

# Configurazione di un Syslog Server esterno su ISE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione destinazione registrazione remota \(UDP Syslog\)](#)

[Esempio](#)

[Configurazione destinazione remota in Categorie di registrazione](#)

[Informazioni sulle categorie](#)

[Verifica e risoluzione dei problemi](#)

---

## Introduzione

Questo documento descrive come configurare External Syslog Server su ISE.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE).
- Server Syslog

### Componenti usati

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

- Identity Services Engine (ISE) versione 3.3.
- Kiwi Syslog Server v1.2.1.4

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

I messaggi syslog provenienti da ISE vengono raccolti e archiviati da log collector. Questi agenti di raccolta log vengono assegnati ai nodi di monitoraggio in modo che MnT memorizzi i log raccolti localmente.

Per raccogliere i registri esternamente, è necessario configurare i server syslog esterni, denominati destinazioni. I log vengono classificati in varie categorie predefinite.

È possibile personalizzare l'output di registrazione modificando le categorie in base alle destinazioni, al livello di gravità e così via.

## Configurazione

È possibile utilizzare l'interfaccia Web per creare destinazioni remote del server syslog a cui vengono inviati i messaggi del registro eventi di sistema. I messaggi di log vengono inviati alle destinazioni remote del server syslog in base allo standard del protocollo syslog (vedere RFC-3164).

### Configurazione destinazione registrazione remota (UDP Syslog)



Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu ( ) e scegliere Amministrazione>Sistema>Log>Destinazioni di log remoto > Fare clic su Aggiungi.



Nota: questo esempio di configurazione si basa su uno screenshot intitolato: Configurazione destinazione di registrazione remota.

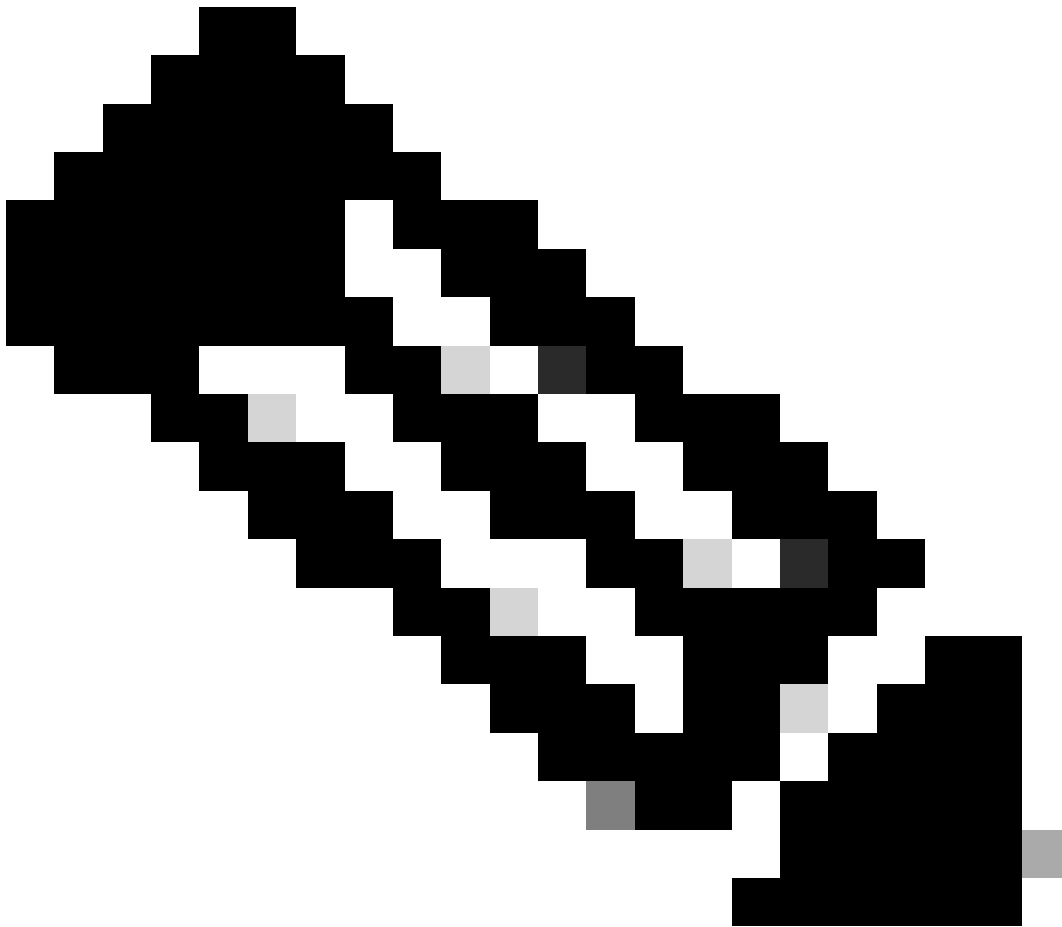
- 
- Nome come Remote\_Kiwi\_Syslog, qui è possibile immettere il nome del server Syslog remoto, utilizzato per scopi descrittivi.
  - Tipo di destinazione come UDP Syslog, in questo esempio di configurazione viene utilizzato UDP Syslog; tuttavia, è possibile configurare altre opzioni dall'elenco a discesa Tipo di destinazione:

UDP Syslog: utilizzato per l'invio di messaggi syslog su UDP, adatto per la registrazione rapida e leggera.

TCP Syslog: utilizzato per l'invio di messaggi syslog tramite TCP, che fornisce affidabilità con controllo degli errori e funzionalità di ritrasmissione.

Secure Syslog: si riferisce ai messaggi syslog inviati tramite TCP con crittografia TLS, che garantiscono l'integrità e la riservatezza dei dati.

- Status as Enabled, è necessario scegliere Enabled dall'elenco a discesa Status.
  - Descrizione, facoltativamente è possibile inserire una breve descrizione della nuova destinazione.
  - Indirizzo host/IP, in cui è possibile immettere l'indirizzo IP o il nome host del server di destinazione in cui sono archiviati i registri. Cisco ISE supporta i formati IPv4 e IPv6 per la registrazione.
- 



Nota: se si intende configurare un server syslog con FQDN, è necessario configurare la memorizzazione nella cache DNS per evitare l'impatto sulle prestazioni. Senza la cache DNS, ISE esegue query sul server DNS ogni volta che un pacchetto syslog deve essere inviato alla destinazione di registrazione remota configurata con FQDN. Questo ha un forte impatto sulle prestazioni di ISE.

Utilizzare `service cache enable` il comando in tutti i PSN della distribuzione per risolvere il problema:

---

---

## Esempio

```
ise/admin(config)# service cache enable hosts ttl 180
```

---

- **Port as 514**, in questo esempio di configurazione, il server Syslog Kiwi è in ascolto sulla porta **514**, che è la porta predefinita per i messaggi syslog UDP. Tuttavia, gli utenti possono modificare questo numero di porta in qualsiasi valore compreso tra 1 e 65535. Assicurarsi che la porta desiderata non sia bloccata da alcun firewall.
- **Codice struttura** come **LOCAL6**, è possibile scegliere il codice struttura syslog da utilizzare per la registrazione dall'elenco a discesa. Le opzioni valide sono da Local0 a Local7.
- **Lunghezza massima: 1024**, in cui è possibile immettere la lunghezza massima dei messaggi di destinazione del log remoto. La lunghezza massima è impostata su **1024** per default nella versione ISE 3.3. I valori sono compresi tra 200 e 1024 byte.



**Nota:** per evitare di inviare messaggi troncati alla destinazione di registrazione remota, è possibile modificare la lunghezza massima come 8192.

---

- **Includi allarmi per questa destinazione**, per semplificarne la gestione, in questo esempio di configurazione l'opzione **Includi allarmi per questa destinazione** non è selezionata; tuttavia, quando si seleziona questa casella di controllo, vengono inviati messaggi di allarme anche al server remoto.

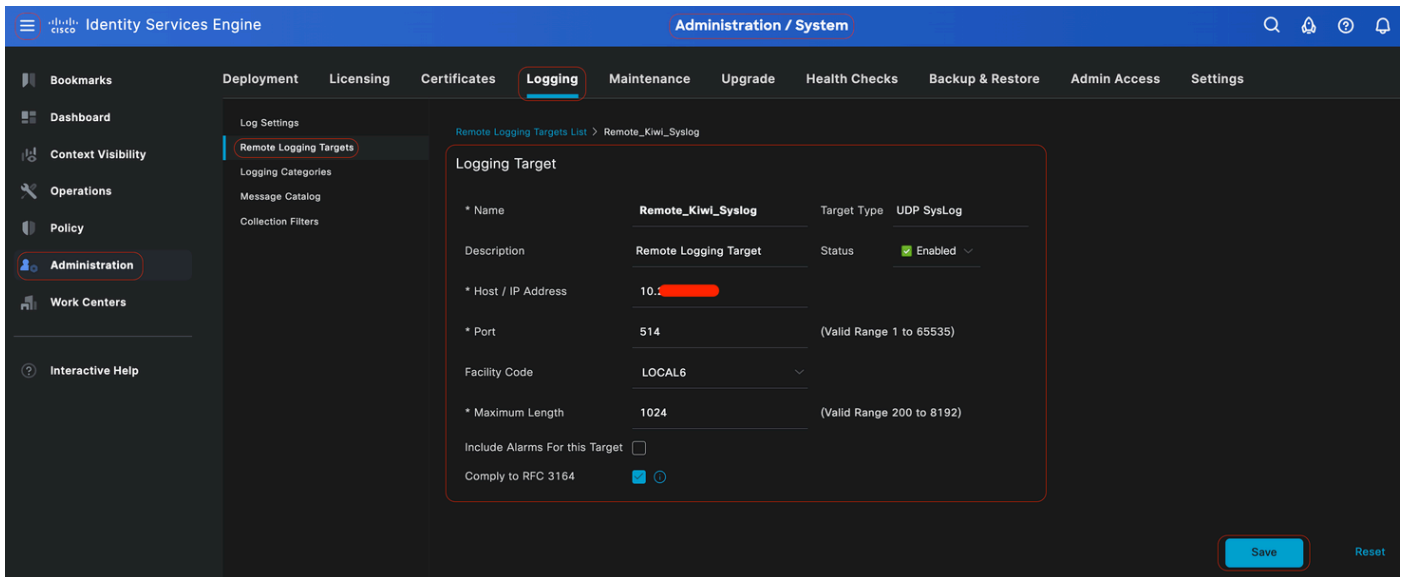
- **L'opzione Conformità alla RFC 3164** è selezionata. Quando si seleziona questa casella di controllo, i delimitatori (, ; { } \\ \) nei messaggi syslog inviati ai server remoti non vengono ignorati anche se si utilizza la barra rovesciata (\).

- 

Al termine della configurazione, fare clic su **Save** (Salva).

•

Dopo il salvataggio, il sistema visualizzerà questo avviso: **si è scelto di creare una connessione non protetta (TCP/UDP) al server. Continuare?**, fare clic su **Sì**.



Configurazione destinazione remota

Configurazione destinazione remota in Categorie di registrazione

Cisco ISE invia eventi verificabili alla destinazione syslog. Una volta configurata la destinazione di registrazione remota, è necessario mappare la **destinazione di registrazione remota** alle categorie previste per inoltrare gli eventi controllabili.

Le destinazioni di registrazione possono quindi essere mappate a ognuna di queste categorie di registrazione. I registri eventi generati da queste categorie di registro vengono generati solo dai nodi PSN e possono essere configurati in modo da inviare i registri rilevanti al server Syslog remoto a seconda dei servizi abilitati in tali nodi:

•

**Audit AAA**

•

**Diagnostica AAA**

•

**Contabilità**

•

## **MDM esterno**

- 

## **ID passivo**

- 

## **Controllo della postura e del provisioning client**

- 

## **Diagnostica provisioning postura e client**

- 

## **Profiler**

I registri eventi generati da queste categorie di registro vengono generati da tutti i nodi nella distribuzione e possono essere configurati in modo da inviare i registri pertinenti al server Syslog remoto:

- 

## **Audit amministrativo e operativo**

- 

## **Diagnostica di sistema**

- 

## **Statistiche di sistema**

In questo esempio di configurazione, si configurerà la destinazione remota in quattro categorie di registrazione, queste 3 per inviare i log del traffico di autenticazione: **Autenticazioni passate**, **Tentativi non riusciti** e **Accounting Radius** e questa categoria per il traffico di registrazione dell'amministratore ISE:





**Nota: questo esempio di configurazione si basa su uno screenshot intitolato: Configurazione destinazione di registrazione remota**

---

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu (



), quindi selezionare **Amministrazione>Sistema>Registrazione>Categorie di registrazione** e fare clic sulla categoria richiesta (**Autenticazioni passate, Tentativi non riusciti e Accounting Radius**).

**Passaggio 1-Livello di gravità del registro:** un messaggio di evento è associato a un livello di gravità, che consente a un amministratore di filtrare i messaggi e di assegnare loro la priorità. Selezionare il livello di gravità del registro, se necessario. Per alcune categorie di registrazione, questo valore è impostato per impostazione predefinita e non è possibile modificarlo. Per alcune categorie di registrazione, è possibile scegliere uno dei seguenti livelli di gravità da un elenco a discesa:

- 

**FATALE:** livello di emergenza. Questo livello significa che non è possibile utilizzare Cisco ISE e che è necessario eseguire immediatamente l'azione necessaria.

- 

**ERRORE:** questo livello indica una condizione di errore critica.

- 

**AVVERTENZA:** questo livello indica una condizione normale ma significativa. Questo è il livello predefinito impostato per molte categorie di registrazione.

•

**INFORMAZIONI:** questo livello indica un messaggio informativo.

•

**DEBUG:** questo livello indica un messaggio di bug diagnostico.

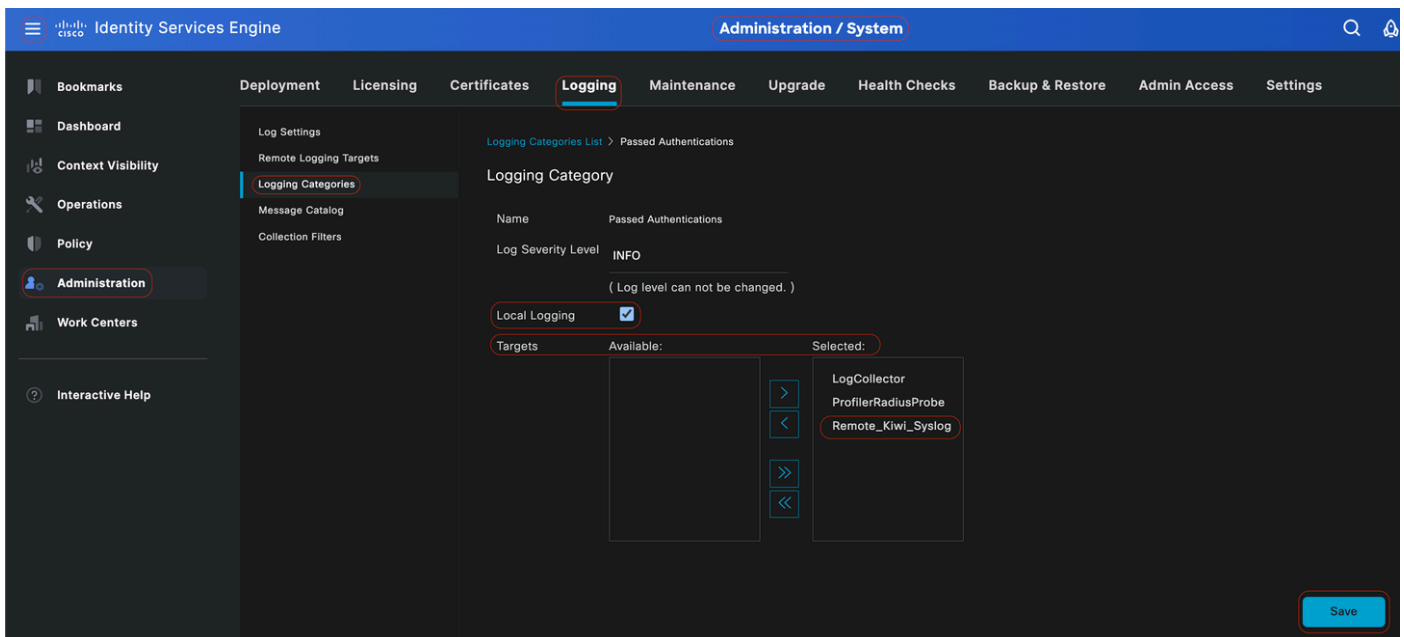
**Passaggio 2- Log locale:** questa casella di controllo abilita la generazione del log locale. Ciò significa che i registri generati dai nomi PSN vengono salvati anche nel nome PSN specifico che genera il registro. È consigliabile mantenere la configurazione predefinita

**Passo 3 - Targets:** quest'area consente di scegliere le destinazioni per una categoria di logging trasferendo le destinazioni tra l'area Available e l'area Selected utilizzando le icone a freccia sinistra e destra.

L'area Available contiene le destinazioni di registrazione esistenti, sia locali (predefinite) che esterne (definite dall'utente).

L'area Selezionati, inizialmente vuota, consente di visualizzare gli oggetti scelti per la categoria.

**Passaggio 4-** Ripetere dal passaggio 1 al passaggio 3 per aggiungere Destinazione remota nelle categorie **Tentativi non riusciti e Accounting Radius**.



*Mapping delle destinazioni remote alle categorie previste*

**Passaggio 5-** Verificare che la destinazione remota sia inclusa nelle categorie richieste. È necessario essere in grado di visualizzare la destinazione remota appena aggiunta.

In questa schermata è possibile visualizzare la destinazione remota **Remote\_Kiwi\_Syslog** mappata alle categorie richieste.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The 'Logging' menu item is highlighted in the top navigation bar. The left sidebar shows the 'Administration' menu item highlighted. The main content area displays a table of logging categories with columns for Parent Category, Category, Targets, Severity, and Local Log status. Several rows are circled in red, including 'Failed Attempts', 'Passed Authentications', 'Administrative and Operational Audit', and 'RADIUS Accounting'.

Parent Category	Category	Targets	Severity	Local Log ...
AAA Audit	AAA Audit	LogCollector	INFO	enable
	Failed Attempts	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
	Passed Authentications	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
AAA Diagnostics	AAA Diagnostics	LogCollector	WARN	enable
	Administrator Authentication and Auth...		WARN	enable
	Authentication Flow Diagnostics		WARN	enable
	Identity Stores Diagnostics		WARN	enable
	Policy Diagnostics		WARN	enable
	RADIUS Diagnostics	LogCollector	WARN	enable
	Guest	LogCollector	INFO	enable
	MyDevices	LogCollector	INFO	enable
	AD Connector	LogCollector	INFO	enable
	TACADS Diagnostics	LogCollector	WARN	enable
ACI Binding	ACI Binding	LogCollector	INFO	enable
Accounting	Accounting	LogCollector	INFO	enable
	RADIUS Accounting	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
	TACADS Accounting	LogCollector	INFO	enable
	Administrative and Operational Audit	LogCollector,Remote_Kiwi_Syslog	INFO	enable
External MDM	External MDM	LogCollector	INFO	enable
PassiveID	PassiveID	LogCollector	INFO	enable
Posture and Client Provisioning Audit	Posture and Client Provisioning Audit	ProfilerRadiusProbe,LogCollector	INFO	enable
Posture and Client Provisioning Diagnostics	Posture and Client Provisioning Diagno...	LogCollector	WARN	enable
Profiler	Profiler	LogCollector	INFO	enable
System Diagnostics	System Diagnostics	LogCollector	WARN	enable
	Distributed Management		WARN	enable
	Internal Operations Diagnostics		WARN	enable
	Licensing	LogCollector	INFO	enable
	Threat Centric NAC	LogCollector	INFO	enable
System Statistics	System Statistics	LogCollector	INFO	enable

Verifica delle categorie

### Informazioni sulle categorie

Quando si verifica un evento, viene generato un messaggio. Esistono diversi tipi di messaggi di eventi generati da più strutture, quali il kernel, la posta, il livello utente e così via.

Questi errori vengono classificati all'interno del Catalogo messaggi e questi eventi sono organizzati gerarchicamente in categorie.

Queste categorie dispongono di Categorie padre contenenti una o alcune categorie.

Categoria padre	Categoria
Audit AAA	Audit AAA Tentativi non riusciti Autenticazione superata
Diagnostica AAA	Diagnostica AAA Autenticazione e autorizzazione

	dell'amministratore Diagnostica flusso di autenticazione Diagnostica archivio identità Diagnostica criteri Diagnostica raggio Guest
Contabilità	Contabilità Accounting Radius
Audit amministrativo e operativo	Audit amministrativo e operativo
Controllo della postura e del provisioning client	Controllo della postura e del provisioning client
Diagnostica provisioning postura e client	Diagnostica provisioning postura e client
Profiler	Profiler
Diagnostica di sistema	Diagnostica di sistema Gestione distribuita Diagnostica delle operazioni interne
Statistiche di sistema	Statistiche di sistema

In questa schermata è possibile vedere che **Guest** è una classe messaggio e classificato come **categoria Guest**. Questa categoria Guest ha una categoria padre chiamata **AAA Diagnostics**.

Category Name	Message Class	Message Code	Message Text	Message Description	Severity
Guest	Guest	86001	Guest user has entered the guest portal login page	Guest user has entered the guest portal login page	INFO
Guest	Guest	86002	Sponsor: Guest user has entered the guest portal login page	Sponsor has suspended a guest user account	INFO
Guest	Guest	86003	Sponsor has enabled a guest user account	Sponsor has enabled a guest user account	INFO
Guest	Guest	86004	Guest user has changed the password	Guest user has changed the password	INFO
Guest	Guest	86005	Guest user has accepted the Use Policy	Guest user has accepted the use policy	INFO
Guest	Guest	86006	Guest user account is created	Guest user account is created	INFO
Guest	Guest	86007	Guest user account is updated	Guest user account is updated	INFO
Guest	Guest	86008	Guest user account is deleted	Guest user account is deleted	INFO
Guest	Guest	86009	Guest user is not found	Guest user record is not found in the database	INFO
Guest	Guest	86010	Guest user authentication failed	Guest user authentication failed. Please check your password and account permis...	INFO
Guest	Guest	86011	Guest user is not enabled	Guest user authentication failed. User is not enabled. Please contact your system ...	INFO
Guest	Guest	86012	User declined Access-Use Policy	Guest user must accept Access-Use policy before network access is granted	INFO
Guest	Guest	86013	Portal not found	Portal is not found in the database. Please contact your system administrator	INFO
Guest	Guest	86014	User is suspended	User authentication failed. User account is suspended	INFO
Guest	Guest	86015	Invalid Password Change	Invalid password change. Use correct password based on the password policy	INFO
Guest	Guest	86016	Guest Timeout Exceeded	Timeout from server has exceeded the threshold. Please contact your system adm...	INFO


## Catalogo messaggi

### Verifica e risoluzione dei problemi

Effettuare un dump TCP sulla destinazione di registrazione remota è il passaggio più rapido per la risoluzione dei problemi e la verifica per confermare se gli eventi di registrazione vengono inviati o meno.

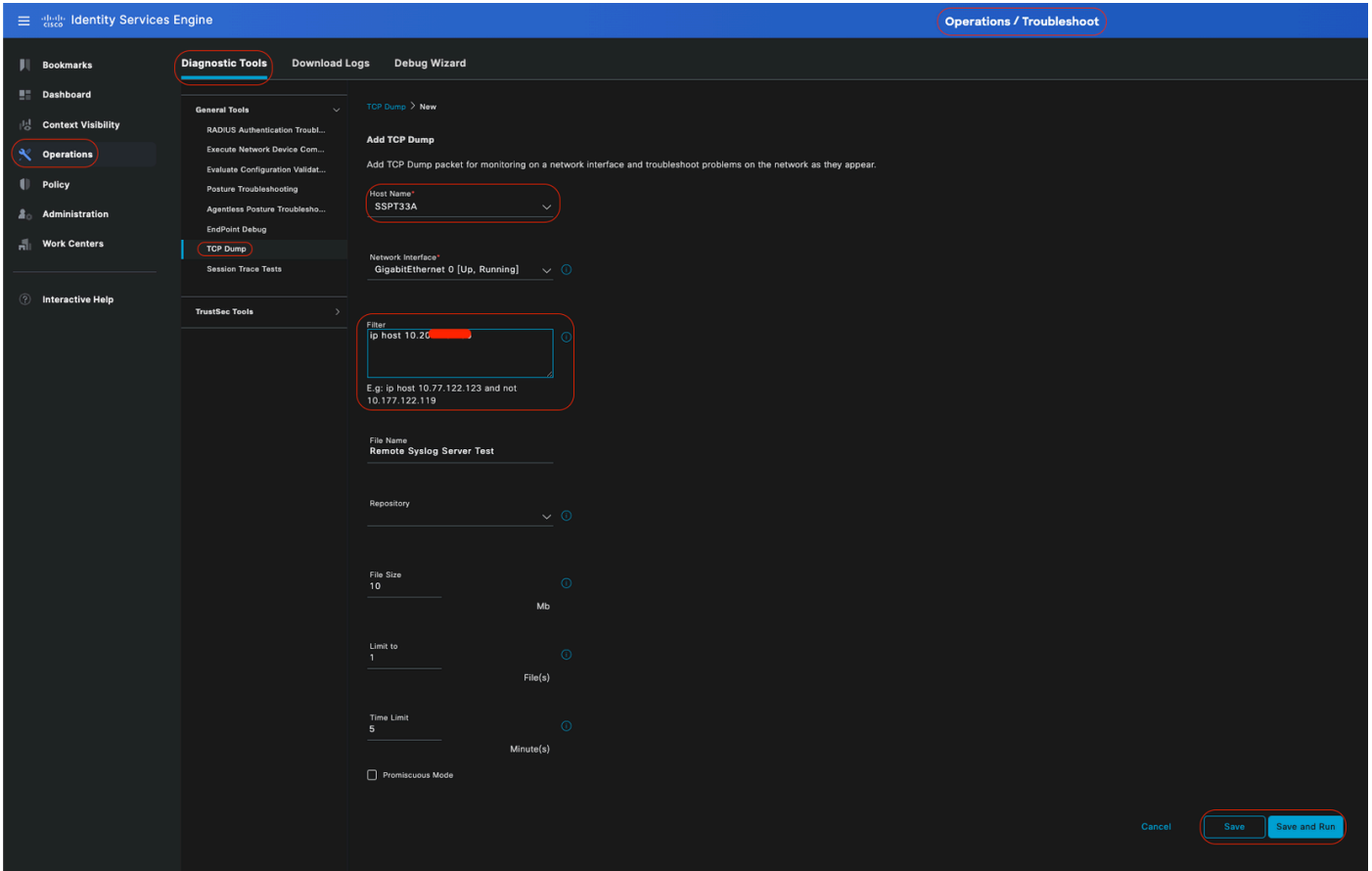
È necessario eseguire l'acquisizione dal PSN che autentica l'utente perché il PSN genererà messaggi di log e questi messaggi verranno inviati alla destinazione remota



Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (  ), quindi selezionare **Operations**> **Troubleshoot**>**TCP Dump**> Fare clic su **Add**.

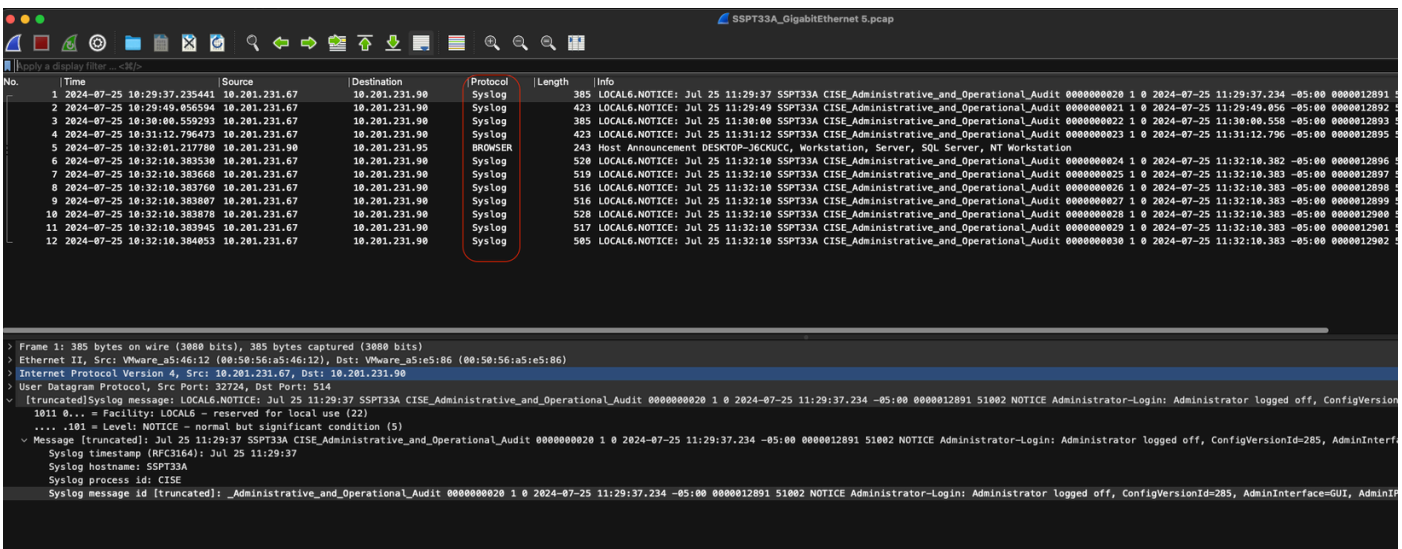
- È necessario filtrare il traffico, aggiungere il campo filtro ip host <indirizzo\_IP\_destinazione\_remota>.

- È necessario acquisire da PSN che gestisce le autenticazioni.



### Dump TCP

In questa schermata, puoi vedere come ISE sta inviando messaggi Syslog per il traffico di registrazione dell'amministratore ISE.



### Traffico syslog





## 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).