

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, à la page 1
- À propos de Smart Call Home, à la page 2
- Lignes directrices relatives aux rapports anonymes et à Smart Call Home, à la page 3
- Configurer les rapports anonymes et Smart Call Home, à la page 4
- Supervision des rapports anonymes et de Smart Call Home, à la page 9
- Historique des rapports anonymes et de Smart Call Home, à la page 10

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.

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.

Configurer les rapports anonymes

Pour configurer les rapports anonymes, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call Home**.

Étape 2 Cochez la case **Enable Anonymous Reporting** (Activer les rapports anonymes).

Étape 3 Cliquez sur **Test Connection** (Tester la connexion) pour vous assurer que votre système est en mesure d'envoyer des messages.

ASDM renvoie un message de réussite ou d'erreur pour vous informer des résultats du test.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration et activer les rapports anonymes.

Configurer Smart Call Home

Pour configurer le service Smart Call Home, la configuration système et les profils d'abonnement aux alertes, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Smart Call Home**.

Étape 2 Cochez la case **Enable Registered Smart Call Home** (Activer le Smart Call Home enregistré) pour activer Smart Call Home et enregistrer votre ASA auprès du TAC de Cisco.

Étape 3 Cliquez deux fois sur **Advanced System Setup** (Configuration système avancée). Cette zone se compose de trois volets. Chaque volet peut être développé ou réduit en cliquant deux fois sur la ligne de titre.

a) Vous pouvez configurer des serveurs de messagerie dans le volet **Mail Servers** (Serveurs de messagerie), par lequel les messages Smart Call Home sont envoyés aux abonnés par courriel.

b) Vous pouvez saisir les renseignements de la personne-ressource dans le volet **Contact Information** (Coordonnées) pour l'ASA qui s'affiche dans les messages de Smart Call Home. Ce volet comprend les renseignements suivants :

- Le nom de la personne-ressource.
- Le numéro de téléphone de la personne-ressource.
- L'adresse postale de la personne-ressource.
- L'adresse courriel de la personne-ressource.
- L'adresse courriel « expéditeur » dans le courriel de Smart Call Home.
- L'adresse courriel « répondre à » dans le courriel de Smart Call Home.
- L'ID du client.
- L'ID du site.
- L'ID de contrat.

c) Vous pouvez ajuster les paramètres de contrôle des alertes dans le volet **Alert Control** (Contrôle des alertes). Ce volet comprend le volet **Alert Group Status** (État du groupe d'alertes), qui répertorie l'état (activé ou désactivé) des groupes d'alertes suivants :

- Le groupe d'alertes de diagnostic.
- Le groupe d'alertes de configuration.
- Le groupe d'alertes d'environnement.
- Le groupe d'alertes d'inventaire.
- Le groupe d'alertes d'instantané.
- Le groupe d'alertes de journal système.
- Le groupe d'alertes de télémétrie.
- Le groupe d'alertes de menace.
- Le nombre maximum de messages Smart Call Home traités par minute.
- L'adresse courriel « expéditeur » dans le courriel de Smart Call Home.

Étape 4 Cliquez deux fois sur **Alert Subscription Profiles** (Profils d'abonnement aux alertes). Chaque profil d'abonnement nommé identifie les abonnés et les groupes d'alertes d'intérêt.

a) Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour afficher le **Subscription Profile Editor** (Éditeur de profil d'abonnement), dans lequel vous pouvez créer un nouveau profil d'abonnement ou modifier un profil d'abonnement existant.
b) Cliquez sur **Delete** (Supprimer) pour supprimer le profil sélectionné.
c) Cochez la case **Active** (Actif) pour envoyer un message Smart Call Home du profil d'abonnement sélectionné aux abonnés.

Étape 5 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour afficher la boîte de dialogue **Add** (Ajouter) ou **Edit Alert Subscription Profile** (Modifier le profil d'abonnement aux alertes).

a) Le champ **Name** (Nom) est en lecture seule et ne peut pas être modifié.
b) Cochez la case **Enable this subscription profile** (Activer ce profil d'abonnement) pour activer ou désactiver ce profil en particulier.
c) Cliquez sur le bouton radio **HTTP** ou **Email** (Courriel) dans la zone **Alert Delivery Method** (Méthode de distribution d'alertes).
d) Saisissez l'adresse courriel ou l'adresse Web dans le champ **Subscribers** (Abonnés).
e) Spécifiez un objet **Reference Identity** (Identité de référence) par nom pour activer les vérifications d'identité de référence RFC 6125 sur le certificat reçu du serveur de journal système.

   Consultez Configurer les identités de référence pour en savoir plus sur l'objet d'identité de référence.

Étape 6 La zone **Alert Dispatch** (Envoi d'alertes) permet à l'administrateur de préciser le type de renseignements Smart Call Home à envoyer aux abonnés et dans quelles conditions. Il existe deux types d'alertes, basées sur le temps et basées sur des événements, choisies en fonction de la façon dont l'alerte est déclenchée. Les groupes d'alertes suivants sont à baser sur le temps : configuration, inventaire, instantané et télémétrie. Les groupes d'alertes suivants sont basés sur des événements : diagnostic, environnement, journal système et menace.

Étape 7 La zone **Message Parameters** (Paramètres de message) vous permet d'ajuster les paramètres qui contrôlent les messages envoyés à l'abonné, y compris le format de message préféré et la taille de message maximum.

Étape 8 Pour les alertes basées sur le temps, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Add** (Ajouter) ou **Edit Configuration Alert Dispatch Condition** (Modifier une condition d'envoi d'alertes de configuration).

a) Spécifiez la fréquence dans le champ **Alert Dispatch Frequency** (Fréquence d'envoi d'alertes) à laquelle envoyer les renseignements aux abonnés :

- Pour un abonnement mensuel, indiquez le jour du mois et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement hebdomadaire, indiquez le jour de la semaine et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement quotidien, indiquez l'heure du jour pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée.
- Pour un abonnement horaire, indiquez la minute de l'heure pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée. Les abonnements horaires s'appliquent uniquement aux groupes d'alertes d'instantané et de télémétrie.

b) Cliquez sur le bouton radio **Basic** (De base) ou **Detailed** (Détaillé) pour fournir le niveau de renseignements souhaité aux abonnés.

c) Cliquez sur **OK** pour enregistrer la configuration

Étape 9 Pour les alertes de diagnostic, d'environnement et de menace, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Diagnostic Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte de diagnostic).

Étape 10 Précisez la gravité de l'événement qui déclenche l'envoi de l'alerte aux abonnés dans la liste déroulante **Event Severity** (Gravité de l'événement), puis cliquez sur **OK**.

Étape 11 Pour les alertes basées sur le temps d'inventaire, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Inventory Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte d'inventaire).

Étape 12 Précisez la fréquence d'envoi des alertes aux abonnés dans la liste déroulante **Alert Dispatch Frequency** (Fréquence d'envoi des alertes), puis cliquez sur **OK**.

Étape 13 Pour les alertes basées sur le temps d'instantané, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Snapshot Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte d'instantané).

a) Spécifiez la fréquence dans le champ **Alert Dispatch Frequency** (Fréquence d'envoi d'alertes) à laquelle envoyer les renseignements aux abonnés :

- Pour un abonnement mensuel, indiquez le jour du mois et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement hebdomadaire, indiquez le jour de la semaine et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement quotidien, indiquez l'heure du jour pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée.
- Pour un abonnement horaire, indiquez la minute de l'heure pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée. Les abonnements horaires s'appliquent uniquement aux groupes d'alertes d'instantané et de télémétrie.

- Pour un intervalle d'abonnement, indiquez la fréquence en minutes à laquelle les renseignements doivent être envoyés aux abonnés. Cette exigence s'applique uniquement au groupe d'alertes d'instantané.

b) Cliquez sur **OK** pour enregistrer la configuration

Étape 14 Pour les alertes basées sur des événements de journal système, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Syslog Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte de journal système).

a) Cochez la case **Specify the event severity which triggers the dispatch of alert to subscribers** (Spécifier la gravité de l'événement qui déclenche l'envoi de l'alerte aux abonnées), et choisissez la gravité de l'événement dans la liste déroulante.

b) Cochez la case **Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers** (Spécifier les ID de message des journaux système qui déclenchent l'envoi de l'alerte aux abonnés).

c) Spécifiez les ID de message des journaux système qui déclenchent l'envoi de l'alerte aux abonnés en fonction des instructions à l'écran.

d) Cliquez sur **OK** pour enregistrer la configuration

Étape 15 Pour les alertes basées sur des événements de télémétrie, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la zone **Alert Dispatch** (Envoi d'alertes) pour afficher la boîte de dialogue **Create** (Créer) ou **Edit Telemetry Alert Dispatch Condition** (Modifier une condition d'envoi d'alerte de télémétrie).

a) Spécifiez la fréquence dans le champ **Alert Dispatch Frequency** (Fréquence d'envoi d'alertes) à laquelle envoyer les renseignements aux abonnés :

- Pour un abonnement mensuel, indiquez le jour du mois et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement hebdomadaire, indiquez le jour de la semaine et l'heure de la journée pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit les valeurs appropriées.
- Pour un abonnement quotidien, indiquez l'heure du jour pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée.
- Pour un abonnement horaire, indiquez la minute de l'heure pour envoyer les renseignements. Si ce n'est pas spécifié, l'ASA choisit une valeur appropriée. Les abonnements horaires s'appliquent uniquement aux groupes d'alertes d'instantané et de télémétrie.

b) Cliquez sur **OK** pour enregistrer la configuration

Étape 16 Cliquez sur **Test** (Tester) pour déterminer si les alertes configurées fonctionnent correctement.

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
```

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. Vous pouvez saisir ces commandes en sélectionnant **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

- **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.

Historique des rapports anonymes et de Smart Call Home

Tableau 1 : 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 l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Smart Call Home.
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 modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Smart Call Home.
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.
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

Nom de la caractéristique	Versions de plateforme	Description
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 modifié la page suivante : **Configuration > Device Management (Gestion des périphériques) > Smart Call Home**.

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.