Configurazione e risoluzione dei problemi di ISE 3.2 con integrazione FMC 7.2.4

Sommario

Introduzione

In questo documento vengono descritte le procedure per integrare Identity Services Engine con Firewall Management Center utilizzando le connessioni alla griglia di Platform Exchange.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- Platform Exchange Grid
- Centro gestione firewall
- Certificati TLS/SSL.

Componenti usati

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

- Patch 3 per Identity Services Engine (ISE) versione 3.2
- Firewall Management Center versione 7.2.4

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.

Questa documentazione fornisce una soluzione per integrare FMC e ISE utilizzando pxGrid versione 2.

Cisco Firepower Management Center (FMC) è una piattaforma centralizzata per il firewall di nuova generazione e il sistema di prevenzione delle intrusioni, che offre gestione delle policy, rilevamento delle minacce e risposta agli incidenti.

Cisco Identity Services Engine è una soluzione completa che fornisce un accesso sicuro agli endpoint tramite servizi di autenticazione, autorizzazione e responsabilità (AAA) e applicazione di policy.

Platform Exchange Grid (pxGrid) consente di scambiare informazioni tra reti multifornitore e multipiattaforma.

Questa integrazione consente di ottenere un monitoraggio sicuro, il rilevamento delle minacce e l'impostazione di policy di rete basate sulle informazioni condivise.

Il framework PxGrid ha 2 versioni. Quella da usare dipende dalla versione ISE e dalla patch che occorre rivedere.

A partire dalla versione ISE 3.1, tutti iGLe connessioni Grid da ISE sono basate sulla versione di pxgrid 2.

PxGrid versione 1.0

TLa prima versione di questo framework (pxGrid v1) è caratterizzato dalla facilità di manutenzione rilevata con il comando show application status ise come viene visualizzato nell'output successivo.

Quando la funzione pxGrid è attivata nel nodo, viene visualizzato il comando pxGrid caratteristiche in stato di esecuzione.

```
ise/admin# show application status ise
ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3688
Database Server                        running          41 PROCESSES
Application Server                     running          6041
Profiler Database                      running          4533
AD Connector                           running          6447
M&T Session Database                   running          2363
M&T Log Collector                      running          6297
M&T Log Processor                      running          6324
Certificate Authority Service          running          6263
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
Identity Mapping Service               disabled
```

Funzionalità di PxGrid versione 1.

In questa versione della piattaforma, è noto che ha un solo nodo pxGrid con i processi pxGrid in stato di esecuzione, mentre gli altri nodi pxGrid sono in stato di standby.

Questi nodi monitorano costantemente lo stato del nodo pxGrid con i servizi correlati in esecuzione.

In questo, il nodo pxGrid primario è stato promosso e l'altro nodo pxGrid ha abilitato i relativi servizi pxGrid.

Tuttavia, ciò rappresentava un periodo di inattività quando si è verificato questo failover.

La prima versione di pxgrid si basa sulla comunicazione nel protocollo XMPP (Extensible Messaging and Presence Protocol), un insieme di tecnologie utilizzate nelle infrastrutture di collaborazione e voce.

Gli argomenti condivisi in una connessione pxGrid v1 sono:

- Directory di sessione
- Metadati profilo endpoint
- Metadati Trustsec
- Funzionalità di Endpoint Protection
- Adaptive Network Control
- Argomento MDM_Offline
- Identità
- SXP

PxGrid versione 2.0

Questo documento descrive l'uso di PxGrid versione 2. Questa piattaforma funziona utilizzando le

operazioni REST su protocolli ISE e WebSocket che apportano miglioramenti, maggiore scalabilità, prestazioni e flessibilità nei modelli di dati.

In questa versione, le funzionalità pxgrid non vengono visualizzate in esecuzione come nella versione precedente con il comando show application status ise.

Per sapere quali meccanismi controllare per verificare la funzionalità pxGrid, consultare la sezione sulla convalida di ISE in questo documento.

Con questa versione, si hanno tutti i nodi pxGrid che si configurano come nodi pxGrid attivi. Questi ultimi sono pronti a partecipare allo scambio di informazioni in qualsiasi momento.

Nella versione 1, solo un nodo ha mantenuto in esecuzione la funzionalità di pxGrid.

Gli argomenti condivisi in una connessione pxGrid v2 sono:

- Directory di sessione
- Errore Radius
- Configurazione profiler
- Integrità del sistema
- MDM
- Stato ANC
- TrustSec
- Configurazione TrustSec
- TrustSec SXP
- Asset endpoint.

Componenti di pxGrid come piattaforma.

Controller PxGrid (ISE): È necessario considerare attendibili tutti i partecipanti che utilizzano pxGrid.

Client: Può essere sottoscrittore ed editore di diversi argomenti.

Autore: Client che condivide informazioni con il controller.

Iscritto: Client che utilizza le informazioni di un argomento.

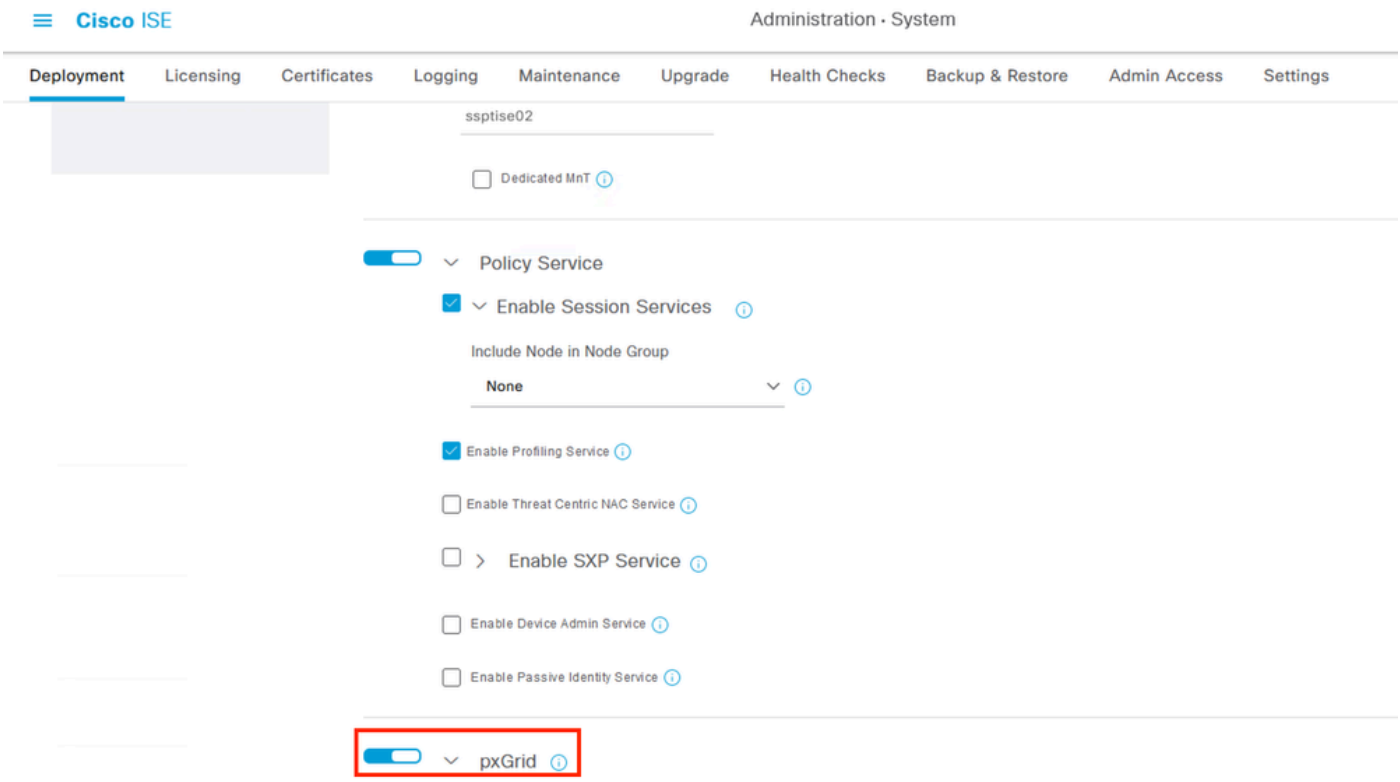
Questa integrazione consente di creare criteri di contenuto in FMC basati sulle informazioni condivise da ISE e sui relativi argomenti pubblicati (relativi all'attività dell'endpoint).

Configurazione

Prepara l'ISE per l'integrazione.

Passaggio 1. Configurare il nodo ISE in modo che esegua l'utente pxGrid su di esso nel menu Amministrazione > Sistema > Distribuzione.

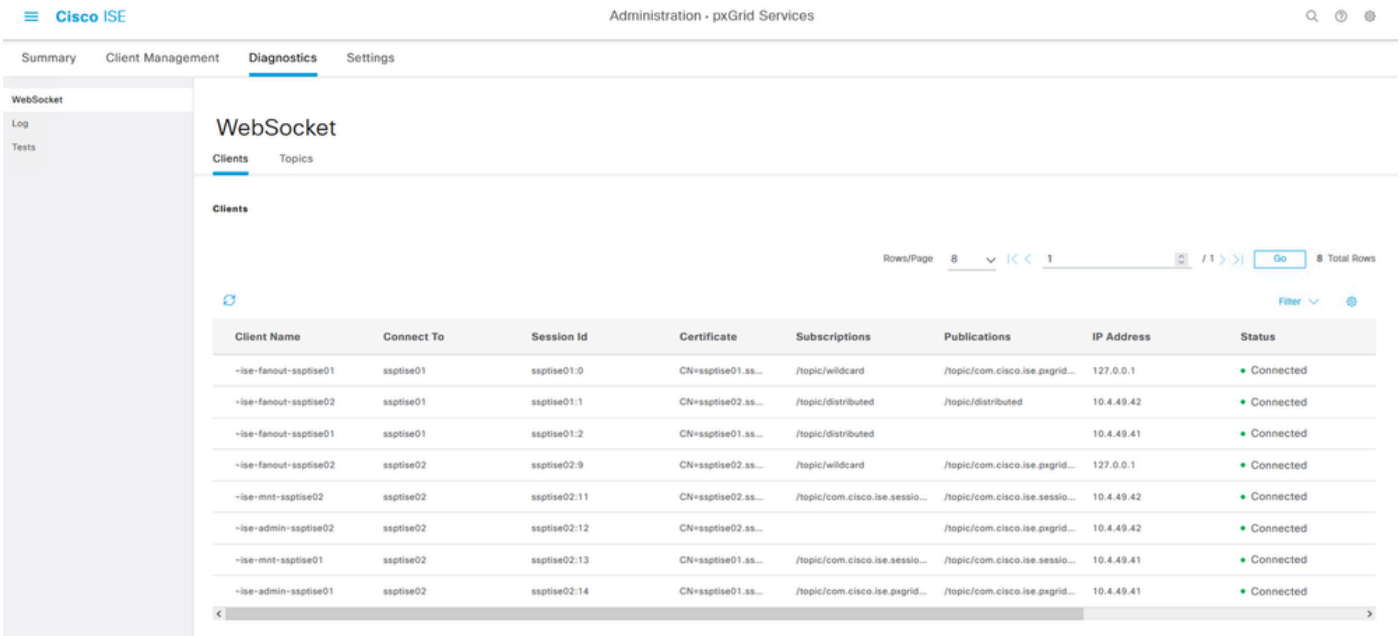
Selezionare i nodi e abilitare la funzionalità pxGrid.



Abilitazione dei servizi ISE pxGrid in un nodo.

Passaggio 2. Dopo aver abilitato i nodi con la funzionalità pxGrid, rivedere lo stato dei Websockets correlati ai client interni connessi.

Selezionare Amministrazione > pxGrid Services > Websocket. Si noti che i client puntano ai servizi ISE direttamente tramite l'indirizzo IP 127.0.0.1.

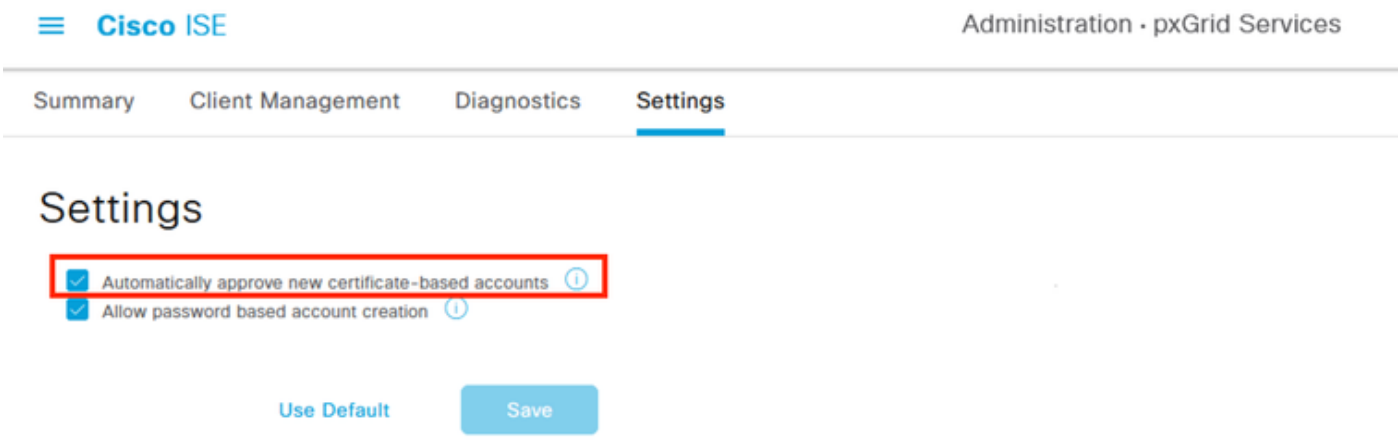


WebSocket interni di ISE.

Passaggio 3. Spostarsi nel menu Amministrazione > pxGrid Services > Impostazioni e selezionare l'opzione per approvare automaticamente i nuovi account basati su certificato,

Questo passaggio è facoltativo a questo punto, tuttavia, per la connessione pxGrid, si consiglia di attivare questa casella di controllo.

In seguito, è possibile accettare manualmente il CCP come destinatario predefinito.



Abilitazione dell'approvazione automatica per gli account basati su certificato pxGrid.

Passaggio 4. Esaminare i certificati relativi alla funzionalità pxGrid dell'ambiente in Amministrazione > Sistema > Certificati di sistema,

È consigliabile disporre di certificati pxGrid omogenei in tutti i nodi della distribuzione firmati dalla stessa CA radice

In questo scenario, vengono utilizzati i certificati ISE interni generati. In questa versione di ISE, dove nell'esempio, la CA radice corrisponde al nodo PAN.

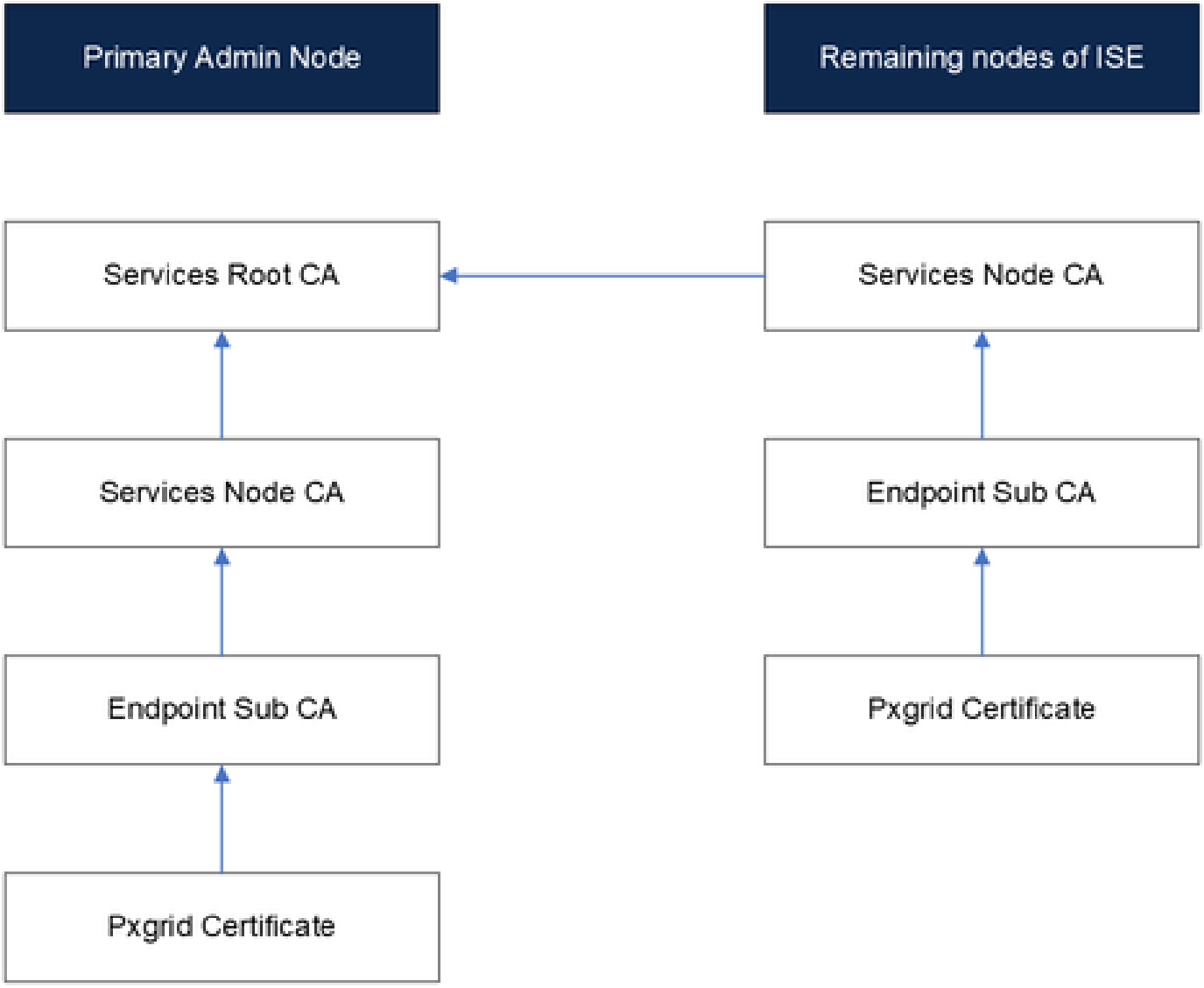
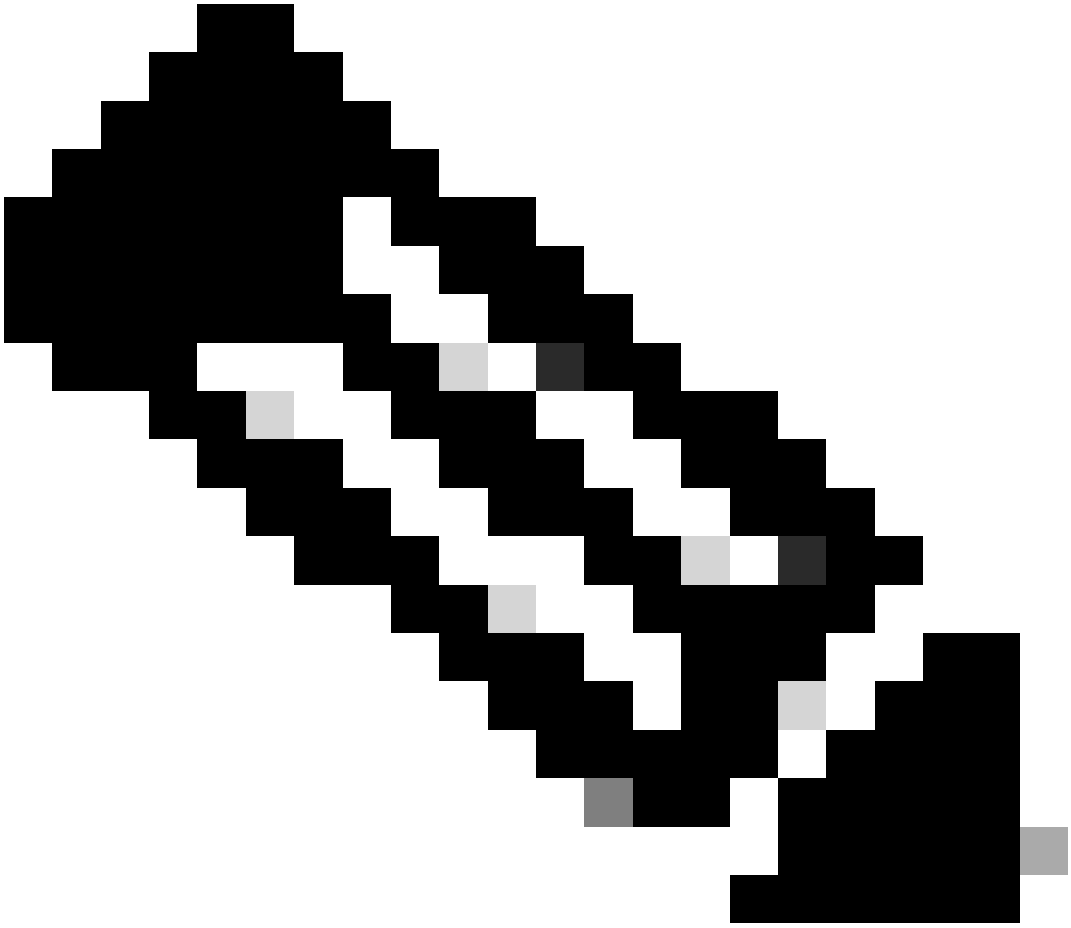
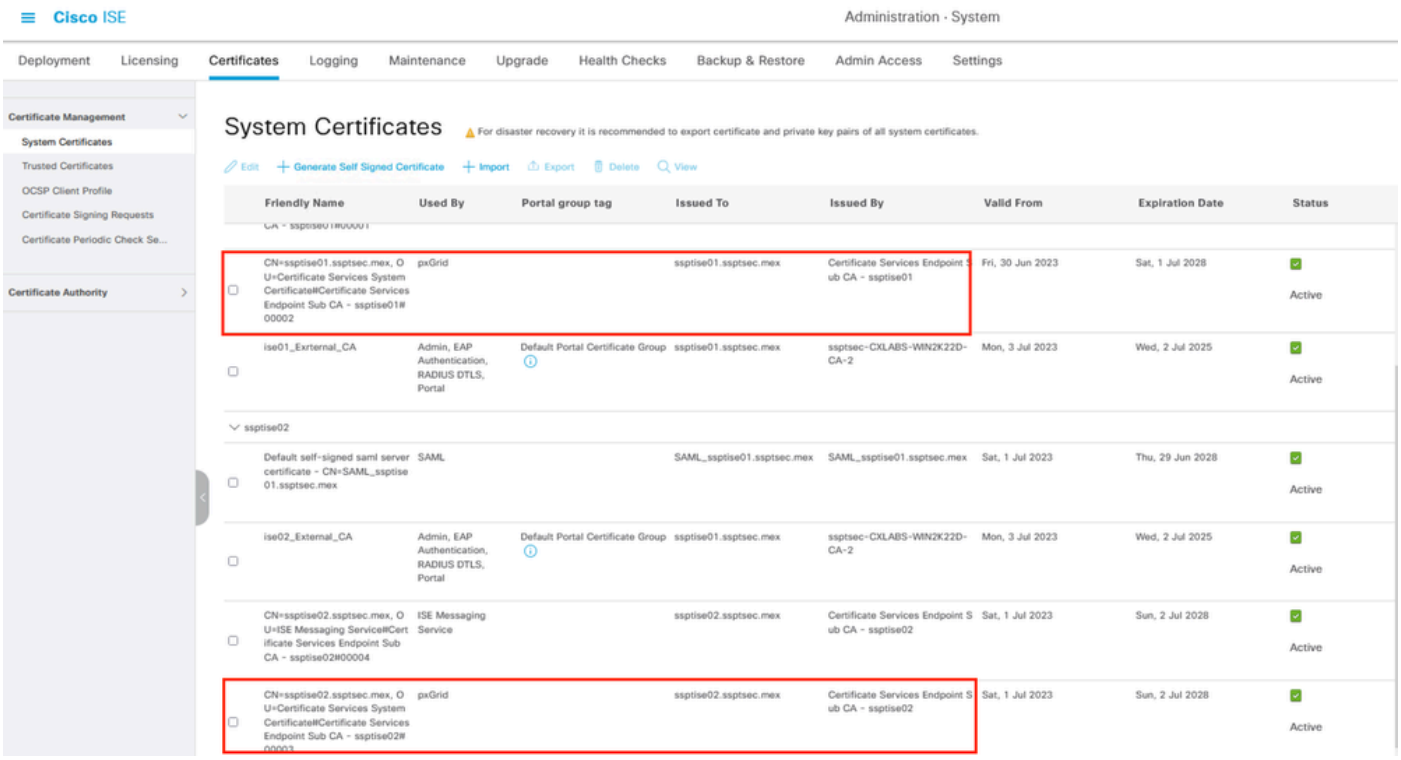


Diagram Internal Certificates su ISE.



Nota: Per ulteriori informazioni sulla struttura interna dei certificati generati con ISE, consultare il documento sulla descrizione dei servizi ISE Internal Certificate Authority.

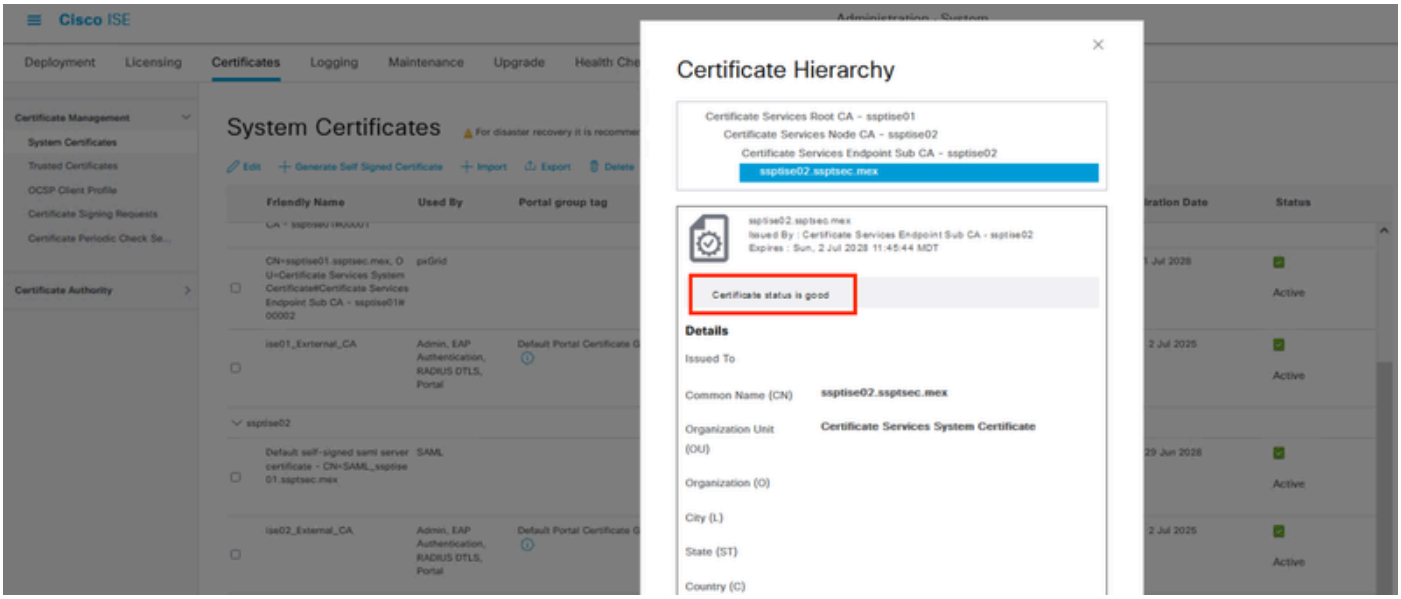


Certificati PxGrid in una distribuzione distribuita.

Passaggio 5. Verificare lo stato dei certificati pxGrid.

Dal menu precedente, selezionare una casella di controllo da un certificato pxGrid di un nodo, quindi selezionare l'opzione Visualizza.

L'output è simile a quello visualizzato nei certificati pxGrid.

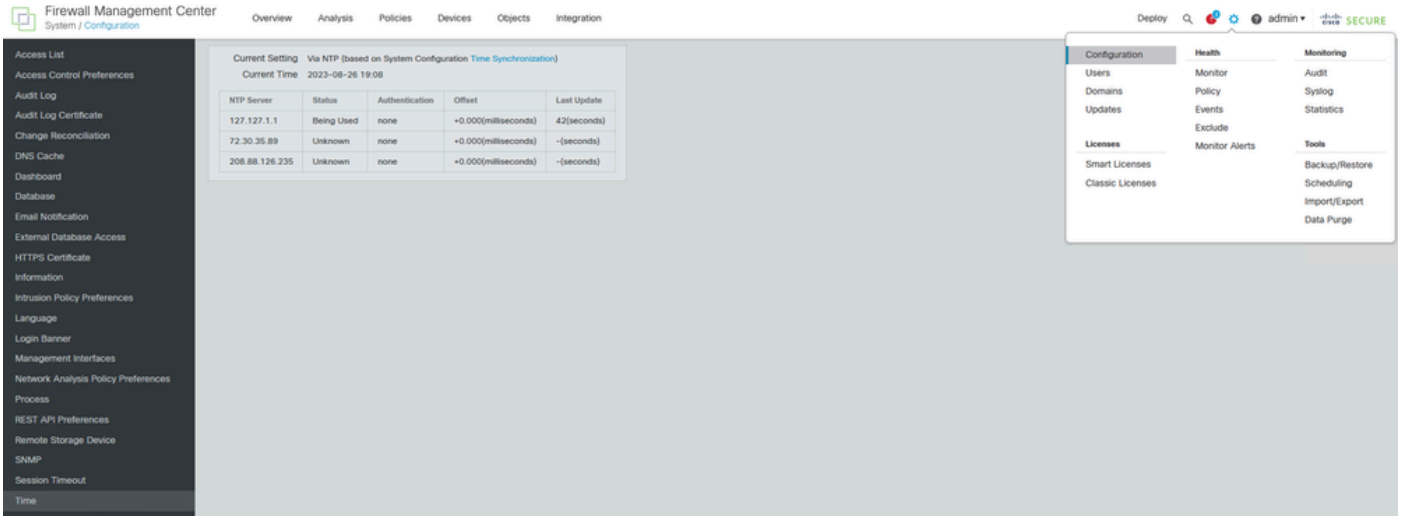


Verifica del certificato pxGrid.

Preparare il CCP per l'integrazione.

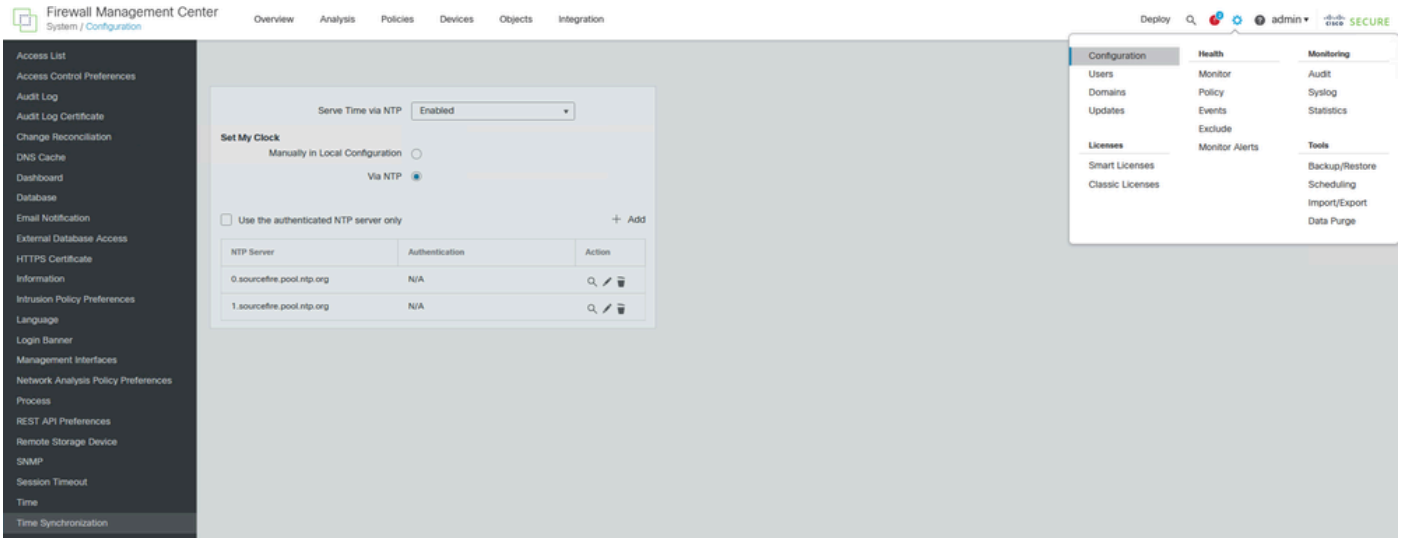
Passaggio 1.Confermare che l'ora interna del CCP sia aggiornato.

Passa a Sistema > Configurazione > Ora e assicurarsi che l'ora configurata sul CCP sia aggiornato.



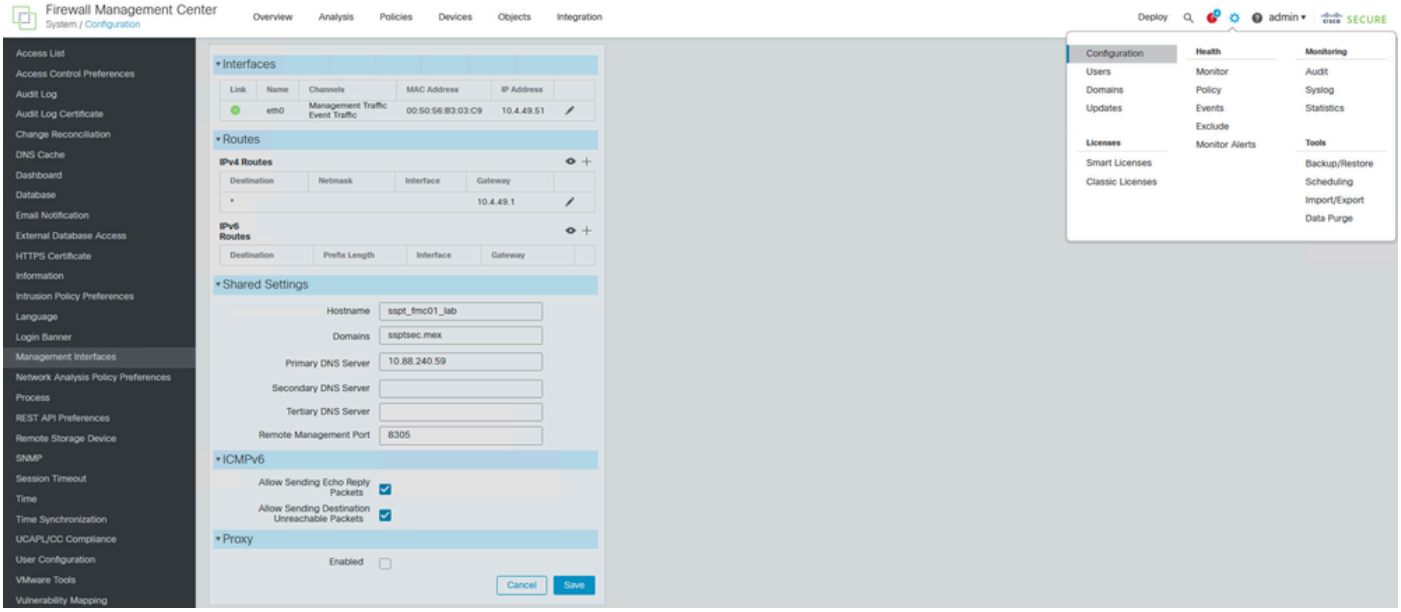
Verifica dell'aggiornamento del CCP.

Se l'ora FMC non è aggiornata, verificare che NTP sia configurato correttamente e in Sincronizza. NTP può essere configurato in Sistema > Configurazione > Tempo > + Aggiungi.



Sincronizzazione ora in FMC.

Passaggio 2. Passa a Sistema > Configurazione > Interfaccia di gestione > Impostazioni condivise e verificare che almeno Server DNS primario campo contiene una IP del server DNS.



Configurazione DNS in FMC.

Passaggio 3. Verificare che il nome host del CCP sia configurato.

Passa a Sistema > Configurazione > Interfaccia di gestione > Impostazioni condivise e verificare che Nome host contiene il nome host del CCP.

È possibile verificare questo passaggio durante la revisione del passaggio precedente in questa sezione.

Impostazione della connessione pxGrid tra ISE e FMC.

Passaggio 1. Passare al menu Amministrazione > pxGrid Services > Gestione client > Certificati.

Nella prima opzione selezionare Crea un singolo certificato (senza richiesta di firma del certificato).

Nella sezione Nome comune (CN), immettere il nome di dominio completo (FQDN) del CCP che l'ISE deve rilasciare un certificato.

Fornire una descrizione.

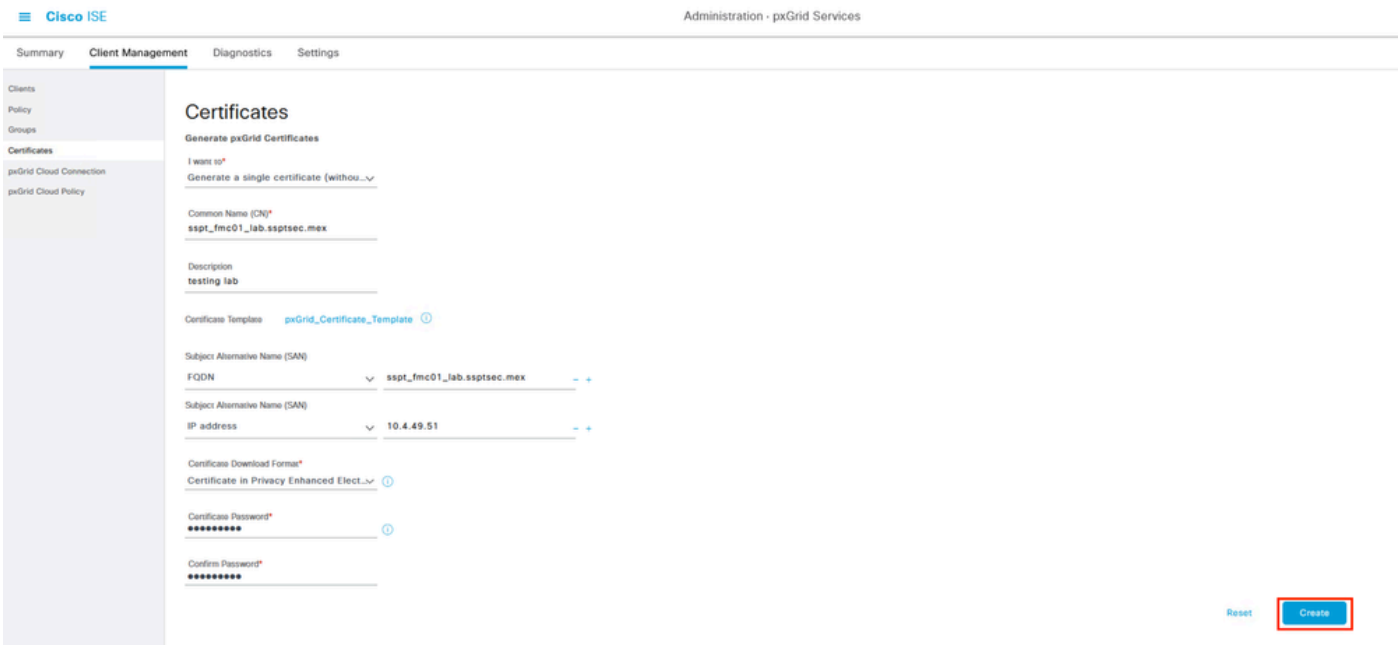
Nella sezione Nome alternativo soggetto (SAN), immettere il nome di dominio completo e l'indirizzo IP del CCP a cui connettersi.

Nella parte inferiore del formato di download dei certificati selezionare l'opzione Certificato in formato PEM (Privacy Enhanced Electronic Mail) dal menu a discesa.

Immettere il formato PEM PKCSS (inclusa la catena di certificati).

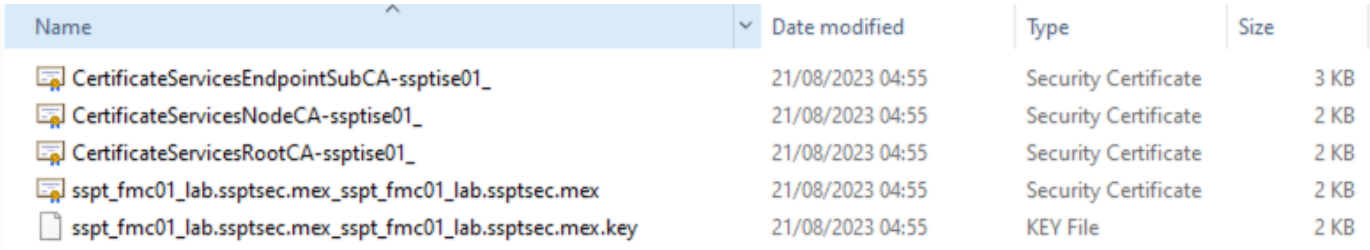
Immettere e memorizzare una password nella casella Password certificato quando si utilizza la password in un secondo momento nel FMC.

Confermare la password, quindi selezionare Crea.



Esempio di generazione di certificati pxGrid.

Passaggio 2. Un file zip viene scaricato nel computer. Decomprimere il file e verificare di disporre dei seguenti file dell'ambiente:

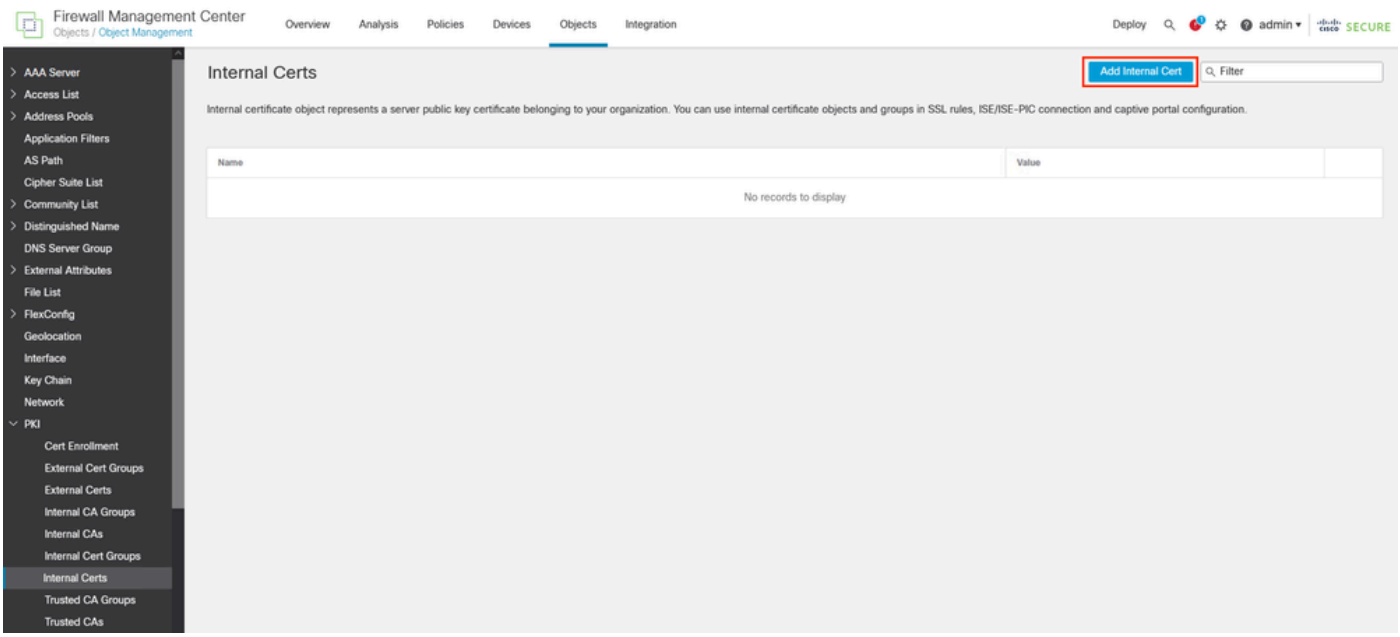


Name	Date modified	Type	Size
CertificateServicesEndpointSubCA-ssptise01_	21/08/2023 04:55	Security Certificate	3 KB
CertificateServicesNodeCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
CertificateServicesRootCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex.key	21/08/2023 04:55	KEY File	2 KB

i certificati PxGrid generati da ISE.

Passaggio 3. In FMC, passare al menu Oggetti > Gestione oggetti > PKI > Certificati interni.

Selezionare l'opzione Aggiungi certificato interno.



Aggiunta del certificato del CCP come certificato interno.

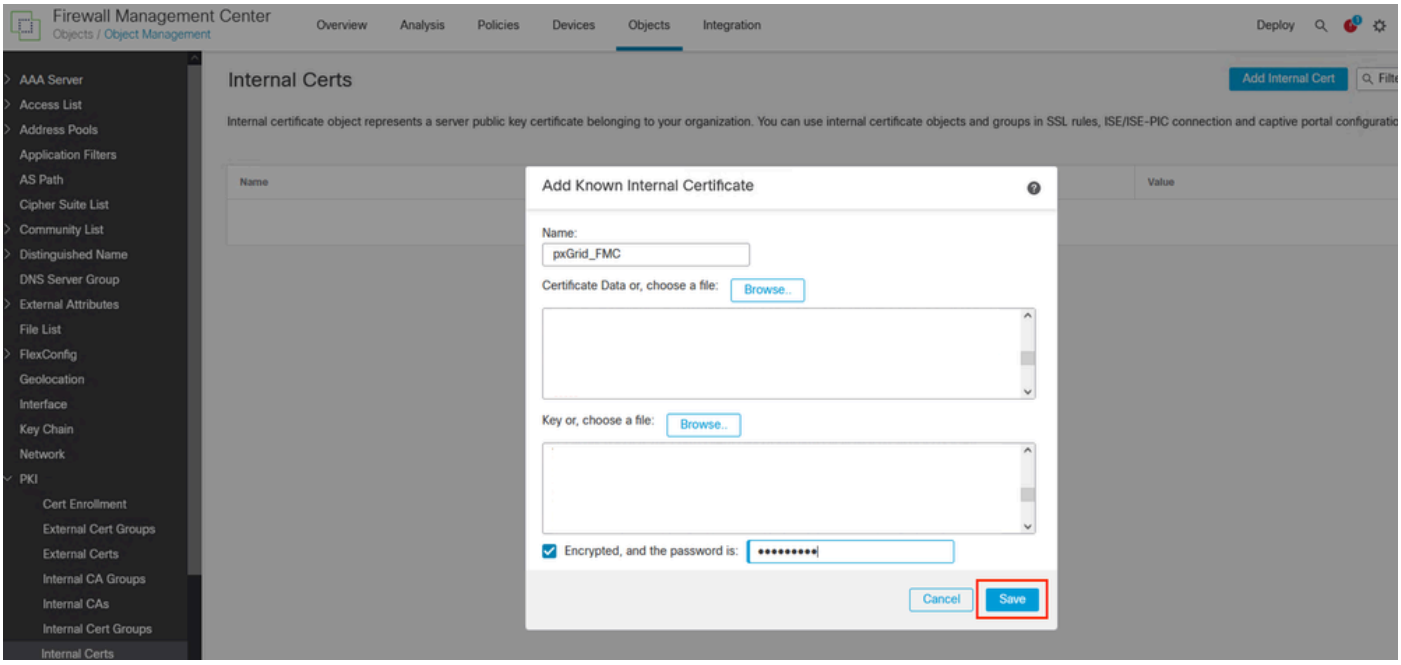
Passaggio 4. Assegnare un nome al certificato allocato nel CCP.

Sfogliare il certificato creato per il CCP dall'ISE nella sezione Dati certificato.

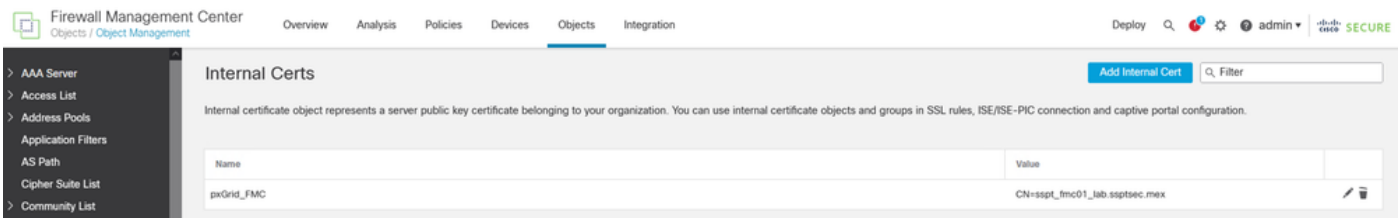
Sfogliare il file con l'estensione .key per riempire il campo successivo.

Selezionare l'opzione Encrypted (Crittografato), quindi immettere la password utilizzata quando è stato creato il certificato su ISE.

Salvare la configurazione.



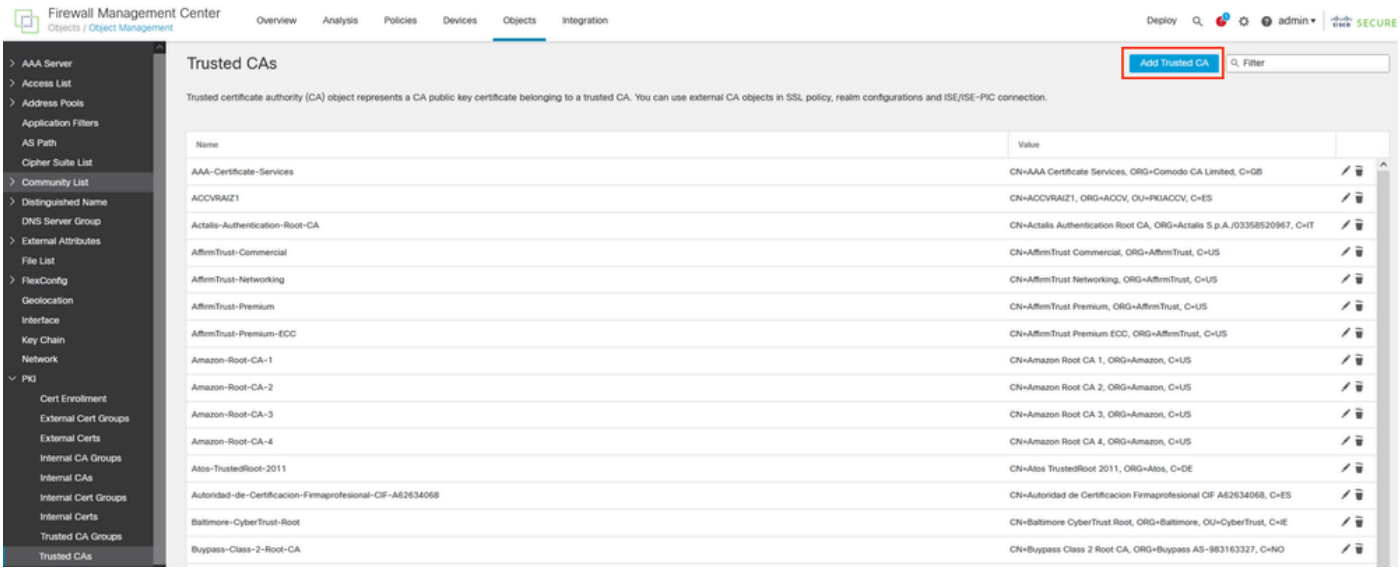
Esportazione del certificato FMC generato da ISE.



Certificato CCP.

Passaggio 5. Passare al menu Oggetti > Gestione oggetti > PKI > CA attendibili,

Selezionare Aggiungi CA attendibili.

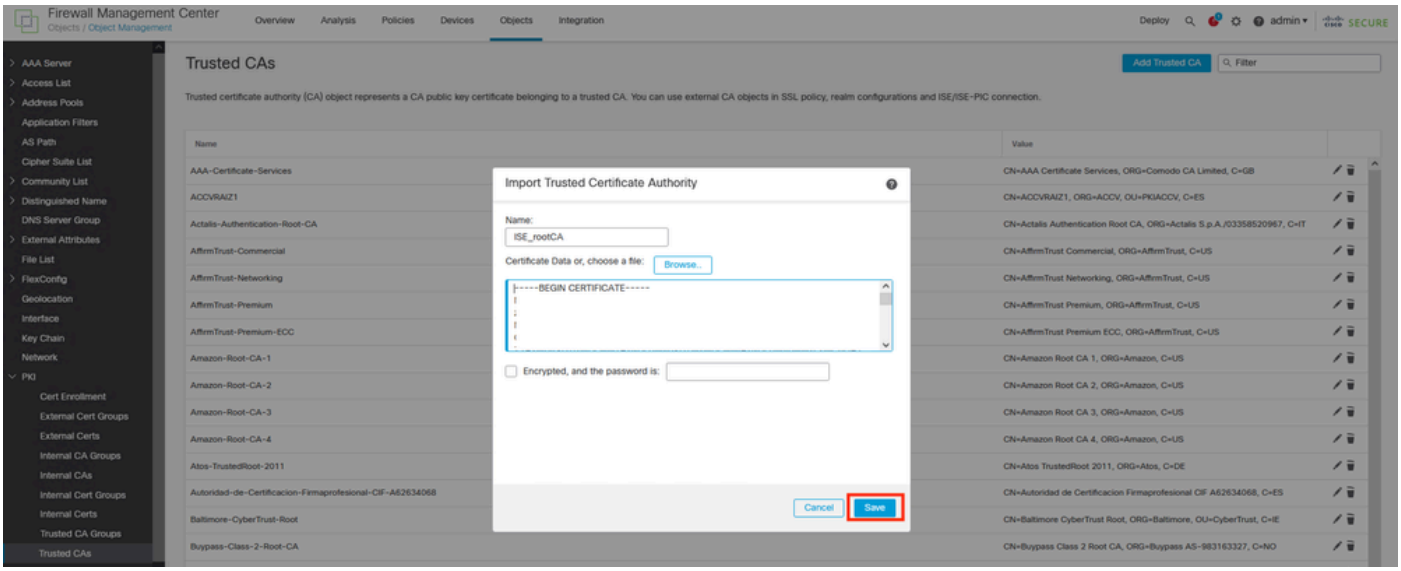


Aggiunta della CA radice ISE come certificato attendibile.

Passaggio 6. Assegnare un nome all'autorità di certificazione.

Individuare e selezionare la rootCA ISE scaricata dal file ISE.

Salvare la configurazione.



Esportazione della rootCA ISE.

Passaggio 7. Passare al menu Integrazione > Altre integrazioni > Origini identità.

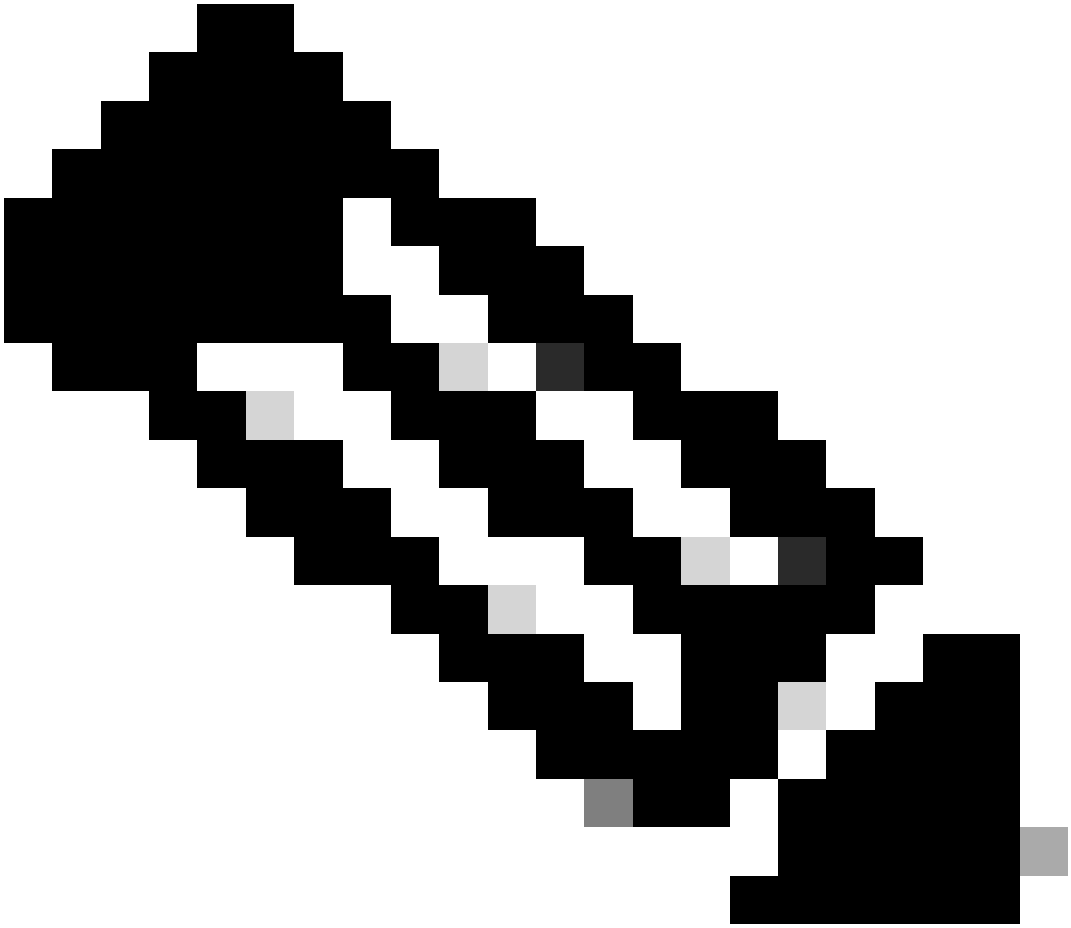
Selezionare in Tipo di servizio: Identity Services Engine,

Immettere l'indirizzo IP o il nome di dominio completo (FQDN) del nodo pxGrid che diventa il nodo principale.

Ripetere la procedura per il nodo PxGrid secondario.

Selezionare dal menu a discesa il certificato pxGrid generato da ISE per la sezione pxGrid Client Certificate,

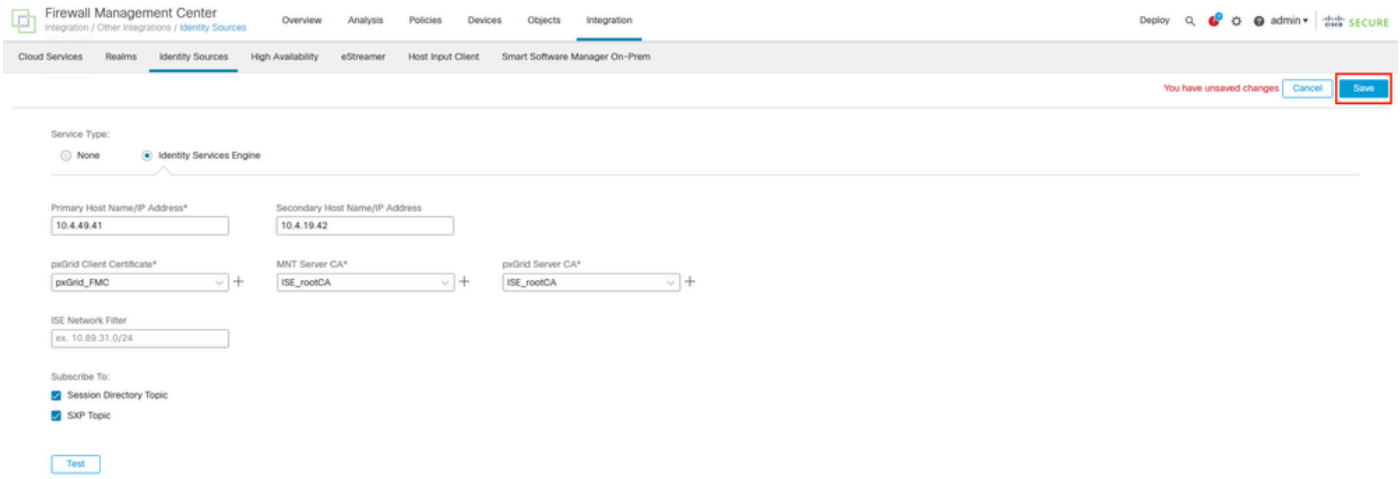
Nella sezione CA MNT Server e CA pxGrid Server, selezionare la CA radice ISE esportata nell'ultimo passaggio.



> Nota: La CA del server pxGrid corrisponde all'autorità di certificazione radice del certificato utilizzato da pxGrid sui nodi pxGrid.
>
> La CA del server MNT corrisponde all'autorità di certificazione del certificato utilizzato da pxGrid sui nodi MNT.

(Facoltativo) È possibile effettuare la sottoscrizione all'argomento Session Directory e SXP da ISE.

Salvare la configurazione.

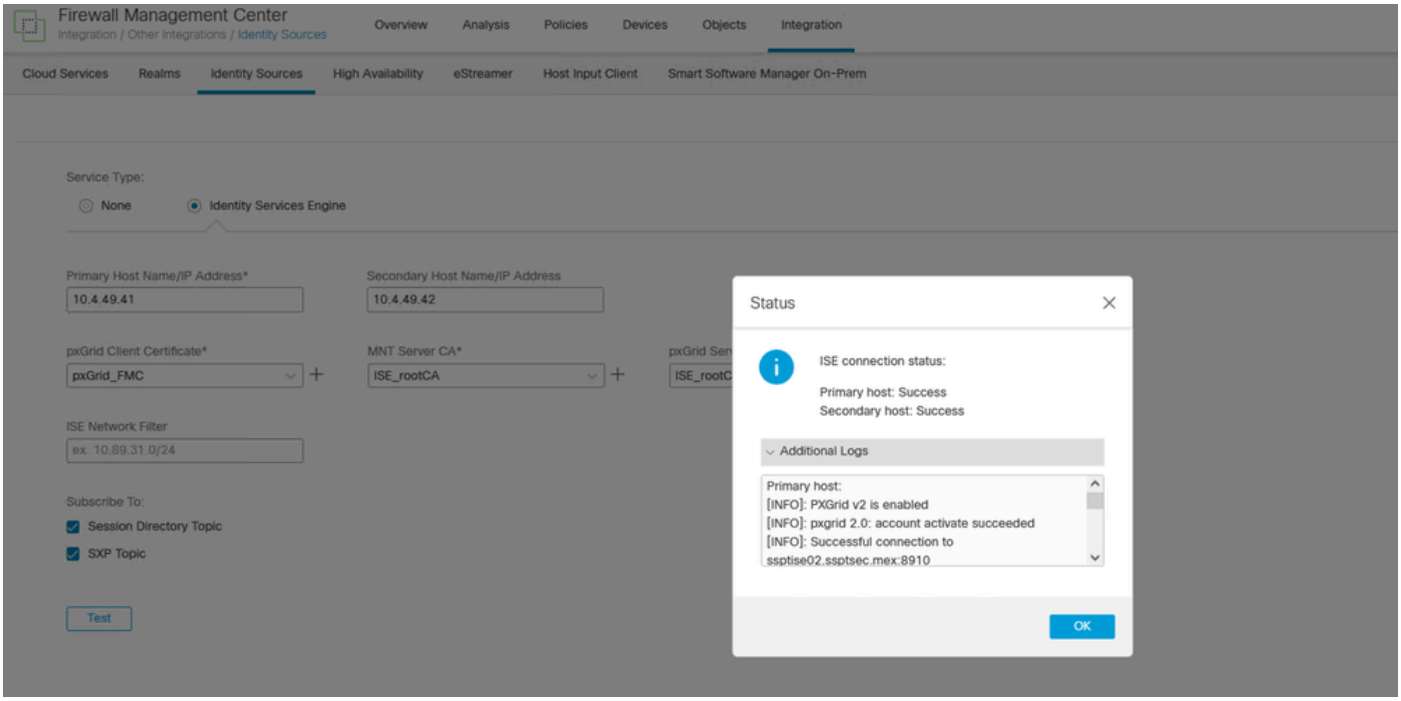


Impostazione di ISE come origine identità in FMC.

Verifica.

Convalida nel CCP.

Nel menu, passare a Integrazione > Altre integrazioni > Origini identità > Identity Services Engine, prima di salvare la configurazione. È possibile verificare le impostazioni per il collegamento pxGrid.



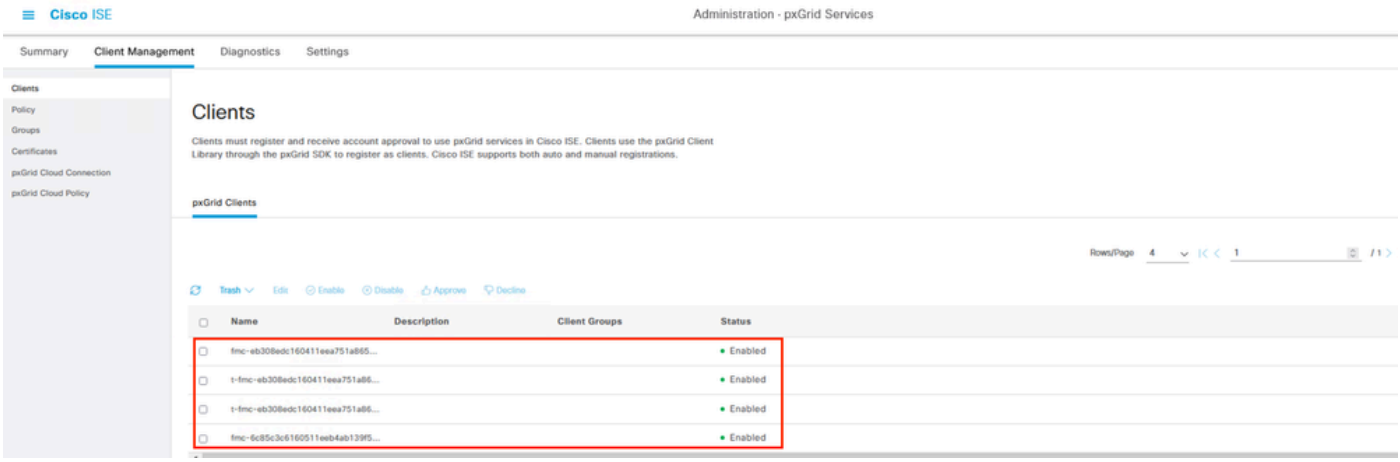
Comunicazione PxGrid riuscita.

```
Primary host:

[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
```

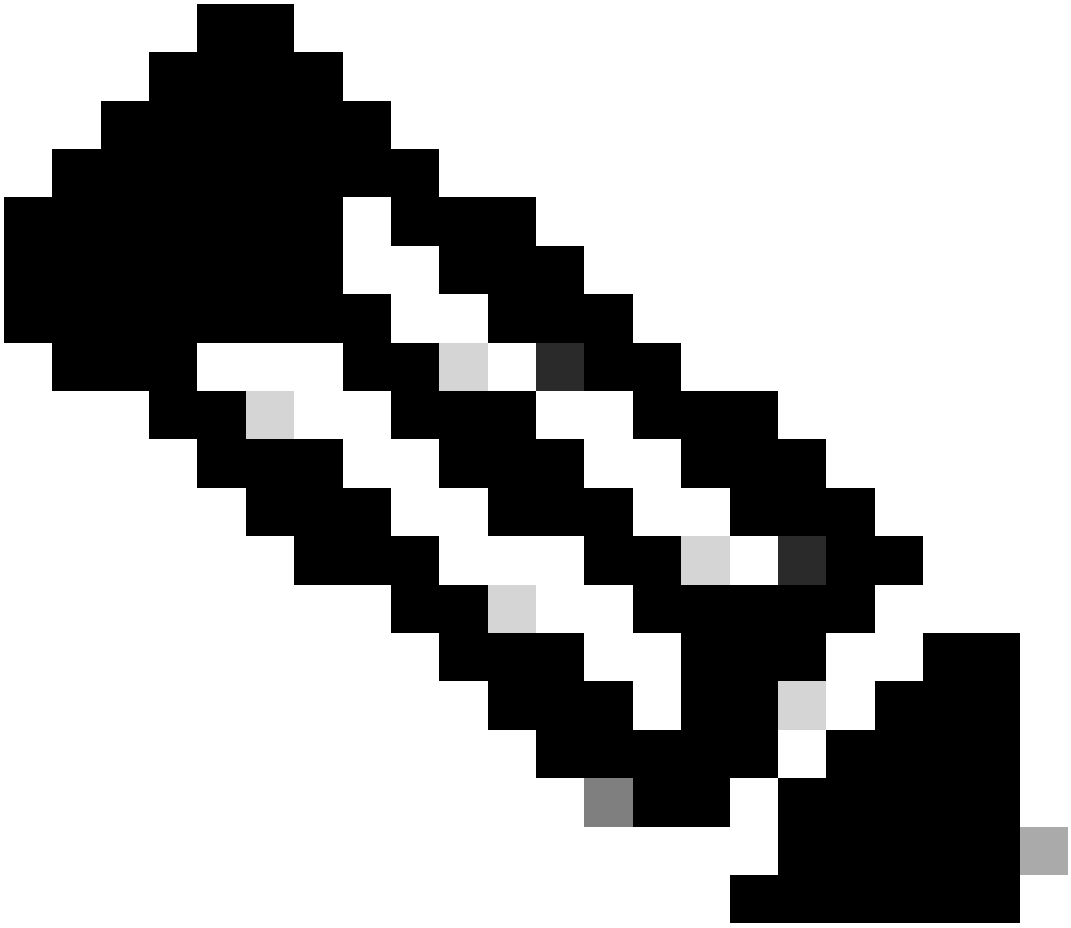
```
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetw
[INFO]: All requested ISE Services are online.

Secondary host:

[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetw
[INFO]: All requested ISE Services are online.
```

Convalida ad ISE.

Quando il client pxGrid FMC è stato integrato correttamente in ISE, tu quindi vedere (nel Amministrazione > pxGrid Services > Gestione client > Menu Client) i client con il nome fmc sono inclusi e attivato.



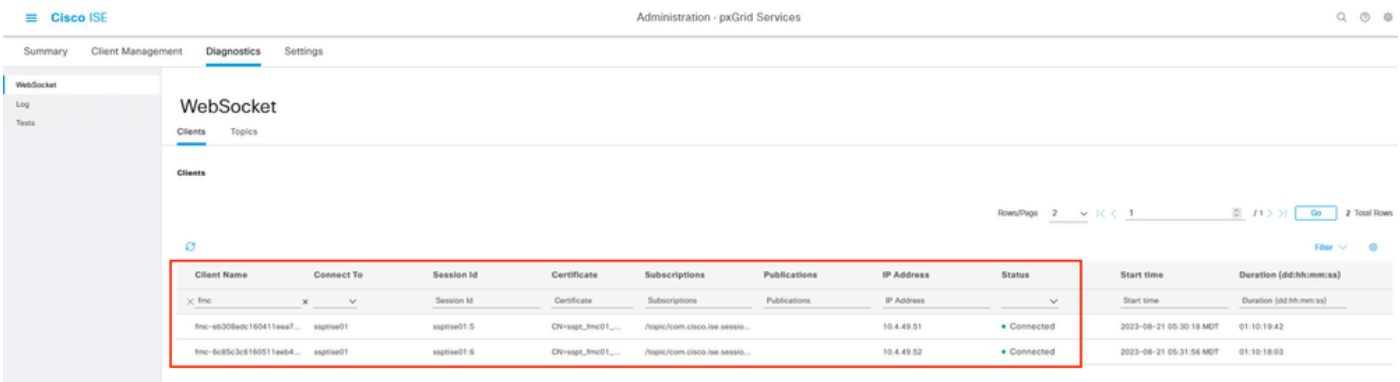
Client PxGrid disponibili e abilitati.



Nota: I client pxGrid il cui prefisso inizia con "t-fmc" sono quelli che vengono utilizzati tramite il pulsante di prova del FMC.

Inoltre, se si passa al menu Amministrazione > pxGrid Services > Diagnostics > WebSocket, viene quindi visualizzata la connessiones verso CCP.

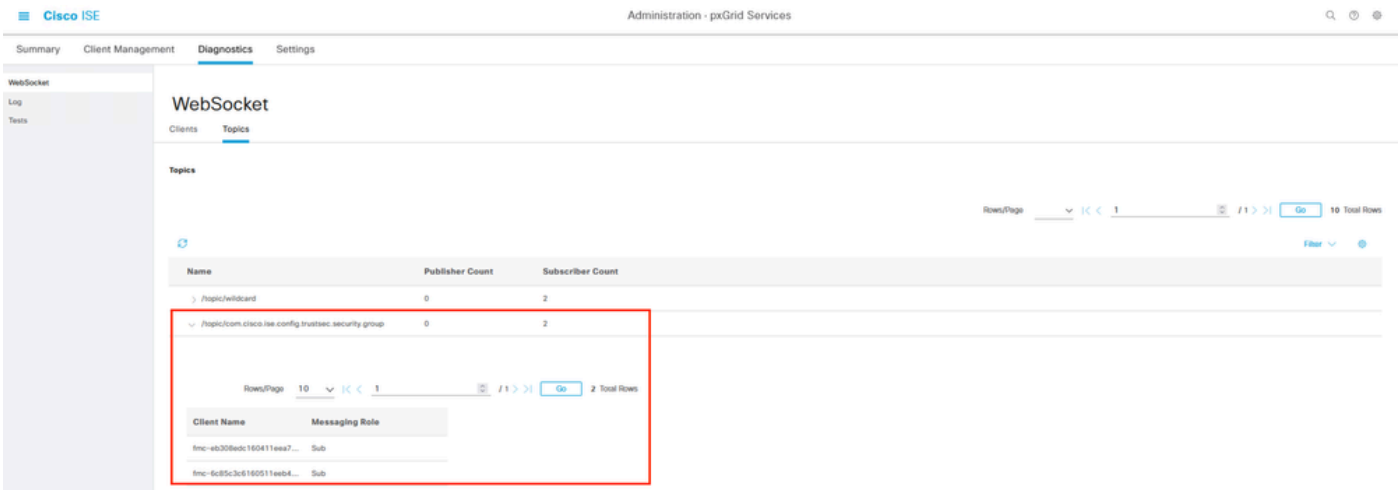
Nello scenario in cui è presente il CCP alta disponibilità, le unità primarie e secondarie verranno visualizzate come illustrato nell'esempio seguente:



WebSockets disponibili su ISE.

Nella scheda successiva da questo menu denominato Targomenti, è possibile verificare che gli abbonati FMC siano stati aggiunti agli argomenti di pxGrid pubblicati da ISE.

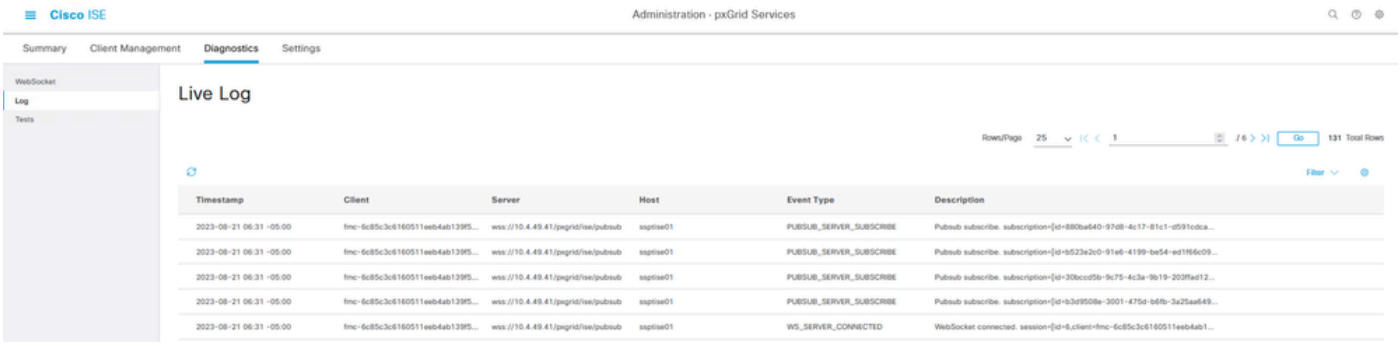
Ad esempio, è disponibile l'argomento relativo al gruppo di protezione da dove tu è possibile osservare che entrambi i CCP sono sottoscritti e ricevono informazioni correlate a SGT pubblicato da ISE.



Argomenti per ogni sottoscrittore pxGrid.

INel menu Amministrazione > pxGrid Services > Diagnostics > Log, eventi importanti correlati alla comunicazione in pxGrid (per i nodi con la funzionalità attivata) sono visualizzati.

Questi rappresentano le informazioni relative all'integrazione.



Registri attivi PxGrid.

Risoluzione dei problemi

Risoluzione dei problemi relativi a FMC.

Confermare che FMC è in grado di risolvere i propri nodi hostname e ISE per nome host.

Ad esempio:

<#root>

```
> expert
admin@sspt_fmc01_lab:~$ ping sspt_fmc01_lab

PING sspt_fmc01_lab (10.4.49.51) 56(84) bytes of data.
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=3 ttl=64 time=0.055 ms
^C
--- sspt_fmc01_lab ping statistics ---
```

3 packets transmitted, 3 received,

```
 0% packet loss, time 27ms

admin@sspt_fmc01_lab:~$ ping ssptise01
PING ssptise01.ssptsec.mex (10.4.49.41) 56(84) bytes of data.
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=2 ttl=64 time=0.646 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=3 ttl=64 time=0.743 ms
^C
--- ssptise01.ssptsec.mex ping statistics ---
```

3 packets transmitted, 3 received,

```
 0% packet loss, time 82ms
rtt min/avg/max/mdev = 0.586/0.658/0.743/0.068 ms
admin@sspt_fmc01_lab:~$
admin@sspt_fmc01_lab:~$ ping ssptise02

PING ssptise02.ssptsec.mex (10.4.49.42) 56(84) bytes of data.
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=2 ttl=64 time=0.609 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=3 ttl=64 time=0.628 ms
^C
--- ssptise02.ssptsec.mex ping statistics ---
```

3 packets transmitted, 3 received

```
, 0% packet loss, time 45ms
rtt min/avg/max/mdev = 0.588/0.608/0.628/0.025 ms
```

Accertarsi che Il processo ADI è attivo e in esecuzione:

<#root>

```
>
```

expert

```
sudo suadmin@sspt_fmc01_lab:~$
```

sudo su

```
root@sspt_fmc01_lab:/Volume/home/admin#
```

pmtool status | grep adi

adi (normal) - Running 7911

Sgarantire che la comunicazione tra FMC e ISE portaTCP 8910 consentito. Dal CCP CLI possiamo configurazione a tcpudump packet capture per confermare la comunicazione bidirezionale.

<#root>

>

expert

sudo suadmin@sspt_fmc01_lab:~$

sudo su

root@sspt_fmc01_lab:/Volume/home/admin#

tcpdump -i any tcp and port 8910

22:34:08.415370 IP

sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910

: Flags [S], seq 3033526171, win 29200, options [mss 1460,sackOK,TS val 2701166399 ecr 0,nop,wscale 7],
22:34:08.415840 IP

ssptise01.ssptsec.mex.8910 > sspt_fmc01_lab.46248

: Flags [S.], seq 3024877968, ack 3033526172, win 28960, options [mss 1460,sackOK,TS val 2268665064 ecr
22:34:08.415894 IP

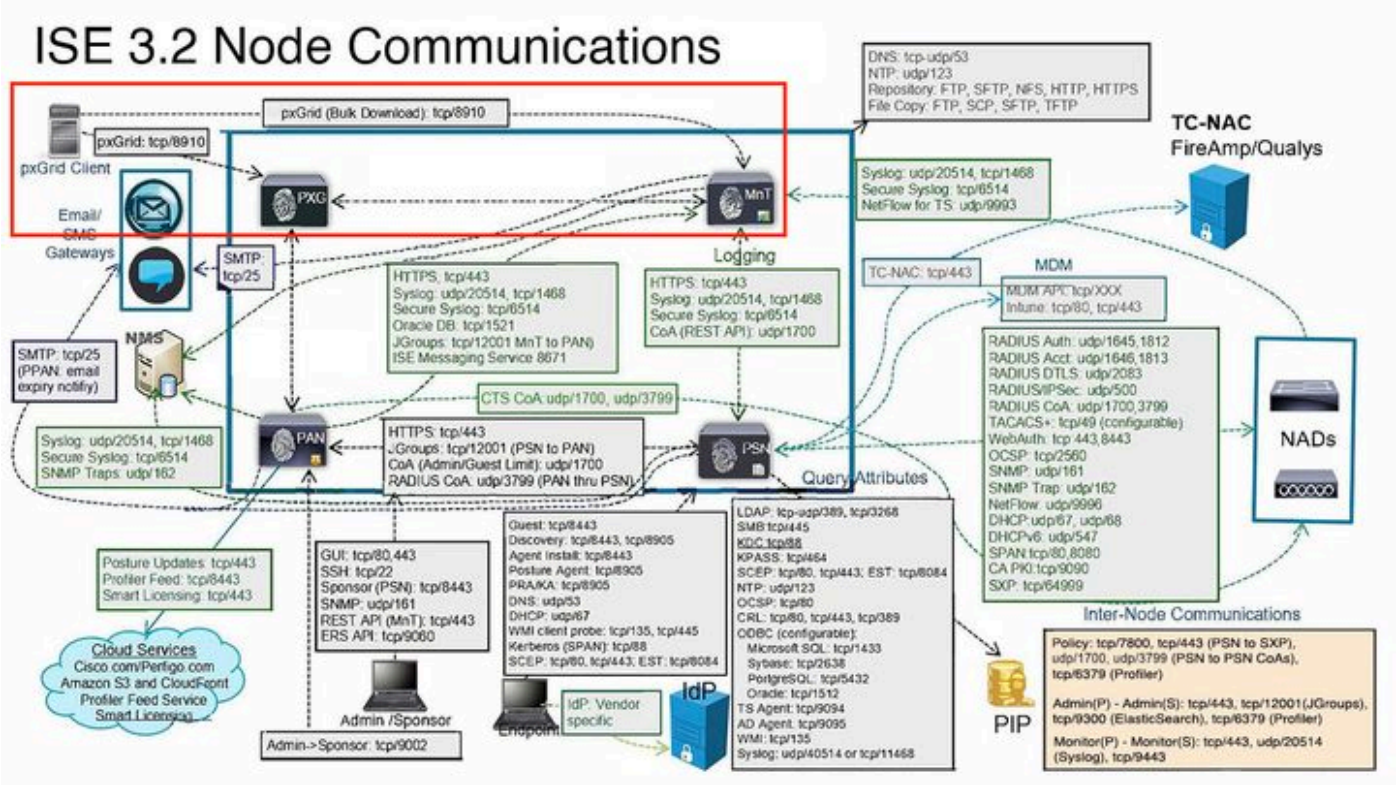
sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910

: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0
[...]

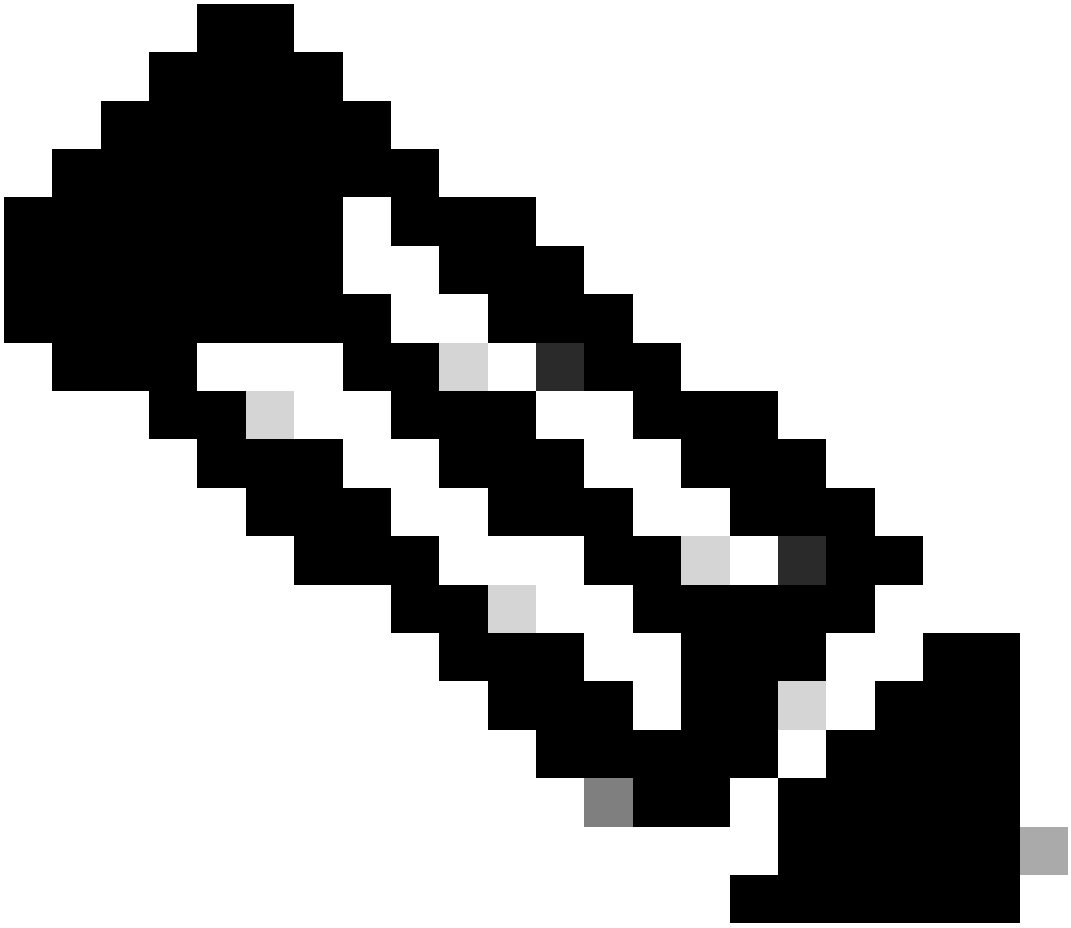
Risoluzione dei problemi relativi ad ISE.

Verificare che le comunicazioni sulla porta 8910 sia operativo.

Questa è la porta utilizzata dal client pxGrids per comunicare con i nodi pxGrid e MnT per il download di massa delle informazioni.



PxGrid in ambiente ISE.



Nota: Il client pxGrid, in questo caso il FMC comunica ai nodi pxGrid e al nodo MNT secondario (SMNT) per ottenere le informazioni (Scaricamento bulk); in caso di errore nel SMNT, cerca le informazioni attraverso il MNT primario.

ISui nodi ISE in cui si trova la comunicazione con il client pxGrid, è possibile rivedere se il porta è apri o se vi sono socket collegati a quella porta.

```
#show ports | include 8910
tcp: (output omitted), :::8910,
```

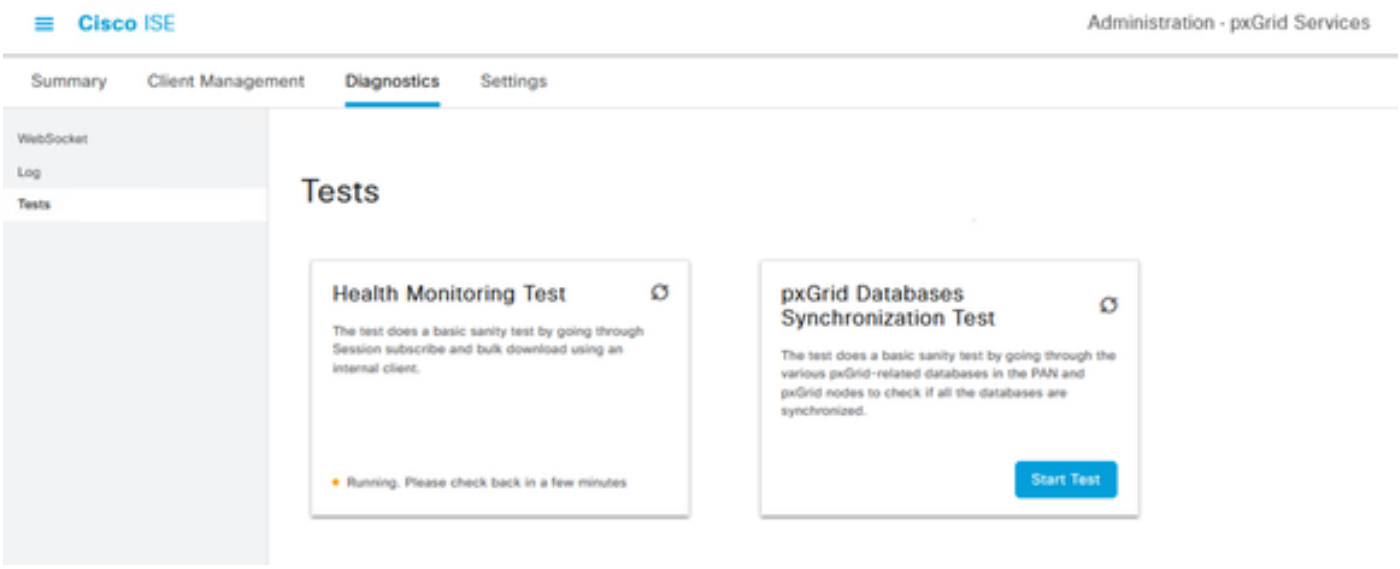
Ci sono 2 test disponibili su ISE che diagnosticano lo stato complessivo delle implementazioni pxGrid.

che si trovano nel menù Amministrazione > pxGrid Services > Diagnostica > Test.

I test illustrati in questa sezione vengono eseguiti internamente sull'ISE.

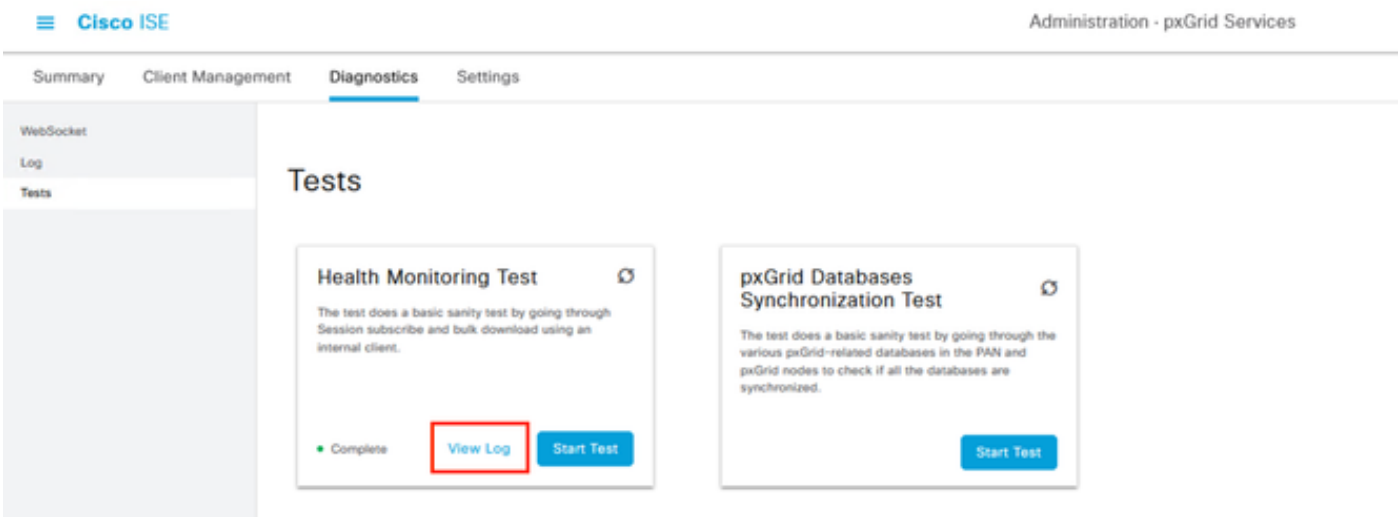
Test di monitoraggio dello stato rivede l'aspetto del servizio pxGridattivo, che valuta se un client può accedere alla directory di sessione, al servizio e agli argomenti pubblicati dal controller pxGrid.

Selezionare il opzione Inizio Test e attendere che i registri vengano raccolti.



Test di monitoraggio dello stato di PxGrid.

Una volta completato il test, selezionare opzione Visualizza registro. In questo esempio, il contenuto del registro è:



Revisione del test di monitoraggio dello stato.

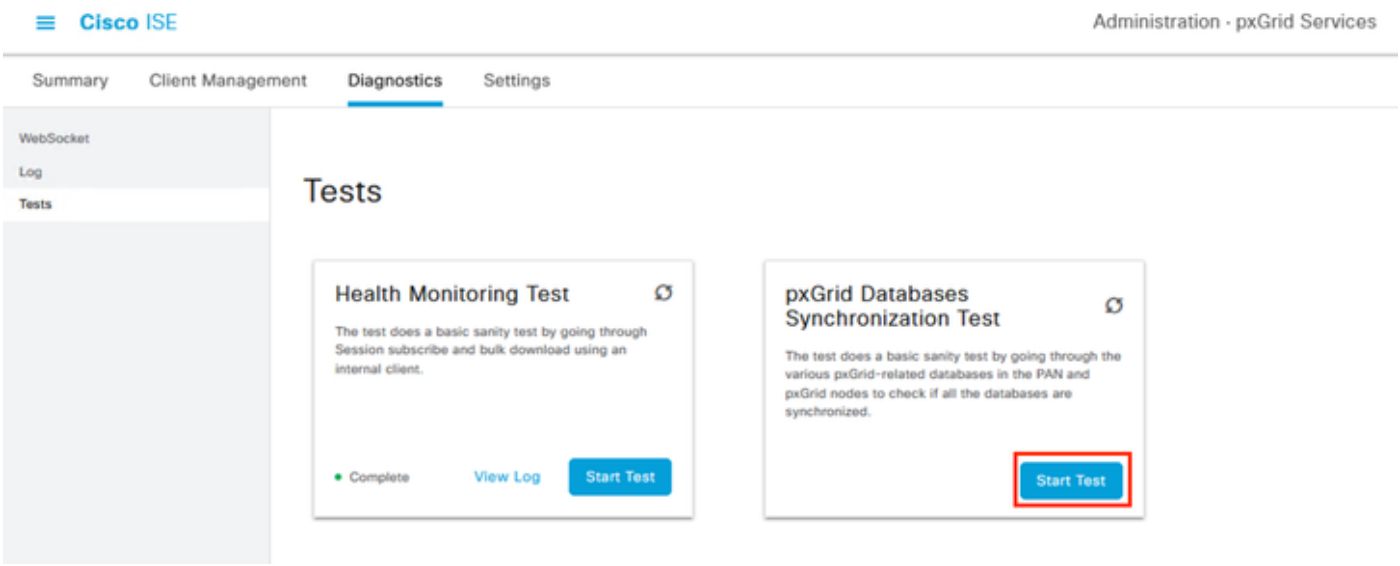
```
22-Aug-2023 17:03:13 [INFO] ************** pxGrid Session Directory Test ***************
22-Aug-2023 17:03:13 [INFO] ----------------- Starting Connection Test -----------------
22-Aug-2023 17:03:14 [INFO] pxGrid Node: ssptise01.ssptsec.mex
22-Aug-2023 17:03:14 [INFO] wsPubsubServiceName=com.cisco.ise.pubsub
22-Aug-2023 17:03:14 [INFO] sessionTopic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:14 [INFO] sessionRestBaseUrl=https://ssptise01.ssptsec.mex:8910/pxgrid/mnt/sd
22-Aug-2023 17:03:14 [INFO] wsUrl=wss://ssptise02.ssptsec.mex:8910/pxgrid/ise/pubsub
```

```
22-Aug-2023 17:03:15 [INFO] ---------------- Connection Test Completed ----------------
22-Aug-2023 17:03:15 [INFO] ------------------ Starting Download Test ------------------
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions read: 0
22-Aug-2023 17:03:15 [INFO] ------------------ Download Test Completed ------------------
22-Aug-2023 17:03:15 [INFO] ------------------ Starting Subscribe Test ------------------
22-Aug-2023 17:03:16 [INFO] STOMP CONNECT host=ssptise02.ssptsec.mex
22-Aug-2023 17:03:16 [INFO] STOMP SUBSCRIBE topic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:16 [INFO] STOMP CONNECTED version=1.2
22-Aug-2023 17:07:16 [INFO] A total of 0 notifications were received.
22-Aug-2023 17:07:16 [INFO] STOMP RECEIPT id=77
22-Aug-2023 17:07:19 [INFO] ------------------ Subscribe Test Completed ------------------
22-Aug-2023 17:07:19 [INFO] ********** pxGrid Session Directory Test Complete **********
```

Il test di sincronizzazione del database PxGrid verifica se le informazioni all'interno dei database è corretto tra i nodi PAN e pxGrid e sincronizzato.

Pertanto, le informazioni inviate ai sottoscrittori pxGrid sono accurato.

Selezionare il opzione Avvia test e attendere che i risultati vengano valutati.



Test di sincronizzazione dei database PxGrid.

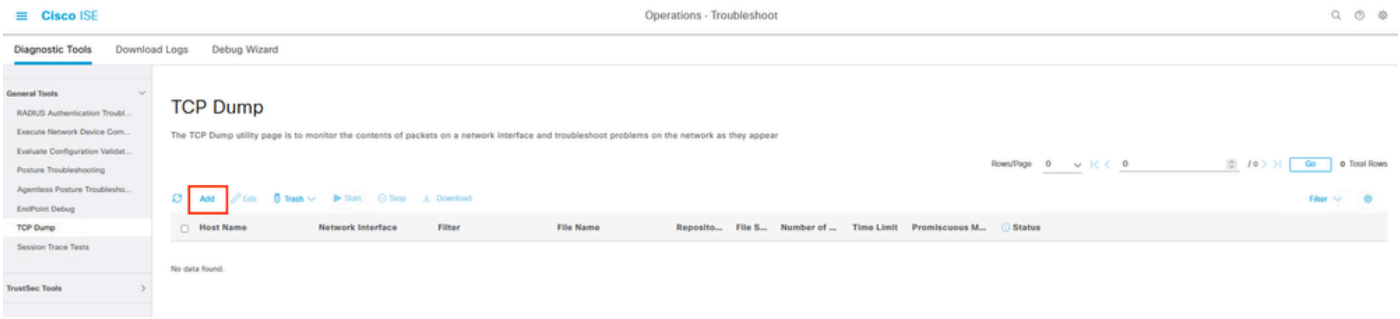
Questo output è stato ottenuto dai log generati.

```
ssptise01.ssptsec.mex : In Sync
ssptise02.ssptsec.mex : In Sync

Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex
```

Raccogli un'acquisizione dai nodi pxGrid che puntano verso il nodo FMC primario.

Passare al menu Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Dump TCP,

Selezionare il opzione a Aggiungi una nuova acquisizione.



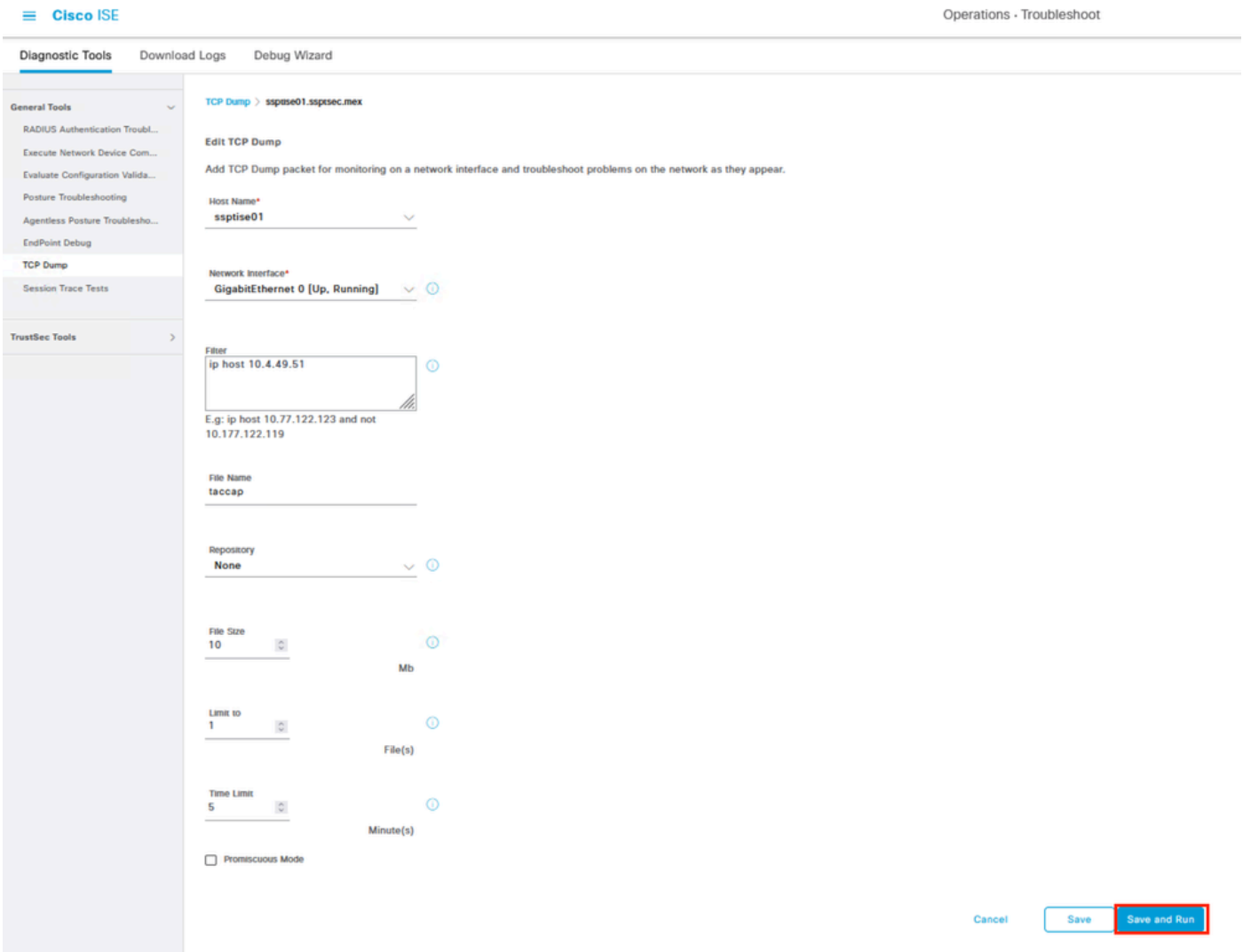
Generazione di un'acquisizione pacchetto su ISE.

Configurare i parametri per l'acquisizione.

Dentro Nome host, selezionare il nodo pxGrid primario selezionato nel CCP.

Filtro il traffico con questo sintassi ip host <FMC IP>

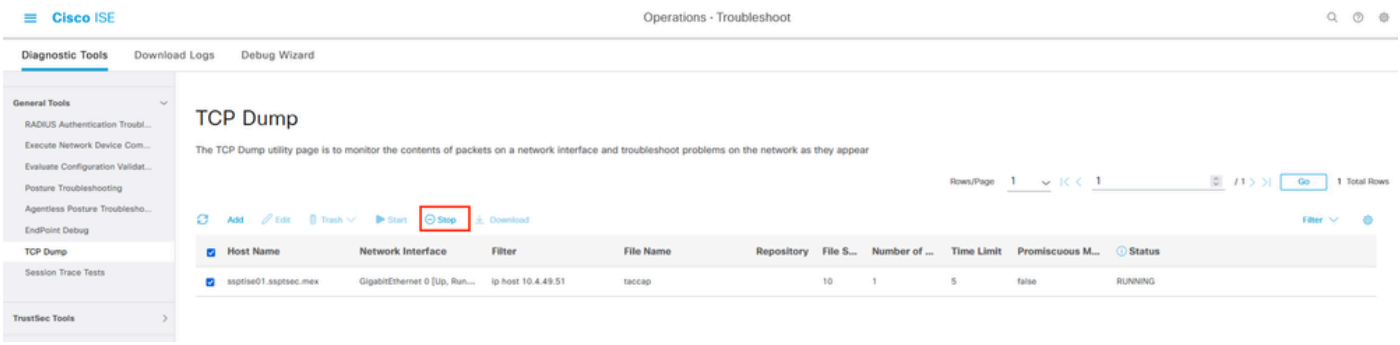
Assegnare un nome all'acquisizione e poi procedere a Salva ed esegui.



Esempio di configurazione di acquisizione pacchetti.

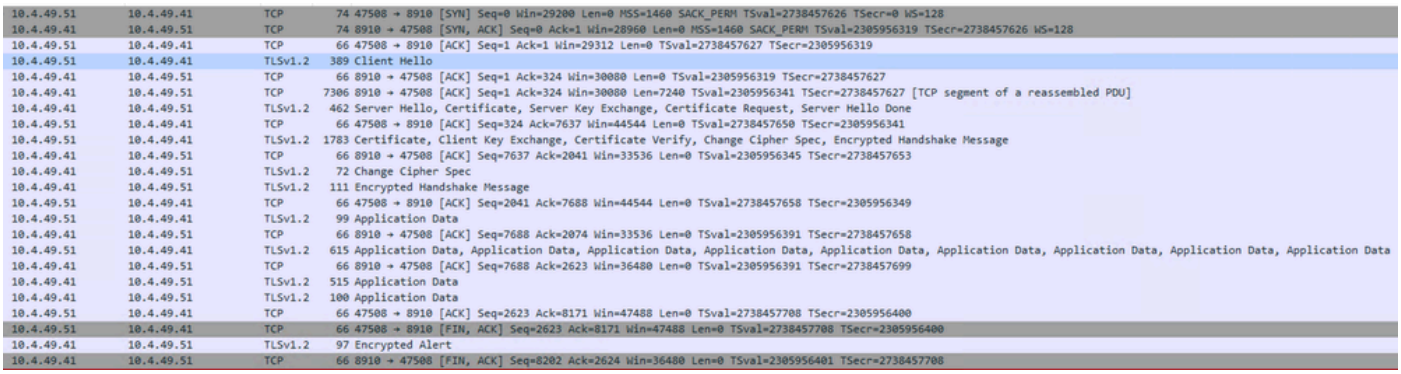
In un'altra finestra, nel menu FMC Integrazione > Altre integrazioni > Identità Fonti, Verificare la connessione con ISE tramite il canale pxGrid.

WQuando ottieni il risultato del test, procedere a Sin alto l'acquisizione ad ISE.



Interruzione dell'acquisizione di un pacchetto su ISE.

Scarica acquisire e avviare l'analisi. In questo scenario viene visualizzata un'acquisizione di una connessione funzionante che può fungere da riferimento.

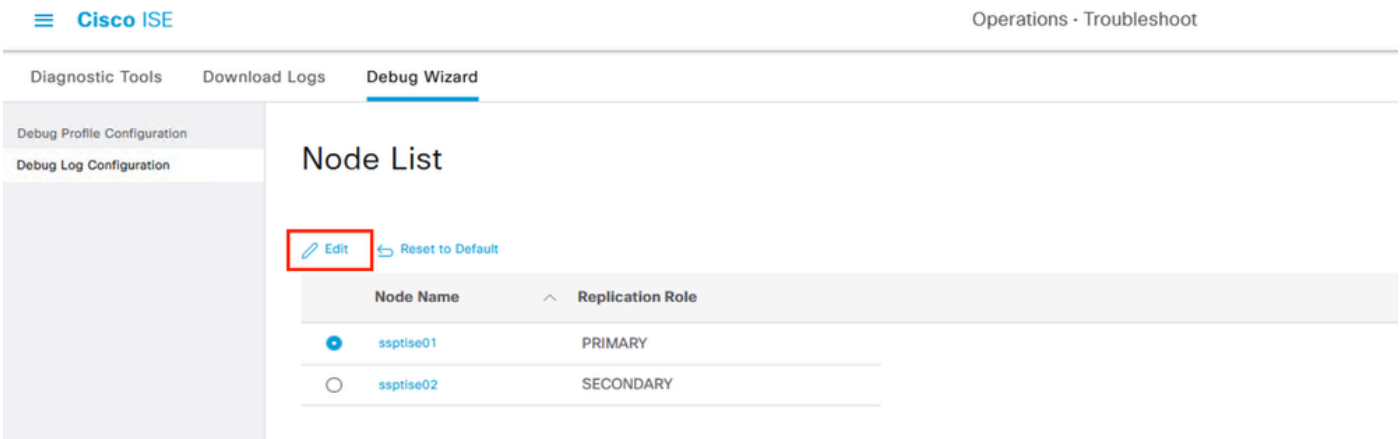


Comunicazione PxGrid tra ISE e FMC.

Inoltre, ad ISE, è possibile raccogliere i debug relativi a pxElaborazione griglia.

Spostarsi nel menu Operazioni > Risoluzione dei problemi > Debug guidato > Debug Configurazione registro,

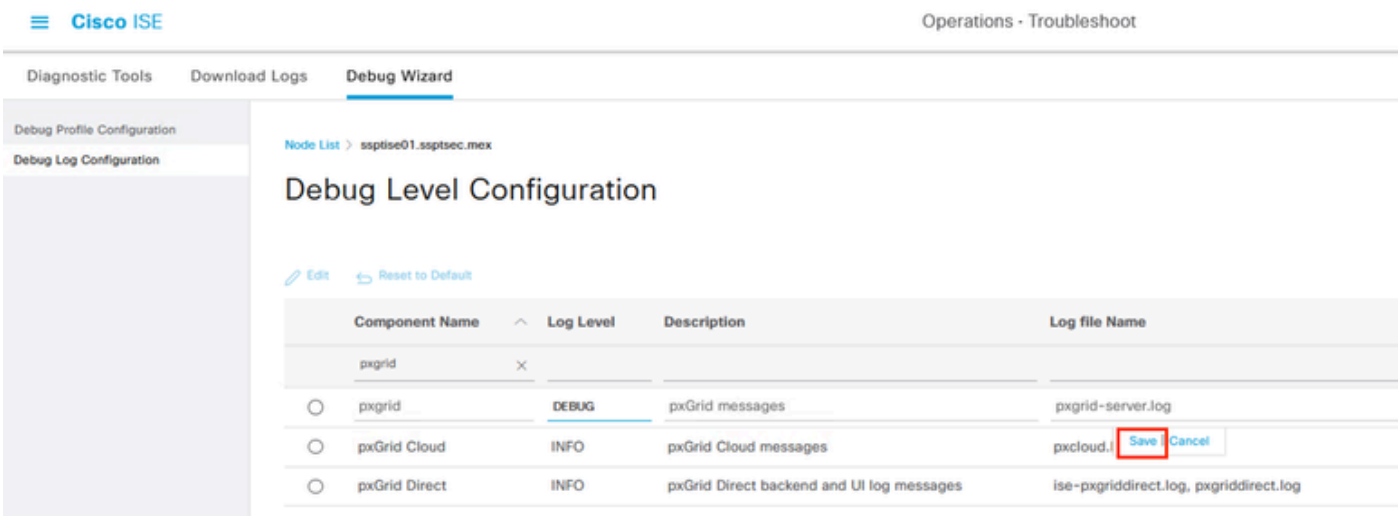
Selezionare il nodo ISE corrispondente da analizzare, quindi Modifica.



Selezione di un nodo di cui eseguire il debug con ISE.

Filtrare i componenti visualizzati e modificare il Livello log su DEBUG di pxgrid componente a procedere con un'analisi.

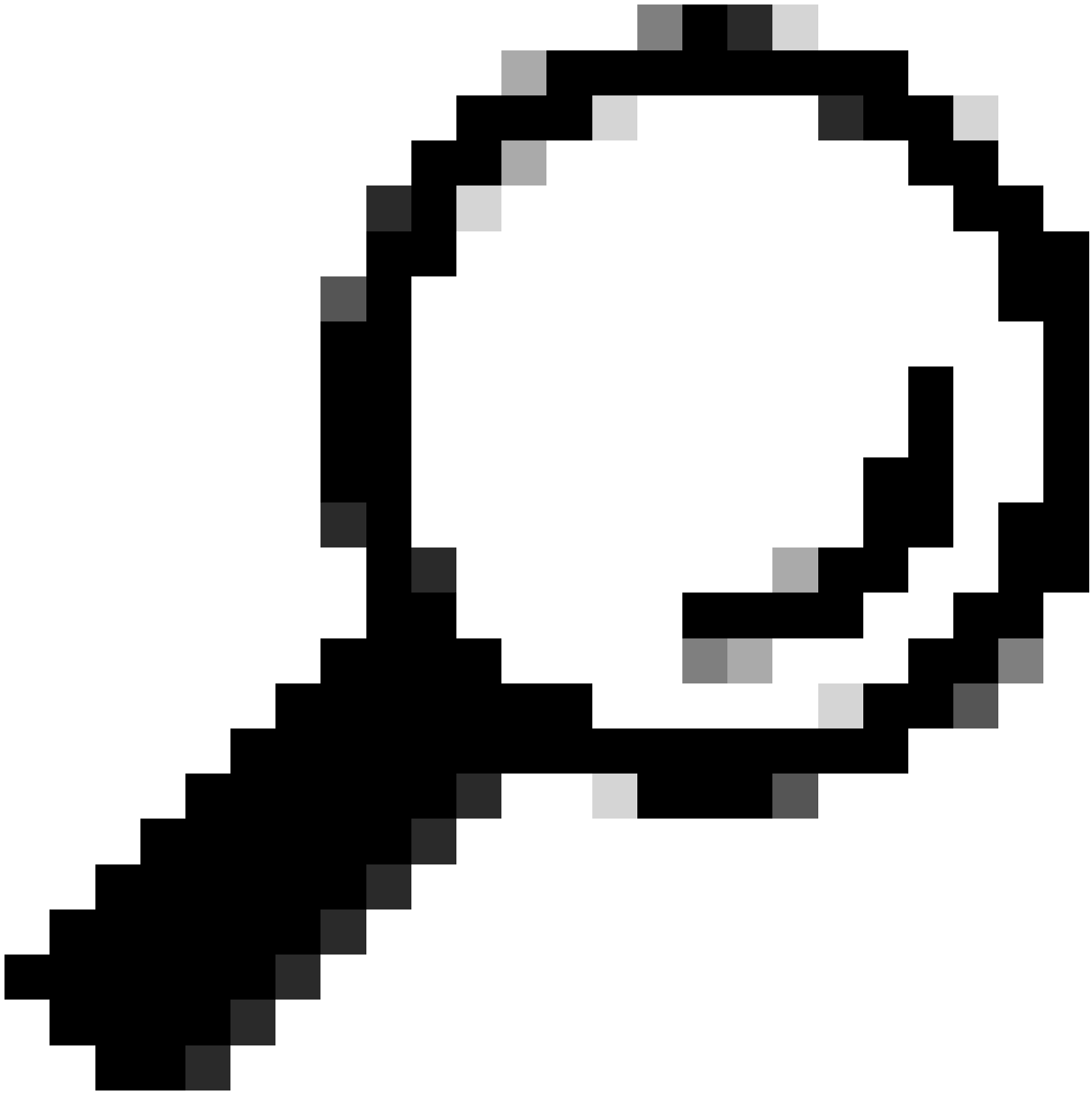
Salva la configurazione.



Modifica del componente pxGrid al livello di debug.

Riprodurre il comportamento da analizzare, quindi procedere per analizzare i registri raccolti nel file pxgrid-server.log. Altri registri da esaminare sul nodo ISE per risolvere i problemi:

```
#show logging application | include pxgrid
ise-pxgriddirect.log
pxgrid/pxgrid-server.log
pxgrid/pxgrid-test.log
pxgrid/pxgrid_dbsync_summary.log
pxgrid/pxgrid_internal_dbsync_summary.log
pxgriddirect.log
```

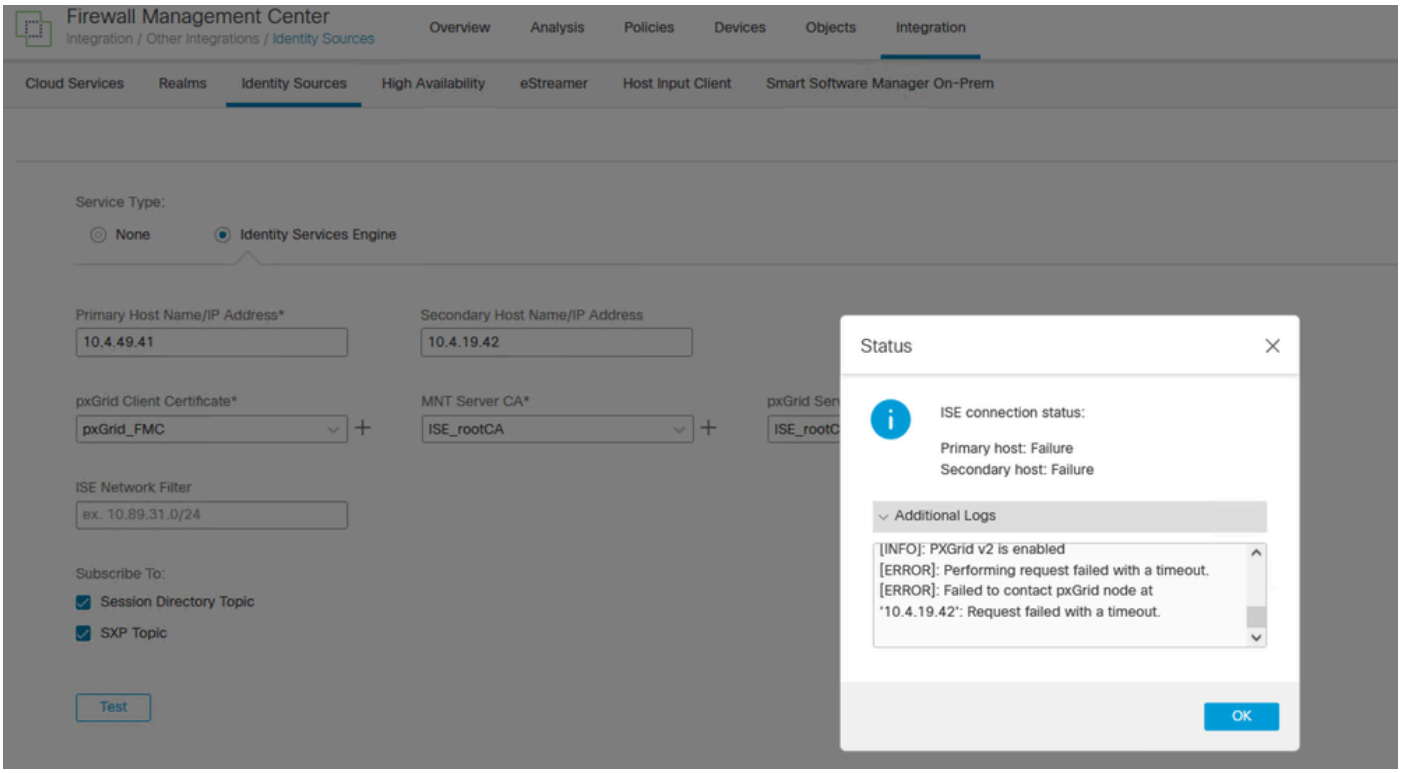


Suggerimento: Per ulteriori consigli sulla raccolta dei log, vedere il video How to Enable Debug on ISE 3.x Versions (Come abilitare i debug sulle versioni ISE 3.x).

Problemi comuni.

Il client sottoscrittore PxGrid non è approvato su ISE.

In questo caso di utilizzo, l'output relativo al pulsante pxGrid del test FMC mostra questo comportamento:



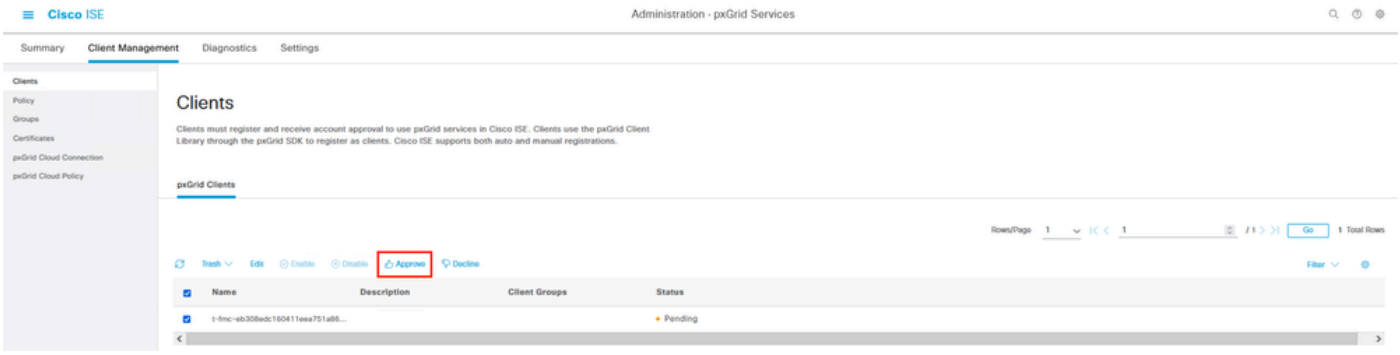
Connessione pxGrid FMC non riuscita.

```
Primary host:

[INFO]: PXGrid v2 is enabled
[ERROR]: pxgrid 2.0: failed account activation. accountState=PENDING
[ERROR]: Failed to contact pxGrid node at '10.4.49.41': pxgrid2.0: Could not activate account

Secondary host:

[INFO]: PXGrid v2 is enabled
[ERROR]: Performing request failed with a timeout.
[ERROR]: Failed to contact pxGrid node at '10.4.19.42': Request failed with a timeout.
```

Su ISE, notare il comportamento nel menu Amministrazione > PxGrid Services > Gestione client > Client che indica che il client pxGrid (FMC) è in attesa di approvazione.

Selezionare il pulsante Approva, confermare la selezione nella finestra successiva e tentare di nuovo l'integrazione.

Questa volta l'integrazione ha successo.

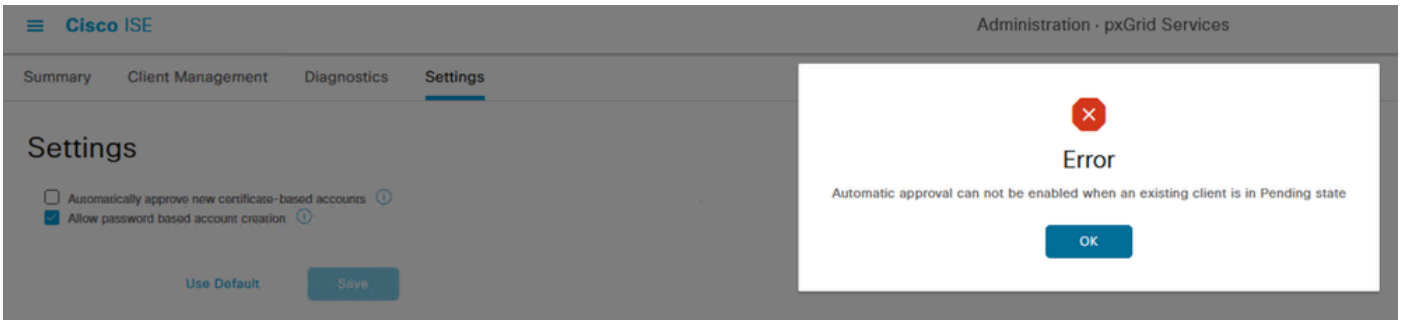


Stato del client FMC in sospeso.

Conferma approvazione del client pxGrid.

Notare se si desidera abilitare l'approvazione automatica dei client pxGrid basati su certificati.

Approvare/Rifiutare i client dalla pagina precedente perché questo allarme può apparire.



Errore relativo all'approvazione dei client pxGrid.

Certificato PxGrid ISE catena incompleto.

In questo scenario, se si passa al menu Amministrazione > Sistema > Certificato, selezionare il certificato pxgrid e selezionare l'opzione Visualizza,

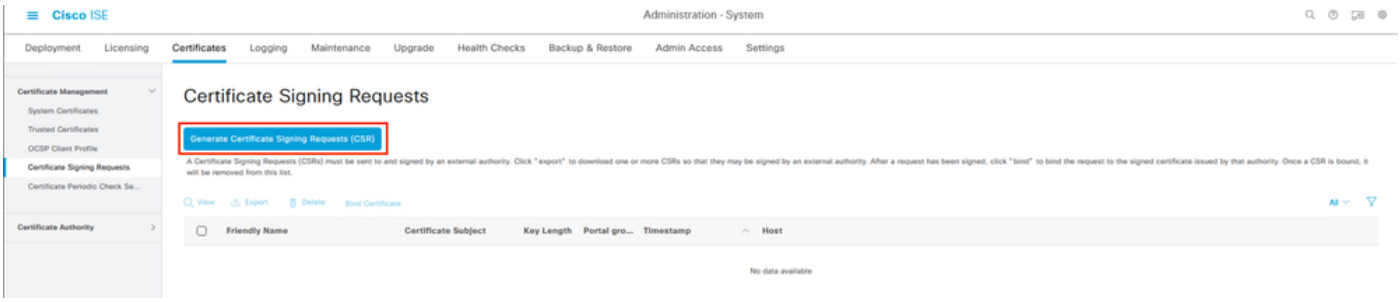
In caso di problemi con il certificato, gli errori correlati sono possibili.

Errore correlato a catena di certificati non completata.

TIl primo passaggio da verificare è se la CA radice ISE è completaterminate nell'opzione Vista (View).

In caso di certificato mancante nella gerarchia, è possibile rilasciare l'intera CA radice di distribuzione ISE.

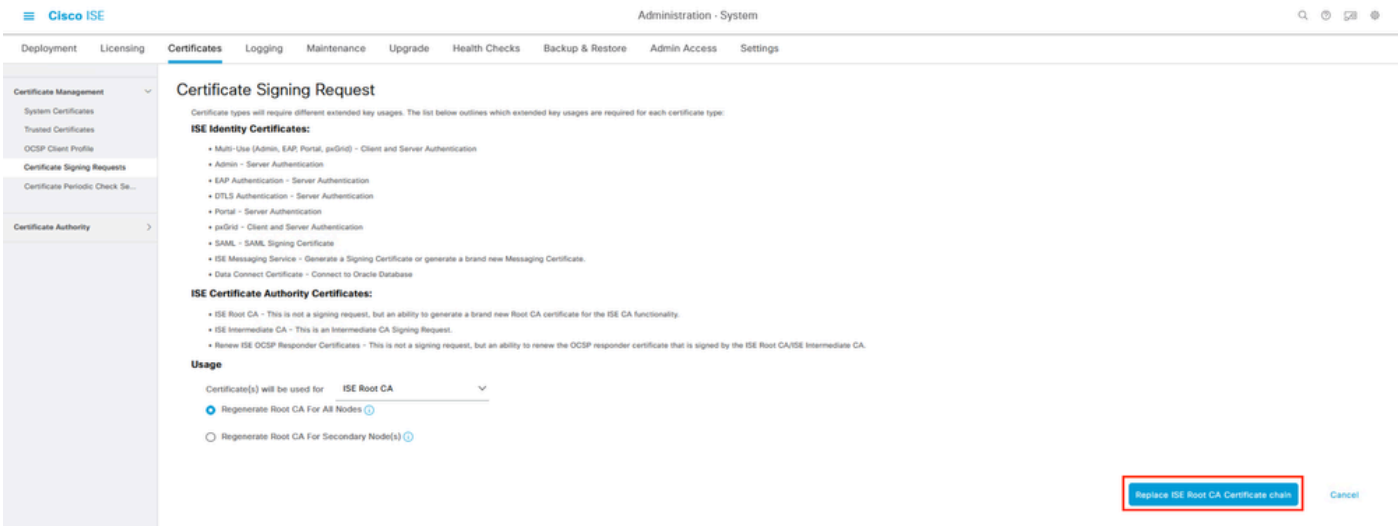
BSelezionare il menu Amministrazione > Sistema > Certificati > Gestione certificati > Richiesta di firma del certificato (CSR) e selezionare il pulsante.



Generazione di un CSR su ISE.

In questo menu selezionare in Uso ISE Root CA e rigenera ISE Root CA per tutti i nodi.

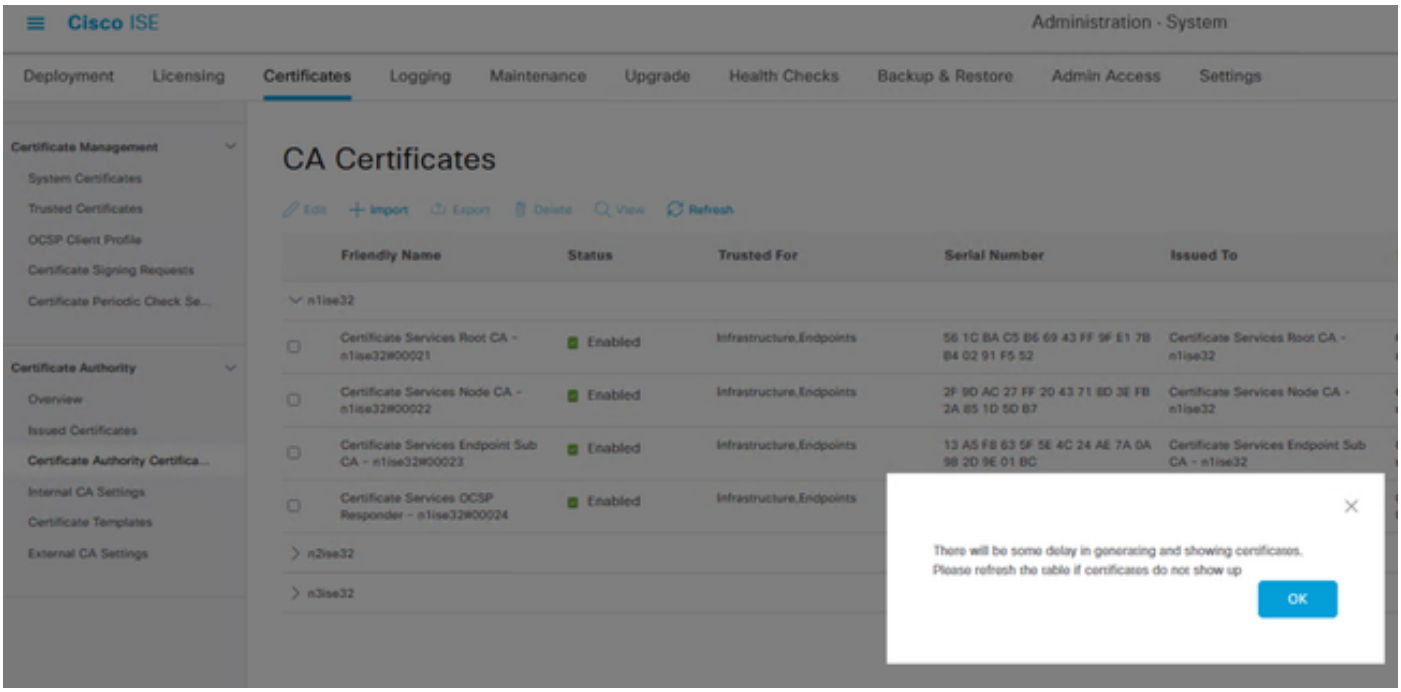
Procedere con il pulsante Sostituisci catena di certificati CA radice ISE.



Configurazione della richiesta di firma del certificato.

Attendere che i certificati vengano generati in tutti i nodi del provider di servizi Internetdi nobiltà.

Al termine, ISE visualizza la notifica successiva.



Conferma della generazione dei certificati.

Confermare se il pxGcatena di attendibilità del certificato rid completata selezionando l'opzione Visualizza in Certificati di sistema.

Riferimento.

[Pagina per sviluppatori Cisco PxGrid.]

[Guida dell'amministratore di Cisco Identity Services Engine, versione 3.2, capitolo: Cisco PxGrid]

[Guida all'installazione di Cisco Identity Services Engine, versione 3.2, capitolo: Guida di riferimento alle porte Cisco ISE]

[Guida di riferimento alla CLI di Cisco Identity Services Engine, versione 2.4]

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).