



Gerenciar logs e rastreamento

NetApp SMI-S Provider

NetApp

January 02, 2026

Índice

- Gerenciar logs e rastreamento 1
 - Visão geral 1
 - Configure as definições de registo 1
 - Níveis de registo 2
 - Gerenciar rastreamento 2
 - Especificar definições de traçado 2
 - Especifique o tamanho do arquivo de rastreamento 4
 - Especifique o número de arquivos de rastreamento salvos 4
 - Ativar ou desativar o log de auditoria para comandos SMI-S. 5

Gerenciar logs e rastreamento

Visão geral

Você pode configurar como o SMI-S Provider gerencia arquivos de log e rastreamento, como especificar os níveis de mensagens a serem registradas e o diretório para o qual os logs são salvos. Você também especifica os componentes a serem rastreados, o destino para o qual as mensagens de rastreamento são escritas, o nível de rastreamento e a localização do arquivo de rastreamento.

Configure as definições de registro

Por padrão, todas as mensagens do sistema são registradas. Além disso, por padrão, os logs de mensagens do sistema estão localizados no `logs` diretório no qual o provedor NetApp SMI-S está instalado. Pode alterar a localização e o nível das mensagens do sistema gravadas no registro do servidor CIM. Por exemplo, você pode optar por ter logs armazenados em um diretório que você especificar e ter apenas mensagens fatais do sistema gravadas no log do servidor CIM.

Antes de começar

- Você já deve ter credenciais de login como Administrador.
- Você já deve ter feito login no sistema host como Administrador.

Passos

1. Acesse o provedor NetApp SMI-S.
2. Execute uma das seguintes ações:

Ação	Comando	Informações adicionais
Altere o nível de registro de mensagens do sistema	cimconfig -s logLevel=new_log_level -p	Se você quiser alterar o nível de log para "INFORMAÇÕES", por exemplo, você digitaria este comando cimconfig -s logLevel=INFORMATION -p
Altere o diretório de log de mensagens do sistema	cimconfig -s logdir=new_log_directory -p Se o <i>new_log_directory</i> contiver espaço, você deve inseri-lo entre aspas (" <i>new log directory</i> ").	Se você quiser alterar o diretório de log para "sherverlogs", por exemplo, você digitaria este comando: cimconfig -s logdir=serverlogs -p

3. Reinicie o servidor CIM:

```
smis cimserver restart
```

Níveis de registo

Você pode especificar os tipos de mensagens registradas (por exemplo, deseja que apenas as mensagens fatais do sistema sejam registradas).

Pode configurar o nível de registo para uma das seguintes opções:

- **TRACE**

Salva mensagens de rastreamento no log cimserver_standard.

- **INFORMAÇÕES**

Regista todas as mensagens do sistema (informativas, de aviso, graves e fatais).

- **AVISO**

Regista mensagens de aviso, graves e fatais do sistema.

- **GRAVE**

Regista mensagens graves e fatais do sistema

- **FATAL**

Regista apenas mensagens fatais do sistema.

Gerenciar rastreamento

Você pode configurar como o SMI-S Provider gerencia arquivos de rastreamento, como especificar os componentes a serem rastreados, o destino para o qual as mensagens de rastreamento são escritas, o nível de rastreamento e a localização do arquivo de rastreamento.

Especificar definições de traçado

Ter o rastreamento ativado é importante para coletar informações para solução de problemas. No entanto, ter o rastreamento ativado pode afetar o desempenho, portanto, considere cuidadosamente o que deve ser rastreado e por quanto tempo você precisa ativar o rastreamento.

Antes de começar

- Você já deve ter credenciais de login como Administrador.
- Você já deve ter feito login no sistema host como Administrador.

Passos

1. Acesse o provedor NetApp SMI-S.
2. Especifique várias definições de rastreio, conforme aplicável:

Ação	Comando
Especifique os componentes a serem rastreados	<code>cimconfig -s traceComponents=<i>components</i> -p</code>
Especifique a facilidade de rastreo	<code>cimconfig -s traceFacility=<i>facility</i> -p</code>
Especifique a localização do arquivo de rastreamento	<code>cimconfig -s traceFilePath=<i>path_name</i> -p</code>
Especifique o nível do traçado	<code>cimconfig -s traceLevel=<i>level</i> -p</code>

3. Reinicie o servidor CIM:

```
smis cimserver restart
```

Valores de definição do traçado

Você pode especificar os componentes a serem rastreados, o alvo de rastreamento e o nível de rastreamento. Opcionalmente, você pode alterar o nome e a localização do arquivo de rastreamento se não quiser usar o nome e a localização do arquivo de rastreamento padrão.

Pode configurar as seguintes definições de rastreo:

- **TraceComponents**

Especifica os componentes a serem rastreados. Por padrão, todos os componentes são rastreados.

- **TraceFacility**

Especifica o destino para o qual as mensagens de rastreamento são escritas:

- Ficheiro

Este é o valor padrão, que especifica que as mensagens de rastreamento são gravadas no arquivo especificado pela opção de configuração `traceFilePath`.

- Registo

Especifica que as mensagens de rastreamento são gravadas no arquivo de log `cimserver_standard`.

- **TraceFilePath**

Especifica a localização do arquivo de rastreamento. Por padrão, o arquivo de rastreamento é chamado `cimserver.trc` e está localizado no `traces` diretório.

- **TraceLevel**

Especifica o nível de rastreamento. Por padrão, o rastreamento é desativado.

Nível do traçado	Rastrear mensagens escritas
0	O rastreamento está desativado.
1	Mensagens graves e de registro.
2	Mensagens básicas de rastreamento de fluxo (detalhes de dados baixos)
3	Fluxo lógico inter-função (detalhe de dados médios)
4	Alto detalhe de dados
5	Detalhes de dados elevados e método de entrada e saída

Especifique o tamanho do arquivo de rastreamento

Se o rastreamento estiver ativado, o tamanho máximo do arquivo de rastreamento será de 100 MB por padrão. Você pode aumentar ou diminuir o tamanho máximo do arquivo de rastreamento definindo a variável de `PEGASUS_TRACE_FILE_SIZE` ambiente . O valor do tamanho do arquivo de rastreamento pode ser de 10 MB a 2 GB.

Antes de começar

- Você já deve ter credenciais de login como Administrador.
- Você já deve ter feito login no sistema host como Administrador.

Passos

1. Acesse o provedor NetApp SMI-S.
2. Crie uma variável de ambiente de sistema ou usuário nomeada com `PEGASUS_TRACE_FILE_SIZE` o novo tamanho de arquivo de rastreamento em bytes.

Documentação do Windows tem mais informações sobre a criação de variáveis de ambiente.

3. Reinicie o servidor CIM:

```
smis cimserver restart
```

Especifique o número de arquivos de rastreamento salvos

Se o rastreamento estiver ativado, sete arquivos de rastreamento serão salvos por padrão. Se precisar de mais ficheiros de rastreio guardados, pode aumentar o número máximo de ficheiros de rastreio guardados através da definição da variável de `PEGASUS_TRACE_FILE_NUM` ambiente . Se aumentar o número máximo de arquivos de rastreamento salvos, você deve garantir que o sistema tenha espaço suficiente em seu disco rígido para acomodar os arquivos de rastreamento.

Antes de começar

- Você já deve ter credenciais de login como Administrador.
- Você já deve ter feito login no sistema host como Administrador.

Sobre esta tarefa

Se o rastreamento estiver ativado, as informações de rastreamento serão gravadas no `cimserver.trc` arquivo. Os arquivos de rastreamento são girados. `cimserver.trc` Quando atinge o tamanho máximo do arquivo de rastreamento, seu conteúdo é movido para o ``cimserver.trc.n` arquivo. Por padrão, `n` é um valor de 0 a 5. Se necessitar de mais ficheiros de rastreio guardados, aumenta o valor de `n`.

Passos

1. Acesse o provedor NetApp SMI-S.
2. Crie uma variável de ambiente de sistema ou usuário nomeada com `PEGASUS_TRACE_FILE_NUM` o novo número de arquivos de rastreamento salvos.

Documentação do Windows tem mais informações sobre a criação de variáveis de ambiente.

3. Reinicie o servidor CIM:

```
smis cimserver restart
```

Ativar ou desativar o log de auditoria para comandos SMI-S.

Todos os comandos SMI-S recebidos são registrados em arquivos de log de auditoria, o que permite que os auditores rastreiem as atividades das operações do cliente WBEM e do uso do provedor. Você pode ativar ou desativar o Registro desses comandos de entrada definindo uma propriedade de configuração dinâmica.

Antes de começar

- Você já deve ter credenciais de login como Administrador.
- Você já deve ter feito login no sistema host como Administrador.

Sobre esta tarefa

Os dados do log de auditoria podem fornecer um Registro de acesso, atividade e alteração de configuração para um servidor CIM. O conteúdo do arquivo de auditoria inclui qual comando foi emitido, por quem o comando foi emitido e a que horas o comando foi emitido.

A propriedade de configuração dinâmica `enableAuditLog` ativa ou desativa o log de auditoria no tempo de execução. Por padrão, `enableAuditLog` é definido como `true`.

A prática comum é deixar o registo de auditoria ativado.

O ficheiro de registo de auditoria (`cimserver_auditlog`) é armazenado no diretório de registo pegasus (`C:\Program Files (x86)\Netapp\smis\pegasus\logs`).

O tamanho máximo do ficheiro de registo de auditoria é de 10 MB. Depois de atingir o limite máximo, o arquivo é renomeado `cimserver_auditlog.0` e um novo `cimserver_auditlog` arquivo é criado para coletar as informações de Registro de auditoria mais recentes.

O provedor NetApp SMI-S mantém os seis arquivos de log de auditoria mais recentes:
`cimserver_auditlog.0` Através ``cimserver_auditlog.5`` do .

Passos

1. Acesse o provedor NetApp SMI-S.
2. Defina o log de auditoria dos comandos SMI-S em tempo de execução:

Ação	Comando
• Ativar o registo de auditoria SMI-S*	<code>cimconfig -s enableAuditLog=true</code>
• Desativar o log de auditoria SMI-S*	<code>cimconfig -s enableAuditLog=false</code>

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.