Comprensione e configurazione della condizione di postura ISE del servizio macOS

Sommario

Introduzione

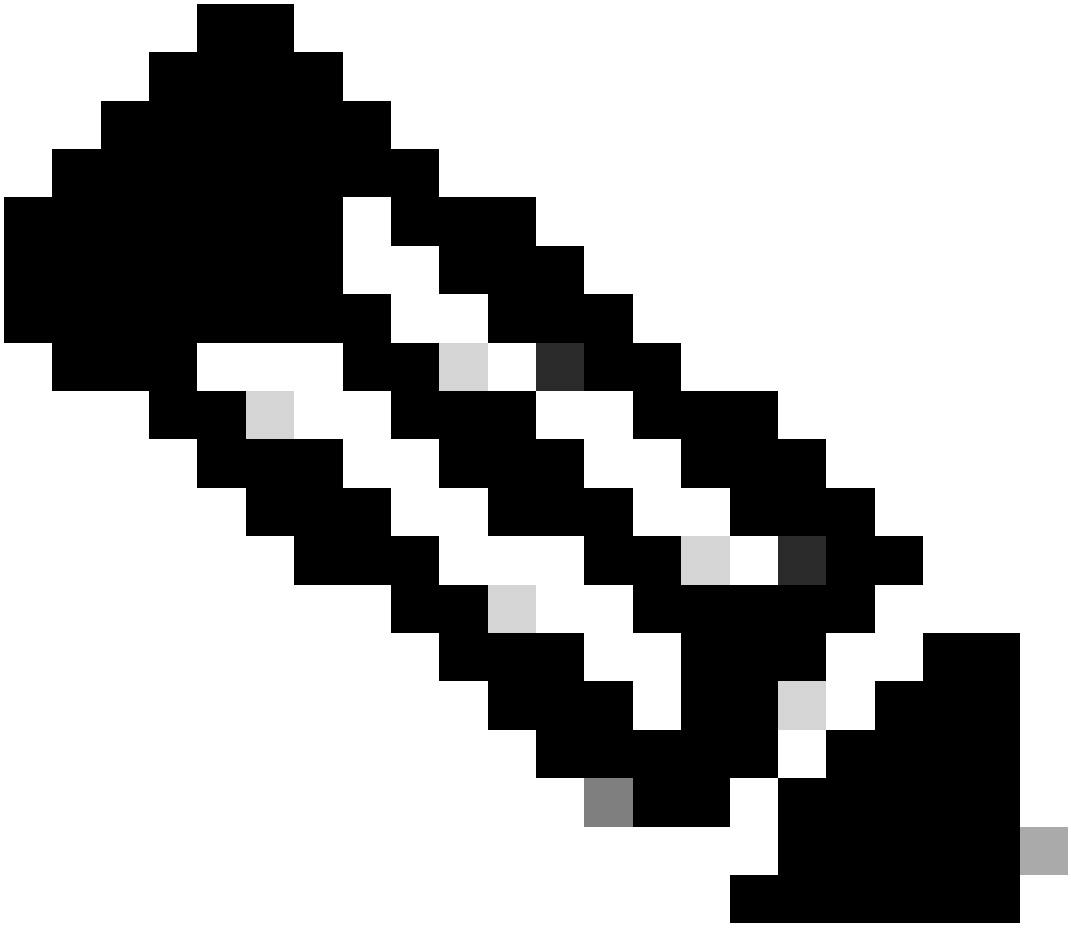
Questo documento descrive il processo di configurazione della condizione del servizio macOS in Cisco ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di macOS.
- Conoscenza del flusso ISE Posture.



Nota: Questo documento descrive la configurazione per la condizione del servizio macOS. La configurazione iniziale della postura non è illustrata in questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE 3.3 patch 1
- dispositivo macoOS con Sonoma 14.3.1
- Cisco Secure Client 5.1.2.42
- Modulo di conformità versione 4.3.3432.6400

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

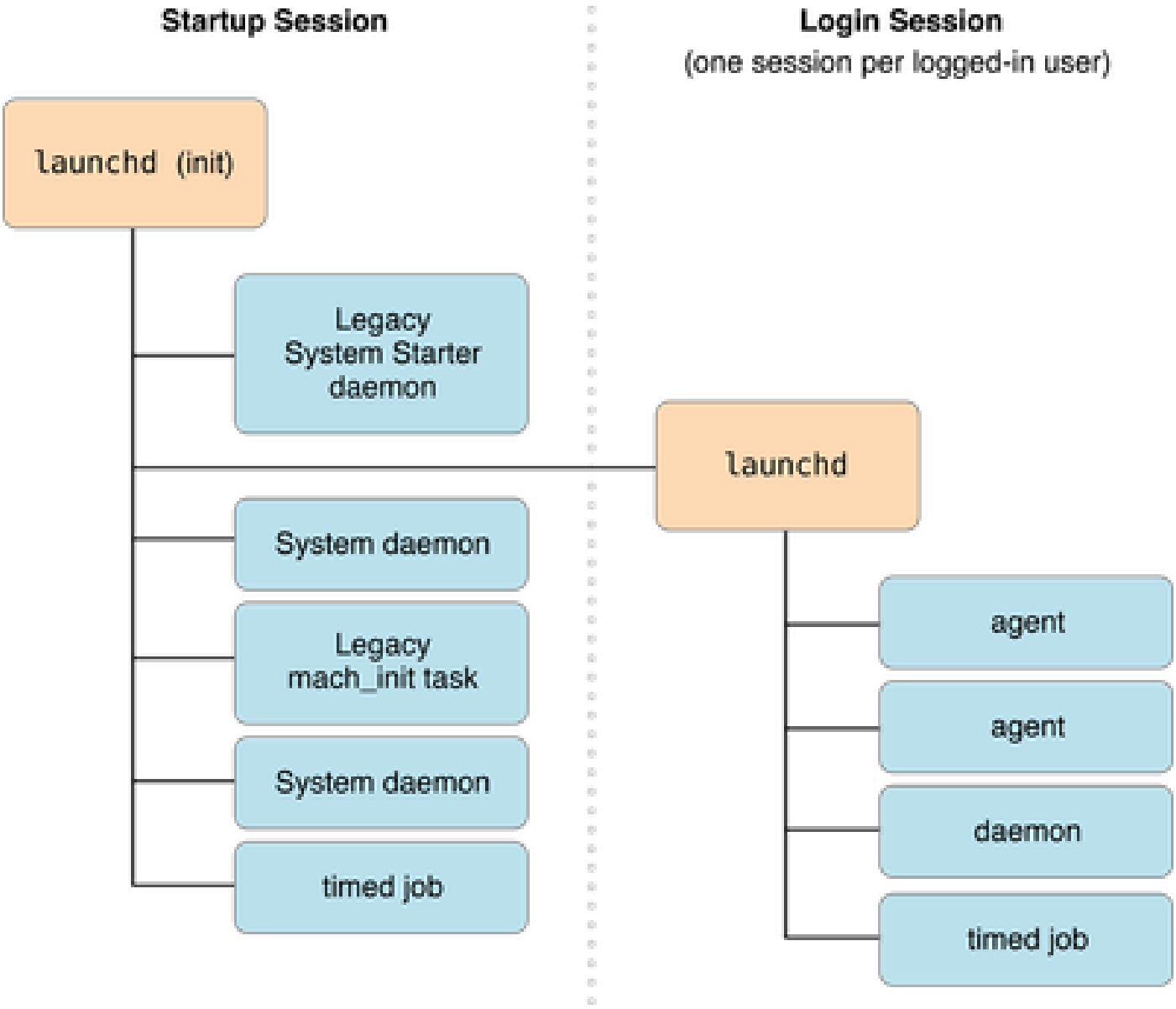
Premesse

La condizione del servizio macOS è utile quando è necessario utilizzare la funzione case per verificare se un servizio è caricato nel dispositivo macOS e consente inoltre di verificare se è in esecuzione o meno. La condizione del servizio macOS può verificare due tipi di servizio diversi: daemon e agenti.

Un daemon è un programma che viene eseguito in background come parte dell'intero sistema (ovvero, non è legato a un particolare utente). Un daemon non può visualizzare alcuna GUI; in particolare, non è consentito connettersi al server di windows. Un server Web è l'esempio perfetto di un daemon.

Un agente è un processo che viene eseguito in background per conto di un utente specifico. Gli agenti sono utili in quanto possono eseguire operazioni che i daemon non sono in grado di eseguire, ad esempio accedere in modo affidabile alla home directory dell'utente o connettersi al server di finestre. Un programma di monitoraggio del calendario è un buon esempio di agente.

Nel diagramma seguente è possibile visualizzare il modo in cui ciascun dispositivo viene caricato in base all'avvio del dispositivo e all'accesso dell'utente:



Ulteriori informazioni su daemon e agenti sono disponibili qui nella documentazione Apple

I demo e gli agenti disponibili sul dispositivo macOS sono disponibili nelle seguenti posizioni:

Posizione	Descrizione
~/Libreria/LaunchAgents	Agenti per utente forniti dall'utente.
/Library/LaunchAgents	Agenti per utente forniti dall'amministratore.
/Library/LaunchDaemons	daemon a livello di sistema forniti dall'amministratore.
/System/Library/LaunchAgents	Agenti per utente di OS X

/System/Library/LaunchDaemons	Daemon a livello di sistema per OS X

È possibile controllare l'elenco di ciascuna categoria dal terminale macOS utilizzando questi comandi:

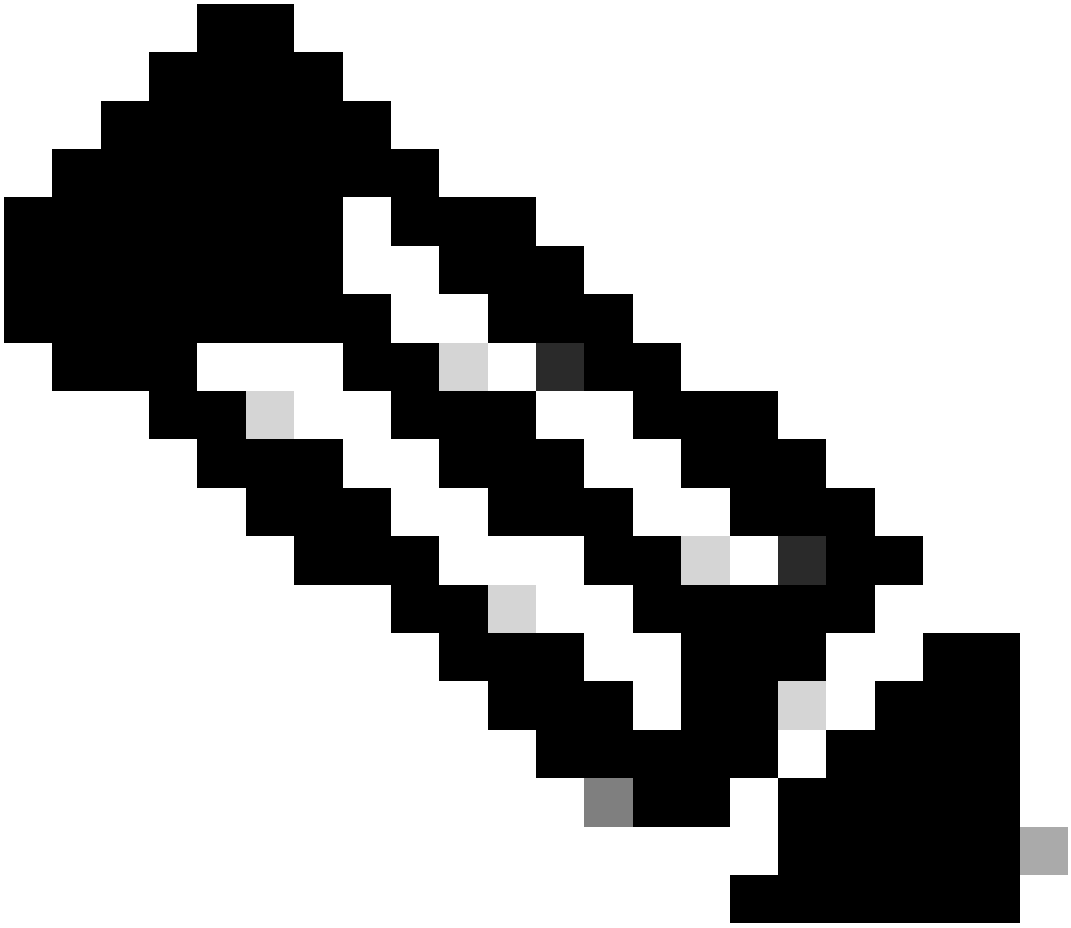
ls -ltr ~/Libreria/LaunchAgent
ls -ltr /Library/LaunchAgents
ls -ltr /Library/LaunchDaemons
ls -ltr /System/Library/LaunchAgents
ls -ltr /System/Library/LaunchDaemons

I percorsi precedenti possono mostrare tutti i daemon e gli agenti disponibili sul dispositivo macOS, ma non tutti sono caricati o in esecuzione.

Configurazione

La configurazione per la condizione del servizio macOS può essere eseguita eseguendo i seguenti passaggi:

1. Identificare il nome del servizio da controllare.
2. (Facoltativo) Controllare i dettagli del servizio per definire se si tratta di un agente o di un delegato.
3. Selezionare l'operatore di servizio da valutare.
4. Configurare il requisito e il criterio di postura per tale condizione.



Nota: La condizione di postura del servizio richiede privilegi elevati per funzionare, quindi è NECESSARIO che ISE PSN sia considerato attendibile da Cisco Secure Client (in precedenza AnyConnect) - Guida di riferimento

Identificare il nome del servizio da controllare

ISE Posture Compliance Module è in grado di verificare la presenza di servizi che sono stati caricati, eseguiti e caricati, nonché eseguiti con il codice di uscita.

Per controllare i servizi caricati, utilizzare il comando sudo LAUNCHCTL dumpstate.

Per controllare i servizi caricati e con un codice di uscita, utilizzare il comando sudo LAUNCHCTL LIST.

I comandi precedenti possono mostrare improvvisamente molte informazioni, ma è sufficiente utilizzare questi comandi per visualizzare il nome effettivo del servizio:

Per verificare solo i nomi dei servizi caricati, utilizzare questo comando:

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

Per verificare solo i nomi dei servizi caricati e con un codice di uscita, utilizzare questo comando:

sudo Launchctl List | sveglio '{if (NR>1) stampa $3}'

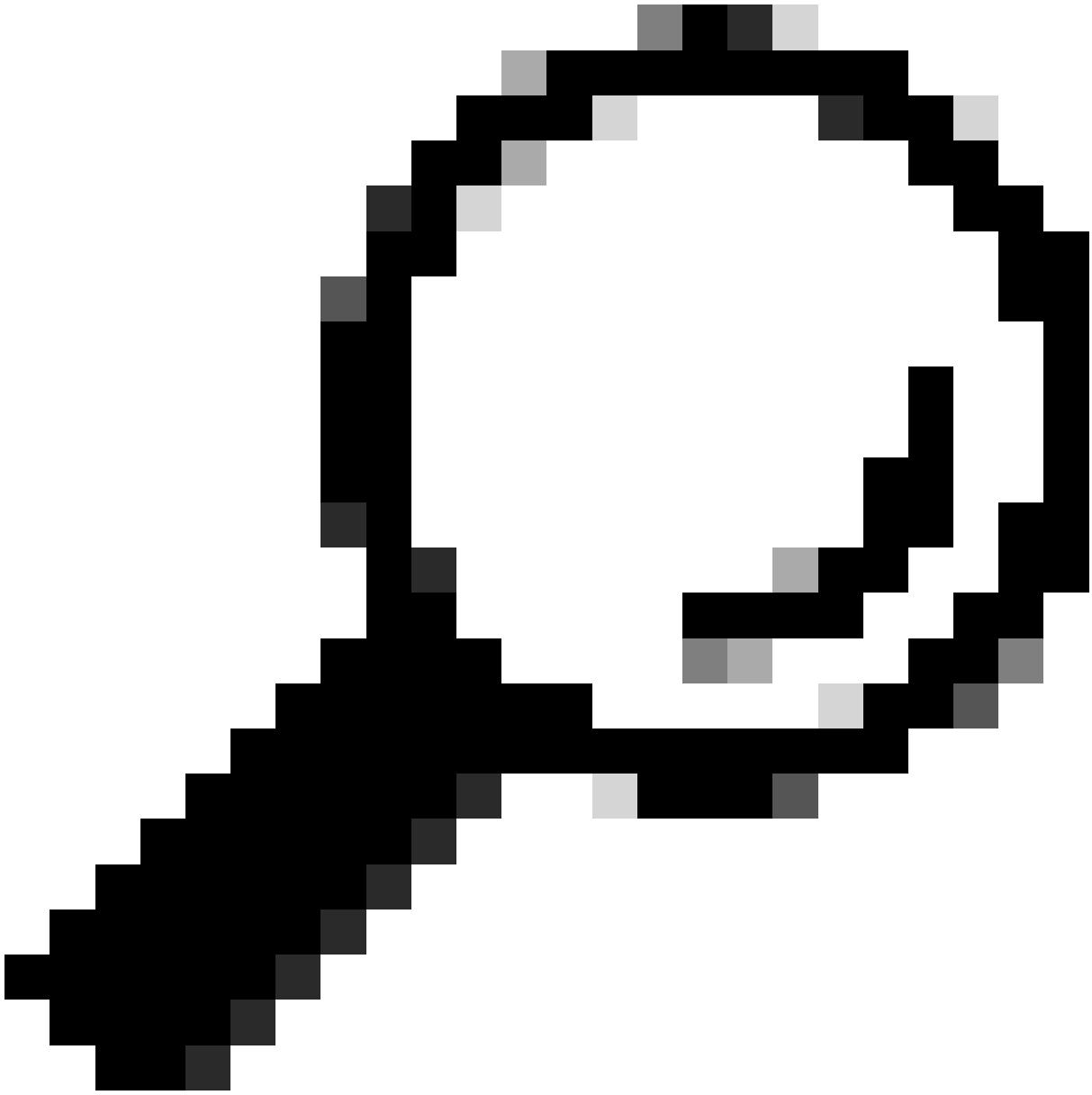
Poiché questi comandi mostrano molte informazioni, al termine di ogni comando è consigliabile utilizzare un altro filtro grep per trovare il servizio desiderato.
Ad esempio, se si cerca un servizio specifico del fornitore, è possibile usare una parola chiave come filtro nella e.

Nel caso dei servizi Cisco, i comandi sono simili al seguente:

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | utilizzato 's|.*/||;s| = {$||' | grep -i cisco
sudo Launchctl List | sveglio '{if (NR>1) stampa $3}' | grep -i cisco

(Facoltativo) Controllare i dettagli del servizio da definire se si tratta di un agente o di un delegato

Nella seconda parte della configurazione di questa condizione, è necessario verificare se il servizio è di tipo daemon o di tipo agente.



Suggerimento: Questo passaggio è facoltativo, in quanto ISE consente di selezionare l'opzione per Daemon o User Agent, quindi è sufficiente selezionare l'opzione e saltare questa parte.

Nel caso in cui si desideri essere granulari in questa condizione, è possibile controllare il tipo eseguendo le operazioni seguenti:

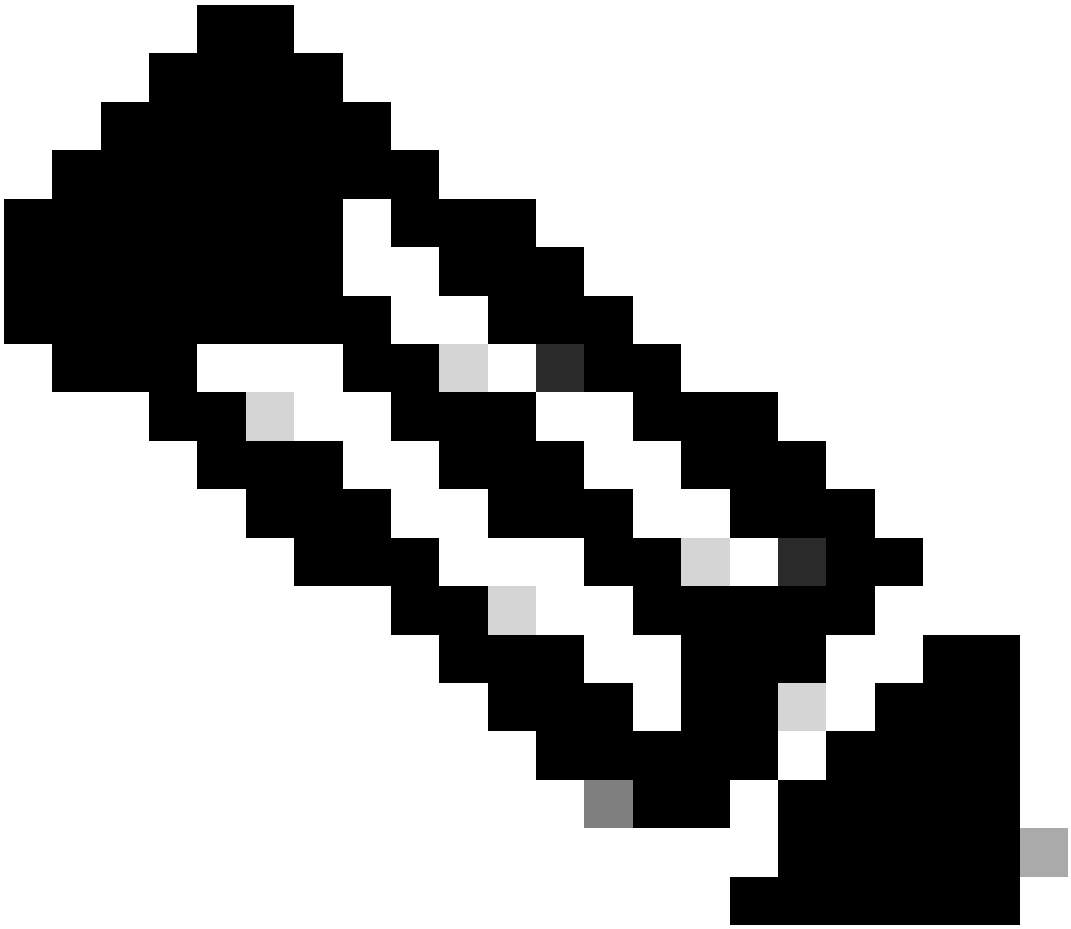
1. Controllare innanzitutto il nome LAUNCHCTL completo del servizio con il comando sudo grep -B 10 -A 10 -E "^\s*state = " << "$(LAUNCHCTL DUMSTATE)" | grep -aiE "\/.*= {" | utilizzato 's|.*/||;s| = {$||' | grep -i {Nome servizio}

Ad esempio, per il comando sudo grep -B 10 -A 10 -E "^\s*state = " << "$(LAUNCHCTL dumpstate)" | grep -aiE "\/.*= {" | invia 's/.\{3\}$//' | grep -i com.cisco.secureclient.iseposture, l'output è: gui/501/com.cisco.secureclient.iseposture.

2. Controllare il tipo di servizio con il comando sudo LAUNCHCTL PRINT { Nome del servizio LAUNCHCTL } | grep -i 'type = Launch'

Nell'esempio seguente, per il comando: sudo LAUNCHCTL PRINT gui/501/com.cisco.secureclient.iseposture | grep -i 'tipo = Launch', output: tipo = LaunchAgent.

Ciò significa che il tipo di servizio è Agent, altrimenti verrebbe visualizzato type = LaunchDaemon.



> Nota: Se le informazioni sono vuote, selezionare l'opzione Daemon Or User Agent in ISE per l'impostazione del tipo di servizio.

Selezionare l'operatore di servizio da valutare

ISE vi permette di selezionare 5 diversi operatori del servizio:

- Caricato

- Non caricato
- Caricato ed in esecuzione
- Caricato con il codice di uscita
- Caricato ed in esecuzione o con codice di uscita

Servizi caricati

Sono tutti i servizi elencati quando si utilizzano questi due comandi:

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | utilizzato 's|.*/||;s| = {$||'
sudo Launchctl List | sveglio '{if (NR>1) stampa $3}'

Servizi non caricati

Sono tutti i servizi per i quali è stato definito il relativo elenco di proprietà (plist), ma che non sono stati caricati, o i servizi per i quali non è stato definito alcun elenco di proprietà (plist), pertanto non possono essere caricati.

Questi servizi non sono facili da identificare ed è molto comune nel caso in cui si desideri verificare che un servizio specifico non esista nel dispositivo macOS.
Ad esempio, se si desidera impedire il caricamento del servizio di zoom sul dispositivo macOS, è possibile inserire us.zoom.ZoomDaemon come valore per il servizio, in questo modo si è certi che zoom non sia in esecuzione o non sia installato affatto.

Non è possibile disinstallare alcuni servizi ed è stato definito il relativo elenco di proprietà.
Ad esempio, con questo comando è possibile verificare che l'elenco di indirizzi dhcp6d è definito:

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

Se si controlla l'elenco dei servizi, è possibile verificare che non è caricato:

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

Se si imposta il valore su com.apple.dhcp6d", il dispositivo macOS è conforme in quanto, anche se è stato definito l'elenco dei servizi, il servizio non viene caricato.

Caricato ed in esecuzione

Non tutti i servizi sono in esecuzione, esistono più stati per ogni servizio, ad esempio in esecuzione, non in esecuzione, in attesa, chiuso, non inizializzato e così via.
Per controllare tutti i servizi in esecuzione, utilizzare questo comando:

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

I servizi elencati con il comando precedente hanno riscontrato la condizione dell'operatore del servizio Loaded & Running.

Caricato con codice di uscita

Alcuni servizi possono terminare con un codice di uscita previsto o imprevisto. Tali servizi possono essere elencati con il comando:

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

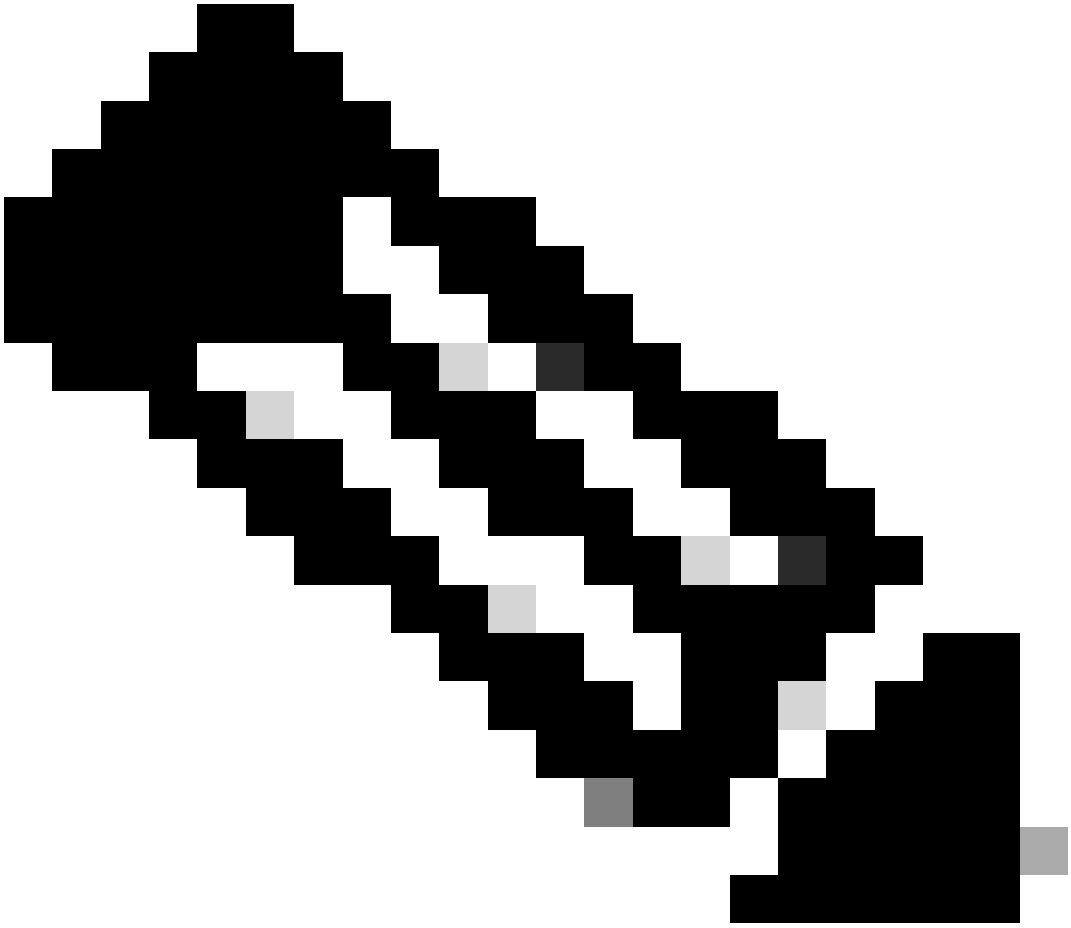
Per conoscere il relativo codice di uscita, è possibile scegliere qualsiasi servizio e utilizzare il comando:

sudo Launchctl print { Nome del servizio Launchctl } | grep -i "ultimo codice di uscita"

Ad esempio:

sudo Launchctl print gui/501/com.apple.mdmclient.agent | grep -i "ultimo codice di uscita"

di output: ultimo codice di uscita = 0

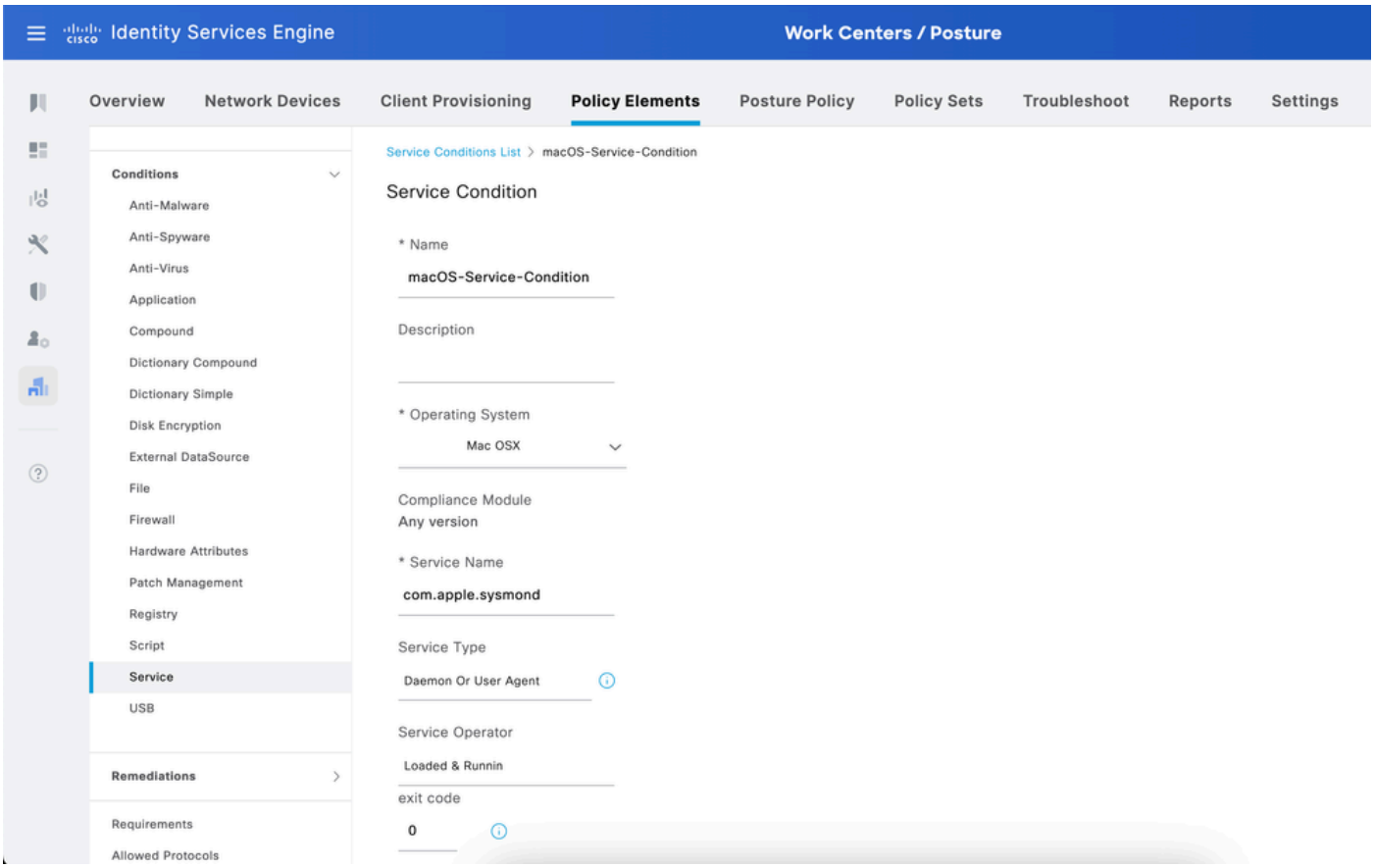


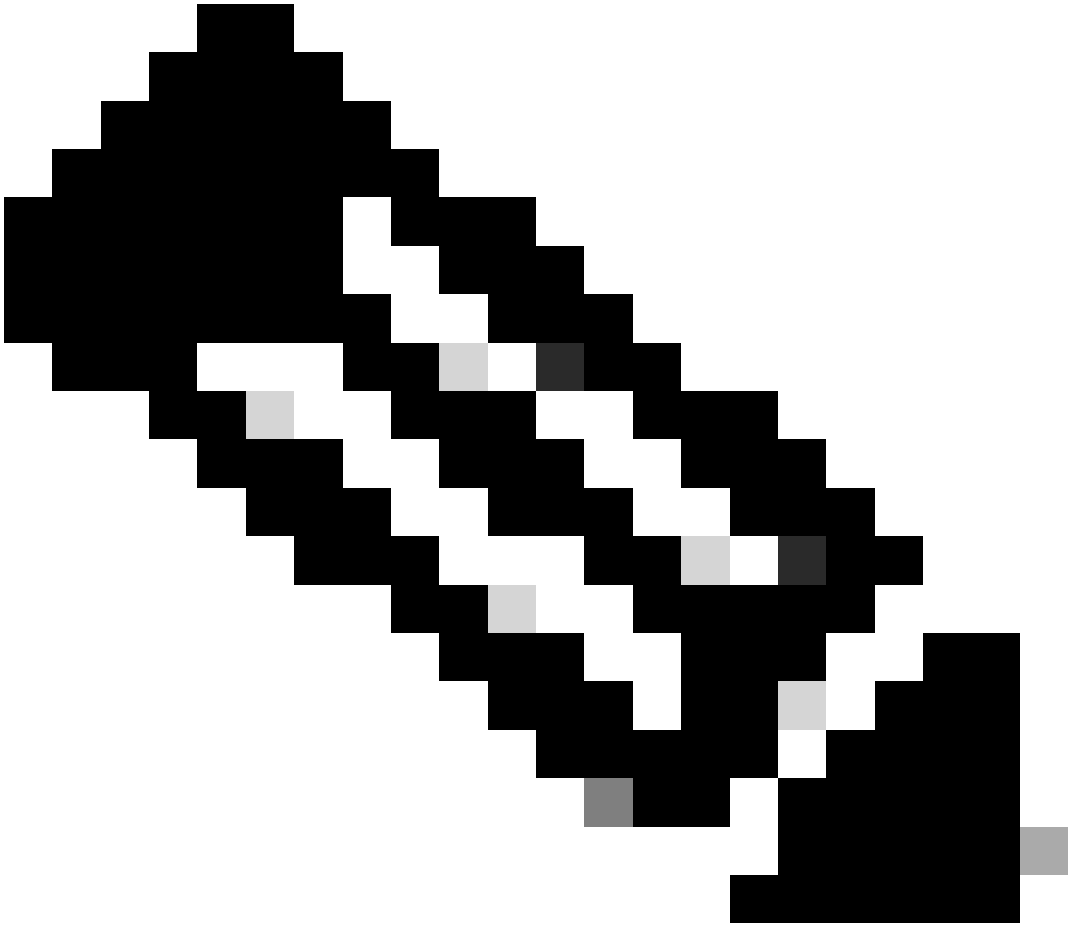
Nota: In questo caso, il codice di uscita 0 indica in genere che il servizio ha eseguito correttamente tutte le operazioni. Se un computer non corrisponde allo 0 come codice di uscita, significa che il servizio non ha eseguito l'azione prevista.

Caricato ed in esecuzione o con codice di uscita

Quest'ultima opzione funziona quando il servizio è Caricato ed in esecuzione o Caricato con il codice di uscita.

Nell'immagine viene mostrato un esempio di condizione di servizio macOS.

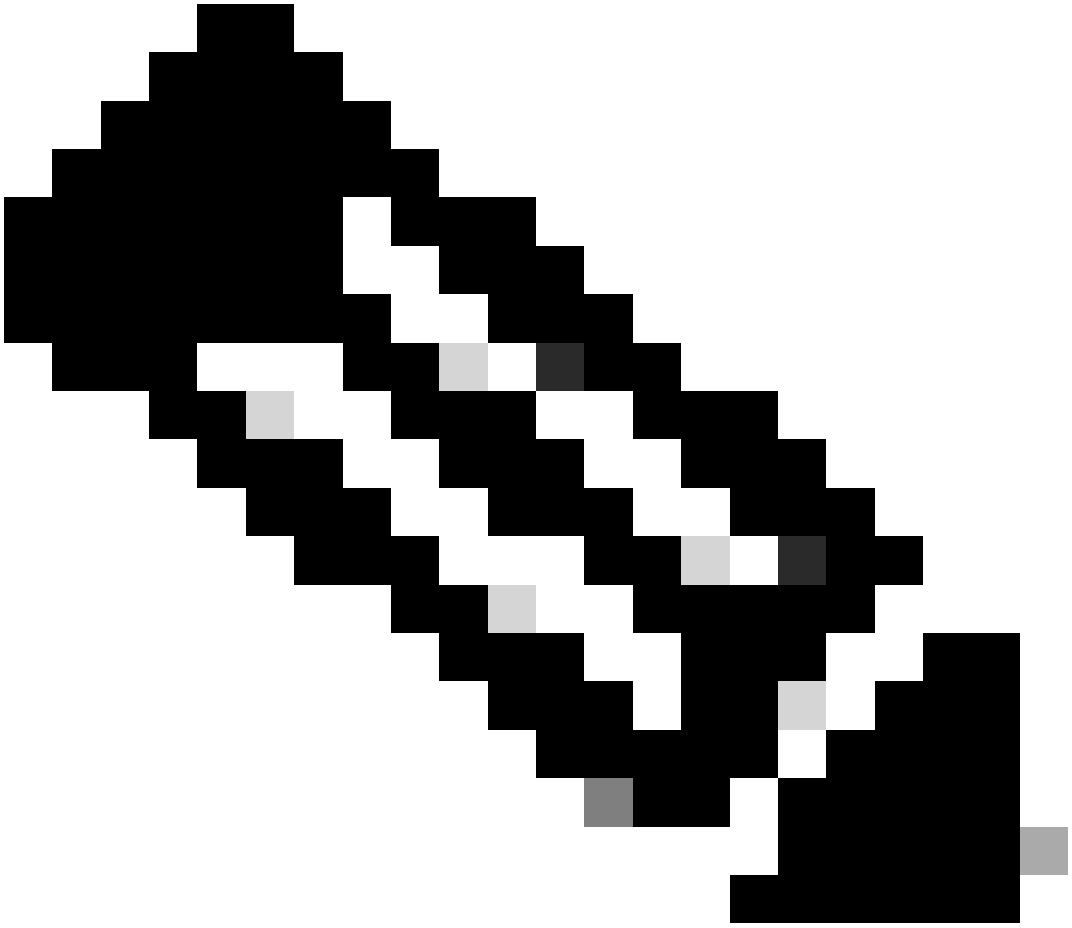

Identity Services Engine
Work Centers / Posture
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
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



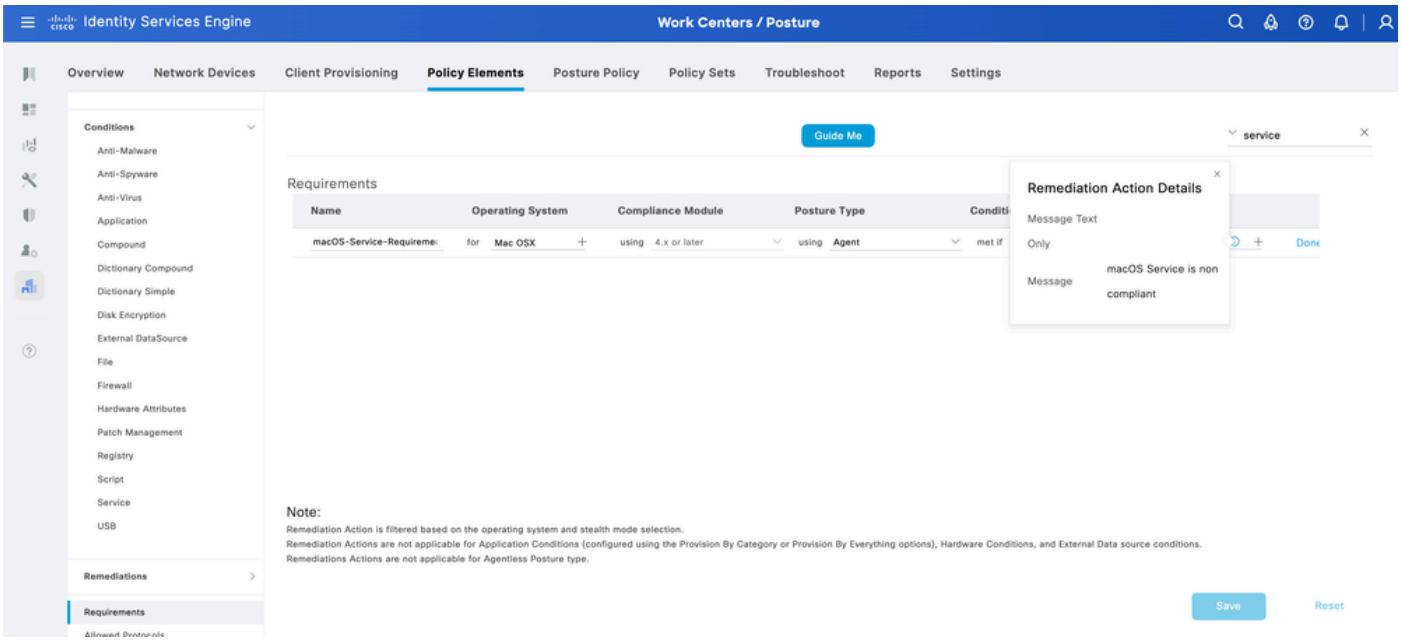
Nota: Al momento, è supportato solo il nome di servizio esatto. È stato richiesto un miglioramento per supportare il carattere jolly nei nomi dei servizi, ID bug Cisco CSCwf01373

Configurare i criteri di requisito e postura per tale condizione

Una volta configurata la condizione, è necessario creare un requisito per tale condizione. Utilizzare l'opzione Solo test messaggio per questo requisito.
Passare a ISE > Work Center > Postura > Requisiti per crearlo.

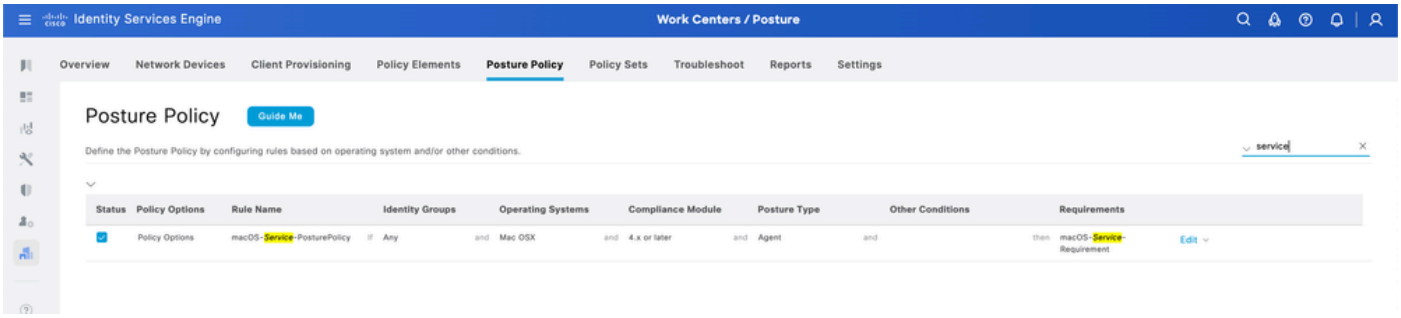


Nota: Non sono disponibili opzioni di monitoraggio e aggiornamento per le condizioni del servizio.



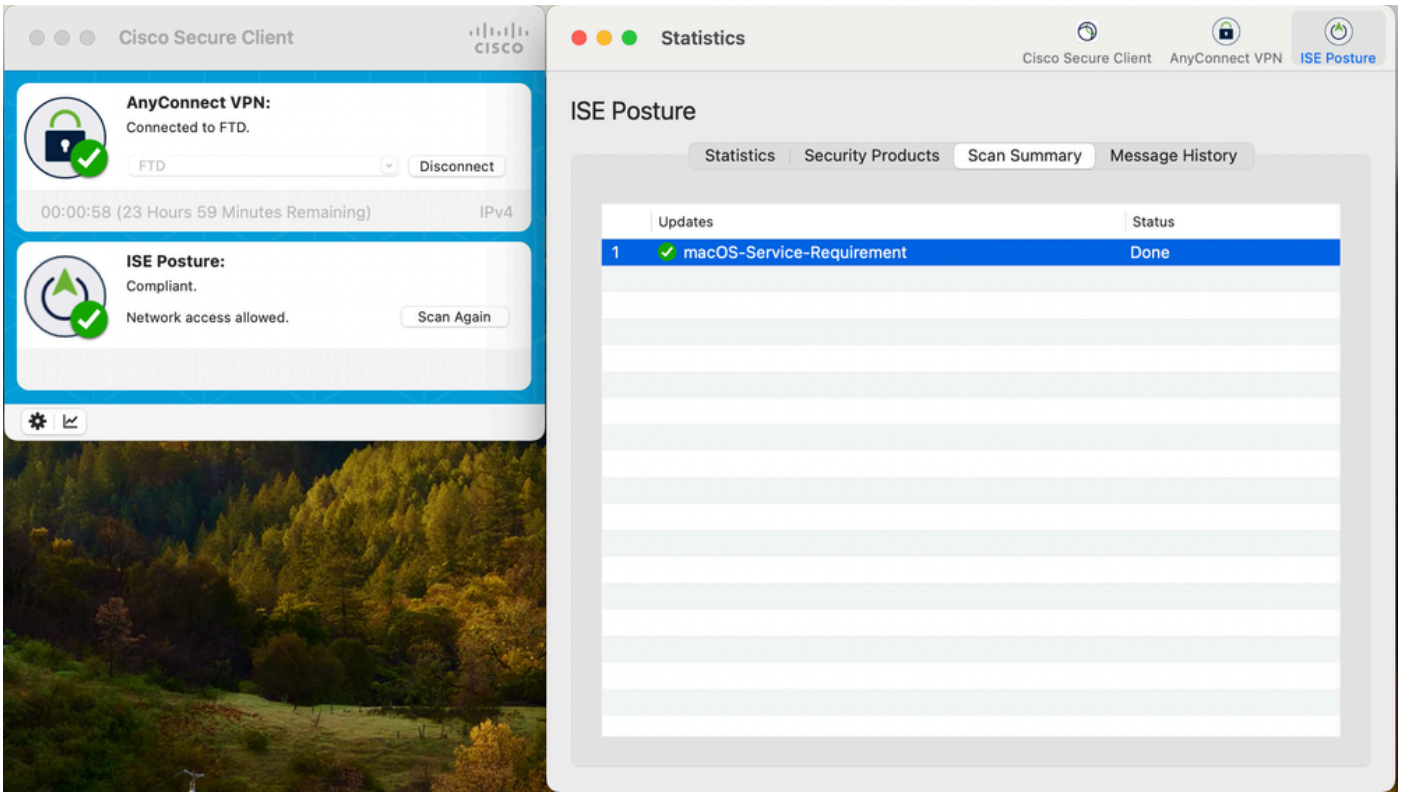
Al termine, l'ultimo passaggio consiste nella configurazione del criterio di postura che utilizza il requisito creato.
Passare a ISE > Work Centers > Posture > Posture Policy per creare la policy.

Abilitare il nuovo criterio, denominarlo come desiderato e selezionare il requisito appena creato.

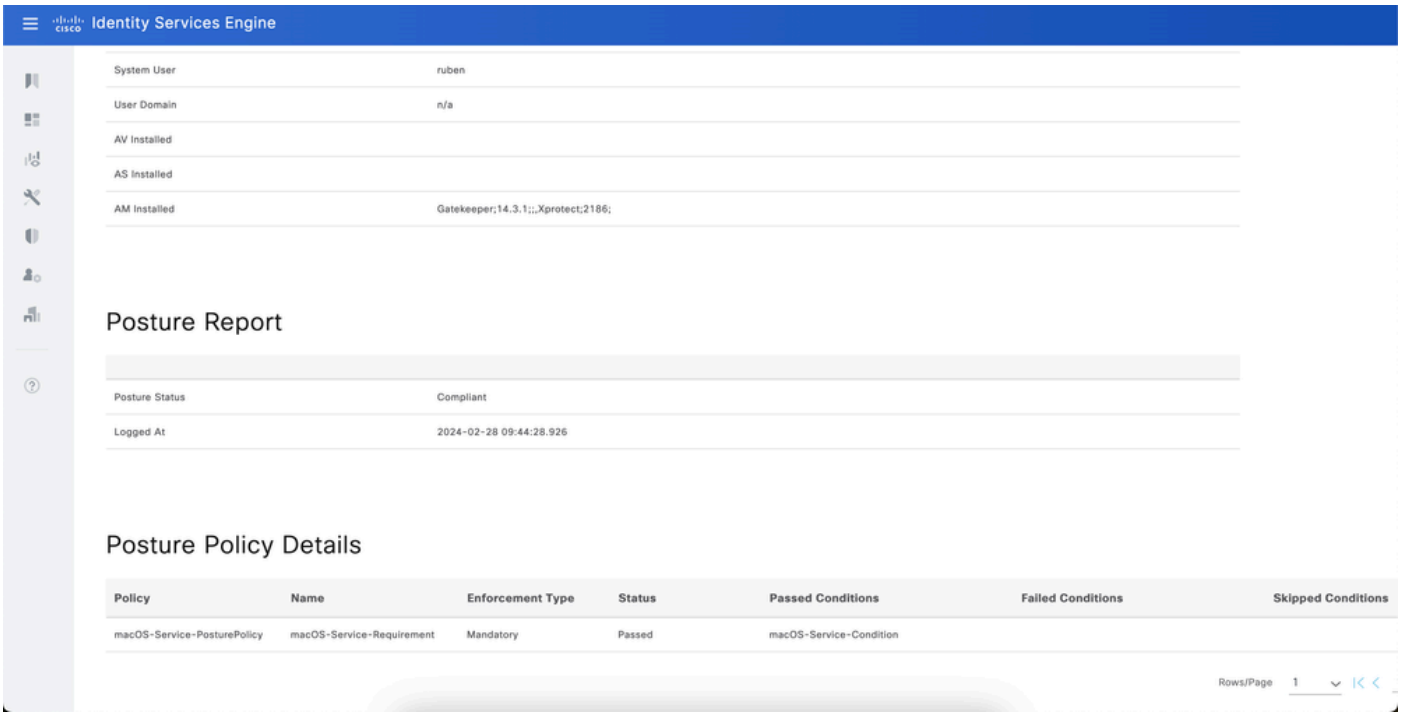


Verifica

È possibile verificare che la condizione di postura di macOS sia stata superata o meno dalla stessa GUI di Cisco Secure Client.



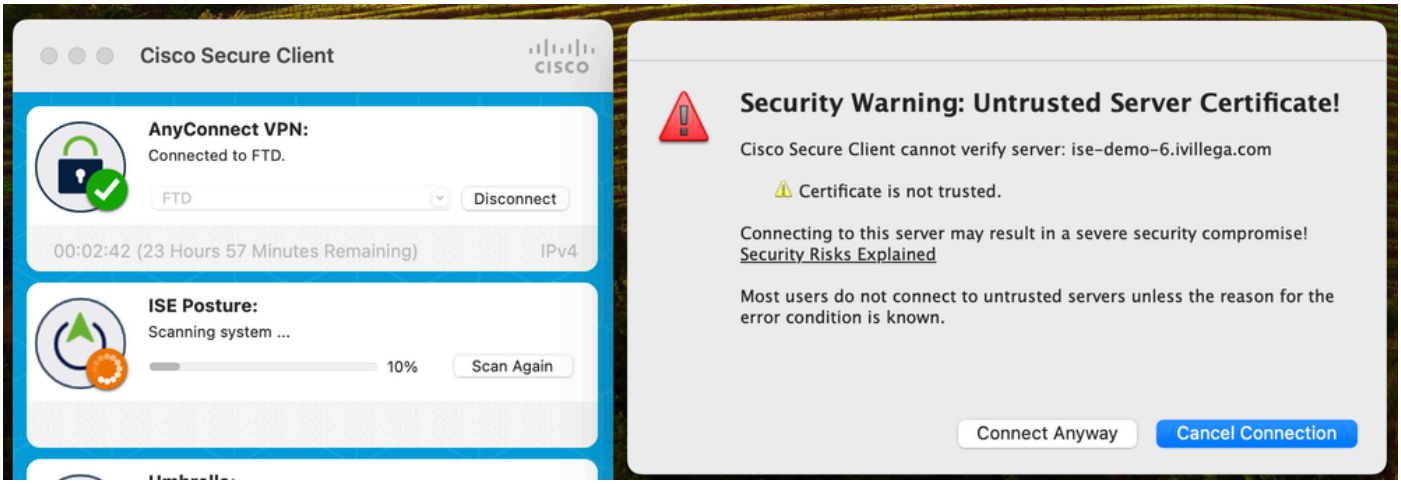
Inoltre, è possibile controllare il report ISE Posture da ISE > Operazioni > Report > Report > Endpoint e utenti > Valutazione postura per endpoint.



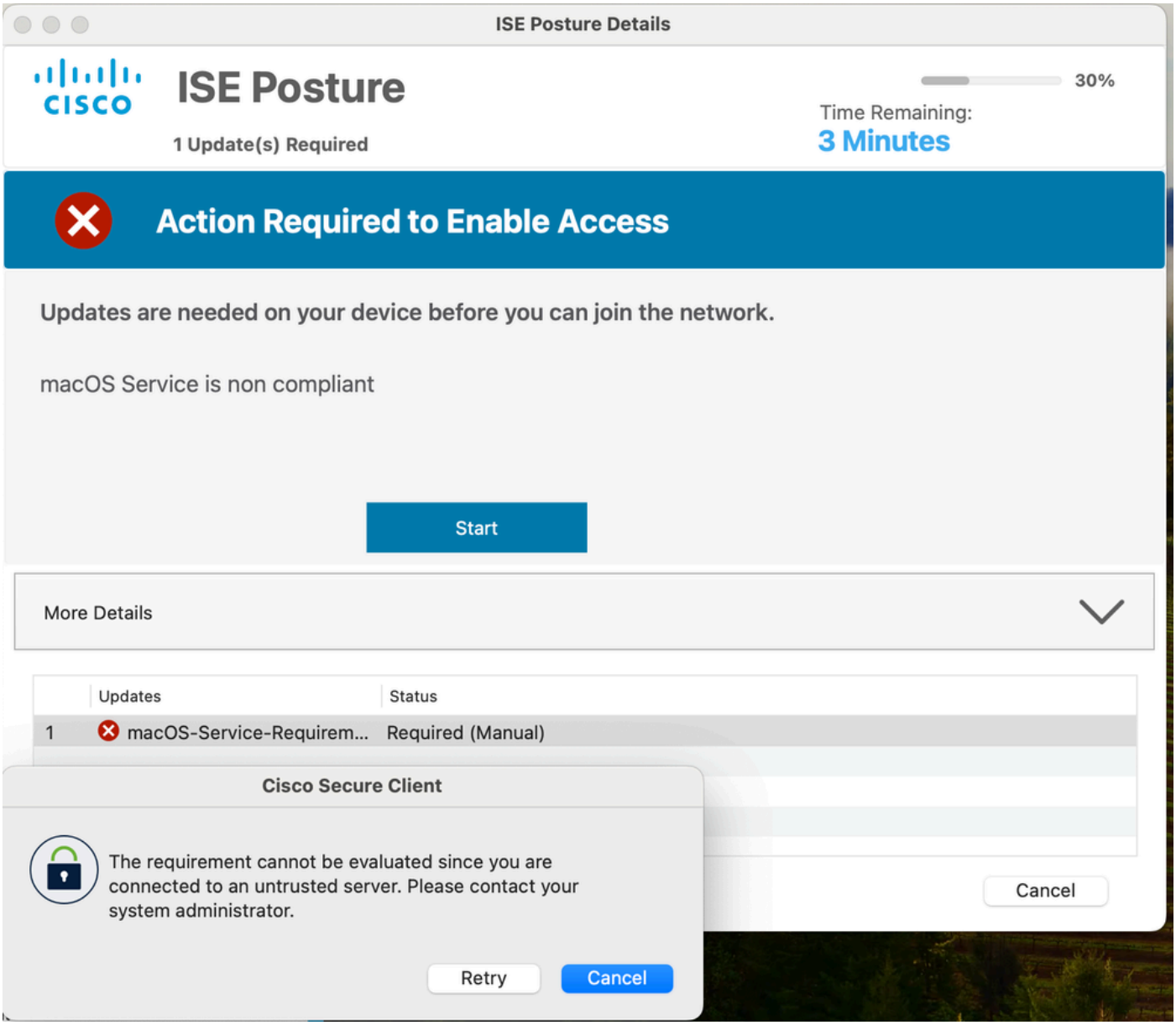
Risoluzione dei problemi

Problemi comuni che possono verificarsi durante la configurazione di questa condizione di postura del servizio macOS sono:

Certificato non attendibile



Come indicato in precedenza, la condizione del servizio richiede autorizzazioni elevate. È essenziale che il certificato per il processo di scansione della postura sia considerato attendibile dal server.
In caso contrario, si verificherà il seguente errore:

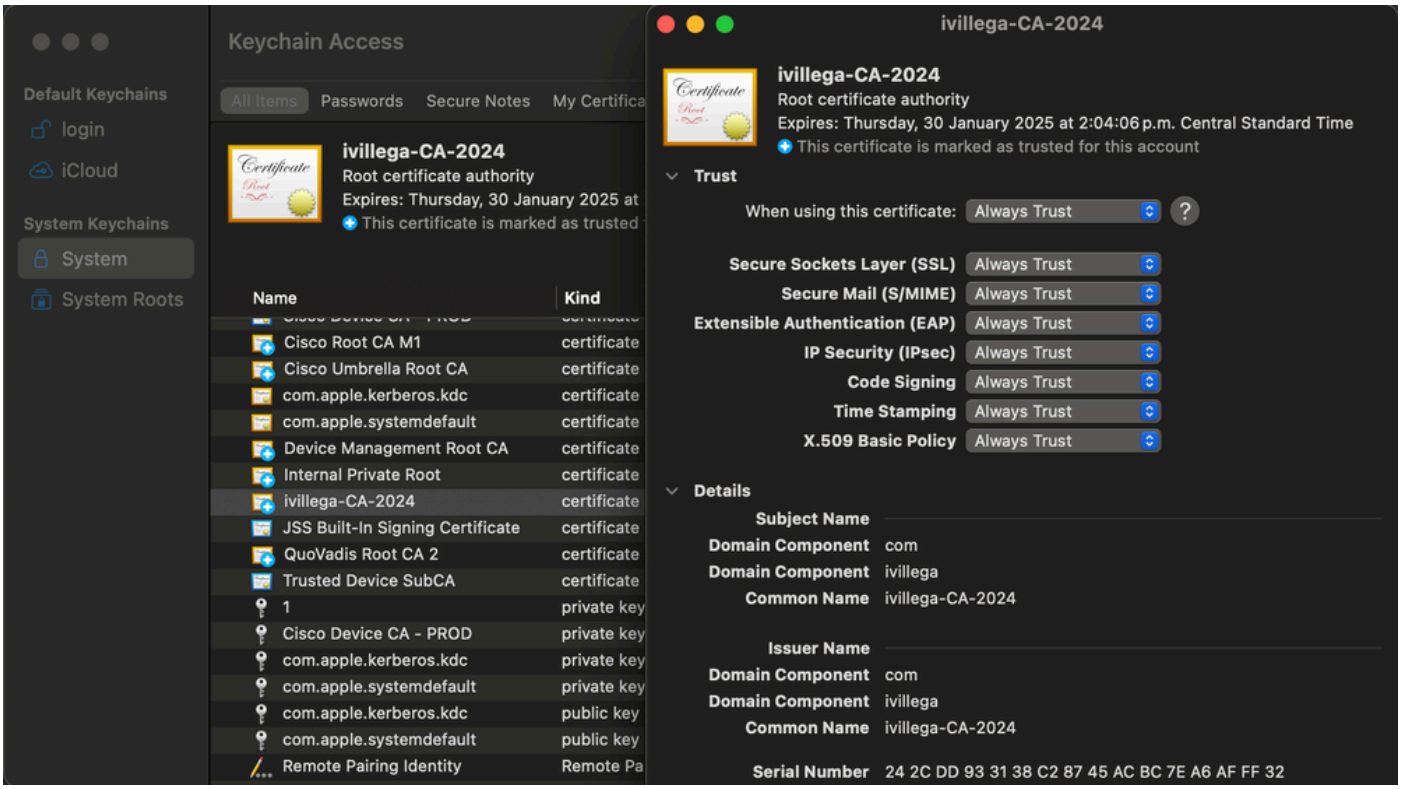


Il modulo ISE Posture individua i server PSN in base all'indirizzo IP o al nome di dominio completo (FQDN). È buona norma disporre dei file di configurazione della postura per individuare i nodi ISE tramite FQDN, in modo che i certificati Admin and Portal (Client Provisioning Portal) includano l'FQDN nel campo CN o nel campo SAN. È inoltre possibile utilizzare certificati jolly. I certificati jolly sono supportati per questo flusso.

A causa dei titoli di sistema, il campo CN non è più attendibile. È consigliabile includere la voce con caratteri jolly o il nome di dominio completo (FQDN) nel campo SAN.

Nel caso in cui i PSN ISE vengano rilevati tramite l'indirizzo IP anziché il nome FQDN, è necessario includere l'indirizzo IP dei nodi nel campo CN o nel campo SAN dei certificati collegati all'utilizzo di Amministratore e Portale.

I moduli ISE Posture considerano attendibile il certificato presentato dal server ISE. Se la relativa CA si trova nell'archivio certificati di sistema dell'accesso Keychain macOS, la CA deve avere l'impostazione Quando si utilizza questo certificato impostata su Sempre attendibile.



È possibile che si verifichi un comportamento errato in base al quale, anche quando il certificato è caricato correttamente e tutti i requisiti CN e SAN sono soddisfatti, il sistema macOS non considera il certificato attendibile. In questi casi, aprire l'applicazione di accesso Keychain, passare alla scheda Archivio certificati di sistema ed eliminare il certificato CA da tale scheda.

Passare quindi all'applicazione terminale macOS ed eseguire questo comando: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain

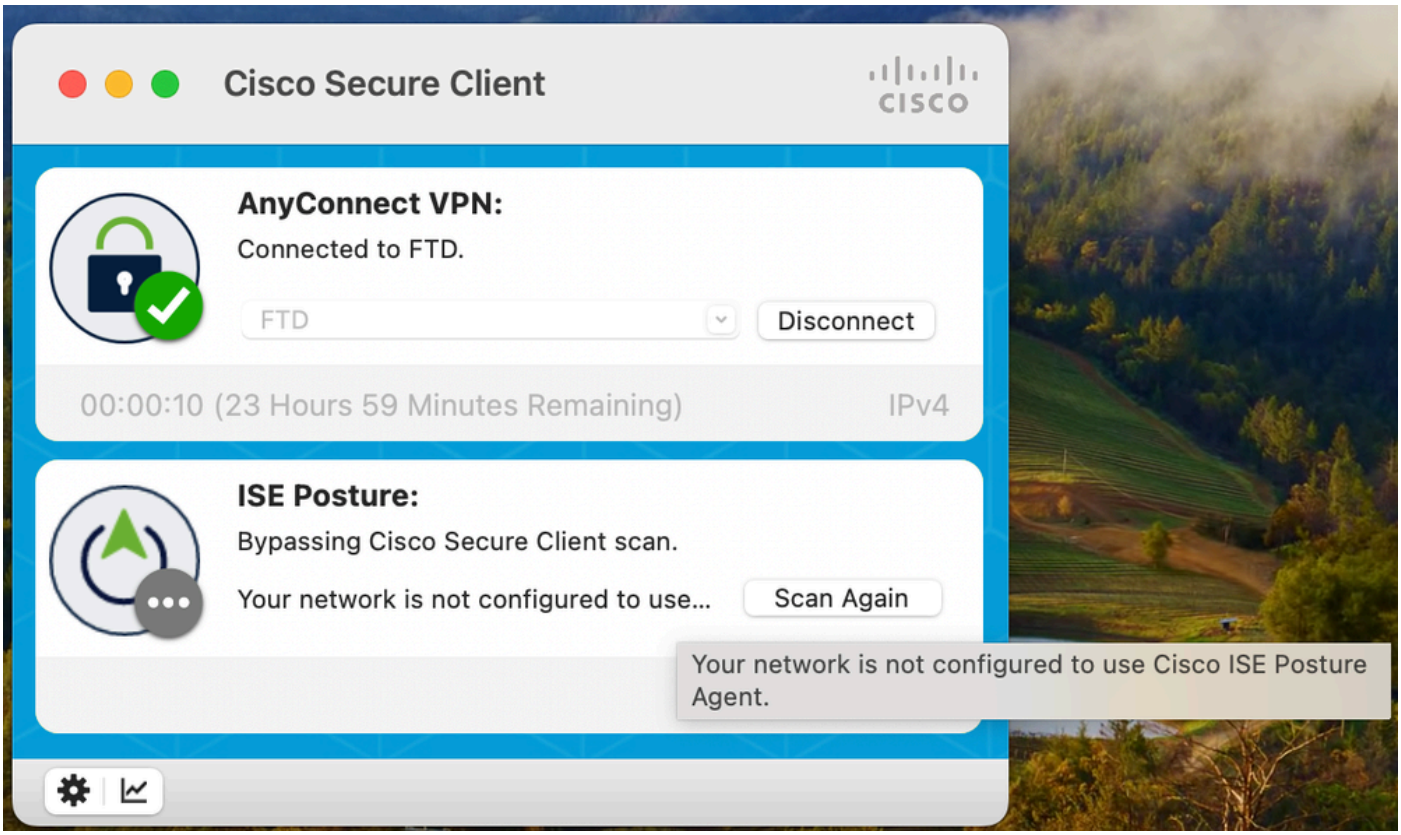
{Percorso del certificato CA}

Se ad esempio il certificato si trova sul desktop, il comando sarà il seguente: sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt

Dopo aver eseguito il comando, riavviare il computer e riprovare.

Ignorare Cisco Secure Client Scan

Potrebbero essere visualizzati anche i messaggi di errore "Bypass Cisco Secure Client Scan" (Ignorare Cisco Secure Client Scan) e "Your network is not configure to use Cisco ISE Posture Agent" (La rete non è configurata per l'utilizzo di Cisco ISE Posture Agent):



Questo messaggio viene visualizzato perché non ci sono profili configurati in Client Provisioning in ISE > Work Center > Posture > Client Provisioning > Client Provisioning Policies.
Anche se si può vedere una condizione per Mac OSX sistemi operativi, ciò non significa che si sta coprendo tutte le versioni macOS.

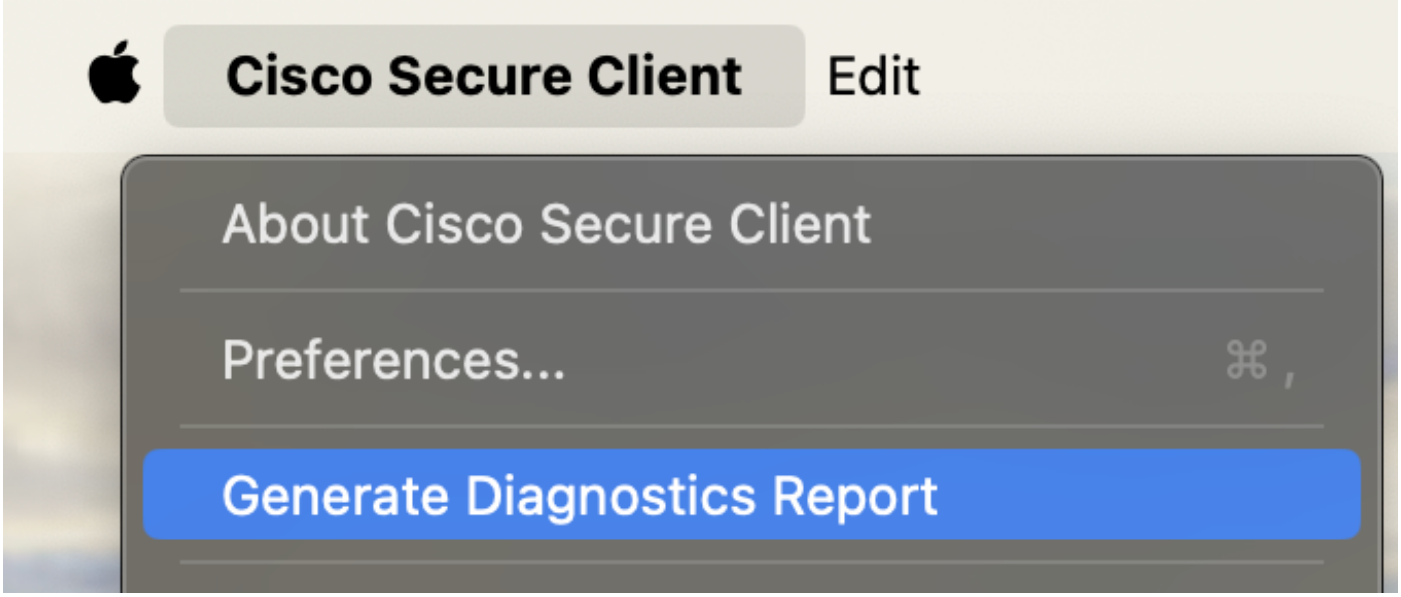
Per impostazione predefinita, ISE non include le versioni macOS più recenti, ad esempio Sequoia (15.6.x), per evitare che venga visualizzato questo messaggio, verificare che la postura sia aggiornata.

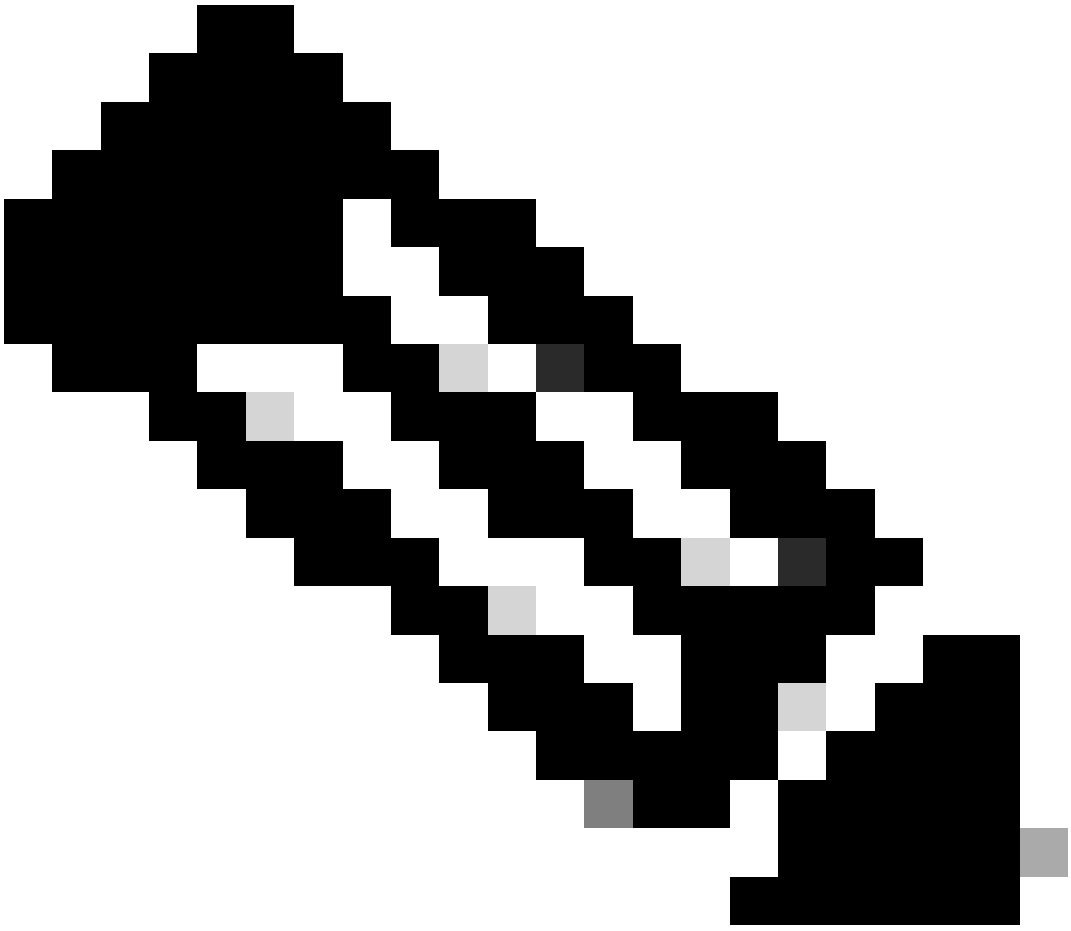
È necessario aggiornare il feed postura da ISE > Work Centres > Posture > Impostazioni > Aggiornamenti software > Aggiornamenti postura.

L'aggiornamento può essere effettuato online direttamente da ISE oppure offline tramite un file zip scaricabile qui dal sito di Posture Offline

Altri problemi

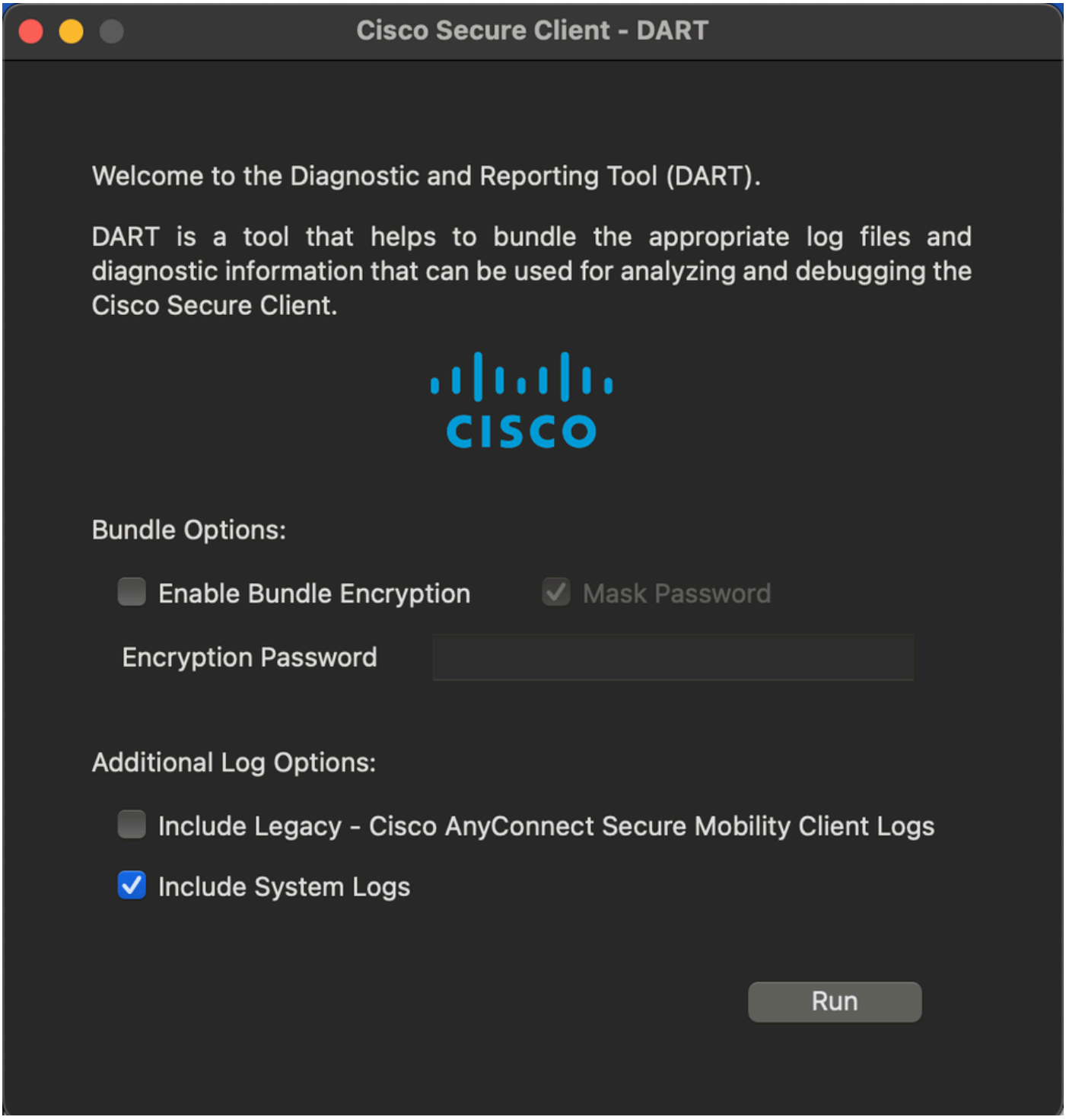
Se si desidera entrare nei dettagli, è possibile raccogliere un pacchetto DART dal dispositivo macOS posturato. A tale scopo, è necessario che sia installato il modulo DART. Con l'applicazione Cisco Secure Client attiva, passare alla barra dei menu e fare clic su Cisco Secure Client, quindi in Genera report di diagnostica.



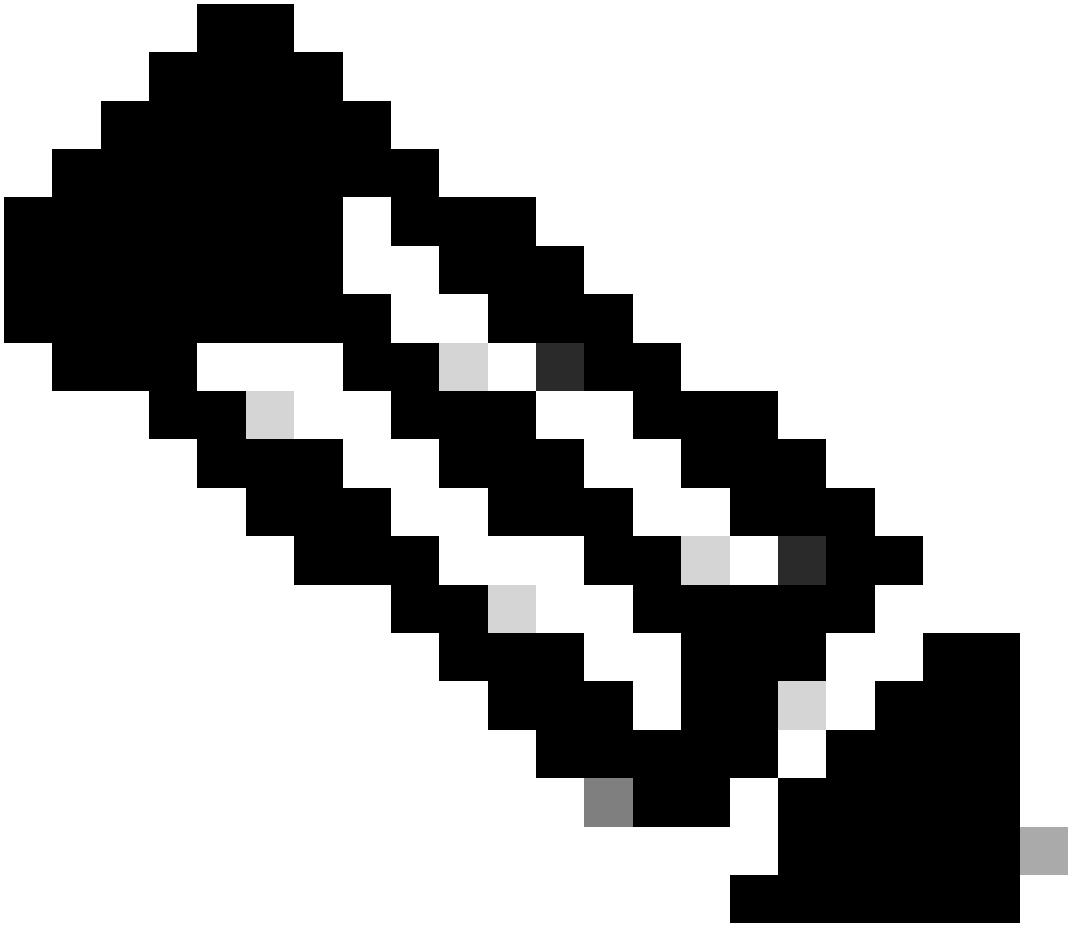


Nota: È importante abilitare l'opzione Includi registri di sistema durante la generazione del

bundle DART, altrimenti il bundle DART non includerà le informazioni sul modulo di postura ISE.



Per motivi di sicurezza, alcuni log possono essere crittografati e non visibili, ma nel file unified_log.log del bundle DART è possibile visualizzare log simili a quelli mostrati di seguito:



Nota: Questo esempio di registro si riferisce alla condizione del servizio macOS configurata in questo documento.

```
[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
```

Inoltre, è possibile impostare il componente posture a livello di log di debug nel nodo PSN ISE che autentica e posiziona l'endpoint.

È possibile configurare questo livello di log da ISE > Operazioni > Risoluzione dei problemi > Debug guidato > Configurazione log di debug. Fare clic sul nome host PSN e modificare il livello di log del componente Posture da INFO a DEBUG.

Utilizzando lo stesso esempio per la condizione di servizio macOS, è possibile visualizzare log simili all'interno del file 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
```

Se il problema persiste, aumentare la richiesta TAC con il team Cisco.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).