Verwaltung von Protokollierung und Nachverfolgung

NetApp SMI-S Provider

NetApp
October 04, 2023

Inhalt

Verwaltung von Protokollierung und Nachverfolgung

Überblick

Sie können konfigurieren, wie SMI-S Provider Protokoll- und Trace-Dateien verwaltet, z. B. die Meldungsebenen festlegen, die protokolliert werden sollen, und das Verzeichnis, in dem Protokolle gespeichert werden. Sie geben auch die Komponenten an, die verfolgt werden sollen, das Ziel, auf das Trace-Meldungen geschrieben werden, die Tracing-Ebene und den Speicherort der Trace-Datei.

Konfigurieren Sie die Protokolleinstellungen

Standardmäßig werden alle Systemmeldungen protokolliert. Darüber hinaus befinden sich standardmäßig die Systemmeldungsprotokolle im `logs` Verzeichnis in dem Verzeichnis, in dem NetApp SMI-S Provider installiert ist. Sie können den Speicherort und die Ebene der Systemmeldungen ändern, die in das CIM-Serverprotokoll geschrieben werden. Sie können beispielsweise festlegen, dass Protokolle in einem von Ihnen angegebenen Verzeichnis gespeichert sind und nur tödliche Systemmeldungen in das CIM-Serverprotokoll geschrieben werden.

Bevor Sie beginnen

- Sie müssen bereits Anmeldedaten als Administrator besitzen.
- Sie müssen sich bereits als Administrator beim Hostsystem angemeldet haben.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Führen Sie eine der folgenden Aktionen durch:

Aktion	Befehl	Weitere Informationen
Ändern Sie die Protokollierungsebene für Systemnachrichten	**`cimconfig -s logLevel=`*`new_log_level`*` -p`**	Wenn Sie die Protokollierungsebene z. B. in „`INFORMATION`“ ändern möchten, geben Sie den folgenden Befehl ein: + **`cimconfig -s logLevel=INFORMATION -p`**
Ändern des Protokollverzeichnisses für Systemmeldung	**`cimconfig -s logdir=new_log_directory -p`** Wenn der *`new_log_directory`* Enthält Leerzeichen. Sie müssen es in Anführungszeichen einschließen (`"`*`new log directory`*`"`).	Wenn Sie beispielsweise das Protokollverzeichnis in „`serverlogs`“ ändern möchten, würden Sie diesen Befehl eingeben: **`cimconfig -s logdir=serverlogs -p`**

3. Starten Sie den CIM-Server neu:

```
smis cimserver restart
```

Protokollierungsstufen

Sie können die Arten von Meldungen angeben, die protokolliert werden (z. B. sollen nur tödliche Systemmeldungen protokolliert werden).

Sie können die Protokollierungsebene auf eine der folgenden Optionen konfigurieren:

- **TRACE**

  Speichert Trace-Meldungen im cimserver_Standard-Protokoll.

- * INFORMATION*

  Protokolliert alle (Informations-, Warn-, schweren und tödlichen) Systemmeldungen.

- **WARNUNG**

  Protokolliert Warnungen, schwere und tödliche Systemmeldungen.

- **SCHWERWIEGEND**

  Protokolliert schwerwiegende und tödliche Systemmeldungen

- * TÖDLICH*

  Protokolliert nur fatale Systemmeldungen.

Ablaufverfolgung verwalten

Sie können konfigurieren, wie SMI-S Provider Trace-Dateien verwaltet, z. B. die zu rückverfolgenden Komponenten, das Ziel, auf das Trace-Nachrichten geschrieben werden, die Ebene der Verfolgung und den Speicherort der Trace-Datei.

Festlegen von Trace-Einstellungen

Die Aktivierung der Ablaufverfolgung ist wichtig, um Informationen zur Fehlerbehebung zu sammeln. Die Aktivierung der Nachverfolgung kann sich jedoch auf die Leistung auswirken. Überlegen Sie daher genau, was verfolgt werden muss und wie lange Sie die Verfolgung aktivieren müssen.

Bevor Sie beginnen

- Sie müssen bereits Anmeldedaten als Administrator besitzen.
- Sie müssen sich bereits als Administrator beim Hostsystem angemeldet haben.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.

2. Geben Sie je nach Bedarf verschiedene Trace-Einstellungen an:

Aktion	Befehl
Geben Sie die Komponenten an, die verfolgt werden sollen	**`cimconfig -s traceComponents=`*`components`*` -p`**
Geben Sie die Trace-Funktion an	**`cimconfig -s traceFacility=`*`facility`*` -p`**
Geben Sie den Speicherort der Trace-Datei an	**`cimconfig -s traceFilePath=`*`path_name`*` -p`**
Geben Sie die Trace-Ebene an	**`cimconfig -s traceLevel=`*`level`*` -p`**

3. Starten Sie den CIM-Server neu:

   ```
   smis cimserver restart
   ```

Werte für die Trace-Einstellung

Sie können die zu verfolgenden Komponenten, das Trace-Ziel und die Tracing-Level angeben. Optional können Sie den Namen und den Speicherort der Trace-Datei ändern, wenn Sie den Standardnamen und den Speicherort der Trace-Datei nicht verwenden möchten.

Sie können die folgenden Trace-Einstellungen konfigurieren:

- **TraceComponents**

  Gibt die Komponenten an, die verfolgt werden sollen. Standardmäßig werden alle Komponenten verfolgt.

- **TraceFacility**

  Gibt das Ziel an, auf das Trace-Meldungen geschrieben werden:

  - Datei

    Dies ist der Standardwert, mit dem festgelegt wird, dass Trace-Meldungen in die Datei geschrieben werden, die durch die Konfigurationsoption traceFilePath angegeben wird.

  - Protokoll

    Gibt an, dass Trace-Meldungen in die cimserver_Standard-Protokolldatei geschrieben werden.

- **TraceFilePath**

  Gibt den Speicherort der Trace-Datei an. Standardmäßig ist die Trace Datei benannt `cimserver.trc` Und befindet sich im `traces` Verzeichnis.

- **TraceLevel**

Gibt den Tastgrad an. Standardmäßig ist die Tracing deaktiviert.

Trace-Ebene	Geschriebene Trace-Nachrichten
0	Tastung ist deaktiviert.
1	Schwere Meldungen und Protokollmeldungen.
2	Grundlegende Flow-Trace-Meldungen (geringe Datendetails)
3	Logikfluss zwischen den Funktionen (mittlere Datendetails)
4	Hohes Datendetail
5	Hohe Datendetails + Methode Eingabe und Beenden

Geben Sie die Größe der Trace-Datei an

Wenn Tracing aktiviert ist, beträgt die maximale Trace-Dateigröße standardmäßig 100 MB. Sie können die maximale Trace-Dateigröße erhöhen oder verringern, indem Sie die Umgebungsvariable einstellen `PEGASUS_TRACE_FILE_SIZE`. Der Wert der Trace-Dateigröße kann 10 MB bis 2 GB betragen.

Bevor Sie beginnen

- Sie müssen bereits Anmeldedaten als Administrator besitzen.
- Sie müssen sich bereits als Administrator beim Hostsystem angemeldet haben.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Erstellen Sie eine System- oder Benutzerumgebvariable mit dem Namen `PEGASUS_TRACE_FILE_SIZE` Mit der neuen Trace-Dateigröße in Bytes.

   Windows-Dokumentation enthält weitere Informationen zum Erstellen von Umgebungsvariablen.

3. Starten Sie den CIM-Server neu:

   ```
   smis cimserver restart
   ```

Geben Sie die Anzahl der gespeicherten Trace-Dateien an

Wenn die Ablaufverfolgung aktiviert ist, werden standardmäßig sieben Trace-Dateien gespeichert. Wenn Sie mehr gespeicherte Trace-Dateien benötigen, können Sie die maximale Anzahl der gespeicherten Trace-Dateien erhöhen, indem Sie die Umgebungsvariable einstellen `PEGASUS_TRACE_FILE_NUM`. Wenn Sie die maximale

Anzahl der gespeicherten Trace-Dateien erhöhen, müssen Sie sicherstellen, dass das System über genügend Speicherplatz auf seiner Festplatte verfügt, um die Trace-Dateien aufzunehmen.

Bevor Sie beginnen

- Sie müssen bereits Anmeldedaten als Administrator besitzen.
- Sie müssen sich bereits als Administrator beim Hostsystem angemeldet haben.

Über diese Aufgabe

Wenn die Ablaufverfolgung aktiviert ist, werden die Nachverfolgungsinformationen in das geschrieben `cimserver.trc` Datei: Die Trace-Dateien werden gedreht. Wenn `cimserver.trc` Erreicht die maximale Größe der Trace-Datei, deren Inhalt wird in den verschoben `cimserver.trc.`*`n`* Datei: Standardmäßig ist `n` Ist ein Wert zwischen 0 und 5. Wenn Sie mehr gespeicherte Trace-Dateien benötigen, erhöhen Sie den Wert von *`n`*.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Erstellen Sie eine System- oder Benutzerumgebvariable mit dem Namen `PEGASUS_TRACE_FILE_NUM` Mit der neuen Anzahl von Trace-Dateien gespeichert.

   Windows-Dokumentation enthält weitere Informationen zum Erstellen von Umgebungsvariablen.

3. Starten Sie den CIM-Server neu:

   ```
   smis cimserver restart
   ```

Aktivieren oder Deaktivieren des Prüfprotokolls für SMI-S-Befehle

Alle eingehenden SMI-S-Befehle werden in Audit-Log-Dateien aufgezeichnet, sodass Auditoren die Aktivitäten des WBEM-Client-Betriebs und der Provider-Nutzung nachverfolgen können. Sie können die Protokollierung dieser eingehenden Befehle aktivieren oder deaktivieren, indem Sie eine dynamische Konfigurationseigenschaft festlegen.

Bevor Sie beginnen

- Sie müssen bereits Anmeldedaten als Administrator besitzen.
- Sie müssen sich bereits als Administrator beim Hostsystem angemeldet haben.

Über diese Aufgabe

Audit-Protokolldaten können eine Aufzeichnung von Zugriffs-, Aktivitäts- und Konfigurationsänderungen für einen CIM-Server bereitstellen. Der Inhalt der Audit-Datei enthält den Befehl, von dem der Befehl ausgegeben wurde, und die Zeit, zu der der Befehl ausgegeben wurde.

Die dynamische Konfigurationseigenschaft `enableAuditLog` Aktiviert oder deaktiviert die Audit-Protokollierung während der Laufzeit. Standardmäßig ist enableAuditLog auf true gesetzt.

In der Praxis wird häufig die Audit-Protokollierung aktiviert lassen.

Die Audit-Log-Datei (`cimserver_auditlog`) Wird im pegasus-Log-Verzeichnis gespeichert (`C:\Program Files (x86)\Netapp\smis\pegasus\logs`).

Die maximale Größe der Audit-Log-Datei beträgt 10 MB. Nach Erreichen der Höchstgrenze wird die Datei umbenannt `cimserver_auditlog.0`, Und eine neue `cimserver auditlog` Die Datei wird erstellt, um die neueren Audit-Protokollierungsinformationen zu erfassen.

NetApp SMI-S Provider verwaltet die sechs neuesten Audit-Log-Dateien: `cimserver_auditlog.0` Bis `cimserver_auditlog.5`.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Legen Sie die Auditprotokollierung von SMI-S-Befehlen zur Laufzeit fest:

Aktion	Befehl
SMI-S-Logging für Audits aktivieren	**`cimconfig -s enableAuditLog=true`**
SMI-S-Audit-Protokollierung deaktivieren	**`cimconfig -s enableAuditLog=false`**