



NetApp SMI-S Provider-Dokumentation

NetApp SMI-S Provider

NetApp
October 22, 2024

Inhalt

| | |
|---|----|
| NetApp SMI-S Provider-Dokumentation | 1 |
| Versionshinweise für NetApp SMI-S-Provider | 2 |
| NetApp SMI-S Provider – Übersicht | 3 |
| Überblick | 3 |
| Neu in dieser Version | 3 |
| Nutzung des NetApp SMI-S Provider | 3 |
| Sizing und Performance für NetApp SMI-S-Provider | 3 |
| NetApp SMI-S Provider-Komponenten | 4 |
| NetApp SMI-S-Provider-Protokolle | 4 |
| Wie NetApp SMI-S Provider mit einem Host interagiert | 5 |
| SMI-S-Profile | 5 |
| Implementierungs-Workflow | 6 |
| Vorbereitungen für die Implementierung | 7 |
| Überblick | 7 |
| Unterstützte Betriebssystemversionen | 7 |
| Hardwareanforderungen | 8 |
| Erforderliche Lizenzen | 8 |
| Unterstützte Cluster-Plattformen | 8 |
| Laden Sie das Softwarepaket NetApp SMI-S Provider herunter | 9 |
| Installation des NetApp SMI-S Provider | 10 |
| Installation des NetApp SMI-S Provider auf einem Windows-Host | 10 |
| Deinstallieren Sie NetApp SMI-S Provider | 11 |
| Deinstallieren Sie NetApp SMI-S Provider von einem Windows-Host | 11 |
| Validierung vor der Konfiguration | 12 |
| Überblick | 12 |
| Überprüfen Sie den CIM-Serverstatus | 12 |
| Fügen Sie einen CIM-Serverbenutzer hinzu | 13 |
| Überprüfen Sie, ob das Storage-System ordnungsgemäß funktioniert | 13 |
| Erstellen eines selbstsignierten Zertifikats für den CIM-Server | 14 |
| Verwalten des CIM-Servers | 16 |
| Management von Storage-Systemen | 17 |
| CIM-Server-Benutzer verwalten | 19 |
| Überblick | 19 |
| Typen von CIM-Benutzern und zugehörigen Vorgängen | 19 |
| CIMOM-Konfigurationseinstellungen verwalten | 21 |
| Verwaltung von Protokollierung und Nachverfolgung | 23 |
| Überblick | 23 |
| Konfigurieren Sie die Protokolleinstellungen | 23 |
| Ablaufverfolgung verwalten | 24 |
| Aktivieren oder Deaktivieren des Prüfprotokolls für SMI-S-Befehle | 27 |
| Verwalten Sie die erweiterten Einstellungen für SMI-S Provider | 29 |
| Überblick | 29 |
| Geben Sie das Intervall für die automatische Cache-Aktualisierung von SMI-S Provider an | 29 |

| | |
|--|----|
| Geben Sie den konkreten Wert für die Einsatzdauer an | 29 |
| Geben Sie den ONTAPI-Timeout-Wert an | 30 |
| Geben Sie die maximale Anzahl von Threads pro Nachrichtendienstwarteschlange an | 30 |
| Aktivieren oder deaktivieren Sie die Authentifizierung für NetApp SMI-S Provider | 31 |
| Aktivieren Sie die Indikationen im SMI-S-Provider | 31 |
| SLP verwalten | 33 |
| Überblick | 33 |
| Legen Sie die Optionen für die SLP-Konfiguration fest | 33 |
| CIMOM-Befehle | 35 |
| Zimconfig | 35 |
| CIM-Benutzerbefehle | 37 |
| cimuser | 37 |
| SMI-S Provider-Befehle | 39 |
| Überblick | 39 |
| smis hinzufügen | 39 |
| smis addSecure | 41 |
| smis cimom | 42 |
| smis Cimserver | 43 |
| smis-Klasse | 44 |
| smis config show | 45 |
| smis crp | 47 |
| smis crsp | 49 |
| smis löschen | 50 |
| smis-Festplatten | 51 |
| smis-Exporte | 52 |
| smis-Initiatoren | 53 |
| smis lizenziert | 54 |
| smis-Liste | 54 |
| smis luns | 55 |
| smis Namespaces | 56 |
| smis-Pools | 57 |
| smis-Aktualisierung | 57 |
| smis slpd | 58 |
| smis-Version | 59 |
| smis Volumes | 59 |
| SLP-Befehle | 61 |
| Slptool | 61 |
| Slptool Findattr | 61 |
| Slptool findsrvs | 62 |
| Fehler bei SMI-S Provider beheben | 64 |
| Überblick | 64 |
| Fehler beim Zugriff verweigert | 64 |
| Mögliche Fehler beim Laden von gemeinsam genutzten Bibliotheken | 64 |
| Verbindung abgelehnt | 65 |
| Filer Rückgabe: Kein ONTAP-Element als Antwort | 65 |

| | |
|--|----|
| Klon-/Snapshot-Vorgänge sind nicht zulässig | 66 |
| Warnung 26130 | 66 |
| HostAgentAccessDenied (ID: 26263) | 66 |
| Verbindung mit localhost:5988 nicht möglich | 67 |
| Verbindung mit localhost:5989 nicht möglich | 68 |
| SMI-S Provider stürzt in Windows ab | 68 |
| Geben Sie Passwörter mit Sonderzeichen ein | 69 |
| Im SMI-S Provider verwendete Klontechnologie | 70 |
| Die Sichtbarkeit wichtiger Objekte bestätigen | 70 |
| Anforderung für die Verwendung von Dateiservern unter Windows | 70 |
| Nicht standardmäßige Firewalls müssen Ports manuell als Ausnahmen hinzugefügt werden | 71 |
| Es kann kein Speichersystem mit einem nicht standardmäßigen HTTP- oder HTTPS-Port hinzugefügt werden | 71 |
| Keine Antwort vom Server | 72 |
| Probleme mit der Laufzeitbibliothek | 72 |
| Der NetApp SMI-S Provider kann sehr lange gestartet werden | 72 |
| Unstimmigkeiten beim Management des gesamten Speicherplatzes für einen Storage Pool (Volume) | 73 |
| Der Netzwerkpfad wurde nicht gefunden | 73 |
| Es sind nicht genügend Systemressourcen vorhanden, um den angeforderten Service abzuschließen | 73 |
| Die Größe der SMB-Freigabe wird in SCVMM auf 0 verkleinert | 74 |
| Der SCVMM-Scan-Vorgang konnte nicht gefunden oder mit SMI-S-Provider kommunizieren | 74 |
| Rechtliche Hinweise | 76 |
| Urheberrecht | 76 |
| Marken | 76 |
| Patente | 76 |
| Datenschutzrichtlinie | 76 |
| Hinweis | 76 |

NetApp SMI-S Provider-Dokumentation

Willkommen bei der NetApp SMI-S Provider Information Library. Hier finden Sie Dokumentation zur NetApp SMI-S Provider-Software, einschließlich Installation und Management von NetApp SMI-S Provider, einer befehlsbasierten Schnittstelle, die NetApp Storage-Systeme erkennt und managt.

Die Dokumentation für frühere Versionen von NetApp SMI-S Provider finden Sie auf der ["NetApp Support Website"](#).

Versionshinweise für NetApp SMI-S-Provider

Der "[Versionshinweise für NetApp SMI-S-Provider](#)" Beschreiben Sie neue Funktionen, Upgrade-Hinweise, feste Probleme, bekannte Einschränkungen und bekannte Probleme.

NetApp SMI-S Provider – Übersicht

Überblick

Mit NetApp SMI-S Provider 5.2.5 können Sie Storage-Systeme verwalten und überwachen sowie LUNs und Volumes von Storage-Systemen, CIMOM-Konfigurationseinstellungen und CIM-Server-Benutzer verwalten.

Der NetApp SMI-S Provider ist eine befehlsbasierte Schnittstelle, die Plattformen erkennt und managt, auf denen ONTAP Software ausgeführt wird. SMI-S Provider verwendet webbasierte WBEM-Protokolle (Enterprise Management), mit denen Sie Storage-Elemente managen, überwachen und in Berichten erfassen können.

NetApp SMI-S-Provider verwendet Schemata, die von zwei Unternehmen standardisiert wurden:

- ["Distributed Management Task Force \(DMTF\)"](#)
- ["Storage Networking Industry Association \(SNIA\)"](#)

SMI-S-Provider ersetzt bei allen Komponenten eines Storage-Netzwerks die Verwendung mehrerer Managed-Object-Modelle, Protokolle und Übertragungen durch ein einzelnes objektorientiertes Modell.

Neu in dieser Version

- Für SMI-S Provider 5.2.5 ist kein Upgrade-Pfad verfügbar.
- Sie müssen SMI-S Provider 5.2.5 als neue Installation verwenden.

Für Windows-Benutzer:

- Diese Version ist nicht kompatibel mit Windows Server 2012 oder System Center Virtual Machine Manager (SCVMM) 2012.
- SMI-S Provider 5.2.5 unterstützt Windows Server 2016, Windows Server 2019, SCVMM 2016 und SCVMM 2019.

Nutzung des NetApp SMI-S Provider

NetApp SMI-S Provider vereinfacht das Managen und Überwachen von Storage-Systemen sowie das Managen von LUNs und Volumes von Storage-Systemen.

Mithilfe von NetApp SMI-S-Provider können Sie Storage-Controller mithilfe von System Center 2016 - Virtual Machine Manager oder System Center 2016 - Virtual Machine Manager managen.

Sizing und Performance für NetApp SMI-S-Provider

Wenn Sie wissen, wie viele Systeme vom NetApp SMI-S-Provider gemanagt werden, können Sie die Performance-Möglichkeiten kennen.

Größe

NetApp SMI-S-Provider können in Clustered Data ONTAP bis zu folgende Objektanzahl managen:

- 100 Storage Virtual Machines (SVMs) (ohne Indikationen)
- 10 Lagerung virtueller Maschinen (mit Indikationen)
- 1,500 LUNs (pro FlexVol Volume)
- 200 CIFS-Dateifreigaben (pro FlexVol Volume)

Wenn die FlexVol sowohl qtrees als auch Volumes enthält, werden die qtrees als Verzeichnisse angezeigt. Beim Löschen von Volumes sollten Sie darauf achten, dass die qtrees nicht versehentlich gelöscht werden.

Leistungshinweis

Bei Konfigurationen mit 5,000 FlexVol Volumes oder 300,000 Snapshot Kopien können im Folgenden Performance-Probleme auftreten `cimcli` Befehl:

- `cimcli ei ONTAP_Snapshot -n root/ontap`
- `cimcli ei ONTAP_SnapshotBasedOnFlexVol -n root/ontap`
- `cimcli ei ONTAP_StorageVolumeStats -n root/ontap`

Das Interoperabilitäts-Matrix-Tool (IMT) enthält die neuesten Informationen zur Dimensionierung und Performance.

NetApp SMI-S Provider-Komponenten

NetApp SMI-S Provider besteht aus drei Komponenten, mit denen Sie Storage-Systeme managen und überwachen können: CIMOM, Provider-Objekte und ein Repository.

- *** CIMOM***

Dies ist die Grundlage für NetApp SMI-S Provider. CIMOM erfasst, validiert und authentifiziert jede Anwendungsanfrage und antwortet anschließend auf die Applikation. Es wird zu einem Kabelkanal für jede Anforderung, indem der entsprechende Provider zur Bearbeitung jeder Anfrage anruft.

- **Provider-Objekte**

Wenn ein Host einen Befehl oder eine Abfrage an SMI-S Provider ausgibt, lädt CIMOM ein freigegebenes Bibliotheksobjekt, ruft es auf, eine Anforderung zu bearbeiten und gibt die daraus resultierenden Informationen an den Host zurück.



Windows-Hosts verwenden DLL-Objekte.

- **Repository**

Für sein Repository verwendet CIMOM eine Flatfile-Datenbank. Es speichert persistente Daten, die auf CIM-Ebene benötigt werden.

NetApp SMI-S-Provider-Protokolle

NetApp SMI-S-Provider verwendet die CIM-XML-Verschlüsselung über HTTPS und Service Location Protocol (SLP).

- **CIM-XML-Kodierung über HTTPS**

Protokoll, das Informationen zwischen einem Web-basierten Enterprise Management (WBEM)-fähigen Management-Client und dem CIMOM-Server austauscht. CIM-XML-Codierung über HTTPS verwendet das CIM-Protokoll als Nutzlast und HTTPS als Transport. HTTP wird auch unterstützt.

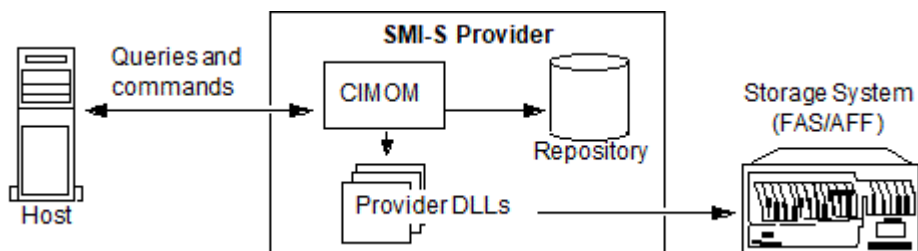
- **SLP**

Discovery-Protokoll, das WBEM-Dienste innerhalb eines LAN erkennt.

Wie NetApp SMI-S Provider mit einem Host interagiert

Wenn eine Client-Anwendung auf einem Host den CIMOM-Server mithilfe von SLP (CIM-XML-Codierung über HTTP) erkennt, fragt der Client das CIMOM nach gemeinsam genutzten Objekten (Objekte, die in der CIM-Sprache modelliert sind) ab. Der CIMOM lädt gemeinsam genutzte Objekte und fragt das Speichersystem ab. Dabei werden gerätespezifische APIs für die angeforderten Informationen verwendet.

Die folgende Abbildung zeigt die Interaktion von NetApp SMI-S Provider mit einem WBEM-Management-Client, wenn SMI-S Provider eine Abfrage oder einen Befehl erhält.

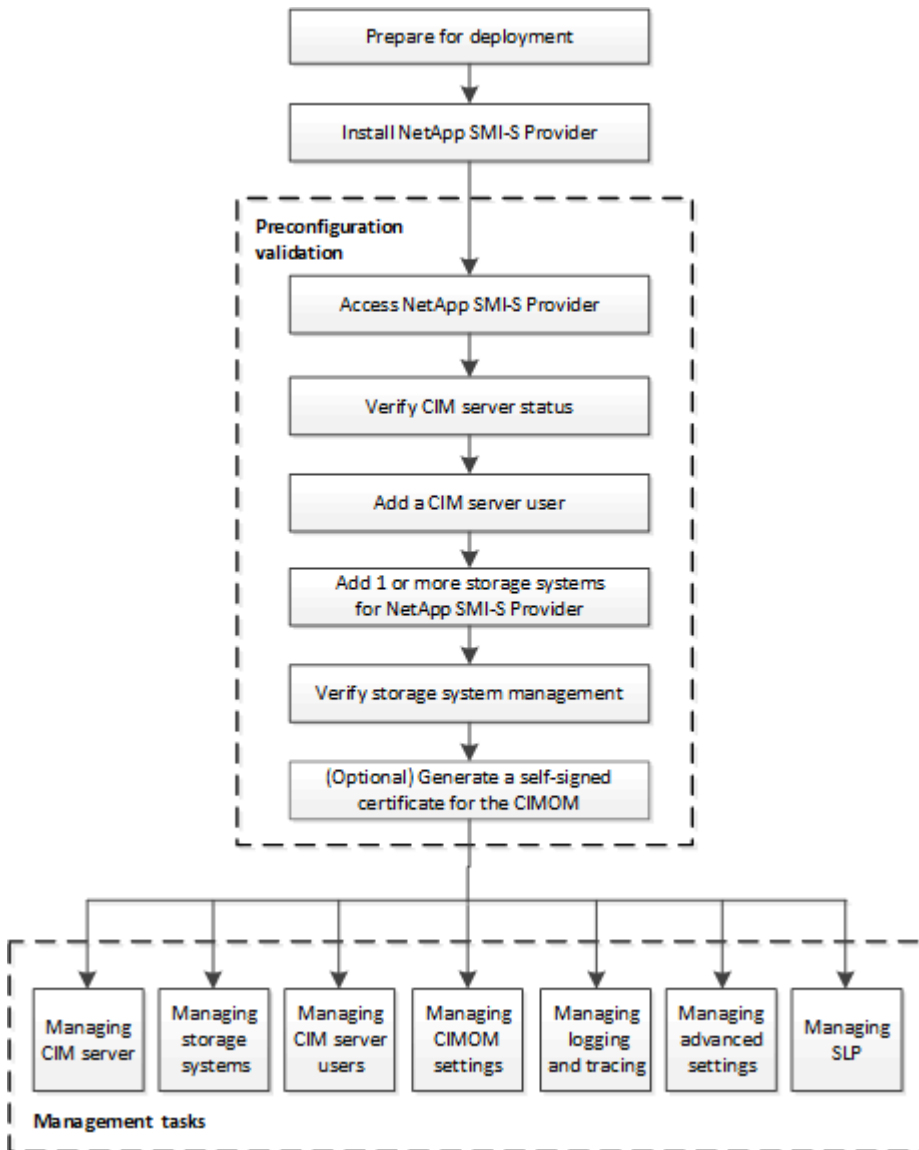


SMI-S-Profile

SMI-S Provider verwendet Profile und Unterprofile, die SMI-S v1.7 erfüllen. Informationen zu SMI-S v1.7 finden Sie auf der Seite SNIA: Technology Standards and Software.

Implementierungs-Workflow

Bevor Sie Ihre Speichersysteme mit SMI-S Provider verwalten und überwachen können, müssen Sie die SMI-S Provider-Software installieren und Ihre vorläufige Konfiguration überprüfen.



Vorbereitungen für die Implementierung

Überblick

Bevor Sie NetApp SMI-S Provider implementieren, müssen Sie überprüfen, ob ein unterstütztes Betriebssystem und eine unterstützte Plattform vorhanden sind, dass Sie über die erforderlichen Lizenzen verfügen und dass Ihre Hosts die Mindestanforderungen erfüllen.

Unterstützte Betriebssystemversionen

Vor der Installation von SMI-S Provider müssen Sie überprüfen, ob auf dem Windows-Host ein unterstütztes Betriebssystem ausgeführt wird.

| Betriebssystem | Unterstützte Versionen | Erforderliche Client Software |
|----------------|---|--|
| Windows | <ul style="list-style-type: none">• Microsoft Windows Server 2016• Microsoft Windows Server 2019 | Die Runtime-Bibliotheken von Microsoft Visual C++ 2010 werden während der Installation von SMI-S Provider automatisch installiert. Um mögliche Probleme im Zusammenhang mit Laufzeitbibliotheken zu vermeiden, müssen Sie Microsoft Visual C++ 2010 Redistributable Package (x86) installieren. Von der folgenden Adresse aus: http://www.microsoft.com |

SCVMM 2016 UR 2.1-Anforderung

System Center Virtual Machine Manager (SCVMM) 2016 Update Rollup (UR) 2.1 ist für das Management des NetApp File Servers mit NetApp SMI-S Provider 5.2.4 und höher erforderlich.

Ohne diese UR zeigt SCVMM 2016 den Wert des an `Total Capacity` Und `Available Capacity` Optionen als `0 GB` Für vorhandene File Shares in NetApp File Server.

Zum Ausführen von SMI-S Provider muss der Provider-Hostcomputer die folgenden Spezifikationen erfüllen:

- Der Provider-Hostcomputer kann nicht zum Hosten eines Hyper-V-Knotens verwendet werden.
- SCVMM darf nicht auf dem Hostcomputer des Anbieters ausgeführt werden.
- Auf dem Host-Rechner des Providers dürfen andere speicherintensive Programme nicht ausgeführt werden.
- Auf dem Provider-Host-Rechner dürfen keine SMI-S-Provider eines anderen Anbieters ausgeführt werden.

Die folgenden Hypervisoren werden unterstützt:

- Microsoft Windows Server 2016 Hyper-V

- VMware ESX 5.0
- VMware ESX 5.1
- VMware ESX 5.5
- VMware ESX 6.0

Hardwareanforderungen

Sie müssen überprüfen, ob der Windows-Host die Mindestanforderungen an die Hardware erfüllt, bevor Sie den NetApp SMI-S Provider installieren.

| Trennt | Anforderungen |
|-------------------------------|---|
| Speicher | <ul style="list-style-type: none"> • 4 GB RAM (mindestens) • 8 GB RAM (empfohlen) |
| Festplattenspeicher benötigen | <ul style="list-style-type: none"> • 1 GB (mindestens) • 4 GB (empfohlen) <p>Die Aktivierung der Protokollierung und Verfolgung erfordert je nach den Einstellungen für die Drehung der Protokoll- und Trace-Dateien zusätzlichen Speicherplatz von bis zu 1 GB.</p> <p>Sie benötigen 100 MB temporären Speicherplatz für die Installation.</p> |
| CPU | <ul style="list-style-type: none"> • Dual-Core 2.0 GHz (mindestens) • Quad-Core 2.0 GHz (empfohlen) |

Erforderliche Lizenzen

Um NetApp SMI-S Provider zu verwenden, müssen Sie über die erforderlichen Lizenzen verfügen.

Für NetApp SMI-S Provider sind folgende Lizenzen erforderlich:

- Zum Erstellen von LUNs auf den Storage-Systemen sind FCP-, iSCSI- oder FCP- und iSCSI-Lizenzen erforderlich.
- Zum Erstellen von Dateifreigaben auf unterstützten ONTAP Storage-Systemen ist eine CIFS-Lizenz erforderlich.
- Zum Erstellen von LUN-Klonen auf Clustered Storage-Systemen, auf denen unterstützte ONTAP Versionen ausgeführt werden, ist eine FlexClone Lizenz erforderlich.

Unterstützte Cluster-Plattformen

Der NetApp SMI-S-Provider unterstützt Cluster-Plattformen mit Data ONTAP 8.3.2 und

ONTAP 9 sowie höher.

Damit NetApp SMI-S Provider Klone von Storage Volumes (LUNs) erstellen kann, muss eine FlexClone Lizenz auf dem Storage-System installiert sein.

NetApp SMI-S-Provider unterstützt die folgenden Plattformen:

- Systeme der FAS Serie
- V-Series Storage-Systemen

Laden Sie das Softwarepaket NetApp SMI-S Provider herunter

Vor der Installation von NetApp SMI-S Provider müssen Sie das Softwarepaket von der NetApp Support-Website herunterladen.

Bevor Sie beginnen

Sie müssen ein NetApp Support Site Konto von erstellt haben "[NetApp Support](#)".

Schritte

1. Rufen Sie auf der NetApp Support-Website die Seite **Downloads > Software** auf.
2. Suchen Sie nach SMI-S Provider (früher Data ONTAP SMI-S Agent), wählen Sie Windows-Betriebssystem und klicken Sie dann auf **Go!**.
3. Wählen Sie die Version aus, die Sie herunterladen möchten, indem Sie auf **Ansicht & Download** klicken.
4. Klicken Sie im Bereich **Software Download** auf **WEITER**.
5. Lesen und akzeptieren Sie die Endnutzer-Lizenzvereinbarung.
6. Wählen Sie die Software-Paketdatei aus, und speichern Sie sie anschließend an Ihrem gewünschten Speicherort.

Installation des NetApp SMI-S Provider

Installation des NetApp SMI-S Provider auf einem Windows-Host

Sie können NetApp SMI-S Provider-Software installieren, sodass Sie Storage-Systeme mit Data ONTAP managen können. Sie können jedoch nicht auf eine frühere Version zurücksetzen oder herunterstufen. Standardmäßig ist die NetApp SMI-S Provider-Software in installiert `C:\Program Files (x86)\NetApp\smis\pegasus` Verzeichnis.

Bevor Sie beginnen

Sie müssen bereits über die folgenden Anmeldedaten und die folgende Software verfügen:

- Anmeldedaten für das Windows-Administratorkonto anmelden
- Softwarepaket NetApp SMI-S Provider

Über diese Aufgabe

Aufgrund des Installationsprozesses führen der CIMOM-Service (unter dem Namen „NetApp SMI-S Provider“ im Service Control Manager) und der SLP-Daemon (im Service Control Manager unter dem Namen „Service Location Protocol“ genannt) als automatische Services aus, die selbst nach einem Neustart eines Hosts automatisch starten.

Dieses Installationsverfahren enthält eine neue Installation.

Schritte

1. Melden Sie sich als Administrator an.
2. Wechseln Sie zum Verzeichnis, das das NetApp SMI-S Provider-Softwarepaket enthält (``smisprovider-version_number.msi``) Und doppelklicken Sie anschließend auf den Paketnamen.
3. Führen Sie die Schritte im Setup-Assistenten aus.

Ergebnis

NetApp SMI-S Provider wird automatisch gegen Ende des Installationsprozesses gestartet.

Deinstallieren Sie NetApp SMI-S Provider

Deinstallieren Sie NetApp SMI-S Provider von einem Windows-Host

Sie können SMI-S Provider bei Bedarf deinstallieren. Je nach Version der vorhandenen Installation müssen Sie beispielsweise die vorhandene Installation von SMI-S Provider deinstallieren, bevor Sie die neueste Version installieren können.

Über diese Aufgabe

Wenn Sie SMI-S Provider deinstallieren und eine Neuinstallation wünschen, müssen Sie den gesamten Inhalt manuell vom CIM-Server löschen.

Wenn Sie keine Neuinstallation wünschen, behält SMI-S Provider nach der Deinstallation die Konfigurations-, Benutzer- und andere Datenbankdateien bei.

Schritte

1. Melden Sie sich als Administrator an.
2. Deinstallieren Sie NetApp SMI-S Provider von einem Windows-Host mithilfe des Dienstprogramms „Software“.

Validierung vor der Konfiguration

Überblick

Bevor Sie SMI-S Provider zum ersten Mal verwenden, müssen Sie Ihre vorläufige Konfiguration überprüfen.

Führen Sie die folgenden Aufgaben durch, bevor Sie SMI-S Provider verwenden:

1. Stellen Sie beim NetApp SMI-S Provider sicher, dass der CIM-Server gestartet wird.
2. Fügen Sie einen CIM-Serverbenutzer hinzu.
3. Überprüfen Sie die Verwaltung des Speichersystems durch Hinzufügen von mindestens einem Speichersystem für SMI-S Provider.
4. **Optional:** Erstellen Sie ein selbstsigniertes Zertifikat für das CIMOM.

Standardmäßig ist die Authentifizierung für SMI-S Provider aktiviert.

Nach der erfolgreichen Durchführung dieser Validierung können Sie beginnen, Ihre Speichersysteme mithilfe von NetApp SMI-S Provider zu managen.

Überprüfen Sie den CIM-Serverstatus

Nach der Installation von NetApp SMI-S Provider müssen Sie überprüfen, ob der CIM-Server nach dem Zugriff auf SMI-S Provider automatisch gestartet wird.

Bevor Sie beginnen

Sie müssen bereits Anmeldedaten als Administrator besitzen.

Schritte

1. Melden Sie sich als Administrator an.
2. Greifen Sie auf NetApp SMI-S Provider zu, indem Sie zu dem Verzeichnis navigieren, in dem sich die ausführbaren Dateien befinden:

| Sie verwenden... | Dann tun Sie das... |
|---|---|
| Eingabeaufforderung (mit erhöhten Administratorrechten) | Navigieren Sie zu C:\Program Files (x86)\NetApp\smis\pegasus\bin |
| Start > Programme Menü | Klicken Sie mit der rechten Maustaste NetApp SMI-S Provider und wählen Sie aus Run as Administrator . |

3. Anzeigen des CIM-Serverstatus:

```
smis cimserver status
```

Wenn der CIM-Server gestartet wurde, wird die folgende Meldung angezeigt:

NetApp SMI-S Provider is running.

Fügen Sie einen CIM-Serverbenutzer hinzu

Bevor Sie das Speichersystem validieren können, müssen Sie einen CIM-Benutzer hinzufügen, der zur Verwendung des CIM-Servers autorisiert ist.

Bevor Sie beginnen

- Sie müssen sich bereits als Administrator angemeldet haben.
- Sie müssen bereits auf SMI-S Provider zugreifen.

Schritte

1. Erstellen Sie ein lokales Benutzerkonto.
2. Fügen Sie den Benutzer der Gruppe Administratoren hinzu.

Weitere Informationen finden Sie unter *Systemdokumentation*.

3. Hinzufügen eines CIM-Serverbenutzers:

```
cimuser -a -u user_name
```

So fügen Sie beispielsweise einen CIM-Serverbenutzer namens „chris“ hinzu:

```
cimuser -a -u chris
```

4. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein, und geben Sie es erneut ein.

Überprüfen Sie, ob das Storage-System ordnungsgemäß funktioniert

Bevor SMI-S Provider konfiguriert werden kann, müssen Sie dem CIMOM-Repository mindestens ein Speichersystem hinzufügen und anschließend überprüfen, ob das Speichersystem ordnungsgemäß funktioniert.

Bevor Sie beginnen

- Sie müssen sich bereits als Administrator angemeldet haben.
- Sie müssen bereits auf SMI-S Provider zugreifen.

Schritte

1. Fügen Sie dem CIMOM-Repository mindestens ein Storage-System hinzu:

| So fügen Sie ein Storage-System mit... | Diesen Befehl eingeben... |
|--|--|
| HTTP-Verbindung zwischen dem Provider und dem Speichersystem | smis add storage_sys storage_sys_user |

| So fügen Sie ein Storage-System mit... | Diesen Befehl eingeben... |
|---|--|
| HTTPS-Verbindung zwischen dem Provider und dem Speichersystem | <code>smis addsecure storage_sys storage_sys_user</code> |

Der Befehl wartet bis zu 15 Minuten, bis der Provider den Cache aktualisiert und antwortet.

2. Überprüfen Sie die Ausgabe für die folgenden Befehle:

| Für diesen Befehl... | Überprüfen Sie, dass... |
|---------------------------|--|
| <code>smis list</code> | Die Anzahl der Elemente entspricht der Anzahl der zu verwaltenden Storage-Systeme. |
| <code>smis disks</code> | Die Anzahl der Festplatten entspricht der Gesamtzahl der Festplatten aller Storage-Systeme. |
| <code>smis luns</code> | Die Anzahl der LUNs entspricht der Gesamtzahl der LUNs auf allen Storage-Systemen. |
| <code>smis pools</code> | Die Anzahl der ONTAP_ConcertePools entspricht der Gesamtzahl der Aggregate auf allen Storage-Systemen. |
| <code>smis volumes</code> | Die Anzahl der Volumes entspricht der Gesamtzahl der Volumes aller Storage-Systeme. |

Erstellen eines selbstsignierten Zertifikats für den CIM-Server

Standardmäßig ist die SSL-Authentifizierung für den CIM-Server aktiviert. Während der Installation des SMI-S Provider wird ein selbstsigniertes Zertifikat für den CIM-Server installiert `pegasus` Verzeichnis. Sie können Ihr eigenes selbstsigniertes Zertifikat generieren und es anstelle des Standardzertifikats verwenden.

Bevor Sie beginnen

- Sie müssen sich bereits als Administrator angemeldet haben.
- Sie müssen bereits auf SMI-S Provider zugreifen.

Schritte

1. Laden Sie die herunter `openssl.cnf` Datei vom folgenden Speicherort:
["http://web.mit.edu/crypto/openssl.cnf"](http://web.mit.edu/crypto/openssl.cnf)
2. Verschieben Sie die `openssl.cnf` Datei in das bin-Verzeichnis:

```
%PEGASUS_HOME%\bin\openssl.cnf
```

3. Stellen Sie die ein `OPENSSL_CONF` Umgebungsvariable zur Position des `openssl.cnf` Datei:

```
C:\ >set OPENSSL_CONF=%PEGASUS_HOME%\bin\openssl.cnf
```

Dadurch wird nur die Umgebungsvariable für die Dauer der aktuellen Eingabeaufforderung festgelegt. Wenn Sie die Umgebungsvariable dauerhaft festlegen möchten, können Sie eine der folgenden Optionen verwenden:

- Navigieren Sie zu **Eigenschaften > Umgebungsvariablen** und aktualisieren Sie die Variable unter **System**.
- Verwenden Sie die Eingabeaufforderung, um die Variable dauerhaft festzulegen:

```
setx OPENSSL_CONF "%PEGASUS_HOME%\bin\openssl.cnf.
```

Die Variable wird festgelegt, wenn Sie eine neue Eingabeaufforderung-Sitzung öffnen.

4. Navigieren Sie zum `%PEGASUS_HOME%\bin` Verzeichnis:

```
C:\>cd %pegasus_home%\bin
```

5. Privaten Schlüssel generieren:

```
openssl genrsa -out cimom.key 2048
```

6. Erstellen einer Zertifikatanforderung:

```
openssl req -new -key cimom.key -out cimom.csr
```

7. Geben Sie bei der entsprechenden Aufforderung Ihre Informationen für die Zertifikatanforderung ein.

8. Generieren Sie das selbstsignierte Zertifikat:

```
openssl x509 -in cimom.csr -out cimom.cert -req -signkey cimom.key -days 1095
```

Sie können eine andere Anzahl von Tagen angeben, für die das Zertifikat gültig ist.

9. Kopieren Sie die `cimom.key` Und `cimom.cert` Dateien auf `pegasus` Verzeichnis (Windows:

```
C:\Program Files (x86)\NetApp\smis\pegasus).
```

Ergebnis

Der Datumsbereich des Zertifikats beginnt am aktuellen Datum und wird für die angegebene Anzahl von Tagen ausgeführt.

Verwalten des CIM-Servers

Sie können den CIM-Server über den SMI-S-Provider starten, stoppen und neu starten sowie dessen Status überprüfen.

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 |
|------------------------------------|-------------------------------------|---|
| Starten Sie den CIM-Server | <code>smis cimserver start</code> | Nach Eingabe des Befehls wird alle drei Minuten eine Statusmeldung angezeigt. Wenn ein Versuch, den CIM-Server zu erreichen, fehlschlägt, werden fünf weitere Versuche unternommen, den Server zu kontaktieren. |
| Beenden Sie den CIM-Server | <code>smis cimserver stop</code> | NA |
| Starten Sie den CIM-Server neu | <code>smis cimserver restart</code> | NA |
| Zeigen Sie den CIM-Serverstatus an | <code>smis cimserver status</code> | NA |

Management von Storage-Systemen

Mithilfe von NetApp SMI-S Provider-Befehlen können Speichersysteme im CIMOM-Repository hinzugefügt, gelöscht und aufgelistet werden. Sie können auch NFS- und CIFS-Exporte und exportierte LUNs für Storage-Systeme auflisten.

Bevor Sie beginnen

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

Über diese Aufgabe

Bei ONTAP müssen Sie eine Management-IP-Adresse für eine SVM und keine Cluster-IP-Adresse angeben und die Anmeldedaten für einen vsadmin-Benutzer angeben. SMI-S-Provider unterstützt keine Cluster-IP-Adressen oder Node-Management-IP-Adressen und unterstützt weder Node-Admin noch Node-SVMs.



Sie sollten den Wert des Datenprotokolls auf `set none` Für die Management-LIF, wenn Sie sie zum SMI-S Provider hinzufügen.

Schritte

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

| Aktion | Befehl | Weitere Informationen |
|--|--|--|
| Fügen Sie ein Speichersystem mit einer HTTP-Verbindung zwischen dem Anbieter und dem Speichersystem hinzu | <code>smis add storage_sys storage_sys_user</code> | Der Befehl wartet bis zu 15 Minuten, bis der Provider den Cache aktualisiert und antwortet. |
| Fügen Sie ein Speichersystem mit einer HTTPS-Verbindung zwischen dem Provider und dem Speichersystem hinzu | <code>smis addsecure storage_sys storage_sys_user</code> | Der Befehl wartet bis zu 15 Minuten, bis der Provider den Cache aktualisiert und antwortet. |
| Listen Sie NFS- und CIFS-Exporte für ein Storage-System auf | <code>smis exports</code> | Keine |
| Listen Sie die Speichersysteme für das CIMOM-Repository auf | <code>smis list</code> | Sie können diesen Befehl ausführen, um die Speichersysteme im CIMOM-Repository zu überprüfen, bevor Sie Speichersysteme hinzufügen oder löschen. |
| Liste der exportierten LUNs für ein Speichersystem | <code>smis luns</code> | Keine |

| Aktion | Befehl | Weitere Informationen |
|---|--------------------------------|---|
| Löschen eines Speichersystems aus dem CIMOM-Repository | smis delete storage_sys | <p>Wenn Sie ein Storage-System nicht mehr managen müssen, können Sie es aus dem CIMOM Repository löschen.</p> <p>Da SMI-S Provider Informationen aus allen Speichersystemen im CIMOM-Repository erfasst, sollten Sie ein nicht verwendetes Speichersystem aus dem Repository löschen, um eine optimale Leistung zu gewährleisten.</p> |
| Die aktuellen Konfigurationsinformationen für den CIM-Server auflisten | smis config show | Keine |
| Geben Sie die FC- und iSCSI-Portinformationen für das Storage-System an | smis initiators | Keine |
| Listen Sie die Speicherpools für das Speichersystem auf | smis pools | Keine |
| Erstellen Sie eine Liste der herkömmlichen und flexiblen Volumes für das Storage-System | smis volumes | Keine |

CIM-Server-Benutzer verwalten

Überblick

Sie können den SMI-S-Provider verwenden, um CIM-Benutzer hinzuzufügen und zu entfernen, die zur Verwendung des CIM-Servers autorisiert sind. Sie können auch alle aktuellen CIM-Benutzer auflisten und ihre Passwörter ändern.

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 ein lokales Benutzerkonto.
3. Fügen Sie den Benutzer der Gruppe Administratoren hinzu.

Weitere Informationen finden Sie unter *Systemdokumentation*.

4. Führen Sie eine der folgenden Aktionen durch:

| Aktion | Befehl | Weitere Informationen |
|--|--------------------------------------|---|
| Fügen Sie einen CIM-Serverbenutzer hinzu | <code>cimuser -a -u user_name</code> | Geben Sie nach Eingabe des Befehls das Passwort ein und geben Sie es bei der entsprechenden Eingabeaufforderung erneut ein. |
| Listen Sie die aktuellen Benutzer auf, die für die Verwendung des CIM-Servers autorisiert sind | <code>cimuser -l</code> | NA |
| Ändern Sie das Kennwort für einen CIM-Serverbenutzer | <code>cimuser -m -u user_name</code> | Geben Sie nach Eingabe des Befehls das neue und das alte Passwort ein, und geben Sie es bei der entsprechenden Aufforderung wieder ein. |
| Entfernen Sie einen CIM-Serverbenutzer, der nicht für die Verwendung des CIM-Servers autorisiert ist | <code>cimuser -r -u user_name</code> | NA |

Typen von CIM-Benutzern und zugehörigen Vorgängen

Bei der Verwendung von SMI-S Provider gibt es verschiedene Benutzertypen, die Sie

einem Benutzer zuweisen können, um den Zugriff auf den CIM-Server zu steuern.

Ab dieser Version kann der Domain-Benutzer die Benutzerdatenbank des SMI-S Provider und andere Konfigurationseinstellungen als Domain-Benutzer der lokalen Administratorengruppe ändern.

In der folgenden Tabelle sind die unterstützten Benutzer des CIM-Servers und die Vorgänge aufgeführt, die jeder Typ ausführen kann.

| Benutzertyp | Betrieb |
|---|--|
| Domänenadministrator der Administratorgruppe | <p>Konfiguration des SMI-S Provider und Benutzerverwaltung mit <code>cimconfig</code> Und <code>cimuser</code> Befehle. Beispiel:</p> <ul style="list-style-type: none"> • Fügen Sie einen Benutzer zum oder aus dem Trust Store von SMI-S Provider hinzu oder entfernen Sie ihn. • Aktivieren, Deaktivieren oder Ändern der Protokollebene und der Ablaufverfolgungskonfiguration • Aktivieren oder deaktivieren Sie die Authentifizierungs-Engine im SMI-S Provider. <p>Storage Management und Verifizierung mit <code>smis</code> Und <code>cimcli</code> Befehle. Beispiel:</p> <ul style="list-style-type: none"> • Storage-Controller oder SVMs zu oder von einem SMI-S-Provider-Repository oder einer Datenbank oder einem Cache hinzufügen oder entfernen. • Aktualisierung von Storage-Controllern oder SVMs im SMI-S-Provider-Cache • Überprüfung des Storage-Controller oder SVM-Managements <p>SCVMM-Erkennungsvorgänge mithilfe der SCVMM-GUI</p> |
| Domänenbenutzer der lokalen Administratorengruppe | Lokaler Benutzer der lokalen Administratorgruppe |
| Integrierter Domain Administrator-Benutzer | Integrierter lokaler Administrator-Benutzer |
| Domänenbenutzer der Benutzergruppe | SCVMM-Erkennungsvorgänge mithilfe der SCVMM-GUI |



Wenn Sie einen SMI-S Provider auf einem Windows-Host haben und einen Benutzernamen „Administrator“ geändert haben, müssen Sie sich aus dem System abmelden und dann wieder anmelden. Der SMI-S Windows Service übernimmt die Authentifizierung in diesem Zeitraum. Dadurch werden Änderungen an den Anmeldeinformationen erst erkannt, wenn sich der Administrator abmeldet und sich dann erneut anmeldet.

CIMOM-Konfigurationseinstellungen verwalten

Sie können SMI-S Provider zum Verwalten der CIMOM-Konfiguration verwenden, z. B. Aktivieren oder Deaktivieren von HTTP- und HTTPS-Verbindungen sowie Ändern von HTTP- und HTTPS-Port-Nummern. Standardmäßig sind HTTP-Verbindungen aktiviert, sodass Clients ohne SSL-Verschlüsselung eine Verbindung zum CIM-Server herstellen können.

Bevor Sie beginnen

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

Über diese Aufgabe

Wenn in Ihrer Umgebung verschlüsselter Datenverkehr vom und zum CIM-Server erforderlich ist, müssen Sie zuerst HTTP-Verbindungen deaktivieren und dann überprüfen, ob HTTPS-Verbindungen für den CIM-Server aktiviert sind.

Schritte

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

| Aktion | Befehl | Weitere Informationen |
|--------------------------------------|--|---|
| Aktivieren Sie die HTTP-Verbindung | <pre>cimconfig -s enableHttpConnection=true -p</pre> | NA |
| Deaktivieren Sie die HTTP-Verbindung | <pre>cimconfig -s enableHttpConnection=false -p</pre> | NA |
| Aktivieren Sie die HTTPS-Verbindung | <pre>cimconfig -s enableHttpsConnection=true -p</pre> | NA |
| Deaktivieren der HTTPS-Verbindung | <pre>cimconfig -s enableHttpsConnection=false -p</pre> | NA |
| Ändern Sie die HTTP-Portnummer | <pre>cimconfig -s httpPort=new_port_number -p</pre> | Standardmäßig ist die HTTP-Portnummer 5988. Wenn Sie sie in 5555 ändern möchten, würden Sie beispielsweise den folgenden Befehl eingeben: <pre>cimconfig -s httpPort=5555 -p</pre> |

| Aktion | Befehl | Weitere Informationen |
|---------------------------------|---|--|
| Ändern Sie die HTTPS-Portnummer | <pre>cimconfig -s httpsPort=<i>new_port_number</i> -p</pre> | <p>Standardmäßig ist die HTTP-Portnummer 5989. Wenn Sie sie in 5556 ändern möchten, würden Sie beispielsweise den folgenden Befehl eingeben:</p> <pre>cimconfig -s httpsPort=5556 -p</pre> |

3. Starten Sie den CIM-Server neu:

```
smis cimserver restart
```

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 | <pre>cimconfig -s logLevel=new_log_level -p</pre> | 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 | <pre>cimconfig -s logdir=new_log_directory -p Wenn der <i>new_log_directory</i> Enthält Leerzeichen. Sie müssen es in Anführungszeichen einschließen (<i>"new log directory"</i>).</pre> | Wenn Sie beispielsweise das Protokollverzeichnis in „serverlogs“ ändern möchten, würden Sie diesen Befehl eingeben: <pre>cimconfig -s logdir=serverlogs -p</pre> |

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 | <code>cimconfig -s traceComponents=<i>components</i> -p</code> |
| Geben Sie die Trace-Funktion an | <code>cimconfig -s traceFacility=<i>facility</i> -p</code> |
| Geben Sie den Speicherort der Trace-Datei an | <code>cimconfig -s traceFilePath=<i>path_name</i> -p</code> |
| Geben Sie die Trace-Ebene an | <code>cimconfig -s traceLevel=<i>level</i> -p</code> |

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 | <code>cimconfig -s enableAuditLog=true</code> |
| SMI-S-Audit-Protokollierung deaktivieren | <code>cimconfig -s enableAuditLog=false</code> |

Verwalten Sie die erweiterten Einstellungen für SMI-S Provider

Überblick

Sie können erweiterte Einstellungen für SMI-S Provider verwalten, z. B. das SMI-S-Cache-Aktualisierungsintervall, das ONTAPI-Timeout und die maximale Anzahl von Threads pro Nachrichtendienst-Warteschlange.

Geben Sie das Intervall für die automatische Cache-Aktualisierung von SMI-S Provider an

Standardmäßig ruft SMI-S Provider Informationen alle fünf Minuten (300 Sekunden) automatisch von Speichersystemen ab. Sie können das Intervall für die automatische Cache-Aktualisierung festlegen (`CACHE_REFRESH_SEC` Umgebungsvariable) auf einen Wert von 300 bis 86400 Sekunden (24 Stunden).

Bevor Sie beginnen

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

Über diese Aufgabe

Wenn Sie den Status des Storage-Systems jederzeit manuell aktualisieren möchten, können Sie das verwenden `smis refresh` Befehl.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Erstellen Sie eine System- oder Benutzerumgebvariable mit dem Namen `CACHE_REFRESH_SEC` Mit dem neuen Aktualisierungsintervall (in Sekunden).

Informationen zum Erstellen von Umgebungsvariablen finden Sie in der Windows-Dokumentation.

3. Starten Sie den CIM-Server neu:

```
smis cimserver restart
```

Geben Sie den konkreten Wert für die Einsatzdauer an

SMI-S Provider verfolgt den Fortschritt von asynchronen Operationen durch die Erstellung von *Concrete Jobs*. Sie können die konkrete Einsatzdauer von 60 Minuten (3600 Sekunden) auf einen Wert von 86400 Sekunden (24 Stunden) erhöhen.

Bevor Sie beginnen

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

Schritt

1. Erstellen Sie eine System- oder Benutzerumgebvariable mit dem Namen `JOB_LIFETIME_SEC` Mit dem neuen Lebenszeitwert (in Sekunden).

Informationen zum Erstellen von Umgebungsvariablen finden Sie in der Windows-Dokumentation.

Geben Sie den ONTAPI-Timeout-Wert an

SMI-S Provider macht ONTAP API (ONTAPI)-Aufrufe zu Storage-Systemen. Standardmäßig beträgt das ONTAPI-Timeout 300 Sekunden. Sie können das Timeout auf einen Wert von 60 bis 300 Sekunden einstellen.

Bevor Sie beginnen

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

Schritt

1. Erstellen Sie eine System- oder Benutzerumgebvariable mit dem Namen `ONTAPI_TIMEOUT_SEC` Mit dem neuen Timeout-Wert (in Sekunden).

Informationen zum Erstellen von Umgebungsvariablen finden Sie in der Windows-Dokumentation.

Geben Sie die maximale Anzahl von Threads pro Nachrichtendienstwarteschlange an

SMI-S Provider ermöglicht standardmäßig 80 Threads pro Nachrichtendienstwarteschlange. Sie können den maximalen Gewindewert als 1 bis 5000 festlegen. Eine Erhöhung der maximalen Anzahl von Threads kann sich auf die Leistung der SMI-S Provider-Maschine auswirken. Überlegen Sie daher genau, ob Sie diesen Wert erhöhen müssen.

Bevor Sie beginnen

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

Über diese Aufgabe

Wenn Ihre Trace-Datei viele Zeilen von `insufficient resources` Ausgabe: Sie müssen die Anzahl der Threads in Schritten von 500 erhöhen.

Wenn Sie die maximale Anzahl von Threads auf weniger als 20 einstellen, verwenden Sie die `cimcli -n root/ontap niall` Befehl, der Provider reagiert nicht mehr und gibt den aus `Insufficient threadpool` Nachricht in der Trace-Datei. In diesem Fall müssen Sie die Anzahl der Threads in Schritten von 500 erhöhen und dann den Provider neu starten.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Erstellen Sie eine System- oder Benutzerumgebvariable mit dem Namen

PEGASUS_MAX_THREADS_PER_SVC_QUEUE Mit dem neuen maximalen Gewindewert.

Informationen zum Erstellen von Umgebungsvariablen finden Sie in der Windows-Dokumentation.

3. Starten Sie den CIM-Server neu:

```
smis cimserver restart
```

Aktivieren oder deaktivieren Sie die Authentifizierung für NetApp SMI-S Provider

Standardmäßig ist die Authentifizierung für SMI-S Provider aktiviert. Wenn die Authentifizierung Fehler auf dem System verursacht, können Sie diese optional deaktivieren. Wenn die Authentifizierung deaktiviert wurde und Sie sie erneut aktivieren möchten, können Sie dies tun.

Bevor Sie beginnen

- Sie müssen bereits Anmeldedaten als Administrator besitzen.
- Sie müssen sich bereits als Administrator angemeldet haben.
- Alle Clients, einschließlich System Center Virtual Machine Manager (SCVMM), müssen mit dem Anbieter verbunden sein, der cimuser und cimpassword verwendet.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Legen Sie die Authentifizierung für SMI-S Provider fest:

| Aktion | Befehl |
|--|---|
| Authentifizierung aktivieren, wenn zuvor deaktiviert | <pre>cimconfig -p -s enableAuthentication=true</pre> |
| Authentifizierung deaktivieren | <pre>cimconfig -p -s enableAuthentication=false</pre> |

CIMOM verwendet keine Windows-Authentifizierung.

3. NetApp SMI-S Provider neu starten:

```
smis cimserver restart
```

Aktivieren Sie die Indikationen im SMI-S-Provider

Warnmeldungen, Dateikontingente und Lifecycle-Angaben sind standardmäßig deaktiviert. Sie können diese Indikationen aktivieren, indem Sie die Umgebungsvariable einstellen PEGASUS_DISABLE_INDICATIONS Bis false.

Bevor Sie beginnen

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

Über diese Aufgabe

Wenn `PEGASUS_DISABLE_INDICATIONS` Ist auf festgelegt `false`, Dann Warnung (`ONTAP_AlertIndication`), Dateisystemkontingente (`ONTAP_FSQuotaIndication`) Und Lifecycle-Indikationen sind für NetApp SMI-S Provider aktiviert.

Schritte

1. Greifen Sie auf NetApp SMI-S Provider zu.
2. Stellen Sie die ein `PEGASUS_DISABLE_INDICATIONS` Umgebungsvariable auf `false`.
3. Starten Sie den CIM-Server neu:

```
smis cimserver restart
```

SLP verwalten

Überblick

Der SLP-Dienst sendet WBEM-Dienste. Wenn der SLP-Dienst aktiviert ist, können Client-Anwendungen den CIMOM-Server ermitteln. Sie können die SLP-Konfigurationseinstellungen auch mit der festlegen `slp.conf` Datei:

Wenn der SLP-Dienst nicht bereits aktiviert ist, können Sie den SLP-Dienst mithilfe der starten `smis slpd start` Befehl. Um den SLP-Dienst zu beenden, verwenden Sie den `smis slpd stop` Befehl.

Legen Sie die Optionen für die SLP-Konfiguration fest

Sie können die bearbeiten `slp.conf` Konfigurationsdatei zum Verwalten des Service Location Protocol Daemon (SLPD) Service.

slp.conf Dateiverwaltung

Der `slp.conf` Die Konfigurationsdatei bietet zusätzliche Optionen, mit denen Sie einen Service-Location-Protokoll-Daemon (SLPD)-Server verwalten können.

Standort

`C:\Program Files (x86)\NetApp\smis\pegasus\cfg`

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Beschreibung

Der `slp.conf` Mit der Konfigurationsdatei können Sie die Anzahl der Schnittstellen ändern, die ein Host auf SLP-Anforderungen abhört, und die Anzahl der IP-Adressen, die ein Host für Multicasting verwendet.

Verwenden Sie einen Texteditor, um das zu öffnen `slp.conf`.

Parameter

- **interfaces**

Gibt die maximale Anzahl von IP-Adressen an, die ein Host für SLP-Anforderungen abhören kann.

- **multicast**

Gibt die maximale Anzahl von IP-Adressen an, die ein Host für Multicasting verwenden kann. Verwenden Sie diesen Parameter, wenn Sie Schnittstellen für SLP-Multicast-Verkehr auf multihomed Systemen konfigurieren.

- **BroadcastOnly**

Erzwingt die Verwendung der Broadcast-Option, anstatt die Multicast-Option zu verwenden, wenn Nachrichten über SLP gesendet werden.

- **securityEnabled**

Aktiviert die Sicherheit für empfangene URLs und Attributlisten.

Beispiel

Im Folgenden finden Sie ein gekürztes Beispiel für `slp.conf` Konfigurationsdatei:

```
#####  
# OpenSLP configuration file  
# Format and contents conform to specification in IETF RFC 2614 so  
the comments use the language of the RFC. In OpenSLP, SLPD  
operates as an SA and a DA. The SLP UA functionality is  
encapsulated by SLPLIB.  
#####  
  
#-----  
# Static Scope and DA Configuration  
#-----  
# This option is a comma delimited list of strings indicating the  
only scopes a UA or SA is allowed when making requests or  
registering or the scopes a DA must support. (default value is  
"DEFAULT");net.slp.useScopes = myScope1, myScope2, myScope3  
  
# Allows administrator to force UA and SA agents to use specific  
DAs. If this setting is not used dynamic DA discovery will be used  
to determine which DAs to use. (Default is to use dynamic DA  
discovery)
```

CIMOM-Befehle

Zimconfig

Sie können das verwenden `cimconfig` Befehl zum Konfigurieren von CIMOM-Einstellungen, z. B. Aktivieren und Deaktivieren von HTTP und HTTPS sowie Ändern der HTTP- und HTTPS-Port-Nummern. Nach Eingabe des `cimconfig` Befehl oder Erstellen einer Umgebungsvariable für den Konfigurationswert von NetApp SMI-S Provider müssen Sie den CIM-Server mithilfe der neu starten `smis cimserver restart` Befehl.

Syntax

```
cimconfig options
```

Standort

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

Berechtigungsebene

Administrator (Windows)

Optionen

- **-c**

Gibt an, dass die Konfigurationseinstellung für die aktuelle CIMOM-Konfiguration gilt.

- **-d**

Gibt an, dass die Konfigurationseinstellung für die Standard-CIMOM-Konfiguration gilt.

- **-g**

Ruft den Wert einer angegebenen Konfigurationseigenschaft ab.

- **-h, --help**

Zeigt die Hilfe für das an `cimconfig` Befehl.

- **-l**

Listet alle CIMOM-Konfigurationseigenschaften auf.

- **-p**

Gibt an, dass die Konfigurationseinstellung beim nächsten Start des CIM-Servers angewendet wird.

- **-s**

Legt den angegebenen Wert für die Konfigurationseigenschaft fest.

- **-U**

Setzt die Konfigurationseigenschaft auf den Standardwert zurück.

- **--Version**

Zeigt die Version des CIM-Servers an.

Beispiel

Ändern Sie die maximale Protokolldateigröße auf 15000 KB:

```
cimconfig -s maxLogFileSizeKBytes=15000
Current value for the property maxLogFileSizeKBytes is set to "15000" in
CIMServer.
smis cimserver restart
```


CIM-Benutzerbefehle

cimuser

Sie können das verwenden `cimuser` Befehl zum Hinzufügen, Entfernen, Löschen, Ändern und Auflisten von CIM-Serverbenutzern sowie zum Verwalten ihrer Passwörter.

Syntax

`cimuser options`

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Administrator (Windows)

Optionen

- **-A**

Fügt einen CIM-Benutzer hinzu.

- **-h, --help**

Zeigt die Hilfe für das an `cimuser` Befehl.

- **-l**

Listet CIM-Benutzer auf.

- **-m**

Ändert das Kennwort eines CIM-Benutzers. Das Passwort kann zwischen 4 und 32 Zeichen lang sein.

- **-n**

Erstellt ein neues Passwort für den angegebenen Benutzer. Das Passwort kann zwischen 4 und 32 Zeichen lang sein.

- **-r**

Entfernt einen angegebenen CIM-Benutzer.

- **-U**

Gibt einen CIM-Benutzernamen an.

- **--Version**

Zeigt die Version des CIM-Servers an.

- **-w**

Gibt das Passwort für den angegebenen Benutzer an.

Beispiel

Erstellen Sie einen CIM-Benutzer namens sydney mit einem Passwort von password1:

```
cimuser -a -u sydney -w password1  
User added successfully.
```

SMI-S Provider-Befehle

Überblick

Sie können das verwenden `smis` Befehle zum Verwalten von Storage-Systemen und zum Anzeigen von Informationen über den CIM-Objektmanager.

Hilfe ist für das verfügbar `smis` Befehl mit dem `-help` Option.

- **Smis -help**

Zeigt eine Befehlsübersicht an.

- **Smis -help Beispiele**

Zeigt Anwendungsbeispiele an.

- **Smis -help *subcommand***

Zeigt die Hilfe für den angegebenen Unterbefehl an.

Der Standard-Timeout-Wert für das `sbis`-Werkzeug beträgt 180 Sekunden.

smis hinzufügen

Der `smis add` Befehl fügt ein Speichersystem mit einer HTTP-Verbindung zu Ihrer Konfiguration hinzu, damit Sie das Gerät verwalten und überwachen können. Sofern dies nicht notwendig ist, sollten Sie verwenden `smis addsecure` Statt `smis add`.

Syntax

```
smis add
```

```
storage_sys storage_sys_user+ [-t {http | https}]
```



Betriebssysteme verwenden andere Sprachen als die USA Englisch kann das nicht verwenden `add` Befehl.

Standort

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

Berechtigungsebene

Administrator (Windows)

Parameter

- ***storage_sys***

Name oder IP-Adresse des Speichersystems, das Sie hinzufügen

Wenn Sie die IP-Adresse angeben, können Sie IPv4 oder IPv6 verwenden. Beispielsweise werden sowohl komprimierte als auch vollständige IPv6-Empfänger unterstützt

1001:0002:0000:0000:0000:0000:0003:0004 Oder **1001:2::3:4**.

- ***storage_sys_user***

Benutzername des Administrators, der das Hinzufügen des Speichersystems verwaltet

- ***storage_sys_pwd***

Optional: Kennwort des Administrators, der das Speichersystem verwaltet, das Sie hinzufügen

Verwenden Sie diesen Parameter nicht aus Sicherheitsgründen als Best Practice. Dieser Parameter wird nur zur Automatisierung und Abwärtskompatibilität bereitgestellt.

- ***[-t {http | https}]***

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Storage-System-Agent und Agent-Client-Protokoll

Der `smis add` Und `smis addsecure` Befehle bestimmen das zwischen dem Speichersystem und dem Provider verwendete Protokoll. Der `[-t {http | https}]` Parameter bestimmt das Protokoll, das zwischen dem Provider und dem Client verwendet wird.

Der `smis addsecure` Befehl und das `[-t {https}]` Der Parameter stellt eine Verbindung über die SSL-Verschlüsselung her, und unverschlüsselter Datenverkehr ist nicht zulässig. Der `smis add` Befehl und das `[-t {http}]` Der Parameter stellt eine Verbindung ohne Verwendung der SSL-Verschlüsselung her, und unverschlüsselter Datenverkehr ist zulässig.

Vor dem Deaktivieren von SSL-verschlüsselten Verbindungen sollten Sie die Sicherheitsanforderungen Ihrer Umgebung berücksichtigen.

Beispiel

Fügen Sie ein Speichersystem mit IPv4 mit einer IP-Adresse von 10.32.1.4 über HTTP hinzu:

```
smis add 10.32.1.4 user2
```

Es wird eine Bestätigungsmeldung angezeigt, dass das Speichersystem erfolgreich hinzugefügt wurde. Wenn ein Fehler aufgetreten ist, wird eine Fehlermeldung angezeigt.

Beispiel

Fügen Sie ein Speichersystem mit IPv6 über HTTP hinzu:

```
smis add 1001:0002:0000:0000:0000:0000:0003:0004 user2  
smis add 1001:2::3:4 user2
```

Es wird eine Bestätigungsmeldung angezeigt, dass das Speichersystem erfolgreich hinzugefügt wurde. Wenn ein Fehler aufgetreten ist, wird eine Fehlermeldung angezeigt.

Beispiel

Fügen Sie ein Speichersystem mit einer IP-Adresse von 10.32.1.4 über HTTP auf einem nicht-englischsprachigen System hinzu:

```
cimcli -n root/ontap ci ontap_filerdata hostname="10.32.1.4"  
username="vsadmin" password="PasSw0Rd" port=80 comMechanism="HTTP"  
--timeout 180
```

smis addSecure

Der `smis addsecure` Befehl fügt ein Speichersystem mit einer HTTPS-Verbindung zu Ihrer Konfiguration hinzu, damit Sie das Gerät verwalten und überwachen können. Sofern dies nicht notwendig ist, sollten Sie verwenden `smis addsecure` Statt `smis add`.

Syntax

```
smis addsecure
```

```
storage_sys storage_sys_user+ [-t {http | https}]
```



Betriebssysteme verwenden andere Sprachen als die USA Englisch kann das nicht verwenden `addsecure` Befehl.

Standort

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

Berechtigungsebene

Administrator (Windows)

Parameter

- ***storage_sys***

Name oder IP-Adresse des Speichersystems, das Sie hinzufügen

Wenn Sie die IP-Adresse angeben, können Sie IPv4 oder IPv6 verwenden. Beispielsweise werden sowohl komprimierte als auch vollständige IPv6-Empfänger unterstützt

1001:0002:0000:0000:0000:0000:0003:0004 Oder 1001:2::3:4.

- ***storage_sys_user***

Benutzername des Administrators, der das Hinzufügen des Speichersystems verwaltet

- ***storage_sys_pwd***

Optional: Kennwort des Administrators, der das Speichersystem verwaltet, das Sie hinzufügen

Verwenden Sie diesen Parameter nicht aus Sicherheitsgründen als Best Practice. Dieser Parameter wird nur zur Automatisierung und Abwärtskompatibilität bereitgestellt.

- [-t {http | https}]

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Storage-System-Agent und Agent-Client-Protokoll

Der `smis add` und `smis addsecure` Befehle bestimmen das zwischen dem Speichersystem und dem Provider verwendete Protokoll. Der [-t {http | https}] Parameter bestimmt das Protokoll, das zwischen dem Provider und dem Client verwendet wird.

Der `smis addsecure` Befehl und das [-t {https}] Der Parameter stellt eine Verbindung über die SSL-Verschlüsselung her, und unverschlüsselter Datenverkehr ist nicht zulässig. Der `smis add` Befehl und das [-t {http}] Der Parameter stellt eine Verbindung ohne Verwendung der SSL-Verschlüsselung her, und unverschlüsselter Datenverkehr ist zulässig.

Vor dem Deaktivieren von SSL-verschlüsselten Verbindungen sollten Sie die Sicherheitsanforderungen Ihrer Umgebung berücksichtigen.

Beispiel

Fügen Sie ein Speichersystem mit IPv4 mit einer IP-Adresse von 10.32.1.4 über HTTPS hinzu:

```
smis addsecure 10.32.1.4 user2 password2
```

Es wird eine Bestätigungsmeldung angezeigt, dass das Speichersystem erfolgreich hinzugefügt wurde. Wenn ein Fehler aufgetreten ist, wird eine Fehlermeldung angezeigt.

Beispiel

Fügen Sie ein Speichersystem mit IPv6 über HTTPS hinzu:

```
smis addsecure 1001:0002:0000:0000:0000:0000:0003:0004 user2 password2  
smis addsecure 1001:2::3:4 user2 password2
```

Es wird eine Bestätigungsmeldung angezeigt, dass das Speichersystem erfolgreich hinzugefügt wurde. Wenn ein Fehler aufgetreten ist, wird eine Fehlermeldung angezeigt.

Beispiel

Fügen Sie ein Speichersystem mit einer IP-Adresse von 10.32.1.4 über HTTPS auf einem nicht-englischsprachigen System hinzu:

```
cimcli -n root/ontap ci ontap_filerdata hostname="10.32.1.4"  
username="vsadmin" password="PasSw0Rd" port=443 comMechanism="HTTPS"  
--timeout 180
```

smis cimom

Der `smis cimom` Der Befehl beschreibt den CIM-Objektmanager.

Syntax

```
smis cimom [-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- [-t {http | https}]

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis cimom` Befehl und seine Ausgabe:

```
smis cimom
PG_ObjectManager.CreationClassName="PG_ObjectManager",
Name="PG:1297121114307-10-229-89-243",
SystemCreationClassName="PG_ComputerSystem",SystemName="10.1.2.3"
```

smis Cimserver

Der `smis cimserver` Befehl startet, stoppt, startet neu oder ruft den Status des CIM-Servers ab.

Syntax

```
smis cimserver
```

```
{start | stop | restart | status}
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Administrator (Windows)

Parameter

- **Start**

Starten Sie den CIM-Server.

- **Stopp**

Beenden Sie den CIM-Server.

- **Neustart**

Starten Sie den CIM-Server neu.

- **Status**

Abrufen des Status des CIM-Servers.

smis-Klasse

Der `smis class` Command listet Informationen über eine bestimmte Klasse oder alle Klassen auf.

Syntax

```
smis class
```

```
name_space {niall | {ei | ni | gi | gc} class_name}} [-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- **name_space**

Namespace, der vom CIMOM unterstützt wird

- **niall**

Alle Instanznamen auflisten

- **Ei**

Instanzen für eine Klasse auflisten

- *** Ni***

Instanznamen für eine Klasse aufzählen

- **gi**

Abrufen von Instanzen für eine Klasse

- **gc**

Klasse für einen Klassennamen abrufen

- **class_name**

Name der Klasse, für die Sie Informationen wünschen

- **[-t {http | https}]**

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis class` Befehl und seine gekürzte Ausgabe:

```
smis class root/ontap gi CIM_StorageVolume
1:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJdC-
mN5",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:01350
27815"
2:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJcmzphT",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
3:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJc30t26",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
4:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJcSgbiT",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
5:
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID="P3Lf
GJcSgrA9",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:
0135027815"
```

smis config show

Der `smis config show` Der Befehl listet die aktuellen Konfigurationsinformationen für den CIM-Server auf.

Syntax

```
smis config show
```

Standort

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

Berechtigungsebene

Administrator (Windows)

Beispiel

Der `smis config show` Und ihre Ausgabe:

```
smis config show
slp:
Current value: true

tracelevel:
Current value: 4

traceComponents:
Current value: XmlIO,Thread, IndicationGeneration, DiscardedData,
CMPIProvider, LogMessages, ProviderManager, SSL, Authentication,
Authorization

traceFilePath:
Current value: traces/cimserver.trc

enableAuditLog:
Current value: true

logLevel:
Current value: WARNING

sslKeyFilePath:
Current value: cimom.key

sslCertificateFilePath:
Current value: cimom.cert

passwordFilePath:
Current value: cimserver.passwd

enableHttpConnection:
Current value: true

enableHttpsConnection:
Current value: true

httpPort:
Current value: 5988

httpsPort:
Current value: 5989

enableAuthentication:
Current value: true
```

smis crp

Der `smis crp` Befehl beschreibt die von NetApp SMI-S Provider unterstützten CIM-registrierten Profile, einschließlich NetApp SMI-S Provider-Profile.

Syntax

`smis crp`

`[-t {http | https}]`

Standort

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis crp` Befehl und seine Ausgabe:

```
smis crp

PG_RegisteredProfile.InstanceID="SNIA:Profile Registration:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.5.0"
PG_RegisteredProfile.InstanceID="SNIA:SMI-S:1.6.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.4.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.5.0"
PG_RegisteredProfile.InstanceID="SNIA:Server:1.6.0"
PG_RegisteredProfile.InstanceID="DMTF:Profile Registration:1.4.0"
PG_RegisteredProfile.InstanceID="DMTF:Indications:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Object Manager Adapter:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Software:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.5.0"
```

ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Multiple Computer System:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Access Points:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Target Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server Performance:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server Performance:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Health:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Storage:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File System Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Filesystem Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Server Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem Quotas:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Location:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:NAS Network Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Capacity Utilization:1.4.0"

smis crsp

Der `smis crsp` Befehl beschreibt von NetApp SMI-S Provider unterstützte CIM-registrierte Unterprofile, einschließlich NetApp SMI-S Provider-Unterprofile.

Syntax

`smis crsp`

`[-t {http | https}]`

Standort

`C:\Program Files (x86)\NetApp\smis\pegasus\bin`

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis crsp` Befehl und seine gekürzte Ausgabe:

```
smis crsp

PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Indication:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.4.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.5.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Software:1.6.0"
PG_RegisteredSubProfile.InstanceID="SNIA:Object Manager Adapter:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:iSCSI Target Ports:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Software:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Disk Drive Lite:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Multiple Computer
System:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Access Points:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Target Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FC Initiator Ports:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.6.0"
```

```
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Masking and Mapping:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Extent Composition:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server
Performance:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Server
Performance:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Physical Package:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Block Services:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Health:1.2.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Storage:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export
Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Export
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File System
Manipulation:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Filesystem
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:File Server
Manipulation:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:FileSystem Quotas:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Job Control:1.3.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Location:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:NAS Network Port:1.4.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.5.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Replication Services:1.6.0"
ONTAP_RegisteredSubProfile.InstanceID="ONTAP:Capacity Utilization:1.4.0"
```

smis löschen

Der `smis delete` Befehl löscht ein Storage-System.

Syntax

```
smis delete
```

```
storage_sys
```

```
[-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Administrator (Windows)

Parameter

- ***storage_sys***

Name oder die IP-Adresse des Speichersystems, das Sie hinzufügen

- ***[-t {http | https}]***

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Löschen Sie ein Speichersystem mit der Bezeichnung Management-1:

```
smis delete mgt-1
```

Wenn keine Fehlermeldung angezeigt wird, wurde das Speichersystem erfolgreich gelöscht.

smis-Festplatten

Der `smis disks` Mit Befehl werden Festplatteninformationen für Storage-Systeme angezeigt. `smis disks` Nur bei Nutzung mit Data ONTAP 7-Mode Controllern.

Syntax

smis-Festplatten

```
[-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- ***[-t {http | https}]***

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis disks` Befehl und seine gekürzte Ausgabe:

```
smis disks
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.3",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.5",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.7",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.6",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.1",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
ONTAP_DiskExtent.CreationClassName="ONTAP_DiskExtent",DeviceID="0c.00.8",SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:0135027815"
```

smis-Exporte

Der `smis exports` Mit dem Befehl werden NAS-Exporte (Network Attached Storage) für Speichersysteme angezeigt.

Syntax

```
smis-Exporte [-t {http | https}]
```

Standort

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- [-t {http | https}]

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis exports` Befehl und seine Ausgabe:


```

smis exports
ONTAP_LogicalFile.CreationClassName="ONTAP_LogicalFile",CSCreationClassNam
e="ONTAP_StorageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="/vol/NAS_vol/Tes
tCFS0528",Name="/vol/NAS_vol/TestCFS0528"
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Sto
rageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="nilesh_vserver_r
ootvol",Id="nilesh_vserver_rootvol:0",Name=""
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Sto
rageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="NAS_vol",Id="NAS
_vol:0",Name=""
ONTAP_Qtree.CreationClassName="ONTAP_Qtree",CSCreationClassName="ONTAP_Sto
rageSystem",CSName="ONTAP:68f6b3c0-923a-11e2-a856-
123478563412",FSCreationClassName="ONTAP_LocalFS",FSName="NAS_vol",Id="NAS
_vol:1",Name=""

```

smis-Initiatoren

Der `smis initiators` Mit dem Befehl werden Informationen zu Fibre Channel- und iSCSI-Ports für Speichersysteme angezeigt.

Syntax

smis-Initiatoren

```
[-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis initiators` Befehl und seine gekürzte Ausgabe:

```
smis initiators
ONTAP_StorageHardwareID.InstanceID="ONTAP:0084259609:iqn.1991-
05.com.microsoft:sf-tpc1"
ONTAP_StorageHardwareID.InstanceID="ONTAP:0084259609:21:00:00:e0:8b:86:f2:
89"
ONTAP_StorageHardwareID.InstanceID="ONTAP:0084259609:iqn.1991-
05.com.microsoft:went2k3x32-01"
```

smis lizenziert

Der `smis licensed` Mit dem Befehl werden die lizenzierten Funktionen für Storage-Systeme aufgeführt.

Syntax

`smis lizenziert`

```
[-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis licensed` Befehl und seine gekürzte Ausgabe:

```
smis licensed
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:cifs"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:cluster"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:fc"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:iscsi"
ONTAP_SoftwareIdentity.InstanceID="ONTAP:0084259609:nfs"
```

smis-Liste

Der `smis list` Befehl zeigt Storage-Systeme an, die hinzugefügt werden.

Syntax

smis-Liste

`[-t {http | https}]`

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis list` Befehl und seine Ausgabe:

```
smis list
ONTAP_FilerData.hostName="10.16.180.122",port=80
```

smis luns

Der `smis luns` Mit Befehl werden LUN-Informationen für Storage-Systeme angezeigt.

Syntax

`smis luns`

`[-t {http | https}]`

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis luns` Befehl und seine gekürzte Ausgabe:

```
smis luns
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="ef805c0d-5269-47c6-ba0fd9cdbf5e2515",
SystemCreationClassName="ONTAP_StorageSystem",SystemName="ONTAP:68f6b3c0-923a-11e2-a856-123478563412"
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="f81cb3bf-2f16-467c-8e30-88bae415ab05",SystemCreationClassName="ONT
AP_StorageSystem",SystemName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412"
ONTAP_StorageVolume.CreationClassName="ONTAP_StorageVolume",DeviceID
="684f5fb9-0fdd-4b97-8678-188774bdcd0",SystemCreationClassName="ONT
AP_StorageSystem",SystemName="ONTAP:68f6b3c0-923a-11e2-
a856-123478563412"
```

smis Namespaces

Der `smis namespaces` Befehl listet die registrierten Namespaces für das CIMOM auf.

Syntax

```
smis Namespaces
```

```
[-t {http | https}]
```

Standort

```
C:\Program Files (x86)\NetApp\smis\pegasus\bin
```

- Windows: C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis namespaces` Befehl und seine gekürzte Ausgabe:

```
smis namespaces
interop
root/ontap
```

smis-Pools

Der `smis pools` Befehl listet die Speicherpools für Speichersysteme auf.

Syntax

```
smis pools
```

```
[-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- `[-t {http | https}]`

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis pools` Befehl und seine gekürzte Ausgabe:

```
smis pools
ONTAP_ConcretePool.InstanceID="ONTAP:0084259609:d46de7f0-3925-11df-8516-
00a0980558ea"
ONTAP_ConcretePool.InstanceID="ONTAP:0084259609:51927ab0-28b5-11df-92b2-
00a0980558ea"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Spare"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Other"
ONTAP_DiskPrimordialPool.InstanceID="ONTAP:0084259609:Present"
```

smis-Aktualisierung

Standardmäßig ruft SMI-S Provider alle 60 Minuten (3600 Sekunden) automatisch Informationen aus den Speichersystemen ab. Sie können das verwenden `smis refresh` Befehl zum manuellen Aktualisieren eines bestimmten Storage-Systems.

Syntax

```
smis refresh storage_system_ip
```

```
[-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- ***storage_system_ip***

Aktualisiert ein bestimmtes Storage-System.

- ***[-t {http | https}]***

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis refresh` Befehl und seine Ausgabe:

```
smis refresh 10.32.1.4
Return Value= 0
```

smis slpd

Der `smis slpd` Befehl startet oder stoppt den SLP-Daemon.

Syntax

```
smis slpd
```

```
{start | stop}
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Administrator (Windows)

Beispiel

Starten Sie den SLP-Daemon:

```
smis slpd start
SLPD started.
```

Beenden Sie den SLP-Daemon:

```
smis slpd stop
SLPD (15564) was successfully stopped.
```

smis-Version

Der `smis version` Mit dem Befehl wird die Version des NetApp SMI-S Provider angezeigt.

Syntax

```
smis version
```

```
[-t {http | https}]
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- [-t {http | https}]

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis version` Befehl und seine Ausgabe:

```
smis version
ONTAP_SMIAGENTSoftware.InstanceID="ONTAP5.2.2"
```

smis Volumes

Der `smis volumes` Mit dem Befehl werden die herkömmlichen und flexiblen Volumes für Storage-Systeme aufgelistet.

Syntax

```
smis volumes
```

```
[-t {http | https}]
```



Für Clustered Data ONTAP müssen Sie den verwenden `smis pools` Befehl anstelle des `smis volumes` Befehl.

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- [-t {http | https}]

Zu verwendenden Protokoll: HTTPS (Standard) oder HTTP

Beispiel

Der `smis volumes` Befehl und seine gekürzte Ausgabe:

```
smis volumes
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="d46de7f0
-3925-
11df-8516-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="397cd140
-3a45-
11df-8516-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="69c472c0
-4b27-
11df-8517-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
ONTAP_LogicalDisk.CreationClassName="ONTAP_LogicalDisk",DeviceID="6c7ea0b0
-3927-
11df-8516-
00a0980558ea",SystemCreationClassName="ONTAP_StorageSystem",SystemName
="ONTAP:0084259609"
```


SLP-Befehle

Slptool

Sie können das verwenden `slptool` Befehl zum Anzeigen von Informationen zu WBEM-Diensten.

Syntax

```
slptool [options] subcommand
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Administrator (Windows)

Optionen

- **-i**

Gibt eine oder mehrere Schnittstellen an.

- **-l**

Gibt ein Sprachkennzeichnung an.

- **-s**

Gibt eine Liste der Bereiche an (getrennt durch Kommas).

- **-U**

Gibt eine Schnittstelle an.

- **-V**

Zeigt die Version von an `slptool` Und OpenSLP.

Slptool Findattr

Der `slptool findattr` Befehl sucht WBEM-Attribute, die in einem Netzwerk ausgeführt werden.

Syntax

```
slptool findattr service
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- **service**

Gibt den Servicetyp an.

Beispiel

Der `slptool findattrs` Befehl und seine gekürzte Ausgabe:

```
slptool findattrs service:wbem
(template-url-syntax=http://10.229.90.227:5988), (service-id=PG:10-229-90-227), (service-hi-name=Pegasus), (service-hi-description=Pegasus CIM Server Version 2.12.0), (template-type=wbem), (template-version=1.0), (template-description=This template describes the attributes used for advertising Pegasus CIM Servers.), (InteropSchemaNamespace=interop), (FunctionalProfilesSupported=Basic Read,Basic Write,Schema Manipulation,Instance Manipulation,Association Traversal,Qualifier Declaration,Indications), (MultipleOperationsSupported=TRUE), (AuthenticationMechanismsSupported=Basic), (AuthenticationMechanismDescriptions=Basic), (CommunicationMechanism=CIM-XML), (ProtocolVersion=1.0), (Namespace=root/PG_Internal,interop,root/ontap,root), (RegisteredProfilesSupported=SNIA:Server,SNIA:Array,SNIA:NAS Head,SNIA:Software,SNIA:Profile Registration,SNIA:SCNAS,SNIA:Storage Virtualizer,SNIA:Indication)
```

Slptool findsrvs

Der `slptool findsrvs` Befehl sucht WBEM-Dienste, die in einem Netzwerk ausgeführt werden.

Syntax

```
slptool findsrvs service
```

Standort

C:\Program Files (x86)\NetApp\smis\pegasus\bin

Berechtigungsebene

Ein Benutzer mit einem gültigen Benutzernamen und Kennwort

Parameter

- **service**

Gibt den Servicetyp an.

Beispiel

Der `slptool findsrvs` Befehl und seine Ausgabe:

```
slptool findsrvs service:wbem
service:wbem:http://10.60.167.143:5988,65535
service:wbem:http://10.60.167.246:5988,65535
service:wbem:https://10.60.167.143:5989,65535
service:wbem:https://10.60.167.246:5989,65535
service:wbem:http://10.60.167.151:5988,65535
service:wbem:http://10.60.167.250:5988,65535
service:wbem:https://10.60.167.151:5989,65535
service:wbem:https://10.60.167.250:5989,65535
service:wbem:http://10.60.167.141:5988,65535
service:wbem:https://10.60.167.141:5989,65535
service:wbem:http://10.60.167.147:5988,65535
service:wbem:https://10.60.167.147:5989,65535
service:wbem:http://10.60.167.139:5988,65535
service:wbem:http://[fe80::7804:75ad:ab59:28c]:5988,65535
service:wbem:http://[fe80::3cb1:12da:f5c3:5874]:5988,65535
service:wbem:http://[2001::4137:9e76:3cb1:12da:f5c3:5874]:5988,65535
service:wbem:https://10.60.167.139:5989,65535
service:wbem:https://[fe80::7804:75ad:ab59:28c]:5989,65535
service:wbem:https://[fe80::3cb1:12da:f5c3:5874]:5989,65535
service:wbem:https://[2001::4137:9e76:3cb1:12da:f5c3:5874]:5989,65535
```

Fehler bei SMI-S Provider beheben

Überblick

Wenn bei einem Problem mit NetApp SMI-S Provider ein Problem auftritt, sollten Sie alle Fehlermeldungen verwenden, die Sie erhalten, um Hilfe bei der Fehlerbehebung zu erhalten.

Fehler beim Zugriff verweigert

- **Nachricht**

```
Access is denied.
```

- **Beschreibung**

Diese Meldung tritt in zwei möglichen Situationen auf:

- Wenn Sie beim Zugriff auf SMI-S Provider nicht als Administrator über die Verknüpfung im Startmenü angemeldet sind
- Wenn das Verzeichnis SMI-S Provider nicht auf `C:\Program Files (x86)\NetApp\smis\pegasus\bin` weist

- **Korrekturmaßnahmen**

Führen Sie die Aktion aus, die der Situation entspricht:

- Melden Sie sich mit Berechtigungen auf Administratorebene an und öffnen Sie SMI-S Provider im Startmenü erneut, oder klicken Sie mit der rechten Maustaste, und wählen Sie **als Administrator ausführen** aus.
- Melden Sie sich mit Berechtigungen auf Administratorebene an, und ändern Sie das Verzeichnis manuell in `C:\Program Files (x86)\NetApp\smis\pegasus\bin`.

Mögliche Fehler beim Laden von gemeinsam genutzten Bibliotheken

- **Nachrichten**

```
Error while loading shared libraries: libssl.so 1.0.0: cannot open shared object file: No such file or directory.
```

Der `smis cimserver` Der Status zeigt an, dass der Cimserver ordnungsgemäß ausgeführt wird, aber alle anderen `/usr/netapp/smis/pegasus/bin/cim` Befehle zeigen verschiedene Fehlermeldungen an.

Sie können beispielsweise die Nachricht erhalten `cimserver not running` Bei Ausführung des `cimserver`, Oder Sie können die Nachricht erhalten `/usr/netapp/smis/pegasus/bin/ cimcli: symbol lookup error: /usr/netapp/smis/pegasus/bin/cimcli: undefined symbol: _ZN7Pegasus16StringConversion21decimalStringToUint64EPKcRy` Bei der Ausführung von `Cimcli`. Diese Beispiele sind nicht All-Inclusive-Angebote.

- **Beschreibung**

Diese Meldung (und ähnliche Meldungen) tritt auf, wenn der angezeigte Pfad `LD_LIBRARY_PATH` Die Umgebung ist nicht auf das Installationsverzeichnis festgelegt.

- **Korrekturmaßnahmen**

Geben Sie einen der folgenden Befehle ein, um den festzulegen `LD_LIBRARY_PATH` Umgebungsvariable zum Installationsverzeichnis:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/netapp/smis/pegasus/lib
```

```
setenv LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/netapp/smis/pegasus/lib
```

Verbindung abgelehnt

- **Nachricht**

```
Connection refused
```

- **Ursache**

Der CIM-Server wurde nicht gestartet.

- **Korrekturmaßnahmen**

Navigieren Sie zum `bin` Verzeichnis in dem Verzeichnis, in dem Sie NetApp SMI-S Provider installiert haben, und geben Sie den folgenden Befehl ein, um zu überprüfen, ob der CIM-Server gestartet wurde:

```
smis cimserver status
```

Wenn der CIM-Server nicht ausgeführt wird, geben Sie den folgenden Befehl ein:

```
smis cimserver start
```

Filer Rückgabe: Kein ONTAP-Element als Antwort

- **Nachricht**

```
Filer return: No ontap element in response.
```

- **Beschreibung**

Diese Nachricht tritt auf, wenn die ONTAPI API API-API-Auszeit. Die standardmäßige ONTAPI API-Zeitüberschreitung beträgt 60 Sekunden, was in einigen Szenarien zu kurz sein kann.

- **Korrekturmaßnahmen**

Ändern Sie die ONTAPI-API-Zeitüberschreitung auf einen Wert größer als 60 Sekunden, indem Sie die Umgebungsvariable einstellen `ONTAPI_TIMEOUT_SEC`, Und starten Sie dann SMI-S Provider neu.

Klon-/Snapshot-Vorgänge sind nicht zulässig

- **Nachricht**

Clone/Snapshot operations are not allowed while LUN clone split operations are going on in the volume. Please wait for some time and try again.

- **Beschreibung**

Dieser Fehler tritt auf, wenn Sie versuchen, Snapshot-Vorgänge während einer LUN-Klonverteilung auszuführen. Snapshot Vorgänge auf einem Volume, auf dem eine LUN aufgeteilt wird, können nicht durchgeführt werden, wenn im Hintergrund die LUN-Klonabteilung ausgeführt wird.

- **Korrekturmaßnahmen**

Versuchen Sie, Ihre Snapshot-Vorgänge durchzuführen, nachdem die LUN aufgeteilt ist.

Warnung 26130

Nachricht

Warning (26130) Storage pool has been allocated to host group where none of hosts in host group has access to storage array.

Beschreibung

Dieser Fehler tritt auf, wenn Sie Storage-Kapazität zuweisen und Hosts, die sich in einer Host-Gruppe befinden, einen Arrayzugriff gewähren. Mit dieser Warnung ist es unmöglich, Virtual Machines auf den Storage-Systemen zu platzieren.

Korrekturmaßnahme

1. Fügen Sie auf jeder Host-Maschine der iSCSI-Initiator-Anwendung die IP-Adresse jedes Speichersystems hinzu.
2. Erstellen Sie bei Bedarf auf jedem Storage-System für jede Host-Maschine eine eindeutige igroup, die mit dem richtigen iSCSI-Node-Namen von der entsprechenden Host-Maschine verknüpft ist.
3. Öffnen Sie für jeden mit Data ONTAP verbundenen Host-Rechner die MPIO-Anwendung, und fügen Sie die folgende Hardware-ID hinzu:
 - Bei Clustered Data ONTAP finden Sie hier **NETAPP LUN C-Mode**.
4. Starten Sie die Hostcomputer neu.
5. Entfernen Sie den Anbieter.
6. Stellen Sie den Speicherpool wieder ein.

HostAgentAccessDenied (ID: 26263)

Nachricht

Registration of storage provider *smis_provider_machine* for user name failed from

`SCVMM_ (machine) with error code HostAgentAccessDenied. Specify valid provider, port and user credentials for storage discovery. ID: 26263`

Beschreibung

Diese Meldung tritt auf, wenn ein Benutzer in SCVMM zur Verbindung mit SMI-S Provider angegeben wird, jedoch nicht zum SMIS Trust Store gehört.

Um die Kommunikation zwischen SCVMM und SMI-S Provider zu ermöglichen, muss ein gültiger CIM-Benutzer (lokaler Administrator-Benutzer oder Domain-Benutzer der Gruppe Lokale Administratoren) zum SMIS Trust Store mithilfe der hinzugefügt werden `cimuser` Befehl.

Korrekturmaßnahme

Fügen Sie den lokalen Administrator-Benutzer (auf dem SMI-S Provider-Rechner) zur CIM-Server-Datenbank mithilfe des hinzu `cimuser` Befehl: `cimuser -a -u admin user -w password`. Anschließend müssen Sie diesen administrativen Benutzer verwenden, wenn Sie NetApp SMI-S Provider zu SCVMM hinzufügen.

Wenn der Domänencontroller zu lang dauert, um den Domain-Benutzer zu authentifizieren, müssen Sie den lokalen Administrator-Benutzer auf dem SMI-S Provider-Rechner verwenden.

Wenn der Fehler weiterhin besteht, können Sie die Authentifizierung im SMI-S-Provider deaktivieren.

Verbindung mit localhost:5988 nicht möglich

- **Nachricht**

```
Cannot connect to localhost:5988. Connection failed. Trying to connect to localhost:5988
```

- **Beschreibung**

Diese Meldung wird angezeigt, wenn HTTPS-Verbindungen deaktiviert sind oder der HTTPS-Port nicht auf 5988 eingestellt ist, oder wenn der Provider nicht mehr funktioniert und sich im hängenden Zustand befindet.

- **Korrekturmaßnahmen**

Überprüfen Sie, ob die Werte von `enableHttpConnection` Und `httpsPort` Korrekt sind:

```
cimconfig -g enableHttpConnection
```

```
cimconfig -g enableHttpsConnection
```

```
cimconfig -g httpPort
```

```
cimconfig -g httpsPort
```

Wenn `enableHttpConnection` Oder `enableHttpsConnection` Ist nicht auf festgelegt ``true``Geben Sie die folgenden Befehle ein:

```
cimconfig -s enableHttpConnection -p
```

```
smis cimserver restart
```

Wenn `httpPort` ist nicht auf 5988 festgelegt. Geben Sie die folgenden Befehle ein:

```
cimconfig -s httpPort=5988 -p
```

```
smis cimserver restart
```

Wenn der Provider nicht mehr funktioniert und sich weiterhin im hängenden Zustand befindet, öffnen Sie den Task-Manager, beenden Sie den Prozess und starten Sie dann den Provider neu.

Verbindung mit localhost:5989 nicht möglich

- **Nachricht**

```
Cannot connect to localhost:5989. Connection failed. Trying to connect to localhost:5989
```

- **Beschreibung**

Diese Meldung wird angezeigt, wenn HTTPS-Verbindungen deaktiviert sind oder der HTTPS-Port nicht auf 5989 eingestellt ist, oder wenn der Provider nicht mehr funktioniert und sich im hängenden Zustand befindet.

- **Korrekturmaßnahmen**

Überprüfen Sie, ob die Werte von `enableHttpsConnection` Und `httpsPort` Korrekt sind:

```
cimconfig -g enableHttpsConnection
```

```
cimconfig -g httpsPort
```

Wenn `enableHttpsConnection` ist nicht auf „true“ festgelegt, geben Sie die folgenden Befehle ein:

```
cimconfig -s enableHttpsConnection -p
```

```
smis cimserver restart
```

Wenn `httpsPort` ist nicht auf 5989 festgelegt. Geben Sie die folgenden Befehle ein:

```
cimconfig -s httpsPort=5989 -p
```

```
smis cimserver restart
```

Wenn der Provider nicht mehr funktioniert und sich weiterhin im hängenden Zustand befindet, öffnen Sie den Task-Manager, beenden Sie den Prozess und starten Sie dann den Provider neu.

SMI-S Provider stürzt in Windows ab

- **Ausgabe**

SMI-S Provider stürzt in Windows ab.

- **Ursache**

Dieses Problem tritt aus verschiedenen Gründen auf, die in Dateien dokumentiert sind, die zum Zeitpunkt des Absturzes generiert wurden.

- **Korrekturmaßnahmen**

Starten Sie den Provider neu und senden Sie die folgenden Informationen an den technischen Support, um weitere Analysen durchzuführen:

- Dump-Datei aus dem C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\logs Verzeichnis
- Log-Dateien aus dem C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\logs Verzeichnis
- Verfolgen von Dateien aus dem C:\Program Files (x86)\NetApp\smis\pegasus\pegasus\traces Verzeichnis

Ähnliche Meldungen werden auch in der Trace-Datei angezeigt:

```
23-May-2013 20:46:36.874 INFO cimserver: createMiniDump: SMI-S Agent has crashed, attempting to generate a dump file
```

```
23-May-2013 20:46:37.14 INFO cimserver: createMiniDump: Process dumped to C:\Program Files (x86)\netapp\smis\pegasus\logs\SMI-S Agent-8be55da-2011_05_23-20_46_36.dmp
```

- Der Dateien version.txt Und cimserver_current.conf Von C:\Program Files (x86)\NetApp\smis\pegasus\pegasus Verzeichnis

Geben Sie Passwörter mit Sonderzeichen ein

- **Ausgabe**

In englischen Betriebssystemen mit einem Passwort, das Sonderzeichen mit dem enthält smis Befehl funktioniert nicht in einer Windows-Umgebung. Dieses Problem wurde bei nicht-englischen Betriebssystemen nicht getestet.

- **Ursache**

In Windows gelten die folgenden Zeichen sowie alle Leerzeichen als Sonderzeichen und führen dazu, dass die Eingabe des Kennworts fehlschlägt, wenn das Kennwort nicht in Anführungszeichen eingeschlossen ist:

, & ' < > ; {} caret "

- **Korrekturmaßnahmen**

Wenn ein Passwort Leerzeichen oder Sonderzeichen enthält, setzen Sie es in doppelte Anführungszeichen (" "), wenn Sie es in verwenden smis Befehl. Beachten Sie, dass das Anführungszeichen (") ein Sonderzeichen ist und niemals in Ihrem Kennwort verwendet werden darf.

Kennwörter mit Sonderzeichen ausstellen

```
smis add 1.2.3.4 Administrator "pass word"
```

```
smis add 1.2.3.4 Administrator "pass&word"
```

Im SMI-S Provider verwendete Klontechnologie

Zum Erstellen von LUN-Klonen müssen Sie eine FlexClone Lizenz für SMI-S Provider besitzen.

SMI-S Provider erstellt LUN-Klone auf diesem Storage-System nur mithilfe von FlexClone Technologie. Wenn Sie keine FlexClone Lizenz haben, generiert SMI-S Provider keine Klone mithilfe der LUN-Klontechnologie und erzeugt die folgende Fehlermeldung:

```
FlexClone license is not enabled on the storage system.
```

Wenn Sie LUN-Klone haben, die mit LUN-Klontechnologie erstellt wurden und die Data ONTAP-Version dann auf 7.3.1 oder höher aktualisiert wird, können Sie diese Klone nicht mit SMI-S-Provider aufteilen. Sie müssen vom Administrator des Storage-Systems gemanagt werden.

Die Sichtbarkeit wichtiger Objekte bestätigen

Nach dem Hinzufügen eines gemanagten Storage-Systems sollten Sie bestätigen, dass alle wichtigen logischen und physischen Objekte im NetApp SMI-S Provider angezeigt werden.

Sie können das verwenden `smis` Befehl zum Anzeigen der Objekte im NetApp SMI-S Provider CIMOM Repository. Verwenden Sie beispielsweise `smis list` Um hinzugefügte Speichersysteme anzuzeigen, und verwenden `smis luns` Um LUN-Informationen anzuzeigen.

Anforderung für die Verwendung von Dateiservern unter Windows

Bei der Verwendung von fileshares (CIFS Shares) unter Windows muss das Volumen, auf dem der Dateifreigabeshare erstellt wird, ein NTFS-only Volume sein.

Wenn Sie einen Dateifreigabeshare erstellen und auf Windows verwenden möchten, muss das Volumen, auf dem der Dateifreigabeshare erstellt wird, ein NTFS-only-Volume sein. Dadurch werden Probleme mit den Anmeldeinformationen, die auf die Dateifreigabe zugreifen, vermieden.

Mit System Center 2016 Virtual Machine Manager (SCVMM) können Sie virtuelle Maschinen (VMs) nur auf File-Haes erstellen, die auf rein NTFS-basierten Volumes erstellt wurden. Gemischte und UNIX-artige Volumes werden nicht unterstützt.

Erstellen eines Volumes für CIFS-Freigaben und SCVMM

Wenn ein Volume erstellt wird, das für CIFS Shares und System Center Virtual Machine Manager (SCVMM) verwendet werden soll, muss es sich um den NTFS-Typ handeln. Geben Sie zum Erstellen des Volumes mit NTFS Folgendes ein: `vol create -vserver <vserver_name> -volume <volume_name>`

```
-aggregate <aggr_name> -size<volume_size> -security-style ntfs
```

Nicht standardmäßige Firewalls müssen Ports manuell als Ausnahmen hinzugefügt werden

- **Ausgabe**

Wenn Sie eine andere Firewall als die standardmäßige Windows-Firewall verwenden, treten möglicherweise die folgenden Probleme auf:

- SMI-S Provider kann nicht mit einem entfernten SMI-S-Client kommunizieren.
- Der SMI-S-Client kann keine Hinweise vom SMI-S-Provider empfangen.

- **Ursache**

Dieses Problem tritt auf, wenn Sie eine andere Firewall als die standardmäßige Windows-Firewall verwenden, ohne zuvor die erforderlichen Ports manuell als Ausnahmen hinzuzufügen.

- **Korrekturmaßnahmen**

Fügen Sie Ports 427, 5988 und 5989 als Ausnahmen zu Ihrer Firewall hinzu.

Es kann kein Speichersystem mit einem nicht standardmäßigen HTTP- oder HTTPS-Port hinzugefügt werden

- **Ausgabe**

Sie können kein Speichersystem hinzufügen, auf dem HTTP oder HTTPS auf einem nicht standardmäßigen Port ausgeführt werden.

- **Ursache**

Standardmäßig verwendet NetApp SMI-S Provider Port 80 für die Kommunikation mit Speichersystemen über HTTP und Port 443 zur Kommunikation über HTTPS.

- **Korrekturmaßnahmen**

Verwenden Sie den folgenden Befehl, um ein Speichersystem hinzuzufügen, das einen anderen Port als 80 für HTTP-Datenverkehr oder Port 443 für HTTPS-Datenverkehr verwendet:

```
cimcli ci -n root/ontap ONTAP_FilerData hostName=storage_sys_ip_address  
port=non_default_port userName=storage_sys_user password=storage_sys_pwd  
comMechanism=HTTP -u agent_user -p agent_pwd-llocalhost:5989 -s
```

-u, -p, -l, und -s Sind optionale Parameter.

Hinzufügen eines Speichersystems, das Port 8000 für HTTP-Datenverkehr verwendet

```
cimcli ci -n root/ontap ONTAP_FilerData hostName=10.60.167.12 port=8000
userName=root password=netappl! comMechanism=HTTP -u root -p netappl! -l
localhost:5989 -s --timeout 180
```

Keine Antwort vom Server

- **Ausgabe**

Der Server reagiert nicht bei Abfrage.

- **Ursache**

Dieses Problem tritt auf, wenn dem CIMOM-Repository kein Speichersystem hinzugefügt wird.

- **Korrekturmaßnahmen**

Geben Sie den folgenden Befehl ein, um sich zu vergewissern, dass ein Storage-System hinzugefügt wurde:

```
smis list
```

Wenn kein Storage-System aufgeführt ist, fügen Sie ein Storage-System hinzu, indem Sie den folgenden Befehl eingeben:

```
smis add storage_sys storage_sys_user storage_sys_pwd
```

Probleme mit der Laufzeitbibliothek

- **Ausgabe**

Es treten Probleme mit der Laufzeitbibliothek auf.

- **Korrekturmaßnahmen**

Installieren Sie das Microsoft Visual C++ 2010 Redistributable Package (x86) von www.microsoft.com.

Der NetApp SMI-S Provider kann sehr lange gestartet werden

- **Beschreibung**

Bei Windows-Systemen mit bereits zu managenden Storage-Systemen, wenn Sie NetApp SMI-S Provider über die starten `smis cimserver` Der Befehl wird erst zurückgegeben, wenn der lokale Cache des Providers mit Daten gefüllt ist. Er wartet maximal 15 Minuten, während der Cache gefüllt ist, und Sie können NetApp SMI-S Provider erst verwenden, wenn er wieder zurückkehrt.

Verwenden der `smis cimserver` Der Befehl ist die empfohlene Methode zum Starten von NetApp SMI-S Provider.

Unstimmigkeiten beim Management des gesamten Speicherplatzes für einen Storage Pool (Volume)

- **Ausgabe**

Wenn Sie ein anderes Storage-Management-Tool wie FilerView verwenden, kann es zu einer anderen Größe kommen, die für den gesamten gemanagten Speicherplatz eines Speicherpools (Volume) gemeldet wird, als die vom SMI-S Provider zurückgegebene Größe.

- **Ursache**

Diese Diskrepanz ist möglich, da die vom SMI-S Provider zurückgegebene Größe die WAFL und Snapshot Reserve enthält, während FilerView und andere Tools nur den nutzbaren Speicherplatz zeigen (ohne WAFL und Snapshot Reserve).

- **Korrekturmaßnahmen**

Dies ist ein erwartetes Verhalten, keine Korrekturmaßnahmen.

Der Netzwerkpfad wurde nicht gefunden

- **Nachricht**

```
Network path not found
```

- **Beschreibung**

Diese Meldung spiegelt ein DNS-Problem wider und tritt während der VM-Bereitstellung auf einer SMB-Freigabe auf, wenn der Host keinen Eintrag auf dem DNS-Server hat.

Normalerweise sollte der Domain-DNS-Server den Hostdatensatz innerhalb von 24 bis 48 Stunden automatisch aktualisieren, wenn ein neuer Host in der Domäne konfiguriert ist. Dieses Update geschieht jedoch nicht immer automatisch.

- **Korrekturmaßnahmen**

- Wenn Sie ein Domänenadministrator sind, aktualisieren Sie den DNS-Hostdatensatz manuell.
- Wenn Sie kein Domänenadministrator sind, aktualisieren Sie die Hostdatei (C:\Windows\System32\drivers\etc\hosts).

Die Host-Datei hat keine Dateierweiterung (.txt).

Es sind nicht genügend Systemressourcen vorhanden, um den angeforderten Service abzuschließen

- **Nachricht**

```
Insufficient system resources exist to complete the requested service
```

- **Beschreibung**

Diese Meldung tritt auf, wenn die maximale Obergrenze für Benutzersitzungen vom gleichen Benutzer pro Verbindung erreicht wurde, wenn eine große Anzahl von VMs auf einer einzelnen Dateifreigabe in SCVMM bereitgestellt wurde.

SCVMM erstellt eine TCP-Verbindung pro Hyper-V-Host, und jede Verbindung erstellt zahlreiche Sitzungen mit zwei Benutzern: Den Computernamen (COMPUTERGELD) des Hyper-V-Hosts und den SCVMM „run as Account“. Die Anzahl der Sitzungen mit COMPUTER-Kosten ist genau eine größer als die Anzahl der virtuellen Festplatten, die auf diesem Hyper-V Host bereitgestellt werden.

Der Standardwert von `Max Same User Session Per Connection` ist 50. Diese Einschränkung blockiert die Implementierung großer VMs mit SCVMM. Wenn Sie mehr als 50 VMs pro Hyper-V Host bereitstellen, tritt dieses Problem auf.

- **Korrekturmaßnahmen**

Erhöhen Sie den Zähler, der die maximale Anzahl von Sitzungen auf derselben Verbindung für das CIFS-Protokoll steuert. Mit dem folgenden Befehl werden beispielsweise die maximalen Benutzersitzungen in derselben Verbindung von der Standardeinstellung 50 auf 100 geändert:

```
SVM::*> cifs op modify -max-same-user-sessions-per-connection 100
```

Die Größe der SMB-Freigabe wird in SCVMM auf 0 verkleinert

- **Ausgabe**

Neue oder bestehende Größe von SMB 3.0-Shares kann im System Center Virtual Machine Manager (SCVMM) auf 0 sinken.

- **Ursache**

Dieses Problem tritt auf, wenn die Neuinitialisierung von Kontingenten aufgrund starker I/O-Vorgänge sehr lange in Data ONTAP dauert, können neue oder bestehende SMB 3.0-Share-Größe in SCVMM auf 0 sinken. Daher können neue VMs nicht auf den neuen oder vorhandenen SMB 3.0 Shares bereitgestellt werden.

- **Korrekturmaßnahmen**

- a. Deaktivieren Sie die Quoten.
- b. Fügen Sie auf jedem Volume, das SMB-Freigaben hostet, eine Standard-Kontingentregel vom Typ „Tree“ hinzu.
- c. Aktivieren Sie die Quoten für die Volumes, zu denen Sie eine Standard Quota Rule hinzugefügt haben, und starten Sie SMI-S Provider neu.

Der SCVMM-Scan-Vorgang konnte nicht gefunden oder mit SMI-S-Provider kommunizieren

- **Ausgabe**

In seltenen Fällen kann SCVMM SMI-S Provider nicht finden.

- **Ursache**

Dieses Problem kann auftreten, wenn die Sicherheitsinfrastruktur mit den neuen Gruppenrichtlinienobjekten aktualisiert wird. Wenn sie nach dem Neustart des SMI-S Provider-Hosts wirksam werden, kann es sein, dass der SCVMM-Host dem SMI-S-Provider oder dem Host nicht vertraut.

- **Korrekturmaßnahmen**

- a. Deinstallieren Sie SMI-S Provider, und installieren Sie ihn erneut.
- b. Führen Sie den Scan-Vorgang in SCVMM für den SMI-S Provider aus.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

<http://www.netapp.com/us/legal/copyright.aspx>

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

<https://www.netapp.com/us/media/patents-page.pdf>

Datenschutzrichtlinie

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Hinweis

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

["Hinweis für NetApp SMI-S Provider"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.