Comprendre et configurer la condition de position ISE du service macOS

Table des matières

Introduction

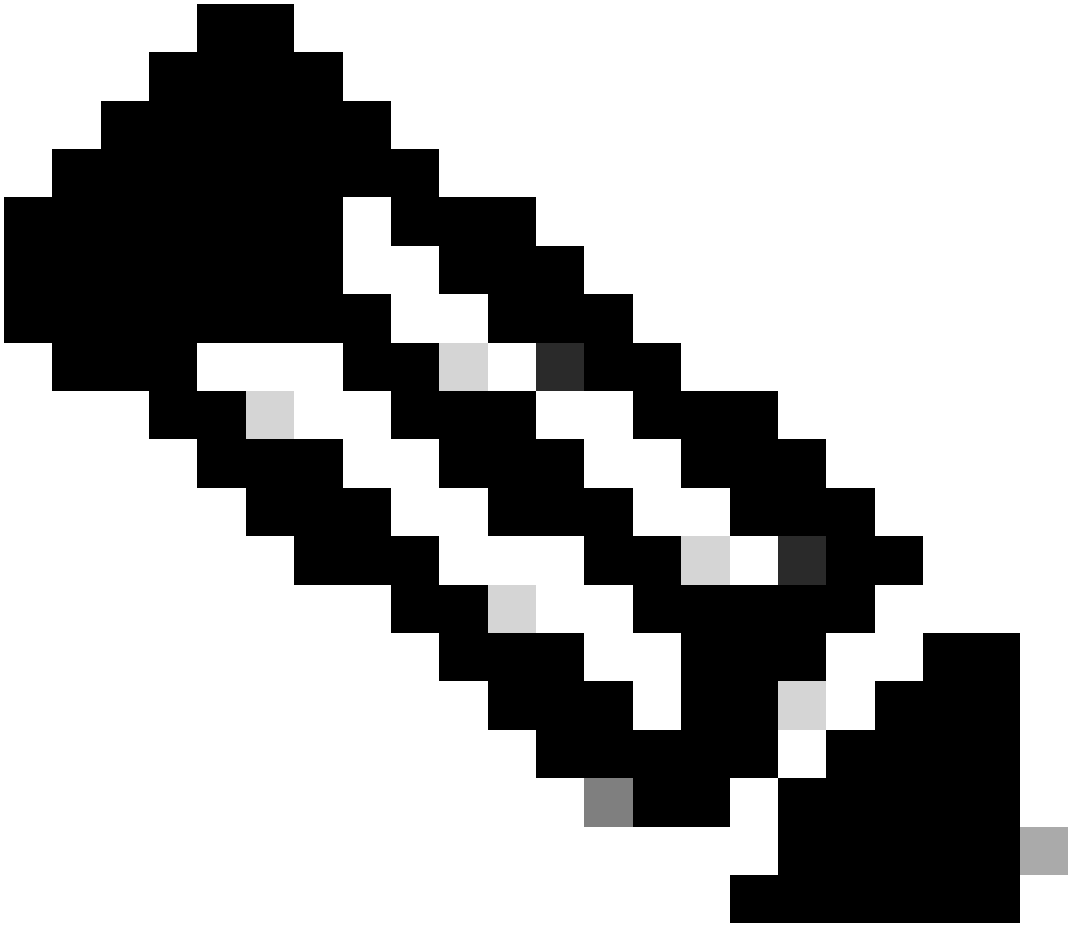
Ce document décrit le processus de configuration de la condition de service macOS dans Cisco ISE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de macOS.
- Connaissance du flux de posture ISE.



Remarque : Ce document couvre la configuration pour la condition de service macOS. La configuration de posture initiale n'est pas traitée dans ce document.

Composants utilisés

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

- Correctif 1 de Cisco ISE 3.3
- périphérique macoOS exécutant Sonoma 14.3.1
- Cisco Secure Client 5.1.2.42
- Module de conformité version 4.3.3432.64000

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.

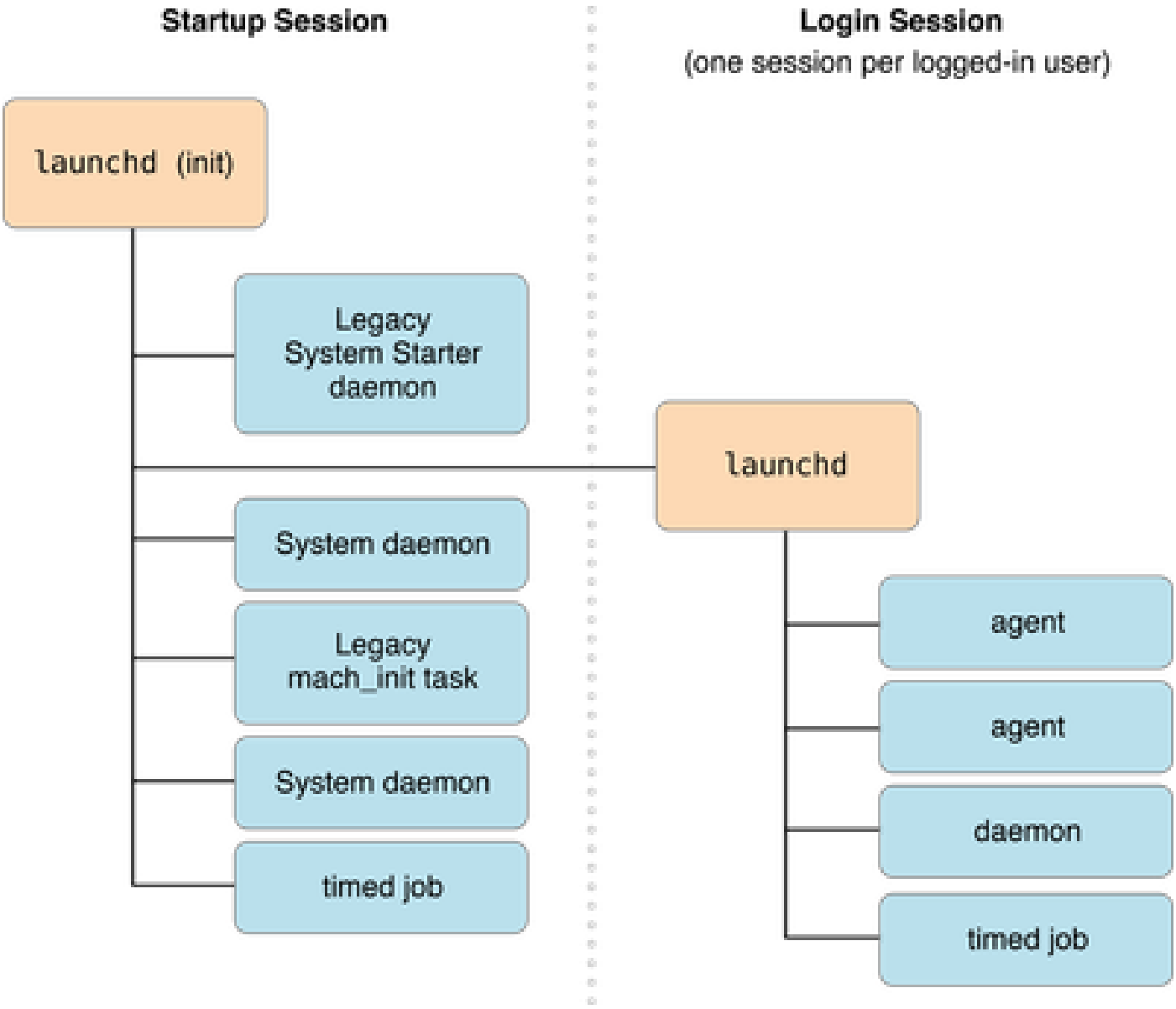
Informations générales

La condition de service macOS est utile lorsque vous devez utiliser case pour vérifier si un service est chargé dans le périphérique macOS, et vous permet également de vérifier s'il est en cours d'exécution ou non. La condition de service macOS peut vérifier deux types de service différents : démons et agents.

Un démon est un programme qui s'exécute en arrière-plan dans le cadre du système global (c'est-à-dire qu'il n'est pas lié à un utilisateur particulier). Un démon ne peut pas afficher d'interface utilisateur graphique ; plus précisément, il n'est pas autorisé à se connecter au serveur windows. Un serveur Web est l'exemple parfait d'un démon.

Un agent est un processus qui s'exécute en arrière-plan pour le compte d'un utilisateur particulier. Les agents sont utiles car ils peuvent effectuer des opérations que les démons ne peuvent pas effectuer, comme accéder de manière fiable au répertoire de base de l'utilisateur ou se connecter au serveur Windows. Un programme de surveillance de calendrier est un bon exemple d'agent.

Dans le schéma ci-dessous, vous pouvez voir comment chaque périphérique est chargé en fonction du démarrage du périphérique et de la connexion de l'utilisateur :



Vous trouverez plus d'informations sur les démons et les agents ici dans la documentation Apple

Les démons et les agents disponibles sur votre périphérique macOS se trouvent aux emplacements suivants :

Emplacement	Description
~/Library/LaunchAgents	Agents par utilisateur fournis par l'utilisateur.
/Library/LaunchAgents	Agents par utilisateur fournis par l'administrateur.
/Library/LaunchDaemons	Démons système fournis par l'administrateur.

/System/Library/LaunchAgents	Agents OS X par utilisateur
/System/Library/LaunchDaemons	Démons système OS X

Vous pouvez vérifier la liste de chaque catégorie à partir de macOS terminal en utilisant ces commandes :

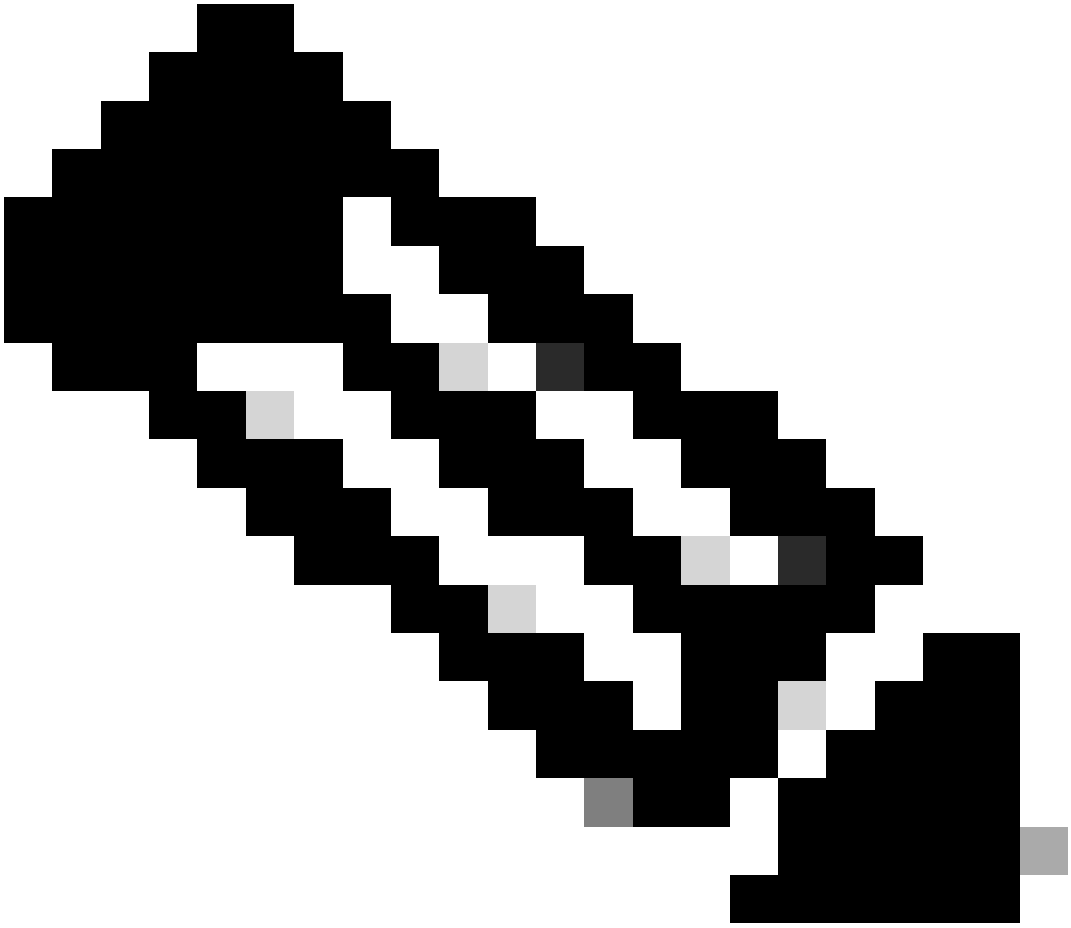
ls -ltr ~/Library/LaunchAgents
ls -ltr /Library/LaunchAgents
ls -ltr /Library/LaunchDaemons
ls -ltr /System/Library/LaunchAgents
ls -ltr /System/Library/LaunchDaemons

Les emplacements précédents peuvent vous montrer tous les démons et agents disponibles sur le périphérique macOS, mais ils ne sont pas tous chargés ou en cours d'exécution.

Configurer

La configuration de la condition de service macOS peut être effectuée en procédant comme suit :

1. Identifiez le nom du service à vérifier.
2. (Facultatif) Vérifiez les détails du service pour déterminer s'il s'agit d'un agent ou d'un démon.
3. Sélectionnez l'opérateur de service à évaluer.
4. Configurez la condition requise et la stratégie de posture pour une telle condition.



Remarque : L'état de la position du service nécessite des privilèges élevés pour fonctionner. Il est donc INDISPENSABLE qu'ISE PSN soit approuvé par Cisco Secure Client (anciennement AnyConnect) - Guide de référence

Identifier le nom de service à vérifier

Le module de conformité de posture ISE est capable de vérifier les services chargés, en cours d'exécution et chargés, et en cours d'exécution avec le code de sortie.

Pour vérifier les services qui sont chargés, utilisez la commande sudo launchctl dumpstate.

Pour vérifier les services qui sont chargés et ont un code de sortie, utilisez la commande sudo launchctl list.

Les commandes précédentes peuvent soudainement afficher beaucoup d'informations. Utilisez plutôt ces commandes pour afficher uniquement le nom de service réel :

Pour vérifier uniquement les noms de service chargés, utilisez cette commande :

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||'

Pour vérifier uniquement les noms de service chargés et dotés d'un code de sortie, utilisez cette commande :

sudo launchctl list | awk '{if (NR>1) print $3}'

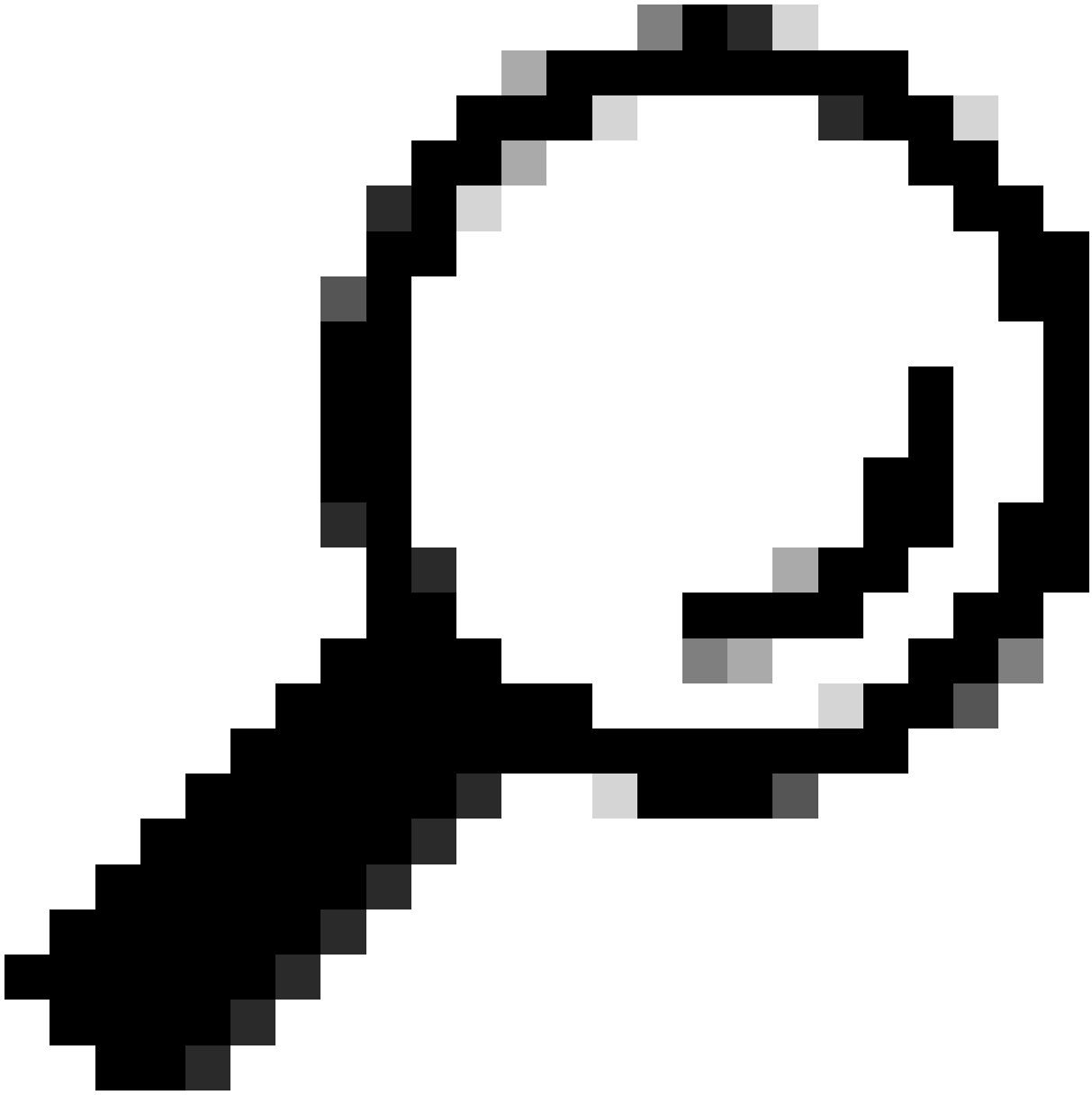
Ces commandes montrent beaucoup d'informations, donc à la fin de chaque commande, il est recommandé d'utiliser un autre filtre grep pour trouver le service que vous recherchez.
Par exemple, si vous recherchez un service spécifique à un fournisseur, vous pouvez utiliser un mot clé comme filtre à l'et à l'.

Dans le cas des services Cisco, les commandes sont les suivantes :

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||' | grep -i cisco
sudo launchctl list | awk '{if (NR>1) print $3}' | grep -i cisco

(Facultatif) Vérifiez les détails du service à définir si son agent ou un démon

Dans la deuxième partie de la configuration de cette condition, vous devez vérifier si votre service est de type démon ou d'agent.



Conseil : Cette étape est facultative, car ISE vous permet de sélectionner l'option pour Daemon Or User Agent, de sorte que vous pouvez simplement sélectionner cette option et sauter cette partie.

Dans le cas où vous voulez être granulaire dans cette condition, vous pouvez vérifier le type en faisant ceci :

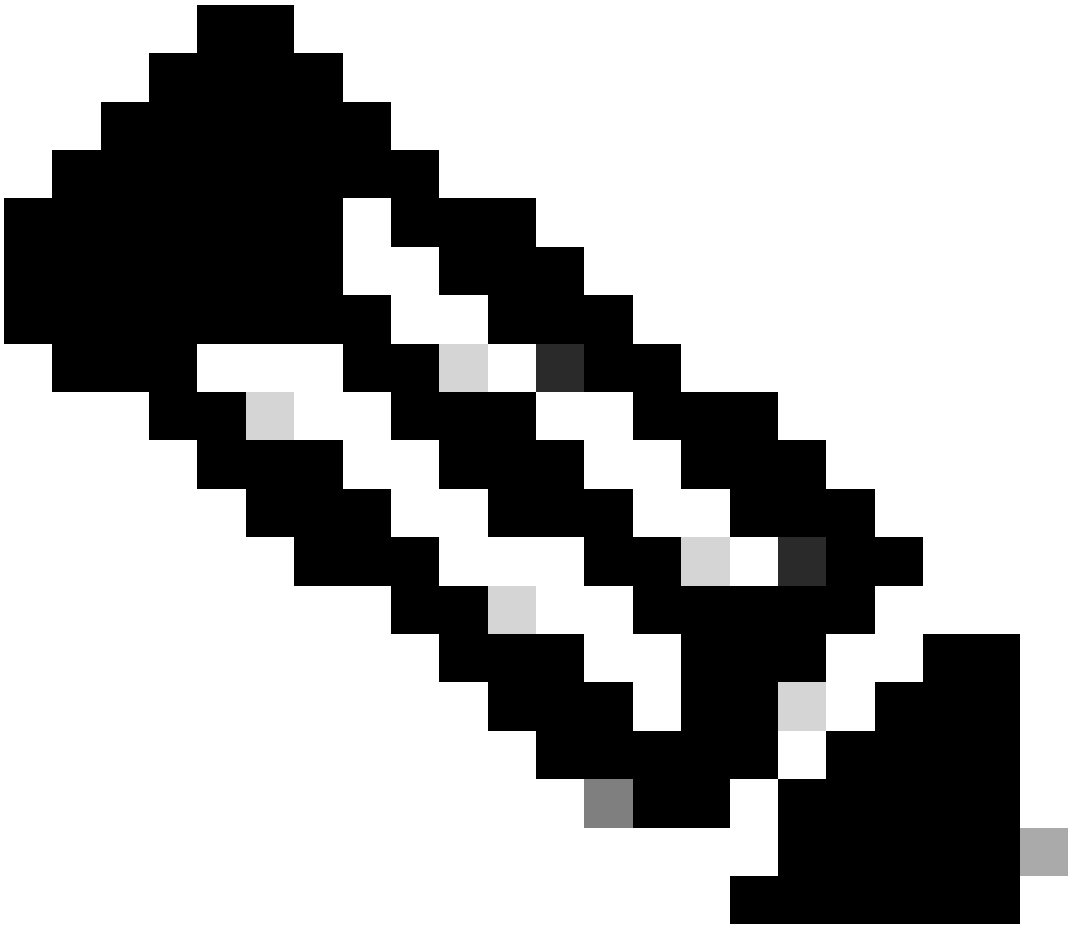
1. Tout d'abord, vérifiez le nom launchctl complet du service avec la commande sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||' | grep -i {Votre nom de service}

Par exemple, pour la commande sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's/.\{3\}$//' | grep -i com.cisco.secureclient.iseposture, le résultat est : gui/501/com.cisco.secureclient.iseposture.

2. Vérifiez le type de service à l'aide de la commande sudo launchctl print { Your launchctl service name } | grep -i 'type = Launch'

En suivant l'exemple, pour la commande : sudo launchctl print gui/501/com.cisco.secureclient.iseposture | grep -i 'type = Launch', le résultat est : type = LaunchAgent.

Cela signifie que le type de service est Agent, sinon il afficherait type = LaunchDaemon.



> Remarque : Si les informations sont vides, sélectionnez l'option Daemon Or User Agent dans ISE pour le paramètre de type de service.

Sélectionnez l'opérateur de service à évaluer

ISE vous permet de sélectionner 5 opérateurs de service différents :

- Chargé
- Non chargé
- Chargé et en cours
- Chargé avec le code de sortie
- Chargé et en cours d'exécution ou avec code de sortie

Services chargés

Tous les services répertoriés lors de l'utilisation de ces deux commandes sont-ils :

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||'
sudo launchctl list | awk '{if (NR>1) print $3}'

Services non chargés

Tous les services dont la liste de propriétés (plist) est définie, mais qui n'ont pas été chargés, ou les services dont la liste de propriétés (plist) n'est même pas définie, ne peuvent donc pas être chargés du tout.

Ces services ne sont pas faciles à identifier, et il est le plus courant pour l'exemple d'utilisation lorsque vous voulez vérifier qu'un service spécifique ne devrait pas exister dans le périphérique macOS.
Par exemple, si vous voulez empêcher le service de zoom d'être chargé sur le périphérique macOS, vous pouvez mettre ici us.zoom.ZoomDaemon comme la valeur pour le service, de cette façon vous vous assurez que le zoom n'est pas en cours d'exécution ou pas installé du tout.

Certains services ne peuvent pas être désinstallés et sa liste de propriétés est définie.
Par exemple, avec cette commande, vous pouvez voir que dhcp6d plist est défini :

ls -ltr /System/Library/LaunchDaemons | grep.com.apple.dhcp6d.plist

En vérifiant la liste des services, vous pouvez voir que n'est pas chargé :

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||' | grep -i.com.apple.dhcp6d
sudo launchctl list | awk '{if (NR>1) print $3}' | grep -i.com.apple.dhcp6d

Si vous définissez la valeur sur com.apple.dhcp6d", le périphérique macOS est conforme, car même si la liste de services est définie, le service n'est pas chargé.

Chargé et en cours

Tous les services ne sont pas en cours d'exécution. Il existe plusieurs états pour chaque service,

par exemple : en cours d'exécution, non en cours d'exécution, en attente, terminé, non initialisé, etc.
Pour vérifier tous les services en cours d'exécution, utilisez cette commande :

sudo grep -B 10 -A 10 -E "^\s*state = running" <<$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||'

Les services répertoriés avec la commande ci-dessus ont atteint la condition d'opérateur de service Loaded & Running.

Chargé avec le code de sortie

Certains services peuvent se terminer par un code de sortie attendu ou inattendu. Ces services peuvent être répertoriés à l'aide de la commande :

sudo grep -B 10 -A 10 "état = e" <<<$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's/.\{3\}$//'

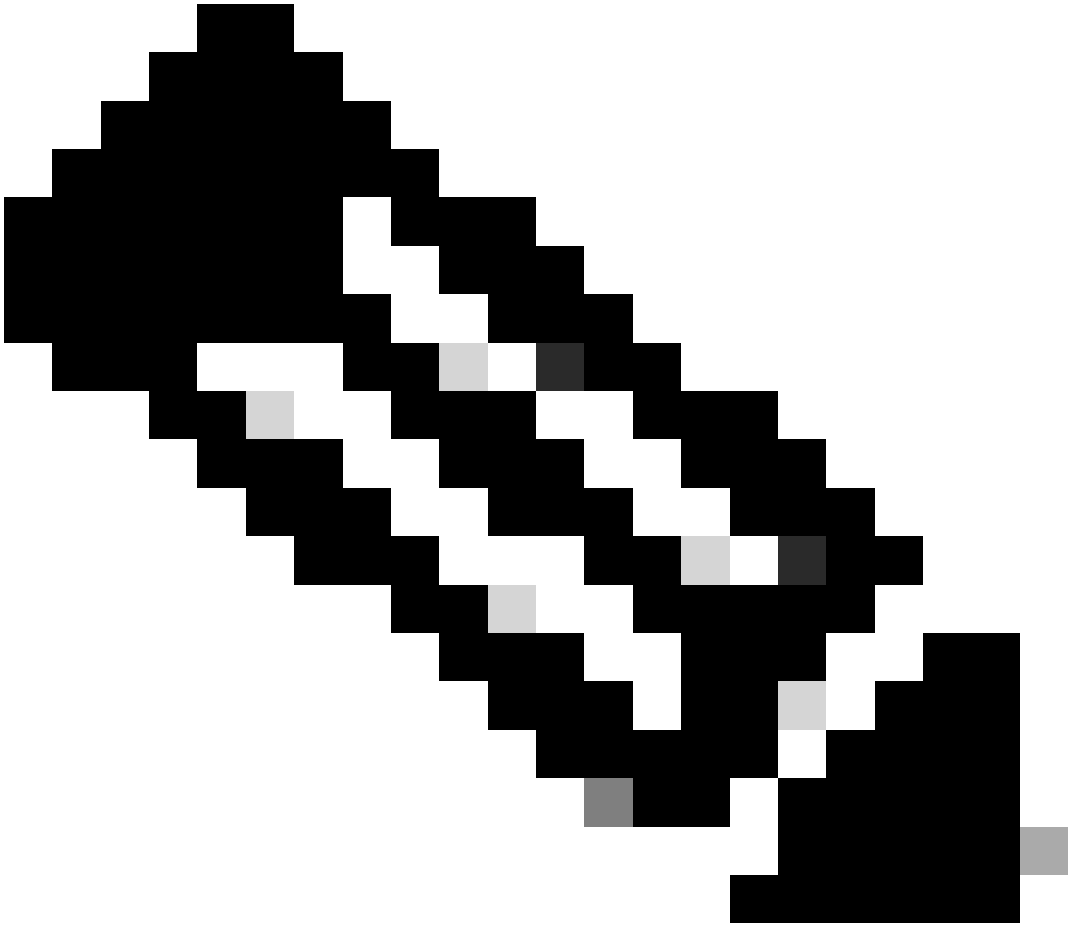
Pour connaître son code de sortie, vous pouvez sélectionner n'importe quel service et utiliser la commande suivante :

sudo launchctl print { Votre nom de service launchctl } | grep -i 'dernier code de sortie'

Exemple :

sudo launchctl print gui/501/com.apple.mdmclient.agent | grep -i 'dernier code de sortie'

dont le résultat est : last exit code = 0

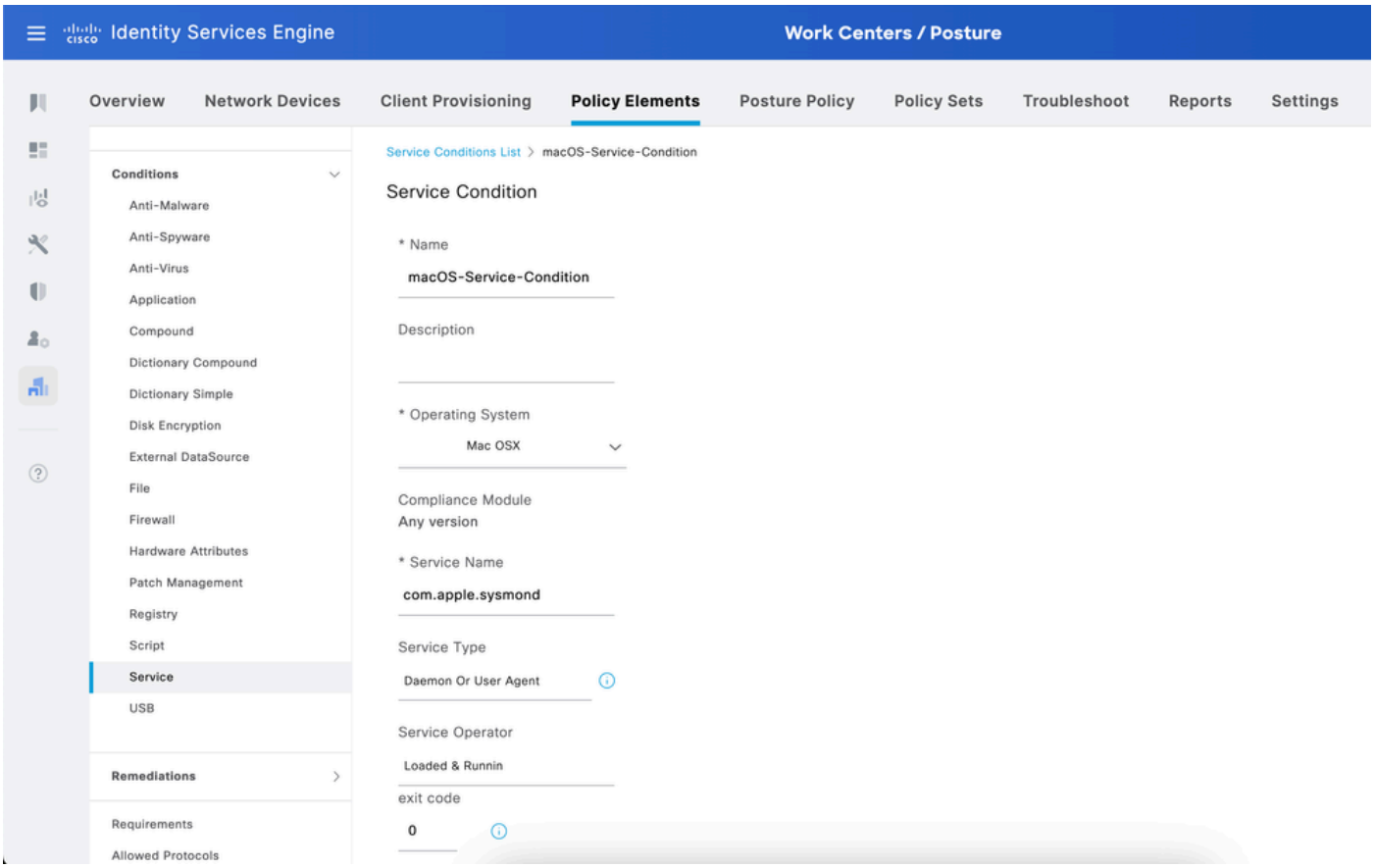


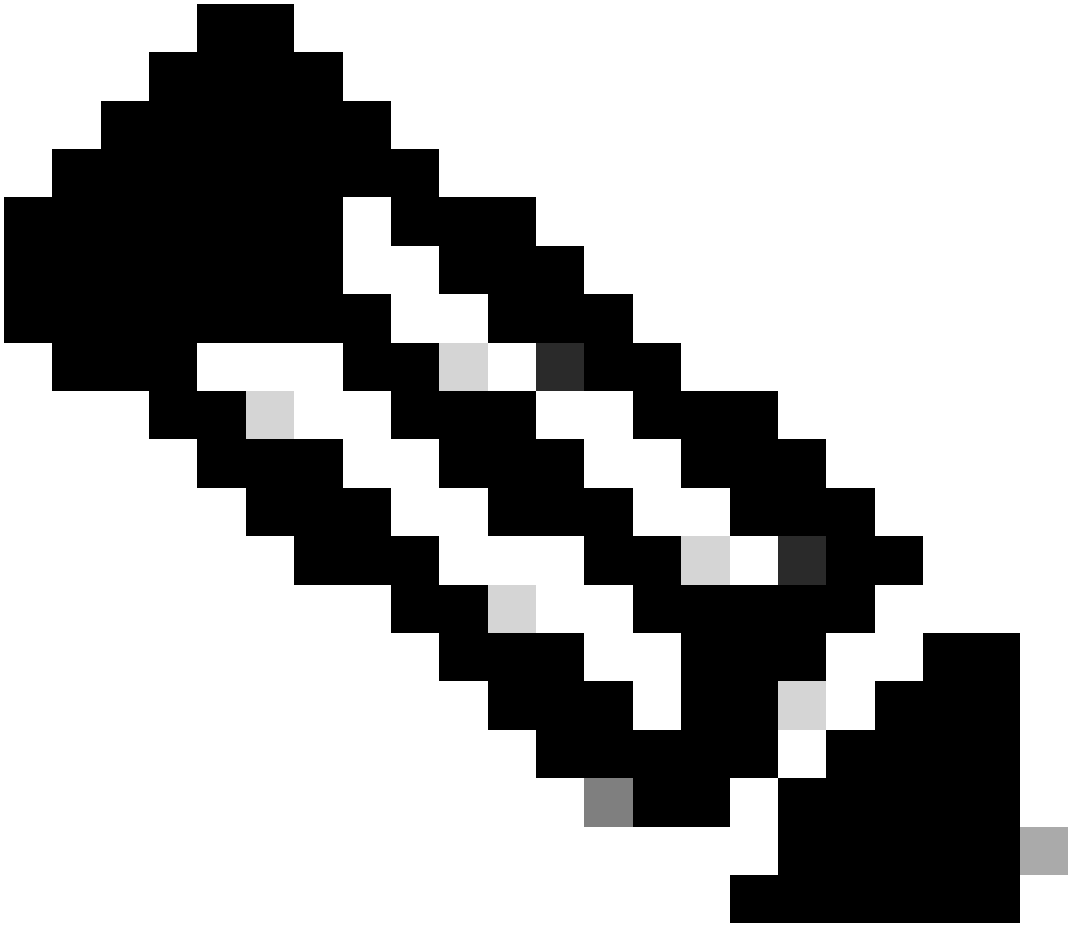
> Remarque : Ici, le code de sortie 0 signifie généralement que tout a été fait correctement par le service. Si un ordinateur ne correspond pas au 0 comme code de sortie, cela signifie que le service n'a pas effectué l'action attendue.

Chargé et en cours d'exécution ou avec code de sortie

Cette dernière option fonctionne lorsque le service est Loaded & Running ou Loaded with exit code.

Cette image présente un exemple de condition de service macOS.

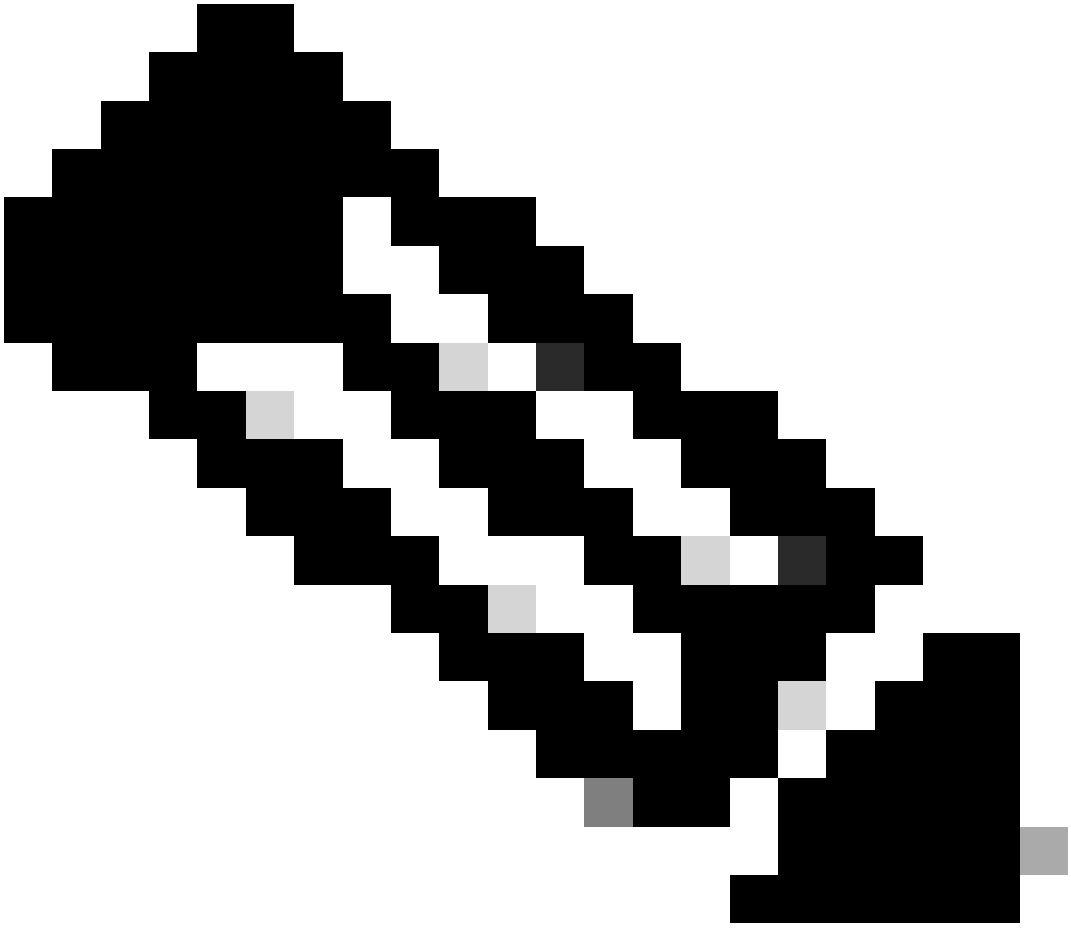

Identity Services Engine
Work Centers / Posture
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall
Hardware Attributes
Patch Management
Registry
Script
Service
USB
Remediations
Requirements
Allowed Protocols
Service Conditions List > macOS-Service-Condition
Service Condition
* Name
macOS-Service-Condition
Description
* Operating System
Mac OSX
Compliance Module
Any version
* Service Name
com.apple.sysmond
Service Type
Daemon Or User Agent
Service Operator
Loaded & Runnin
exit code
0



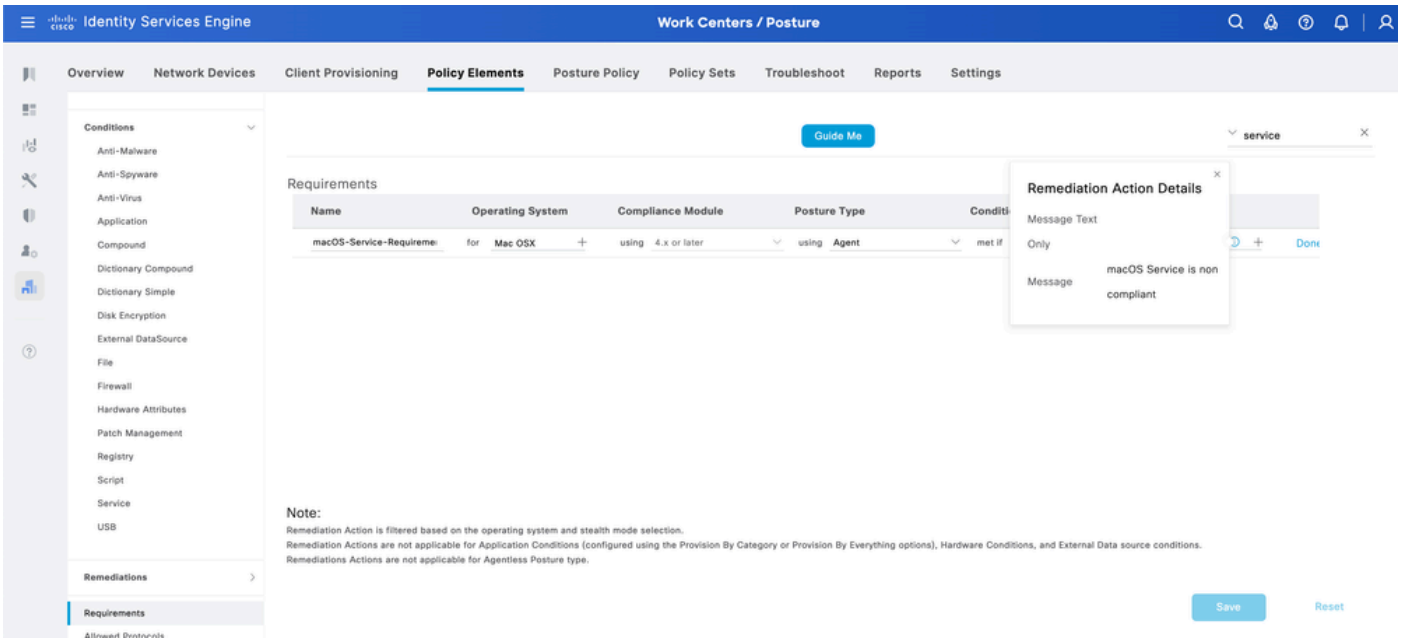
Remarque : Actuellement, seul le nom exact du service est pris en charge. Il y a une demande d'amélioration pour prendre en charge le caractère générique dans les noms de service, ID de bogue Cisco CSCwf01373

Configurer la condition requise et la politique de posture pour une telle condition

Une fois la condition configurée, vous devez créer une condition pour cette condition, utilisez l'option Test de message uniquement pour cette condition.
Accédez à ISE > Work Centers > Posture > Requirements pour le créer.

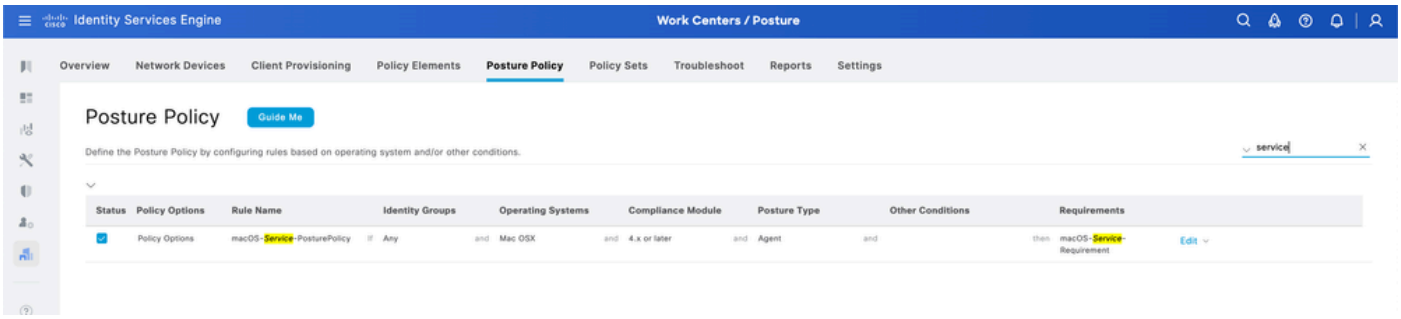


Remarque : Il n'existe aucune option de correction pour les conditions de service.



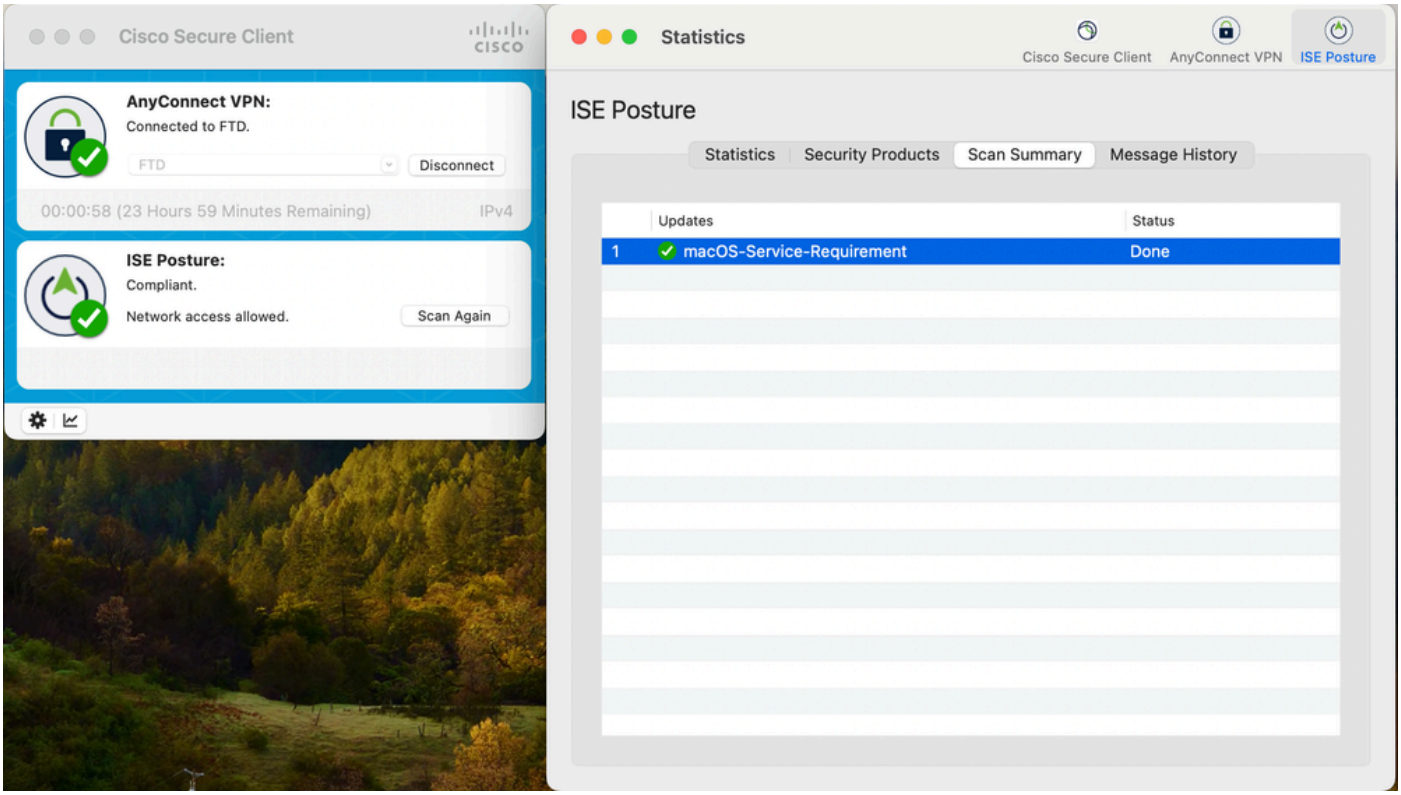
Une fois cela fait, la dernière étape consiste à configurer la politique de posture qui utilise la condition créée.
Accédez à ISE > Work Centers > Posture > Posture Policy pour créer la stratégie.

Activez la nouvelle stratégie, nommez-la comme vous le souhaitez et sélectionnez le besoin que vous venez de créer.

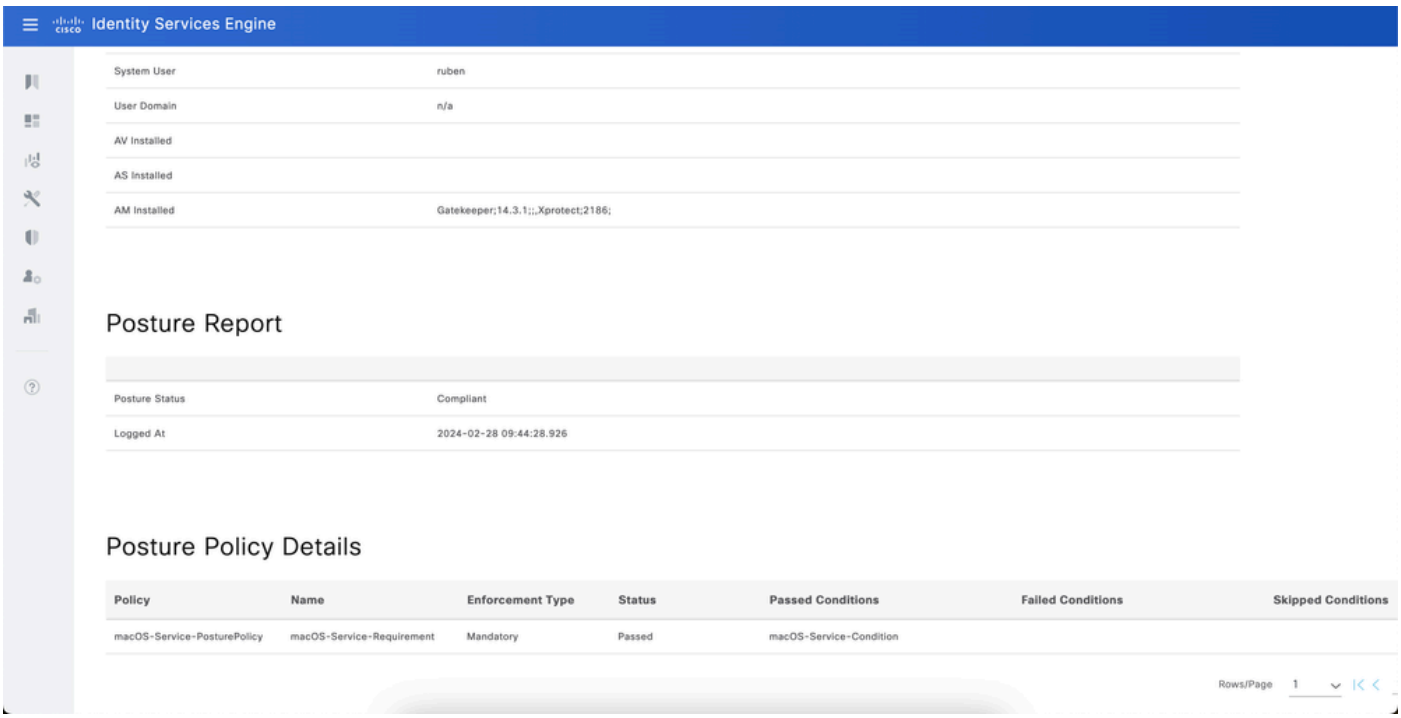


Vérifier

Vous pouvez vérifier que la condition de posture macOS a réussi ou échoué, à partir de l'interface utilisateur graphique du client sécurisé Cisco elle-même.



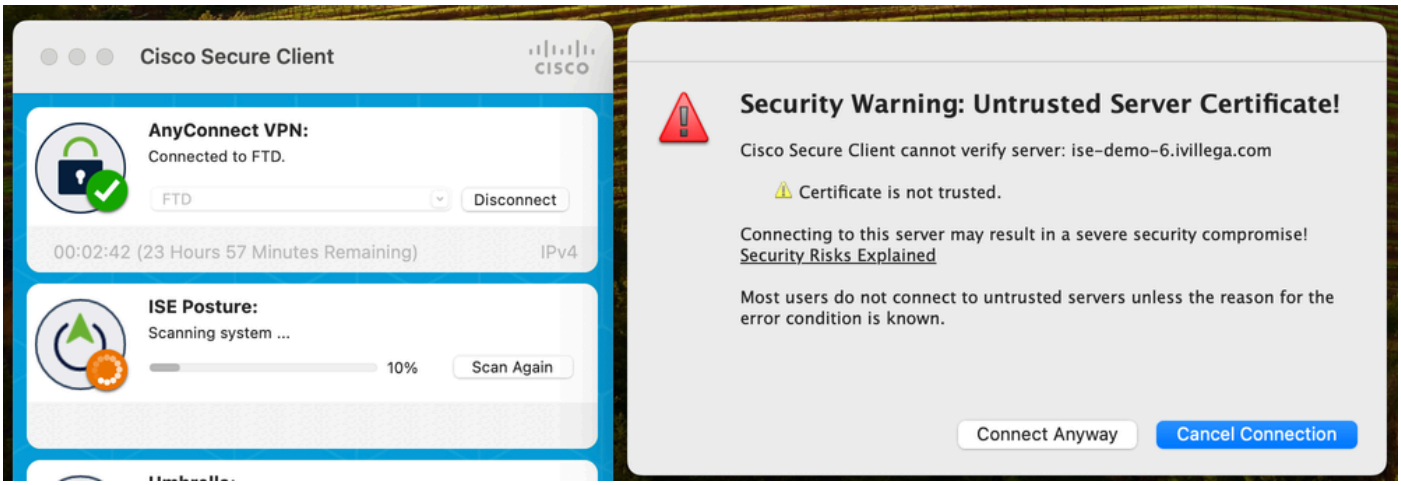
Vous pouvez également vérifier le rapport de position ISE à partir de ISE > Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint.



Dépannage

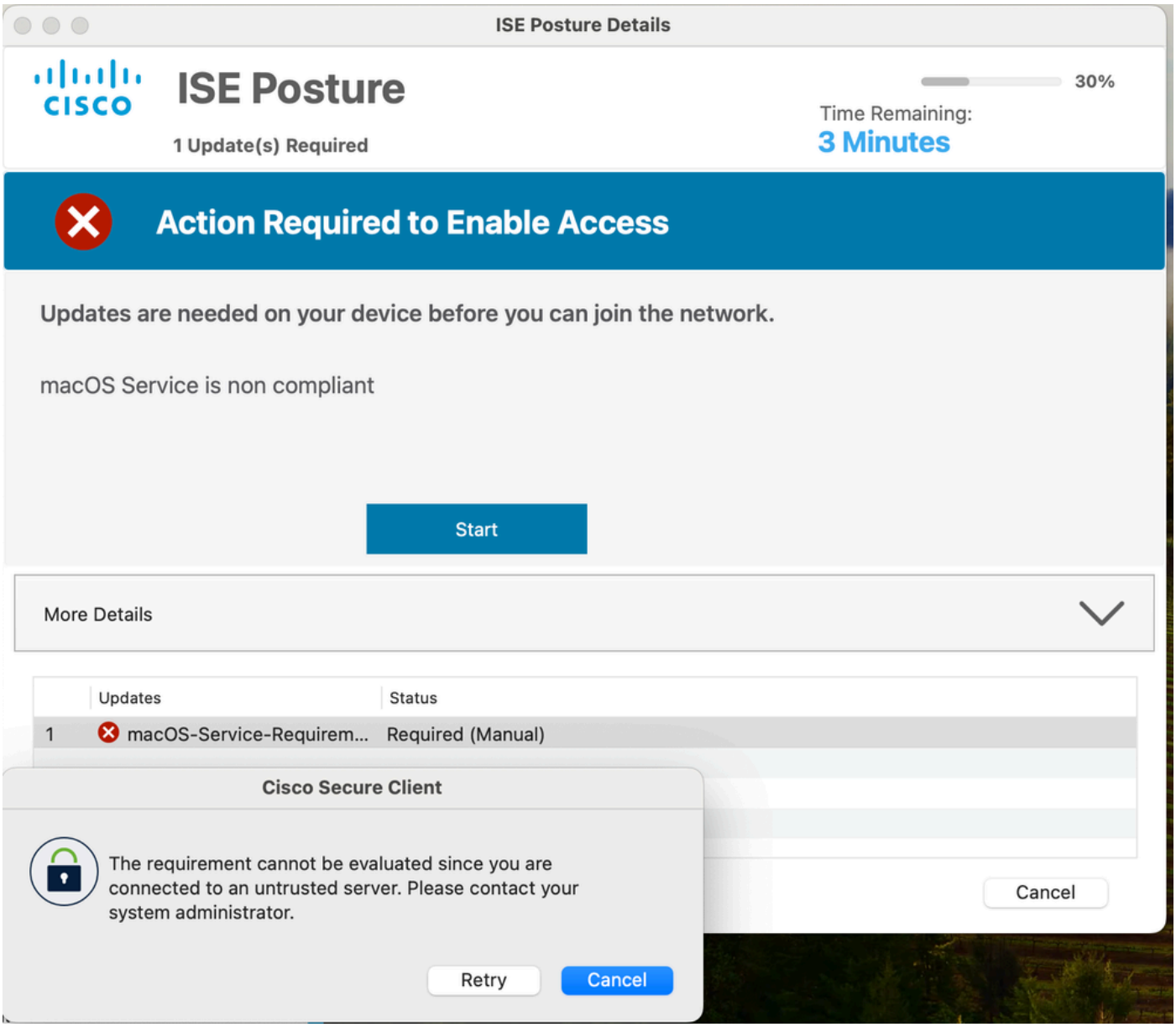
Les problèmes courants que vous pouvez rencontrer lors de la configuration de cette condition de position de service macOS sont les suivants :

Certificat non approuvé



Comme indiqué précédemment, la condition de service nécessite des autorisations élevées. Il est impératif que le certificat pour le processus d'analyse de position soit approuvé par le serveur.

Sinon, vous rencontrez cette erreur :

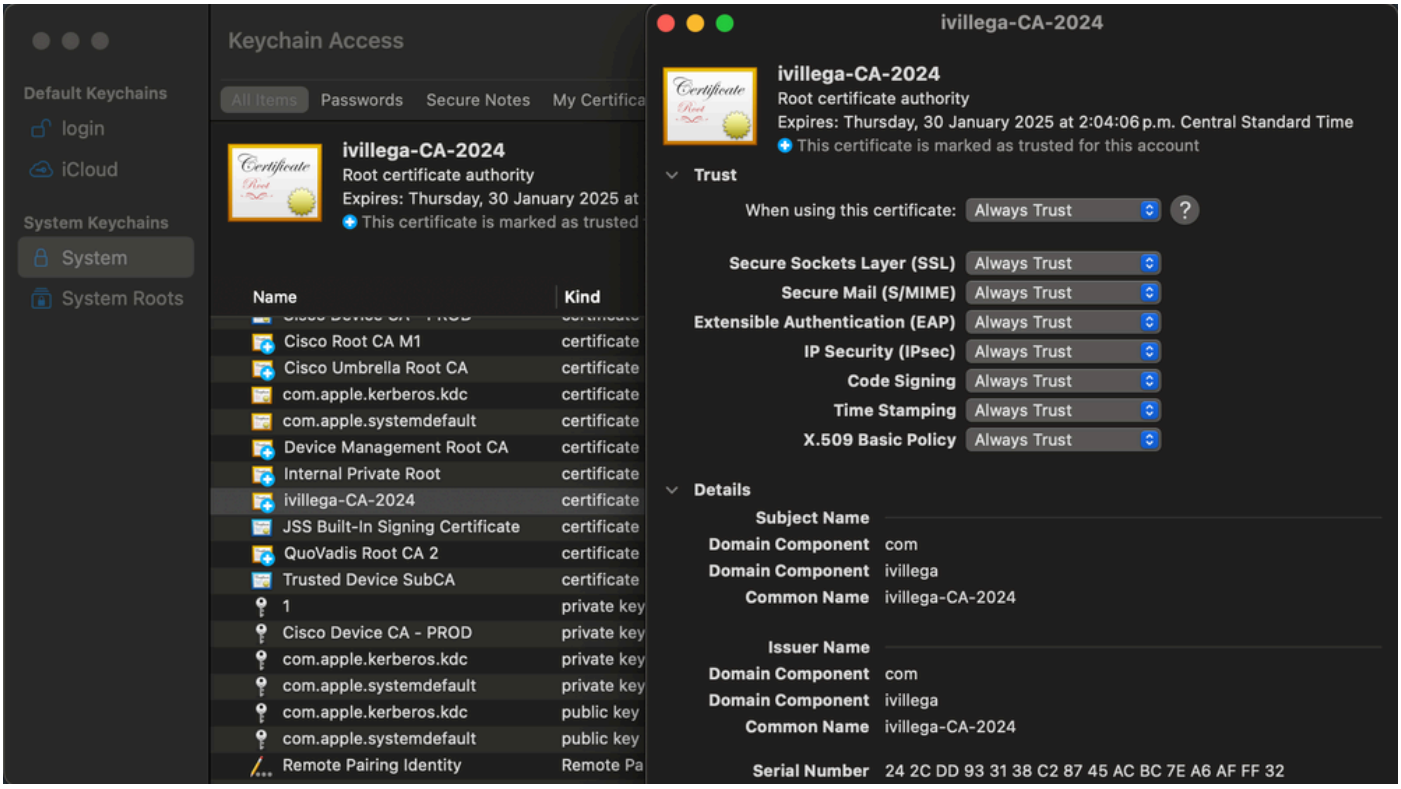


Le module de posture ISE détecte les serveurs PSN par adresse IP ou par nom de domaine complet (FQDN). La meilleure pratique consiste à disposer des fichiers de configuration de la position pour détecter les noeuds ISE via le FQDN, de sorte que les certificats Admin et Portal (Client Provisioning Portal) doivent inclure le FQDN dans le champ CN ou SAN. Vous pouvez également utiliser un certificat générique pour ce flux. Les certificats génériques sont pris en charge pour ce flux.

En raison des garanties du système, le champ CN ne peut plus être fiable à l'avenir. Il est recommandé d'inclure l'entrée générique ou le nom de domaine complet dans le champ SAN.

Dans le cas où les PSN ISE sont découverts via une adresse IP au lieu d'un nom de domaine complet, il est nécessaire que l'adresse IP des noeuds soit incluse dans le champ CN ou le champ SAN du ou des certificats liés à l'utilisation Admin et Portal.

Les modules de posture ISE font confiance au certificat présenté par le serveur ISE. Si son autorité de certification se trouve dans le magasin de certificats système de l'accès macOS Keychain, cette autorité de certification doit avoir le paramètre Lors de l'utilisation de ce certificat défini sur Toujours faire confiance.



Vous pouvez rencontrer le comportement incorrect que même lorsque le certificat est chargé correctement et que toutes les exigences CN et SAN sont satisfaites, le système macOS ne fait toujours pas confiance au certificat. Dans de tels cas, ouvrez l'application d'accès à la chaîne de clés, naviguez vers l'onglet Magasin de certificats système, et supprimez le certificat CA de là.

Accédez ensuite à l'application macOS Terminal et exécutez cette commande : sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain

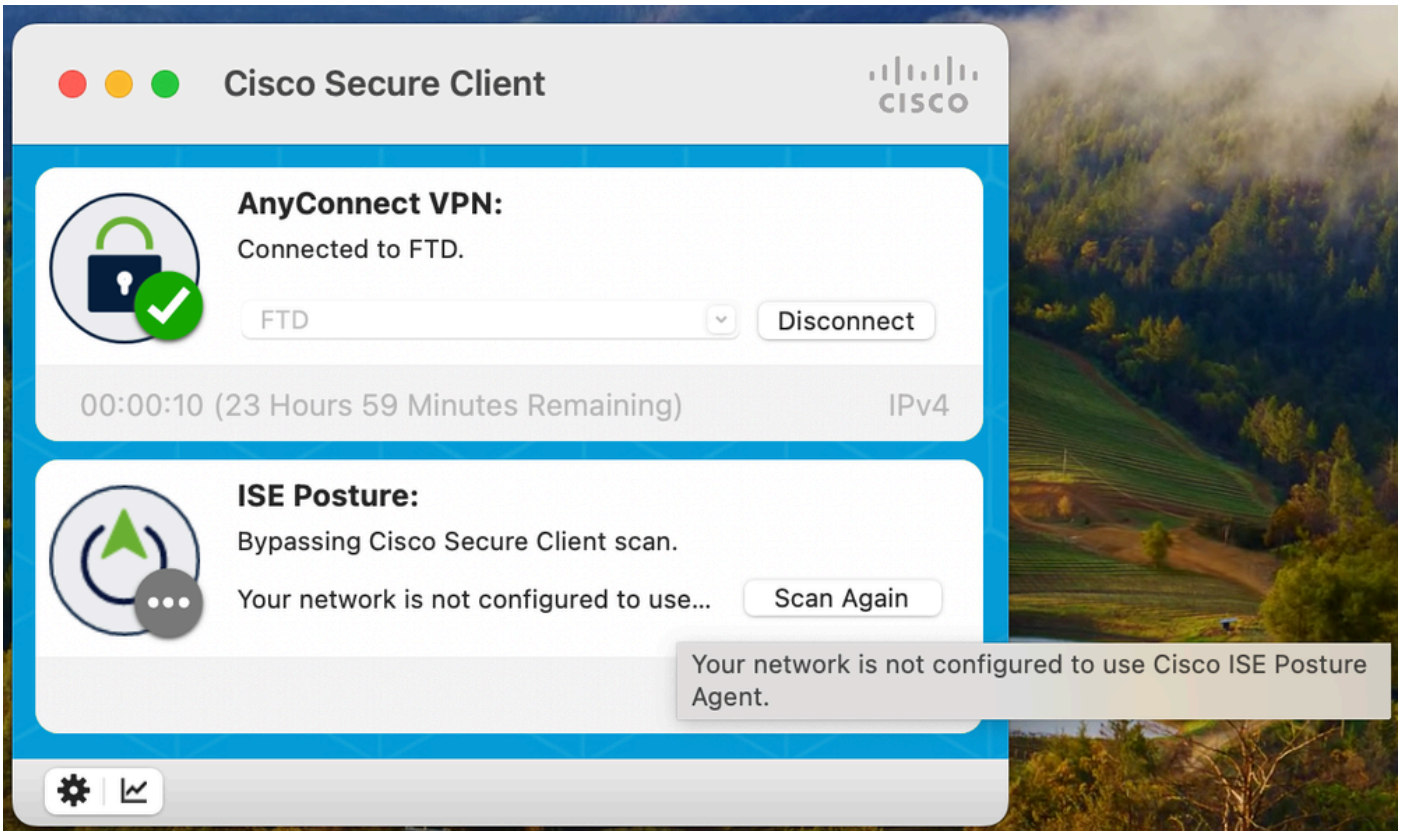
{Chemin d'accès à votre certificat CA}

Par exemple, si votre certificat est dans votre bureau, la commande est la suivante : sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt

Après avoir exécuté la commande, redémarrez l'ordinateur et réessayez.

Contournement de Cisco Secure Client Scan

Vous pouvez également rencontrer les messages d'erreur « Bypass Cisco Secure Client Scan » et « Your network is not configured to use Cisco ISE Posture Agent » :



Ce message s'affiche car aucun profil n'est configuré dans le provisionnement client dans ISE > Work Centers > Posture > Client Provisioning > Client Provisioning Policies.
Même si vous pouvez voir une condition pour les systèmes d'exploitation Mac OSX, cela ne signifie pas que vous couvrez toutes les versions de macOS.

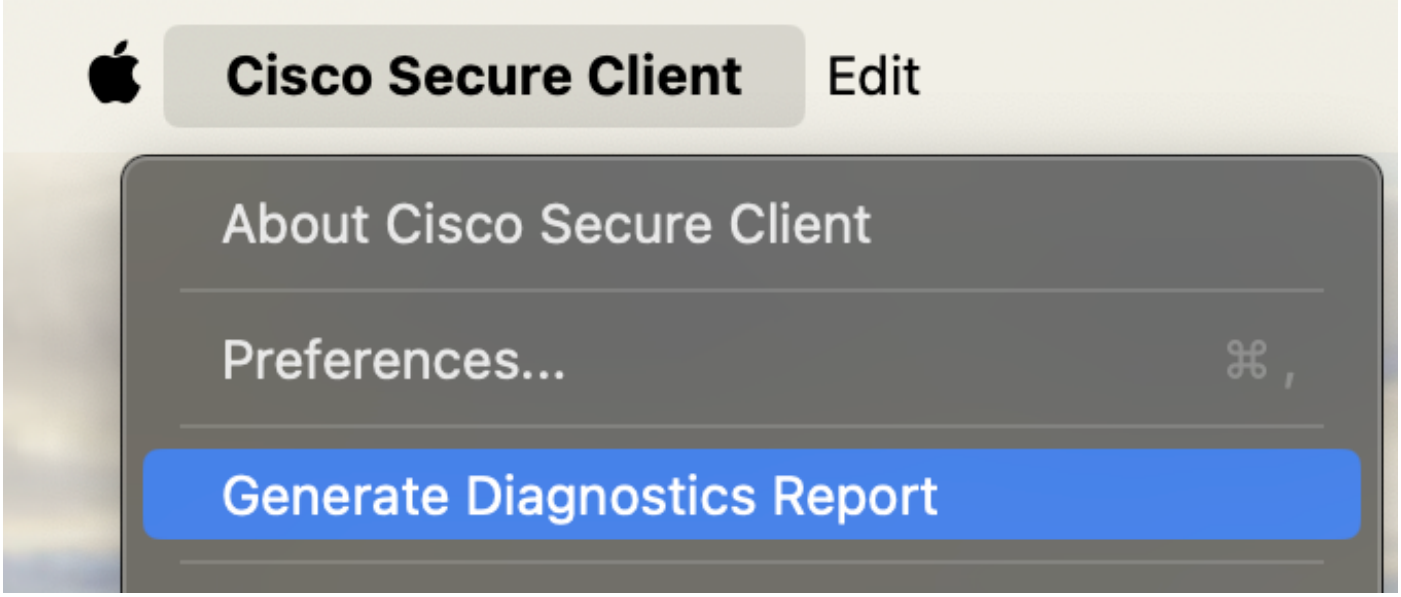
Par défaut, ISE n'inclut pas les dernières versions de macOS, telles que Sequoia (15.6.x), pour éviter ce message, assurez-vous que la posture est mise à jour.

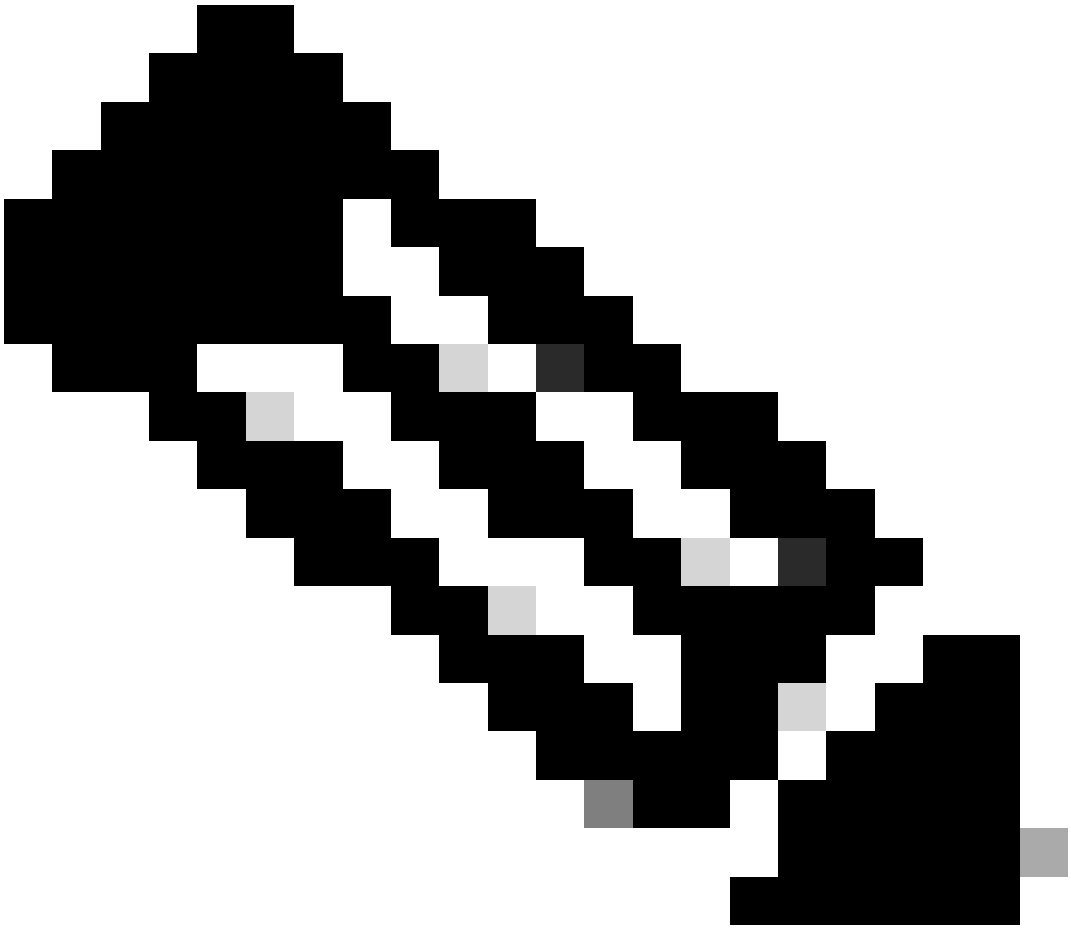
Vous devez mettre à jour le flux Posture à partir de ISE > Work Centers > Posture > Settings > Software Updates > Posture Updates.

Il peut être mis à jour en ligne directement à partir d'ISE ou hors ligne via un fichier zip téléchargeable ici à partir du site Posture Offline

Autres questions

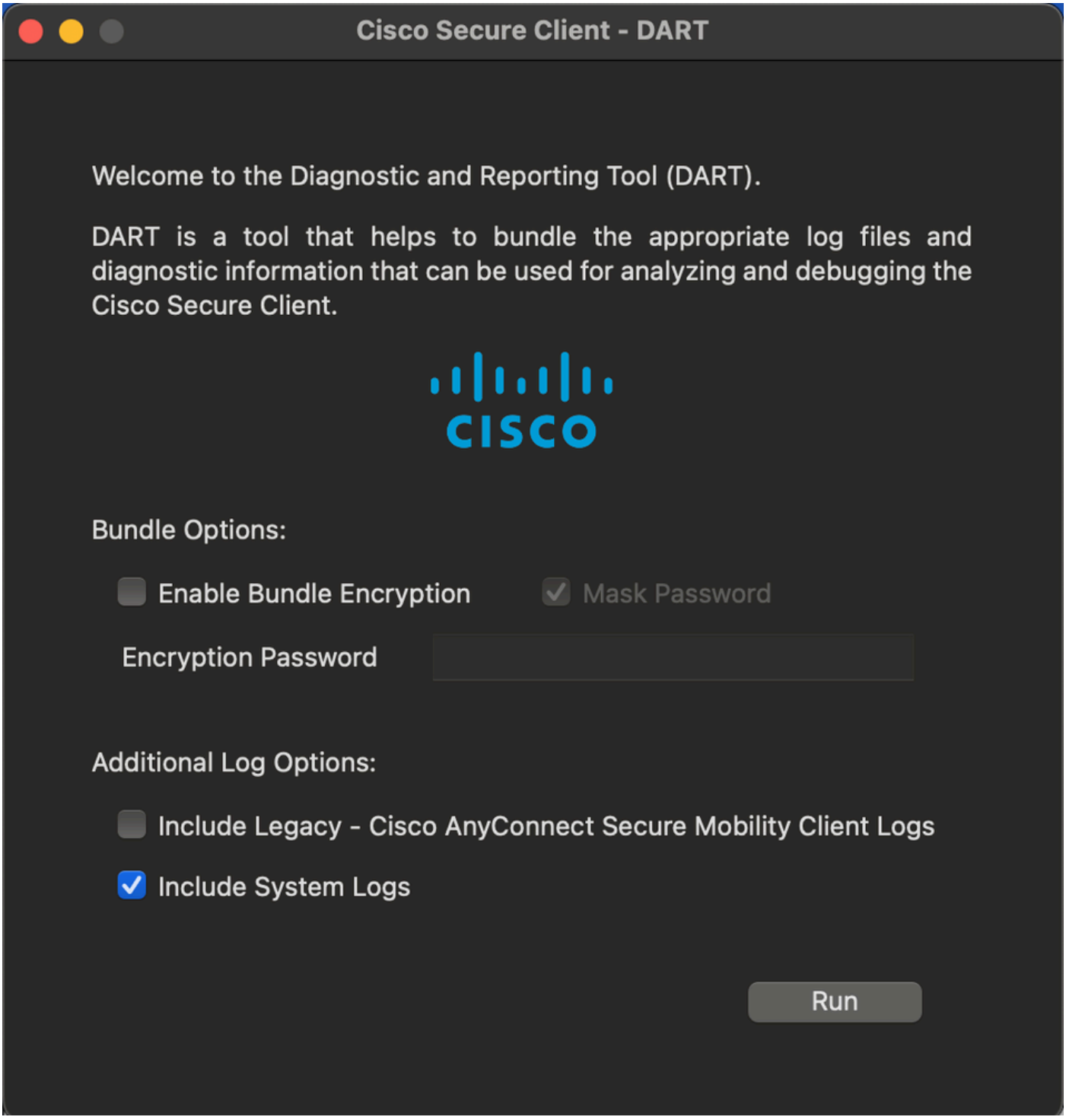
Si vous voulez aller dans les détails, vous pouvez recueillir un bundle DART à partir du périphérique macOS posté. Pour cela, vous devez avoir le module DART installé, puis, avec l'application Cisco Secure Client active naviguez vers la barre de menu et cliquez sur Cisco Secure Client, puis, dans Générer des rapports de diagnostic.



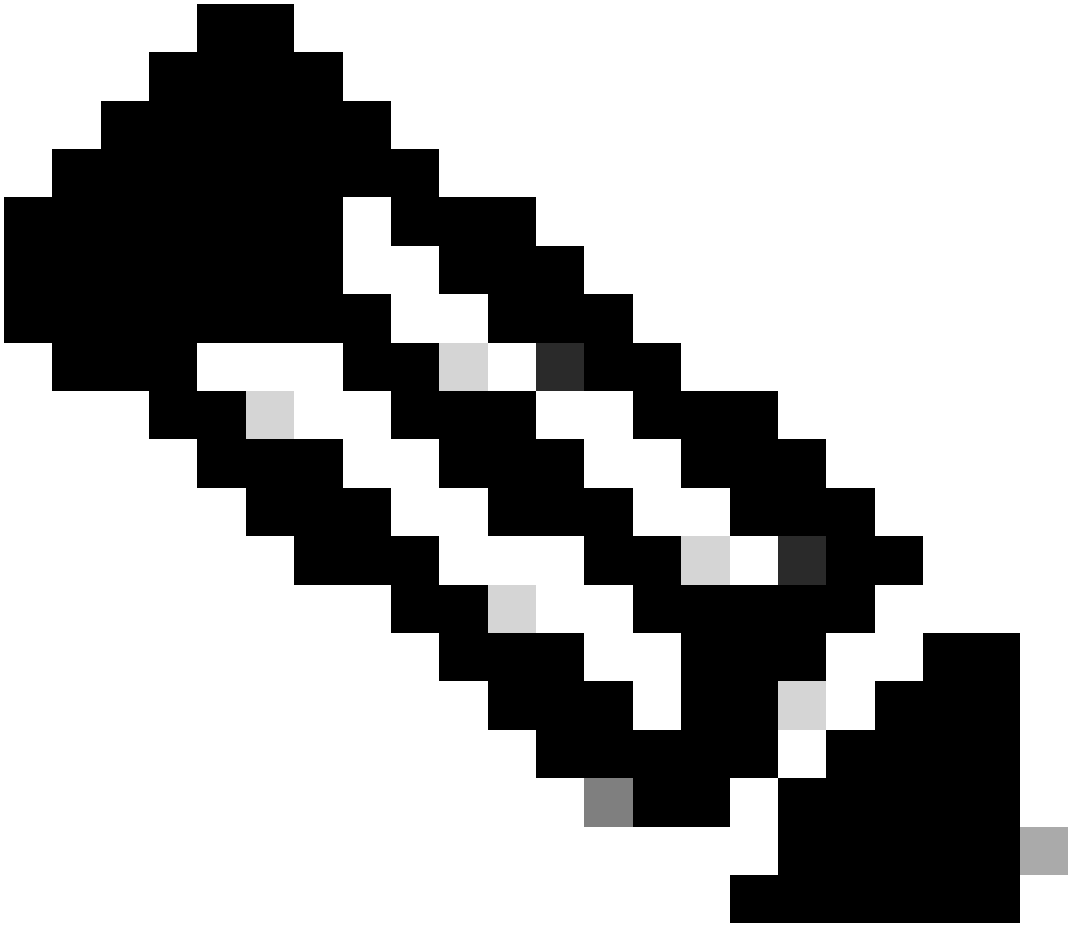


Remarque : Il est important d'activer l'option Include System Logs lors de la génération du

bundle DART, sinon le bundle DART n'inclura pas les informations du module de posture ISE.



Pour des raisons de sécurité, certains journaux peuvent être chiffrés et non visibles, mais dans le fichier unified_log.log du bundle DART, vous pouvez voir des journaux similaires, comme indiqué :



Remarque : Cet exemple de journal concerne la condition de service macOS configurée dans ce document.

```
[Tue Feb 27 10:30:58.576 2024][csc_iseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 File
```

```
macOS-Service-Condition
```

```
3
```

303

com.apple.sysmond

running

0

)
[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: processPostureData Thread Id: 0x4A9FD7C0 File: Au

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: SMP_initCheck Thread Id: 0x4A9FD7C0 File: SMNavPo

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

",isElevationAllowed:1,nRemediationTimeLeft:0}
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 Fi

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

)
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: Rqmt.cpp
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: CheckSvc.
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: completeCheck Thread Id: 0x4A9FD7C0 File: Rqm

En outre, vous pouvez définir le composant posture au niveau du journal de débogage dans le noeud PSN ISE qui authentifie et positionne le point de terminaison.

Vous pouvez configurer ce niveau de journal à partir de ISE > Operations > Troubleshoot > Debug Wizard > Debug Log Configuration. Cliquez sur le nom d'hôte PSN et changez le niveau de journal du composant Posture de INFO à DEBUG.

En utilisant le même exemple pour la condition de service macOS, vous pouvez voir des journaux similaires dans ise-psc.log :

2024-02-27 10:30:58.658 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.runtime.Pos

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

2024-02-27 10:30:58.659 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.util.Status

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

]

```
2024-02-27 10:31:06.044 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-8][[]] cisco.cpm.posture.util.AgentU
```

Si les problèmes persistent, soumettez un ticket TAC à l'équipe Cisco.

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.