

Risoluzione dei problemi relativi all'integrazione Secure Network Analytics (SNA) - Identity Services Engine (ISE) "Connessione non riuscita - Impossibile trovare il servizio in questo cluster ISE"

Sommario

[Introduzione](#)

[CISCO ISE Integration](#)

[Motivi di errore potenziale](#)

[Verifica e risoluzione dei problemi](#)

[Cause note](#)

[Problemi di replica nell'implementazione ISE](#)

[Verifica catena di certificati ISE PxGrid](#)

Introduzione

Questo documento descrive come convalidare i problemi di integrazione ISE per SMC versione 7.3.2 e successive. SNA presenta PxGrid v2.0 per il componente di integrazione ISE con la versione 7.3.2. In questo documento vengono illustrati alcuni messaggi di errore specifici che è possibile visualizzare quando si configura l'integrazione Cisco ISE sulla versione 7.3.2 e successive.

Per ulteriori informazioni su PxGrid v2.0 e sulle relative funzionalità, visitare - [PxGrid v2.0](#)

CISCO ISE Integration

Quando SMC si integra con ISE, richiede di abbonarsi al servizio appropriato in base alle caselle di controllo selezionate nell'interfaccia utente di configurazione -

Integration options ⓘ

Integrated Product ⓘ

- Cisco ISE
- Cisco ISE PIC (Passive Identity Connector)

- Adaptive Network Control ⓘ
- Static SGT Classifications ⓘ
- Sessions ⓘ
- Track sessions derived from machine authentications ⓘ

Servizi ISE

In base alle caselle di controllo selezionate, SMC può richiedere:

Servizio: com.cisco.ise.config.anc

Servizio: com.cisco.ise.trustsec

Servizio: com.cisco.ise.session

Servizio: com.cisco.ise.pubsub

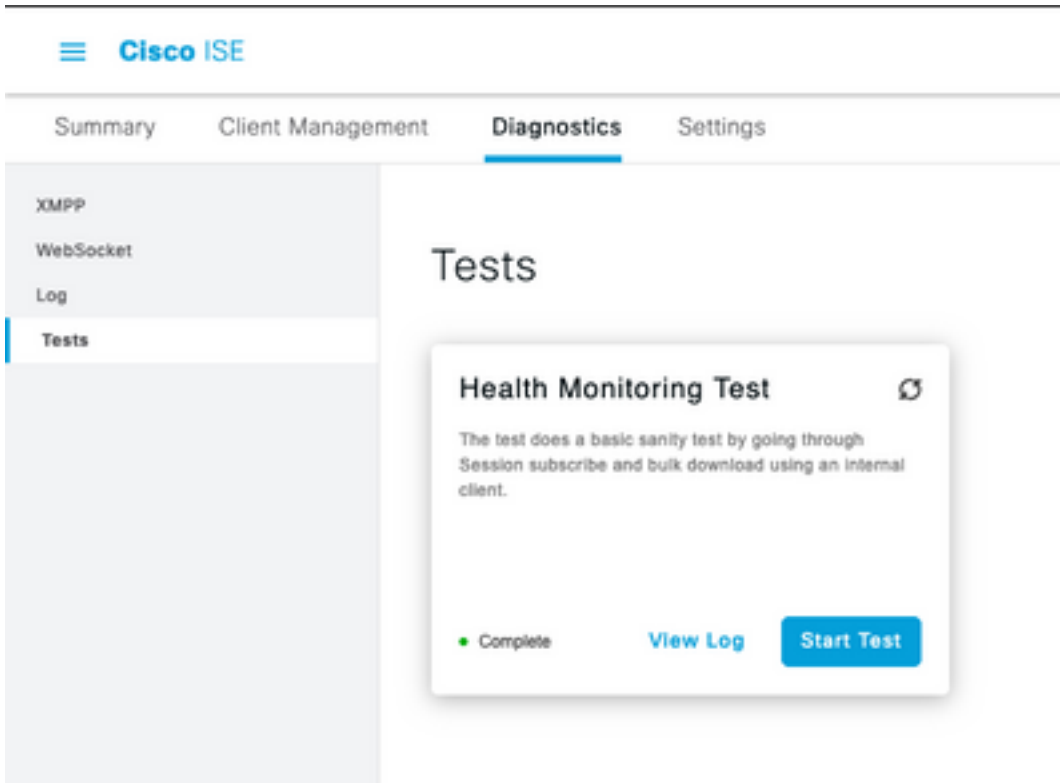
A sua volta, SMC comunica con un nodo ISE per abbonarsi al servizio. Quando SMC richiede un servizio al nodo ISE, si aspetta di sapere quali nodi ISE possono servire quell'argomento o servizio.

Motivi di errore potenziale

- "Stato connessione: impossibile trovare il servizio com.cisco.ise.pubsub non riuscito in questo cluster ISE"
- "Stato connessione: impossibile trovare il servizio com.cisco.ise.anc non riuscito in questo cluster ISE."
- "Stato connessione: impossibile trovare il servizio com.cisco.ise.session non riuscito in questo cluster ISE."
- "Stato connessione: impossibile trovare il servizio com.cisco.ise.trustsec non riuscito in questo cluster ISE."

Verifica e risoluzione dei problemi

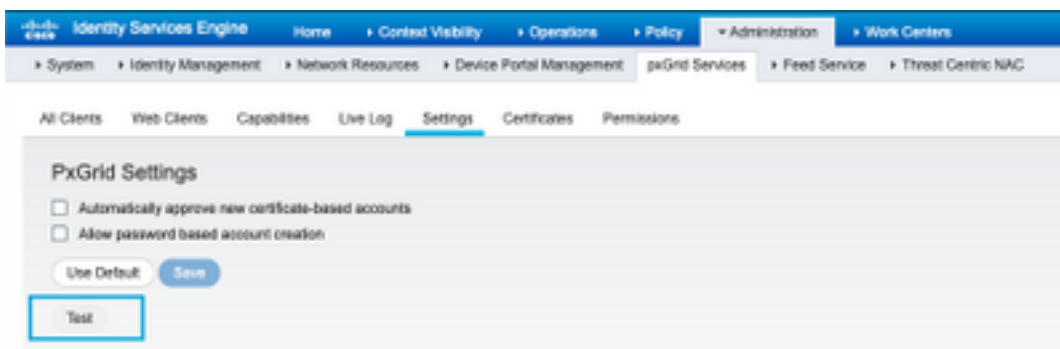
Selezionare **Amministrazione > Servizi PxGrid > Diagnostica > Test** ed eseguire lo strumento di test Monitoraggio stato (ISE 3.0 e versioni successive)



Strumento di test

monitoraggio dello stato

Per ISE 2.4, 2.6 e 2.7:



Strumento di test

monitoraggio dello stato

I risultati del test possono essere visualizzati nella CLI del nodo PXGrid indicato nel piè di pagina della pagina in cui è presente Connected via XMPP <nomehost>.

Eseguire il comando "**show logging application pxgrid/pxgrid-test.log**"

L'output quando il collegamento è riuscito indica:

```
asc-ise24p12-347/admin# applicazione show logging pxgrid/pxgrid-test.log
2021-10-29 01:46:32 INFO TestGridConnection:55 - Avvio della connessione di test pxgrid.....
2021-10-29 01:46:33 INFO TestGridConnectionHelper:307 - SUMMARY>
Subscribe=CONNECTING,session-cnt=0; BulkDownload=NON AVVIATO,bd-session-cnt=0
2021-10-29 01:46:33 INFO Configurazione:313 - Connessione all'host asc-ise24p12-
347.rtpaaa.net
2021-10-29 01:46:33 INFO Configurazione:318 - Connesso OK all'host asc-ise24p12-
347.rtpaaa.net
2021-10-29 01:46:33 INFO Configurazione:343 - Accesso client all'host asc-ise24p12-
347.rtpaaa.net
2021-10-29 01:46:34 INFO Configurazione:345 - Accesso client OK per l'host asc-ise24p12-
```

347.rtpaaa.net

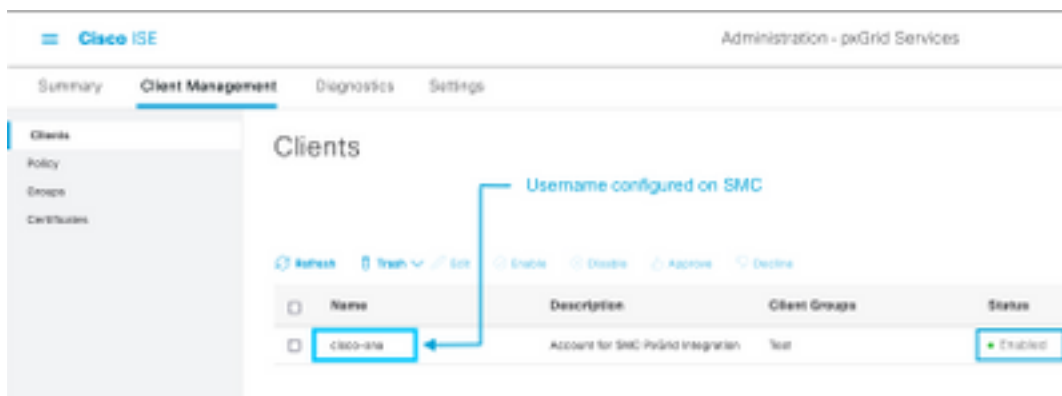
```
2021-10-29 01:46:35 INFO NotificationHandlerSmack:70 - fine aggiornamento stato connessione.
2021-10-29 01:46:35 INFO TestGridConnectionHelper:312 - SUMMARY>
Subscribe=CONNECTED,session-cnt=0; BulkDownload=NON AVVIATO,bd-session-cnt=0
2021-10-29 01:50:36 INFO TestGridConnection:164 - SUMMARY>
Subscribe=CONNECTED,session-cnt=0;BulkDownload=SUCCESS,bd-session-cnt=0
2021-10-29 01:50:36 INFO NotificationHandlerSmack:81 - stato connessione cancellato...
2021-10-29 01:50:36 INFO TestGridConnectionHelper:322 - Client disconnesso
2021-10-29 01:50:36 INFO TestGridConnection:75 - SUMMARY>
Subscribe=DISCONNECTED,session-cnt=0;BulkDownload=DISCONNECTED,bd-session-cnt=0
```

Verificare se l'account utilizzato per collegare SMC ad ISE è abilitato:

Verificare che il client sia approvato e, se è in sospeso, approvarlo

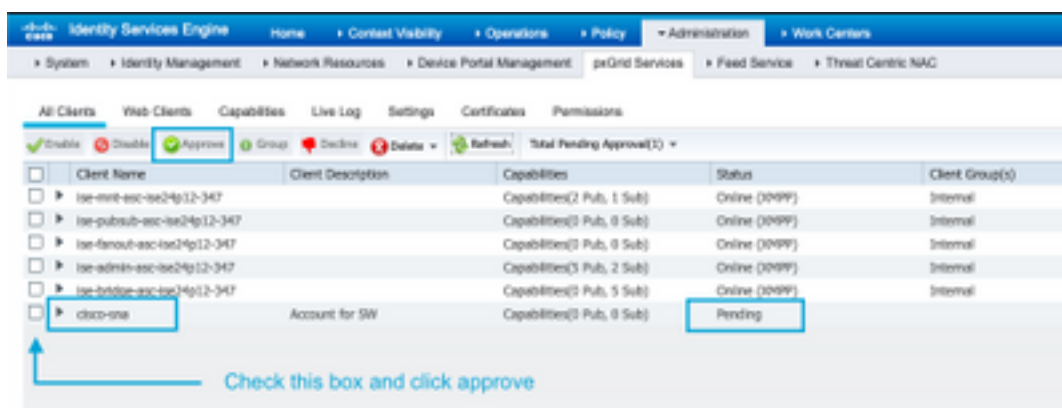
ISE 3.0 e successive:

Amministrazione > Servizi PxGrid > Gestione client > Client:



ISE 2.4, 2.6 e 2.7:

Amministrazione > Servizi PxGrid > Tutti i client



Per verificare lo stato della connessione del client SMC PxGrid e il nodo ISE a cui è connesso, selezionare **Amministrazione > Servizi PxGrid > Diagnostica > WebSocket**



Cause note

- I nodi con PxGrid Persona abilitata devono affrontare problemi di replica nell'implementazione ISE
- Problemi relativi all'attendibilità dei certificati PxGrid

Problemi di replica nell'implementazione ISE

La replica è fondamentale per mantenere aggiornate le informazioni su tutti i nodi membri di una distribuzione. Se un nodo che esegue la persona PxGrid segnala problemi di replica, è possibile che non disponga di informazioni aggiornate sugli argomenti e i servizi che può servire per i client PxGrid.

Se il nodo segnala un errore di replica o una replica lenta:



Replication Failed

O



Slow Replication Error

Questa è una possibile causa del fallimento dell'integrazione.

Per intraprendere azioni correttive:

Verificare la connettività IP con il nodo ISE, accedere tramite SSH e verificare che i servizi siano in esecuzione emettendo:

```
# show application status ise
```

Esempio

```
asc-ise30p2-353/admin# mostra stato applicazione ise
```

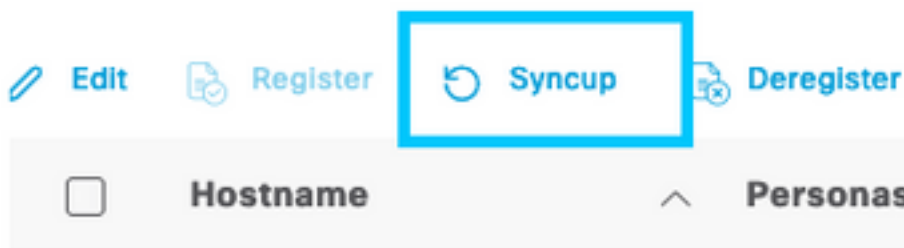
```
ISE NOME PROCESSO STATO ID PROCESSO
```

Listener del database con 24872 in esecuzione
Server di database che esegue 114 PROCESSES
Application Server con 40137
Database Profiler con 35916
Motore di indicizzazione ISE disabilitato
Connettore AD con 40746
Database sessione M&T disabilitato
Processore log M&T disabilitato
Servizio Autorità di certificazione con 40609
Servizio EST con 7903
Servizio motore SXP disabilitato
Docker Daemon con 28517
Servizio TC-NAC disabilitato
Servizio PxGrid Infrastructure disabilitato
Servizio sottoscrittore del server di pubblicazione pxGrid disabilitato
Gestione connessione pxGrid disabilitata
Controller pxGrid disabilitato
Servizio WMI PassiveID disabilitato
Servizio syslog ID passivo disabilitato
Servizio API PassiveID disabilitato
Servizio Agente ID passivo disabilitato
Servizio endpoint ID passivo disabilitato
Servizio SPAN ID passivo disabilitato
Server DHCP (dhcpd) disabilitato
Server DNS (denominato) disabilitato
Servizio di messaggistica ISE con 29277
Servizio database gateway API ISE con 32173
Servizio ISE API Gateway con 38161
Servizio criteri di segmentazione disabilitato
Servizio autenticazione REST disabilitato
Connettore SSE disabilitato

Eseguire la sincronizzazione manuale del nodo interessato in **Amministrazione > Sistema > Distribuzione**

Selezionare i problemi di segnalazione del nodo e fare clic su **Sincronizza**

Deployment Nodes



Nota: Ciò determina il riavvio dei servizi nel nodo da sincronizzare e potrebbe rendere il nodo fuori

servizio per 30 minuti. Si consiglia di eseguire questa attività in una finestra di modifica controllata.

Verifica catena di certificati ISE PxGrid

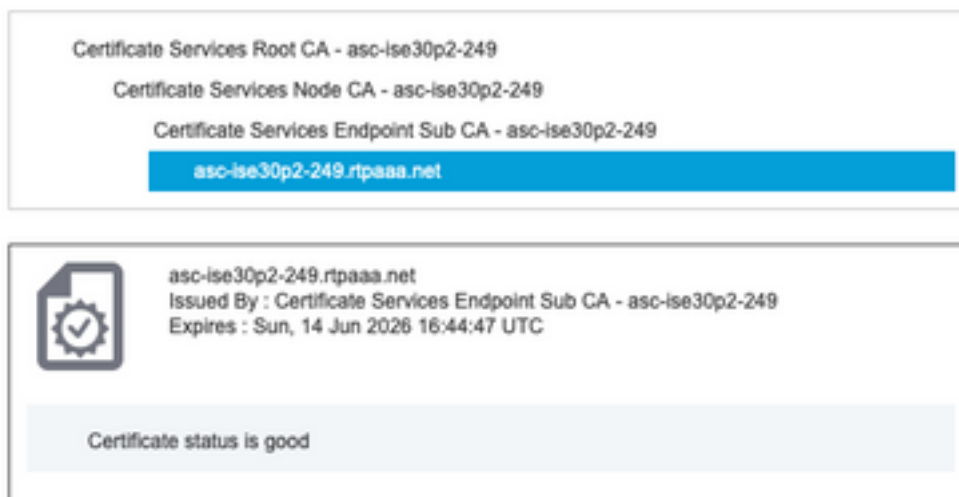
Selezionare **Amministrazione > Sistema > Certificati** sull'interfaccia utente di ISE

A ogni nodo con l'utente PxGrid abilitato è associato un certificato con il ruolo PxGrid.

Questi certificati possono essere firmati da un'autorità di certificazione di terze parti o dall'autorità di certificazione interna ISE. Selezionare la casella accanto al certificato e alla visualizzazione attiva, in cui sono elencati i dettagli del certificato e la catena di certificati. Nei dettagli del certificato è inoltre presente un indicatore di stato che indica se il certificato è valido o se la catena è incompleta.

Se il certificato è firmato dalla CA interna di ISE:

Certificate Hierarchy



Sono disponibili 4 livelli, a partire dall'alto:

1. ISE Root CA - Questo è il certificato CA e ogni distribuzione ha solo 1 ISE Root CA che è il nodo Admin primario.
2. ISE Node CA - Si tratta di una CA intermedia il cui certificato è rilasciato dalla CA radice ISE ed è anche il nodo Admin primario
3. ISE Endpoint Sub CA - Terzo livello e emittente del certificato di identità PxGrid. Ogni nodo dell'implementazione ha la propria ISE Endpoint Sub CA rilasciata da ISE Node CA (Primary Admin node)
4. Certificato di identità PxGrid - Si tratta del certificato che il nodo ISE presenta a un client PxGrid, ad esempio SMC durante l'integrazione e la comunicazione

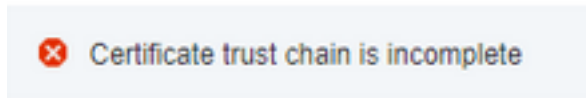
Se si dispone di un certificato firmato dalla CA dell'organizzazione indipendente da ISE e/o da una CA nota di terze parti:

Verificare che la CA radice e le CA intermedie che hanno firmato il certificato PxGrid siano installate nell'archivio dei certificati di sicurezza attendibili su ISE in **Amministrazione > Sistema >**

Certificati > Gestione certificati > Certificati attendibili

In entrambi i casi, quando si visualizza il certificato, l'interfaccia utente deve indicare **"Stato certificato valido"**.

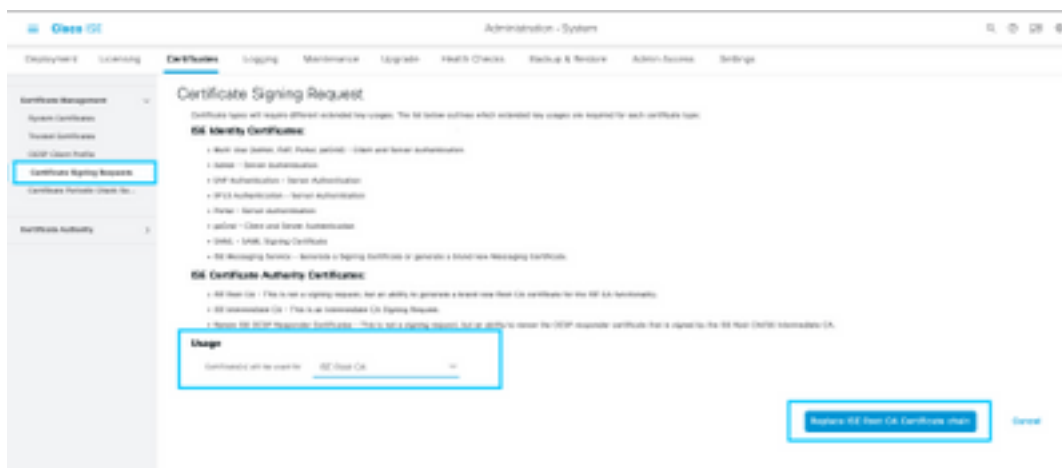
Condizione di errore:



Problemi relativi all'attendibilità dei certificati PxGrid

Se la catena di certificati è incompleta quando la CA interna ISE è in uso, è necessario rigenerare la CA radice ISE che rigenera i certificati ISE PxGrid come parte del processo. Aggiornare l'archivio di attendibilità del CSM con la CA radice ISE appena generata e la CA nodo ISE dall'amministratore primario e il certificato della CA secondaria dell'endpoint ISE da ogni nodo PxGrid.

Per sostituire la catena di CA radice ISE, selezionare **Amministrazione > Sistema > Certificati > Gestione certificati > Richieste di firma del certificato** e selezionare **Genera richiesta di firma del certificato** che presenta questa interfaccia utente:



Nell'elenco a discesa, selezionare **ISE Root CA** e selezionare **Replace ISE Root CA Certificate Chain**

Se la catena di certificati è incompleta quando una CA esterna è in uso, aggiungere i certificati mancanti all'archivio di certificati ISE in **Amministrazione > Sistema > Certificati > Gestione certificati > Certificati attendibili** e riavviare i servizi sul nodo eseguendo il comando "application stop ise" seguito da "application start ise" nella CLI di ISE. I certificati CA vengono aggiunti accedendo alla GUI della distribuzione ISE sul nodo di amministrazione principale, ma i servizi devono essere riavviati tramite CLI sul nodo che ha visualizzato l'errore di stato del certificato.

Nota: Il riavvio dei servizi disconnette il nodo per 15-20 minuti.

Se i problemi persistono dopo aver preso queste misure correttive, contattare il [supporto](#) per assistenza.

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).