

Use o sistema de depuração para solucionar problemas do ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Instrução do problema](#)

[1- Pasta do sistema](#)

[Como acessar a pasta do sistema:](#)

[Exemplo de pastas do sistema disponíveis:](#)

[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 mensagens 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#](#)

[Pasta 2-Logging](#)

[Antes de começar](#)

[Depurar Configuração do Perfil](#)

[Definir os níveis dos componentes de volta ao padrão](#)

[Como acessar a pasta de registro:](#)

[Algumas pastas do sistema disponíveis](#)

[Comando Quebrando](#)

[Explicação:](#)

[Localizar arquivo necessário](#)

Introdução

Este documento descreve como solucionar problemas e detectar erros enquanto eles ocorrem, executando `show logging` comandos através da CLI.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity Services Engine (ISE).

- Interface de linha de comando (CLI).

Componentes Utilizados

As informações neste documento são baseadas na versão 3.3 do Identity Services Engine (ISE).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O ISE utiliza uma estrutura específica para armazenar arquivos de log, que são detalhados neste artigo. Para conseguir isso, use a CLI para executar a detecção de erros em tempo real, executando `show logging` comandos.

Instrução do problema

O Cisco Identity Services Engine (ISE) mantém pastas para armazenar mensagens de log locais. Dependendo da natureza do problema, você pode utilizar dois comandos principais `show logging` para diagnosticar e solucionar problemas:

1- Pasta do sistema

A Pasta Sistema exibe syslogs do sistema, permitindo que você visualize erros ao vivo. Esse recurso de registro ajuda a identificar problemas relacionados ao sistema, como problemas com os serviços do ISE.

Como acessar a pasta do sistema:

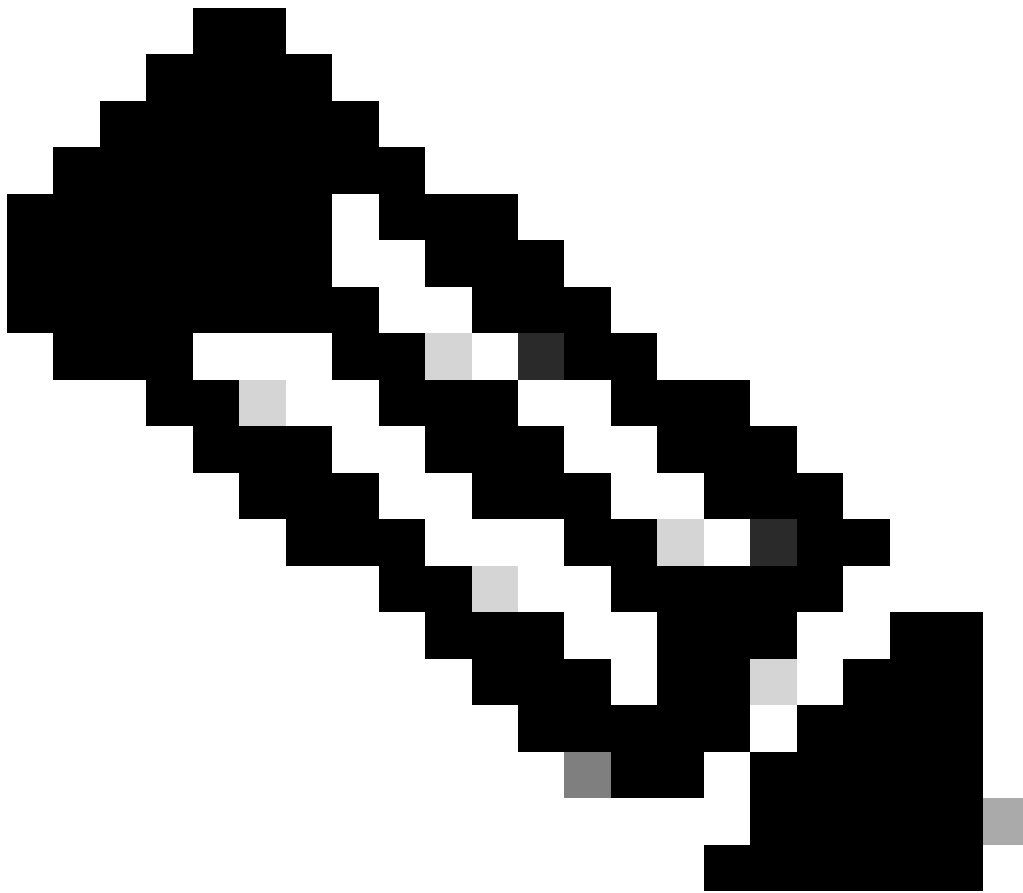
Você pode acessar esta pasta a partir do CLI usando estes comandos:

- `show logging system <LogFile>`

Exemplo de pastas do sistema disponíveis:

```
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#
```

Exemplo: informações sobre o serviço de aplicativos do ISE - `show logging system ade/ADE.log tail`



Nota: Para interromper a execução do registro, basta pressionar **Ctrl + C** uma vez.

2- Pasta de registro

A Pasta de registro exibe syslogs de aplicativos, permitindo que você visualize erros ao vivo. Esse recurso de registro ajuda a identificar problemas relacionados a recursos específicos, como problemas de comunicação, postura, serviços de convidado, criação de perfil, etc.

Antes de começar

Na maioria das vezes em que você estiver replicando um problema, será necessário definir os componentes apropriados no nível de depuração ou de rastreamento. Navegue para **Operation > Troubleshoot > Debug Wizard > Debug Log Configuration**, selecione o nó, clique no nível de



Aviso: a habilitação do log de depuração para **runtime-aaa**, **runtime-logging** e **runtime-config** afeta significativamente o desempenho do sistema. Esses logs não devem ser definidos para depuração por **mais de 15 minutos** para evitar degradação de desempenho.

Depurar Configuração do Perfil

O Assistente de depuração contém modelos de depuração predefinidos com a ajuda dos quais você pode solucionar problemas em nós do ISE. Você pode configurar o nível de severidade do log de depuração para componentes individuais dentro do modelo. Ele fornece modelos de depuração predefinidos que simplificam o processo de configuração de registro detalhado para vários componentes.

Esses modelos são projetados para lidar com cenários comuns de solução de problemas, facilitando para os administradores configurar e ativar rapidamente as configurações de depuração necessárias.

Para usar ou configurar um modelo, vá para **Operation > Troubleshoot > Debug Wizard > Debug Profile Configuration:**

The screenshot displays the 'Debug Profile Configuration' interface in the Cisco Identity Services Engine. The top navigation bar shows 'Operations / Troubleshoot'. The left sidebar has 'Operations' selected. The main content area is titled 'Debug Profile Configuration' and includes a sub-header 'Debug Log Configuration'. Below this, there is a table of debug nodes, all of which are currently disabled. The table has columns for Name, Description, Status, and Node Applied. A red box highlights the table area.

Name	Description	Status	Node Applied
<input type="checkbox"/> 802.1X/MAB	802.1X/MAB	DISABLED	
<input type="checkbox"/> Active Directory	Active Directory	DISABLED	
<input type="checkbox"/> Application Server Issues	Application Server Issues	DISABLED	
<input type="checkbox"/> BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED	
<input type="checkbox"/> Context Visibility	Context Visibility	DISABLED	
<input type="checkbox"/> Guest portal	Guest portal	DISABLED	
<input type="checkbox"/> Licensing	Licensing	DISABLED	
<input type="checkbox"/> MinT	MinT	DISABLED	
<input type="checkbox"/> Posture	Posture	DISABLED	
<input type="checkbox"/> Profiling	Profiling	DISABLED	
<input type="checkbox"/> Replication	Replication	DISABLED	
<input type="checkbox"/> TACACS	TACACS	DISABLED	
<input type="checkbox"/> TrustSec	TrustSec	DISABLED	

Depurar Configuração do Perfil

Já existem alguns modelos predefinidos, ou clique em **Adicionar** para criar o seu próprio.

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

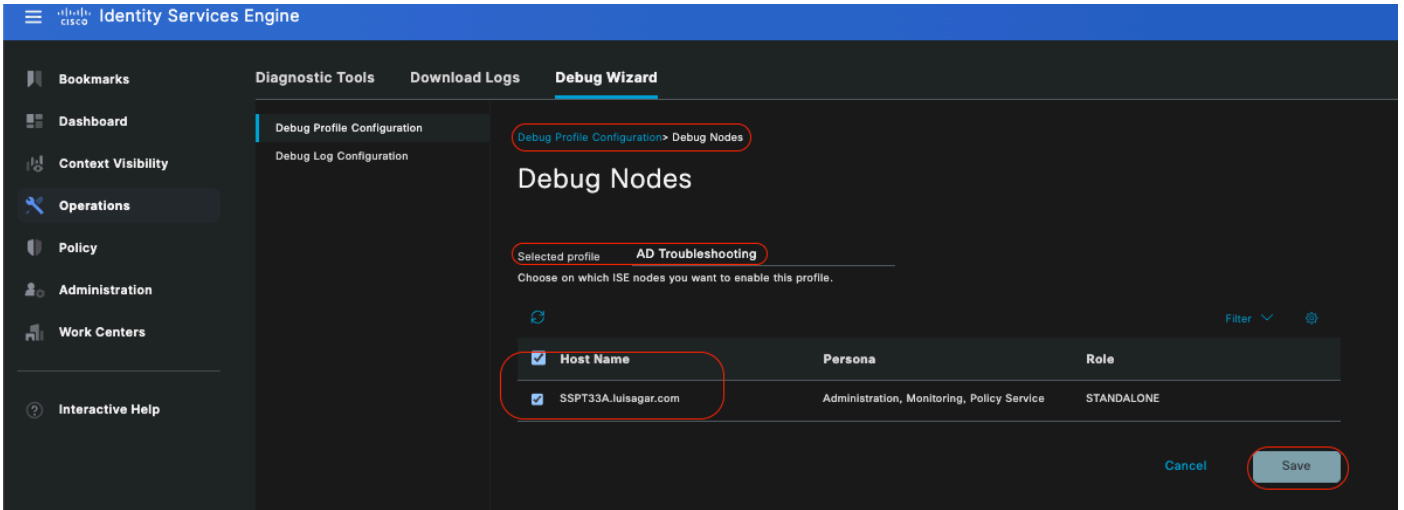
You can choose the desired log severity level from the "Log Level" drop-down list for each component of this profile.

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

Adicionando novo modelo

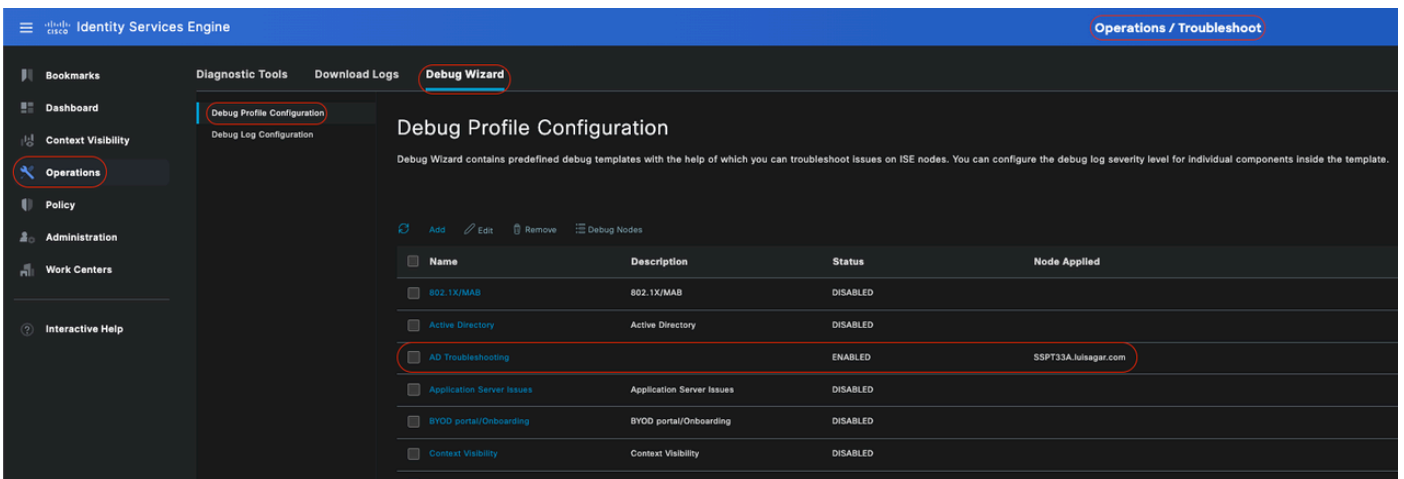
Ativar um modelo

Ao ativar um modelo, o nível do componente que você modificou entra em vigor. Selecione **Template** e clique em **Debug Nodes**. Selecione o nó ao qual deseja aplicar o modelo e clique em **Salvar**:

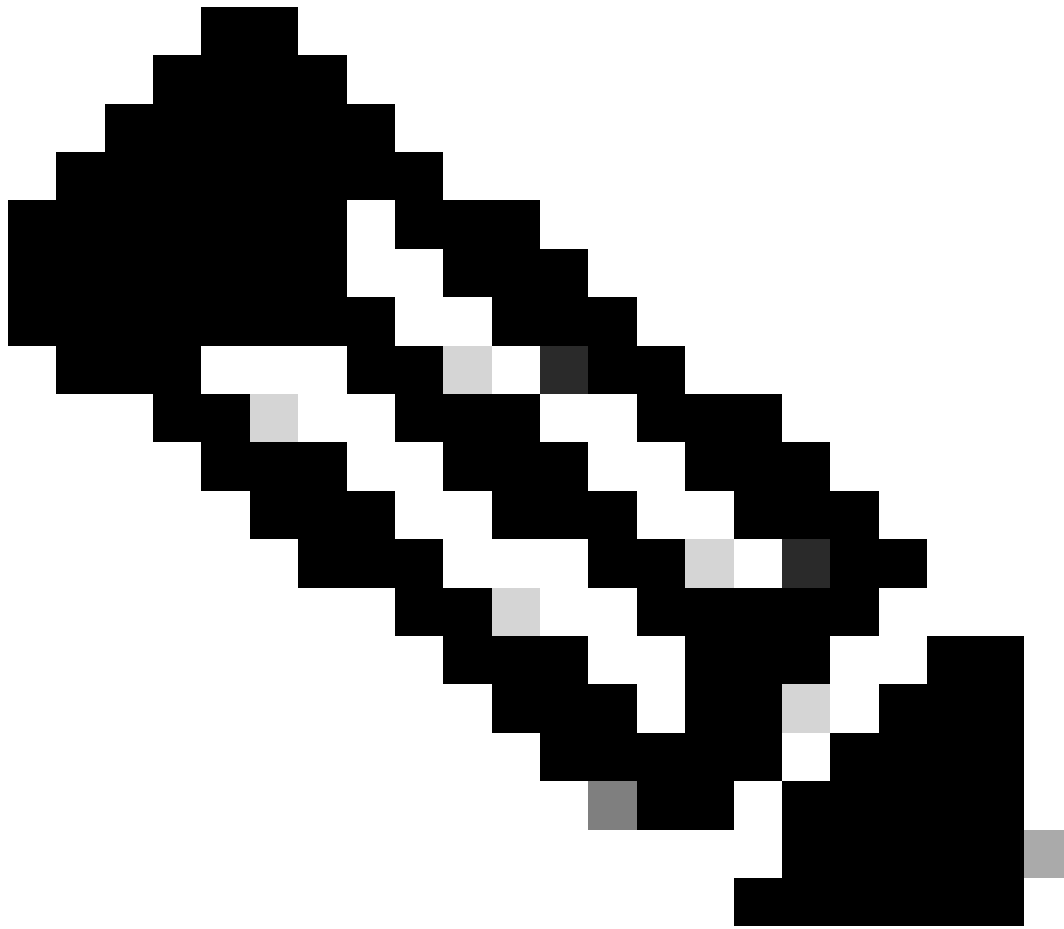


Nós de depuração

Agora, o modelo deve ter o nó atribuído a ele:

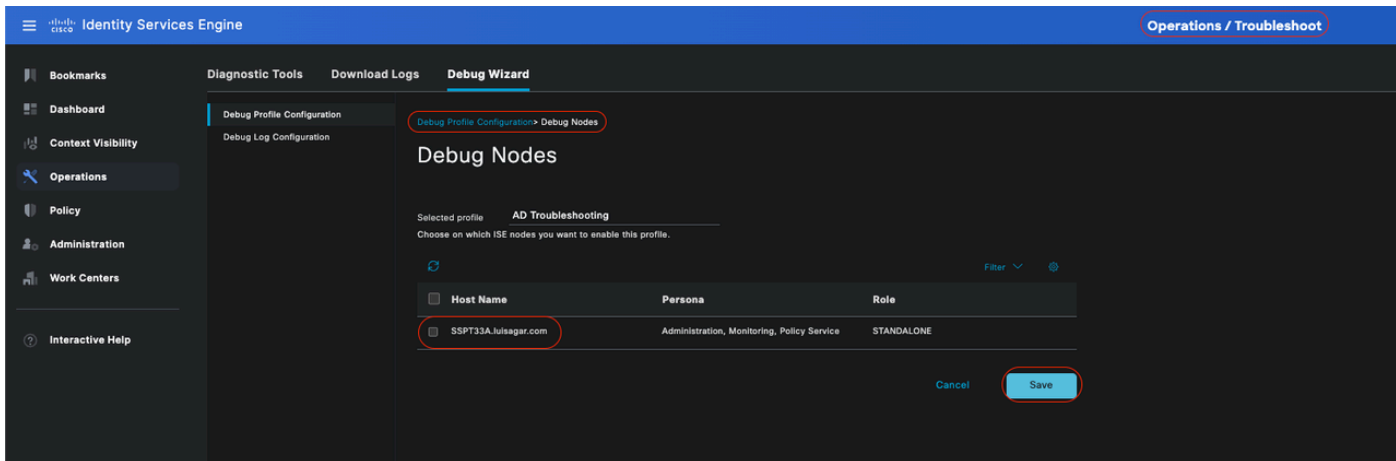


Verificando



Observação: Nenhum dos níveis de componente entrará em vigor até que você use o modelo em um nó específico.

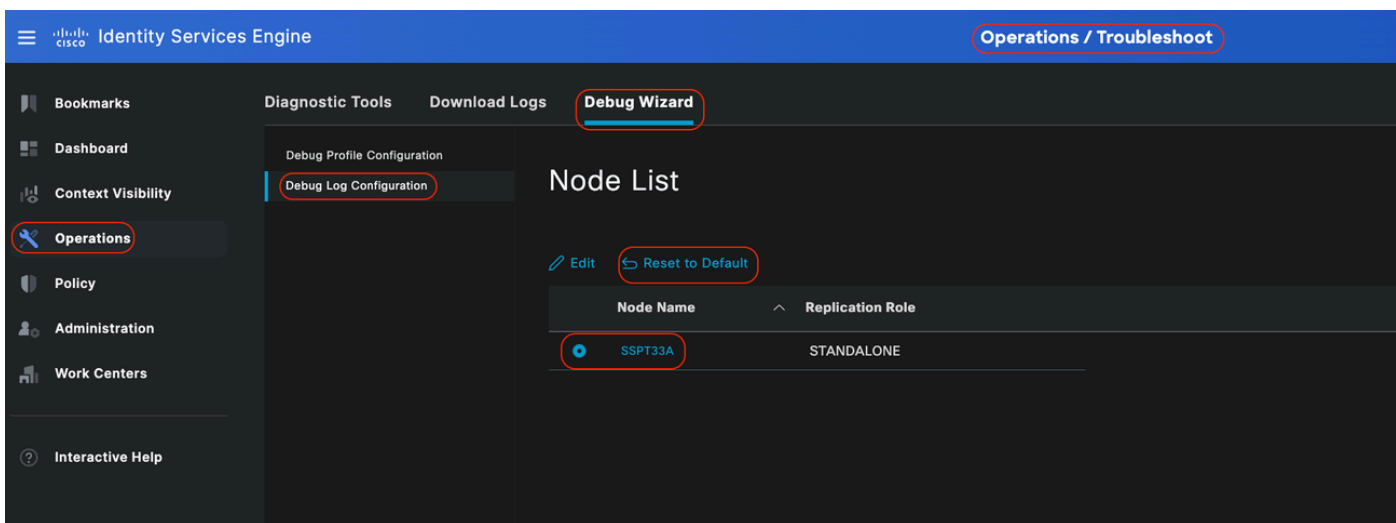
Desativar modelo de perfil de depuração, selecione o modelo. Clique em **Debug Nodes**. Desmarque o nó ao qual o modelo é aplicado e clique em **Salvar**:



Desativando modelo

Definir os níveis dos componentes de volta ao padrão

Navegue até **Operation > Troubleshoot > Debug Wizard > Debug Log Configuration** . Selecione o nó. Clique em **Reset toDefault** (Redefinir paraPadrão) e em **Yes**.



Redefinir para o padrão



Aviso: se você usar a opção **Redefinir para o padrão** enquanto um modelo do **Perfil de depuração** estiver ativado, o **Depurar Profiletemplate** permanecerá **ativado**, mas os componentes retornarão às suas configurações padrão, causando uma **incompatibilidade**. É importante não usar a opção **Reset to Default** se houver **Debug Profile templates** ativados.

Para obter informações mais detalhadas e exemplos específicos, consulte a documentação oficial da Cisco, pois este documento fornece uma matriz abrangente de componentes e registros de depuração: [Solucionar problemas e Ativar depurações no ISE](#)

Como acessar a pasta de registro:

Você pode acessar esta pasta a partir do CLI usando estes comandos:

- show logging application <logfile>

Algumas pastas do sistema disponíveis

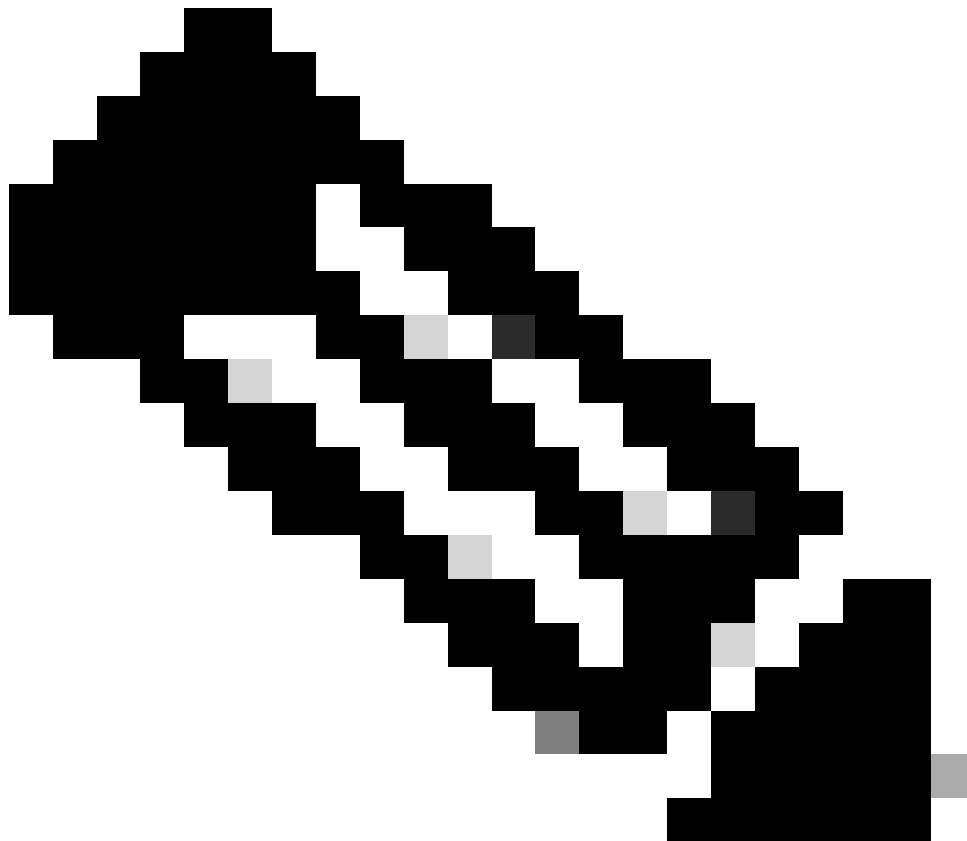
SSPT33A/admin#**show logging application** 11947 Jul 18 2024 12:20:28 ad_agent.log 96501 Jul 18 2024 13:29:33 collector.log 116751 Jul 18 2024 13:30:00 guest.log 196958 Jul 18 2024 13:01:20 ise-elasticsearch.log 5136021 Jul 18 2024 13:31:24 ise-psc.log 172755 Jul 18 2024 13:29:04 profiler.log 10596813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

Exemplo: informações sobre o serviço de convidado do ISE - show logging application profiler.log tail

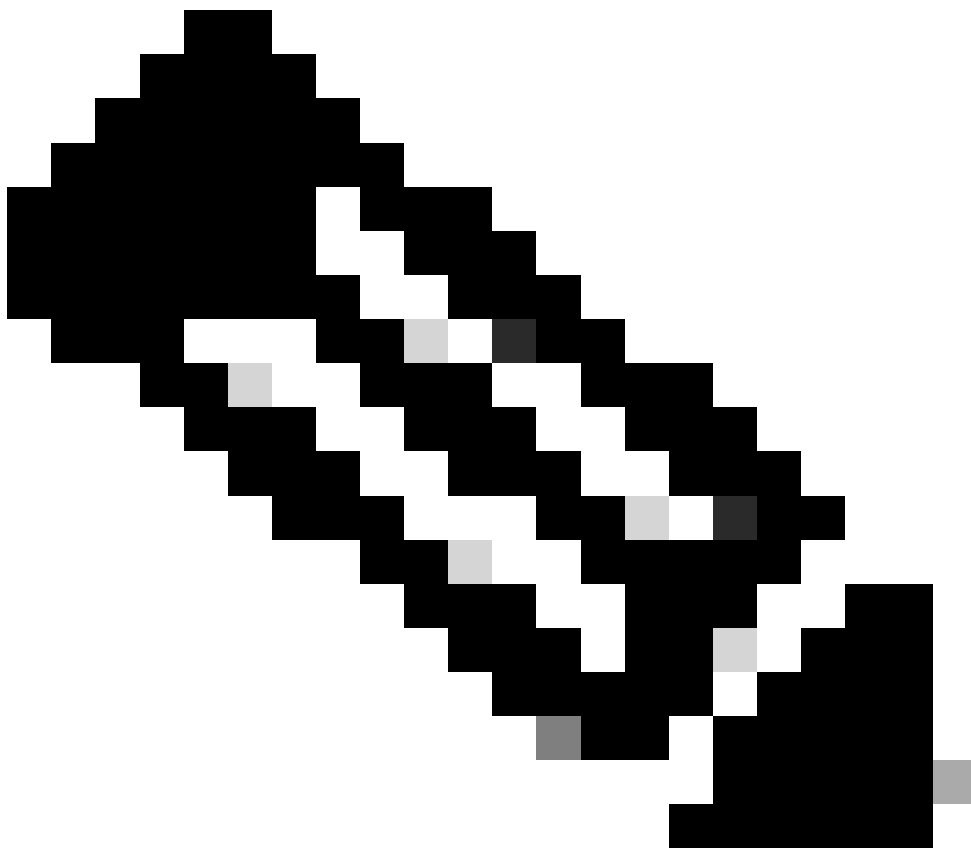
Exemplo: informações sobre o serviço de convidado do ISE - **show logging application guest.log tail**

Além de procurar uma mensagem específica, use uma palavra-chave para procurá-la. Exemplo: Informações sobre o 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,**



Observação: este comando `show logging application localStore/iseLocalStore.log | incluir 70000\ AVISO\` não funciona dependendo do nível de patch ou da versão do ISE (anterior). Você também pode executar este comando `show logging application localStore/iseLocalStore.log | incluir "AVISO 70000"`



Observação: para interromper o registro, basta pressionar **Ctrl + C** uma vez.

Comando Quebrando

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

Explicação:

- **show**: este comando é usado para exibir informações.
- **logging**: Refere-se a logs ou arquivos de log.
- **application**: especifica o aplicativo ou processo cujos logs você deseja exibir.
- **guest.log**: Especifica o arquivo de log chamado guest.log.
- **include**: Esta parte do comando filtra a saída para incluir apenas linhas que correspondam a um padrão ou palavra-chave específico.
- **portalwebaction**: A palavra-chave ou padrão a ser procurado na saída do comando anterior (show logging application guest.log).

Localizar arquivo necessário

Se não tiver certeza do nome de log específico, você poderá filtrar para ver mais opções. Este é um exemplo, clique em **enter** para ver a saída:

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#

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.