Implementazione della postura senza reindirizzamento ISE

Sommario

Introduzione

Questo documento descrive l'uso e la configurazione del flusso di postura senza reindirizzamento e i suggerimenti per la risoluzione dei problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Flusso di postura su ISE
- Configurazione dei componenti di postura su ISE
- Reindirizzamento ai portali ISE

Per una migliore comprensione dei concetti descritti più avanti, si consiglia di esaminare:

Confronta le versioni precedenti di ISE con ISE Posture Flow in ISE 2.2
Gestione e postura delle sessioni ISE

Componenti usati

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

- Cisco ISE versione 3.1
- Cisco Secure Client 5.0.01242

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

Il flusso di ISE Posture è costituito dai seguenti passaggi:

0. Autenticazione/autorizzazione. In genere viene eseguito subito prima dell'inizio del flusso di postura, ma può essere ignorato in alcuni casi di utilizzo, ad esempio in caso di rivalutazione della postura (PRA). Poiché l'autenticazione non attiva la scoperta della postura, questa non è considerata essenziale per ogni flusso di postura.

1. Individuazione. Processo eseguito dal modulo Secure Client ISE Posture per trovare il proprietario PSN della **sessione attiva corrente**.
2. Provisioning client. Processo eseguito da ISE per effettuare il provisioning del client con le versioni corrispondenti del modulo ISE Posture di Cisco Secure Client (in precedenza AnyConnect) e del modulo di conformità. In questo passaggio viene eseguito il push al client anche della copia locale del profilo di postura contenuto nel PSN specifico e firmato da tale PSN.
3. Scansione del sistema. Le policy di postura configurate sull'ISE vengono valutate dal Modulo di conformità.
4. Correzione (facoltativo). Eseguito in caso di criteri di postura non conformi.
5. CoA. La riautorizzazione è necessaria per concedere l'accesso finale alla rete (conforme o non conforme).

Questo documento è incentrato sul processo di rilevamento del flusso ISE Posture.

Cisco consiglia di utilizzare il reindirizzamento per il processo di rilevamento. In alcuni casi, tuttavia, il reindirizzamento non è implementabile, ad esempio nell'utilizzo di dispositivi di rete di terze parti in cui non è supportato. Questo documento ha lo scopo di fornire una guida generale e le best practice per implementare e risolvere la postura senza reindirizzamento in tali ambienti.

La descrizione completa del flusso senza reindirizzamento è descritta in Confronta le versioni precedenti di ISE con ISE Posture Flow in ISE 2.2.

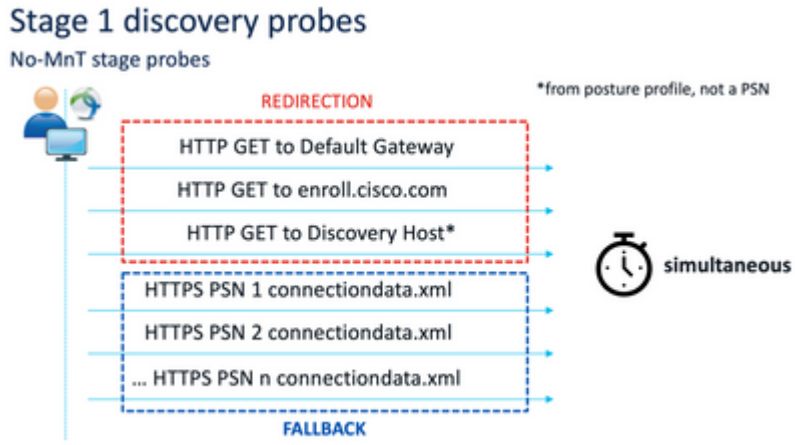
Esistono due tipi di sonde per il rilevamento della postura che non utilizzano il reindirizzamento:

1. Connectiondata.xml
2. Call Home List

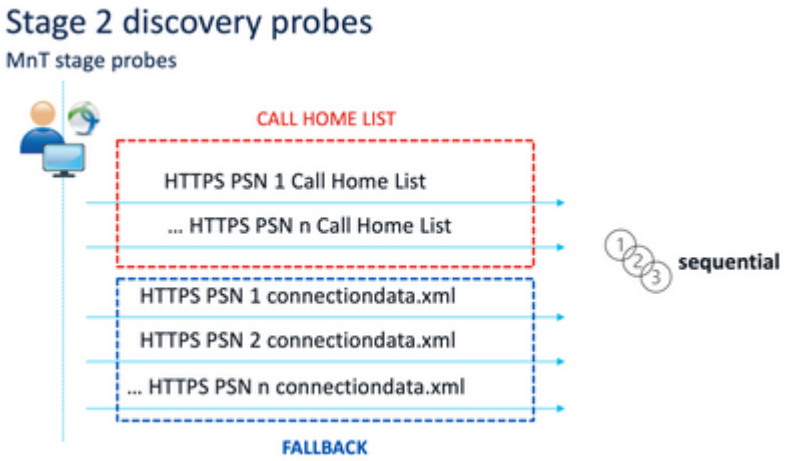
Connectiondata.xml

Connectiondata.xml è un file creato e gestito automaticamente da Cisco Secure Client. È costituito da un elenco di PSN a cui il client si è connesso in precedenza per la postura, pertanto si tratta solo di un file locale e il relativo contenuto non è persistente in tutti gli endpoint.

Lo scopo principale di connectiondata.xml è quello di fungere da meccanismo di backup per i probe di individuazione delle fasi 1 e 2. Nel caso in cui i probe di reindirizzamento o Call Home List non siano in grado di trovare un PSN con una sessione attiva, Cisco Secure Client invia una richiesta diretta a ciascuno dei server elencati in connectiondata.xml.



Probe di individuazione Fase 1



Probe di individuazione Fase 2

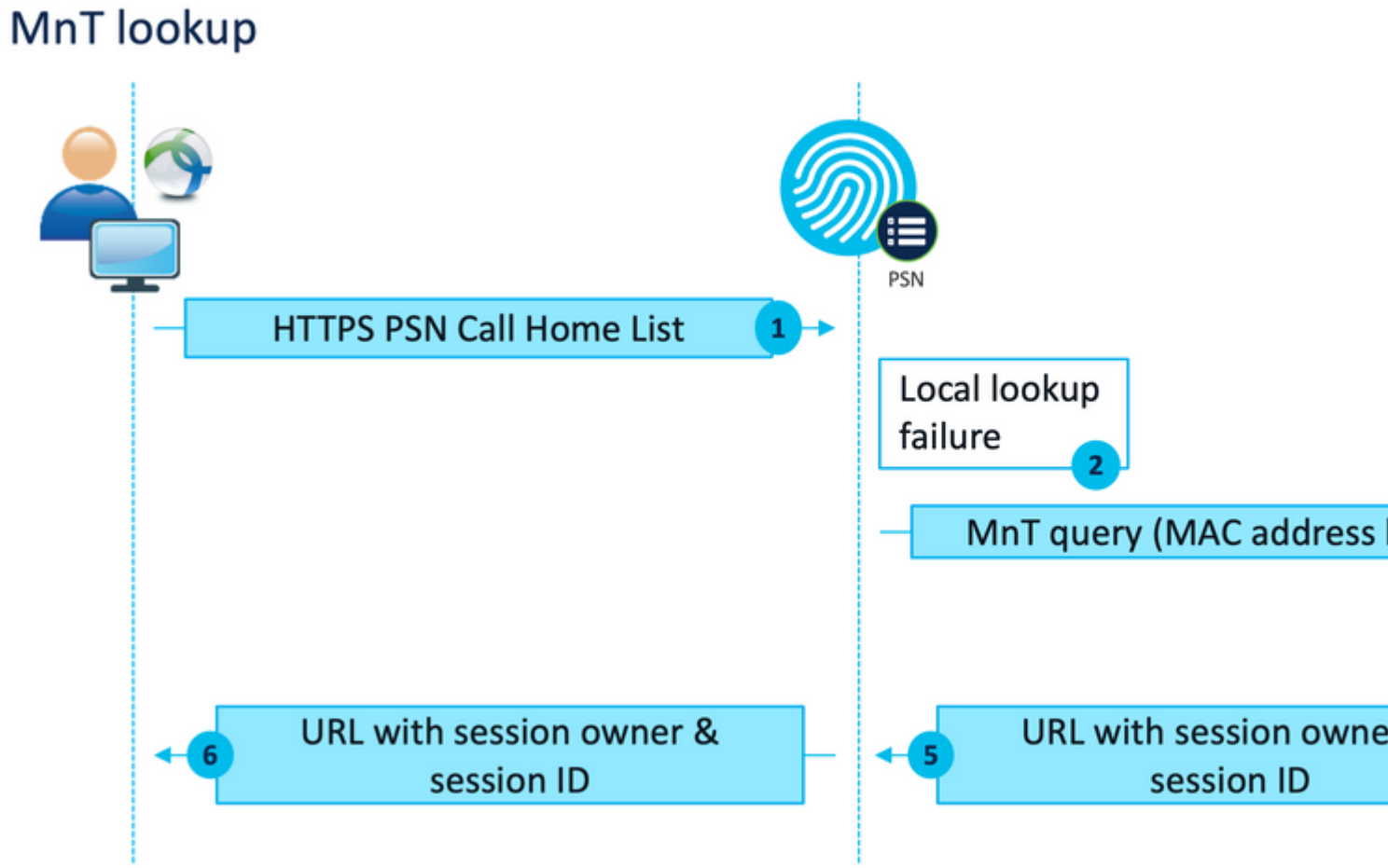
Un problema comune causato dall'uso dei probe connectiondata.xml è un sovraccarico dell'implementazione ISE dovuto a un elevato numero di richieste HTTPS inviate dagli endpoint. È importante considerare che, sebbene il file connectiondata.xml sia efficace come meccanismo di backup per evitare interruzioni complete sia per il reindirizzamento che per i meccanismi di postura senza reindirizzamento, non è una soluzione sostenibile per un ambiente di postura, pertanto è necessario diagnosticare e risolvere i problemi di progettazione e configurazione che causano il fallimento delle principali sonde di rilevamento e che determinano problemi di rilevamento.

Call Home List

Call Home List è una sezione del profilo di postura in cui è specificato un elenco di PSN da utilizzare per la postura. A differenza di connectiondata.xml, questo file viene creato e gestito da un amministratore ISE e

potrebbe richiedere una fase di progettazione per una configurazione ottimale. L'elenco di PSN nell'elenco Home chiamata deve corrispondere all'elenco dei server di autenticazione e accounting configurato nel dispositivo di rete o nel servizio di bilanciamento del carico per RADIUS.

I probe Call Home List consentono l'utilizzo di una ricerca MnT durante la ricerca di sessioni attive in caso di errore di ricerca locale in un PSN. La stessa funzionalità si estende ai probe di connectiondata.xml solo quando vengono utilizzati durante l'individuazione della Fase 2. Per questo motivo, tutte le sonde della fase 2 sono anche chiamate sonde di nuova generazione.



Flusso di ricerca MnT

Progettazione

Poiché un processo di rilevamento senza reindirizzamento spesso comporta un flusso più complesso e una quantità maggiore di elaborazione su PSN e MnT rispetto a un flusso di reindirizzamento, durante l'implementazione possono verificarsi due problemi comuni:

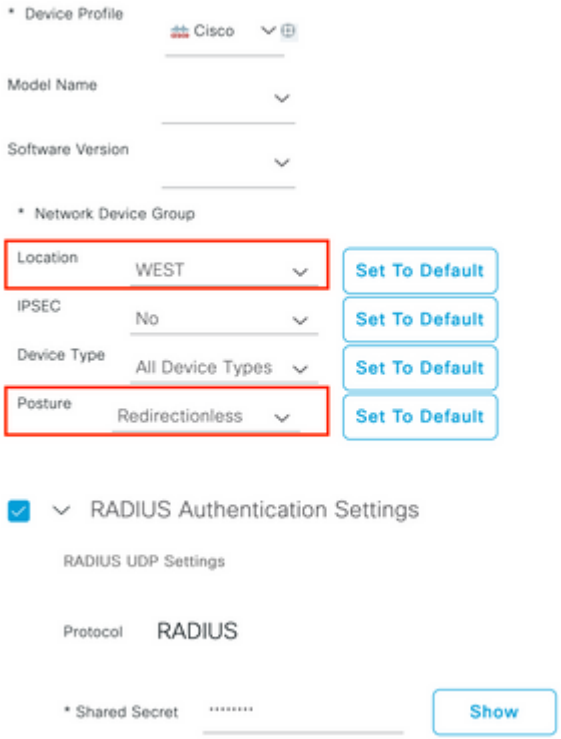
1. Rilevamento efficace
2. Prestazioni dell'implementazione ISE

Per far fronte a queste sfide, si consiglia di progettare l'elenco call home in modo da limitare il numero di PSN che un determinato endpoint può utilizzare per la postura. Per le distribuzioni di medie e grandi dimensioni, è necessario distribuire la distribuzione per creare più elenchi chiamate a domicilio con un numero ridotto di PSN. Di conseguenza, l'elenco di PSN utilizzato per l'autenticazione RADIUS per un determinato dispositivo di rete deve essere limitato allo stesso modo in modo da corrispondere all'elenco chiamate a domicilio corrispondente.

Durante lo sviluppo della strategia di distribuzione PSN per determinare il numero massimo di PSN in ogni elenco chiamate a casa, è possibile prendere in considerazione i seguenti aspetti:

- Numero di PSN nella distribuzione
- Specifiche hardware dei nodi PSN e MnT
- Numero massimo di sessioni di postura simultanee nella distribuzione
- Numero di dispositivi di rete
- Ambienti ibridi (reindirizzamento simultaneo e implementazione della postura senza reindirizzamento)
- Numero di adattatori utilizzati dagli endpoint
- Posizione dei dispositivi di rete e dei PSN
- Tipi di connessione di rete utilizzati per la postura (cablata, wireless, VPN)

2. Ad ISE, selezionare **Administration** > **Network Resources** > **Network Devices**, quindi fare clic su **Add**. Configurare i gruppi di dispositivi di rete in base alla progettazione e abilitare **le impostazioni di autenticazione RADIUS** per configurare il **segreto condiviso**.



Configurazione dispositivo di rete

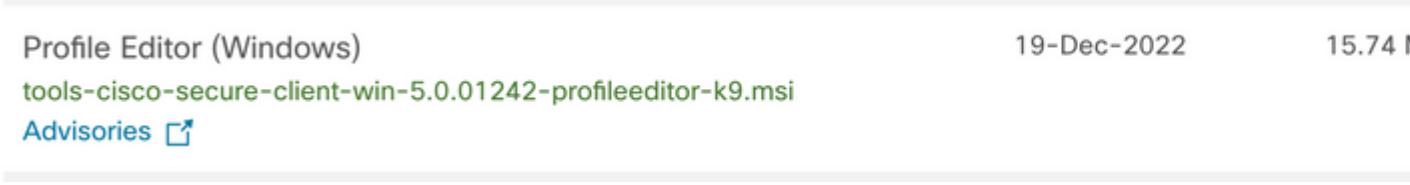
Provisioning client

Esistono due modi per fornire al client il software e il profilo appropriati per eseguire la postura in un ambiente senza reindirizzamento:

1. Provisioning manuale (pre-installazione)
2. Portale di provisioning client (distribuzione Web)

Provisioning manuale (pre-installazione)

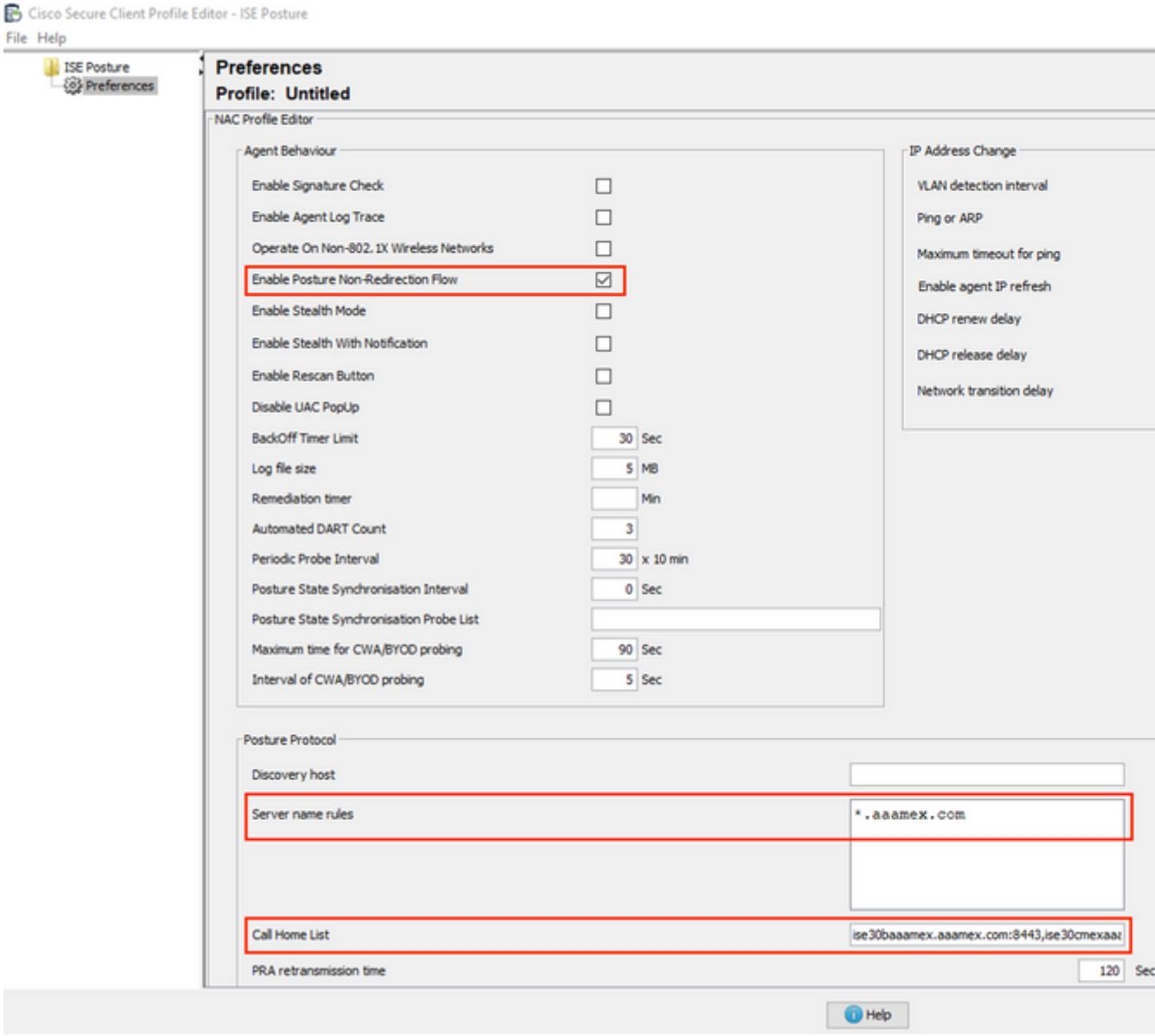
1. Scaricare e installare Cisco Secure Client Profile Editor da Cisco Software Download.



Pacchetto Editor profili

2. Aprire ISE Posture Profile Editor:
   - Verificare che l'opzione **Abilita flusso di non reindirizzamento della postura** sia abilitata.
   - Configurare le **regole dei nomi server** separate da virgole**.** Utilizzare un asterisco singolo * per consentire la connessione a qualsiasi PSN, i valori dei caratteri jolly per consentire la connessione a qualsiasi PSN in un dominio specifico o i nomi FQDN dei PSN per limitare la connessione a specifici PSN.

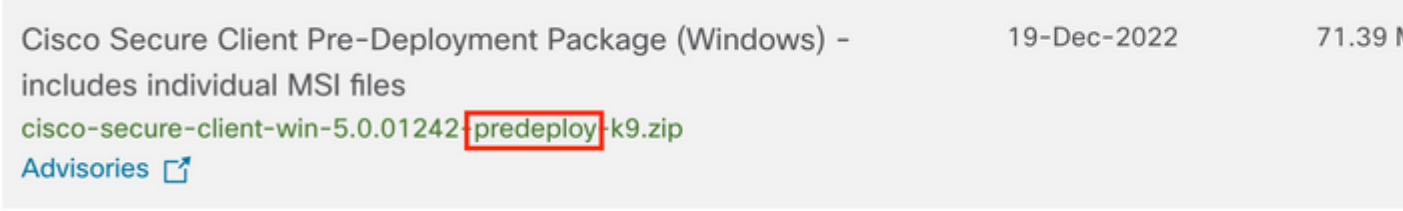
- Configurare **Call Home List** per specificare l'elenco di PSN separati da virgole. Assicurarsi di aggiungere la porta del portale di provisioning client con il formato FQDN:porta o IP:porta.



Configurazione profilo postura con Editor profili

> **Nota**: fare riferimento al passo 4 della sezione Criteri di provisioning client per istruzioni su come verificare la porta del portale di provisioning client, se necessario.

3. Ripetere il passaggio 2 per ogni elenco call home in uso.
4. Scaricare il pacchetto di pre-distribuzione di Cisco Secure Client da Cisco Software Download.



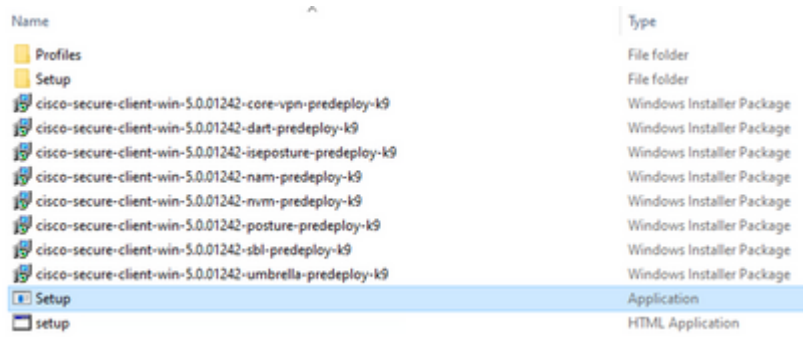
Pacchetto pre-distribuzione Cisco Secure Client

5. Salvare il profilo come ISEPostureCFG.xml.
6. Distribuire il profilo e i file di installazione in un file di archivio oppure copiare i file nei client.

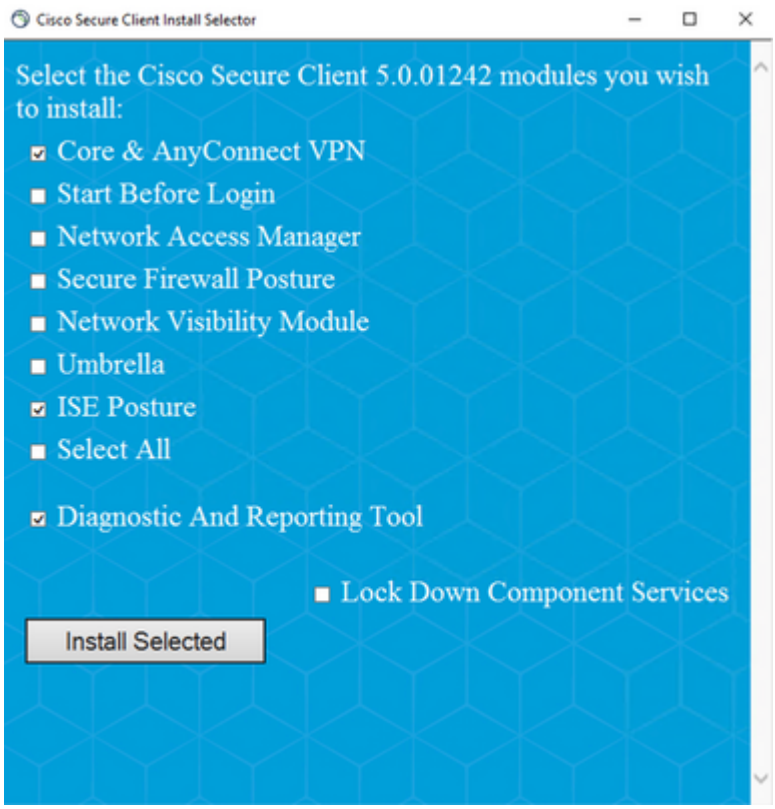
> **Avviso**: verificare che gli stessi file Cisco Secure Client si trovino anche sugli headend a cui si intende connettersi: Secure Firewall ASA, ISE, ecc. Anche quando si utilizza il provisioning manuale, ISE deve essere configurato per il provisioning del client con la versione software corrispondente. Per istruzioni dettagliate, consultare la sezione Configurazione dei criteri di provisioning del client.

---

7. Sul client, aprire il file zip in ed eseguire il programma di installazione per installare i moduli Core e ISE Posture. In alternativa, è possibile utilizzare i singoli file msi per installare ciascun modulo; in questo caso, è necessario verificare che il modulo core-vpn sia installato per primo.



Contenuto del pacchetto pre-distribuzione di Cisco Secure Client



Cisco Secure Client Installer

> **Suggerimento**: installare lo strumento di diagnostica e segnalazione da utilizzare per la

---

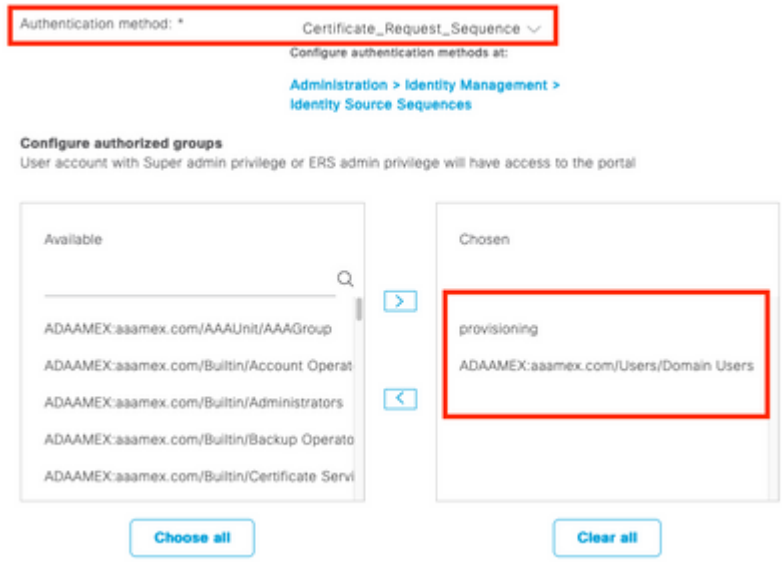
risoluzione dei problemi.

8. Al termine dell'installazione, copiare l'xml del profilo di postura nelle seguenti posizioni:
   - Windows: %ProgramData%\Cisco\Cisco Secure Client\ISE Posture
   - MacOS: /opt/cisco/secureclient/iseposture/

Portale di provisioning client (distribuzione Web)

ISE Client Provisioning Portal può essere utilizzato per installare il modulo Cisco Secure Client ISE Posture e il profilo di postura ISE. Può essere utilizzato anche per eseguire il push del profilo di postura da solo se il modulo ISE Posture è già installato sul client.

1. Passare a **Work Center** > **Posture** > **Client Provisioning** > **Client Provisioning** Portal per aprire la configurazione del portale. Espandere la sezione **Impostazioni portale** e individuare il campo **Metodo di autenticazione**, quindi selezionare la **sequenza di origine identità** da utilizzare per l'autenticazione nel portale.
2. Configurare i gruppi di identità interni ed esterni autorizzati a utilizzare il portale di provisioning client.



Metodo di autenticazione e gruppi autorizzati nelle impostazioni del portale

3. Nel campo **Nome di dominio completo (FQDN)** configurare l'URL utilizzato dai client per accedere al portale. Per configurare più FQDN, immettere i valori separati da virgole.

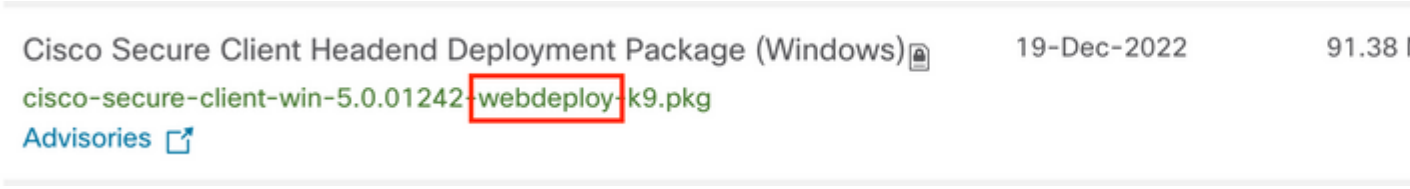
4. Configurare i server DNS per risolvere l'URL del portale nei PSN del corrispondente elenco chiamate a casa.
5. Fornire l'FQDN agli utenti finali per accedere al portale e installare il software ISE Posture.

Nota: per utilizzare l'FQDN del portale, i client devono disporre della catena di certificati Amministratore PSN e della catena di certificati del portale installati nell'archivio attendibile e il certificato Amministratore deve contenere l'FQDN del portale nel campo SAN.

Criteri di provisioning client

Il provisioning client deve essere configurato su ISE indipendentemente dal tipo di provisioning (pre-distribuzione o distribuzione Web) utilizzato per installare Cisco Secure Client sugli endpoint.

1. Scaricare il pacchetto Cisco Secure Client webdeploy da Cisco Software Download.

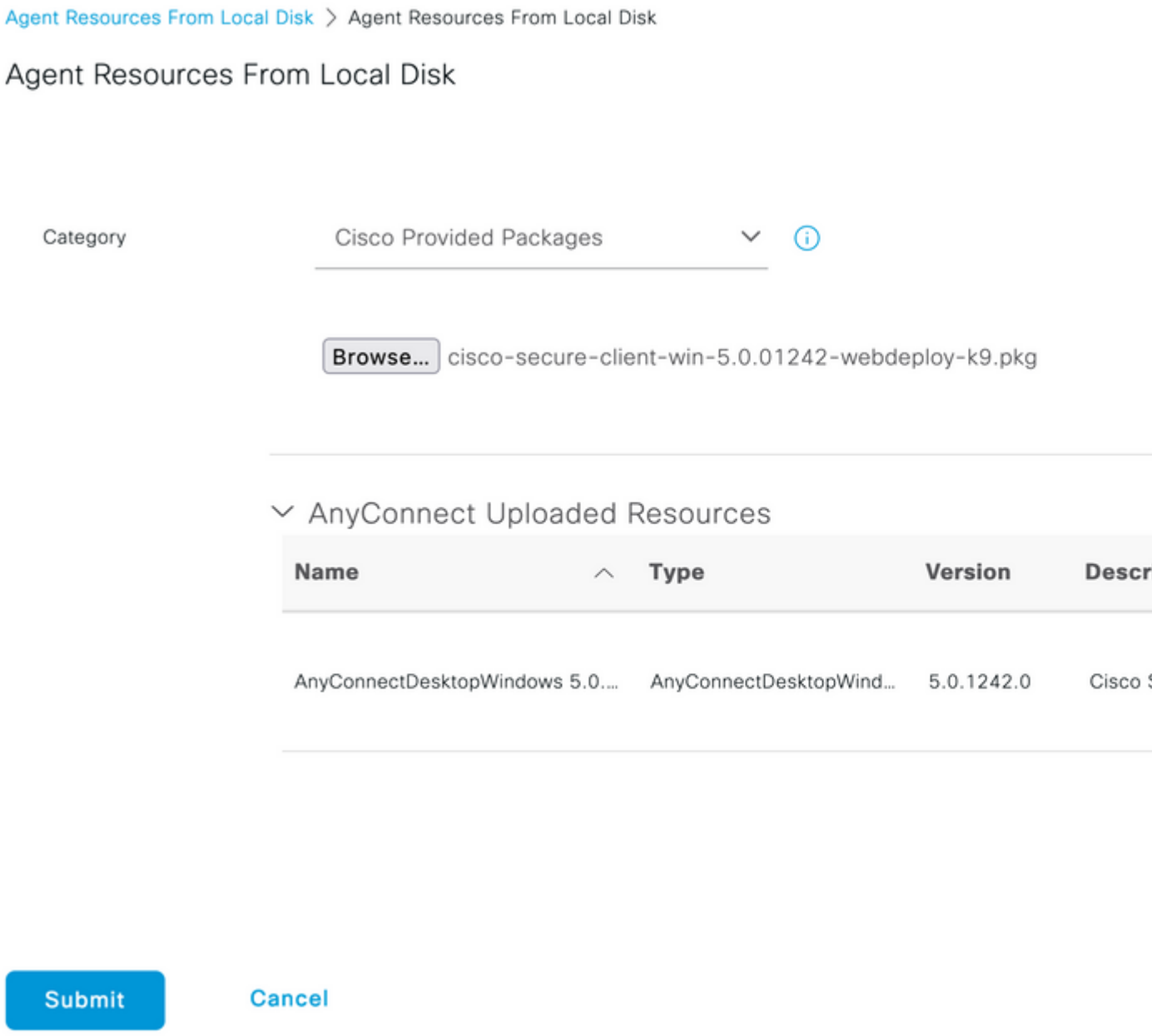


Pacchetto Cisco Secure Client WebDeployment

2. Scarica l'ultimo pacchetto di distribuzione Web del Modulo di conformità da Download del software Cisco.

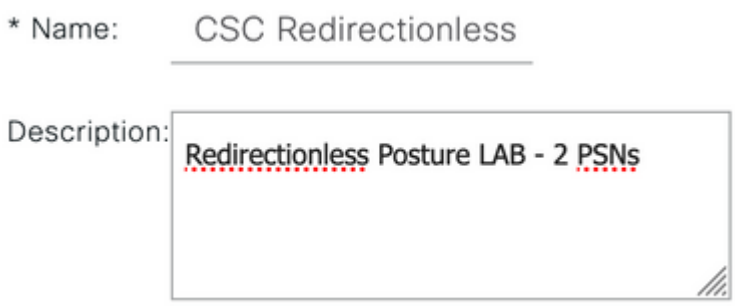
Pacchetto WebDeployment di ISE Compliance Module

3. Ad ISE, selezionare Work Center > Posture > Client Provisioning > **Resources** e fare clic su **Add** > **Agent resources from local disk**. Selezionare **Cisco Provided Packages** dal menu a discesa Category (Categoria) e caricare il pacchetto Cisco Secure Client webdeploy precedentemente scaricato. Ripetere la stessa procedura per caricare il Modulo di conformità.



Carica i pacchetti forniti da Cisco a ISE

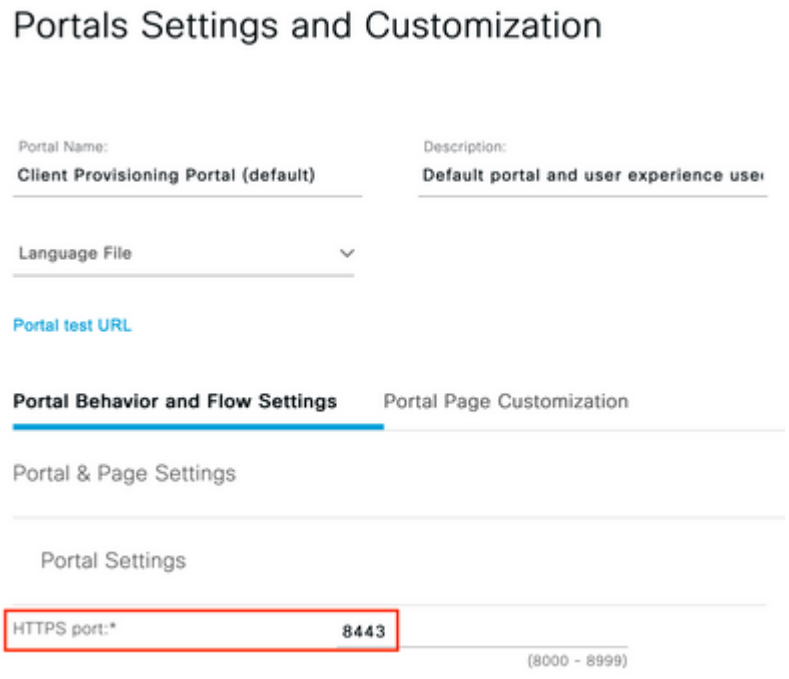
4. Tornando alla scheda **Risorse**, fare clic su **Aggiungi** > **Profilo postura di AnyConnect**. Nel profilo:
   - Configurare un **nome** che possa essere utilizzato per identificare il profilo all'interno di ISE.
   - Configurare le **regole dei nomi server** separate da virgole**.** Utilizzare un asterisco singolo * per consentire la connessione a qualsiasi PSN, i valori dei caratteri jolly per consentire la connessione a qualsiasi PSN in un dominio specifico o i nomi FQDN dei PSN per limitare la connessione a specifici PSN.
   - Configurare **Call Home List** per specificare l'elenco di PSN separati da virgole. Assicurarsi di aggiungere la porta del portale di provisioning client utilizzando il formato FQDN:porta o IP:porta.



Configurazione profilo ISE Posture I

ISE Posture Profile, configurazione II

Per trovare la porta da utilizzare nell'elenco Call Home, passare a **Centri di lavoro** > **Postura** > **Provisioning client** > **Portale di provisioning client**, selezionare il portale in uso ed espandere Impostazioni portale.



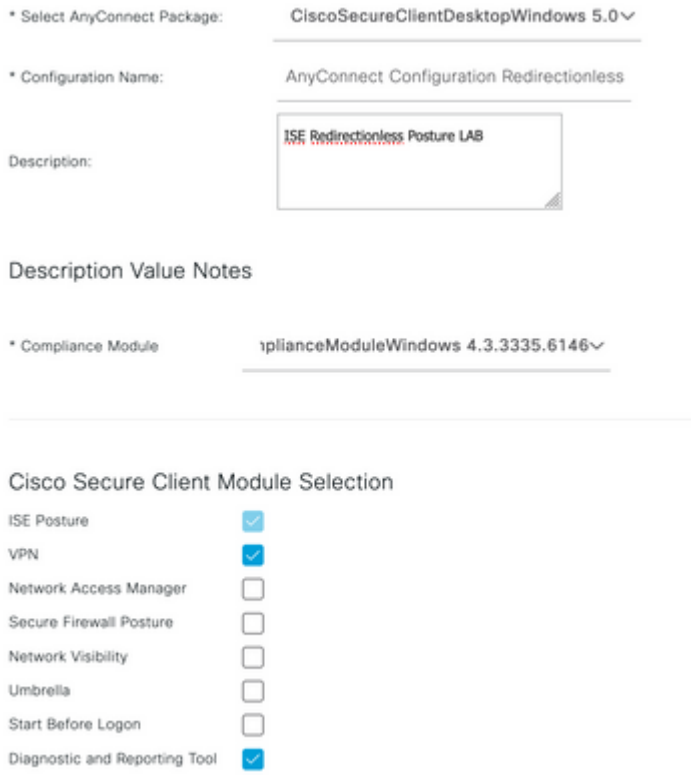
Porta del portale di provisioning client

5. Nella scheda **Risorse**, fare clic su **Aggiungi** > **Configurazione di AnyConnect**. Selezionare il pacchetto Cisco Secure Client e il modulo di conformità da utilizzare.

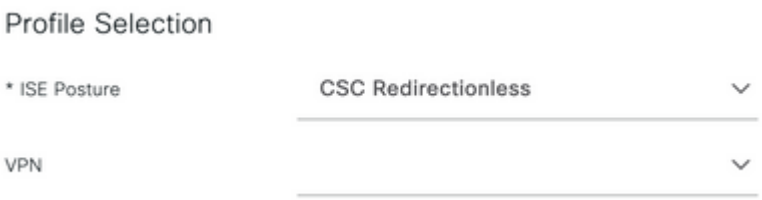
> **Avviso**: se Cisco Secure Client è stato pre-distribuito ai client, verificare che la versione su ISE corrisponda alla versione sugli endpoint. Se per la distribuzione Web si usa ASA o FTD, anche la versione sul dispositivo deve corrispondere.

---

6. Scorrete verso il basso fino alla sezione **Selezione postura (Posture Selection)** e selezionate il profilo creato al passo 1. Fare clic su **Submit** (Invia) in fondo alla pagina per salvare la configurazione.



Configurazione AnyConnect



Selezione profilo

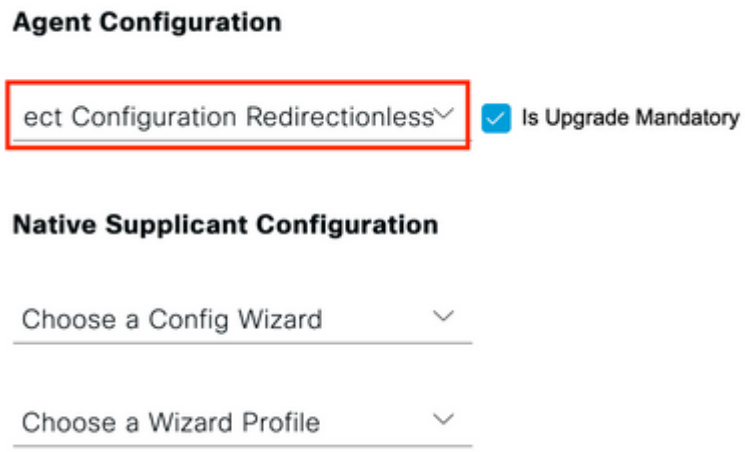
7. Passare a **Centri di lavoro** > **Postura** > **Provisioning client** > **Criteri di provisioning client**. Individuare il criterio utilizzato per il sistema operativo richiesto e fare clic su **Modifica**. Fare clic sul segno **+** nella colonna **Risultati** e selezionare la configurazione AnyConnect dal passaggio 5 nella sezione **Configurazione agente**.

> **Nota**: in caso di più elenchi chiamate a domicilio, utilizzare il campo **Altre condizioni** per inviare il profilo corretto ai client corrispondenti. Nell'esempio, il gruppo di posizione del

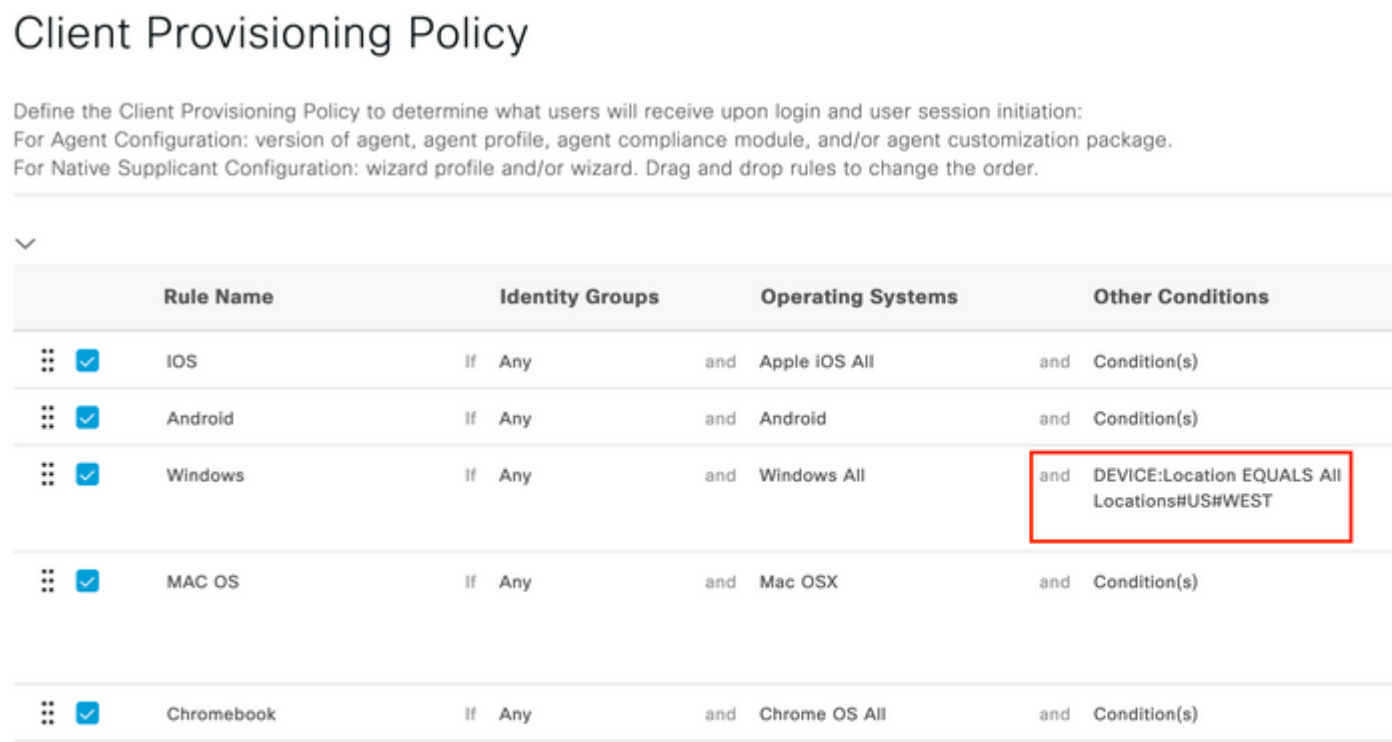
---

dispositivo viene utilizzato per identificare il profilo di postura sottoposto a push nel criterio.

Suggerimento: se per lo stesso sistema operativo sono configurati più criteri di provisioning client, è consigliabile escluderli a vicenda, ovvero un determinato client dovrebbe essere in grado di eseguire un solo criterio alla volta. Gli attributi RADIUS possono essere utilizzati nella colonna **Altre condizioni** per distinguere un criterio da un altro.



Configurazione agente criteri di provisioning client



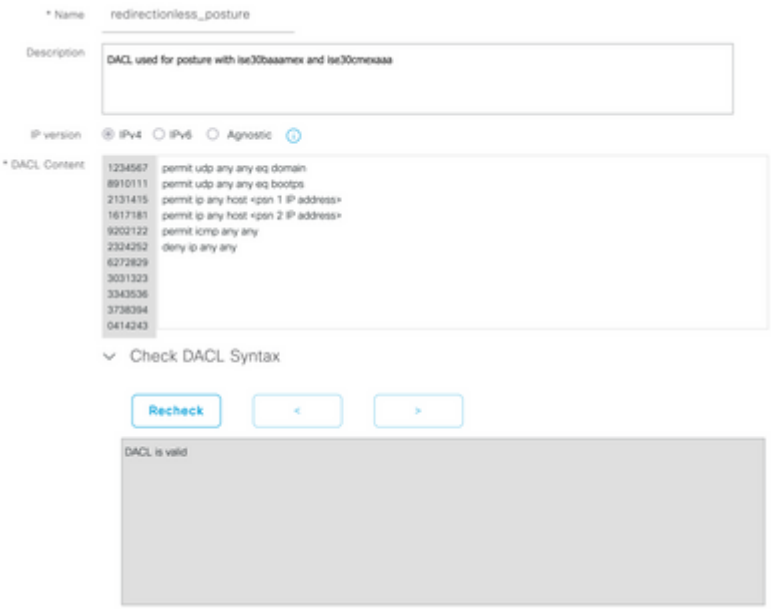
Criterio di provisioning client

8. Ripetere i passaggi da 4 a 7 per ogni Call Home List e profilo di postura corrispondente in uso. Per gli ambienti ibridi, è possibile utilizzare gli stessi profili per i client di reindirizzamento.

Authorization

Profilo di autorizzazione

1. Selezionare Policy > Policy Elements > Results > **Authorization** > **Downloadable ACLs (Criterio > Elementi criteri** > Risultati > **Autorizzazione** > **ACL scaricabili)** e fare clic su **Add**.
2. Creare un DACL per consentire il traffico verso DNS, DHCP (se utilizzato), ISE PSN e bloccare altro traffico. Accertarsi di autorizzare tutto il traffico necessario per l'accesso prima di ottenere l'accesso conforme.



Configurazione DACL

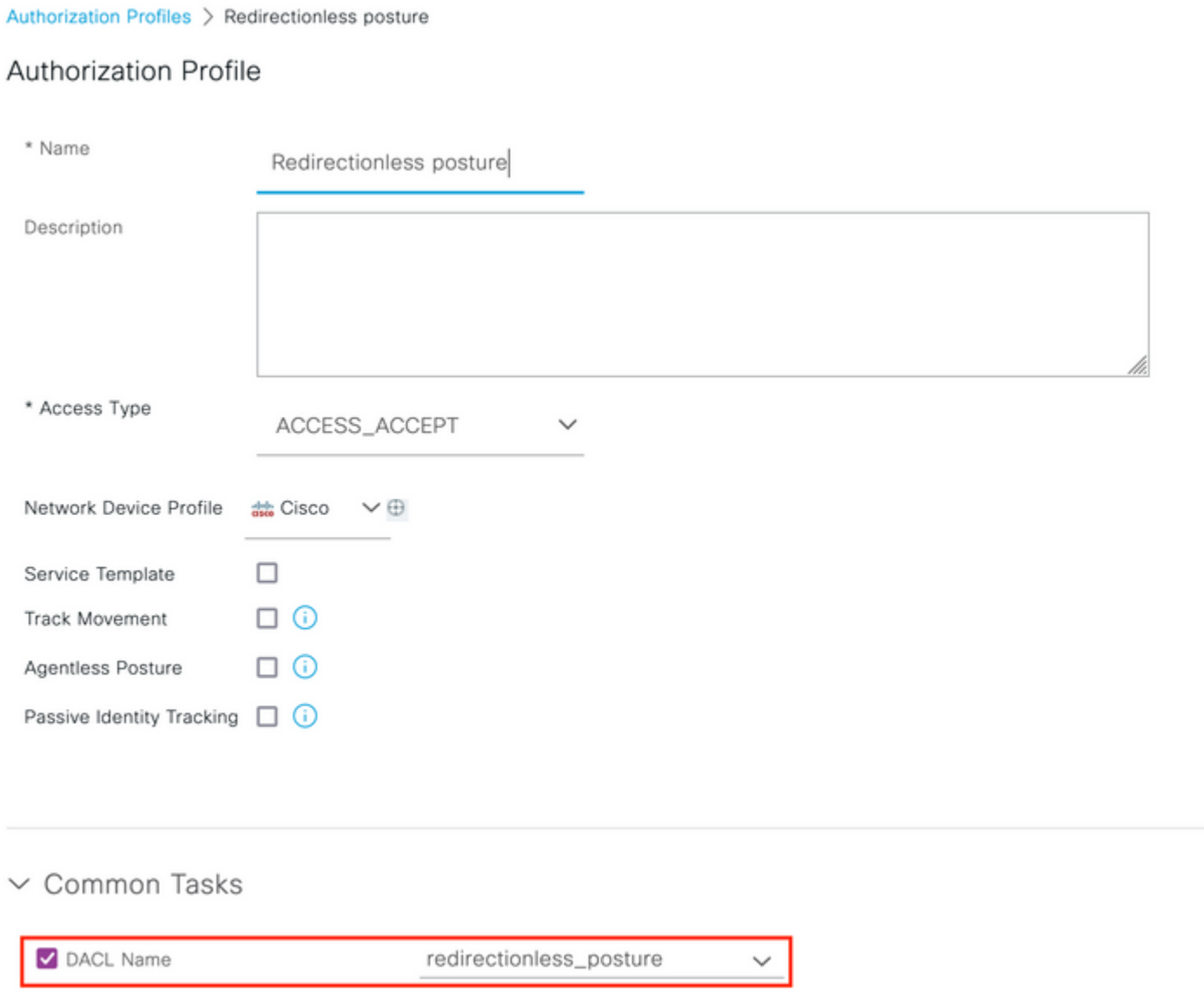
permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

permit ip any host

deny ip any any

Attenzione: alcuni dispositivi di terze parti potrebbero non supportare DACL, in questi casi è necessario utilizzare un Filter-ID o altri attributi specifici del fornitore. Per ulteriori informazioni, consultare la documentazione del fornitore. Se non si usano gli ACL, configurare l'ACL corrispondente nel dispositivo di rete.

3. Passare a Criterio > Elementi criterio > Risultati > **Autorizzazione** >**Profili autorizzazione** e fare clic su **Aggiungi**. Assegnare un nome al profilo di autorizzazione e selezionare **Nome DACL** da **Attività comuni.** Dal menu a discesa, selezionare il DACL creato al punto 2.



Profilo di autorizzazione

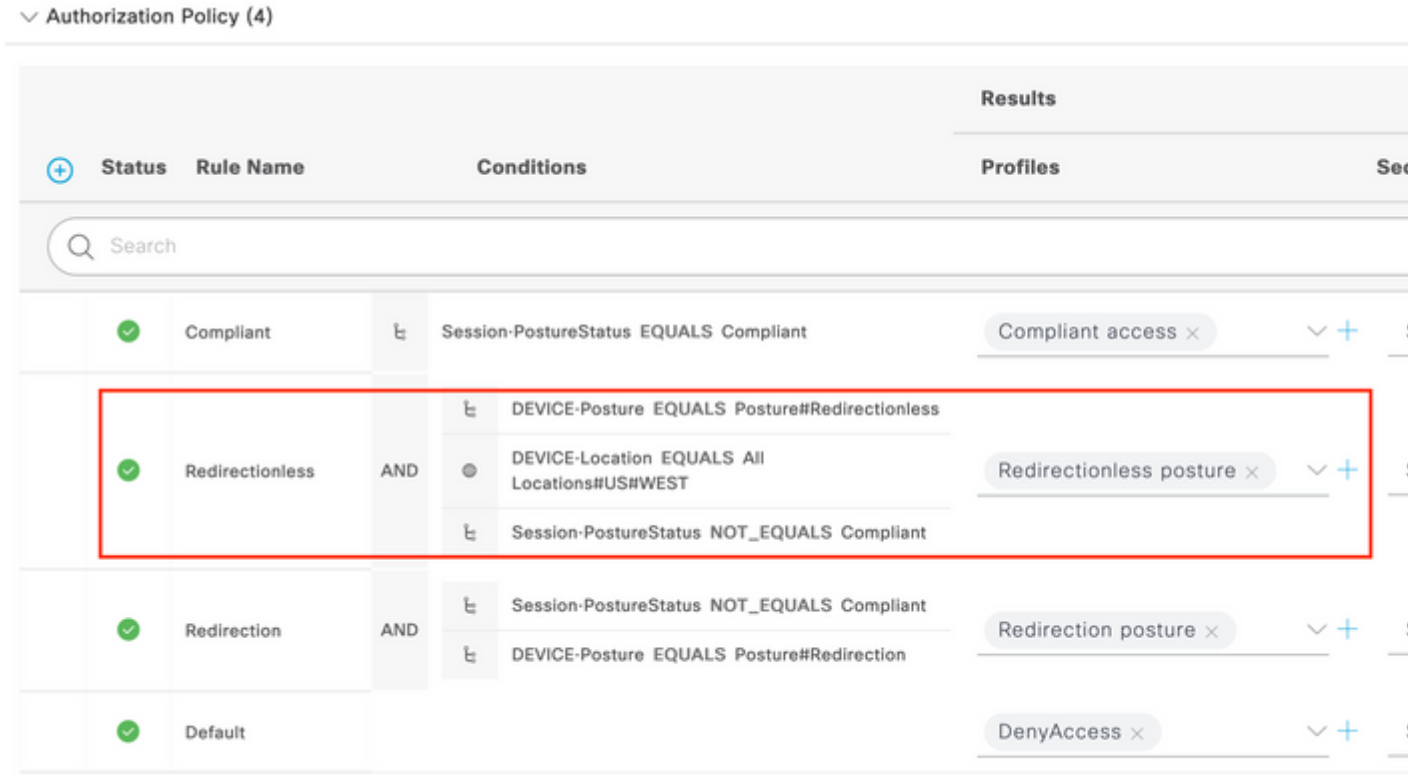
Nota: se non si utilizzano gli ACL, utilizzare **Filter-ID** da **Common Tasks** o da **Advanced Attribute Settings** per eseguire il push del nome ACL corrispondente.

4. Ripetere i passaggi da 1 a 3 per ogni elenco call home in uso. Per gli ambienti ibridi, è necessario un

solo profilo di autorizzazione per il reindirizzamento. La configurazione del profilo di autorizzazione per il reindirizzamento esula dall'ambito di questo documento.

Criteri di autorizzazione

1. Passare a **Criterio** > **Set di criteri** e aprire il set di criteri in uso o crearne uno nuovo.
2. Scorrere verso il basso fino alla sezione **Criteri di autorizzazione**. Creare un criterio di autorizzazione utilizzando **Session PostureStatus NOT_EQUALS Compliant** e selezionare il profilo di autorizzazione creato nella sezione precedente.



Criteri di autorizzazione

3. Ripetere il passaggio 2 per ogni profilo di autorizzazione con l'elenco chiamate a casa corrispondente in uso. Per gli ambienti ibridi, è necessaria una sola regola di autorizzazione per il reindirizzamento.

Risoluzione dei problemi

Conforme su Cisco Secure Client e postura Non applicabile (in sospeso) su ISE

Sessioni non aggiornate/fantasma

La presenza di sessioni obsolete o fantasma nella distribuzione può generare errori intermittenti e apparentemente casuali con il rilevamento della postura senza reindirizzamento, che determinano il blocco degli utenti in un accesso di postura sconosciuta/non applicabile su ISE, mentre l'interfaccia utente di Cisco Secure Client mostra un accesso conforme.

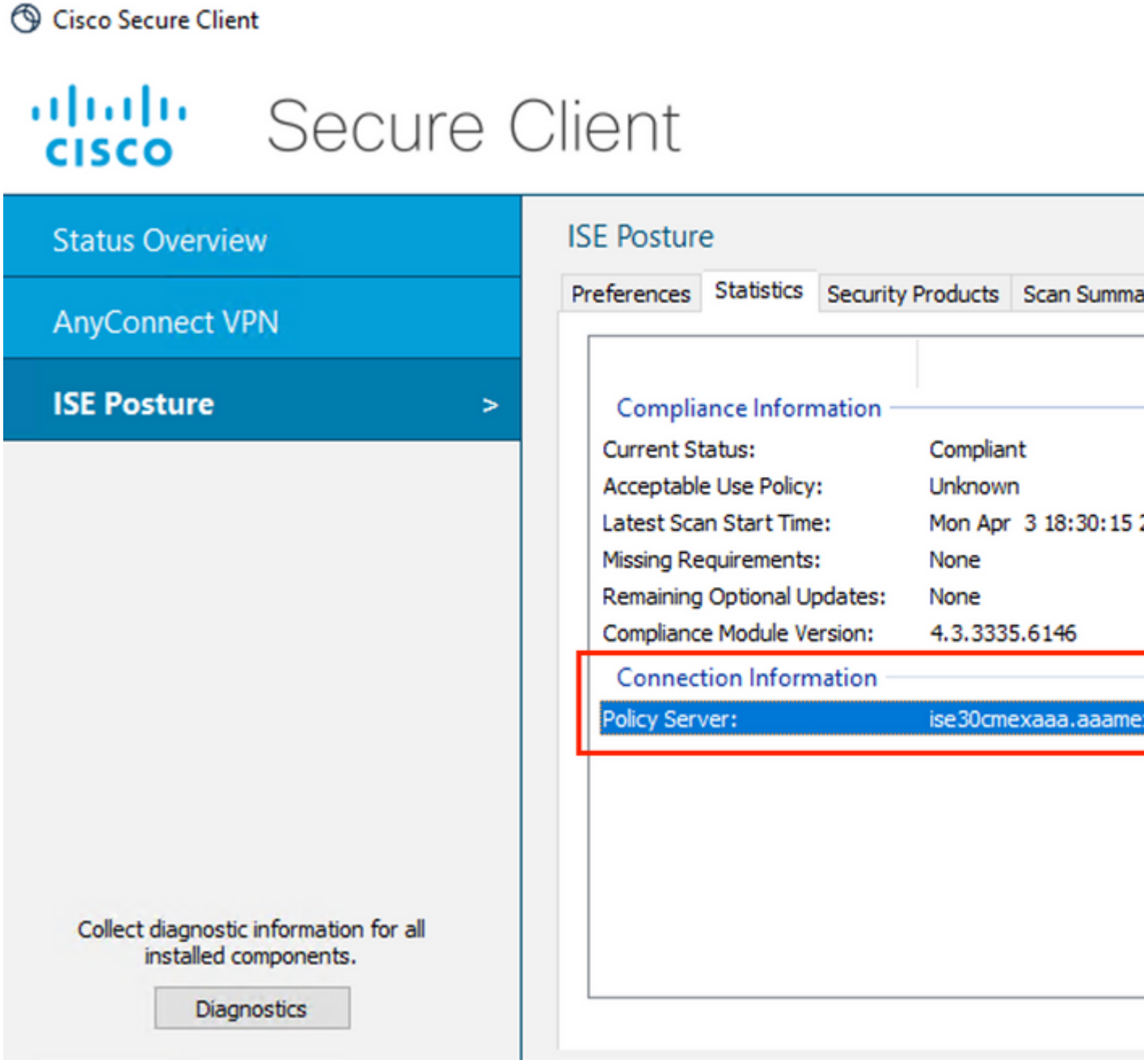
Le sessioni obsolete sono sessioni obsolete che non sono più attive. Vengono creati da una richiesta di autenticazione e dall'avvio dell'accounting, ma non viene ricevuta alcuna interruzione dell'accounting nel PSN per cancellare la sessione.

Le sessioni fantasma sono sessioni che non sono mai state effettivamente attive in un particolare PSN. Vengono creati da un aggiornamento temporaneo di accounting, ma non viene ricevuto alcun arresto di accounting nel PSN per cancellare la sessione.

Identificazione

Per identificare un problema di sessione non aggiornata/fantasma, verificare il PSN utilizzato nell'analisi del sistema sul client e confrontarlo con il PSN che esegue l'autenticazione:

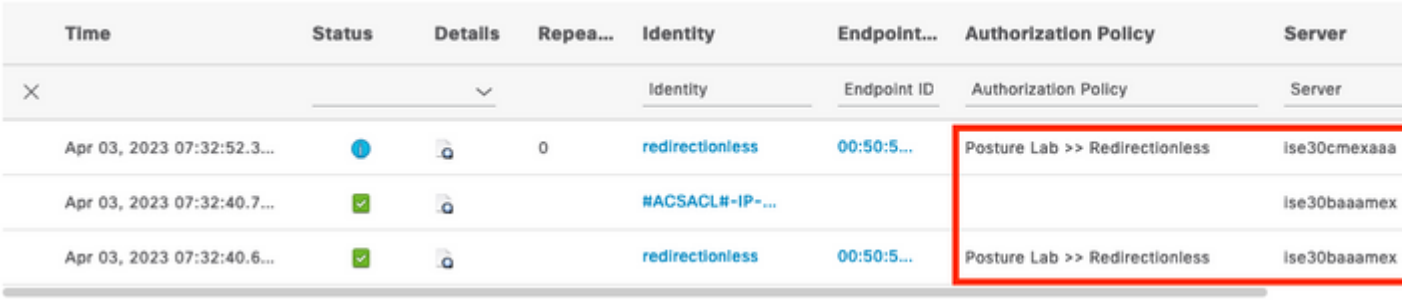
1. Nell'interfaccia utente di Cisco Secure Client, fare clic sull'**icona gear** nell'angolo in basso a sinistra. Dal menu a sinistra, aprire la sezione **ISE Posture** e passare alla scheda **Statistics** (Statistiche). Prendere nota di Policy Server in Informazioni connessione.



Policy Server per ISE Posture in Cisco Secure Client

2. Nei log live di ISE RADIUS, tenere presente quanto segue:

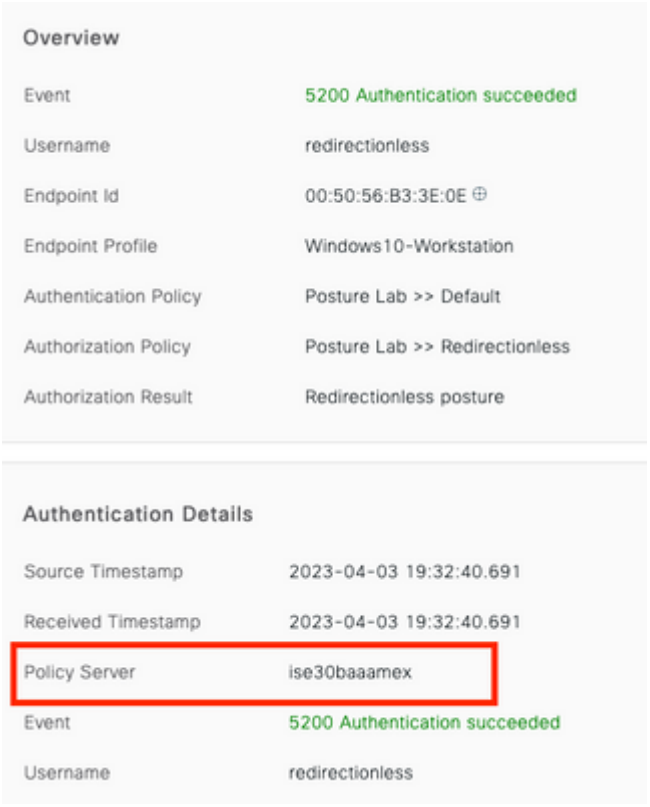
- Modifica nello stato della postura
- Modifica nel server
- Nessuna modifica nei criteri di autorizzazione e nel profilo di autorizzazione
- Nessun registro CoA attivo



Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server
				Identity	Endpoint ID	Authorization Policy	Server
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baaamex
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baaamex

Registri attivi per sessioni obsolete/fantasma

3. Aprire la sessione attiva o i dettagli del log di ultima autenticazione. Prendere nota di Policy Server, se si differenzia dal server osservato nel passaggio 1, indica un problema con sessioni non aggiornate/fantasma.



Overview

Event	5200 Authentication succeeded
Username	redirectionless
Endpoint Id	00:50:56:B3:3E:0E
Endpoint Profile	Windows10-Workstation
Authentication Policy	Posture Lab >> Default
Authorization Policy	Posture Lab >> Redirectionless
Authorization Result	Redirectionless posture

Authentication Details

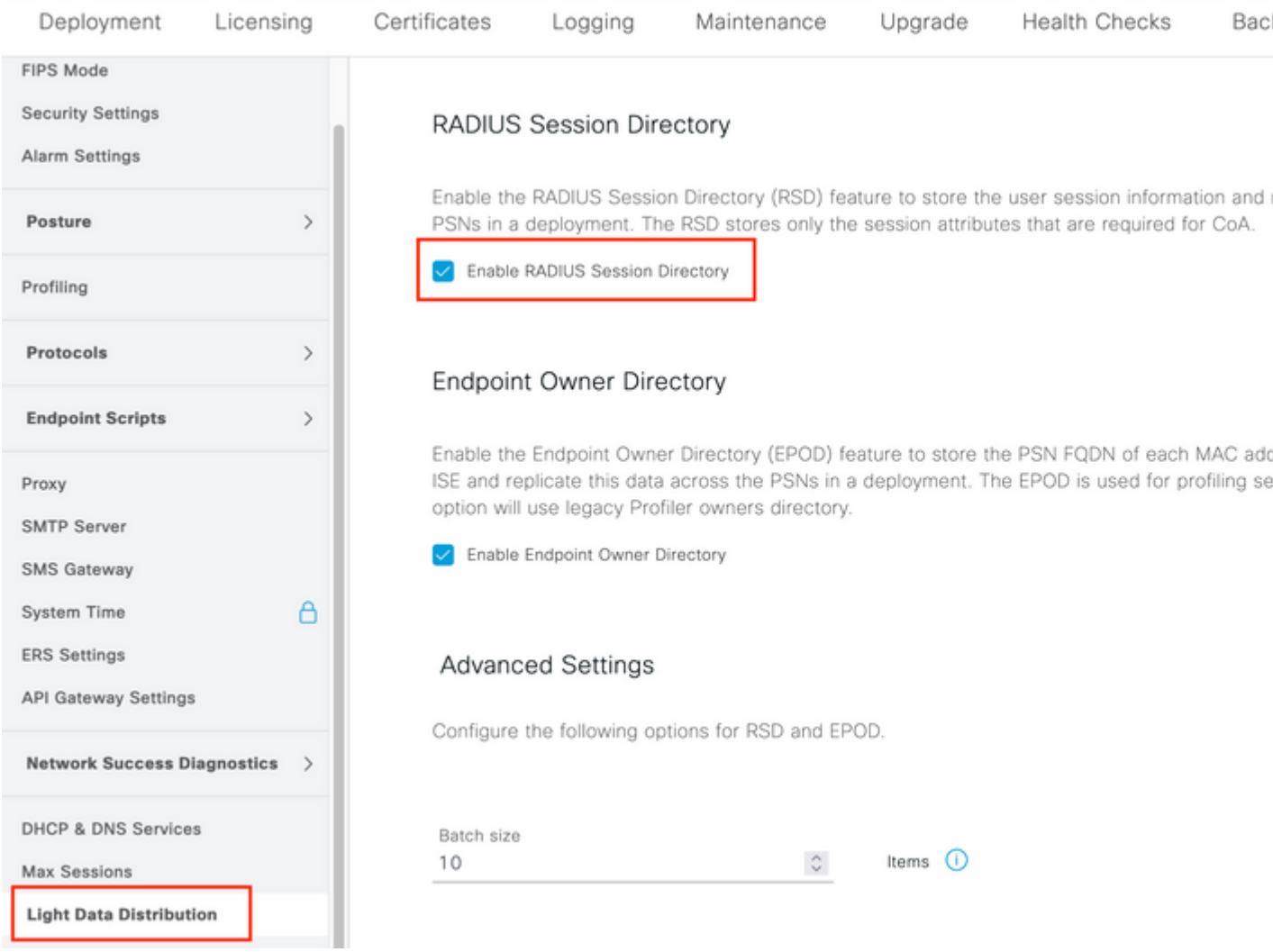
Source Timestamp	2023-04-03 19:32:40.691
Received Timestamp	2023-04-03 19:32:40.691
Policy Server	ise30baaamex
Event	5200 Authentication succeeded
Username	redirectionless

Dettagli del server dei criteri nel registro attivo

Soluzione

Le versioni ISE superiori a ISE 2.6 patch 6 e 2.7 patch 3 implementano RADIUS Session Directory come soluzione per scenari di sessioni obsolete/fantasma in un flusso di postura senza reindirizzamento.

1. Passare a Amministrazione > **Sistema** > **Impostazioni** > **Distribuzione dati luce** e verificare che la casella di controllo **Abilita directory di sessione RADIUS** sia abilitata.



Abilita directory di sessione RADIUS

2. Dalla CLI di ISE verificare che **ISE Messaging Service** sia in esecuzione su **tutti i PSN** eseguendo il comando **mostra aumento stato applicazioni.**

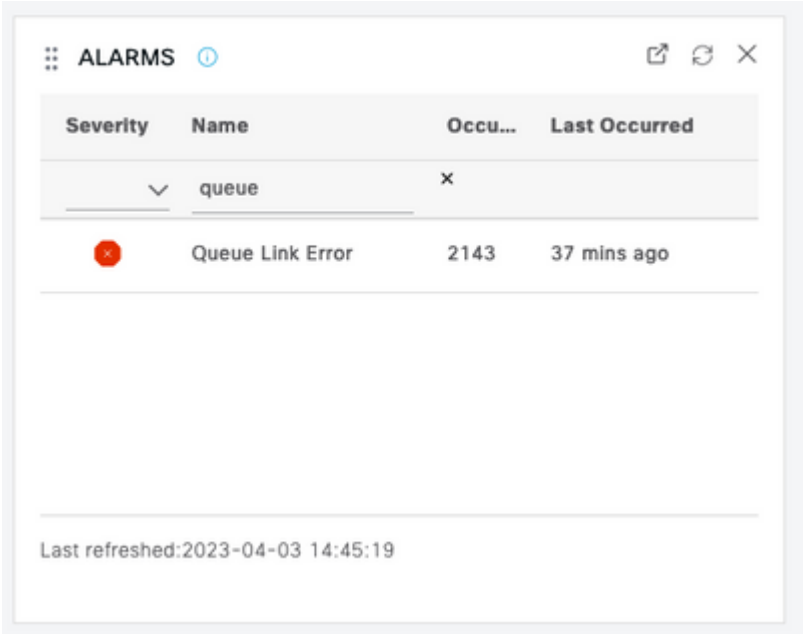
```
ise30cmexaaa/admin# show application status ise

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
```

Servizio di messaggistica ISE in esecuzione

> **Nota**: questo servizio fa riferimento al metodo di comunicazione utilizzato per RSD tra PSN e deve essere in esecuzione indipendentemente dallo stato dell'impostazione del servizio di messaggistica ISE per syslog che può essere impostata dall'interfaccia utente ISE.

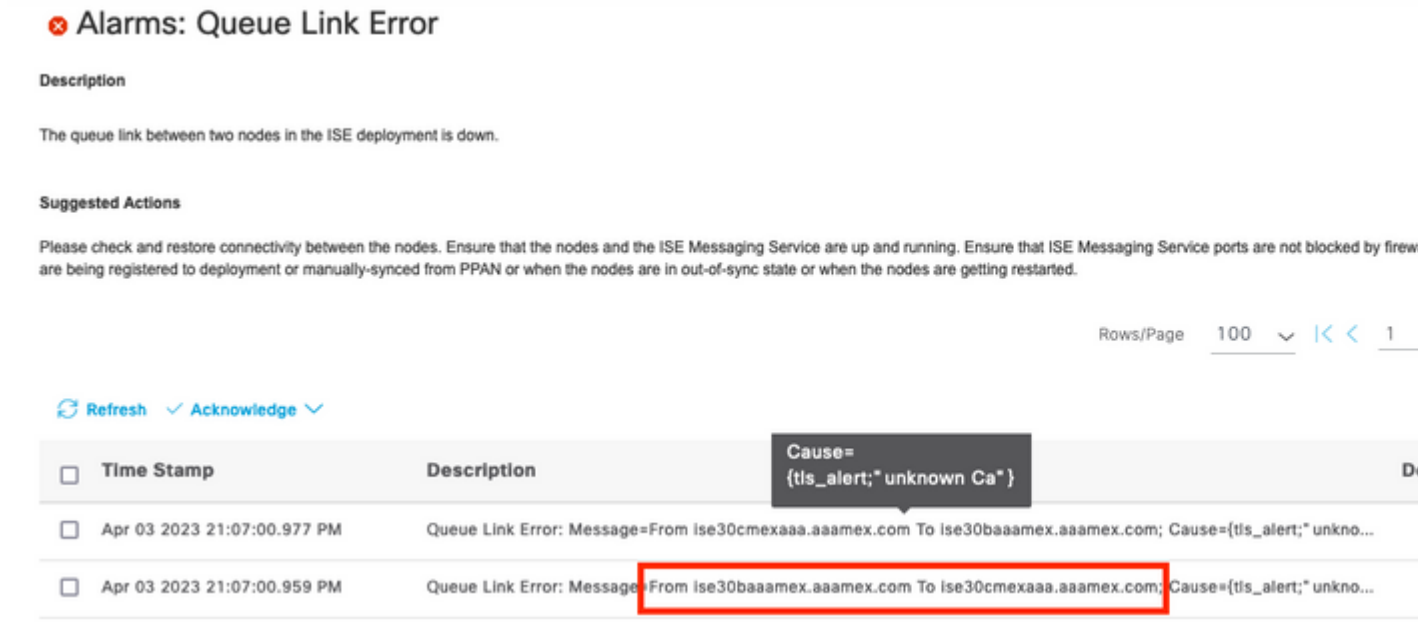
---

3. Passare a ISE **Dashboard** e individuare la dashlet **Alarms**. Verificare se sono presenti avvisi di **errore collegamento coda**. Fare clic sul nome dell'allarme per visualizzare ulteriori dettagli.



Avvisi errori collegamento coda

4. Verificare se gli allarmi vengono generati tra i PSN utilizzati per la postura.



Dettagli avviso di errore collegamento coda

5. Posizionare il puntatore del mouse sulla descrizione dell'allarme per visualizzare i dettagli completi e prendere nota del campo Causa. Le due cause più comuni dell'errore di collegamento alla coda sono:
   - Timeout: indica che le richieste inviate da un nodo a un altro nodo sulla porta 8671 non ricevono risposta entro la soglia. Per risolvere il problema, verificare che la porta TCP 8671 sia consentita tra i nodi.
   - CA sconosciuta: indica che la catena di certificati che firma il certificato di messaggistica ISE non è valida o è incompleta. Per correggere l'errore:
     a. Passare a **Amministrazione** > **Sistema** > **Certificati** > **Richieste di firma certificato**.
     b. Fare clic su **Generate Certificate Signing Requests (CSR)**.
     c. Dal menu a discesa selezionare **ISE Root CA** e fare clic su **Sostituisci catena di certificati ISE Root CA**.
     Se ISE Root CA non è disponibile, selezionare **Certificate Authority** > **Internal CA settings** (CA interna), fare clic su **Enable Certificate Authority** (Abilita CA radice), quindi tornare al CSR e rigenerare la CA radice.
     d. Generare un nuovo CSR e selezionare **ISE Messaging Service** dal menu a discesa.
     e. Selezionare tutti i nodi dalla distribuzione e rigenerare il certificato.

Nota: durante la rigenerazione dei certificati è previsto il rilevamento degli allarmi di errore del collegamento di coda con causa CA sconosciuta o Econnjected. Dopo la generazione del certificato, controllare gli allarmi per verificare che il problema sia stato risolto.

Prestazioni

Identificazione

Problemi di prestazioni quali l'utilizzo elevato della CPU e il carico medio elevato relativo alla postura senza reindirizzamento possono influire sul PSN e sui nodi MnT e sono spesso accompagnati o preceduti dai seguenti eventi:

- Casuale o intermittente *Nessun server dei criteri ha rilevato* errori in Cisco Secure Client
- *Il limite massimo di risorse ha raggiunto* i rapporti per il *pool di thread del servizio portale e ha raggiunto* gli eventi del *valore di soglia*. Passare a Operazioni > **Rapporti** > **Rapporti** > **Audit** > **Audit operazioni** per visualizzare i rapporti.

- Allarmi *elevati per la ricerca da query di postura a MNT*. Questi allarmi sono generati solo su ISE versione 3.1 e successive.

Soluzione

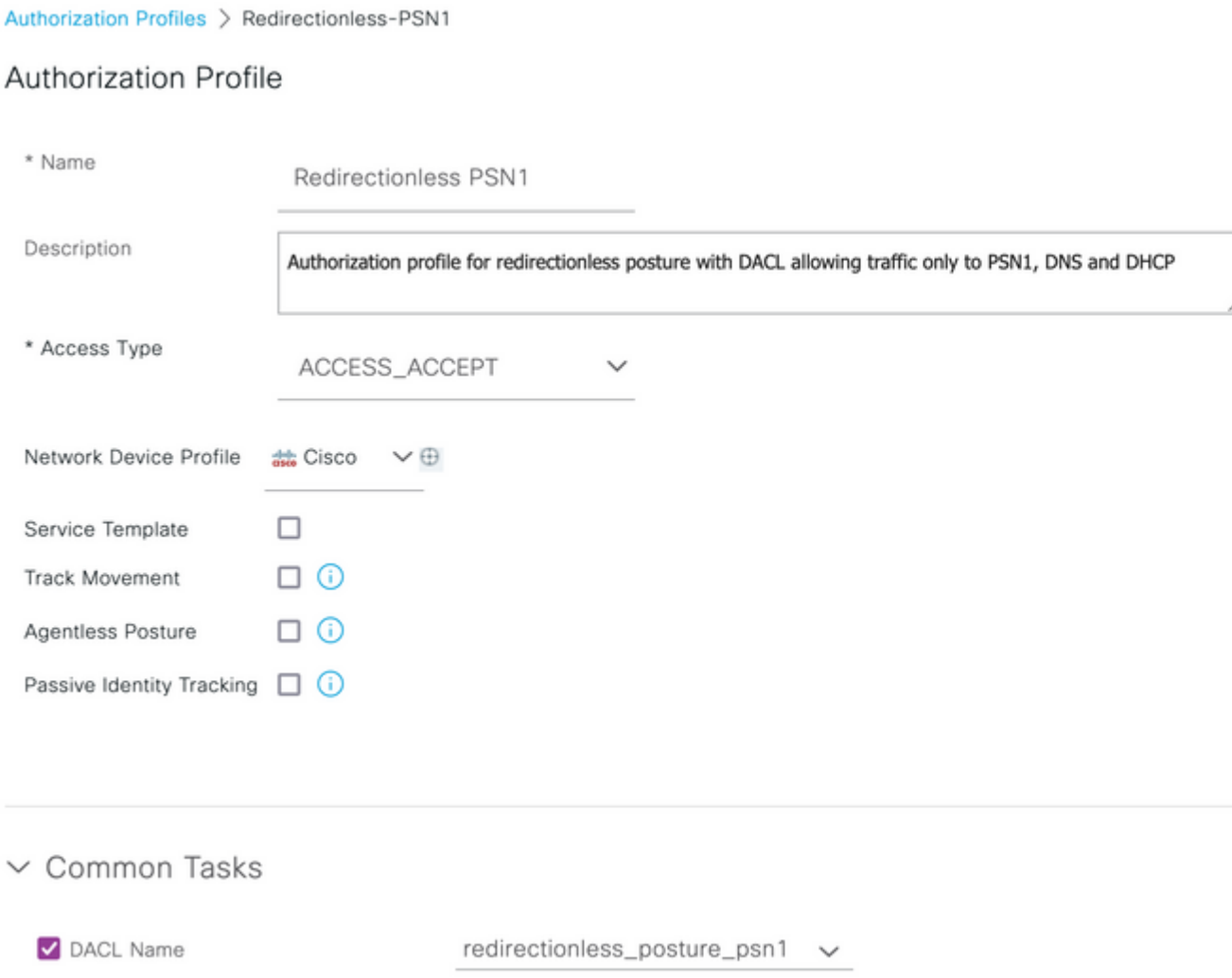
Se le prestazioni dell'installazione sono influenzate dalla postura senza reindirizzamento, ciò indica spesso un'implementazione inefficace. Si raccomanda di rivedere i seguenti aspetti:

- Numero di nomi di servizio (PSN) utilizzati per elenco chiamate iniziali. Valutare la possibilità di ridurre il numero di PSN utilizzabili per la postura per endpoint o dispositivo di rete in base alla progettazione.
- Porta del portale di provisioning client in Call Home List. Verificare che il numero di porta del portale sia incluso dopo l'IP o il nome di dominio completo di ogni nodo.

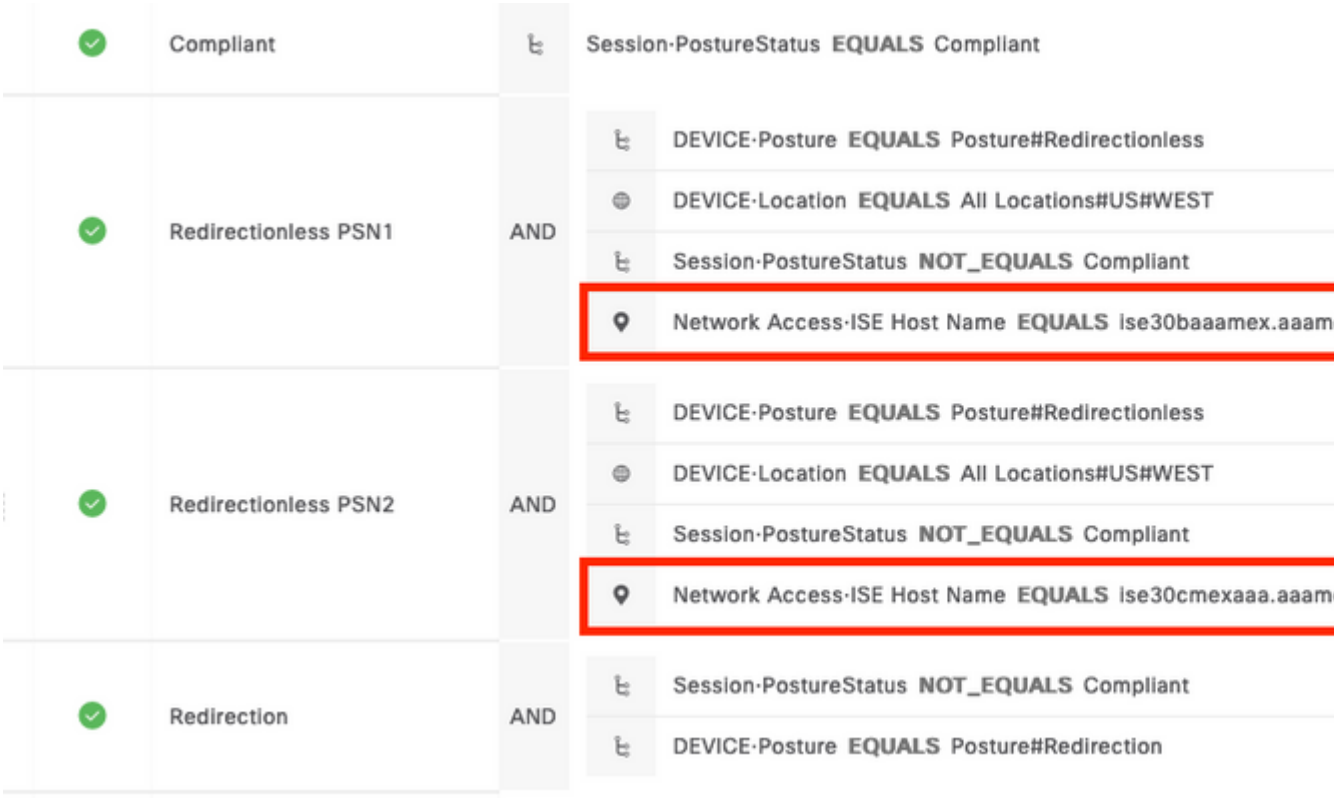
Per ridurre l'impatto:

1. Cancellare il file connectiondata.xml dagli endpoint rimuovendo il file dalla cartella Cisco Secure Client e riavviare il servizio ISE Posture o Cisco Secure Client. Se i servizi non vengono riavviati, il file precedente viene rigenerato e le modifiche non diventano effettive. Questa azione deve essere eseguita anche dopo la revisione e la modifica degli elenchi Call Home.
2. Utilizzare i DACL o altri ACL per bloccare il traffico diretto ai PSN ISE per le connessioni di rete ove non pertinente:

    - Per le connessioni in cui la postura non viene applicata nei criteri di autorizzazione ma che si applicano agli endpoint con Cisco Secure Client ISE Posture module installato, bloccare il traffico proveniente dai client su tutti i PSN ISE per le porte TCP 8905 e la porta del portale di provisioning client. Questa azione è consigliata anche per la postura con implementazione di reindirizzamento.
    - Per le connessioni in cui la postura è applicata nei criteri di autorizzazione, consentire il traffico dai client al PSN di autenticazione e bloccare il traffico verso altri PSN nella distribuzione. Questa azione può essere implementata temporaneamente durante la revisione del progetto.



Profilo di autorizzazione con DACL per PSN singolo



Criteri di autorizzazione per PSN

Contabilità

L'accounting RADIUS è essenziale per la gestione delle sessioni ad ISE. Poiché la postura si basa su una sessione attiva da eseguire, una configurazione errata o non corretta può influire anche sul rilevamento della postura e sulle prestazioni ISE. È importante verificare che l'accounting sia configurato correttamente sul dispositivo di rete per l'invio di richieste di autenticazione, l'avvio dell'accounting, l'interruzione dell'accounting e gli aggiornamenti di accounting a un singolo PSN per ogni sessione.

Per verificare i pacchetti di accounting ricevuti su ISE, selezionare **Operations** > **Reports** > **Reports** > **Endpoints and Users** > **RADIUS Accounting.**

Informazioni correlate

- Supporto tecnico e download 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).