.
- Si vous n'avez pas reçu d'invite, vous pouvez activer la création de rapports anonymes ou Smart Call Home en effectuant les étapes dans Configurer les rapports anonymes, à la page 10 ou dans Configurer Smart Call Home, à la page 11.

Configurer les rapports anonymes

Pour configurer les rapports anonymes, procédez comme suit.

Procédure

Étape 1 Activez la fonctionnalité Rapports anonymes et créez un nouveau profil anonyme.

call-home reporting anonymous

Exemple :

```
ciscoasa(config)# call-home reporting anonymous
```

La saisie de cette commande crée un point de confiance et installe un certificat utilisé pour vérifier l'identité du serveur Web Cisco.

Étape 2 (Facultatif) Assurez-vous que vous disposez d'une connexion au serveur et que votre système peut envoyer des messages.

call-home test reporting anonymous

Exemple :

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

Un message de réussite ou d'erreur renvoie les résultats du test.

Configurer Smart Call Home

La configuration du service Smart Call Home sur votre ASA comprend les tâches suivantes :

Procédure

Étape 1 Activez le service Smart Call Home. Consultez Activer Smart Call Home, à la page 11.

Étape 2 Configurez le serveur de messagerie par lequel les messages Smart Call Home sont envoyés aux abonnés. Consultez Configurer le serveur de messagerie, à la page 16.

Étape 3 Configurez les coordonnées pour les messages Smart Call Home. Consultez Configurer les coordonnées du client, à la page 14.

Étape 4 Définissez les paramètres de traitement des alertes, tels que le taux maximum d'événements qui peuvent être gérés. Consultez Configurer l'abonnement des groupes d'alertes, à la page 13.

Étape 5 Configurez les profils d'abonnement aux alertes. Consultez Configurer un profil de destination, à la page 18.

Chaque profil d'abonnement aux alertes identifie les éléments suivants :

- Les abonnés à qui les messages Smart Call Home sont envoyés, comme un serveur Smart Call Home chez Cisco ou une liste de destinataires de courriels.
- Catégories d'informations pour lesquelles vous souhaitez recevoir des alertes, comme les informations de configuration ou d'inventaire.

Activer Smart Call Home

Pour activer Smart Call Home et activer votre profil call-home, procédez comme suit :

Procédure

Étape 1 Activez le service Smart Call Home.

service call-home

Exemple :

```
ciscoasa(config)# service call-home
```

Étape 2 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call home
```

Déclarer et authentifier le point de confiance d'une autorité de certification

Si Smart Call Home est configuré pour envoyer des messages à un serveur web par HTTPS, vous devez configurer l'ASA pour faire confiance au certificat du serveur web ou au certificat de l'autorité de certification (CA) qui a émis le certificat. Le certificat de serveur Cisco Smart Call Home Production est émis par Verisign. Le certificat de serveur Cisco Smart Call Home Staging est émis par Digital Signature Trust Company.

Remarque Vous devez définir le point de confiance pour aucun type de client/aucune utilisation de validation afin d'empêcher son utilisation pour la validation VPN.

Pour déclarer et authentifier le certificat de sécurité du serveur Cisco et établir la communication avec le serveur HTTPS de Cisco pour le service Smart Call Home, procédez comme suit :

Procédure

Étape 1 (Mode de contexte multiple seulement) Installez le certificat dans le contexte d'administration.

changeto context *admincontext*

Exemple :

```
ciscoasa(config)# changeto context contextA
```

Étape 2 Configurez un point de confiance et préparez l'inscription du certificat.

crypto ca trustpoint *trustpoint-name*

Exemple :

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

Remarque
Si vous utilisez HTTP comme méthode de transport, vous devez installer un certificat de sécurité via un point de confiance, ce qui est requis pour HTTPS. Recherchez le certificat spécifique à installer à l'adresse URL suivante :

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

Étape 3 Spécifiez une méthode d'inscription de certificat manuelle par copier-coller.

enroll terminal

Exemple :

```
ciscoasa(ca-trustpoint)# enroll terminal
```

Étape 4 Authentifiez la CA nommée. Le nom de la CA doit correspondre au nom du point de confiance spécifié dans la commande **crypto ca trustpoint**. À l'invite, collez le texte du certificat de sécurité.

crypto ca authenticate trustpoint

Exemple :

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

Étape 5 Spécifiez la fin du texte du certificat de sécurité et confirmez l'acceptation du certificat de sécurité saisi.

quit

Exemple :

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

Configurer les groupes d'alertes d'environnement et d'instantané

Pour configurer les groupes d'alertes d'environnement et d'instantané, procédez comme suit :

Procédure

Entrez dans le mode de configuration des groupes d'alertes.

alert-group-config {**environment** | **snapshot**}

Exemple :

```
ciscoasa(config)# alert-group-config environment
```

Configurer l'abonnement des groupes d'alertes

Pour abonner un profil de destination à un groupe d'alertes, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Activez le groupe d'alertes Smart Call Home spécifié.

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

Exemple :

```
ciscoasa(cfg-call-home)# alert-group syslog
```

Utilisez le mot clé **all** pour activer tous les groupes d'alertes. Par défaut, tous les groupes d'alertes sont activés.

Étape 3 Entrez en mode de configuration du profil pour le profil de destination indiqué.

profile *profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

Étape 4 Abonnez-vous à tous les groupes d'alertes disponibles.

subscribe-to-alert-group all

Exemple :

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

Étape 5 Abonnez ce profil de destination au groupe d'alertes de configuration.

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

Exemple :

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

Le mot clé **periodic** configure le groupe d'alertes de configuration pour la notification périodique. La période par défaut est quotidienne.

Le mot clé **daily** spécifie l'heure à laquelle l'envoi doit être effectué, au format *hh:mm*, avec une horloge de 24 heures (par exemple, 14:30).

Le mot clé **weekly** spécifie le jour de la semaine et l'heure au format *day hh:mm*, où le jour de la semaine est saisi (par exemple, lundi).

Le mot clé **monthly** spécifie la date numérique, de 1 à 31, et l'heure au format *date hh:mm*.

Configurer les coordonnées du client

Pour configurer les coordonnées du client, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le numéro de téléphone du client. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

phone-number *phone-number-string*

Exemple :

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

Étape 3 Spécifiez l'adresse du client, qui est une chaîne de format libre pouvant comporter jusqu'à 255 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

street-address *street-address*

Exemple :

```
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

Étape 4 Spécifiez le nom du client, qui peut comporter jusqu'à 128 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

contact-name *contact-name*

Exemple :

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

Étape 5 Spécifiez l'ID de client Cisco, qui peut comporter jusqu'à 64 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

customer-id *customer-id-string*

Exemple :

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

Étape 6 Spécifiez l'ID de site du client, qui peut comporter jusqu'à 64 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

site-id *site-id-string*

Exemple :

```
ciscoasa(cfg-call-home)# site-id site1234
```

Étape 7 Spécifiez l'identification du contrat du client, qui peut comporter jusqu'à 128 caractères. Les espaces sont autorisés, mais vous devez utiliser des guillemets autour de la chaîne si elle contient des espaces.

contract-id *contract-id-string*

Exemple :

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

Exemple

L'exemple suivant montre comment configurer les coordonnées :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

Configurer le serveur de messagerie

Nous vous conseillons d'utiliser HTTPS pour le transport des messages, car il est le plus sécurisé. Cependant, vous pouvez configurer une destination de courriel pour Smart Call Home, puis configurer le serveur de messagerie pour qu'il utilise le transport par courriel.

Pour configurer le serveur de messagerie, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le serveur de messagerie SMTP.

mail-server*ip-address* **name priority** [**1-100**] [**all**]

Exemple :

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

Vous pouvez spécifier jusqu'à cinq serveurs de messagerie, en utilisant cinq commandes distinctes. Vous devez configurer au moins un serveur de messagerie pour utiliser le transport par courriel des messages Smart Call Home.

Plus le numéro est bas, plus la priorité du serveur de messagerie est élevée.

L'argument *ip-address* peut être une adresse de serveur de messagerie IPv4 ou IPv6.

Exemple

L'exemple suivant montre comment configurer un serveur de messagerie principal (nommé « smtp.exemple.com ») et un serveur de messagerie secondaire à l'adresse IP 10.10.1.1 :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

Configurer la limitation de débit du trafic

Pour configurer la limitation de débit du trafic, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le nombre de messages que Smart Call Home peut envoyer par minute. La valeur par défaut est de 10 messages par minute.

rate-limit *msg-count*

Exemple :

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Envoyer des communications à Smart Call Home

Pour envoyer des communications Smart Call Home spécifiques, procédez comme suit :

Procédure

Choisissez une des options suivantes :

- Option 1 : envoyer manuellement un message de test à l'aide d'une configuration de profil.

call-home test [*test-message*] **profile** *profile-name*

Exemple :

```
ciscoasa# call-home test [testing123] profile CiscoTAC-1
```

- Option 2 : envoyer un message de groupe d'alertes à un profil de destination, si il est spécifié. Si aucun profil n'est spécifié, envoyez des messages à tous les profils inscrits aux groupes d'alertes d'inventaire, de configuration, d'instantané ou de télémétrie.

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  Exemple :

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- Option 3 : envoyer la sortie de commande à une adresse courriel. La commande de l'interface de ligne de commande spécifiée peut être n'importe quelle commande, y compris les commandes pour tous les modules enregistrés.

  call-home send*cli command* [**email** *email*]

  Exemple :

  ```
  ciscoasa# call-home send cli destination email username@example.com
  ```

  Si vous spécifiez une adresse courriel, la sortie de la commande est envoyée à cette adresse. Si aucune adresse courriel n'est spécifiée, la sortie est envoyée au TAC de Cisco. Le courriel est envoyé au format texte de journal avec le numéro de service, si il est spécifié, dans la ligne d'objet.

  Le numéro de service est requis uniquement si aucune adresse courriel n'est spécifiée ou si une adresse courriel du TAC de Cisco est spécifiée.

Configurer un profil de destination

Pour configurer un profil de destination pour le courriel ou pour HTTP, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Entrez en mode de configuration du profil pour le profil de destination indiqué. Si le profil de destination spécifié n'existe pas, il est créé.

profile *profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# profile newprofile
```

Vous pouvez créer un maximum de 10 profils actifs. Le profil par défaut consiste à renvoyer les renseignements au TAC de Cisco. Si vous souhaitez envoyer des renseignements de connexion à un autre emplacement (par exemple, votre propre serveur), vous pouvez configurer un profil distinct.

Étape 3 Configurez la destination, la taille du message, le format du message et la méthode de transport pour le récepteur de messages Smart Call Home. Le format de message par défaut est XML et la méthode de transport activée par défaut est le courriel.

destination address {**email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

Exemple :

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
ExampleService
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

L'option **reference-identity** active les vérifications d'identité de référence RFC 6125 sur le certificat de serveur reçu. Celles-ci s'appliquent uniquement aux destinations configurées avec une adresse HTTP. Les vérifications d'ID sont effectuées en fonction d'un objet d'identité de référence précédemment configuré. Consultez Configurer les identités de référence pour en savoir plus sur l'objet d'identité de référence.

L'e-mail-address est l'adresse courriel du destinataire du message Smart Call Home, qui peut comporter jusqu'à 100 caractères. Par défaut, la taille maximum de l'URL est de 5 Mo.

Utilisez le format de texte court pour envoyer et lire un message sur un appareil mobile et utilisez le format de texte long pour envoyer et lire un message sur un ordinateur.

Si le récepteur du message est le serveur principal Smart Call Home, assurez-vous que la valeur **preferred-msg-format** est XML, car le serveur dorsal n'accepte que les messages au format XML.

Utilisez cette commande pour rétablir la méthode de transport par courriel.

Copier un profil de destination

Pour créer un nouveau profil de destination en copiant un profil existant, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le profil à copier.

profile *profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# profile newprofile
```

Étape 3 Copiez le contenu d'un profil existant vers un nouveau profil.

copy profile *src-profile-name dest-profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

Le profil existant (*src-profile-name*) et le nouveau profil (*dest-profile-name*) peuvent comporter jusqu'à 23 caractères.

Exemple

L'exemple suivant montre comment copier un profil existant :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

Renommer un profil de destination

Pour modifier le nom d'un profil existant, procédez comme suit :

Procédure

Étape 1 Entrez en mode de configuration call-home.

call-home

Exemple :

```
ciscoasa(config)# call-home
```

Étape 2 Spécifiez le profil à renommer.

profile *profilename*

Exemple :

```
ciscoasa(cfg-call-home)# profile newprofile
```

Étape 3 Modifiez le nom d'un profil existant.

rename profile *src-profile-name dest-profile-name*

Exemple :

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

Le profil existant (*src-profile-name*) et le nouveau profil (*dest-profile-name*) peuvent comporter jusqu'à 23 caractères.

Exemple

L'exemple suivant montre comment renommer un profil existant :

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

Supervision des rapports anonymes et de Smart Call Home

Consultez les commandes suivantes pour superviser les services de création de rapports anonymes et les services Smart Call Home.

- **show call-home detail**

  Cette commande affiche la configuration détaillée de Smart Call Home actuelle.

- **show call-home mail-server status**

  Cette commande affiche l'état actuel du serveur de messagerie.

- **show call-home profile** {profile name | **all**}

  Cette commande affiche la configuration des profils Smart Call Home.

- **show call-home registered-module status** [**all**]

  Cette commande affiche l'état du module enregistré.

- **show call-home statistics**

  Cette commande affiche l'état détaillé de Smart Call Home.

- **show call-home**

  Cette commande affiche la configuration de Smart Call Home actuelle.

- **show running-config call-home**

  Cette commande affiche la configuration en cours d'exécution de Smart Call Home actuelle.

- **show smart-call-home alert-group**

  Cette commande affiche l'état actuel des groupes d'alertes Smart Call Home.

- **show running-config all**

  Cette commande affiche les détails du profil d'utilisateur des rapports anonymes.

Exemples de Smart Call Home

L'exemple suivant montre comment configurer le service Smart Call Home :

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly Monday
 23:30
```

Historique des rapports anonymes et de Smart Call Home

Tableau 3 : Historique des rapports anonymes et de Smart Call Home

Nom de la caractéristique	Versions de plateforme	Description
Smart Call Home	8.2(2)	Le service Smart Call Home offre des diagnostics proactifs et des alertes en temps réel sur l'ASA, et assure une meilleure disponibilité du réseau et une efficacité opérationnelle accrue. Nous avons introduit ou modifié les commandes suivantes : **active (call home)**, **call-home, call-home send alert-group, call-home test, contact-email-addr**, **customer-id (call home)**, **destination (call home)**, **profile**, **rename profile**, **service call-home, show call-home, show call-home detail**, **show smart-call-home alert-group**, **show call-home profile**, **show call-home statistics**, **show call-home mail-server status**, **show running-config call-home**, **show call-home registered-module status all**, **site-id**, **street-address**, **subscribe-to-alert-group all**, **alert-group-config**, **subscribe-to-alert-group configuration**, **subscribe-to-alert-group diagnostic**, **subscribe-to-alert-group environment**, **subscribe-to-alert-group inventory periodic**, **subscribe-to-alert-group snapshot periodic**, **subscribe-to-alert-group syslog**, **subscribe-to-alert-group telemetry periodic**.
Rapports anonymes	9.0(1)	Vous pouvez contribuer à l'amélioration de la plateforme ASA en activant les rapports anonymes, qui permettent à Cisco de recevoir en toute sécurité un minimum de renseignements sur les erreurs et l'intégrité d'un appareil. Nous avons introduit les commandes suivantes : **call-home reporting anonymous**, **call-home test reporting anonymous**.
Smart Call Home	9.1(2)	La commande **show local-host** a été remplacée par la commande **show local-host | include interface** pour la création de rapports sur les groupes d'alertes de télémétrie.

Nom de la caractéristique	Versions de plateforme	Description
Smart Call Home	9.1(3)	Un message Smart Call Home est envoyé à Cisco pour signaler des événements de grappe importants si vous avez activé la mise en grappe et configuré Smart Call Home pour vous abonner au groupe d'alertes de diagnostic avec un niveau de gravité Critique. Un message de mise en grappe Smart Call Home est envoyé uniquement pour les trois événements suivants : • Lorsqu'une unité rejoint la grappe • Lorsqu'une unité quitte la grappe • Lorsqu'une unité de grappe devient l'unité de contrôle de grappe Chaque message envoyé comprend les renseignements suivants : • Le nombre de membres actifs dans la grappe • La sortie de la commande **show cluster info** et de la commande **show cluster history** sur l'unité de contrôle de grappe
Identités de référence pour les connexions sécurisées au serveur Smart Call Home	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 lors de la validation PKI pour les connexions TLS au serveur Smart Call Home. 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 : **[no] crypto ca reference-identity**, **call home profile destination address http**.

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.