Implémenter une position sans redirection ISE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Connectiondata.xml
  - Liste Call Home
- Conception
- Configurer
  - Groupes de périphériques réseau (facultatif)
  - Périphérique réseau
  - Provisionnement client
    - Provisionnement manuel (pré-déploiement)
    - Portail d'approvisionnement client (Web Deploy)
    - Politique de provisionnement client
  - Autorisation
    - Profil d'autorisation
    - Politique d'autorisation
- Dépannage
  - Conforme au client sécurisé Cisco et non applicable à la position (en attente) sur ISE
    - Sessions obsolètes/fantômes
    - Identifier
    - Solution
  - rendement
    - Identifier
    - Solution
  - Gestion de comptes
- Informations connexes

Introduction

Ce document décrit l'utilisation et la configuration du flux de posture sans redirection et des conseils de dépannage.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Flux de posture sur ISE
- Configuration des composants de posture sur ISE
- Redirection vers les portails ISE

Pour une meilleure compréhension des concepts décrits plus loin, il est recommandé de passer par :

Comparer le flux de redirection de position ISE au flux sans redirection de position ISE
Dépannage de la gestion et de la position des sessions ISE

Composants utilisés

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

- Cisco ISE version 3.3
- Cisco Secure Client 5.0.01242

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le flux de posture ISE se compose des étapes suivantes :

0. Authentification/Autorisation. Généralement effectuée juste avant le début de l'écoulement de posture, mais elle peut être contournée pour certains cas d'utilisation tels que la réévaluation de posture (PRA).

Comme l'authentification elle-même ne déclenche pas la découverte de posture, cela n'est pas considéré comme essentiel pour chaque flux de posture.

1. Découverte. Processus effectué par le module Secure Client ISE Posture pour trouver le propriétaire PSN de la session active en cours.
2. Provisionnement client. Processus effectué par ISE pour fournir au client les versions correspondantes du module de posture ISE et du module de conformité Cisco Secure Client (anciennement AnyConnect). Dans cette étape, la copie locale du profil de posture contenu dans et signé par le PSN particulier est également envoyée au client.
3. Analyse du système. Les stratégies de position configurées sur ISE sont évaluées par le module de conformité.
4. Correction (Facultatif). Effectué dans le cas où les politiques de posture ne sont pas conformes.
5. CoA. Une nouvelle autorisation est nécessaire pour accorder un accès réseau final (conforme ou non conforme).

Ce document se concentre sur le processus de découverte du flux de posture ISE.

Cisco recommande d'utiliser la redirection pour le processus de détection. Cependant, dans certains cas, la redirection n'est pas possible à mettre en oeuvre, par exemple lorsque des périphériques réseau tiers ne sont pas pris en charge. Ce document vise à fournir une orientation générale et les meilleures pratiques pour mettre en oeuvre et dépanner une posture sans redirection dans de tels environnements.

La description complète du flux sans redirection est décrite dans Comparer le flux de redirection de la posture ISE au flux sans redirection de la posture ISE

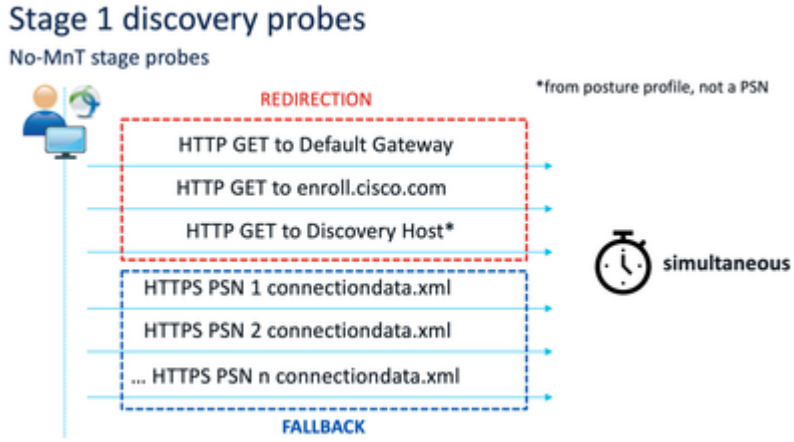
Il existe deux types de sondes de détection de position qui n'utilisent pas la redirection :

1. Connectiondata.xml
2. Liste Call Home

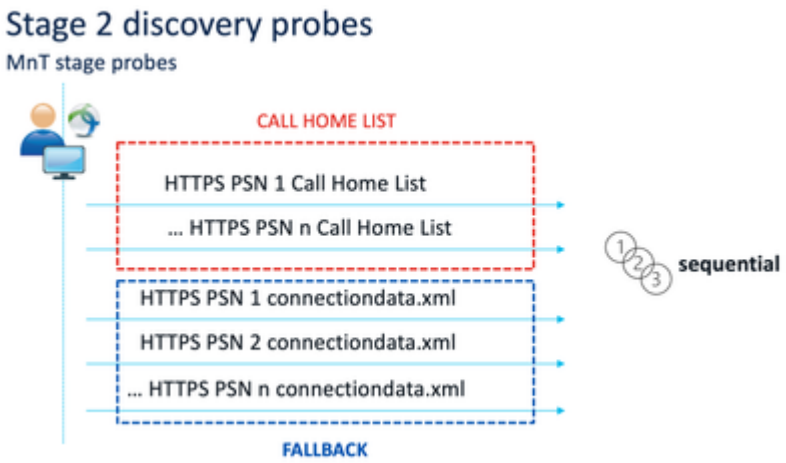
Connectiondata.xml

Le fichier Connectiondata.xml est un fichier créé et mis à jour automatiquement par Cisco Secure Client. Il se compose d'une liste de PSN auxquels le client s'est précédemment connecté avec succès pour la posture, par conséquent, il ne s'agit que d'un fichier local et son contenu n'est pas persistant sur tous les terminaux.

Le but principal de connectiondata.xml est de fonctionner comme mécanisme de sauvegarde pour les sondes de détection des étapes 1 et 2. Si les sondes de redirection ou Call Home List ne parviennent pas à trouver un PSN avec une session active, Cisco Secure Client envoie une requête directe à chacun des serveurs répertoriés dans le fichier connectiondata.xml.



Étape 1 - Sondes de détection



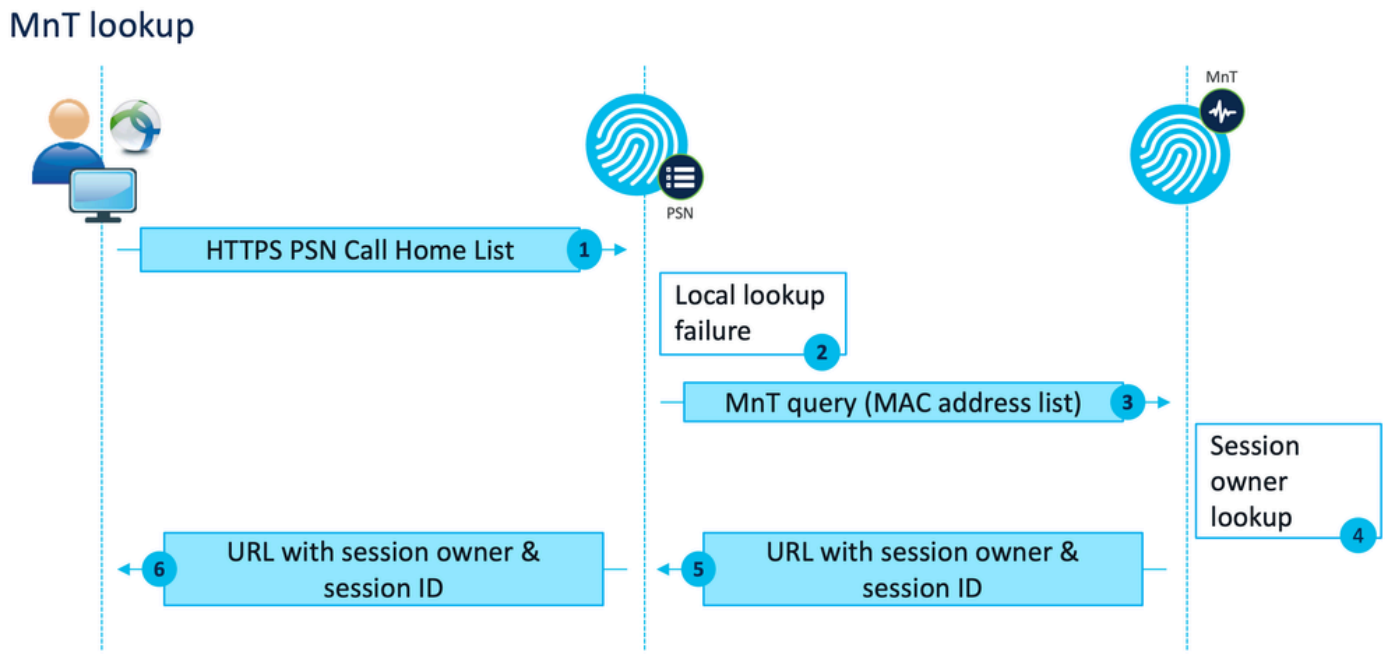
Étape 2 - Sondes de détection

Un problème courant causé par l'utilisation de sondes connectionData.xml est une surcharge du déploiement ISE due à un grand nombre de requêtes HTTPS envoyées par les points de terminaison. Il est important de considérer que, bien que le fichier connectiondata.xml soit efficace en tant que mécanisme de sauvegarde pour éviter les pannes complètes des mécanismes de redirection et de posture non réorientable, il ne constitue pas une solution durable pour un environnement de posture. Par conséquent, il est nécessaire de diagnostiquer et de résoudre les problèmes de conception et de configuration qui provoquent la défaillance des sondes de détection principales et qui entraînent des problèmes de détection.

Liste Call Home

La liste Call Home est une section du profil de posture dans laquelle une liste de PSN est spécifiée pour être utilisée pour la posture. Contrairement au fichier connectiondata.xml, il est créé et géré par un administrateur ISE et peut nécessiter une phase de conception pour une configuration optimale. La liste des PSN dans la liste Call Home correspond à la liste des serveurs d'authentification et de gestion des comptes qui est configurée dans le périphérique réseau ou l'équilibreur de charge pour RADIUS.

Les sondes Call Home List permettent l'utilisation d'une recherche MnT lors d'une recherche de session active en cas d'échec d'une recherche locale dans un PSN. La même fonctionnalité s'étend aux sondes connectiondata.xml uniquement lorsqu'elles sont utilisées lors de la détection de l'étape 2. Pour cette raison, toutes les sondes de l'étape 2 sont également appelées sondes de nouvelle génération.



Flux de recherche MnT

Conception

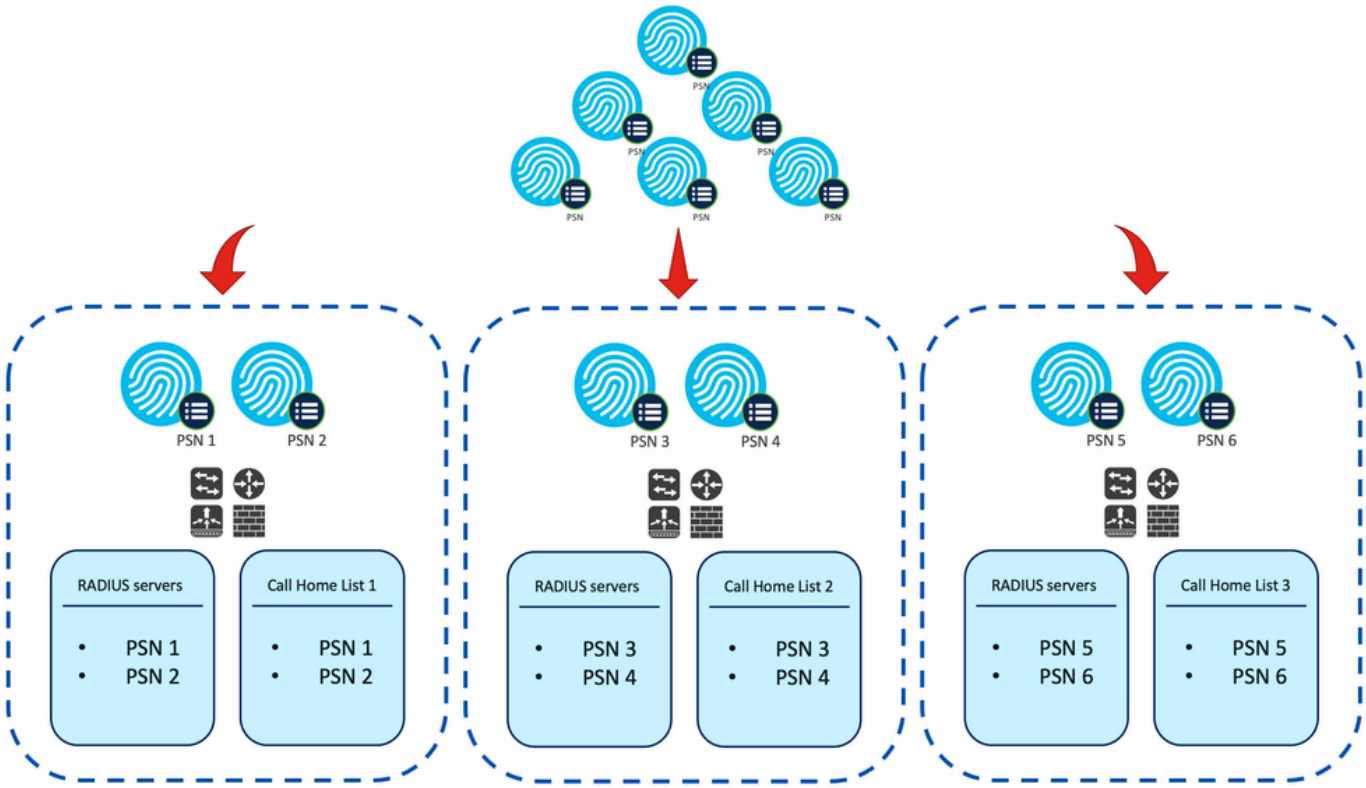
Comme un processus de découverte sans redirection implique souvent un flux plus complexe et un plus grand nombre de traitements sur PSN et MnT par rapport à un flux de redirection, il existe deux défis communs qui peuvent survenir au cours de la mise en oeuvre :

1. Découverte efficace
2. Performances du déploiement ISE

Afin de faire face à ces défis, il est recommandé de concevoir la liste Call Home pour limiter le nombre de PSN qu'un terminal donné peut utiliser pour la posture. Pour les déploiements moyens et importants, il est nécessaire de distribuer le déploiement afin de créer plusieurs listes Call Home avec un nombre réduit de PSN, en conséquence la liste des PSN qui sont utilisés pour l'authentification RADIUS pour un périphérique réseau donné peut être limitée de la même manière pour correspondre à la liste Call Home correspondante.

Ces aspects peuvent être pris en considération lors du développement de la stratégie de distribution PSN afin de déterminer le nombre maximal de PSN dans chaque liste Call Home :

- Nombre de PSN dans le déploiement
- Spécifications matérielles des noeuds PSN et MnT
- Nombre maximal de sessions de posture simultanées dans le déploiement
- Nombre de périphériques réseau
- Environnements hybrides (redirection simultanée et implémentation de posture sans redirection)
- Nombre de cartes utilisées par les points d'extrémité
- Emplacement des périphériques réseau et des PSN
- Types de connexion réseau utilisés pour la position (filaire, sans fil, VPN)



Exemple : Distribution PSN pour une posture sans redirection

Conseil : Utilisez Network Device Groups pour classer les périphériques réseau en fonction de la conception.

Configurer

Groupes de périphériques réseau (facultatif)

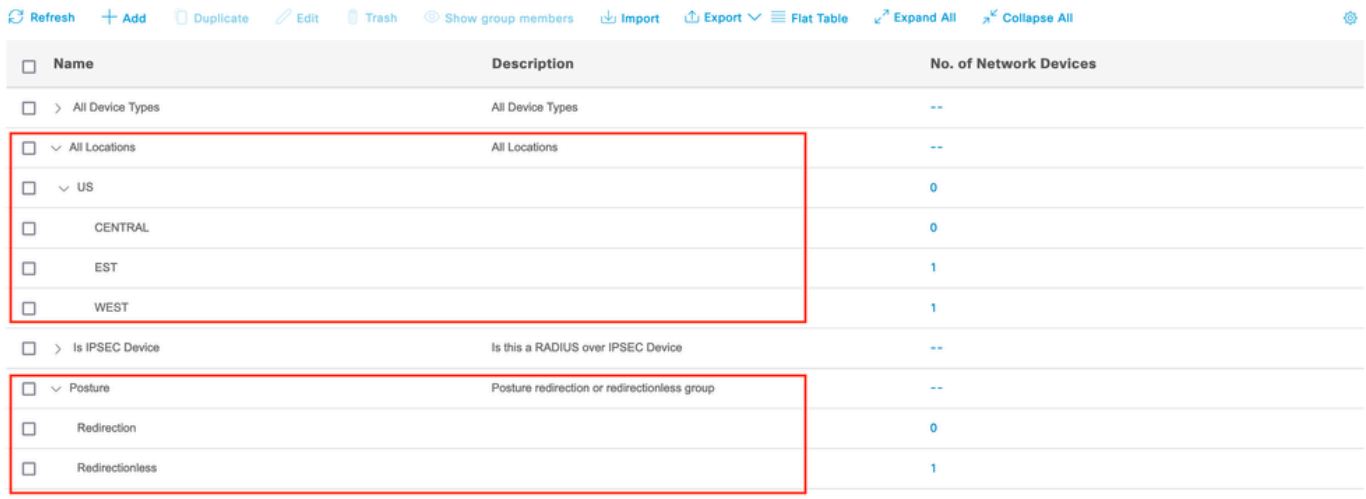
Les groupes de périphériques réseau peuvent être utilisés pour identifier et mettre en correspondance les périphériques réseau avec leur liste de serveurs RADIUS et leur liste Call Home correspondantes. Dans le cas d'environnements hybrides, ils peuvent également être utilisés pour identifier les périphériques qui prennent en charge la redirection à partir de périphériques qui ne le prennent pas en charge.

Si la stratégie de distribution développée pendant la phase de conception repose sur des groupes de périphériques réseau, suivez les étapes suivantes pour les configurer sur ISE :

1. Accédez à Administration > Network Resources Network Resource Groups.
2. Cliquez sur Add pour ajouter un nouveau groupe, indiquez un nom et sélectionnez le groupe parent, le cas échéant.
3. Répétez l'étape 2 pour créer tous les groupes nécessaires.

Dans les exemples utilisés tout au long de ce guide, le groupe de périphériques de localisation est utilisé pour identifier la liste des serveurs RADIUS et la liste Call Home, et un groupe de

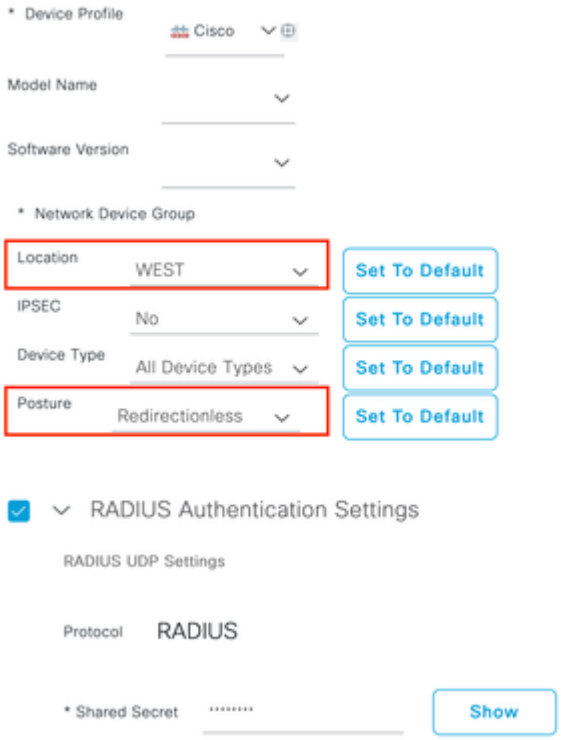
périphériques de posture personnalisé est utilisé pour identifier la redirection à partir de périphériques de posture non redirigés.



Groupes de périphériques réseau

Périphérique réseau

1. Le périphérique réseau peut être configuré pour l'authentification, l'autorisation et la comptabilité RADIUS. Reportez-vous à la documentation de chaque fournisseur pour connaître les étapes de configuration. Configurez la liste des serveurs RADIUS en fonction de la liste Call Home correspondante.
2. Sur ISE, accédez à Administration > Network Resources > Network Devices et cliquez sur Add. Configurez les groupes de périphériques réseau conformément à la conception et activez les paramètres d'authentification RADIUS pour configurer le secret partagé.



Configuration des périphériques réseau

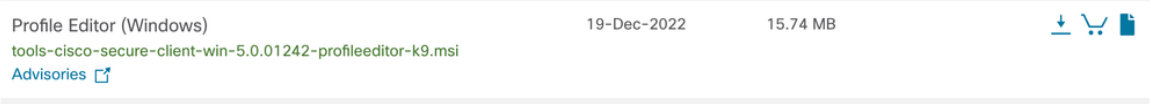
Provisionnement client

Il existe deux façons de fournir au client le logiciel et le profil appropriés pour effectuer la posture dans un environnement sans redirection :

1. Mise en service manuelle (pré-déploiement)
2. Portail d'approvisionnement client (déploiement Web)

Provisionnement manuel (pré-déploiement)

1. Téléchargez et installez Cisco Secure Client Profile Editor à partir de Cisco Software Download.



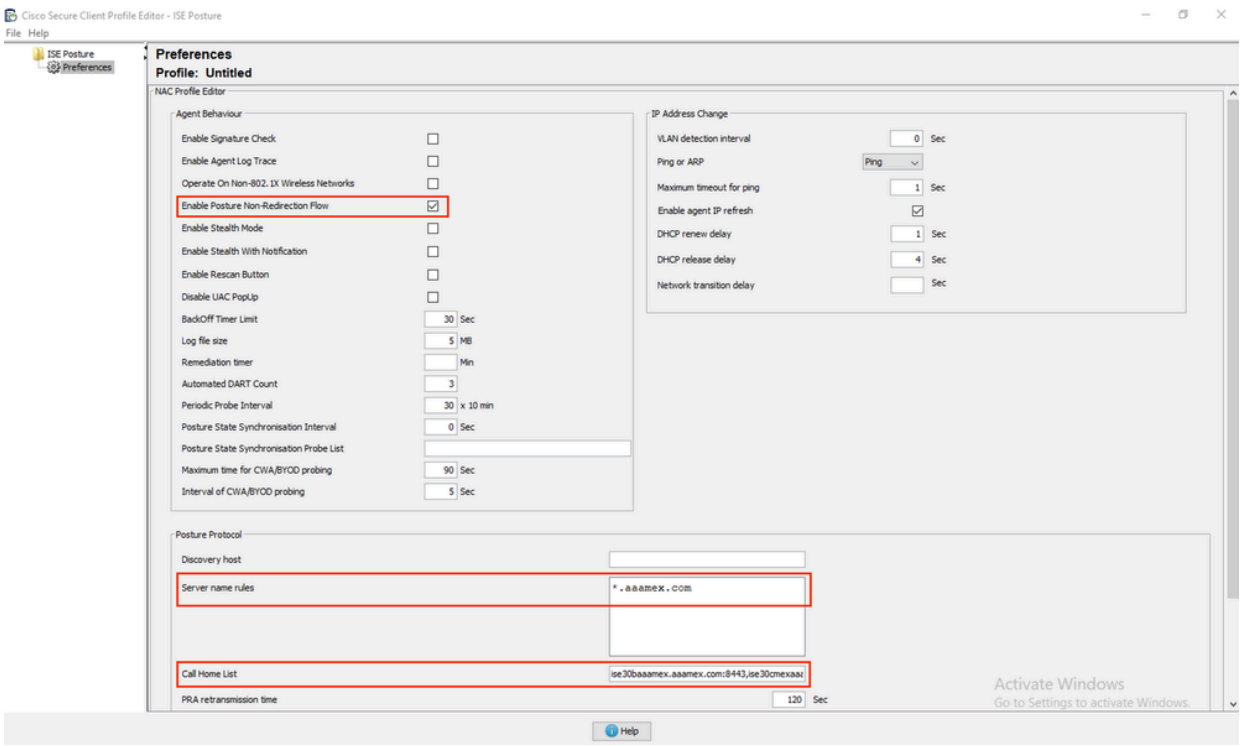
Package Éditeur de profil

2. Ouvrez l'éditeur de profil de posture ISE :
   - Assurez-vous que l'option Enable Posture Non-Redirection Flow est activée.
   - Configurez les règles de nom de serveur séparées par des virgules. Choisissez l'une des configurations suivantes :
     - Un seul astérisque * pour permettre la connexion à n'importe quel PSN.
     - Valeurs génériques (par exemple, *.aaamex.com) pour autoriser la connexion à tout PSN dans des domaines spécifiques.
     - Liste des FQDN PSN, séparés par des virgules, pour restreindre la connexion à des PSN spécifiques. Si elle est utilisée, cette liste doit correspondre à la liste

Call Home.

- Configurez Call Home List pour spécifier la liste de PSN séparés par des virgules. Veillez à ajouter le port du portail d'approvisionnement du client au format FQDN:port ou IP:port.

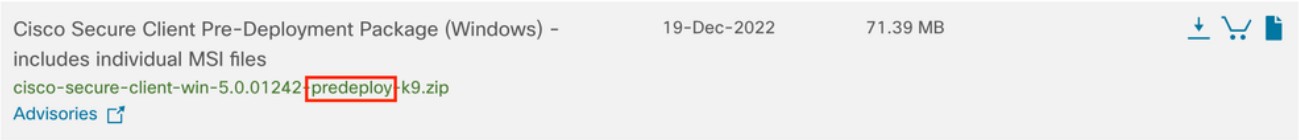
> Remarque : Les noms de domaine complets et les adresses IP utilisés dans la liste Call Home doivent être inclus dans le nom commun ou le nom alternatif du sujet des certificats du portail d'approvisionnement client des PSN correspondants.



Configuration du profil de posture avec l'Éditeur de profil

> Remarque : Reportez-vous à l'étape 4 de la section Politique d'approvisionnement du client pour obtenir des instructions sur la façon de vérifier le port du portail d'approvisionnement du client si nécessaire.

3. Enregistrez le profil sous le nom ISEPostureCFG.xml.
4. Répétez les étapes 2 et 3 pour créer un nouveau profil de position pour chaque liste Call Home en cours d'utilisation.
5. Téléchargez le package de prédéploiement du client sécurisé Cisco à partir de [Téléchargement de logiciels Cisco.]



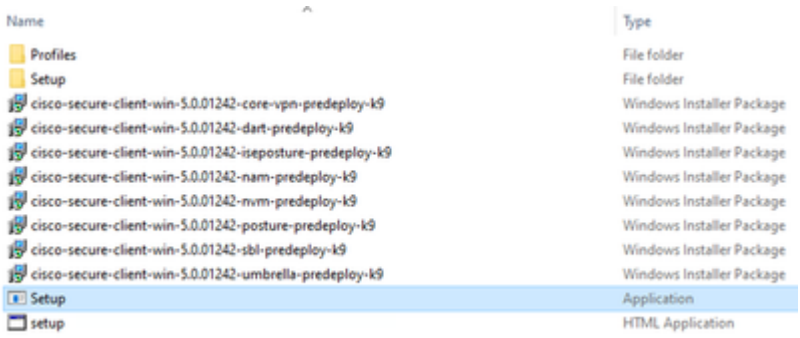
Package de pré-déploiement Cisco Secure Client

6. Distribuez les fichiers de profil et d'installation dans un fichier d'archive ou copiez les fichiers vers les clients.

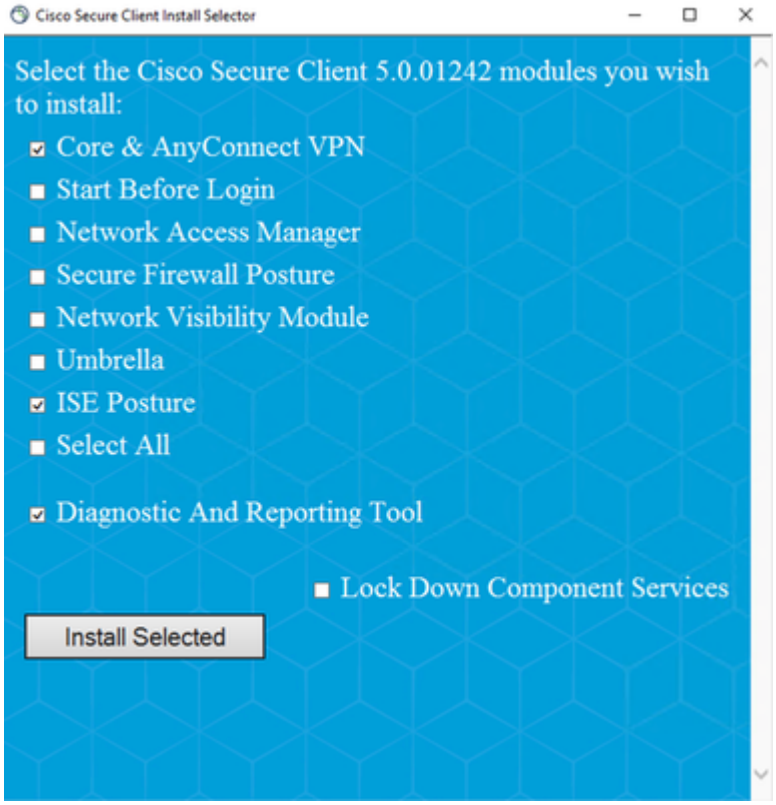
Avertissement : Assurez-vous que les mêmes fichiers Cisco Secure Client figurent également sur les têtes de réseau auxquelles vous prévoyez de vous connecter : Pare-feu sécurisé ASA, ISE, etc. Même lorsque le provisionnement manuel est utilisé, ISE doit être configuré pour le provisionnement client avec la version logicielle correspondante. Reportez-vous à la section Configuration de la stratégie de provisionnement du client pour obtenir des instructions détaillées.

---

7. Sur le client, ouvrez le fichier zip et exécutez le programme d'installation pour installer les modules Core et ISE Posture. Vous pouvez également utiliser les fichiers msi individuels pour installer chaque module. Dans ce cas, vous devez vous assurer que le module core-vpn est installé en premier.



Contenu du package de prédéploiement de Cisco Secure Client



Cisco Secure Client Installer

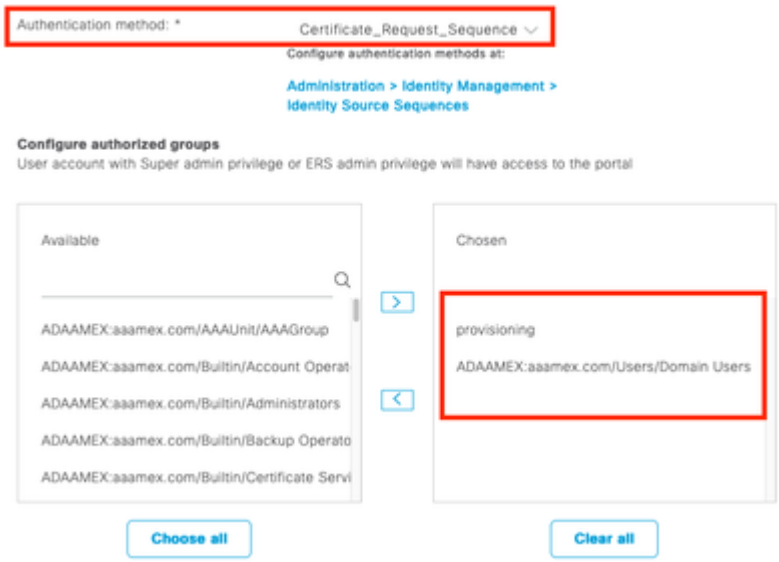
Conseil : Installez l'outil Diagnostic and Reporting Tool à utiliser à des fins de dépannage.

8. Une fois l'installation terminée, copiez le fichier xml de profil de posture aux emplacements suivants :
   - Fenêtres: %ProgramData%\Cisco\Cisco Secure Client\ISE Posture
   - MacOS : /opt/cisco/secureclient/iseposture/

Portail d'approvisionnement client (Web Deploy)

ISE Client Provisioning Portal peut être utilisé pour installer le module Cisco Secure Client ISE Posture et le profil de posture d'ISE. Il peut également être utilisé pour pousser le profil de posture seul si le module de posture ISE est déjà installé sur le client.

1. Accédez à Work Centers > Posture > Client Provisioning > Client Provisioning Portal pour ouvrir la configuration du portail. Développez la section Paramètres du portail et localisez le champ Méthode d'authentification, sélectionnez la séquence source d'identité à utiliser pour l'authentification dans le portail.
2. Configurez les groupes d'identité internes et externes qui sont autorisés à utiliser le portail d'approvisionnement du client.



Méthode d'authentification et groupes autorisés dans les paramètres du portail

3. Dans le champ Nom de domaine complet (FQDN), configurez l'URL qui est utilisée par les clients pour accéder au portail. Pour configurer plusieurs noms de domaine complets, entrez les valeurs séparées par des virgules.



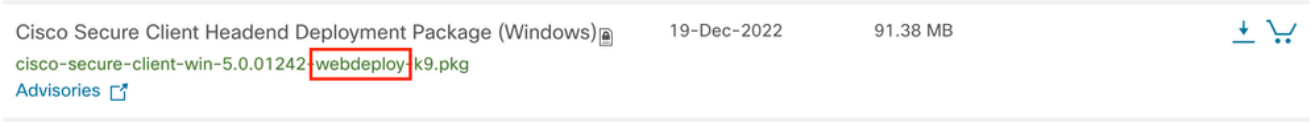
4. Configurez le ou les serveurs DNS pour résoudre l'URL du portail vers les PSN de la liste Call Home correspondante.
5. Fournir le nom de domaine complet aux utilisateurs finaux pour qu'ils puissent accéder au portail afin d'installer le logiciel ISE Posture.

Remarque : Pour utiliser le nom de domaine complet du portail, les clients doivent disposer de la chaîne de certificats Admin PSN et de la chaîne de certificats Portal installées dans le magasin de confiance, et le certificat Admin doit contenir le nom de domaine complet du portail dans le champ SAN.

Politique de provisionnement client

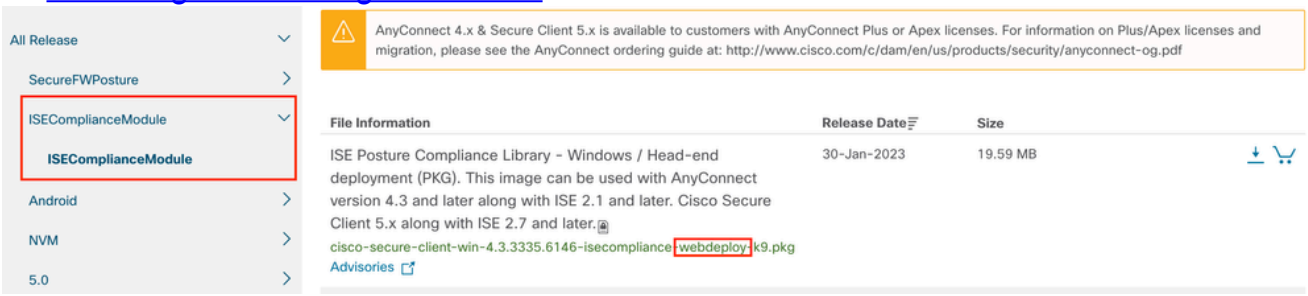
La mise en service du client doit être configurée sur ISE, quel que soit le type de mise en service (pré-déploiement ou déploiement Web) utilisé pour installer Cisco Secure Client sur les terminaux.

1. Téléchargez le package de déploiement Cisco Secure Client Headend depuis Téléchargement de logiciels Cisco.



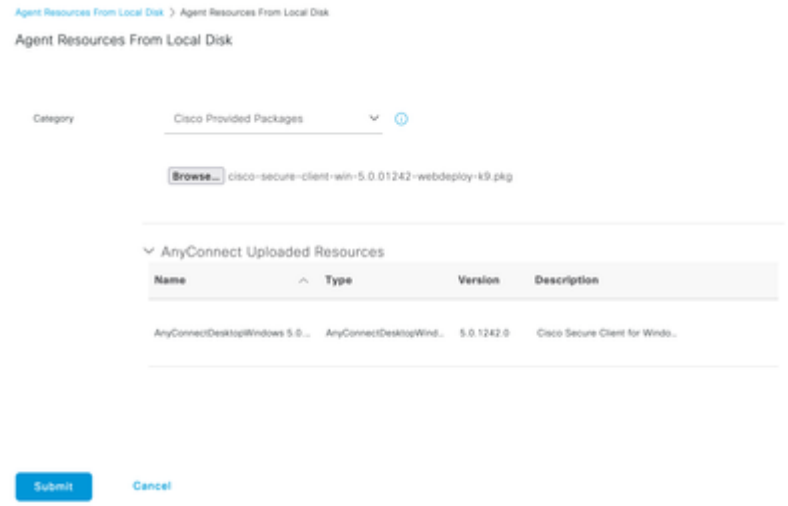
Package Cisco Secure Client Webdeploy

2. Téléchargez le dernier package de déploiement Web du module de conformité ISE à partir de [Téléchargement de logiciels Cisco.](#)



Module de conformité ISE - Package Webdeploy

3. Sur ISE, accédez à Work Centers > Posture > Client Provisioning > Resources et cliquez sur Add > Agent resources from local disk. Sélectionnez Cisco Provided Packages dans le menu déroulant Category et téléchargez le Cisco Secure Client Headend Deployment Package précédemment téléchargé. Répétez la même procédure pour télécharger le module de conformité.



Télécharger les packages fournis par Cisco vers ISE

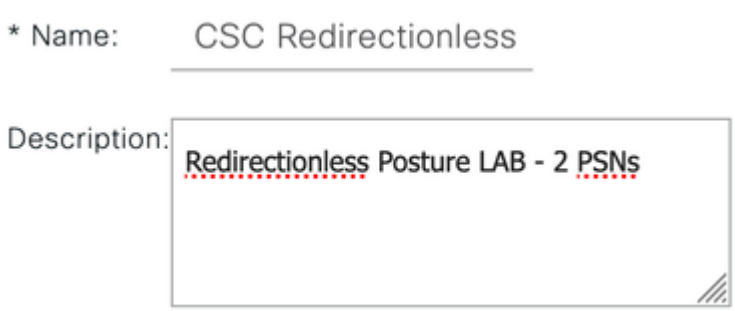
4. De nouveau dans l'onglet Resources, cliquez sur Add > Agent Posture Profile. Sur le profil :
   - Configurez un nom qui peut être utilisé pour identifier le profil et la liste Call Home dans ISE.
   - Assurez-vous que Enable extra probes so non-redirection flow can work est défini sur Yes.
   - Configurez la liste des serveurs Discovery Backup. Sélectionnez les PSN qui correspondent à la liste Call Home en cours de configuration.
     Il s'agit de la liste des PSN enregistrés dans ConnectionData.xml après la première connexion.
   - Configurez les règles de nom de serveur séparées par des virgules. Choisissez l'une

des configurations suivantes :

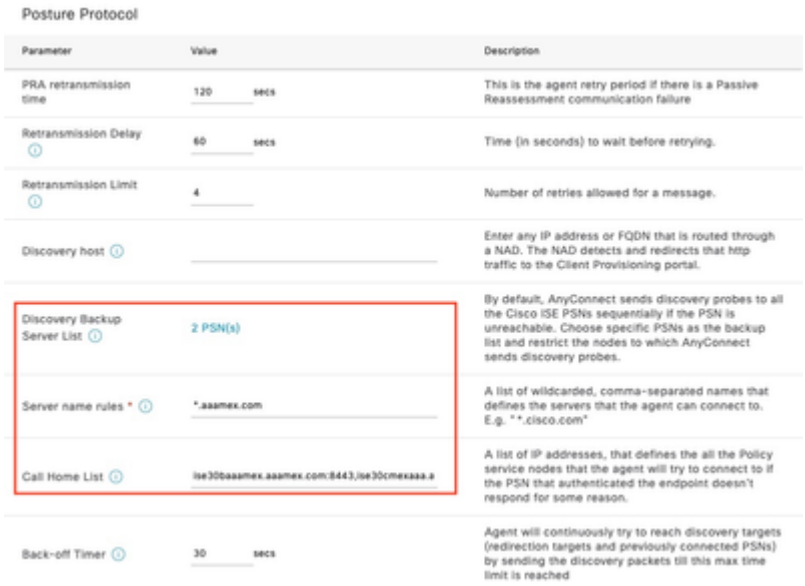
- Un seul astérisque * pour permettre la connexion à n'importe quel PSN.
- Valeurs génériques (par exemple, *.aaamex.com) pour autoriser la connexion à tout PSN dans des domaines spécifiques.
- Liste des FQDN PSN, séparés par des virgules, pour limiter la connexion à des PSN spécifiques. Si elle est utilisée, cette liste doit correspondre à la liste Call Home.

- Configurez Call Home List pour spécifier la liste de PSN séparés par des virgules. Assurez-vous d'ajouter le port du portail d'approvisionnement du client au format FQDN:port ou IP:port.
  Pour rechercher ou modifier le port CPP, accédez à Work Centers > Posture > Client Provisioning > Client Provisioning Portal, sélectionnez le portail en cours d'utilisation, développez Portal Settings et recherchez le port HTTPs.

Remarque : Les noms de domaine complets et les adresses IP utilisés dans la liste Call Home doivent être inclus dans le nom commun ou le nom alternatif du sujet des certificats du portail d'approvisionnement client des PSN correspondants.



Configuration du profil de posture de l'agent



Configuration du protocole de posture dans le profil de posture de l'agent

5. De nouveau dans l'onglet Resources, cliquez sur Add > Agent Configuration. Sélectionnez le package Cisco Secure Client et le module de conformité à utiliser.

Avertissement : Si le client sécurisé Cisco a été pré-déployé sur les clients, assurez-vous que la version sur ISE correspond à la version sur les terminaux. Si ASA ou FTD est utilisé pour le déploiement Web, la version de ce périphérique peut également correspondre.

---

6. Faites défiler jusqu'à la section Sélection de la posture et sélectionnez le profil qui a été créé à l'étape 1. Cliquez sur Envoyer au bas de la page pour enregistrer la configuration.

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1.2.042

* Configuration Name:

SecureClient Configuration Redirectionless

Description:

Redirectionless Lab Call Home List 1

Description Value Notes

* Compliance Module: CiscoSecureClientComplianceModuleWindows

Cisco Secure Client Module Selection

ISE Posture	☑
VPN	☑
Zero Trust Access	☐
Network Access Manager	☐
Secure Firewall Posture	☐
Network Visibility	☐
Umbrella	☐
Start Before Logon	☐
Diagnostic and Reporting Tool	☑

Profile Selection

* ISE Posture: CSC Redirectionless

VPN:

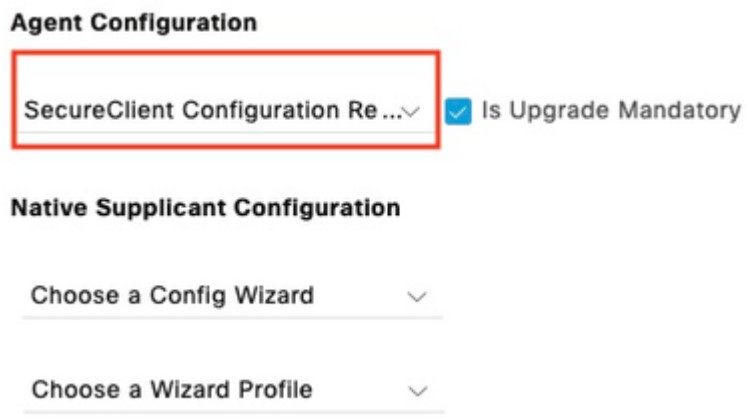
Configuration des agents

☐

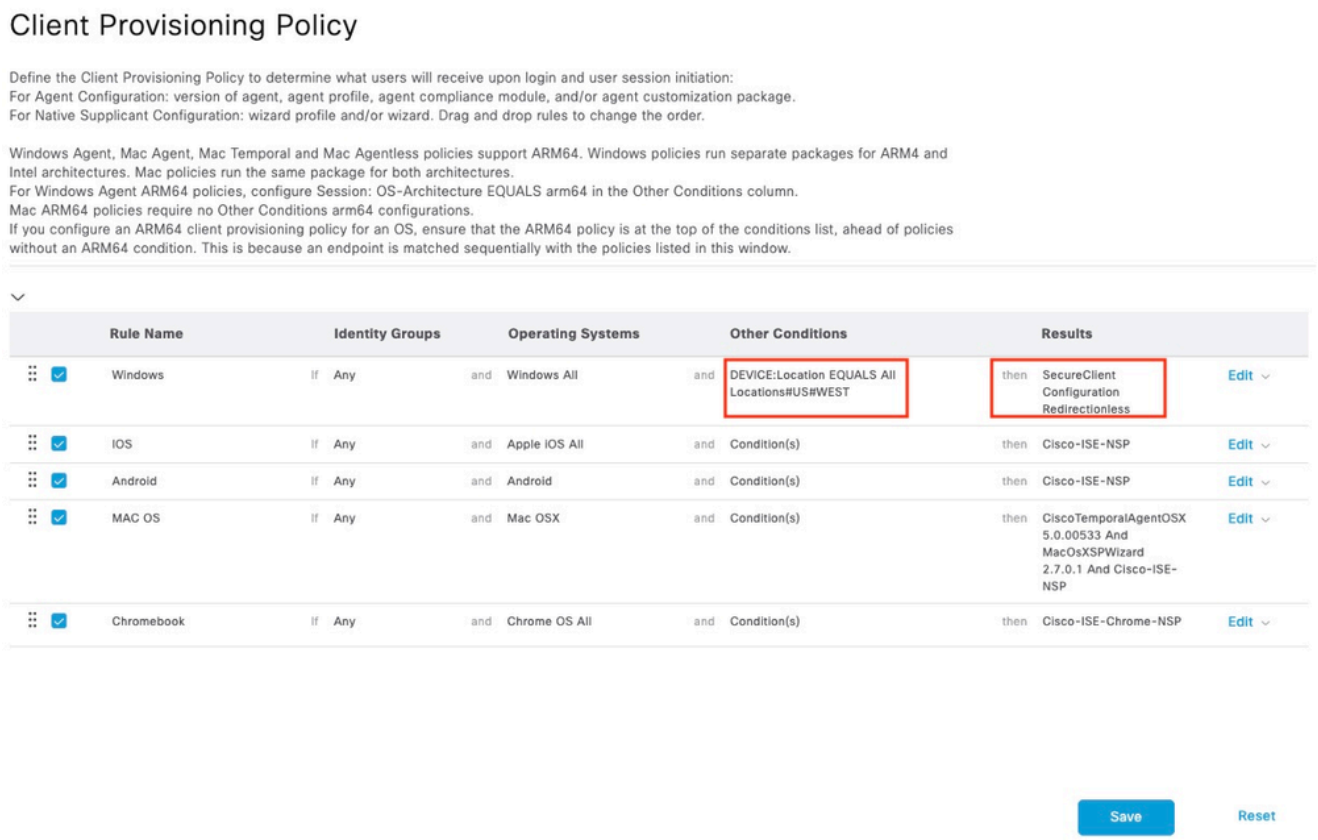
7. Accédez à Work Centers > Posture > Client Provisioning > Client Provisioning policy. Localisez la stratégie utilisée pour le système d'exploitation requis et cliquez sur Edit. Cliquez sur le signe + dans la colonne Résultats et sélectionnez la configuration de l'agent à l'étape 5 sous la section Configuration de l'agent. Cliquez sur Enregistrer en bas de la page.

Remarque : Dans le cas de plusieurs listes Call Home, utilisez le champ Other Conditions pour pousser le bon profil vers les clients correspondants. Dans cet exemple, Device Location Group est utilisé pour identifier le profil de posture qui est poussé dans la stratégie.

Conseil : Si plusieurs stratégies d'approvisionnement de clients sont configurées pour le même système d'exploitation, il est recommandé de les rendre mutuellement exclusives, c'est-à-dire qu'un client donné ne peut accéder qu'à une seule stratégie à la fois. Les attributs RADIUS peuvent être utilisés sous la colonne Other Conditions pour différencier une politique d'une autre.



Configuration de l'agent dans la politique de provisionnement client



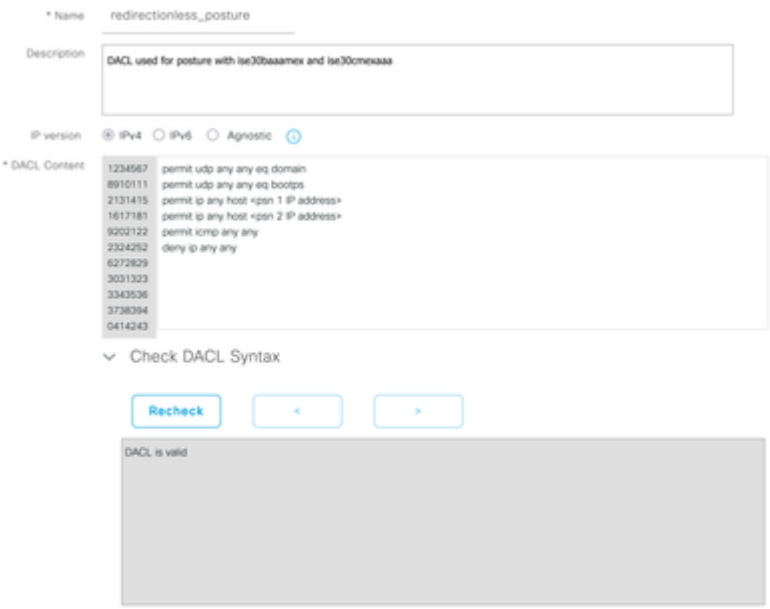
Politique de provisionnement client

8. Répétez les étapes 4 à 7 pour chaque liste Call Home et le profil de position correspondant en cours d'utilisation. Pour les environnements hybrides, les mêmes profils peuvent être utilisés pour rediriger les clients.

Autorisation

Profil d'autorisation

1. Accédez à Policy > Policy Elements > Results > Authorization > Downloadable ACLs et cliquez sur Add.
2. Créez une DACL pour autoriser le trafic vers DNS, DHCP (le cas échéant), les PSN ISE et bloquer tout autre trafic. Assurez-vous d'autoriser tout autre trafic nécessaire à l'accès avant l'accès conforme final.



Configuration DACL

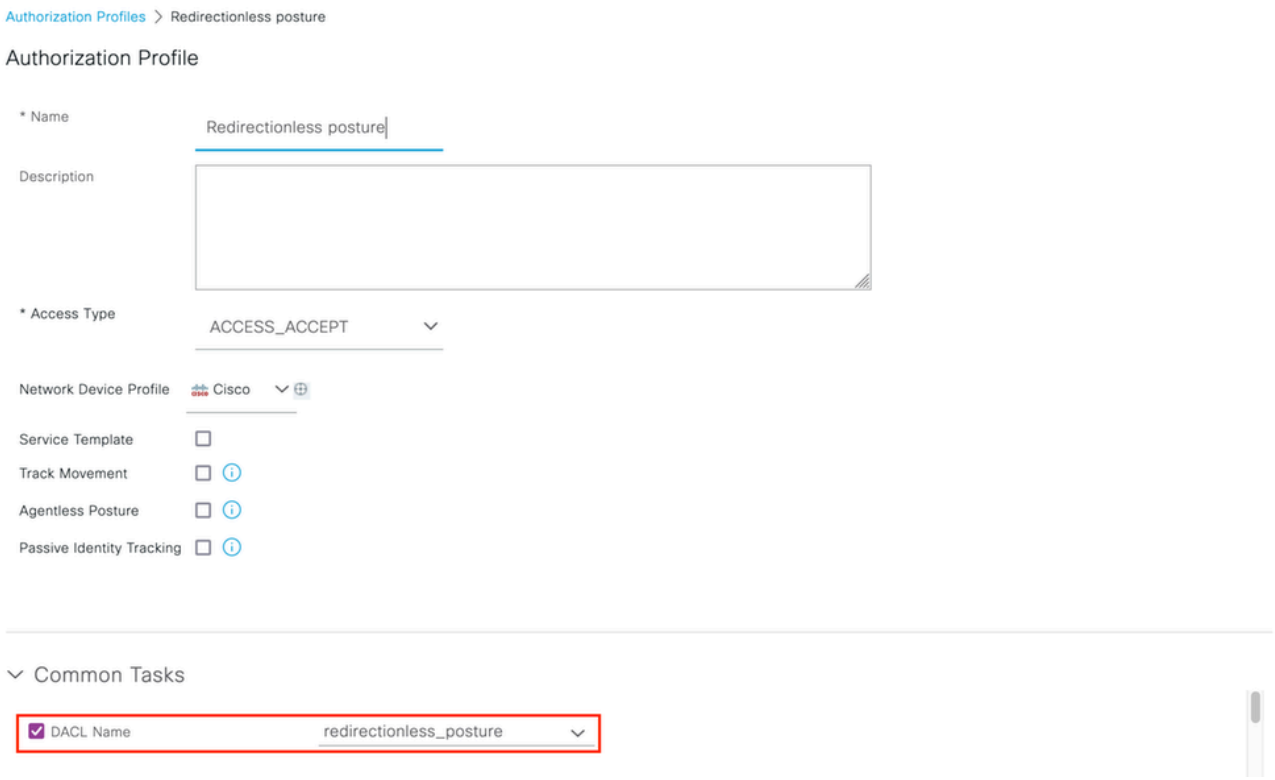
permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

permit ip any host

deny ip any any

⚠ Mise en garde : Certains périphériques tiers ne prennent pas en charge les listes de contrôle d'accès numériques. Dans ce cas, il est nécessaire d'utiliser un ID de filtre ou d'autres attributs spécifiques au fournisseur. Reportez-vous à la documentation du fournisseur pour plus d'informations. Si aucune liste de contrôle d'accès n'est utilisée, assurez-vous de configurer la liste correspondante dans le périphérique réseau.

3. Accédez à Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation et cliquez sur Ajouter. Attribuez un nom au profil d'autorisation et sélectionnez le nom DACL dans Tâches courantes. Dans le menu déroulant, sélectionnez la DACL créée à l'étape 2.



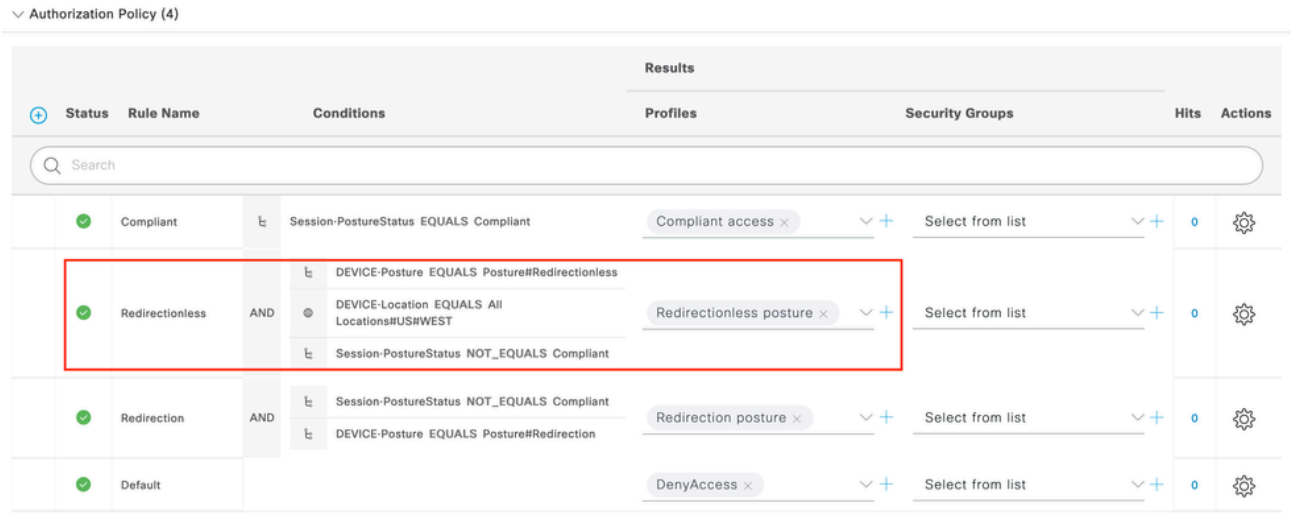
Profil d'autorisation

Remarque : Si les listes de contrôle d'accès DACL ne sont pas utilisées, utilisez Filter-ID from Common Tasks ou the Advanced Attribute Settings pour pousser le nom de la liste de contrôle d'accès correspondante.

4. Répétez les étapes 1 à 3 pour chaque liste Call Home utilisée. Pour les environnements hybrides, un seul profil d'autorisation est nécessaire pour la redirection. La configuration du profil d'autorisation pour la redirection sort du cadre de ce document.

Politique d'autorisation

1. Accédez à Policy > Policy Sets et ouvrez le policy set en cours d'utilisation ou créez-en un nouveau.
2. Faites défiler jusqu'à la section Authorization Policy. Créez une stratégie d'autorisation à l'aide de Session PostureStatus NOT_EQUALS Compliant et sélectionnez le profil d'autorisation créé dans la section précédente.



Stratégies d'autorisation

3. Répétez l'étape 2 pour chaque profil d'autorisation avec la liste Call Home correspondante utilisée. Pour les environnements hybrides, une seule politique d'autorisation de redirection est nécessaire.

Dépannage

Conforme au client sécurisé Cisco et non applicable à la position (en attente) sur ISE

Sessions obsolètes/fantômes

La présence de sessions obsolètes ou fantômes dans le déploiement peut générer des pannes intermittentes et apparemment aléatoires avec la découverte de posture sans redirection, ce qui a pour conséquence que les utilisateurs sont bloqués dans une posture d'accès inconnu/non applicable sur ISE alors que l'interface utilisateur du client sécurisé Cisco montre un accès conforme.

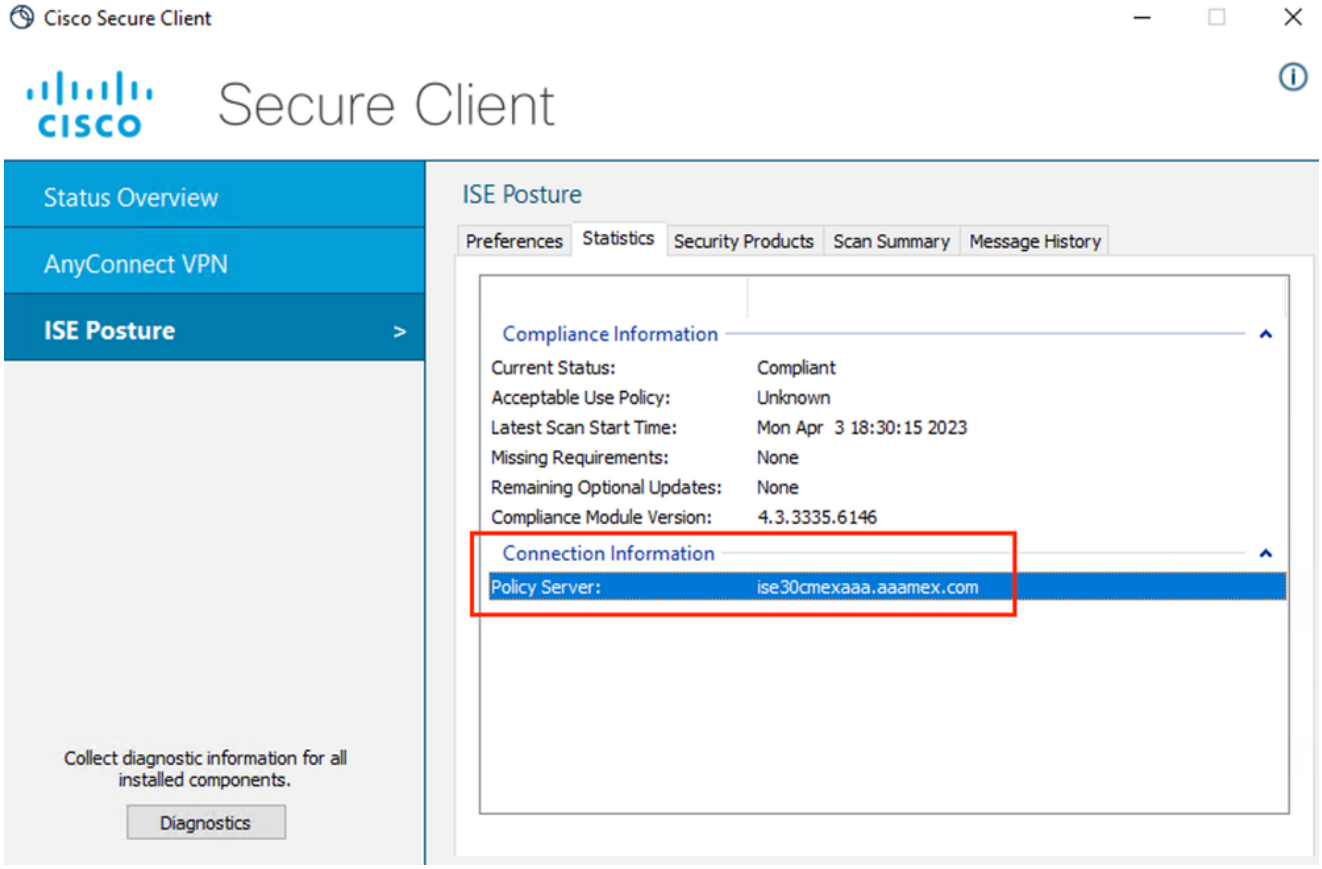
Les sessions obsolètes sont d'anciennes sessions qui ne sont plus actives. Ils sont créés par une demande d'authentification et un démarrage de la gestion des comptes, mais aucun arrêt de la gestion des comptes n'est reçu sur le PSN pour effacer la session.

Les sessions fantômes sont des sessions qui n'ont jamais été actives dans un PSN particulier. Ils sont créés par une mise à jour intermédiaire de la comptabilité, mais aucun arrêt de la comptabilité n'est reçu sur le PSN pour effacer la session.

Identifier

Pour identifier un problème de session obsolète/fantôme, vérifiez le PSN utilisé dans l'analyse du système sur le client et comparez-le au PSN effectuant l'authentification :

1. Dans l'interface utilisateur du client sécurisé Cisco, cliquez sur l'icône de l'engrenage dans le coin inférieur gauche. Dans le menu de gauche, ouvrez la section Position ISE et accédez à l'onglet Statistiques. Notez le serveur de stratégie dans les informations de connexion.



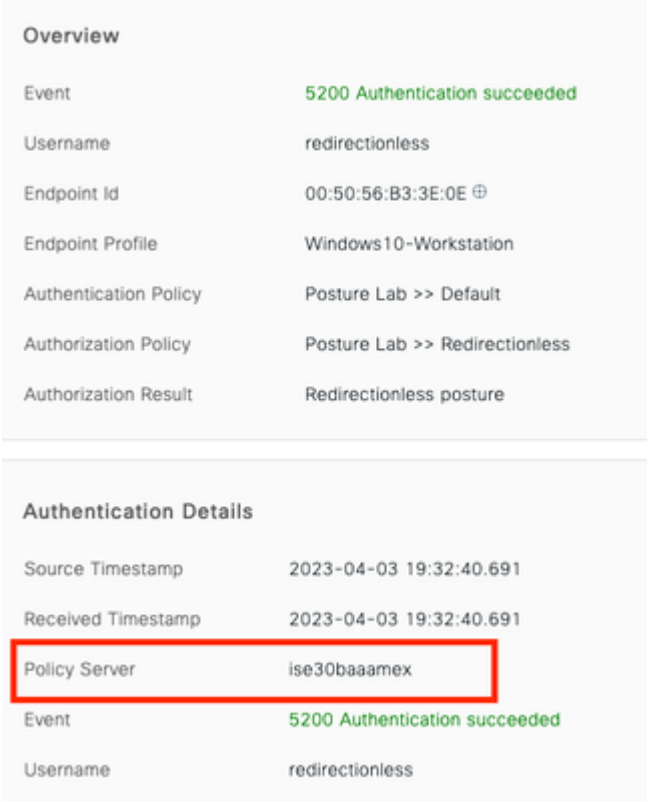
Policy Server pour la position ISE dans Cisco Secure Client

2. Dans les journaux en direct d'ISE RADIUS, prenez note des points suivants :
   - Changement d'état de posture
   - Modification du serveur
   - Aucun changement dans la politique d'autorisation et le profil d'autorisation
   - Pas de journal en direct CoA



Journaux actifs pour les sessions obsolètes/fantômes

3. Ouvrez la session active ou les détails du dernier journal d'authentification en direct. Notez que le serveur Policy Server, s'il diffère du serveur observé à l'étape 1, indique un problème avec les sessions obsolètes/fantômes.

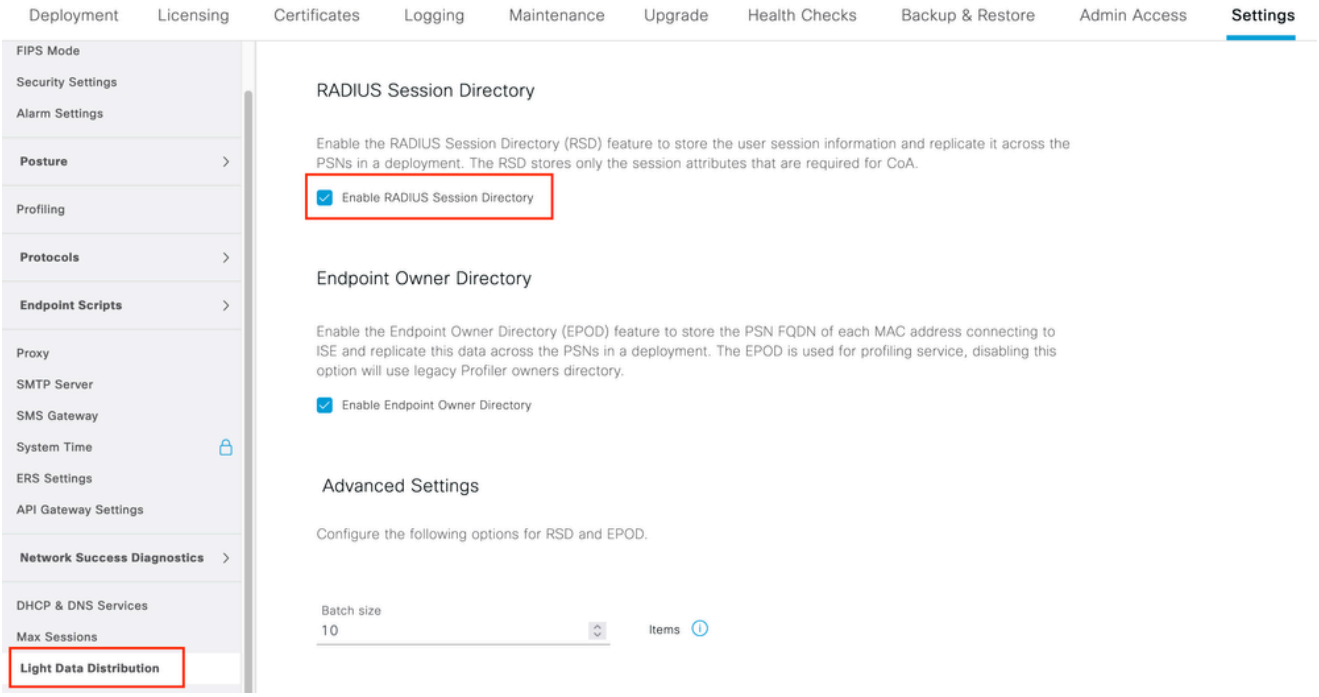


Serveur de stratégie dans les détails du journal en direct

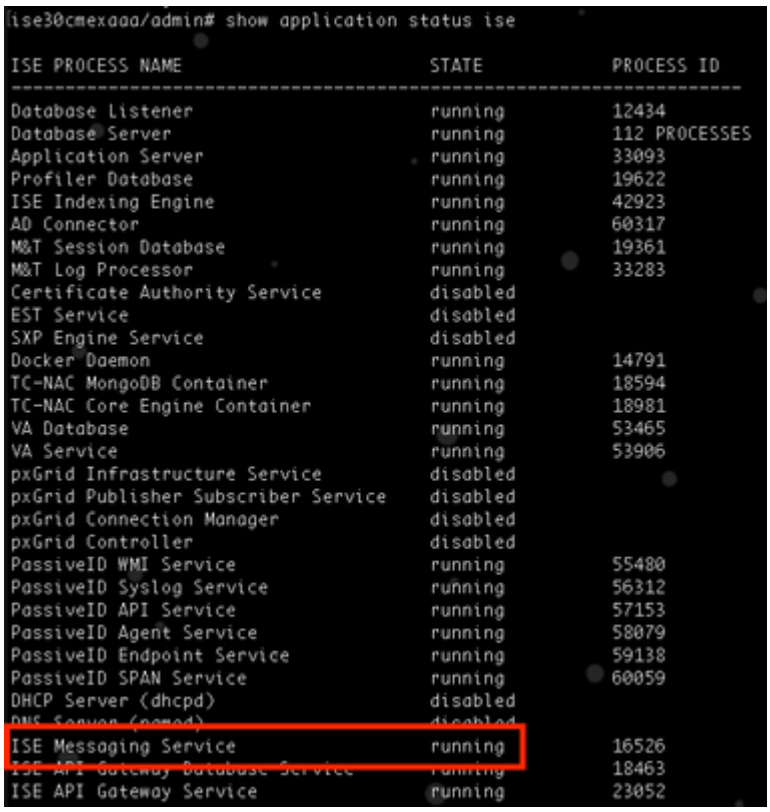
Solution

Les versions ISE postérieures aux correctifs 6 et 3 de la version 2.6 de la version ISE mettent en oeuvre le répertoire de session RADIUS comme solution pour un scénario de session obsolète/fantôme dans un flux de posture non redirigé.

1. Accédez à Administration > System > Settings > Light Data Distribution et vérifiez que la case à cocher Enable RADIUS Session Directory est activée.



2. À partir de l'interface de ligne de commande ISE, vérifiez que le service de messagerie ISE est en cours d'exécution sur tous les PSN en exécutant la commande show applications status ise.



```
ise30cmexaaa/admin# show application status ise

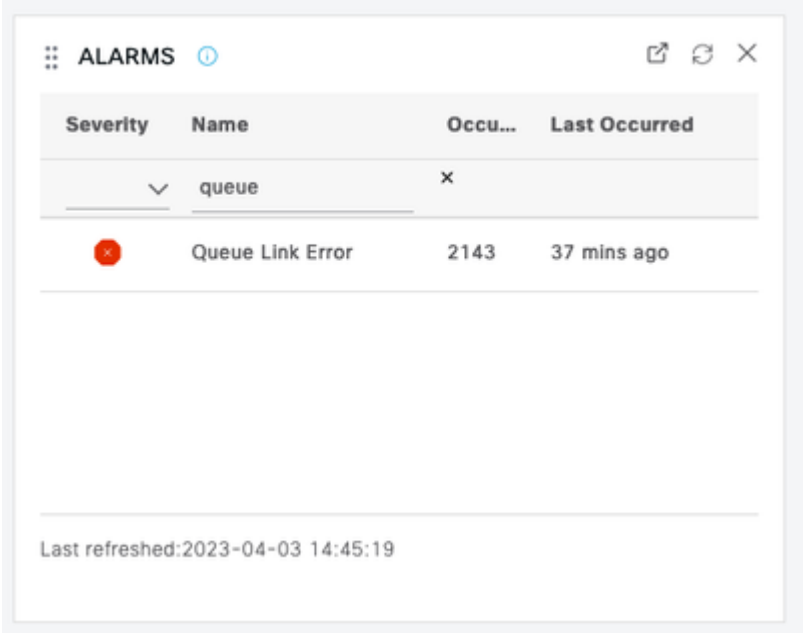
ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          12434
Database Server                        running          112 PROCESSES
Application Server                     running          33093
Profiler Database                      running          19622
ISE Indexing Engine                    running          42923
AD Connector                           running          60317
M&T Session Database                   running          19361
M&T Log Processor                      running          33283
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          14791
TC-NAC MongoDB Container               running          18594
TC-NAC Core Engine Container           running          18981
VA Database                            running          53465
VA Service                             running          53906
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  running          55480
PassiveID Syslog Service               running          56312
PassiveID API Service                  running          57153
PassiveID Agent Service                running          58079
PassiveID Endpoint Service             running          59138
PassiveID SPAN Service                 running          60059
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          16526
ISE API Gateway Database Service       running          18463
ISE API Gateway Service                running          23052
```

Service de messagerie ISE en cours

Remarque : Ce service fait référence à la méthode de communication qui est utilisée pour RSD entre PSN et peut être exécuté quel que soit l'état du paramètre de service de messagerie ISE pour Syslog qui peut être défini à partir de l'interface utilisateur ISE.

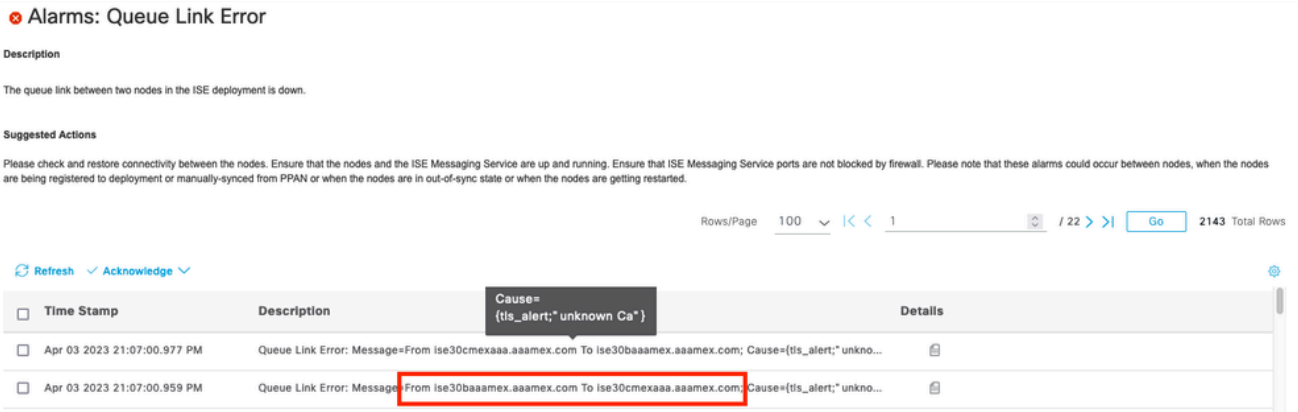
---

3. Accédez à Tableau de bord ISE et localisez le dashlet Alarmes. Vérifiez s'il existe des alarmes d'erreur de liaison de file d'attente. Cliquez sur le nom de l'alarme pour afficher plus de détails.



Alarmes d'erreur Queue Link

4. Vérifiez si les alarmes sont générées entre les PSN utilisés pour la posture.



Détails d'alarme Queue Link Error

5. Passez le curseur sur la description de l'alarme pour afficher tous les détails et prendre note du champ Cause. Les deux causes les plus courantes d'erreur de liaison de file d'attente sont :
   - Délai d'attente : indique que les requêtes envoyées par un noeud à un autre noeud sur le port 8671 ne reçoivent pas de réponse dans le seuil. Pour corriger le problème, vérifiez que le port TCP 8671 est autorisé entre les noeuds.
   - CA inconnue : indique que la chaîne de certificats qui signe le certificat de messagerie ISE n'est pas valide ou est incomplète. Pour corriger cette erreur :
     a. Accédez à Administration > Système > Certificats > Demandes de signature de certificat.
     b. Cliquez sur Générer des demandes de signature de certificat (CSR).
     c. Dans le menu déroulant, sélectionnez ISE Root CA et cliquez sur Replace ISE Root CA Certificate chain.
     Si l'autorité de certification racine ISE n'est pas disponible, accédez à Certificate Authority > Internal CA settings et cliquez sur Enable Certificate Authority, puis revenez au CSR et régénérez l'autorité de certification racine.

d. Générez un nouveau CSR et sélectionnez ISE Messaging Service dans le menu déroulant.
e. Sélectionnez tous les noeuds du déploiement et régénérez le certificat.

Remarque : Il est prévu d'observer les alarmes d'erreur de liaison de file d'attente avec la cause Inconnu CA ou Econrefusé pendant que les certificats sont régénérés. Surveillez les alarmes après la génération du certificat pour confirmer que le problème est résolu.

rendement

Identifier

Les problèmes de performances tels qu'une utilisation CPU élevée et une charge moyenne élevée liés à une posture sans redirection peuvent avoir un impact sur PSN ainsi que sur les noeuds MnT et sont souvent accompagnés ou précédés par les événements suivants :

- Aléatoire ou intermittente, aucune erreur détectée par le serveur de stratégie, dans Cisco Secure Client.
- Les rapports de limite de ressources maximale atteinte pour le pool de threads de service Portal ont atteint les événements de valeur de seuil. Accédez à Opérations > Etats > Etats > Audit > Audit des opérations pour voir les états.
- La requête de posture à la recherche MNT est une alarme élevée. Ces alarmes sont uniquement générées sur ISE 3.1 et les versions ultérieures.

Solution

Si la performance du déploiement est affectée par une position sans redirection, cela indique souvent une implémentation inefficace. Il est recommandé de réviser ces aspects :

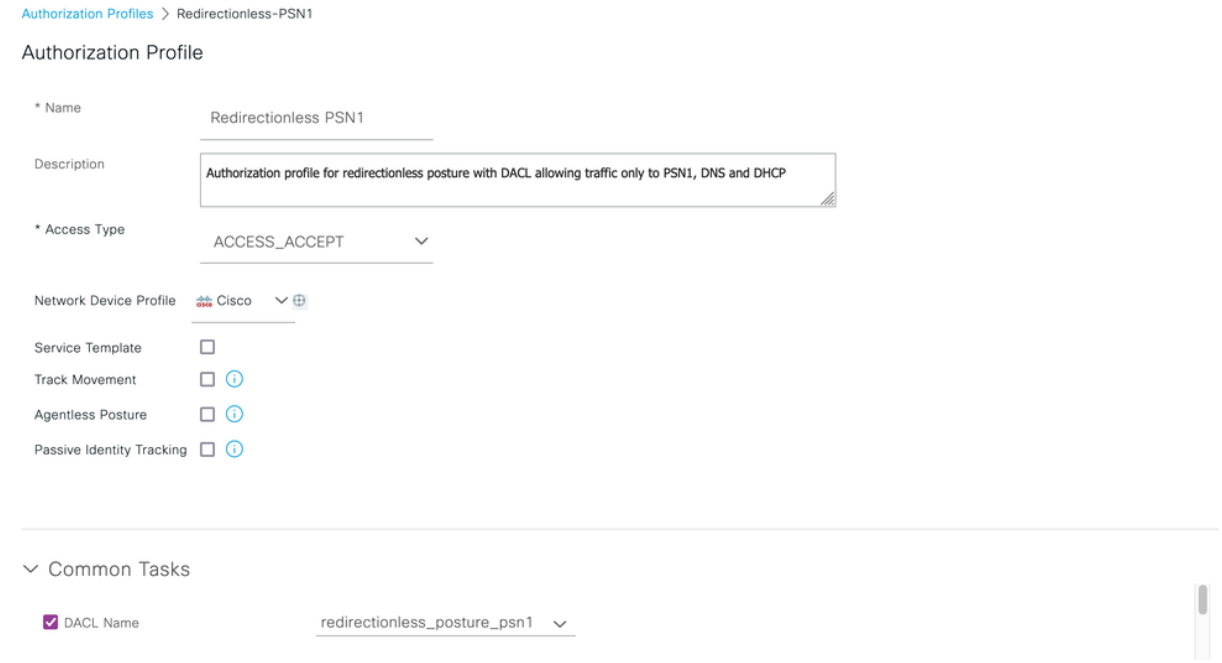
- Nombre de PSN utilisés par liste Call Home. Envisagez de réduire le nombre de PSN pouvant être utilisés pour chaque terminal ou périphérique réseau, conformément à la conception.
- Port du portail d'approvisionnement client dans la liste Call Home. Assurez-vous que le numéro de port du portail est inclus après l'adresse IP ou le nom de domaine complet de chaque noeud.

Pour atténuer l'impact :

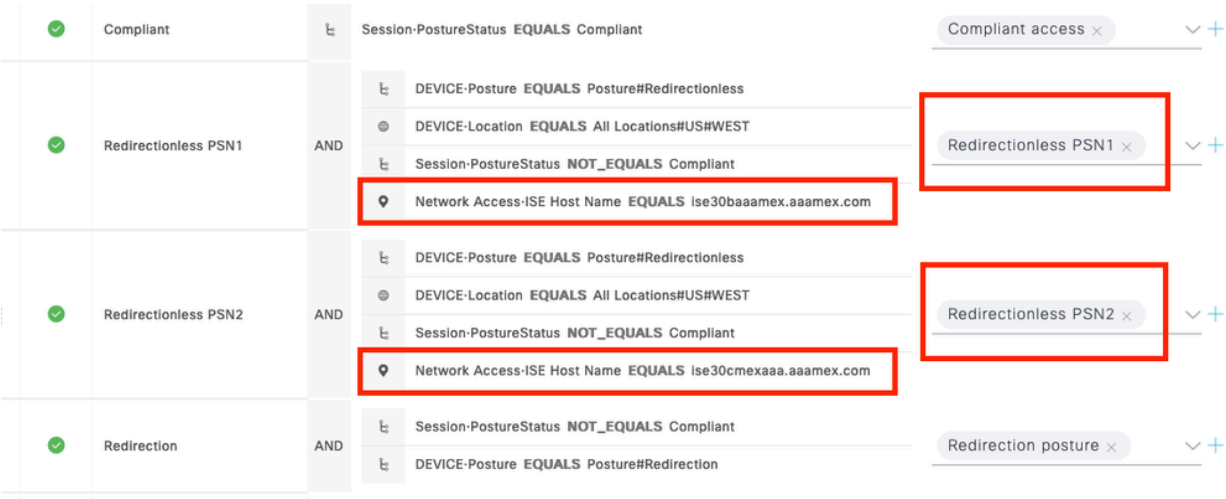
1. Effacez le fichier connectiondata.xml des points d'extrémité en supprimant le fichier du dossier Cisco Secure Client et en redémarrant le service de posture ISE ou Cisco Secure Client. Si les services ne sont pas redémarrés, l'ancien fichier est régénéré et les modifications ne prennent pas effet. Cette action peut également être effectuée après la révision et la modification des listes Call Home.

2. Utilisez des DACL ou d'autres ACL pour bloquer le trafic vers les PSN ISE pour les connexions réseau lorsque cela n'est pas pertinent :

   - Pour les connexions où la position n'est pas appliquée dans les stratégies d'autorisation, mais qui s'appliquent aux terminaux avec le module Cisco Secure Client ISE Posture installé, bloquez le trafic des clients vers tous les PSN ISE pour les ports TCP 8905 et le port Client Provisioning Portal. Cette action est également recommandée pour la posture avec mise en oeuvre de la redirection.
   - Pour les connexions où la position est appliquée dans les stratégies d'autorisation, autorisez le trafic des clients vers le PSN d'authentification et bloquez le trafic vers d'autres PSN dans le déploiement. Cette action peut être mise en oeuvre temporairement pendant la révision de la conception.



Profil d'autorisation avec DACL pour PSN unique



Politiques d'autorisation par PSN

Gestion de comptes

La comptabilité RADIUS est essentielle pour la gestion des sessions sur ISE. Étant donné que la position dépend de l'exécution d'une session active, une configuration incorrecte ou un manque de comptabilité peut également avoir un impact sur la découverte de position et les performances ISE. Il est important de vérifier que la gestion des comptes est correctement configurée sur le périphérique réseau pour envoyer des demandes d'authentification, le démarrage de la gestion des comptes, l'arrêt de la gestion des comptes et les mises à jour de la gestion des comptes à un seul PSN pour chaque session.

Pour vérifier les paquets de comptabilité reçus sur ISE, accédez à Operations > Reports > Reports > Endpoints and Users > RADIUS Accounting.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.