

Utilizzare il sistema di debug per risolvere i problemi relativi ad ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Dichiarazione di problema](#)

[1- Cartella di sistema](#)

[Come accedere alla cartella di sistema:](#)

[Esempio di cartelle di sistema disponibili:](#)

[2-Cartella di registrazione](#)

[Prima di iniziare](#)

[Configurazione profilo di debug](#)

[Ripristinare i livelli predefiniti dei componenti](#)

[Come accedere alla cartella di registrazione:](#)

[Alcune cartelle di sistema disponibili](#)

[Suddivisione del comando](#)

[Spiegazione:](#)

[Trova il file necessario](#)

Introduzione

Questo documento descrive come risolvere i problemi e rilevare gli errori mentre si verificano eseguendo i **show logging** comandi dalla CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE).
- Command Line Interface (CLI).

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la versione 3.3 di Identity Services Engine (ISE).

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

ISE sfrutta una struttura specifica per archiviare i file di log, descritti in dettaglio in questo articolo. Per ottenere questo risultato, usare la CLI per eseguire il rilevamento degli errori in tempo reale eseguendo show logging i comandi.

Dichiarazione di problema

Cisco Identity Services Engine (ISE) gestisce cartelle per l'archiviazione dei messaggi di log locali. A seconda della natura del problema, è possibile utilizzare due comandi principalishow logging per la diagnosi e la risoluzione:

1- Cartella di sistema

La cartella System visualizza i syslog di sistema, consentendo di visualizzare gli errori in tempo reale. Questa funzionalità di registrazione consente di identificare problemi relativi al sistema, ad esempio problemi con i servizi ISE.

Come accedere alla cartella di sistema:

È possibile accedere a questa cartella dalla CLI utilizzando questi comandi:

- **show logging system <LogFile>**

Esempio di cartelle di sistema disponibili:

```
SSPT33A/admin#show logging system 5105179 Jul 17 2024 20:09:49 ade/ADE.log 29542 Jan 02 2024 16:36:28 anaconda/anaconda.log
1012889 Jan 02 2024 16:36:28 anaconda/syslog 564 Jan 02 2024 17:07:06 boot.log 1416192 Jul 06 2024 13:57:25 btmp 292292 Jul 17 2024
20:09:07 lastlog 0 Jan 02 2024 16:31:58 maillog 4623022 Jul 17 2024 20:11:43 messages 548756 Jul 01 2024 23:50:00 sa/sa01 4173362 Jul 17
2024 20:11:11 secure 0 Jan 02 2024 16:31:58 spooler 16896 Jul 17 2024 19:38:55 wtmp SSPT33A/admin#
```

Esempio: informazioni sul servizio dell'applicazione ISE - show logging system ade/ADE.log tail



Nota: per interrompere la registrazione, premere una volta **Ctrl + C**.

2- Cartella di registrazione

La cartella Registrazione visualizza i syslog dell'applicazione, consentendo di visualizzare gli errori in tempo reale. Questa funzionalità di registrazione consente di identificare i problemi relativi a funzionalità specifiche, ad esempio problemi di comunicazione, postura, servizi guest, profilatura e così via.

Prima di iniziare

Nella maggior parte dei casi, durante la replica di un problema, è innanzitutto necessario impostare i componenti appropriati a livello di debug o di traccia. Selezionare Operazione > Risoluzione dei problemi > Debug guidato > Configurazione log di debug, selezionare il nodo, fare clic sul livello di log in Nome componente, selezionare il livello di log richiesto, quindi fare clic su **Salva**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface, specifically the 'Debug Wizard' section under 'Operations / Troubleshoot'. The 'Debug Level Configuration' table is displayed, showing various components and their log levels. The 'Active Directory' component is selected, and its log level is set to 'DEBUG'. A 'Save' button is visible in the 'Log Filter' column for the 'Active Directory' row.

Component Name	Log Level	Description	Log file Name	Log Filter
accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled
Active Directory	DEBUG	Active Directory client internal messages	ad_agent.log	Save Cancel
admin-ca	FATAL	CA Service admin messages	ise-psc.log	Disabled
admin-infra	ERROR	Infrastructure action messages	ise-psc.log	Disabled
admin-license	WARN	License admin messages	ise-psc.log	Disabled
ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled
anc	DEBUG	Adaptive Network Control (ANC) debug...	ise-psc.log	Disabled
api-gateway	TRACE	API Gateway native objects logs	api-gateway.log	Disabled
apiservice	INFO	ISE API Service logs	api-service.log	Disabled

Impostazione componente



Nota: è importante tenere presente che, dopo aver ricreato il problema, è necessario ripristinare i livelli predefiniti dei componenti.



Avviso: l'abilitazione del log di debug per **runtime-aaa**, **runtime-logging** e **runtime-config** influisce significativamente sulle prestazioni del sistema. Per evitare un calo delle prestazioni, il debug di questi registri non deve essere impostato su **oltre 15 minuti**.

Configurazione profilo di debug

Debug guidato contiene modelli di debug predefiniti con l'aiuto di cui è possibile risolvere i problemi sui nodi ISE. È possibile configurare il livello di gravità del log di debug per i singoli componenti all'interno del modello. Sono disponibili modelli di debug predefiniti che semplificano il processo di impostazione della registrazione dettagliata per vari componenti.

Questi modelli sono progettati per risolvere gli scenari di risoluzione dei problemi più comuni, consentendo agli amministratori di configurare e

attivare rapidamente le impostazioni di debug necessarie.

Per utilizzare o configurare un modello, andare a **Operazione > Risoluzione dei problemi > Debug guidato > Configurazione profilo di debug:**

The screenshot displays the 'Debug Profile Configuration' interface in the Cisco Identity Services Engine. The top navigation bar includes 'Operations / Troubleshoot'. The left sidebar has 'Operations' selected. The main content area shows a table of debug profiles:

Name	Description	Status	Node Applied
802.1X/MAB	802.1X/MAB	DISABLED	
Active Directory	Active Directory	DISABLED	
Application Server Issues	Application Server Issues	DISABLED	
BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED	
Context Visibility	Context Visibility	DISABLED	
Guest portal	Guest portal	DISABLED	
Licensing	Licensing	DISABLED	
MnT	MnT	DISABLED	
Posture	Posture	DISABLED	
Profiling	Profiling	DISABLED	
Replication	Replication	DISABLED	
TACACS	TACACS	DISABLED	
TrustSec	TrustSec	DISABLED	

Configurazione profilo di debug

Sono già presenti alcuni modelli predefiniti oppure fai clic su **Aggiungi** per crearne uno personalizzato.

Identity Services Engine Operations / Troubleshoot

Bookmarks | Diagnostic Tools | Download Logs | **Debug Wizard**

Dashboard | Context Visibility | **Operations** | Policy | Administration | Work Centers | Interactive Help

Debug Profile Configuration
Debug Log Configuration

Debug Profile Configuration > New

Add New Profile

Name: AD Troubleshooting

Description

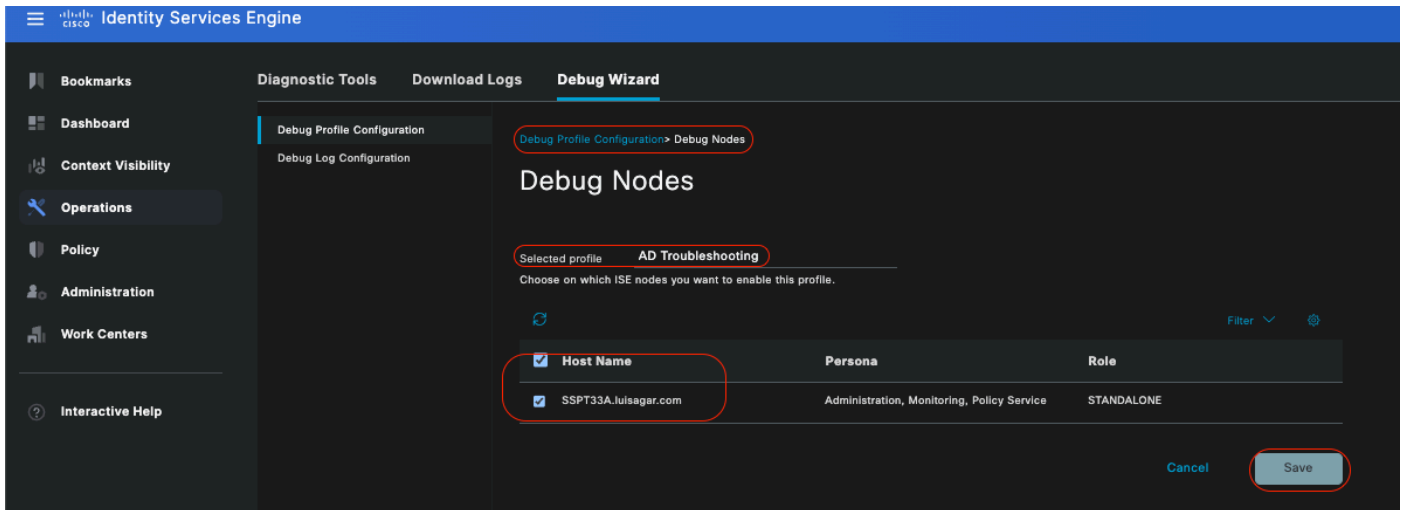
You can choose the desired log severity level from the "Log Level" drop-down list for each component of this profile.

Component Name	Log Level	Description	Log file Name
accessfilter	INFO	RBAC resource access filter	ise-pac.log
Active Directory	TRACE	Active Directory client internal messages	ad_agent.log
admin-ca	INFO	CA Service admin messages	ise-pac.log
admin-infra	INFO	Infrastructure action messages	ise-pac.log
admin-license	INFO	License admin messages	ise-pac.log
ai-analytics	INFO	AI Analytics	ai-analytics.log
anc	INFO	Adaptive Network Control (ANC) debug me...	ise-pac.log
api-gateway	INFO	API Gateway native objects logs	api-gateway.log
apiservice	INFO	ISE API Service logs	api-service.log
bootstrap-wizard	INFO	Bootstrap wizard messages	ise-pac.log
ca-service	INFO	CA Service messages	caservice.log
ca-service-cert	INFO	CA Service Cert messages	ise-pac.log
CacheTracker	WARN	PSC cache related debug messages	tracking.log
cellular-config	INFO	Cellular-config related log messages	ise-pac.log
cellular-config-api	INFO	Cellular-config API related log messages	api-service.log
cellular-config-ui	INFO	Cellular-config UI related log messages	ise-pac.log
cellular-mnt	INFO	Debug collector on M&T nodes for Cellular ...	collector.log
certprovisioningportal	INFO	Certificate Provisioning Portal debug messa...	guest.log
cisco-mnt	INFO	Debug M&T database access logging	ise-pac.log
client-webapp	INFO	Client Provisioning admin server debug mes...	guest.log
collector	WARN	Debug collector on M&T nodes	collector.log
cpm-clustering	INFO	Node group runtime messages	ise-pac.log
cpm-mnt	INFO	Debug M&T UI logging	ise-pac.log
EDF	INFO	Entity Definition Framework logging	edf.log

Aggiunta di un nuovo modello

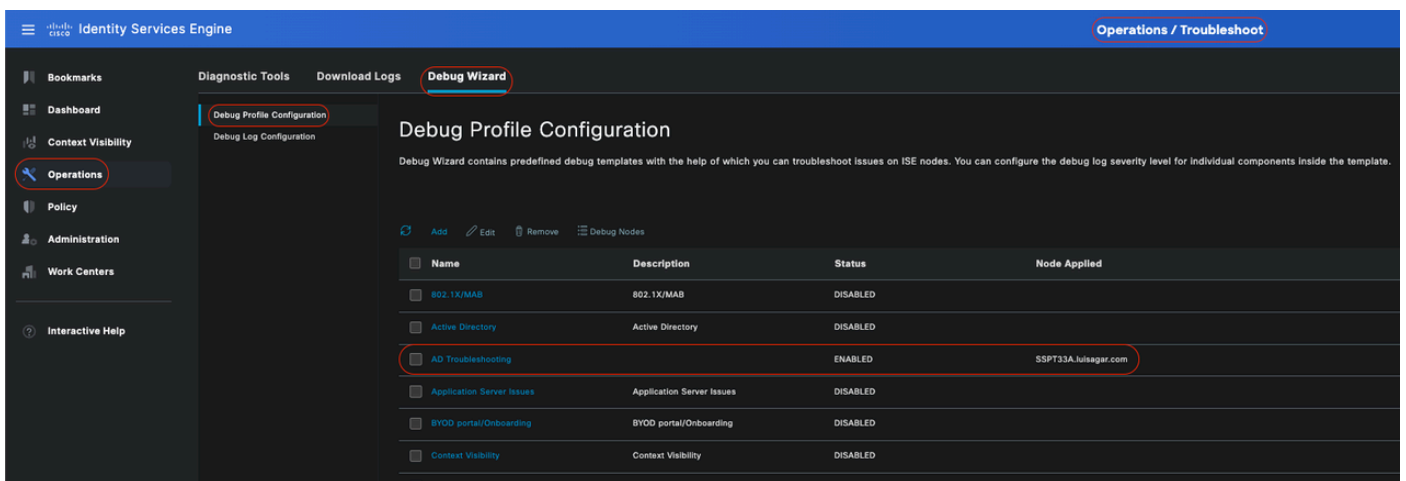
Attivare un modello

L'attivazione di un modello rende effettivo il livello di componente modificato. Selezionare **Template** (Modello), quindi fare clic su **Debug Nodes** (Nodi di debug). Selezionare il nodo a cui si desidera applicare il modello, quindi fare clic su **Salva**:



Nodi di debug

A questo punto, al modello deve essere assegnato il nodo:

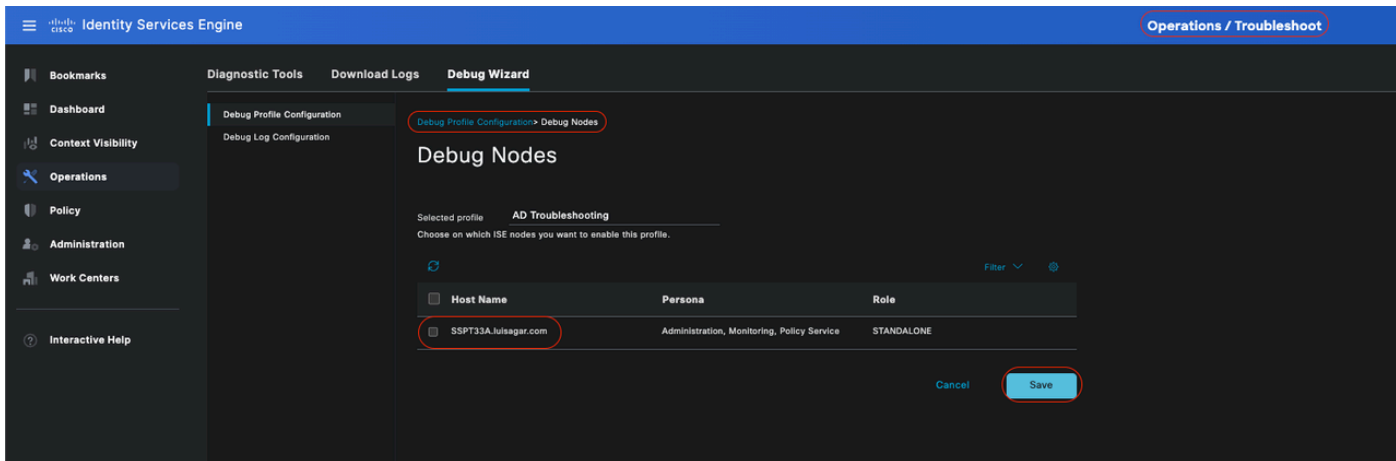


Verifica



Nota: nessuno dei livelli di componente diventa effettivo finché non si utilizza il modello su un nodo specifico.

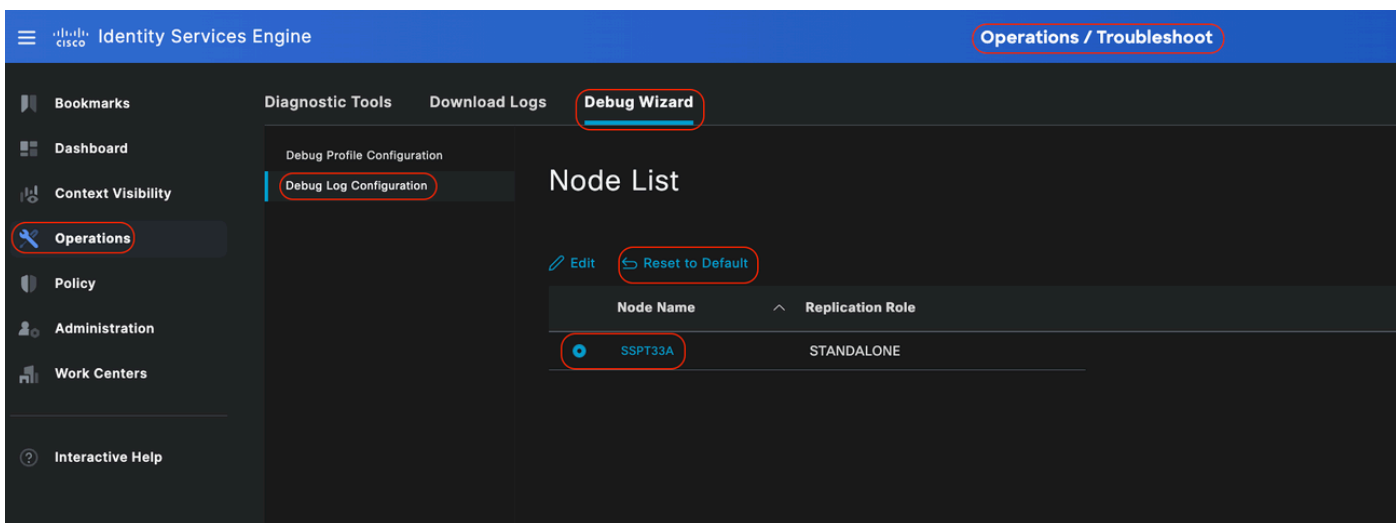
Disabilitare il modello Debug Profile, selezionare il modello. Fare clic su **Debug nodi**. Deselezionare il nodo a cui è applicato il modello e fare clic su **Salva**:



Disattivazione modello

Ripristinare i livelli predefiniti dei componenti

Passare a **Operazione > Risoluzione dei problemi > Debug guidato > Configurazione log di debug**. Selezionare il nodo. Fare clic su **Reset toDefault**, quindi su **Yes**.



Ripristina valori predefiniti



Avvertenza: se si utilizza l'opzione **Ripristina predefiniti** mentre un modello di **profilo di debug** è abilitato, il modello di profilo di **debug rimane** abilitato, ma i componenti tornano alle impostazioni predefinite, causando una mancata corrispondenza. È importante non utilizzare l'opzione **Ripristina valori predefiniti** se sono abilitati i **modelli di profilo di debug**.

Per informazioni più dettagliate ed esempi specifici, consultare la documentazione ufficiale di Cisco perché questo documento fornisce una matrice completa dei componenti e dei log di debug: [Risoluzione dei problemi e abilitazione dei debug su ISE](#)

Come accedere alla cartella di registrazione:

È possibile accedere a questa cartella dalla CLI utilizzando questi comandi:

- show logging application <logfile>

Alcune cartelle di sistema disponibili

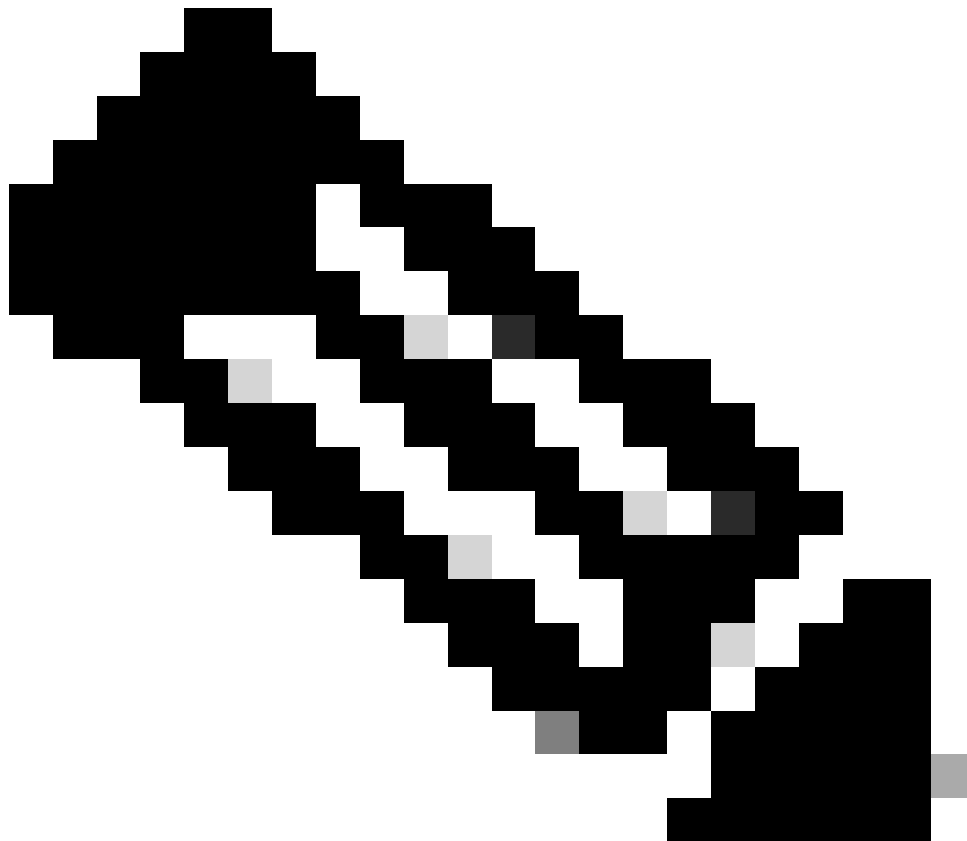
SSPT33A/admin#**show logging application** 11947 Jul 18 2024 12:20:28 ad_agent.log 96501 Jul 18 2024 13:29:33 collector.log 116751 Jul 18 2024 13:30:00 guest.log 196958 Jul 18 2024 13:01:20 ise-elasticsearch.log 5136021 Jul 18 2024 13:31:24 ise-psc.log 172755 Jul 18 2024 13:29:04 profiler.log 10596813 Jul 18 2024 13:31:10 prrt-server.log 28496 Jul 18 2024 12:37:04 redis.log 3489 Jul 18 2024 12:36:44 replication.log

Esempio: Informazioni sul servizio clienti ISE - show logging application profiler.log tail

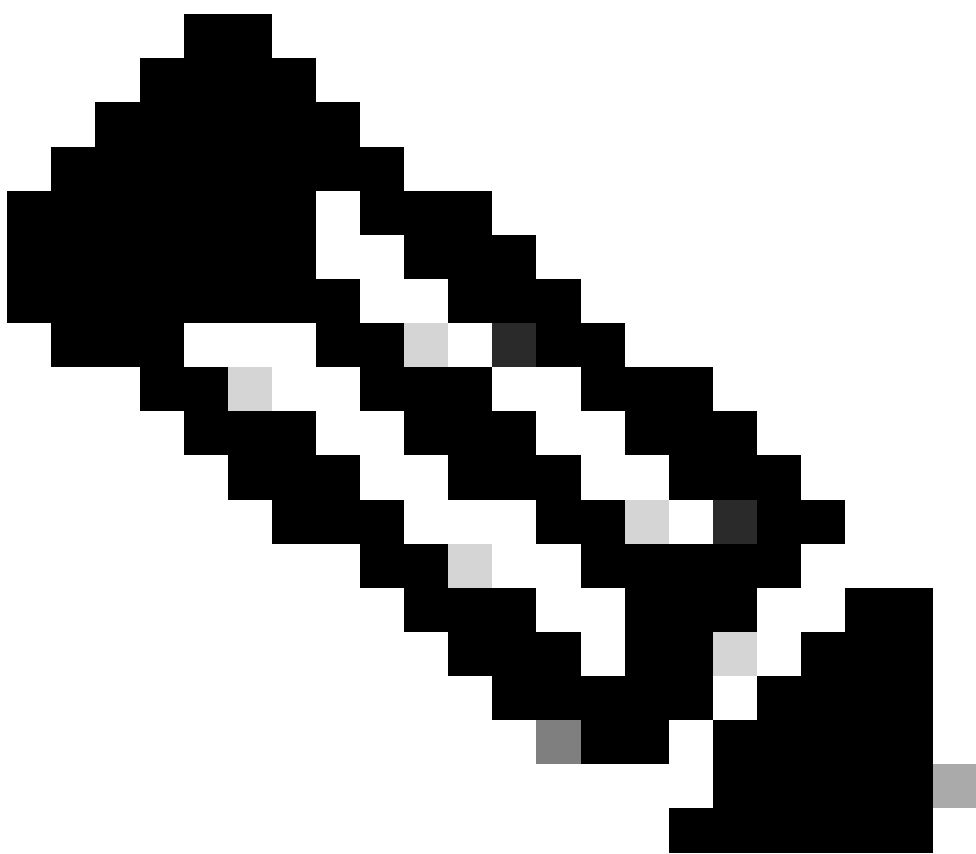
Esempio: Informazioni sul servizio clienti ISE - **show logging application guest.log tail**

Oltre a cercare un messaggio specifico, utilizzare una parola chiave per cercarlo. Esempio: Informazioni su ISE - show logging application localStore/iseLocalStore.log | include 70000\ NOTICE\

05:00 0000423187 70000 NOTICE System-Stats: ISE Utilization, ConfigVersionId=14667, SysStatsUtilizationCpu=5.41%, SysStatsUtilizationNetwork=eth0: rcvd = 2052\; sent = 4062 \;rcvd_dropped = 0\; sent_dropped = 0, SysStatsUtilizationNetwork=cni-podman1: rcvd = 1577511\; sent = 115782 \;rcvd_dropped = 0\; sent_dropped = 0, SysStatsUtilizationNetwork=veth2f590a1a: rcvd = **2024-07-18 00:08:46.369 -05:00 0000423194 70000 NOTICE System-Stats: ISE Utilization, ConfigVersionId=14667, SysStatsUtilizationCpu=1.36%, SysStatsUtilizationNetwork=eth0: rcvd = 1959\; sent = 3012 \;rcvd_dropped = 0\; sent_dropped = 0, SysStatsUtilizationNetwork=cni-podman1: rcvd = 1576019\; sent = 114411 \;rcvd_dropped = 0\; sent_dropped = 0, SysStatsUtilizationNetwork=veth2f590a1a: rcvd = SysStatsUtilizationDiskSpace=8% /opt, SysStatsUtilizationDiskSpace=1% /mnt/encpart, SysStatsUtilizationDiskSpace=8% /opt/podman/containers/storage/overlay, AverageRadiusRequestLatency=0, AverageTacacsRequestLatency=0, DeltaRadiusRequestCount=0, DeltaTacacsRequestCount=0, SysStatsUtilizationLoadAvg=0.40, SysStatsCpuCount=16, SysStatsProcessMemoryMB=18082, ActiveSessionCount=0,**



Nota: questo comando **mostra l'applicazione di registrazione localStore/iseLocalStore.log | include 70000\ NOTICE** non funziona a seconda del livello di patch o della versione ISE (precedente). In alternativa, è possibile eseguire questo comando **show logging application localStore/iseLocalStore.log | includere "AVVISO 70000"**



Nota: per interrompere la registrazione, premi semplicemente **Ctrl + C** una volta.

Suddivisione del comando

```
SSPT33A/admin#show logging application guest.log | include portalwebaction
```

Spiegazione:

- **show**: questo comando viene utilizzato per visualizzare informazioni.
- **logging**: fa riferimento ai log o ai file di log.
- **application**: specifica l'applicazione o il processo di cui si desidera visualizzare i registri.
- **guest.log**: specifica il file di log denominato guest.log.
- **include**: questa parte del comando filtra l'output in modo da includere solo le righe che corrispondono a un pattern o a una parola chiave specifici.
- **portalwebaction**: la parola chiave o il pattern da cercare nell'output del comando precedente (show logging application guest.log).

Trova il file necessario

Se non si è certi del nome specifico del registro, è possibile filtrare per visualizzare ulteriori opzioni. Questo è un esempio. Fare clic su **Invio** per visualizzare l'output:

ise3-3a/admin#**show logging application | include pxgrid** 14059847 Jul 18 2024 20:46:09 pxgrid/pxgrid-server.log 5367398 Jul 12
2024 23:59:39 pxgrid/pxgrid-server.log.2024-07-12-1 16261440 Jul 13 2024 23:59:44 pxgrid/pxgrid-server.log.2024-07-13-1 16261440 Jul 14
2024 23:59:49 pxgrid/pxgrid-server.log.2024-07-14-1 16261794 Jul 15 2024 23:59:53 pxgrid/pxgrid-server.log.2024-07-15-1 16261625 Jul 16
2024 23:59:58 pxgrid/pxgrid-server.log.2024-07-16-1 16261479 Jul 17 2024 23:59:45 pxgrid/pxgrid-server.log.2024-07-17-1 0 Jul 12 2024
15:42:36 pxgrid/pxgrid_dbsync_summary.log 0 Jul 12 2024 15:42:36 pxgrid/pxgrid_internal_dbsync_summary.log 16744 Jul 15 2024 20:45:49
pxgriddirect-connector.log 2841 Jul 15 2024 20:45:44 pxgriddirect-service.log 6277 Jul 12 2024 16:33:53 pxgriddirect-service.log.2024-07-12-1
ise3-3a/admin#

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).